FireEye Cyber Defense Summit 2017

Creative Red Teaming (2 days)

As cyber security professionals and technologies continue to evolve and become better at prevention, detection, and remediation, attackers are forced to continually evolve their Tools, Tactics, and Procedures (TTPs) to remain effective. This is especially true with the most advanced attack groups operating that need to remain undetected for extended periods of time to effectively accomplish their mission. Mandiant is on the front lines investigating these types of breaches. This gives us unparalleled access to understand not only how advanced attackers operate and what TTPs they're leveraging, but also what attack methodologies are most effective across industries.

Standard red team classes teach students how to run vulnerability scans, Nmap, Metasploit and other commercial tools to obtain domain administrator access. This class covers the important open source tools required to perform a red team assessment, but more importantly, teaches you how to be creative and "live off the land" by using native tools to accomplish the same goals without getting caught. Getting domain admin is just par for the course, we go deeper into accomplishing objectives that prove big impact to clients. For example, if your client is a big retailer and you got access to their retail network where they store encrypted credit card numbers, we teach you how to go the extra mile and understand how applications encrypt that data. If an application can decrypt credit card numbers, we teach you how to analyze code to decrypt data as well. This not only proves you can get an initial vector, escalate privileges, bypass firewalls to get access to secure networks, but also weaknesses in how they encrypt their sensitive data…and that's just one example!

This intense two-day course is designed to teach advanced offensive techniques to provide you with the ultimate skillset to test your existing security controls. You will learn proven Mandiant Red Team methodologies that start with the successful TTPs we see used by advanced attackers and builds upon them to be even more effective and stealthy. You will even learn how to successfully complete your mission even if part of your team is caught. This course makes heavy use of labs so that you get to practice everything you learn in a realistic scenario. By learning how to implement and protect against effective TTPs you learn how to help your organization best prevent, detect, and respond to cyber threats.

Modules Included

- **Overview and Introduction** – Covers the basics required to proceed through the course.
- **OSINT, Initial Vectors, and Bypassing Anti-Virus (AV)** – Learn how to identify your target, fingerprint your target, initially compromise your target, and how to bypass AV to avoid detection when executing your initial payloads.
- **Persistence** – Covers older techniques and the latest techniques to persist your target. Does not just cover host based persistence, but also creative ways to persistence networks without a host and privileges.
- **Privilege Escalation and Lateral Movement** – Tools and methodologies that take the lowest privileged user and escalate to high privilege user while covertly moving through your target network. Covers both local and domain privilege escalation.
- **Overcoming Challenges** – Will teach you have to avoid and bypass various challenges such as application whitelisting, encryption, multi-factor authentication, sandboxes, and more.

- **Completing the Mission** – learn how to covertly take data off the network in a secure fashion and moving pivoting through firewalls to take data off "secure" networks.
- **Project Management** – Understand how to setup and manage projects, measuring risk, the reporting process, and rules of engagement.

What Students Should Bring

This is a fast-paced technical course designed to provide hands-on experience conducting covert no-holds barred cyber-attack simulations to accomplish various objectives within in a corporate environment, similar to how an advanced adversary would perform. This course provides an opportunity to learn how real attackers conduct offensive operations, how we improve upon those operations, and to understand how to be creative with exiting technology to accomplish your goals. The content and pace is intended for students with a background in conducting penetration tests, security assessments, IT administration, and/or incident response.

Course Prerequisites

- Students must have working knowledge of the Windows Operating system, file systems, registry and use of the Windows command line.
- Students should have some experience with the following:
- Active Directory and basic Windows security controls; Common network protocols; Linux Operating Systems; Scripting languages such as PowerShell, Python, or Perl; Assessing web applications using the OWASP top 10.

What Students Should Bring

Laptop with a Kali Rolling virtual machine. Students must possess local administrator rights to their host OS and VMs and must be able to install software provided on a USB stick. Students must also have an Ethernet port, for laptops that don't have one, please bring an adapter. The course will provide the students with:

- Class handouts and slides
- A vulnerable virtual machine for some labs
- Thumb drive containing class materials, labs, and tools
- FireEye/Mandiant gear