Who's watching your back?

Foundstone®
Professional Services A DIVISION OF McAFEE

Training Datasheet

Ultimate Hacking - Two-Day

Taking Hacking to a New Level

DURATION
- Two (2) Days

WHAT YOU'LL LEARN
- Learn how hackers and malicious intruders analyze and develop target vectors aimed at your critical assets
- Understand the strategy behind finding weaknesses before they become a security risk
- Learn the proven Foundstone Penetration Testing Methodology
- Develop the mindset of a malicious attacker and identify the true risk to your organization
- Use the tools and methodologies hackers use efficiently, in a controlled and safe environment
- Develop your own security toolkit from tried and tested tools

COURSE MATERIALS
- Student manual
- Class handouts
- Foundstone authored book
- Free Tools CD with course tools
- BackTrack3 - the top rated bootable Linux distribution
- Foundstone t-shirt

SUGGESTED NEXT COURSE(S)
- Ultimate Hacking Expert
- Ultimate Hacking Wireless
- Ultimate Web Hacking

Leaving your network vulnerable to exploits can be catastrophic; but learning how hackers and malicious intruders analyze and target your assets can give you a serious advantage in today's high-tech world. Evolving from the Ultimate Hacking education series, this revamped course is taking hacking to the next level with new modules, new exploits and new hacker techniques. The core of the course is the Foundstone Professional Services proven Penetration Testing Methodology, and as always, the course is taught by instructors that bring real-world penetration testing experience to the classroom. You'll learn step-by-step procedures for executing attacks; conducting penetration tests; blocking attacks on Internet and intranet networks and on host-level systems in our hands-on classroom environment. By learning how to leverage these security techniques and methodologies, you can actively defend your critical internal and external assets against malevolent threats.

Who Should Take This Class

System and network administrators, security personnel, auditors, and/or consultants concerned with network and system security should take this course. Basic UNIX and Windows competency is required for the course to be fully beneficial.

Level of Experience

1-3 years network security experience

Exercises

All topics are supported by hands-on exercises and labs specifically designed to increase knowledge retention. Classroom exercises provide the hands-on experience needed to secure an organization's Internet presence and internal network. Students learn how to identify, exploit, and resolve popular and lesser-known vulnerabilities in Windows and UNIX systems.

Course Outline: New Format & Material

Day 1 – Penetrating a Windows Environment

The day begins with enumeration of Windows operating systems and follows the hacker methodology, teaching students how to hack Windows operating systems from start to finish. This day will concentrate on a variety of common attacks, and students will learn how to penetrate Windows systems on internal networks. After gaining access to target systems, students will learn how to escalate their privileges in Windows using techniques applicable to common corporate environments. The day wraps up with a major hands-on Windows lab.

Introduction
- Hacker methodology
- Attack platforms & basic tools (XP, BT3, Cygwin, etc)

Module 1 – Windows
- Network enumeration - Resource kits, built in, etc.
- Host enumeration (Cain & Abel, LDAP browsers, Getmac, Sc, Nbtstat, Nbtenum, Dumpsec, etc.)
- Enumeration countermeasures
- Null Sessions and authenticated sessions
- Penetration - brute forcing (Hydra, SQL Ping 3, Brutus, etc.), exploitation (Metasploit and other frameworks)
- Penetration countermeasures

- ARP poisoning, sniffing, and Man-in-the-Middle attacks – Cain & Abel (VNC, RDP, MSSQL, HTTP/HTTPS, etc.), Wireshark, Berkley Packet Filter notation, countermeasures
- Privilege escalation attacks – Shatter attacks, DLL injection, client side attacks, WMI
- Privilege escalation countermeasures
- Pillaging – disabling antivirus, Pwdumpx, LSAdump, Cachedump, Creddump, etc
- Password cracking/recovery - John the Ripper, Cain & Abel, lcp, rainbow tables, etc
- Pillaging countermeasures
- Getting interactive – netcat, psexec, osql, etc
- Getting interactive countermeasures
- Expanding influence – LSA secrets, pass the hash tool (gsecdump, msvctl, pshtoolkit), trojans, rootkits (Hacker defender FUtoo, etc), call hooking, key loggers, port redirection (Fpipe)
- Expanding influence countermeasures
- Cleanup - covering tracks (logs, a/v, users)
- Cleanup countermeasures

Windows Lab

The day ends with a hands-on lab involving the students hacking their way into the Hacme Corporation Windows Environment. Using the Foundstone hacking methodology, students will start off by enumerating the Windows systems and hack their way from one machine to another until ultimately owning the prized backend systems. This lab is modeled after real-world corporate environments and takes several hours to complete.

Day 2 – Penetrating a UNIX Environment

Day two focuses on the hacker methodology as it applies to UNIX/Linux systems. Students will learn how to hack UNIX/Linux operating systems from start to finish. The lecture and hands-on opportunities will teach students common techniques for hacking (and securing) UNIX-based systems.

Module 2 – UNIX

- Overview of UNIX/Linux – distributions, differences, defaults
- Enumeration – NFS, RPCs
- Enumeration countermeasures
- Penetration – brute forcing (Hydra), remote exploits (X server, buffer overflows, RPC exploits, etc), physical attacks, etc
- Penetration countermeasures
- Privilege escalation attacks – local exploits (file permissions, sudo, cron), misconfigurations
- Privilege escalation countermeasures
- Pillaging – password cracking, rainbow tables
- Pillaging countermeasures
- Getting interactive – netcat, xterm, reverse telnet, Metasploit Meterpreter, covert channels
- Getting interactive countermeasures
- Expanding influence – trojans (SSHeater), rootkits, key loggers, port redirection (Datapipe), network mapping
- ARP poisoning, sniffing, and Man-in-the-Middle attacks – Cain & Abel, Dsniff, Driftnet, Wireshark, Berkley Packet Filter notation, countermeasures
- Cleanup - covering tracks (log cleaning)
- Cleanup countermeasures

Ultimate Lab

The day ends with a major, challenging lab requiring the students to use the hacker methodology as they hack their way through all the lab servers. This Ultimate Lab consists of mostly UNIX-based systems (and a few Windows 2003 servers), and is modeled after the common case scenario of limited but exploitable default system installations and misconfigurations found in today's UNIX systems and variants. Students will need to attack these systems using exploits for vulnerabilities encountered in real-world penetration tests.