SecureNinja
The Cybersecurity Experts

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Advanced Cyber War Boot Camp

COURSE DESCRIPTION

SecureNinja's (5) five-day Cyber War immersion course is heavily focused on advanced persistence and data exfiltration. Students will draw from the instructors extensive experience with multiple offensive groups (3-letter agencies, military, as well as groups from other nations) and this class covers a lot of the same things these groups wanted to learn as well as some new ways to do things (e.g. using Powershell or IPv6).

WHO WOULD BENEFIT

IT System Administrators, IT Security Professionals

PREREQUISITES

This class is designed for advanced penetration testers, red teams, and offensive cyber operations groups.

COURSE LENGTH

- 5 Days
- 40 Hours

FOLLOW ON COURSES

- Exploit Development Boot Camp
- Advanced Systems & Applications Attack & Defense

COURSE DETAILS

Day 1: Gaining Access From The Outside

- Identifying/Bypassing External Security Mechanisms
    - Load Balancers
    - Intrusion Prevention Systems
    - Web Application Firewalls
- Advanced Targeting & Exploitation
    - Email Address Harvesting
    - Client-Side Application Fingerprinting
    - Bypassing Anti-Virus
    - Dealing with Egress Filtering
    - Bypassing Authenticating Proxies

Day 2: Advanced Persistence

- Persistence with and without Metasploit (Windows 7/8)

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

    - Advanced Meterpreter Features
    - Writing Meterpreter Post Modules
    - Building your own implant (non-meterpreter custom backdoor)
- Advanced Tunneling (Windows 7/8)
    - Socks Tunneling
    - ICMP Tunneling
    - SSH Tunneling
    - IPV6 Tunneling
    - Direct Access

Day 3: Advanced Post-Exploitation & Data Exfiltration

- Data-Mining Windows 7/8
    - Stealing hashes, Kerberos tickets, and passwords
    - Stealing User Certificates
    - Finding and Stealing Critical Data
    - Attacking 2008/2012 Active Directory
    - Advanced Network Enumeration
    - Data-Mining 2008/2012 Active Directory with security settings enabled
    - Finding and attacking databases via Active Directory
- Attacking Sharepoint
    - Version fingerprinting, directory brute-forcing, password stealing
    - Frontpage Access Files, DLLs, Virtual Directories
    - File upload vulnerabilities, command-execution vulnerabilities

Day 4: Data Exfiltration and Powershell For Hackers

- Data Exfiltration
    - Aggregating files
    - Staging Serves
    - Dealing with network segmentation issues
- Post-Exploitation With Powershell
    - Host Enumeration
    - Privilege Escalation
    - Stealing passwords and hash dumping
    - Network Enumeration
    - Download your toolkit to multiple hosts and execute it remotely

Day 5: Cyber Operation

Get your sleep the night before, eat your Wheaties the morning of because you are about to participate in a Cyber Operation and it is gonna be intense! You will be tasked with finding and stealing data from a highly protected target network. You will be given a description of data that you must steal the target network that has a combination of hardened workstations (similar to a STIG), Anti-Virus and Host-Based Intrusion Prevention Systems. In addition to common technical challenges, there will be a wide range of environmental variables that I've experienced in real operations to make it as realistic as possible.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com