

Who's watching your back?

**Foundstone**<sup>®</sup>  
Professional Services A DIVISION OF McAfee

## Training Datasheet

# Ultimate Hacking

## Taking Hacking to a New Level

### DURATION

- Four (4) 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 mind set 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 and scripts
- BackTrack3 the top rated bootable Linux distribution
- Foundstone T-shirt
- Foundstone tote bag

### SUGGESTED NEXT COURSE(S)

- Ultimate Hacking Expert

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 exclusively by Foundstone Consultants who 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 highly acclaimed 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 net-

work. 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 – Information Gathering & Scanning

On the first day, students adopt the mind set of an external attacker scoping out the target corporation and identifying holes in the company's Internet accessible systems. Emphasis is placed on the proven methodology developed by Foundstone Consultants in the field. Following the methodology, the lecture and mini labs concentrate on the initial steps from an external perspective of network penetration testing.

#### Introduction

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

#### Module 1– Footprinting

- Publicly available info
- whois/ARIN lookups
- Reverse lookups
- Google hacking

#### Module 2 – Scanning

- Host discovery – nmap, xprobe, superscan/scanline
- Service discovery – nmap, superscan/scanline, snmp
- Service versioning – nmap, httpprint
- netcat, openssl
- Vulnerability scanning – Nikto, Nessus

### Scanning Lab

This mini lab requires the student to use the tools and techniques taught on day one to footprint and scan Foundstone's Hacme corporate network. The mini lab consists of a wide variety of machines on the Internet (Windows XP, Windows 2003, Linux, Solaris, etc.). These machines are specifically made available to the class for the purpose of running live scans. This lab gives students the opportunity to run the tools in a realistic manner against live machines on the student network.

### Day 2 – Penetrating the External Network

Day two focuses on hacking from an external perspective. After all necessary information gathering and scanning are complete: the attacker's focus shifts towards hacking available web applications and backend servers. Emphasis is placed on Foundstone's Web Application Penetration Testing methodology - a proven web hacking methodology used by Foundstone consultants in the field. Students will find multiple opportunities for hands on experiences interwoven into this lecture. After learning professional techniques for hacking web applications, the students will try their hands at hacking Foundstone's Hacme Casino.

### Module 3 – External Perspective

- Overview of E-commerce Architectures
- HTTP/HTTPS primer
- Authentication - HTTP basic, form based, common vulnerabilities
- Authentication best practices
- Authorization - direct browsing, vertical/horizontal privilege escalation
- Authorization best practices
- Session handling - cookies
- Session handling best practices
- Data validation - parameter manipulation, XSS, CSRF, SQL Injection, etc
- Data validation best practices
- OWASP Top Ten

### External Lab

The days ends with a hands-on lab requiring to perform a variety of attacks on Hacme Casino. Students will follow the methodology and employ the tools taught during the day in order to perform SQL Injection, XSS, CSRF, application logic, and other attacks. This external lab is modeled

after an online casino website and contains a variety of real world vulnerabilities commonly found in today's application.

### Day 3 – Penetrating a Windows Environment

Day three 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.

### Module 4 – 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 countermeasure
- ARP poisoning, sniffing, and Man-in-the-Middle attacks - Cain & Abel (VNC, RDP, MSSQL, HTTP/HTTPS, etc), Wireshark, Berkley Packet Filter
- Privilege escalation attacks - Shatter attacks, DLL injection, client side attacks, WMI
- Privilege escalation countermeasures
- Pillaging - disabling antivirus, Pwdumpx, LSAdump, Cacchedump, 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, msvct, 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
- gsecdump

### Windows Lab

The days ends with a hands-on lab involving the students hacking their way into the Hacme Corporation Windows Environment. Using the Foundstone hacking methodology, the 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 will take several hours to complete.

### Day 4 – Penetrating a Unix Environment

This day 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 5 – 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, eterm, 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 days 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 installation 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.