

CompTIA.

CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 8



Avoiding Detection and Covering Tracks

Objectives

- Given a scenario, perform active reconnaissance.
- Given a scenario, perform post-exploitation techniques.
- Explain use cases of the following tools during the phases of a penetration test.

Lesson 8

Topic 8A

Evade Detection

Flying Under the Radar

- During the reconnaissance phase, the team need to test to see if they can pass through network defenses unnoticed.
- Nmap has several ways to be stealthy:
 - Using fragmentation along with randomizing the order of hosts being scanned.
 - Spoofing options that trick the device by using a decoy, reporting a fake address, and/or using a specific port number.

Using a Decoy

- During a port scan on a host, you can use decoys to make it appear as if the packets are coming from a trusted or random device.
- The object is to create bogus packets from the “decoys” so the actual attacker "blends in" with the crowd.
 - This option can be used by issuing the command: `-D [decoy1, decoy2, decoy3, etc.] <target>.`
 - Another option is to use randomly generated decoy using the following option: `nmap -sS -sV -D RND:3 nmap.scanme.org`

Reporting a Fake Address

- One option to confuse the IDS is to use a bogus IP address to make it appear as if the packets are coming from another source.
- Another option to make the probe appear to be coming from a specific device by generating a bogus source MAC address
- You can achieve this in one of two ways:
 - Specify a random MAC based on the vendor category, i.e., `nmap -sT --spoof-mac apple scanme.nmap.org`, which creates a random Apple MAC address
 - Use a specific MAC address such as `nmap -sT --spoof-mac B7:B1:F9:BC:D4:56 scanme.nmap.org`, which creates a random hardware address.

Modifying a Port Number

- You can use Nmap offers an option to use a specific source port number by using either of the following commands:
 - `--source-port <portnum>`, for example: `nmap --source-port 53 scanme.nmap.org`
 - `-g <portnum>`, for example: `nmap -g 53 scanme.nmap.org`
- In either option, the probe will appear to have originated from port 53, which is used by a DNS server

Slowing the Scans

- Most modern network appliances are tuned to recognize a standard TCP SYN and other evasion and spoofing techniques.
- For example, Snort is a popular open-source IDS that holds many of the signatures to detect Nmap scans.
 - If aggressive scanning is detected, Snort will issue an alert.
- When testing, the team can avoid detection by using the `-T` switch to slow the scans or use other options to avoid detection.

Bypassing Network Access Control (NAC)

- NAC appliances restrict traffic by allowing only authorized hosts to access the corporate infrastructure.
- The most common way to bypass NAC is by accessing an *authenticated* device

Then use the device to slip by the NAC appliance.

- For example, a malicious actor can use a rogue WAP to get an authorized device to connect.
 - The attacker machine will then use it to relay malicious traffic into the protected network.

Living off the Land (LoTL)

- LoTL attacks are called *fileless malware* as there are no viruses used.
 - The attack uses tools that are part of the OS or admin tools
 - Generally, won't trigger any alarms and are harder to detect.
- Some of the tools include the following:
 - Microsoft PowerShell (PS)
 - Windows Management Instrumentation (WMI)
 - Visual Basic Scripts (VBScript) and Mimikatz

Covering your Tracks

- An attacker will try to make it as difficult for investigators to identify how the attack began and who is responsible
- Covering tracks is done in order to:
 - Attempt to conceal the source of a malicious act and remove any residual traces of that event before leaving the target environment.
 - Clean up after a PenTesting exercise by removing shells, tester-created credentials, and tools.

Tiding Logs and Entries

- The team can erase a whole log file or certain items. In addition, they can modify the time values to hinder the investigation.
- Methods to clear event logs include:
 - Use Metasploit's meterpreter and issue the command `clearev`, which will clear all Windows event logs.
 - Using the CLI in Windows, you can clear individual log categories.
 - On a Linux system there are several methods to clear logs
 - In some cases, you don't want to remove all logs, just specific entries.

Changing Log Entries

- Instead of removing an entry or an entire log, you can alter the log entries, and frame another individual.
- Methods to achieve this include:
 - Modify a user logon entry in Windows security logs
 - Steal a privileged user's token and then perform a malicious task

Modifying Timestamps

- A good forensic investigator will attempt to reconstruct a narrative of events by correlating event data.
- If you can modify the time that certain events are recorded, you can deceive the investigators during a forensic investigation.
- Changing time-based values is not just limited to event logs.
 - You can also alter a file's MACE metadata using Metasploit's meterpreter tool called TimeStomp
 - Allows you to delete or modify timestamp-related information on files.

Erasing or Shredding Data


- It's possible to delete the entries by using one of the following:
 - When using a Bash shell enter either `echo "" > ~/.bash_history` or `history -c`.
 - In a Windows OS, clear the history by pressing Alt+F7 or terminate the process.
 - While in PowerShell, clear the history by using the Clear-History cmdlet.
- To completely removed a file, you can do the following:
 - On a Linux system, you can use the command `shred`.
 - On a Windows system, overwrite a volume using: `format d: /fs:NTFS /p:1`.

Review Activity: Evade Detection

- List ways you can fly under the radar when scanning
- Discuss how you can bypass a NAC device
- Describe a Living off the Land attack
- Outline how the team can erase or modify a whole log file or change certain items in a log
- Discuss how and why you might alter timestamps
- Explain why the team might erase or shred data

Lab Activity

Assisted Lab: Using ProxyChains

- Lab types
 - Assisted labs guide you step-by-step through tasks
 - Applied labs set goals with limited guidance
- Complete lab
 - Submit all items for grading and check each progress box
 - Select “Grade Lab” from final page
- Save lab 
 - Select the hamburger menu and select “Save”
 - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
 - Select the hamburger menu and select “End”

Lesson 8

Topic 8B

Use Steganography to Hide and Conceal

Using Steganography to Hide and Conceal

- Today, there are hundreds of steganography tools available to conceal a message in plain site
- Steghide is an open-source CLI tool used to conceal a payload in either an image or audio file.
 - Can compress, conceal, and encrypt data using images such as JPEG and BMP, along with audio files using WAV and AU formats.
- OpenStego is like most other tools, in that you embed a message in a carrier file. However, you can also embed a watermark.

Masking using Alternate Data Streams

- NTFS Alternate Data Streams were originally designed to provide compatibility with non-Windows file systems.
- However, this method can also be used to allow data to be stored in hidden files that are linked to a regular visible file.
- The streams are not limited in size and there can be more than one stream linked to the visible file.
- This allows an attacker to hide their tools and data on a compromised system and retrieve them later.

Other Methods used to Conceal Information


- Snow is a CLI steganography tool that conceals a data payload within the whitespace of a text file that uses the ASCII format.
 - Data can either be concealed using plaintext, or the message can be encrypted.
- Coagula and Sonic Visualizer are tools that use *sound* to conceal an image into a .wav file, and then convert the text in the spectrogram.
 - Create an image that contains text, then convert the image into a .wav file
 - Reveal the text by using an audio spectrogram

Review Activity: Use Steganography to Hide and Conceal

- Discuss Steganography, and list examples of some tools used to embed a message in a carrier file.
- Describe how NTFS Alternate Data Streams can hide information
- Outline how you can hide information in white space
- Explain how Coagula and Sonic Visualizer can convert an image into music.

Lab Activity

Assisted Lab: Navigating Steganography Tools

- Lab types
 - Assisted labs guide you step-by-step through tasks
 - Applied labs set goals with limited guidance
- Complete lab
 - Submit all items for grading and check each progress box
 - Select “Grade Lab” from final page
- Save lab 
 - Select the hamburger menu and select “Save”
 - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
 - Select the hamburger menu and select “End”

Lesson 8

Topic 8C

Establish a Covert Channel

Preventing Data Exfiltration

- Data exfiltration is when data that is stored inside a private network is transferred to an external network without authorization
- This can be the result of the following:
 - A social engineering attack such as a phishing email requesting data
 - Downloading data to an insecure device, such as a USB drive
 - Fileless malware such as a PowerShell-based attack using custom payloads
 - Transmitting data to non-secured cloud resources

Using a Secure Shell (SSH)

- When communicating with a remote, Linux machine, it's common to use SSH, a protocol that provides a way to communicate securely
 - For an SSH session to take place, one computer will act as a client and one computer will act as a server.
 - Once the session is started, the client can then manipulate objects, transfer files, or manage the computer by issuing commands
- Malicious actors constantly try to exploit a vulnerable SSH server
 - Nmap has several commands and scripts that the team can use to see if the target is vulnerable.

Hacking with Netcat

- A CLI utility used to read from, or write to, a network connection.
 - It can create or connect to a TCP server
 - Act as a simple proxy or relay, transfer files
 - Launch executables (such as a backdoor shell) when a connection is made
 - Test services and daemons, and even scan ports.
- The basic syntax of Netcat is `nc [options] [target address] [port(s)]`.

Evolving with Ncat

- Ncat is an Interactive CLI tool used to read and write data over a network. It's similar to Netcat, yet has advanced features
- When establishing a link, Ncat can operate in either:
 - **Connect (or client) mode** – If the host is in this mode, Ncat will attempt to initiate a connection to a listening service.
 - **Listen (or server) mode** – If the host is in this mode, Ncat will listen for an incoming connection request.
- Ncat is built into Nmap and includes support for Windows, Linux, and Mac OS.

Providing Remote Management with WinRM

- WinRM comes installed with Windows and can be accessed via a CLI or PowerShell.
- To activate the service, issue the command `c:\users> winrm quickconfig`
 - This will configure the firewall exceptions and start the service.
- After initial configuration on both systems, you can then gain access to the remote system.
 - Once in, you can execute commands to manage and monitor clients and servers.

Managing Remotely Using PSEXec

- PsExec is a lightweight program that is part of the Sysinternals suite that provides interactivity for CLI programs.
 - Uses SMB to issue commands to a remote system without having to manually install client software.
- Can be used along with Mimikatz to allow a malicious actor to move laterally within a system and issue commands.
 - `PSEXec \\192.168.1.50 -s "C:\bad-app.exe"`

Using a Proxy

- Proxy servers are used on a network to mediate communications between a client and another server.
- Can filter and often modify communications, as well as provide caching services to improve performance.
- Malicious actors can also use proxies to conceal their location.
 - Called ProxyChaining, this provides an extra layer of protection by forcing a specific TCP connection so that websites do not see your real IP address.

Using ProxyChains4

- ProxyChains4 is a command-line tool that enables PenTesters to mask their identity and/or source IP address
 - Sends messages through intermediary or proxy servers.
- To stay anonymous during port scanning, you can use TOR through ProxyChains4
 - Traffic is sent through a specific tunnel
 - Encrypting the traffic will conceal the contents of the packets.

Review Activity: Establish a Covert Channel

- Define Data exfiltration and ways this can occur
- Describe how using SSH can be a vulnerability
- Compare features of Netcat and Ncat
- Explain how the team can use WinRM and PSEXEC to provide remote management of a system
- Outline what's involved in using a proxy
- Discuss ways the team can stay anonymous during port scanning

Lesson 8



Summary