Chapter 3 – Passive Recon and Active Recon

1. What is Subdomain Enumeration?

It is the process of listing out all the valid subdomains that are part of larger domains. Each subdomain is related to a specific function.

1. In [www.aast.edu](http://www.aast.edu), identify the subdomain, root domain, and the top level domain.

Top Level Domain: edu

Root Domain: aast

Sub Domain: www

1. What other subdomains might exist beside www ?

* mail.aast.edu
* studentportal.aast.edu

1. What is Recon -ng and how is it used?

It is an open-source reconnaissance framework for collecting information (active and passive). Modules are used when you use Recon -ng.

Examples:

* recon/hosts-hosts/resolve(active recon): This module is used to take a list of hostnames and performs DNS resolution to get the corresponding IP address
* recon/domains-hosts/bing\_domain\_web(passive recon): This module quries Bing’s research engine to discover search domains
* recon/domains-hosts/google\_site\_web(passive recon): This module finds hosts with given domains
* recon/domains-hosts/brute\_hosts( active recon): This module discovers sub domains by bruteforcing common sub domain names

1. What is DNSdumpster?

DNSDumpster.com can be used to discover subdomains, and their IP addresses and attempt to geolocate them.

1. What is Subfinder?

A tool that’s used for finding subdomains.

1. What is amass?

Performs network mapping of attack surfaces and external asset discovery.

1. What is whois?

It’s a database that has information about a domain as soon as someone buys it and uses it. It provides information about ownership and registration details and expiration dates and so on.

1. What is wappalyzer?

It is a technology profiler that tells how the website was built.

1. What is a nmap?

It is a network discovery and auditing tool. This tool enables us to scan for

* Open ports and services
* Discover services + their version
* Guess the operating system running on a target machine
* Monitoring hosts

1. What is TCP-SYN-Scan (-sS)?

It is fast and stealthy

Requires privilege

1. Why is it stealthy?

**Because the three-way handshake connection is not completed.**

* It first sends a SYN packet as if to establish a connection
* Then the target responds with one of those three things: SYN/ACK, RST, and no response
* SYN/ACK 🡪 port is open. The scanner doesn’t complete the connection
* RST🡪 This indicates the port is closed.
* No response🡪 This indicates the port is filtered (blocked by a firewall)

1. What is the TCP-Connect-Scan (-sT)?

Relies on the operating system and is slower than sS.

1. What is the UDP-Scan (-sU)?

It is an unreliable and slow scan and it is unreliable because there is no acknowledgement.

1. What does the TCP connect Scan?

There is a three-way handshake connection.

* The client sends a TCP request to the target server along with a SYN flag set.
* Then the server response by acknowledging it along with the flag.(SYN AND ACK)
* Then the client completes the handshake by sending a TCP request with an ACK flag set.

1. In the TCP connect scan, what happens when the port is closed?

The response will be a TCP packet with the RST flag set. Now the nmap can establish that the port is closed.

1. In the TCP connect scan, what happens when the port is open?

The response will be a TCP packet with the SYN/ACK flag set. Now, the sender completes the handshake by sending an ACK flag set along with a TCP packet.

1. In the UDP scan, when there’s no response, what does that mean?

Nmap refers to that as open | filtered. This means that the port might be open but it is being blocked by a firewall. Then the request is sent another time. Then if there’s still no response and is marked open | filtered.

1. What happens if there’s a response during the UDP Scan?

This means the port is open.

1. In the UDP connect scan, what happens when the port is closed?

The receiver responds with an ICMP ping packet contains a message that says the port is unreachable.

1. What is a Nmap Ping Sweep?

* NMAP send an ICMP packet to each possible IP for a specific network
* When it receives a response, it indicates that this device is alive
* Example: nmap -sn 192.168.0.1-254

1. What does this “nmap -F scanme.nmap.org” dp?

It scans 100 top ports only.

1. nmap -p 22,53,80,443,500-1000 scanme.nmap.org?

This checks specific ports and a port range.

1. nmap -O scanme.nmap.org?

It is used to detect the operating system.

1. nmap -A scanme.nmap.org?

This is aggressive scanning and it checks the OS and its version, script scanning, and traceroute.

1. How to scan a single host IP 10.0.0.1?

Nmap 10.0.0.1

1. How to scan a subnet range?

Nmap 192.168.10.0/24

1. Scan a range of IPs from 10.1.1.5-10.1.1.100

Nmap 10.1.1.5-100

1. How to scan IP addresses in a text file?

nmap iL hosts.txt

1. How to scan 3 Specified Ips?

Nmap 10.0.0.1 10.1.1.6 10.3.1.2

1. Resolve then scan IP address

Nmap www.subdomian.com

1. Scan a specific port for a specific host

Nmap -p80 10.1.1.1

1. Range of ports?

Nmap -p20-23 10.1.1.1

1. Multiple ports?

Nmap -p80,88,8080 10.1.1.1

1. All ports?

Nmap -p- 10.1.1.1

1. UDP and TCP?

Nmap -sS –s U -p U:53,T:22 10.10.10.1

1. HTTP AND SSH?

Nmap -sp http,ssh 10.1.1.1

1. Version of the operating system?

Nmap -sO 10.1.21.3

1. Version detection scan of open ports?

Nmap -sV 10.1.1.1

1. Service version detection an OS version and traceroute

Nmap -sA 10.10.10.1

1. What is Fuzzing?

It is a way of finding bugs using automation

1. What are the steps for fuzzing?
2. Determining the entry points: what inputs exist, parameters, headers
3. Decide on the payload list: what data to feed into the application
4. Fuzz: systematically input the payload list
5. Give an example of a payload?

SecList Payload

1. What is a SecList Payload?

A collection of wordlists used for fuzzing. It detects already known vulnerabilities. Another way is generating payloads randomly.

1. What are the tools for fuzzing?

* Dirb
* Ffuf
* wfuzz
* gobsuter
* dirsearch

1. What is a phishing attack?

This is a cybercrime where the attacker deceives the victim by contacting them via email, telephone or message to lure individuals into giving them private info by disguising as a legitimate institution. This can result in identifying theft or financial loss.

1. How do they lure them?

* Too good to be true offers
* The messages or phone calls give you a sense of urgency

1. What are the features of a phishing email?

* Hyperlinks
* Attachments
* Unusual sender

1. Give an example of a tool that’s used for creating phishing templates and detecting the results.

Gophish

1. What differs from masscan and zmap from nmap?

It is way faster.

1. Who creates SSL/TLS certificates?

**Certificate Authority**

1. Who is SSL/TLS certificates created for?

For domains

1. How do those certificates protect against malicious activities?

Through **Certificate Transparency Logs**

1. What is DNS Brute forcing?

It is a technique where we prepared a long list of common subdomains to our target domain and try to DNS resolve this new list in hopes of finding valid subdomains of our target domains

1. Give me examples of DNS common subdomains.

Admin.example.com

Internal.dev.example.com

Secret.example.com

Backup01.example.com

1. What is a vulnerability scanner?

It enables organizations to monitor networks and systems for security vulnerabilities.

1. Give an example of a vulnerability scanner.

Acunetix, Nexpose rapid7, nuclei vulnerability scanner