eJPT Certification

Section: Footprinting and Scanning

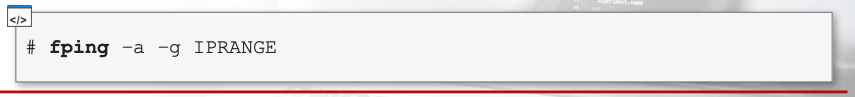
08/7/2020

**Learning Objectives**

* Discovering and mapping network environments.
* Tools, methods, and techniques to perform proper reconnaissance on the network level.

**Mapping a Network**

* Why is it important?
  + Enables you to perform efficient penetration test.
  + Knowledge of your in-scope targets.
  + Ability to create a technological map.
* After the information gathering stage the penetration tester begins fingerprinting and enumeration of the nodes on the client’s network.
* Every host connected to the internet or private network must have a unique IP address which identifies it.
  + Address block, 200.200.0.0/16 means that that the network could contain up to 65536 (2^16) hosts with IP addresses in the 200.200.0.0 – 200.200.255.255 range.
  + The pentester must figure out which of the 65536 IP addresses are assigned to a node.
* **Ping Sweeping**
  + This is the fastest and most efficient way to check all 65536 hosts.
  + Ping, is a command that is designed to test if a machine is alive on the network. The ping command is used on the command line.
    - **A screenshot of a cell phone

      Description automatically generated**Example: ping [www.example-site.com](http://www.example-site.com)
  + Ping works by sending one or more special ICMP packets (type 8- echo request) to a host.
  + If the destination host replies with ICMP echo reply packets, then the host is alive.
    - ICMP is a protocol used to carry diagnostic messages. ICMP uses the services provided by IP, but it is actually a part of the Internet protocol.
  + Ping sweeping automatically perform the same operation to every host in a subnet or IP range, saving us from typing hundreds or thousands of ping commands.
* **Fping**
  + ****an improved version of the standard ping utility on Linux. Can also be used for ping sweeping.
  + **– a** option forces the tool to show only hosts that are alive, while **-g** option tells the tool that we want to perform a ping sweep instead of a standard ping.
    - IP range can be defined by using CIDR Notation or by specifying the start and the ending addresses of the sweep.
  + When you run fping on a LAN you are directly attached to, even when using the -a option, you get a warning message (ICMP Host Unreachable) about offline hosts.
    - **A screenshot of a cell phone

      Description automatically generated**To get by these messages we can redirect standard error messages to /dev/dull.

**Nmap Ping Scan**

* Nmap (Network Mapper)
  + Open source tool.
  + Network exploration and security auditing.
  + Can perform ping scans by using **-sn** command
    - Can specify targets on command line in CIDR format as a range and by using wildcard notation.

**A screenshot of a cell phone

Description automatically generated**

* + We can also save a host list in a file and input the list using the -**iL** command
    - Example:

**A picture containing knife

Description automatically generated**

**OS Fingerprinting**

* In this step we transform the list of live networks we have curated from our nmap scan and begin fingerprinting our IP addresses.
* OS fingerprinting – the process of determining the operating system used by a host on a network.
  + To find out the OS of the target system you have to send network requests to the host and then analyze the responses back.
    - This works because of small differences in the network stack implementation of the various OS’s.
  + Fingerprinting tools send a series of specifically crafted requests to the target host. In return, the fingerprinting tool examines the responses and creates a signature of the host behavior.
  + Signatures are compared against a database of known operating systems signatures.
    - A little bit of guesswork, but utilizing proper tools cuts down the process significantly.
* During a pentest you will have to perform this type of recon on every network node, including:
  + Routers
  + Firewalls
  + Hosts
  + Servers
  + Printers
  + Etc.

**OS Fingerprinting with Nmap**

* To perform OS fingerprinting with Nmap you must use the **-o** command and specify your target(s).
  + You can add -**Pn** to skip the ping scan if we know that our targets are alive
    - Example



* + A screenshot of a cell phone

    Description automatically generatedWe can fine tune our fingerprinting process by implementing filters into our nmap command.

A screenshot of a cell phone

Description automatically generated

**Port Scanning**

* Why is this important?
  + Prepare for vulnerability assessment phase.
  + Perform stealth reconnaissance.
  + Detect firewalls.
* Begin port scanning after network mapping and operating systems are performed.
* Now it’s time to discover daemons and services running those nodes: port scanning.
  + Daemons are long-running background processes that runs on a server and answers requests for services.
    - Examples: inetd, httpd, nfsd, sshd, named, and Ipd.
* Port scanning is used to find open TCP and UDP ports on target hosts.
  + Enables pentesters to learn information about target’s daemon, in terms of software and version, is listening on a specific port.
* The ultimate goal of port scanning is to find the software name and version of the daemons running on each host.
* **Under the Hood of a Port Scanner**
  + Sends probes to the targets and analyzes the responses.
  + Port scanners automate probes request and response analysis. Give information about the targets but also lets you detect if there is a firewall between you and the target.
* **TCP Connect Scan**
  + If the scanner receives a RST packet, the port is closed.
  + If the scanner completes the 3-way handshake, then the port is open. After connecting, the scanner sends an RST packet to the target host to abruptly close the connection.

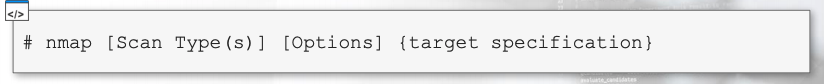
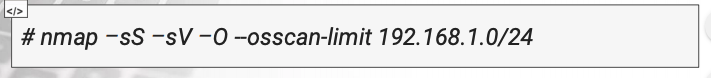
**A picture containing clock

Description automatically generated**

* + **A picture containing clock, meter

    Description automatically generatedExample of a closed port**
* **TCP Connect Scan**
  + Every TCP connect scan probe gets recorded in the daemon logs, because from the applications point of view the probe looks like a legit connection. This can be easily detected by system administrators.
* **TCP SYN Scan**
  + Stealthy by design.
  + During a SYN scan, the scanner does not perform a full handshake it just sends a SYN packet and analyzes the response coming from the target machine.
  + A TCP packet with the SYN flag enabled is sent to the <host> : <port> pair and:
    - If scanner receives RST packet, then port is marked as closed.
    - If scanner receives ACK packet, then port is open. After marking the port as open, the scanner sends an RST packet to the target host to stop the handshake.
    - Because the handshake is never complete there is no real connection to the destination daemon. This means that the scan cannot be detected by the host and is not logged in the daemon logs.

**Scanning with Nmap**

* Nmap syntax:
* ****Example:
* Most commonly used scan types:
  + -sT performs a TCP connect scan.
    - Gets recorded in the application logs on the target system.
  + -sS peforms a SYN scan.
    - A well-configured IDS will still detect the scan
  + -sV performs a version detection scan.
    - Mixes TCP connect scan with some probes, which are used to detect what application is listening on a particular port.
      * Not stealthy.
      * TCP connect scan reads from the server the **banner** of the daemon listening on a port.
        + If the daemon does send a banner by itself, Nmap sends some probes to understand what the listening application is. The idea behind this is to guess the application and its version by studying It’s behavior.

**Specifying the Targets**

* You can specify targets by using DNS names, IP address lists, CIDR notation, wildcards, ranges, octets lists, and input files.