CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 6

Scanning Logical Vulnerabilities

Objectives

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

Lesson 6

Topic 6A

Scan Identified Targets

Discovering Network Hosts

- A discovery scan (or ping sweep) is used to find hosts on a network that are up and responding.
    - Probes include using protocols such as TCP, UDP, and SCTP.
- If a firewall is blocking standard probes, you can try other scans:
    - TCP SYN Ping or TCP ACK Ping
    - UDP Ping, IP Protocol Ping, and ARP Scan

Scanning Ports

- Once live hosts are identified, the next step is to run a port scan to see if any live hosts have ports that are open and listening.
  - Ports include Port 25 (SMTP), Port 53 (DNS), and Port 80 (HTTP)
  - The actual number of open ports on a single host will depend on the number of services and listening applications that are running on that machine.
- The scan can either attempt to fully connect with the host, or they can use a stealth scan so they can remain undetected.

Fully Connecting with the Target

- A full scan or TCP connect scan will use a standard TCP three-way handshake.
    - Once the connection is made, the scanner will send a TCP reset (RST) to the server to kill the connection.
    - The scanner then logs the connection and moves on to the next port to attempt to connect to the next service.
- Full scans produce the most results but are also the "noisiest" and the most likely to be detected.

Operating in Stealth Mode

- To avoid detection the team can use a stealth scan, where the communication is one-sided, and no response expected.

- Stealth scans include the following:
  - TCP SYN (or half-open) scan
  - FIN scan
  - NULL scan
  - XMAS Tree scan

Testing Web Applications

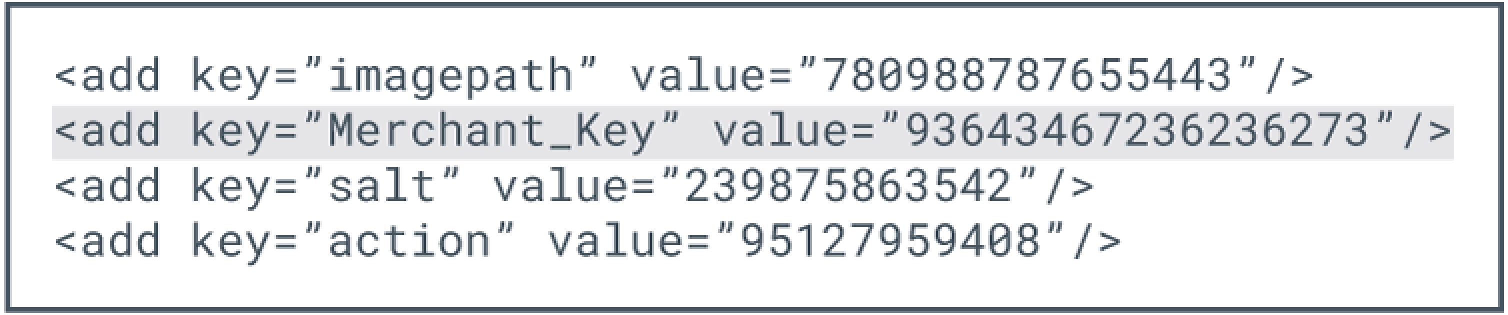
- Scanning a web server and applications generally involves:
    - Crawling through web pages to gather usable content
    - Scraping data, examining links and discovering assets
- Results will depend on whether running a credentialed or non-credentialed scan.
    - **Credentialed scan** uses credentials which can produce more information
    - **Noncredentialled scan** uses fewer permissions, and many times can only find missing patches or updates.

Interacting with the Web Application

- Web scanners will examine elements:
  - Form fields and code for identified vulnerabilities and sensitive content.
- Today there are many commercial web application scanners, from vendors such as Acunetix, Qualys, and Netsparker.
- In addition, there are also open-source scanners and web crawlers, such as those built within Kali Linux

Examining API Requests

- An API is a set of commands that is used to send and receive data between systems, such as a client and a server
  - More secure as the client never interfaces directly with the server.
- The PenTest team should search for exposed information such as an API key in the source code, as shown in the graphic:



```
<add key=”imagepath” value=”780988787655443”/>
<add key=”Merchant_Key” value=”93643467236236273”/>
<add key=”salt” value=”239875863542”/>
<add key=”action” value=”95127959408”/>
```

Automating Vulnerability Scanning

- Vulnerability scanners are designed to check for new and existing vulnerabilities, then present a report to the analyst for evaluation.
- Application vulnerability testing methods are grouped into two main categories:
  - **Static Application Security Testing (SAST)** is done early in the software development life cycle to examine the code for security vulnerabilities.
  - **Dynamic Application Security Testing (DAST)** is done after the code is placed in production.

Using Automated Tools

- When using automated tools, they must be constantly updated with the latest vulnerabilities
- Security Content Automation Protocol (SCAP), is a US standard
    - Used to ensure applications are in-line with mandated security requirements.
    - Continuously monitors systems for vulnerabilities

Review Activity: Scan Identified Targets

- Compare discovery scans with port scans
- Outline how full scan or TCP connect scan works
- Discuss why you would operate a scan in stealth mode
- Review what happens when scanning a web server and applications
- Explain the significance of examining API requests
- Compare vulnerability scanning methods and list the benefits of automating the scanning process

Lesson 6

Topic 6B

Evaluate Network Traffic

Sniffing Using Wireshark

- Sniffing traffic is a way to passively obtain information, such as:
  - Network hosts, services, and device types
  - Protocols, such as: TCP, ARP, SMTP, and HTTP
  - Subnets, IP, and MAC addresses
  - Host information from traffic contained in NBNS messages.
  - User account names found in Kerberos traffic.

Effectively Monitoring Traffic

- To effectively use packet analysis, the team will need to select an appropriate location to visualize the traffic.
- Some guidelines to effectively monitor network traffic:
  - The sniffer's interface must be in promiscuous mode to gather all traffic.
  - If the team is testing a WLAN, the sniffer must be within radio range.

Capturing Data

- If the traffic is in cleartext, you can capture credentials, files, images, messages, and data meant for other users and machines.
- Even if the payload is encrypted, you can still extrapolate vital information:
  - Source and destination address and ports
  - WLAN SSIDs and accompanying cleartext messages.
  - Handshakes and outside wrapper IP addresses of VPN traffic
  - DHCP traffic will display MAC address, as well as host name in plain text.

Scanning with Nessus

- Nessus is a powerful scanning tool that can scan either an enterprise or home network.

- Nessus can complete a basic or advanced network scan, along with other scans to measure the effectiveness of your security controls.

- Once the scan is complete, you'll be able to view and analyze the results

Improving the Scanning Process

- Scanning an enterprise network can be a time-consuming process.
  - To improve the efficiency of the scan, the team can create a policy that includes key network credentials that can be used for future scans.
- In addition to vulnerability scans, Nessus can help ensure the network is properly segmented.
  - Network segmentation logically separates each segment using subnets, VLANs, and or firewalls to isolate each segment
  - Separating the networks prevents them from being able to communicate with one another.

Gathering ARP Traffic

- The team can use MAC addresses can be useful in several ways.
  - Discover hosts on a network.
  - Use MAC addresses to launch an ARP poisoning attack.
- To gather ARP traffic, the team can use the following:
  - Nessus, which has several plugins to enumerate MAC addresses on targets
  - Nmap using the following command: nmap -PR -sn <target>.
  - Arping is a tool found in Kali Linux.

Review Activity: Evaluate Network Traffic

- Explain what information can be obtained when sniffing traffic
- Describe how the team can use Nessus
- Outline how and why the team might gather ARP traffic

Lesson 6

Topic 6C

Uncover Wireless Assets

Securing Access Points

- Wireless networks allow us to freely roam and keep connected with the outside world.
  - Along with this convenience comes the threat of malicious actors joining an unsecured network and being able to access our communications.
  - As a result, it’s best to periodically check the security of WAP
- During reconnaissance, the PenTest will focus on discovering open and unsecured WAPs that the target might have in place

Wardriving Open Access Points

- War driving is a technique that involves driving around to search for open access points using a laptop or smartphone.
- The team can use tools such as Aircrack-ng, Kismet, or Wifite to search for open WAPs.
    - It’s also beneficial to have packet analysis software running during the test to gather and save the information.
    - After analysis, the information can then be used to launch an active attack.

Mapping WAP Using WiGLE

- WiGLE is an OSINT tool to help during the reconnaissance phase
- Once you are in the interface, you can do the following:
  - Enter a location, such as a city or specific address
  - Choose an appropriate date range
  - Select an option, for example “Possible Freenet"
- Once you have selected a location and set your filters, the interface will be populated with dots.
  - Each dot represents an access point, where you can zoom in to learn more about that AP.

Amplifying the WiFi Signal

- A Wi-Fi signal is the amount of power used in an access point or station.
  - The goal is to have a good Signal-to-Noise Ratio (SNR).
- The signal strength of a wireless antenna is referred to as decibels per isotropic (dBi) and can vary according to the design.
- When either war driving or PenTesting the wireless network, amplifying the signal can make a difference in the results.

Selecting an Antenna Design

- When conducting the PenTest, it's best to select an antenna based on the specific needs.
- For example, the antenna can be:
  - Directional in the signal coverage is limited to a specified direction.
  - Omni-directional transmits a signal in all directions.
  - Parabolic which has a curved surface that has a fixed pattern, like a laser beam.

Review Activity: Uncover Wireless Assets

- Describe why it’s essential to test the security of the organization's WAPs
- Explain how the team can use wardriving during the PenTest
- Compare the different types of antennas

Lesson 6

Summary