CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 5

Preparing the Vulnerability Scan

Objectives

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

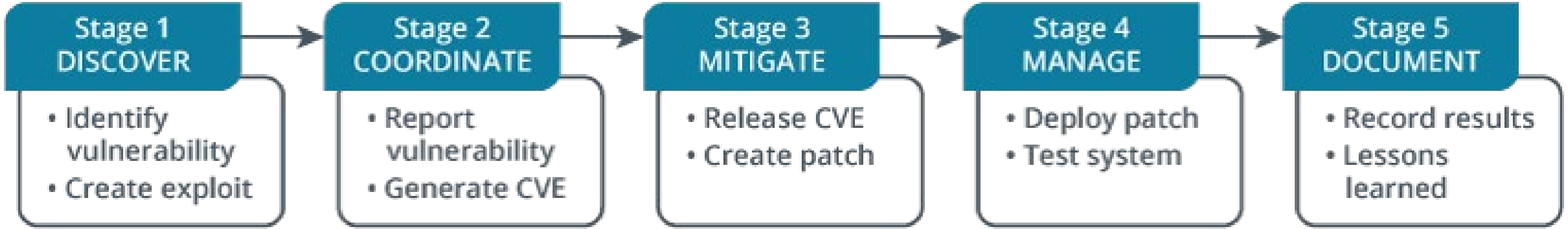
Lesson 5

Topic 5A

Plan the Vulnerability Scan

Understanding Vulnerabilities

- A key part of PenTesting is to identify vulnerabilities that can be exploited accidentally or intentionally and cause a security breach.
- Vulnerabilities move through a lifecycle, discovery through awareness and documentation, as shown in the graphic:



Stage 1 DISCOVER
- Identify vulnerability
- Create exploit

Stage 2 COORDINATE
- Report vulnerability
- Generate CVE

Stage 3 MITIGATE
- Release CVE
- Create patch

Stage 4 MANAGE
- Deploy patch
- Test system

Stage 5 DOCUMENT
- Record results
- Lessons learned

Lifecycle of a vulnerability

Stages of a Vulnerability

1. **Discover** – Recognizing a potential vulnerability exists
2. **Coordinate** - both the vulnerability and the potential to exploit the vulnerability are known.
3. **Mitigate** is when vendors and software designers look at the vulnerability and devise a strategy to deal with the vulnerability.
4. **Manage** is when the patch has been released.
5. **Document** - the vulnerability has been tested, and everyone involved will take a moment to document what has been done.

Exploiting the Unknown

- A **zero-day attack** takes advantage of a software vulnerability that is unknown or undisclosed by the software vendor.
- The process is as follows:
  1. The vulnerability is found in the wild
  2. At some point, the vulnerability, are now known by the vendor
  3. The vendor will mitigate or remediate the vulnerability by creating a patch.
- **Risk gap** is the time between when the vendor releases a patch, and the patch is applied.

Reducing Risks to Data

- Key considerations in performing a PenTest is the goal of protecting an organizations’ data.

- Unauthorized access to the data can result in the following:

  - **Exposing sensitive data** occurs when someone or something exposes sensitive or personal data, which is a violation of confidentiality.

  - **Data modification** or corruption is when data has been altered in some way, which is a violation of integrity.

Grabbing Banners

- Used during reconnaissance to gather information about network hosts and the services running on open ports.
- You can use Wget, Netcat, Nmap, Curl, and other tools to grab banners from services and protocols
  - The banners can help you focus your attacks on specific services.
- For example, when using Nmap issue the following command to get some basic information about a target IP:
  - nmap -sV <target IP> -p <port number>

Mapping the Network

- Uses active probing to gather information related to the network:
  - MAC and IP addresses, ports, services, and operating systems
  - Device types, virtual machines, host names and protocols
  - Subnets and how the devices are interconnected.
- Having a topology map of the network is valuable to the team
  - It defines the choice of tools and strategies when moving to the attack phase.

Running Scans

- Scanning probes targets on the network in order to identify issues:
  - Weak encryption and authentication protocols
  - System vulnerabilities and security flaws
  - Lack of compliance with data privacy regulations
- The following are general purpose vulnerability scanners:
  - Open Vulnerability Assessment Scanner (OpenVAS)
  - Nexpose Community Edition and Retina Community
  - Nessus/Tenable and Nmap

Scanning Considerations

- During the planning phase of the PenTest, the organization will define some of the parameters of the PenTest in the project scope
  - Time to run scans, bandwidth limitations and fragile systems
- Scanning can be either intrusive or nonintrusive.
  - A **nonintrusive** scan is passive and only reports identified vulnerabilities
  - An **intrusive scan** can identify and then *exploit* vulnerabilities.
- When using an intrusive scan, the team should use caution, as this type of scanning can cause damage to the system.

Comparing the Different Types of Scans

- Scanning can include the following :
  - Web applications, network, applications along with compliance scans
- Once the scan is complete, validate any vulnerabilities
  - The most common way to validate is to attempt to exploit the vulnerabilities and produce evidence of success.
- Keep in mind the limits of various scanning tools.
  - Use an actual scanning tool such as OpenVAS or Nexpose to *conduct* the scan
  - Follow with Metasploit *validate* the results.

Review Activity: Plan the Vulnerability Scan

- Outline the importance of identifying vulnerabilities
- List the phases of a vulnerability
- Describe what the team can discover when mapping the network
- Explain some of the goals when scanning the network
- Review what to consider prior to scanning the network

Lesson 5

Topic 5B

Detect Defenses

Identifying Load Balancers

- During scanning, it’s important for the team to identify any devices such as load balancers that can misdirect probes or attacks.
- Load balancing helps ensure network hosts receive a response to a request in a timely manner, which improves network performance.
  - The team can detect the presence of a load balancer by using the load balancing detector (lbd) app in Kali Linux
- In addition to load balancers, there are other devices that can cause false results on security scans:
  - Reverse proxies, intrusion prevention/detection systems, and firewalls.

Recognizing Firewalls

- Firewalls are used to monitor and control traffic on a network
- A web application firewall (WAF) is a dedicated firewall, which guards against common attacks such as XSS and SQLi attacks.
- The team can identify a WAF in following ways:
  - A WAF can give away their presence by adding a cookie in the HTTP packets.
  - Some WAF products use a technique called header alternation, which changes the original response header to confuse the attacker.
  - Some WAF will identify themselves by their response, for example you might see the following: <title> myDefender blocked your request</title>.

Testing the Firewall

- The team will test firewalls to see if specially crafted packets are able to slip past the firewall for either of the following reasons:
  - The packet *matches* a permit rule.
  - The packet *doesn't match* a deny rule.
- Another reason a specially crafted packet can slip through is because not all firewalls are capable of payload inspection.
- In some cases, the packets may have slipped through because the Access Control List (ACL) was not configured correctly.

Scanning the Firewall

- The team can port-scan the public address of the host or firewall to see which ports are open or are listening.
- Firewalking is another method to discover details of the network
    - Firewalking uses a combination of traceroute and port scanning to discover the details of the internal network.
- To streamline the workflow the team can use automated tools
    - In addition to custom nmap scripts, there are several automated tools for WAF detection available on GitHub such as Wafw00f and WAFNinja.

Avoiding AV detection

- In general, there are a few methods to avoid AV detection:

1. Create a metamorphic virus, which transforms as they propagate and makes pattern detection nearly impossible.

2. Obfuscate a known signature using a tool such as ObfuscatedEmpire

3. Use specialized tools or payloads such as fileless malware that use OS embedded functions that are difficult to detect.

Using the Social Engineering Toolkit

- Using SET along with Metasploit, the team can create a malicious payload
  - Such as a virus, worm, or Trojan, and embed the payload in a PDF.
- Once complete, the team can run a test to see if the payload is detected when introduced on the network.

Review Activity: Detect Defenses

- Outline why it’s important for the team to identify any devices such as load balancers, reverse proxies and firewalls during scanning
- List ways the team can identify a web application firewall
- Discuss reasons why specially crafted packets can slip past a firewall
- Review ways the team can learn the details of a firewall
- Compare methods to avoid AV detection
- Describe how to use SET to create a malicious payload

Lab Activity

Assisted Lab: Exploring OpenVAS

- 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 5

Topic 5C

Utilize Scanning Tools

Analyzing the Attack Surface

- During the footprinting and reconnaissance phase, the team will have used a variety of OSINT tools to gather information.
- In addition, the team might also utilize tools specific to the types of targets on the network
    - Web-based tools that scan remote targets for hosts, services, and other details.

Using Censys and OpenVAS

- **Censys** is an attack surface analyzer, to identify exposed systems.
- Once you have run the scan, you can examine more details:
  - Services running, ports in use, along with any software vendors that were recognized.
- **OpenVAS** will list the vulnerabilities along with a risk rating that summarizes the overall state of the site that was tested.
  - Below the summary, you will see details that include the CVSS value and the CVE number.

Crafting Packets

- During the PenTest, the team may use packet crafting
  - To test firewall rules, evade intrusion detection, or cause a denial of service.
- Packets can be crafted using the following methods:
  - Command line, GUI, script options or packet crafting tools such as Yersinia and Bit-Twist
- The type of packet you craft will depend on the firewall product.

Evaluating Web Applications

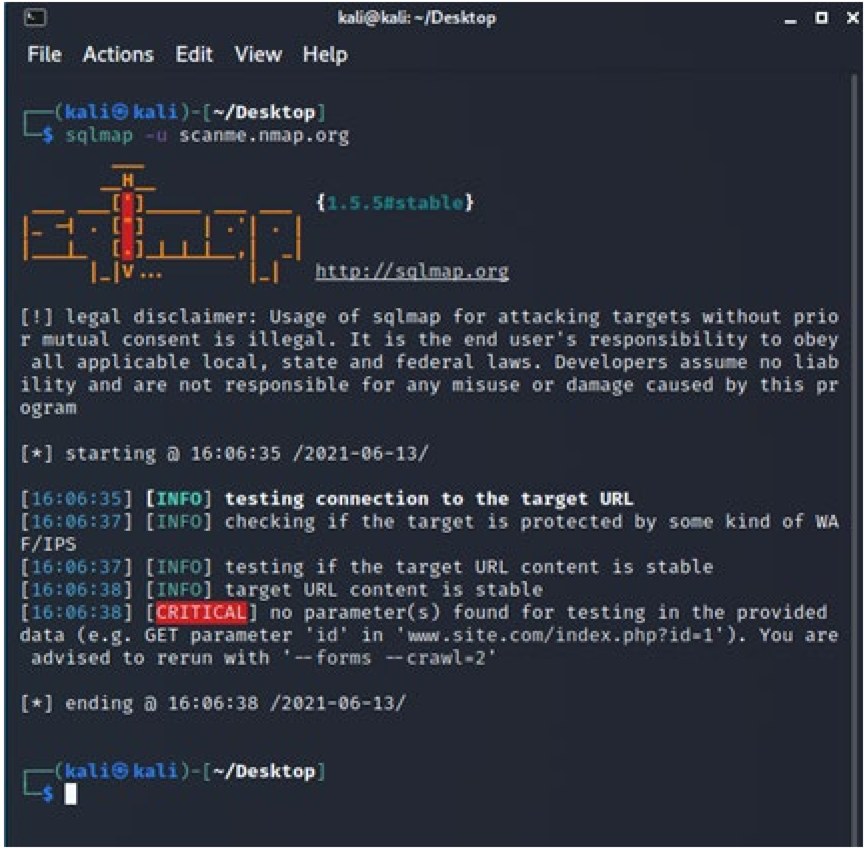
- Web servers are often public-facing, whereas database servers are almost always on the private network.
- If you have access to the internal network, you can try scanning the SQL server directly using TCP port 1433 or UDP port 1434.
  - Test to see if you can pass illegal commands to the SQL server
  - Attempt to launch an SQL injection attack.

Scanning the Web Server and Database

- Some possibilities for scanning include:
  - Web server on TCP 80 or 443 for server-specific vulnerabilities
  - Servers that run on nonstandard ports
  - Web applications for SQL-injection-related vulnerabilities
- There are many web application vulnerability scanners available:
  - Arachni, Skipfish, Grabber, Wapiti, OWASP ZAP, and Metasploit Pro.

Using SQLmap

- An open-source database scanner
- Locates and exploits SQL injection flaws.



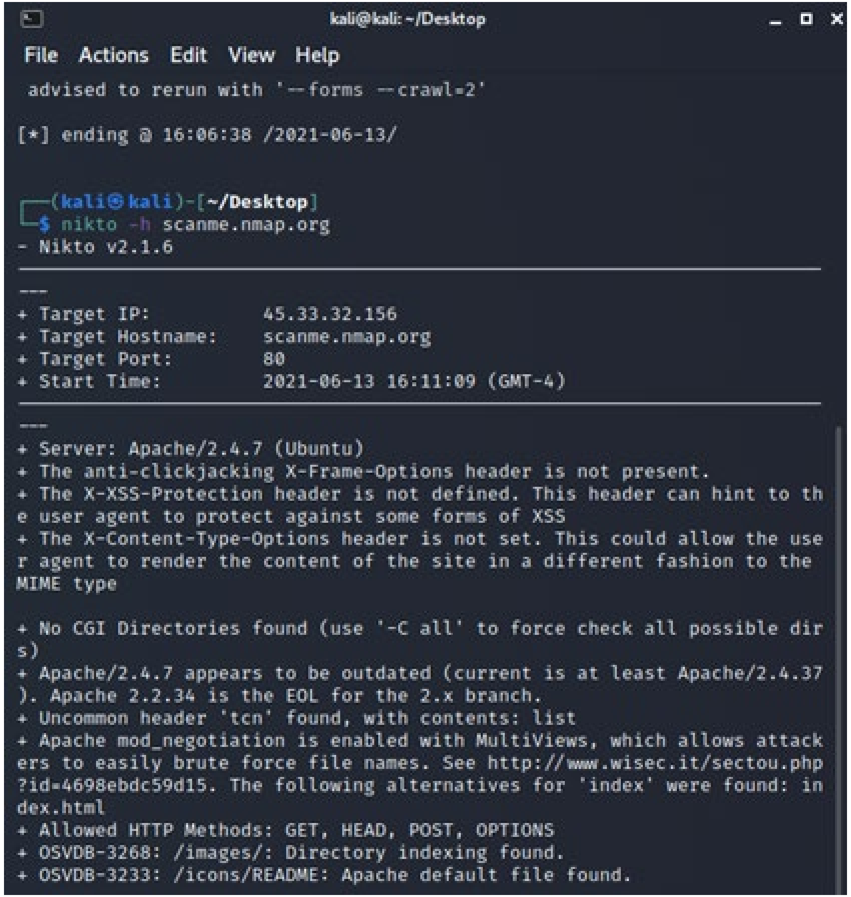
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sqlmap -u scanme.nmap.org
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.5#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prio
r mutual consent is illegal. It is the end user's responsibility to obey
 all applicable local, state and federal laws. Developers assume no liab
ility and are not responsible for any misuse or damage caused by this pr
ogram

[*] starting @ 16:06:35 /2021-06-13/

[16:06:35] [INFO] testing connection to the target URL
[16:06:37] [INFO] checking if the target is protected by some kind of WA
F/IPS
[16:06:37] [INFO] testing if the target URL content is stable
[16:06:38] [INFO] target URL content is stable
[16:06:38] [CRITICAL] no parameter(s) found for testing in the provided
data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are
 advised to rerun with '--forms --crawl=2'

[*] ending @ 16:06:38 /2021-06-13/


┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Checking SSL/TLS Vulnerabilities

- Most websites today rely on cryptographic concepts such as SSL/TLS to protect data in transit from exposure.
- As a result, the team will also want to check for vulnerabilities:
  - **Logjam** vulnerability can weaken the encryption complexity
  - **Freak** vulnerability attacks the RSA-export keys and can allow a malicious actor to decrypt the communication stream
  - **Poodle** vulnerability alters the way SSL 3.0 handles block cipher mode padding to be able to select content within the SSL session

Using Nikto

- Can test for a variety of vulnerabilities:
    - Anticlickjacking
    - X-Frame-options header
    - Dangerous files
    - CGIs



```
 advised to rerun with '--forms --crawl=2'

[*] ending @ 16:06:38 /2021-06-13/


┌──(kali㉿kali)-[~/Desktop]
└─$ nikto -h scanme.nmap.org
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2021-06-13 16:11:09 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to th
e user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the use
r agent to render the content of the site in a different fashion to the
MIME type

+ No CGI Directories found (use '-C all' to force check all possible dir
s)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37
). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attack
ers to easily brute force file names. See http://www.wisec.it/sectou.php
?id=4698ebdc59d15. The following alternatives for 'index' were found: in
dex.html
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
```

Review Activity: Utilize Scanning Tools

- Compare how Censys and OpenVAS identify exposed systems
- Explain why and how the team can craft packets
- Discuss ways to test web server and the database
- Describe how SQLmap can test for SQL injection flaws
- Explain why you should check for SSL/TLS Vulnerabilities
- List ways Nikto can test for vulnerabilities

Lab Activity

Assisted Lab: Using Web Scanners

- 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 5

Summary