CompTIA

CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 16

Leveraging the Attack: Pivot and Penetrate

Objectives

- Given a scenario, research attack vectors and perform network attacks.
- Given a scenario, perform post-exploitation techniques.
- Explain use cases of the following tools during the phases of a penetration test.

Lesson 16

Topic 16A

Test Credentials

Offline Password Attacks

- Offline password attack is when a malicious actor obtains a copy of usernames and passwords and attacked offline.
    - An example could be /etc/shadow in Linux or the SAM database in Windows
- Once obtained they then run an attack on their own machine
    - This is known as “password cracking.”
- An alternative is to get the credentials in hashed format
    - This is also known as hash cracking.

Attempting a Dictionary Attack

- A **dictionary attack** is the most straightforward type of automated password attack.
    - A password cracking tool goes through a list of words until it either finds the password or exhausts the list.
- There are practical limits to using a dictionary attack.
    - You must first know the username.
    - Password lists can become unwieldy in size and may be difficult for the password cracker (or its system) to load or manage.
    - Most systems have policies that lock out a user after a certain limit has been exceeded.

Bypassing Lock Out Limits

- There are several techniques used to bypass lock out limits when attempting an on-line attack. These include:
  - Steal a copy of the file or database that contains the user credentials and attempting to crack the passwords offline
  - Induce the system to "dump" its hashed passwords you can crack them offline
  - Run the password cracker against a network service that does not have a lockout policy
  - Run the password cracker against a user account such as administrator or root that is exempt from a lockout policy

Using a Brute Force Attack

- A **brute force attack** is one in which the attacker tries many passwords in the hope of eventually guessing the right one.
- Brute force attacks are limited by processing power and other resources (such as memory and storage space).
- **Password spraying** is the concept of controlled brute forcing by *testing several accounts* with common or targeted passwords.

Attacking Linux and Windows Passwords

- Linux passwords are stored as hash values in /etc/shadow.
  - Identify the hash algorithm in use then attempt to crack the hash
- Windows stores local usernames and passwords in the Security Account Manager (SAM).
  - Passwords are stored as two types of hashes: LanMan (LM) and NT hash
  - The Windows Local Security Authority (LSASS) uses LSA secrets to store a variety of user, service, and application passwords.
  - In some cases, they can be found in memory after the user logs on, or the computer boots up, and can be dumped using tools like Mimikatz.

Evaluating Password Cracking Tools

- Many password-cracking tools available, many are multi-featured.
  - **hashcat -** can speed up the process by using different attack methods (dictionary, mask, hybrid) to add complexity and variability.
  - **medusa** - Parallel brute-forcer for network logins. Its focus is to support numerous network services that allow remote authentication.
  - **brutespray** - Tool that allows to interpret results from an Nmap scan to automatically start medusa against the identified open ports.

Alternative Methods to Obtain Credentials

- Use of social engineering to obtain user credentials
- Install a physical or software-based keylogger to capture login credentials
  - Hardware-based USB keyloggers (requires physical access)
  - Meterpreter keyscan_start and keyscan_dump

Review Activity: Test Credentials

- Describe what activity occurs in an offline password attack
- Outline how a Dictionary attack works
- List ways the team can bypassing lock out limits
- Discuss what's involved when using a brute force attack
- Compare methods to attack Linux and Windows passwords
- List some password cracking tools
- Review alternative methods to obtain credentials

Lab Activity

Assisted Lab: Exploring Password Attacks with john the Ripper and Hydra

- 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 16

Topic 16B

Move Throughout the System

Upgrading a Restrictive (Linux)

- There are cases in which the shell we obtain is a restrictive shell.
- There are technical shortcomings that are important to a penetration tester
    - Such as SSH not working properly in a restrictive shell, which might affect our attempts to create a tunnel through it for further attacks.
- To be able to continue to manipulate the environment, the team will need to upgrade the shell

Moving Laterally

- Lateral movement is the process of moving from one part of a computing environment to another.
  - You may be able to discover additional, or new, vulnerabilities in the environment that you would otherwise miss if you stayed in place.
- Once you compromise the patient zero host, you can:
  - Sweep the network for other hosts, as well as enumerate network protocols, ports, and logical mapping.
  - Helps discover where additional hosts are and what hosts you can move to.

Lateral Movement with Remote Access Services

- You can leverage shells for the remote access.
- Similarly, you can use CLI services for lateral movement:
  - Remote Desktop Protocol (RDP) comes with Windows systems.
  - Virtual Network Computing (VNC) cross-platform allows full remote-control.
- Remote management services enable you to issue commands to remote systems:
  - WinRM and PowerShell, and PsExec.
  - Using RPC/DCOM can help you evade notice.

Pivoting into Other Areas

- Pivoting is when you compromise one host that enables you to spread out to other hosts that would otherwise be inaccessible.
- This is necessary when you want to move to a different network segment than the one you are currently on.
- Techniques that can enable pivoting include:
  - Port forwarding, VPN pivoting, SSH pivoting
  - Modifying routing tables

Obtaining the Hash

- A pass the hash attack is when you log on using the username and the *hash* of the password, rather than the password itself.
    - You obtain the hash by inducing the operating system or application to dump them from RAM, the Windows Registry, or a credentials file.
- You can use Mimikatz and other tools such as Responder.py to *obtain hashes* from different services on the network.
    - Once you have the hashes, there are several tools you can use to test usability and pass, or crack, them such as Hydra and Medusa

Escalating Privileges

- Privilege escalation is one of the primary objectives in any penetration test.
  - It allows the attacker to gain control, access or change sensitive files, and leave permanent backdoors.
- Privilege escalation (PrivEsc) is used to gain access to the restricted resources:
  - **Vertical Privilege Escalation** Obtaining access to an account of *higher* privileges than the one you currently have.
  - **Horizontal Privilege Escalation** Obtaining access to a *regular user* account of different privilege than the one currently in use.

Gaining Control in Windows

- In addition to kernel-specific exploits, there are other types of exploits that can elevate privilege.
  - They take advantage of services, drivers, and applications running in SYSTEM or administrator privilege.
  - Like kernel exploits, most are run locally after gaining access to the target.
- Some examples include:
  - Credential attacks, Local UAC bypass,
  - Search for sensitive information in shared folders, Search for missing patches or common misconfigurations that can lead to privilege escalation.

Escalating Privileges in Linux

- Once you have compromised a Linux host, you'll most likely need to escalate your privilege to achieve your objectives.
- Here are some examples of ways to escalating privilege in Linux:
  - User application compromise
  - Locate services that are owned by (running as) root and see if you can compromise them
  - Exploit badly configured cron jobs to gain root access.

Review Activity: Move Throughout the System

- Explain why the team will need to upgrade a restrictive shell
- Outline what the team can achieve when moving laterally
- Describe how the team can achieve lateral movement with remote access services
- Discuss what can achieved when pivoting into other areas
- Review ways to escalate privileges
- Compare ways to gain control in a Windows and Linux environment

Lesson 16

Topic 16C

Maintain Persistence

Creating a Foothold

- Persistence is the quality by which a threat continues to exploit a target while remaining undetected for a significant period.
- Some of the goals involved in persistence include:
    - Exfiltrating portions of sensitive data over a period rather than all at once.
    - Exfiltrating sensitive data that changes over time.
    - Compromising systems, networks, applications, and other assets for days, weeks, months, or even years.
    - Monitoring user behavior over time.

Avoiding an Advanced Persistent Threat (APT)

- APT is an implementation of persistence
  - Relies on highly customized, complex exploits.
- APTs tend to target organizations that hold a great deal of power over others.
  - Can go years before being discovered, exfiltrating significant volumes of sensitive data from a target
  - Represent some of the most insidious and harmful threats to targeted organizations.

Bypassing Restrictions

- Various techniques can help you maintain access on the target.
- For example, certain user accounts are more closely monitored or more tightly access-controlled than others.
  - Creating a new account can help you bypass these restrictions when you need to authenticate.
- Remote access services can also be used for persistence. Other common persistence techniques include:
  - Backdoors and Trojans, Bind and Reverse Shells
  - Services and Daemons, Registry Startup and Scheduled Tasks

Using Backdoors and Trojans

- A backdoor is a hidden mechanism that provides you with access to a system through some alternative means.
  - The goal is to escape the notice of the system's typical users while enabling unauthorized users to access that system.
- One example of a backdoor is a remote access tool (RAT), also known as a remote access trojan.
  - Primarily downloaded to a victim's computer through Trojan horse malware
  - The function of a RAT may strictly offer an interactive shell or full GUI services and are designed to remain hidden from view

Remote Access Services

- Remote access services like Telnet, SSH, RDP, VNC, etc., can also enable persistence.
- You can even leverage backdoor accounts with these services, to remotely control the target system.
  - However, remaining stealthy while using these services is especially difficult.

Employing Reverse and Bind Shells

- A shell is any program that can be used to execute a command. There are essentially two types of shell attacks: bind and reverse.
- A bind shell is established when the target system "binds" its shell to a local network port.
- A reverse shell is established when the target machine communicates with an attack machine listening on a specific port.

Comparing Services and Daemons

- In the Windows world, a service is any program that runs in the background and are a type of non-interactive process.

- In the Unix-like world, a daemon is like a service.
  - They run in the background but are not attached to any terminal; therefore, they can continue to run on the system even when a terminal is closed.

- If you install a remote access daemon on the target:
  - You could shell into the target at any time and even regain that shell immediately after the system has rebooted.

Registry and Startup Locations

- In Windows, to get a particular program or command to start upon boot, you can add the program or modify the Registry keys
- In Linux, (depending on the distribution) /etc/init.d/ and /etc/systemd/ can provide similar run-on-boot functionality
    - Some distributions maintain backwards compatibility with RC scripts: /etc/rc.local/ and entries in the rc.common file.

Scheduling Tasks

- A scheduled task or job is will initiate a process or run of a script that the system performs on a set schedule.
- Scheduled tasks can help during the PenTest campaign:
  - You could create a scheduled task that silently runs an exfiltration command in the background to automate persistence while remaining undetected.
- Using Task Scheduler you can do quite a bit, including:
  - Set the task's actual action, e.g., running a program, what account to run the task under, along with special conditions when the task should run

Using cron Jobs

- In Linux, cron jobs are the primary method of scheduling tasks/jobs.
- The cron daemon runs the specified shell command at the date and/or time specified in the user's crontab file.
- You can edit this file by entering crontab -e at a shell.
  - Be aware that the jobs you create with crontab -e will run as the current user.

Maintaining Persistence

- When using persistence techniques, some guidelines include:
  - Try to maintain a foothold in the organization to continue your attack after the main phase has concluded.
  - Demonstrate persistence to the client without necessarily keeping assets compromised for a long period of time.
  - Create a shell using Netcat to open a backdoor for command execution.
  - Use Task Scheduler in Windows to run a compromising command or program on a consistent schedule.
  - Use cron jobs in Linux to do likewise.

Review Activity: Maintain Persistence

- Outline some of the goals involved in maintaining persistence
- Explain the concept of an Advanced Persistent Threat
- Review ways the team can bypass restrictions
- Discuss what can be accomplished with Backdoors and Trojans
- Describe how remote access services can enable persistence.

Review Activity: Maintain Persistence

- Describe the concept of reverse and bind shells
- Discuss the benefit of using a remote access daemon
- Compare ways to schedule tasks and jobs in either Windows or Linux environments
- List some guidelines when using persistence techniques

Lesson 16

Summary