Course: 5 Selecting Pen Testing Tools

CompTIA PenTest+ Exam (PT0-001)

SAGEFOX

Nmap Scoping and Output Options

Episode 1

SAGEFOX

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

NMAP

- Nmap (Network Mapper)
  - One of the most common and most useful tools for reconnaissance
  - nmap –A does much of what we're about to see

4.1 Given a scenario, use Nmap to conduct information gathering exercises
4.1.1 SYN scan (-sS) vs. full connect scan (-sT)

Nmap cookbook http://index-of.es/Networking/Nmap_cookbook-the-fat-free-guide-to-network-scanning.pdf

SYN SCAN vs. FULL CONNECT SCAN

- SYN (stealth) scan
  - nmap –sS target
  - Sends SYN packet and examines response (SYN/ACK means the port is open)
  - If SYN/ACK received, nmap sends RST to terminate the connection request
- Full connect scan
  - nmap –sT target
  - Completes the handshake steps to establish a connection (more reliable)

4.1 Given a scenario, use Nmap to conduct information gathering exercises
4.1.1 SYN scan (-sS) vs. full connect scan (-sT)

Nmap cookbook http://index-of.es/Networking/Nmap_cookbook-the-fat-free-guide-to-network-scanning.pdf

PORT SELECTION (-p)

- Scans a range of ports nmap-p <range of ports> target
  - -p 21
  - -p 1-10000
  - -p U:53,137,161T:21-37,80,8080
  - OR –exclude-port <range of ports>

4.1.2 Port selection (-p)
4.1.3 Service identification (-sV)

SERVICE IDENTIFICATION (-sV)

- Service identification (-sV)
  - nmap –sV <target>
  - Attempts to determine service and version info
    - --version-intensity <level>, where level can be 0 (light) to 9 (execute all probes)

4.1.2 Port selection (-p)
4.1.3 Service identification (-sV)

GATHERING INFORMATION WITH NMAP

- OS fingerprinting (-O)
  - Detects target OS
  - nmap –O <target>
- Disabling ping (-Pn)
  - Skips host discovery (assumes all are online)
  - nmap –Pn <target>

4.1.4 OS fingerprinting (-O)
4.1.5 Disabling ping (-Pn)
4.1.6 Target input file (-iL)

GATHERING INFORMATION WITH NMAP

- Target input file (-iL)
  - Uses a text file that contains a list of targets
    - nmap –iL <inputFileName>
  - Can also exclude targets from a range
    - nmap –excludefile <excludeFileName>

4.1.4 OS fingerprinting (-O)
4.1.5 Disabling ping (-Pn)
4.1.6 Target input file (-iL)

TIMING (-T)

- Changes how long nmap waits for a response (default is –T 3)
  - Values range from 0 (Paranoid, slow) to 5 (Insane, fast)

4.1.7 Timing (-T)
4.1.8 Output parameters
4.1.8.1 -oA
4.1.8.2 -oN
4.1.8.3 -oG
4.1.8.4 –oX

See –oS (script kiddie format)

OUTPUT PARAMETERS

- -oA – Combined format
  - Normal .txt, XML .xml, and grepable .txt
- -oN
  - Normal output file (.nmap)
- -oG
  - Grepable output file (.gnmap)
- -oX
  - XML output format (.xml)

4.1.7 Timing (-T)
4.1.8 Output parameters
4.1.8.1 -oA
4.1.8.2 -oN
4.1.8.3 -oG
4.1.8.4 –oX

See –oS (script kiddie format)

Pen Testing Toolbox

Episode 2

SAGEFOX

RECONNAISSANCE

- For reconnaissance, use:
  - Nmap
  - Whois
  - Nslookup
  - Theharvester
  - Shodan
  - Recon-NG
  - Censys
  - Aircrack-NG
  - Kismet
  - WiFite
  - SET
  - Wireshark
  - Hping
  - Metasploit framework

4.2 Compare and contrast various use cases of tools
4.2.1 Use cases
4.2.1.1 Reconnaissance
4.2.1.2 Enumeration
4.2.1.3 Vulnerability scanning
4.2.1.4 Credential attacks

ENUMERATION

- To list targets, use:
  - Nmap
  - Nslookup
  - Wireshark
  - Hping

4.2 Compare and contrast various use cases of tools
4.2.1 Use cases
4.2.1.1 Reconnaissance
4.2.1.2 Enumeration
4.2.1.3 Vulnerability scanning
4.2.1.4 Credential attacks

VULNERABILITY SCANNING

- To scan for vulnerabilities, use:
  - Nmap
  - Nikto
  - OpenVAS
  - SQLmap
  - Nessus
  - W3AF
  - OWASP ZAP
  - Metasploit framework

4.2 Compare and contrast various use cases of tools
4.2.1 Use cases
4.2.1.1 Reconnaissance
4.2.1.2 Enumeration
4.2.1.3 Vulnerability scanning
4.2.1.4 Credential attacks

CREDENTIAL ATTACKS

- For offline password cracking, use:
  - Hashcat
  - John the Ripper
  - Cain and Abel
  - Mimikatz
  - Aircrack-NG

4.2 Compare and contrast various use cases of tools
4.2.1 Use cases
4.2.1.1 Reconnaissance
4.2.1.2 Enumeration
4.2.1.3 Vulnerability scanning
4.2.1.4 Credential attacks

CREDENTIAL ATTACKS

- For brute-forcing services, use:
  - SQLmap
  - Medusa
  - Hydra
  - Cain and Abel
  - Mimikatz
  - Patator
  - W3AF
  - Aircrack-NG

4.2 Compare and contrast various use cases of tools
4.2.1 Use cases
4.2.1.1 Reconnaissance
4.2.1.2 Enumeration
4.2.1.3 Vulnerability scanning
4.2.1.4 Credential attacks

PERSISTENCE

- Once you have exploited a target, use these to make sure you can get back in:
  - SET
  - BeEF
  - SSH
  - NCAT
  - NETCAT
  - Drozer
  - Powersploit
  - Empire
  - Metasploit framework

4.2.1.5 Persistence
4.2.1.6 Configuration compliance
4.2.1.7 Evasion
4.2.1.8 Decompilation

CONFIGURATION COMPLIANCE

- To evaluate a configuration to determine if it's compliant with a standard or regulation, use:
  - Nmap
  - Nikto
  - OpenVAS
  - SQLmap
  - Nessus

4.2.1.5 Persistence
4.2.1.6 Configuration compliance
4.2.1.7 Evasion
4.2.1.8 Decompilation

EVASION

- To evade detection, use:
  - SET
  - Proxychains
  - Metasploit framework

4.2.1.5 Persistence
4.2.1.6 Configuration compliance
4.2.1.7 Evasion
4.2.1.8 Decompilation

DECOMPILATION

- To decompile executables, use:
  - Immunity debugger
  - APKX
  - APK studio

4.2.1.5 Persistence
4.2.1.6 Configuration compliance
4.2.1.7 Evasion
4.2.1.8 Decompilation

PENETRATION TESTING USE CASES

- Forensics
  - To carry out digital forensics, use:
    - Immunity debugger
- Debugging
  - To debug code, use:
    - OLLYDBG
    - Immunity debugger
    - GDB
    - WinDBG
    - IDA

4.2.1.9 Forensics
4.2.1.10 Debugging
4.2.1.11 Software assurance
4.2.1.11.1 Fuzzing
4.2.1.11.2 SAST
4.2.1.11.3 DAST

SOFTWARE ASSURANCE

- For general software assurance, use:
  - Findsecbugs
  - SonarQube
  - YASCA
- For fuzzing, use:
  - Peach
  - AFL

4.2.1.9 Forensics
4.2.1.10 Debugging
4.2.1.11 Software assurance
4.2.1.11.1 Fuzzing
4.2.1.11.2 SAST
4.2.1.11.3 DAST

PENETRATION TESTING USE CASES

- Forensics – Immunity debugger
- Debugging – OLLYDBG, Immunity debugger, GDB, WinDBG, IDA
- Software assurance – Findsecbugs, SonarQube, YASCA
  - Fuzzing – Peach, AFL
  - SAST (Static Application Security Testing)
  - DAST (Dynamic Application Security Testing)

4.2.1.9 Forensics
4.2.1.10 Debugging
4.2.1.11 Software assurance
4.2.1.11.1 Fuzzing
4.2.1.11.2 SAST
4.2.1.11.3 DAST

Using Kali Linux

Episode 3

SAGEFOX

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

KALI LINUX DEMO

- Kali Linux demo

Scanners and Credential Tools

Episode 4

SAGEFOX

SCANNERS

Tool	Notes	URL
Nikto	Web server vulnerability scanner	https://github.com/sullo/nikto
OpenVAS (Open Vulnerability Assessment System)	Open Source vulnerability scanner and manager	http://www.openvas.org/
SQLmap (Structured Query Language)	Automatic SQL injection and database takeover tool	http://sqlmap.org/
Nessus	Commercial vulnerability scanner (free for non-professional use)	https://www.tenable.com/products/nessus/nessus-professional

4.2.2 Tools
4.2.2.1 Scanners
4.2.2.1.1 Nikto
4.2.2.1.2 OpenVAS
4.2.2.1.3 SQLmap
4.2.2.1.4 Nessus

CREDENTIAL TESTING TOOLS

Tool	Category	Notes	URL
Hashcat	Offline	Advanced password recovery (world's fastest)	https://hashcat.net/hashcat/
Medusa	Online	Parallel network login auditor	http://foofus.net/goons/jmk/medusa/medusa.html
Hydra	Online	Parallelized login cracker	http://sectools.org/tool/hydra/
Cewl		Custom wordlist generator	https://digi.ninja/projects/cewl.php
John the Ripper	Offline	Password cracker	http://www.openwall.com/john/

4.2.2.2 Credential testing tools
4.2.2.2.1 Hashcat
4.2.2.2.2 Medusa
4.2.2.2.3 Hydra
4.2.2.2.4 Cewl
4.2.2.2.5 John the Ripper

CREDENTIAL TESTING TOOLS, cont'd

Tool	Category	Notes	URL
Cain and Abel	Online/offline	Windows password recovery tool	http://www.oxid.it/cain.html
Mimikatz	Online/offline	A little tool to play with Windows security	https://github.com/gentilkiwi/mimikatz
Patator	Online	Multi-purpose brute-forcer	https://github.com/lanjelot/patator
Dirbuster		Multi-threaded app to brute force directories and file names on web servers	https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
W3AF	Online	Web Application Attack and Audit framework	http://w3af.org/

SAGEFOX

4.2.2.2.6 Cain and Abel
4.2.2.2.7 Mimikatz
4.2.2.2.8 Patator
4.2.2.2.9 Dirbuster
4.2.2.2.10 W3AF

ANALYZE TOOL OUTPUT

- Password cracking – demo John the Ripper

4.3 Given a scenario, analyze tool output or data related to a penetration test.
4.3.1 Password cracking

ANALYZE TOOL OUTPUT

- Pass the hash – demo Mimikatz

4.3.2 Pass the hash

Code Cracking Tools

Episode 5

SAGEFOX

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

DEBUGGERS

Tool	Notes	URL
OLLYDBG	Windows 32-bit	http://www.ollydbg.de/
Immunity debugger	Write exploits, analyze malware, and reverse engineer binary files	https://www.immunityinc.com/products/debugger/
GDB	GNU project debugger	https://www.gnu.org/software/gdb/
WinDBG	Windows debugger	https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools
IDA	Cross platform debugger	https://www.hex-rays.com/products/ida/debugger/index.shtml

4.2.2.3 Debuggers
4.2.2.3.1 OLLYDBG
4.2.2.3.2 Immunity debugger
4.2.2.3.3 GDB
4.2.2.3.4 WinDBG
4.2.2.3.5 IDA

SOFTWARE ASSURANCE TOOLS

Tool	Notes	URL
Findbugs/findsecbugs	Auditor of Java web applications	https://find-sec-bugs.github.io/
Peach	Fuzzer – automated testing	https://www.peach.tech/products/peach-fuzzer/
AFL	American Fuzzy Lop - fuzzer	http://lcamtuf.coredump.cx/afl/
SonarQube	Continuous inspection – automated testing	https://www.sonarqube.org/
YASCA	Yet Another Source Code Analyzer	https://github.com/scovetta/yasca

4.2.2.4 Software assurance
4.2.2.4.1 Findbugs/findsecbugs
4.2.2.4.2 Peach
4.2.2.4.3 Dynamo
4.2.2.4.4 AFL
4.2.2.4.5 SonarQube
4.2.2.4.6 YASCA

Open Source Research Tools

Episode 6

SAGEFOX

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

OPEN SOURCE INTELLIGENCE (OSINT) TOOLS

Tool	Notes	URL
Whois	Domain details (contacts, name servers, etc.)	https://whois.icann.org/en (and many more)
Nslookup	DNS information	Installed or available on most OSs
Foca	Fingerprint Organizations with Collected Archives – finds document metadata	https://github.com/ElevenPaths/FOCA
Theharvester	Gathers info from many sources (email, hosts, open ports, etc.)	https://github.com/laramies/theHarvester
Shodan	Finds Internet connected devices	https://www.shodan.io/
Maltego	Data mining for investigations	https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php
Recon-NG	Web reconnaissance	https://bitbucket.org/LaNMaSteR53/recon-ng
Censys	Finds Internet connected devices	https://censys.io/

4.2.2.5 OSINT
4.2.2.5.1 Whois
4.2.2.5.2 Nslookup
4.2.2.5.3 Foca
4.2.2.5.4 Theharvester
4.2.2.5.5 Shodan
4.2.2.5.6 Maltego
4.2.2.5.7 Recon-NG
4.2.2.5.8 Censys

ANALYZE TOOL OUTPUT

- Whois demo
- Nslookup demo

4.3.2 Pass the hash

Wireless and Web Pen Testing Tools

- Episode 7

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

WIRELESS TOOLS

Tool	Notes	URL
Aircrack-NG	Monitoring, attacking, testing, cracking	https://www.aircrack-ng.org/
Kismet	Wireless detector, sniffer and intrusion detection system	https://www.kismetwireless.net/
WiFite	Wrapper for other wireless tools (current version is WiFite2)	https://github.com/derv82/wifite2

4.2.2.6 Wireless
4.2.2.6.1 Aircrack-NG
4.2.2.6.2 Kismet
4.2.2.6.3 WiFite

WEB PROXIES

Tool	Notes	URL
OWASP ZAP	Zed Attack Proxy – Web application security scanner	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
Burp Suite	Graphical tool for testing web application security	https://portswigger.net/burp

4.2.2.7 Web proxies
4.2.2.7.1 OWASP ZAP
4.2.2.7.2 Burp Suite

SOCIAL ENGINEERING TOOLS

Tool	Notes	URL
SET	Social Engineering Toolkit – penetration testing using social engineering	https://www.trustedsec.com/social-engineer-toolkit-set/
BeEF	Browser Exploitation Framework – focus is on web browser	http://beefproject.com/

4.2.2.8 Social engineering tools
4.2.2.8.1 SET
4.2.2.8.2 BeEF

ANALYZE TOOL OUTPUT

- Proxying a connection - demo

4.3.5 Proxying a connection

Remote Access Tools

Episode 8

SAGEFOX

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

REMOTE ACCESS TOOLS

Tool	Notes	URL
SSH	Secure shell	Included or available in most OSs
NCAT	Similar to nc, but from Nmap developers	https://nmap.org/ncat/
NETCAT	Same as nc	Included or available in most OSs
Proxychains	Forces TCP connections through a proxy	https://github.com/haad/proxychains

4.2.2.9 Remote access tools
4.2.2.9.1 SSH
4.2.2.9.2 NCAT
4.2.2.9.3 NETCAT
4.2.2.9.4 Proxychains

NCAT and NETCAT can:

Connect to any port
Set up bind and reverse shells

ANALYZE TOOL OUTPUT

- Setting up a bind shell - demo

4.3.3 Setting up a bind shell

ANALYZE TOOL OUTPUT

- Getting a reverse shell - demo

4.3.4 Getting a reverse shell

Analyzers and Mobile Pen Testing Tools

Episode 9

SAGEFOX

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

NETWORKING TOOLS

Tool	Notes	URL
Wireshark	Packet sniffer/protocol analyzer	https://www.wireshark.org/
Hping	Packet assembler/analyzer	http://www.hping.org/

SAGEFOX

4.2.2.10 Networking tools
4.2.2.10.1 Wireshark
4.2.2.10.2 Hping

MOBILE TOOLS

Tool	Notes	URL
Drozer	Android security and attack framework	https://labs.mwrinfosecurity.com/tools/drozer/
APKX	Android APK decompiler	https://github.com/b-mueller/apkx
APK Studio	Android app decompiler	http://vaibhavpandey.com/apkstudio/

SAGEFOX

4.2.2.11 Mobile tools
4.2.2.11.1 Androzer
4.2.2.11.2 APKX
4.2.2.11.3 APK studio

Other Pen Testing Tools

Episode 10

SAGEFOX

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

MISCELLANEOUS TOOLS

Tool	Notes	URL
Searchploit	Search tool for exploit database	https://www.exploit-db.com/searchsploit/
Powersploit	Post-exploitation framework (MS PowerShell)	https://github.com/PowerShellMafia/PowerSploit
Responder	Microsoft network poisoner	https://github.com/SpiderLabs/Responder
Impacket	Python classes for working with network protocols	https://github.com/CoreSecurity/impacket
Empire	PowerShell/Python post-exploitation agent	https://github.com/EmpireProject/Empire
Metasploit framework	Comprehensive penetration testing framework	https://www.metasploit.com/

SAGEFOX

4.2.2.12 MISC
4.2.2.12.1 Searchsploit
4.2.2.12.2 Powersploit
4.2.2.12.3 Responder
4.2.2.12.4 Impacket
4.2.2.12.5 Empire
4.2.2.12.6 Metasploit framework