CYBER ZONE TECHNOLOGIES (P) LTD

AN ISO 9001 : 2008 CERTIFIED COMPANY

Vulnerability Assessment and Penetration Testing

Module 1: Vulnerability Assessment & Penetration Testing: Introduction

1.1 Brief Introduction of Linux
1.2 About Vulnerability Assessment and Penetration Testing
1.3 Cyber Zone Security Labs
1.4 Virtual Labs Overview and Implementation
1.5 Reporting

Module 2: Getting Comfortable with Linux and Windows

2.1Finding Your Way around Linux and Windows
- 2.1.1 Booting Up Linux and Windows
- 2.1.2 The Linux Menu& Commands
- 2.1.3 Hands-on-Practice

2.2 Managing Linux Services and Password breaking
- 2.2.1 Root Passwordand Grub Password
- 2.2.2 SSH Service
- 2.2.3 HTTP Service
- 2.2.4 Hands-on-Practice

2.3 The Perl, Python Environment
2.4 Intro to Perl, python scripting
- 2.4.1 Practical Perl Usage – Practical
- 2.4.2 Practical Python Usage– Practical
- 2.4.3 Hands-on-Practice

Module 3: Network Essential Tools

3.1 Netcat
- 3.1.1 Connecting to a TCP/UDP Port
- 3.1.2 Listening on a TCP/UDP Port
- 3.1.3 Transferring Files with Netcat
- 3.1.4 RemoteAdministration with Netcat

3.1.5 Hands-on-Practice

3.2 Ncat

3.2.1 Hands-on-Practice

3.3 Sniffing

3.3.1 Vulnerable Protocols in a network

3.3.2 Wireshark, Cain and Abel

3.3.3 Configure Wireshark and Cain and Abel

3.3.4 Capturing Packets and analysis, Man-in-the middle attack, Stealing Passwords, Web Pages ,Spoofing Pages, ARP Spoofing

3.3.5 Hands-on-Practice

Module 4: Passive Information Gathering

4.1 Open Web Information Gathering

4.1.1 Google Hacking

4.1.2 Hands-on-Practice

4.2 Email Harvesting

4.2.1 Hands-on-Practice

4.3 Additional Resources

4.3.1 Passive Reconnaissance

4.3.2 Maltego

4.3.3 Hands-on-Practice

4.4 Recon-ng

Module 5: Active Information Gathering

5.1 DNS Enumeration

5.1.1 Interacting with a DNS Server

5.1.2 Automating Lookups

5.1.3 Forward Lookup Brute Force

5.1.4 Reverse Lookup Brute Force

5.1.5 DNS Zone Transfers

5.1.6 Relevant Tools in Linux and Windows

5.1.7 Hands-on-Practice

5.2 Ping Sweeping

5.3 Network Enumeration

5.4 Port Scanning

5.4.1 TCP CONNECT / SYN Scanning

5.4.2 UDP Scanning

5.4.3 Common Port Scanning Pitfalls

5.4.4 Port Scanning with Zenmap, masscan, Advanced Port Scanner

5.4.5 OS Fingerprinting

5.4.6 Banner Grabbing /Service Enumeration

Module 6: Network Vulnerability Scanning

Module 7: Multiple USB Boot and Fuzzing

Module 8: Buffer Overflow and Exploitation

8.5 Generating Shellcode with Metasploit
8.6 Getting a Shell
    8.6.1Hands-on-Practice
8.7 Improving the Exploit
    8.7.1 Hands-on-Practice

Module 9: Linux Buffer Overflow Exploitation

9.1 Setting Up the Environment
9.2 Crashing Crossfire
    9.2.1Hands-on-Practice
9.3 Controlling EIP
9.4 Finding Space for Our Shellcode
9.5 Improving Exploit Reliability
9.6 Discovering Bad Characters
    9.6.1Hands-on-Practice
9.7 Finding a Return Address
9.8 Getting a Shell
    9.8.1Hands-on-Practice

Module 10: Working with Exploits

10.1 Searching for Exploits
    10.1.1 Finding Exploits in Windows and Linux
    10.1.2 Finding Exploits on the Web
10.2 Customizing and Fixing Exploits
    10.2.1 Setting Up a Execution Environment
    10.2.2 Dealing with Various Exploits
    10.2.3 Hands-on-Practice

Module 11: Shell Exploitation

11.1 A Word About Anti-Virus Software
11.2 File Transfer Methods
    11.2.1 Introduction of Shell and Uses
    11.2.2 Uploading Files
    11.2.3 Hands-on-Practice

Module 12: Privilege Escalation

12.1 Privilege Escalation Exploits
    12.1.1 Local Privilege Escalation Exploit in Linux Example
    12.1.2 Local Privilege Escalation Exploit in Windows Example
12.2 Configuration Issues

12.2.1 Incorrect File and Service Permissions
12.2.2 Think Like a Network Administrator
12.2.3 Blocking of Ping Request
12.2.4 Disable Temporary Ping Request
12.2.5 Port Blocking
12.2.6 Blocking of Port on desired IP Address
12.2.7 Hands-on-Practice

Module 13: Client Side Attacks

13.1 Trick and Know Your Target System
13.1.1 Passive Client Information Gathering
13.1.2 Active Client Information Gathering
13.1.3 Social Engineering and Client Side Attacks
13.1.4 Hands-on-Practice

13.2 Java Signed Applet Attack
13.2.1 Hands-on-Practice

Module 14: Web Application Attacks

14.1 OWSAP TOP 10 Vulnerabilities
14.1.1 Injection
14.1.2 Broken Authentication and Session Management
14.1.3 Cross Site Scripting (XSS)
14.1.3.1 Hands-on-Practice
14.1.4 IDOR(Insecure Direct Object References)
14.1.5 Security Misconfiguration
14.1.6 Sensitive Data Exposure
14.1.7 Missing Function Level Access Control
14.1.7.1 Hands-on-Practice
14.1.8 Cross Site Request Forgery
14.1.9 Using Known Vulnerable Components
14.1.10 Unvalidated redirects and forwards
14.2 NIC Vulnerability
14.2.1 Malicious File Upload
14.2.2 No lockout & Password Policy
14.2.3 Directory Browsing
Hands-on-Practice
14.2.4 Password Auto Complete
14.2.5 Auto fill Feature
14.2.6 Audit Trail for Admin User
14.2.7 Click Jacking

14.2.8 HTTP Response splitting

14.3 Internet Information Service Attack

Module 15: Web Application Security Audit and Exploitation Tool

15.1 Acunetix Web Vulnerability Scanner

15.2 BurpSuite

15.3 Dirbuster

15.4 Havij

15.5 SQLMap

15.6 SQL Poizon

15.7 Hands-on-Practice

Module 16: Web Application Security Patching

16.1 Brief Introduction of Security Patching

16.2 Patching codes

16.3 Hands-on-Practice

Module 17: Password Breaking Attacks

17.1 Preparing for Brute Force

17.1.1 Dictionary Files

17.1.2 Brute Force Attack

17.1.3 Pwdump and Fgdump

17.1.4 Password Profiling

17.1.5 Hands-on-Practice

17.2 Offline-Online Password Attacks

17.2.1 Hydra, Medusa, and Cain and abel

17.2.2 Ophcrack

17.2.3 Syskey Password breaking

17.2.4 Hands-on-Practice

17.3 Password Hash Attacks

17.3.1 Password Hashes

17.3.2 Cain and abel

17.3.3 John the Ripper

17.3.4 Rainbow Tables Attack

17.3.5 By Passing Password using backdoor

17.3.6 Hands-on-Practice

Module 18: Proxy Server, Port Redirection and Tunneling

- 18.1 Port Forwarding and Redirection
  - 18.1.1 Local Port Forwarding
  - 18.1.2 Remote Port Forwarding
- 18.2 Introduction to Proxy and its Uses
- 18.3 Working with Proxy tool
- 18.4 IP-Port based Proxy
- 18.5 Web-based Proxy
- 18.6 Browser based Proxy
- 18.7 HTTP Tunneling
- 18.8 SSH Tunneling
- 18.9 Virtual Private Network
- 18.10 Hands-on-Practice

Module 19: Working with Metasploit Framework

- 19.1 Metasploit User Interfaces
- 19.2 Setting up Metasploit Framework on Linux
- 19.3 Exploring the Metasploit Framework
- 19.4 Auxiliary Modules
  - 19.4.1 Getting Familiarwith MSF Syntax
  - 19.4.2 Metasploit Database Access
  - 19.4.3 Hands-on-Practice
- 19.5 Exploit
  - 19.5.1 Hands-on-Practice
- 19.6 Metasploit Payloads
  - 19.6.1 Staged vs. Non-Staged Payloads
  - 19.6.2 Meterpreter Payloads
  - 19.6.3 Experimenting with Meterpreter
  - 19.6.4 Executable Payloads
  - 19.6.5 Reverse HTTPS Meterpreter
  - 19.6.6 Metasploit Exploit MultiHandler
  - 19.6.7 Revisiting ClientSide Attacks
  - 19.6.8 Hands-on-Practice
  - 19.6.9 Building Your Own MSF Module
  - 19.6.10 Hands-on-Practice
- 19.7 Post Exploitation with Metasploit
  - 19.7.1 Meterpreter Post Exploitation Features
  - 19.7.2 Post Exploitation Modules

Module 20: Using Metasploit To Bypass Antivirus

20.1 Generating Payloads with Metasploit
20.2 Working with Encoder
20.3 Working with Tools and Payloads
20.4 Software Protectors
20.5 Hands-on-Practice

Module 21: Reiteration in Steps: Vulnerability Assessment and Penetration Testing

21.1 Revisal of Vulnerability Assessment
21.2 Revisal of Penetration Testing

Module 22: Projects

22.1 Web Application vulnerability Audit
22.2 Website Penetration testing Project
22.3 Network Audit