WHAT IS A PENTESTER

Pentest Methodology

- Penetration Testing Execution Standard www.penteststandard.org
- Open Source Security Testing Methodology Manual (OSSTMM): www.isecom.org/OSSTMM.3.pdf
- NIST 800-115 (National Institute of Standards and Technology) https://csrc.nist.gov/pubs/sp/800/115/final
- OWASP Testing Guide (Open Web Application Security Project): www.owasp.org/images/1/19/OTGv4.pdf

The 7 sections of the PTES

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting

Pentest Types

- Black box
- White box
- Gray box

Vulnerability Scanning

- Nessus https://www.tenable.com/products/nessus
- Nexpose https://www.rapid7.com/products/nexpose/
- Openvas https://openvas.org/
- Qualys https://www.qualys.com/

PREREQUISITE SKILLS

Security Controls

- Administrative controls
- Logical controls
- Physical controls

Access Control

- Role-based Access Control
- Mandatory Access Control
- Discretionary Access Control

Incident Response

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-incident Activity

Cyber Kill Chain

1. Find
2. Fix
3. Track
4. Target
5. Engage
6. Assess

CVE-(four digit year)-(four digit number unique to the year)

Dark Web

- Tor
- I2P

EDUCATION RESOURCES

Pentesting Courses

- Online Training Companies SANSInstitute https://www.sans.org/emea/
- eLearnSecurity https://security.ine.com/
- Pentester Academy https://www.pentesteracademy.com/
- PentesterLab https://pentesterlab.com/

Pentesting Books

Penetration Testing: A Hands-on Introduction to Hacking (No Starch Press, 2014)

Penetration Testing for Dummies

Penetration Testing Essentials (Jones & Bartlett Learning, 2015)

The Hacker Playbook: Practical Guide to Penetration Testing Series

Tribe of Hackers Red Team: Tribal Knowledge from the Best in Offensive Cybersecurity

Penetration Testing: Security Analysis

Unauthorised Access: Physical Penetration Testing for IT Security Teams

Advanced Penetration Testing: Hacking the World's Most Secure Networks

Web Resources

- Daniel Miessler https://danielmiessler.com/
- Penetration Testing Lab https://pentestlab.blog/
- https://jhalon.github.io/becoming-a-pentester/

CERTIFICATIONS & DEGREES

Pentesting Certifications

Entry-Level Certifications

- EC-Council's Certified Ethical Hacker (CEH)
  - Introduction to Ethical Hacking
  - Footprinting and Reconnaissance
  - Scanning Networks
  - Enumeration
  - Vulnerability Analysis
  - System Hacking
  - Malware Threats
  - Sniffing
  - Social Engineering
  - Denial-of-Service
  - Session Hijacking
  - Evading IDS,Firewalls and Honeypots
  - Hacking Web Servers
  - Hacking Web Applications
  - SQL Injection
  - Hacking Wireless Networks
  - Hacking Mobile Platforms
  - IoT Hacking
  - Cloud Computing
  - Cryptography
- PenTest+
- eLearn Security Junior Penetration Tester
  - Getting Comfortable with Kali
  - Linux
  - Command Line Fun
  - Practical Tools
  - Bash Scripting
  - Passive Information Gathering
  - Active Information Gathering
  - Vulnerability Scanning
  - Web Application Attacks
  - Introduction to Buffer Overflows
  - Windows Buffer Overflows
  - Linux Buffer Overflows
  - Client-Side Attacks
  - Locating Public Exploits
  - Fixing Exploits
  - File Transfers
  - Antivirus Evasion
  - Privilege Escalation
  - Password Attacks
  - Port Redirection and Tunneling
  - Active Directory Attacks
  - The Metasploit Framework
  - PowerShell Empire
  - Assembling the Pieces:
  - Penetration Test Breakdown
  - Trying Harder: The Labs

Intermediate-Level Certifications:

- Offensive Security Certified Professional (OSCP)
- GIAC Penetration Tester

Advanced-Level Certifications

- Offensive Security Certified Expert (OSCE)
  - Cross Site Scripting Attacks
  - Directory Traversal / LFI Attacks
  - Backdooring PE Files
  - Advanced Exploitation Techniques
  - ASLR
  - Egghunters
  - Exploit Writing (Zero-Day Approach)
  - Attacking Network Infrastructure
  - Bypassing Cisco Access Lists Using •
  - Spoofed •SNMP Requests
  - Sniffing Remote Traffic via GRE tunnels
  - Compromising Router Configs
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

Specialization Web Application Pentesting Certifications

- GIAC Web Application Penetration Tester (GWAPT)
- eLearn Security Web Application Penetration Testing (eWAPT)
- Offensive Security Web Expert (OSWE):

Wireless Pentesting Certifications

- Offensive Security Wireless Professional
  - IEEE 802.11
  - Wireless Networks
  - Packets and Network Interaction
  - Linux Wireless Stack and Drivers
  - Aircrack-ng Essentials
  - Cracking WEP with Connected Clients
  - Cracking WEP via a Client
  - Cracking Clientless WEP Networks
  - Bypassing WEP Shared Key Authentication
  - Cracking WPA/WPA2 PSK with Aircrack-ng
  - Cracking WPA with JTR and Aircrack-ng
  - Cracking WPA with coWPAtty
  - Cracking WPA with Pyrit
  - Additional Aircrack-ng Tools
  - Wireless Reconnaissance
  - Rogue Access Points
- GIAC Assessing and Auditing Wireless Networks (GAWN)

Mobile Pentesting Certifications:

- Mobile Application Security and Penetration Testing (MASPT)
- GIAC Mobile Device Security Analyst (GMOB)

Certification Study Resource EC-Council

- Hacking Wireless Networks for Dummies
- CompTIA PenTest+ Study Guide
- CompTIA PenTest+ Website
- Cybrary's Advanced Penetration Testing course
- Linux Server Security: Hack and Defend

Advanced Penetration Testing: Hacking the World's Most Secure Networks

- Using Java applets for malware payload delivery
- How security operations centers work
- Windows PowerShell
- Hijacking DLLs
- North Korean networking technologies
- Asymmetric cryptography
- IDS evasion
- VBA attacks

The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws:

- HTML5 exploitation
- SQL injection
- HTTP parameter pollution
- Cross-domain integration techniques
- JavaScript exploitation

DEVELOPING A PLAN

- ☐ Windows
- ☐ Linux
- ☐ Networking
- ☐ Security
- ☐ Scripting
- ☐ Active Directory (AD)
- ☐ Web Technologies
- ☐ Wireless Technologies
- ☐ Internet of Things (IoT)
- ☐ Hacking
- ☐ Web Hacking
- ☐ Wireless Hacking
- ☐ Social Engineering
- ☐ Physical Pentesting
- ☐ Android
- ☐ iOS
- ☐ macOS
- ☐ Firewall Configuration
- ☐ Python
- ☐ Java
- ☐ Reverse Engineering
- ☐ Antivirus
- ☐ Firewalls
- ☐ Critical Thinking
- ☐ Talking to Businesspeople
- ☐ Empathizing with End Users
- ☐ Creativity
- ☐ Perseverance

EDUCATION OF A HACKER

Pentester Blueprint Formula

Technology Knowledge
+
Hacking Knowledge
+
Hacker Mindset

Pentester Blueprint Formula

Types of Pentesting

- Black Box Testing
- White Box Testing
- Gray Box Testing

BUILDING A LAB

Hacking Systems

- TrustedSec www.trustedsec.com
- FireEye's Commando VM script

Popular Pentesting Tools

Kali Linux
Nmap
Wireshark

Vulnerability Scanning Applications:

https://www.metasploit.com/
https://www.tenable.com/
www.openvas.org
https://shop.hak5.org/

Hacking Targets

- PentestBox https://pentestbox.org/
- VulnHub https://www.vulnhub.com/
- https://www.offsec.com/labs/

GAINING EXPERIENCE

Capture the Flag

Bug Bounties

- Bugcrowd https://www.bugcrowd.com/
- Hackerone https://www.hackerone.com/
- Synack https://www.synack.com/

A PENTESTER BLUEPRINT V 1.0

Resource : The Pentester BluePrint: Starting a Career as an Ethical Hacker Paperback – 4 January 2021 by Phillip L. Wylie (Author), Kim Crawley (Author)

HACKMYBOX.COM