668 - Ethical Hacking and Countermeasures

Course Contents:

Introduction: The importance of security, The various phases involved in hacking, An overview of attacks and exploit categories, The legal implications.

Footprinting: Introduced to footprinting, Information gathering methodology, Tools used for the reconnaissance phase, countermeasures.

Scanning: Detecting 'live' systems on target network, Discovering services running/ listening on target systems, port scanning techniques, active and passive fingerprinting, Automated discovery tools.

Enumeration: Identifying valid user accounts or poorly protected resource shares, active connections to systems and directed queries, Null Session, NetBIOS Enumeration, SNMP enumeration, Applications and banners.

System Hacking: Remote password guessing, Eavesdropping, Denial of Service, Buffer overflows, Privilege escalation, Password cracking, keystroke loggers, sniffers, Remote control and backdoors, Port re direction, Covering tracks, Hiding files

Trojans and Backdoors: Defining Trojans and Backdoors, Understanding the various backdoor genre, Trojan tools, Prevention methods and countermeasures, Anti-Trojan software.

Sniffers: Active and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing and Spoofing.

Denial of Service: DOS and Distributed DOS Attacks, Types of denial of service attacks, Tools for running DOS attacks, Tools for running DDOS attacks, Denial of Service Countermeasures

Social Engineering: Common Types of Attacks, Online Social Engineering, Reverse Social Engineering, Policies and Procedures, Employee awareness.

Session Hijacking: Spoofing Vs Hijacking, Types of session hijacking, TCP/IP concepts, Performing Sequence prediction, ACK Storms, Session Hijacking Tools.

Web Server Hacking: Web Servers and Common Vulnerabilities, Apache Web Server Security, IIS Server Security, Attacks against Web Servers, Countermeasures

Web Application Vulnerabilities: Common Web Application Security Vulnerabilities, Penetration Methodologies, Input Manipulation, Authentication And Session Management, Tools and Countermeasures

Password cracking: HTTP Authentication Basic & Digest, NTLM Authentication, Certificate Based Authentication, Forms Based Authentication, Password Guessing, Password cracking Tools.

SQL injection: Exploiting the weakness of Server Side Scripting, Using SQL Injection techniques to gain access to a system, SQL Injection Scripts, Prevention and Countermeasures

Buffer Overflow: What is a Buffer Overflow, Exploitation, CPU / OS Dependency, Understanding Stacks, Stack Based Buffer Overflow, Defense against Buffer Overflows

Hacking wireless networks: Introduction to 802.1, WEP, Cracking WEP Keys, WLAN Scanners, WLAN Sniffers, Securing Wireless Networks.

Viruses: Types of viruses, virus signatures, Anti-virus software, few examples.

Linux Hacking: Scanning and mapping Networks, Password Cracking in Linux, Sniffing, Session Hijacking, Linux Rootkits, IP Chains and IP Tables, Linux Security Countermeasures

Evading Firewalls, IDS and Honeypots: Intrusion Detection System, Integrity Verifiers, Intrusions Detection, Anomaly Detection, Signature Recognition, Protocol Stack Verification, Application Protocol Verification, Hacking Through Firewalls, Honey Pots

Main Reading

1. "Hacking Exposed", Osborne/ Mc Graw Hill.
2. "Hacking Exposed: Network Security Secrets and solutions", Osborne/ Mc Graw Hill.
3. "Hacking Exposed: Linux Security Secrets and Solutions", Mc Graw Hill.
4. "Hacking Exposed: Windows Security Secrets and Solutions", Mc Graw Hill.
5. "Hacking Exposed: Web Application Security Secrets and Solutions", Mc Graw Hill/Osborne.

Supplementary Reading

1. Shon Harris, Allen Harper, Criss Eagle, Jonathan Ness , "Gray at Hacking – The Ethical Hacker's Handbook" , Mc Graw Hill.
2. Ryan Russel, Elias Levy, Jeremy Ruch & others, "Hack Proofing Your Network – Internet TradeCraft", SYNGRESS.
3. Mike Schiffman, "Hacker's Challenge: Test your Incident response Skills using twenty scenarios", Osborne/ Mc Graw Hill.