CompTIA

CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 9

Exploiting the LAN and Cloud

Objectives

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

Lesson 9

Topic 9A

Enumerating Hosts

Discovering Services

- On an enterprise network, there are many services running that can provide intel that can be useful to the PenTest team, that include:
  - **SMTP** (TCP port 25) - Extract email addresses. Enumerate SMTP server information. Search for open relays.
  - **DNS** (TCP port 53) - Elicit DNS zone transfers and discover DNS subdomains.
  - **SMB** (TCP port 139) - Retrieve directory information, list, and transfer files.

Enumerating Shares

- Shares can be enumerated on either Microsoft or Linux/Unix hosts
  - **Microsoft hosts:** Microsoft File and Print service, using SMB protocol via TCP ports TCP 139 or 445
  - **Linux/Unix (*nix) hosts:** NFS daemon via TCP and UDP port 2049
- In addition to the OS built-in commands, you can also use:
  - **Metasploit** - a platform for launching attacks against known software vulnerabilities
  - **ShareEnum** - a Sysinternals tool that can scan a domain, workgroup, or IP address range

Evaluating Websites

- Discovering the resources and technology that the web server is using will help you choose more effective vectors
- You can use Nmap to enumerate information using one of several scripts you can use for popular web applications:
  - `nmap --script=http-enum <target>`
- Some websites are configured to use non-standard ports.
  - If you're not sure of the port, you can scan all of them to try to determine what services are bound to these ports

Enumerating Windows Hosts

- After completing a ping sweep to identify interesting hosts, the next logical step is to enumerate hosts on the network.
- When enumerating Windows hosts, there are several tools you can use, including the built-in tools within the OS. For example:
  - **net view** - To view shares from other hosts in the network
  - **net user** - To list all users on the machine.
- There are also several popular tools for Windows host enumeration that include PowerShell, Nmap, and Metasploit.

Query Active Directory for Information

- AD stores, organizes, and enables access to other objects and provides essential network services
- In addition to Nmap and Metasploit, the team can use PowerShell to enumerate information such as users, groups, and domains.
- Some of the PS cmdlets available for AD enumeration include:
  - **Get-NetDomain** Get the current user's domain
  - **Get-NetLoggedon** Get users that are logged on to a given computer:
  - **Get-NetGroupMember** Get a list of domain members in a given group

Discovering Linux Systems

- Once you compromise a Linux machine in Metasploit, you can use the `post/linux/enum_system` module to get information
- Enumeration modules include:
  - `enum_configs`
  - `enum_network`
- It's also possible to use the built-in Bash commands:
  - **finger** - Views a user's home directory along with login and idle time.
  - **cat /etc/passwd** - Lists all users on the system

Review Activity: Enumerating Hosts

- List some network services to enumerate and describe how the information can be useful to the team.
- Outline shares found on either Microsoft or Linux/Unix hosts along with ways the team can enumerate the information.
- Discuss the resources and technology that the web server is using and how this can help the team choose more effective vectors
- Explain why it might be beneficial to query AD for Information

Lab Activity

Assisted Lab: Demonstrating Enumeration Techniques

- 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 9

Topic 9B

Attack LAN Protocols

Moving Between VLANS

- VLANs are used to organize devices by security need and/or to limit the impact of broadcast traffic on the larger network.
- VLAN hopping is moving from one VLAN to another.
- To launch this attack, a malicious actor can do one of the following:
  - Launch a Macof attack, which overflows the MAC table on a vulnerable switch so that it behaves like a hub, repeating frames out all ports.
  - Configure the interface of an attacker machine to become a trunk port. This will then allow traffic from any VLAN to flow over that link.

Launching an On-Path Attack

- An on-path attack is when a malicious actor sits in the middle or in the path of a connection.
  - Both sides think they are communicating directly with each other, but they are doing it through the on-path attack.
  - The on-path attack then captures information
- Examples of on-path attacks include:
  - SSL/TLS stripping attack
  - Wi-Fi Pineapple (or rogue WAP)

Spoofing Lan Protocols

- An on-path attack is generally done by using either a spoofing or cache poisoning strategy, such as any of the following:
  - Domain Name System (DNS) cache poisoning
  - Address Resolution Protocol (ARP) spoofing
  - MAC address spoofing
- For any of these attacks, when a device needs to deliver a message to the victim, it will instead send the message to the malicious actor.

Poisoning LLMNR and NBT-NS

- **Responder** is a man-in-the-middle type tool designed to intercept and poison LLMNR and NBT-NS requests
  - LLMNR and NBT-NS are services used to resolve network addresses.
- With this attack, the victim must be tricked into querying a nonexistent name or prevented from using a legitimate DNS service.
- Once a request is intercepted, Responder will return the attacker's host IP as the name record
  - This causes the querying host to establish a session with the attacker.

Grabbing Password Hashes

- One way to circumvent an authentication process is to use a hash
- **Pass the Hash** (NTLM relay) attack is when attacker steals hashed user credentials and uses them to try to authenticate to a system
- **Kerberoasting** extracts service account credential hashes from AD, and then performs an offline crack to obtain the password.
  - Once you obtain the password, you can then to take control of the system.
  - Kerberoasting is a significant attack as many services have admin privileges, and their passwords are seldom changed.

Chaining Exploits

- Exploit chaining uses multiple exploits to form a larger attack.
- Success of the attack will depend on all exploits doing their part.
  - Using multiple forms of attacks makes them difficult to defend against.
- Some examples of exploit chaining include:
  - A Metasploit exploit that results in a user-level shell, followed by a local privilege escalation attack to give the shell system-level privileges.
  - Breaking into a private network, planting a malicious device, then using that device to discover and attack vulnerable systems.

Review Activity: Attack LAN Protocols

- Explain how a VLAN hopping works
- Describe an on-path attack
- List some spoofing or cache poisoning attacks
- Discuss the benefit of poisoning LLMNR and NBT-NS requests
- Outline how to circumvent an authentication process using a hash
- Review how chaining exploits lead to a more successful attack

Lesson 9

Topic 9C

Compare Exploit Tools

Testing with Metasploit Framework (MSF)

- MSF is a multi-purpose PenTesting framework organized into modules, such as Exploits, Payloads, and Auxiliary.
- Once you specify a module, set options, such as:
  - **RHOSTS**, **LHOST**, and **RPORT**
- If you are using an exploit, you will also need to specify the payload.
  - The most popular payload is Meterpreter
- Both Metasploit Framework and Metasploit Pro allow you to search and select scanning modules.

RECOGNIZING OTHER TOOLS

- The following are some of the tools used when working on a LAN:
  - **Impacket tools** is a collection of tools used in a Windows environment.
  - **Responder** is used to poison NetBIOS, LLMNR, and MDNS requests.
  - **mitm6** is an IPv6 DNS hijacking tool
- In addition to the tools used to launch attacks, the PenTest team will need to be aware of all possible exploits.
  - The team can use Exploit DB, which provides a complete collection of public exploits and vulnerable software in a searchable database.

Review Activity: Compare Exploit Tools

- Discuss how the team can use the Metasploit Framework (MSF)
- List some of other tools used when working PenTesting on a LAN
- Describe how the team can use Exploit DB

Lab Activity

Assisted Lab: Exploring the Basics of Metasploit

- 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 9

Topic 9D

Discover Cloud Vulnerabilities

Configuring Cloud Assets

- A **cloud federation** is combination of infrastructure, platform services, and software which can increase the risk of attack
  - The elastic computing power can make it easier for an attacker to run extensive password-cracking algorithms or host a C&C botmaster.
- The stakeholders will need to identify precisely where responsibilities lie in terms of threat and vulnerability management.
  - They will need to make sure that the provider reports the outcomes of any security-related auditing to the team.

Running Applications in the Cloud

- Applications can be deployed either in a virtualized or containerized environment.
- Container images can have several vulnerabilities that include:
  - Embedded malware, missing critical security updates, outdated software
  - Configuration defects, hand-coded cleartext passwords
- Prior to deploying a container, the network administrator should test and mitigate any vulnerabilities
  - Once trusted, preserve the container image.

Understanding Cloud Storage Vulnerabilities

- Containers can host objects
  - Most have customizable attributes along with methods to control access.
- It’s essential to properly configure cloud assets, as consumer side configuration misconfigurations can increase risks
  - Storage is also potentially vulnerable
- Understand the design of a CSP's storage permissions.
  - Policies should be created to guide the application of permissions settings so that storage containers and objects are not exposed to unnecessary risk.

Comparing Identity and Account Types

- Every unique subject in the organization is identified and associated with an account. The different types include:
  - Personnel, endpoints, servers, software and roles
- An IAM system usually contains technical components like directory services and repositories, and access management tools
- Typical IAM tasks might include:
  - Auditing account activity, evaluating identity-based threats and vulnerabilities
  - Maintaining compliance with regulations, and managing accounts

Recognizing Account Management Risks

- Malicious actors target employees to gain access the network.
- To avoid an attack, provide oversight when using either privileged or shared accounts, as both can represent a vulnerability.
  - A **privileged account** allows the user to perform additional tasks
  - A **shared account** is when authentication credentials are shared
- Reduce risk by providing training and education targeted to specific user groups and provide strong access control methods

Review Activity: Discover Cloud Vulnerabilities

- Explain the importance of properly configuring cloud assets.
- Review how to reduce risks when running applications.
- Discuss cloud storage vulnerabilities
- Outlining the different types of identities and account types
- Describe potential risks when dealing with account management

Lesson 9

Topic 9E

Explore Cloud-Based Attacks

Attacking the Cloud

- The cloud is vulnerable to the same types of attacks that affect many applications.
  - Attacks against delivery models such as SaaS, can result in a data breach.
- In addition to the financial impact of recovery fees and/or loss of intellectual property, a company can face fines and legal action.
- Attacks include:
  - Malware injection attack, side-channel attacks, and direct-to-origin attacks

Harvesting Credentials

- Steal usernames and passwords with the goal of escalating privilege
  - To take control, access/change files, and open a backdoor.
- Several types of attacks can elevate privilege by taking advantage of services, drivers, and apps running in SYSTEM or admin privilege.
- Some examples of methods to elevate privilege include:
  - **Weak process permissions** - Find processes with weak controls and then see if you can inject malicious code into those processes.
  - **Missing patches and misconfigurations** - Search for missing patches or common misconfigurations that can lead to privilege escalation.

Denying Service

- A DoS attack can target a protocol, device, OS, or service. The results of a DoS attack will depend on the affected system.
  - An attack against a server will consume all resources, including CPU, memory, disk space, and can lock out legitimate users.
  - A related attack is resource exhaustion, which consumes system resources.
- Some examples of DoS attack types and tools:
  - **Attacks:** Packet flood, Slowloris, HTTP flood and DNS amplification
  - **Tools:** Nmap, Slowloris script, R-U-Dead-Yet (RUDY) and Hyenae

Auditing the Cloud

- Today, there are several tools available to perform automated vulnerability scanning and PenTesting on cloud assets:
  - **ScoutSuite** is an open-source tool written in Python that can be used to audit instances and policies created on multicloud platforms
  - **Prowler** is an audit tool for use with Amazon Web Services only.
  - **Pacu** is designed as an exploitation framework to assess the security configuration of an AWS account.
  - **Cloud custodian** is a management tool designed to help the administrator create policies based on resource types.

Review Activity: Explore Cloud-Based Attacks

- Describe some of the attacks on cloud resources.
- Review the goal of harvesting credentials
- Discuss methods to achieve privilege escalation.
- Explain the effect of a DOS attack and list some examples of attacks and tools used to launch the attack
- List tools available to perform automated vulnerability scanning and PenTesting on cloud assets

Lab Activity

APPLIED Lab: Using VSFTP Manual and Metasploit

- 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 9

Summary