Course 2: Surveying the Target

Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001)

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Scanning and Enumeration

Episode 1

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

PENTEST+ EXAM OBJECTIVES

DOMAIN	PERCENTAGE OF EXAM
1.0 Planning and Scoping	15%
2.0 Information Gathering and Vulnerability Identification	22%
3.0 Attacks and Exploits	30%
4.0 Penetration Testing Tools	17%
5.0 Reporting and Communication	16%
TOTAL	**100%**

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

INFORMATION GATHERING

- Scanning
  - Process of looking at some number of “things” to determine characteristics
  - Commonly used in pen testing to uncover target vulnerabilities
- Many types of scan targets
  - Networks
  - Network devices
  - Computers
  - Applications/services

2.1 Given a scenario, conduct information gathering using appropriate techniques
2.1.1 Scanning

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

ENUMERATION

- Counting the detected instances of some target class
- Pen testing target classes
  - Hosts
  - Networks
  - Domains
  - Users
  - Groups
  - Network shares
  - Web pages
  - Applications
  - Services
  - Tokens
  - Social networking sites

2.1.2 Enumeration
2.1.2.1 Hosts
2.1.2.2 Networks
2.1.2.3 Domains
2.1.2.4 Users
2.1.2.5 Groups
2.1.2.6 Network shares
2.1.2.7 Web pages
2.1.2.8 Applications
2.1.2.9 Services
2.1.2.10 Tokens
2.1.2.11 Social networking sites

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Scanning and Enumeration Demo

Episode 2

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

SCANNING AND ENUMERATION DEMO – NMAP AND WHOIS

- Nmap demo
- Whois demo

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Packet Investigation

Episode 3

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

PACKET INVESTIGATION

- Packet crafting
  - Creating specific network packets to gather information or carry out attacks
  - Tools – netcat, nc, ncat, hping
- Packet inspection
  - Capturing and analyzing network packets
  - Wireshark

2.1.3 Packet crafting
2.1.4 Packet inspection

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

INSPECTING TARGETS

- Fingerprinting
  - Determining OS type and version a target is running
- Cryptography
  - Inspecting certificates

2.1.5 Fingerprinting
2.1.6 Cryptography
2.1.6.1 Certificate inspection

EAVESDROPPING

- RF communication monitoring
- Sniffing
  - Intercepting packets and inspecting their contents
  - Wired
    - Wireshark and tcpdump
  - Wireless
    - Aircrack-ng

2.1.7 Eavesdropping
2.1.7.1 RF communication monitoring
2.1.7.2 Sniffing
2.1.7.2.1 Wired
2.1.7.2.2 Wireless

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Packet Inspection Demo

Episode 4

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

PACKET INSPECTION DEMO

- Wireshark Demo

Application and Open-Source Resources

Episode 5

DECOMPILATION

- Compiler – translates source code into executable instructions
- Decomompiler – attempts to convert executable instructions back into source code
  - Output is generally awkward to read at best
- Sometimes target is not a direct executable (i.e. Java)

2.1.8 Decompilation
2.1.9 Debugging

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

DEBUGGING

- Running an executable in a controlled manner
- Debuggers make it easy to stop and examine memory at will
- Can reveal a program's secrets and weaknesses
- Tools - windbg

2.1.8 Decompilation
2.1.9 Debugging

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

OPEN SOURCE INTELLIGENCE GATHERING

- Open Source Intelligence Gathering (OSINT)
- Sources of research
  - CERT (Computer Emergency Response Team) - https://www.us-cert.gov/
  - NIST (National Institute of Standards and Technology) - https://csrc.nist.gov/
  - JPCERT (Japan's CERT) - https://www.jpcert.or.jp/english/vh/project.html

2.1.10 Open Source Intelligence Gathering
2.1.10.1 Sources of research
2.1.10.1.1 CERT
2.1.10.1.2 NIST
2.1.10.1.3 JPCERT

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

OPEN SOURCE INTELLIGENCE GATHERING, cont'd

- More sources of research
  - CAPEC (Common Attack Pattern Enumeration & Classification) - https://capec.mitre.org/
  - Full disclosure – Popular mailing list from the folks who brought us nmap - http://seclists.org/fulldisclosure/
  - CVE (Common Vulnerabilities and Exposures) - https://cve.mitre.org/
  - CWE (Common Weakness Enumeration) - https://cwe.mitre.org/

2.1.10.1.4 CAPEC
2.1.10.1.5 Full disclosure
2.1.10.1.6 CVE
2.1.10.1.7 CWE

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Vulnerability Scanning

Episode 6

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

VULNERABILITY SCAN

- Structured approach to examining targets to identify known weaknesses
- Many different types
- Determine if any known weaknesses exist

2.2 Given a scenario, perform a vulnerability scan.
2.2.1 Credentialed vs. non-credentialed

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

CREDENTIALED VS. NON-CREDENTIALED

- Credentialed (authenticated) – accessing resources using valid credentials
  - More detailed, accurate information
- Non-credentialed (non-authenticated) – anonymous access to exposed resources
  - Fewer details, often used in early phases of attacks/tests

2.2 Given a scenario, perform a vulnerability scan.
2.2.1 Credentialed vs. non-credentialed

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

TYPES OF SCANS

- Discovery scan – used to find potential targets
  - Identity/info gathering early on
  - nmap ping sweep
    - nmap –sP target

2.2.2 Types of scans
2.2.2.1 Discovery scan
2.2.2.2 Full scan
2.2.2.3 Stealth scan
2.2.2.4 Compliance scan

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

TYPES OF SCANS

- Full scan – scans ports, services, and vulnerabilities
  - Full scan with fingerprinting
    - nmap –A <target>
      - Not stealthy
    - perl nikto.pl –h <target>
    - OpenVAS
      - Open-source version of Nessus
- Port scan
  - nmap –p <ports> <target>v

2.2.2 Types of scans
2.2.2.1 Discovery scan
2.2.2.2 Full scan
2.2.2.3 Stealth scan
2.2.2.4 Compliance scan

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

TYPES OF SCANS

- Stealth scan – attempt to avoid tripping defensive control thresholds
  - nmap –sS <target>
- Compliance – scan for specific known vulnerabilities that would make a system non-compliant

2.2.2 Types of scans
2.2.2.1 Discovery scan
2.2.2.2 Full scan
2.2.2.3 Stealth scan
2.2.2.4 Compliance scan

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Vulnerability Scanning Demo

Episode 7

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

SCANNING DEMO

- Nmap
- Nikto
- OpenVAS

Scanning demo
Nmap
Nikto
OpenVAS

Target and Asset Considerations

Episode 8

CONTAINER SECURITY

- Container – scaled-down VM
- Instances that run on top of base OS VM
- Docker, Puppet, Vagrant
- Application scan
  - Dynamic – target environment is running and responds to queries
  - Static – scan input consists of post-execution data stores

2.2.3 Container security
2.2.4 Application scan
2.2.4.1 Dynamic vs. static analysis

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

SCANNING CONSIDERATIONS

- Time to run scans – approved schedule (planning)
- Protocols used – largely dependent on target selection
- Network topology – network layout (diagram) of test targets
- Bandwidth limitations – tolerance to impact (affects availability)

2.2.5 Considerations of vulnerability scanning
2.2.5.1 Time to run scans
2.2.5.2 Protocols used
2.2.5.3 Network topology
2.2.5.4 Bandwidth limitations
2.2.5.5 Query throttling
2.2.5.6 Fragile systems/non-traditional assets

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

SCANNING CONSIDERATIONS

- Query throttling – slow down test iterations to avoid exceeding bandwidth
  - nmap -T
- Fragile systems/non-traditional assets
  - How to avoid impacting fragile mission critical systems?

2.2.5 Considerations of vulnerability scanning
2.2.5.1 Time to run scans
2.2.5.2 Protocols used
2.2.5.3 Network topology
2.2.5.4 Bandwidth limitations
2.2.5.5 Query throttling
2.2.5.6 Fragile systems/non-traditional assets

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

ANALYZE SCAN RESULTS

- Asset categorization
  - Identify and rank assets by relative value
  - Vulnerable assets with little value could be a waste of time
- Adjudication
  - Determine which results are valid
    - False positives
    - Filter out false positives

ANALYZE SCAN RESULTS, cont'd

- Prioritization of vulnerabilities
  - Highest impact vulnerabilities - ease of exploit vs. payoff
- Common themes
  - Vulnerabilities
  - Observations
  - Lack of best practices

2.3.3 Prioritization of vulnerabilities
2.3.4 Common themes
2.3.4.1 Vulnerabilities
2.3.4.2 Observations
2.3.4.3 Lack of best practices

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Nmap Timing and Performance Options

Episode 9

SCANNING DEMO

- Nmap demo

Nmap demo

Prioritization of Vulnerabilities

Episode 10

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

LEVERAGE INFORMATION

- Leveraging information to prepare for exploitation
- Map vulnerabilities to potential exploits
  - Look up vulnerabilities found for possible exploits
  - Nmap – vulners and vulscan scripts
  - Metasploit (search vulnerability)

2.4 Explain the process of leveraging information to prepare for exploitation.
2.4.1 Map vulnerabilities to potential exploits
2.4.2 Prioritize activities in preparation for penetration test
Demo

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

LEVERAGE INFORMATION

- Prioritize activities in preparation for penetration test
  - Will standard exploits work?
  - Will exploits need to be 'tweaked'?
  - Additional steps to prepare test?

2.4 Explain the process of leveraging information to prepare for exploitation.
2.4.1 Map vulnerabilities to potential exploits
2.4.2 Prioritize activities in preparation for penetration test
Demo

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

DEMO

- Demo
- https://null-byte.wonderhowto.com/how-to/easily-detect-cves-with-nmap-scripts-0181925/

Demo

Common Attack Techniques

Episode 11

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

COMMON ATTACK TECHNIQUES

- Cross-compiling code – compile exploit for another OS
  - Some Windows exploits can be compiled to run in Linux
  - https://www.hackingtutorials.org/exploit-tutorials/mingw-w64-how-to-compile-windows-exploits-on-kali-linux/
- Exploit modification - may need to modify for success of evasion
- Exploit chaining - compromise one device/system to gain access to another
- Proof-of-concept development - exploit development

2.4.3 Describe common techniques to complete attack
2.4.3.1 Cross-compiling code
2.4.3.2 Exploit modification
2.4.3.3 Exploit chaining
2.4.3.4 Proof-of-concept development (exploit development)

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

COMMON ATTACK TECHNIQUES

- Social engineering
  - Help me
  - Urgent
  - Deceptive
- Credential brute forcing
- Enlightened Attacks
  - Dictionary
  - Rainbow table

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Credential Attacks

Episode 12

DEMO – PASSWORD CRACKING

- Demo – Hydra
- Bad usernames and passwords
  - Daniel Miessler's SecLists - https://github.com/danielmiessler/SecLists/tree/master/Passwords

Demo - Hydra

Weaknesses in Specialized Systems

Episode 13

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

WEAKNESSES IN SPECIALIZED SYSTEMS

- ICS (Industrial Control Systems)
  - Environmental conditions
  - Exposure to real world (live) events
- SCADA (Supervisory Control and Data Acquisition)
- Mobile – lack of updates, compromised settings, dangerous apps, etc.
- IoT (Internet of Things) – default (weak) security (wide open)
- Embedded
  - Computers embedded in other systems – IoT, automobiles, industrial devices, etc.

2.5 Explain weaknesses related to specialized systems
2.5.1 ICS
2.5.2 SCADA
2.5.3 Mobile
2.5.4 IoT
2.5.5 Embedded

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

WEAKNESSES IN SPECIALIZED SYSTEMS

- Point-of-sale system
  - Attractive due to connection to payment devices (cash, readers, etc.)
- Biometrics – accuracy is still evolving
  - What if primary reader fails to detect?
  - What is the manual process?

2.5.6 Point-of-sale system
2.5.7 Biometrics
2.5.8 Application containers
2.5.9 RTOS

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

WEAKNESSES IN SPECIALIZED SYSTEMS

- Application containers
  - Containers and VMs are not foolproof sandboxes
  - Compromising (breaking out) may allow access to external resources
- RTOS (Real-time operating system)
  - Designed to provide fast, lightweight services, not security

2.5.6 Point-of-sale system
2.5.7 Biometrics
2.5.8 Application containers
2.5.9 RTOS