CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 7

Analyzing Scanning Results

Objectives

- Given a scenario, analyze the results of a reconnaissance exercise.
- Given a scenario, perform vulnerability scanning.
- Given a scenario, research attack vectors and perform wireless attacks.

Lesson 7

Topic 7A

Discover Nmap and NSE

Scanning Interesting Targets

- Nmap is the most widely used network scanner today and has a wide range of flexible options and expanded capabilities:
  - Host and service discovery
  - Operating system fingerprinting
  - Gathering MAC addresses
  - Detect vulnerable hosts

Timing and Performance Considerations

- Vulnerability scanning is part of the PenTest exercise; however, the process can be aggressive or intrusive
- You can adjust the scan by using the timing option: -T <0 - 5>, where T0 is the slowest and T5 is the fastest
- In some cases, network devices enforce rate limiting, which limits the data flow by either policing or shaping the traffic.
    - Nmap will detect whether rate limiting is in place and will adjust the scan to avoid flooding the network.

Using TCP or UDP when Scanning

- TCP can provide more detailed results when scanning. Nmap has a variety of scans that use TCP that include:
  - A TCP ACK scan is used to bypass firewall rulesets
  - A full (or TCP connect) scan and Christmas tree scan
- UDP scans are generally slower and more difficult. In addition, open and filtered ports rarely send any response.
  - Because of this, the team may choose not to run a UDP scan.

Scripting with Nmap Scripting Engine (NSE)

- NSE scripts are a core component of Nmap that allows users to customize activity and automate the scanning process.
    - Perform advanced network discovery
    - Determine vulnerabilities
    - Uncover the existence of malware such as Trojans and backdoors.
- To use an Nmap script, type the following:
    - nmap - - script <name of script>

Using the Nmap Library of Scripts

- Scripts are grouped into several different categories that include:
  - **Malware**—scripts capable of detecting malware.
  - **Discovery**—scripts that can discover networks, services, and hosts.
  - **Vulnerabilities** –a variety of exploitation commands.
- To use more than one script in a command, use a comma between each command
- A powerful option is to use the base script identifier and the wildcard option, or run all scripts in a specific category

Review Activity: Discover Nmap and NSE

- Outline reasons Nmap is the most widely used scanner today
- Explain ways to throttle back the scanning process
- Compare TCP and UDP scanning techniques
- Discuss the variety of NSE scripting options

Lab Activity

Assisted Lab: Understanding Nmap Common Usage

- 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 7

Topic 7B

Enumerate Network Hosts

Mapping the Network

- Prior to launching an attack, the team will need to map the network
  - To provide details on hosts and services running on the target environment.
- When evaluating the network, it’s important to gather as many details as possible. Some of the scans include:
  - **Ping Scans** - to learn which machines are responding.
  - **TCP Scans** - to check for open and listening TCP ports
  - **OS Footprinting** - to identify the operating systems in use on the network.

Detecting Interesting Hosts

- The team will need to use a variety of scans to get a solid grasp on the environment.
- By default, Nmap uses the following during host discovery:
  - TCP SYN packet to port 443
  - TCP ACK packet to port 80
  - ICMP type 8 (echo request)
  - ICMP type 13 (timestamp request)
  - ARP requests to obtain MAC address details

Adjusting the Scans

- The team may need to adjust the scans if they run into problems.
- For example, if a firewall is blocking the default ICMP pings, the team has other options. For example, they can try the following:
  - **TCP ACK Ping -PA <portlist>** This will set the ACK flag in the TCP header.
  - **UDP Ping -PU <portlist>** This scan uses User Datagram Protocol (UDP).
- Nmap will display the ports that were detected, which can be in one of four states:
  - Open, closed, filtered and unfiltered

The Host Discovery Phase

- During host discovery, the team has some options as follows:
  - Skip the discovery phase altogether and treat all hosts as if they are online by using the switch `−Pn`.
  - Complete the network discovery *without* doing a port scan using the switch `−sn.`
  - Run a script without either a ping or port scan by using the two options `−Pn −sn` together.

Fingerprinting the Operating System

- Nmap can detect the OS and version in use along with service detection for a single host or a range of devices.
  - Once the vulnerable machine(s) are identified, the vulnerabilities can either be mitigated, or the team can attempt to actively attack the system.
- During fingerprinting, the team can use passive or active scanning.
  - **Passive** - gathers network traffic using a packet sniffer such as Wireshark, without actively attempting to contact any hosts.
  - **Active** - actively sends probes to a target and then analyzes the packets that are returned.

Determining the OS

- Once a response is received from the target, Nmap will make a best effort estimate of what OS is in use.

- Some of the key elements used to determine the OS include:

  - **Don’t Fragment (DF) bit**—Is the DF bit in the IPv4 header on or off?

  - **Window Size (WS)—**What does the OS use as a WS?

  - **Time to Live (TTL)—**What is the TTL value set on the outbound packet?

Review Activity: Enumerate Network Hosts

- Outline what’s involved when mapping the network
- Explain the different scans Nmap uses during host discovery
- List techniques the team can use to modify the intensity of a scan
- Review options the team can use during host discovery
- Describe ways to fingerprint the OS
- Discuss methods Nmap uses to determine a target’s OS

Lab Activity

Assisted Lab: Understanding Scan Output

- 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 7

Topic 7C

Analyze Output from Scans

Examining Network Traffic

- Depending on the type of test, the team will need to gather as much information on the target
- Some of the questions the team will need to find out include:
  - Which host(s) and devices are interesting and worth pursuing?
  - Where is the target located?
  - What is it we want when we gain access to a device or host?
  - When and how should we attack?

Testing Methods

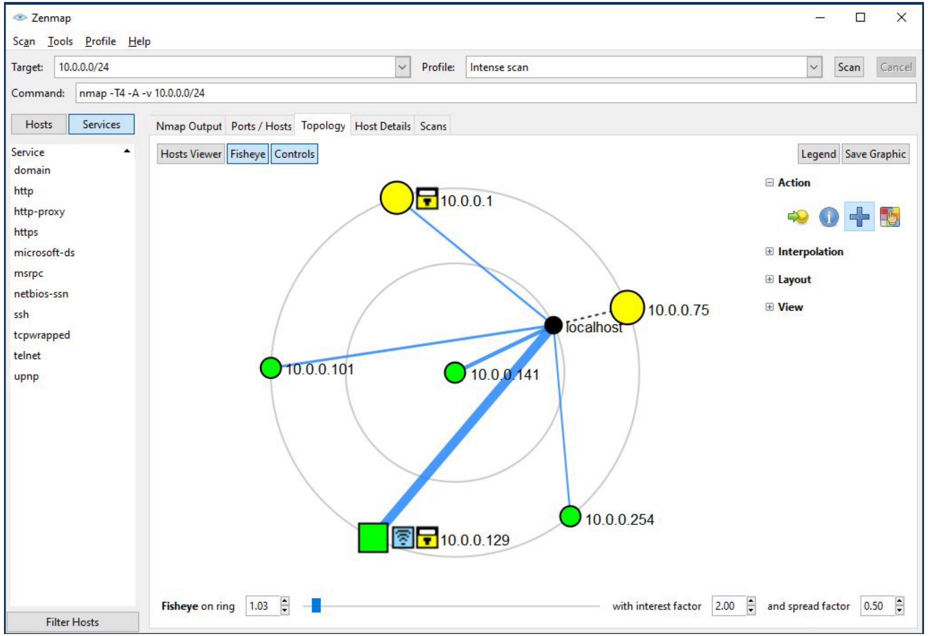
- Depending on the parameters of the project scope, the team might use one of three methods when testing:
  - **Unknown environment -** no information is presented to the team
  - **Partially known environment** the team is given some information
  - **Known environment** the team is given all details of the environment
- Once the team learns more information, they can outline the network topology and identify the boundaries more clearly.

Reporting with Nmap

- Nmap can provide exceptional results when discovering network devices and related vulnerabilities.
- When viewing the results of a scan, Nmap has several available formats for outputting the results as follows:
  - **Interactive output** – human readable output and is the default
  - **XML output (-oX)** - a flexible format option
  - **Grepable output (-oG)** - creates a grepable friendly file
  - **Normal output (-oN)** is like interactive; however, you can save the results of an Nmap scan to a text file for later analysis.

Interfacing With Zenmap

- A GUI companion to Nmap
  - Can be used on a variety of platforms, including Windows.
- Creates a visual of the network topology
  - To assess devices and provide an insight when planning an attack.



Target: 10.0.0.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 10.0.0.0/24

Service

domain

http

http-proxy

https

microsoft-ds

msrpc

netbios-ssn

ssh

tcpwrapped

telnet

upnp

Fisheye on ring 1.03 with interest factor 2.00 and spread factor 0.50

Footprinting using DNS

- Can reveal additional targets that can help the team learn more about the structure of an organization's network.

- DNS can fall victim to several threats that include:
  - A flood or amplification attack.
  - Cache poisoning.
  - Exposure of the zone file.

Targeting the DNS Servers

- When dealing with DNS there are two servers can be at risk for compromise: Authoritative and Recursive
- Nmap has several methods to test DNS for vulnerabilities.
- For example, you can use the following to discover the target host's services: nmap --script=dns-service-discovery -p 5353 <target>
  - The script uses the DNS Service Discovery protocol to get a list of services.
  - Once obtained, Nmap will follow up by sending probes to get more information.

Transferring Zone Information

- A zone file is a text file that contains information and resource records (RR) for a specific namespace.
- The following are some of the RR found in a zone file:
  - Type A Maps a hostname to a 32-bit IPv4 address of the host
  - Type AAAA Maps a hostname to a 128-bit IPv6 address of the host
  - PTR (Pointer) used for reverse DNS lookups
  - MX Mail Exchange record

Exposing the Zone File

- If not properly configured, the zone file can be exposed and leak resource record information.
- An attack occurs when an entity poses as a DNS client server and asks for a copy of the zone records.
- This can be achieved using the Nmap script dns-zone-transfer.domain.
    - If the server honors the request, it will return the zone file.

Poisoning The DNS Cache

- If the server is not properly configured, this can lead to an attack, such as a DNS cache poisoning attack.
  - Corrupts the cache of a recursion server to point to a bogus IP address.
- To test for vulnerabilities the team can attempt to perform a dynamic DNS update without authentication using the following:

  -
    ```
    nmap -sU -p 53 --script=dns-update --script-
    args=dns-update.hostname=target.example.com,dns-
    update.ip=192.0.2.1 <target>
    ```

Exposing Vulnerable Web Servers

- During the PenTesting exercise, the team can test the organization's web server using a few methods:
  - Manually examine the source code and elements within the site for comments or other interesting artifacts
  - Examine the web or access logs that show the activity for a website.
  - Intercept traffic using a proxy between the web client and the server.

Using Burp Suite

- Burp Suite is an integrated platform used to test the security of web applications.
    - Acts as a local proxy to capture the HTTP requests and responses
- When using a proxy, the team can gather more data to check for security issues that occur during a web transaction.
    - Vulnerabilities can include cryptographic weaknesses, missing or weak authentication, and other web vulnerabilities .
- When discovered, Burp Suite will list the details of the vulnerabilities within the dashboard.

Review Activity: Analyze Output from Scans

- List some of the questions the team will need to find out when examining network traffic
- Describe some of methods used when testing
- Discuss how Burp Suite can be used to test web applications.

Lab Activity

APPLIED Lab: Using Scanning a Vulnerable System

- 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 7

Summary