Phase 2

Identify Targets and Run Scans

Phase 2: Identify Targets and Run Scans

Tool/Resources 1: Nmap
Description: Nmap or Network Mapper is a free and open-source tool for vulnerability testing, port scanning, and network mapping. When used properly, Nmap can protect and optimize networks and information. Nmap can help user to map out networks and conduct extensive network inventories. With the ability to scan for devices, Nmap can check if any are not up-to-date and patch them. It also has many functions to help the user to find vulnerabilities within the network.

Ways to use Nmap:

- Network Mapping: With Nmap, users can form a network map that includes servers, routers, switches, and other devices by using scanned ports. Users can also see how the devices are connected from the network map.
- Port Rules Discovery: Users can find out if a port is open or closed by a firewall with a low-level scan from Nmap. It is a technique to check their work when they are setting firewalls.
- Shadow IT Hunting: With the ability to check and discover all types of devices and their location on the network, Nmap can identify the devices (shadow IT) that are not supposed to be there. From there, the user can remove the suspicious device.
- Operating System Detection: Nmap allows the user to scan for the Operation System's patch level and estimated uptime to check if the device is up-to-date or has any vulnerabilities.
- Service Discovery: Nmap can scan to determine what the discovered devices perform. As well as report on which applications are running and what version of the application are being used.

Commands:

- Scan for a range of IP addresses
    - Command: *nmap <IP range>*, Example: nmap 192.168.1.0/24
    - This command will scan the entire CIDR range of IP addresses.
- Scanning the Ports
    - Command: *nmap -p <number> <localhost IP>*, Example: nmap -p 1-80 192.168.1.121
    - This command will scan the ports and provide detail about the ports.
- Scan for Open Ports
    - Command: *nmap -p- <IP address>*, Example: nmap -p- 192.168.1.121
    - This command will find all open ports on a specific target.
- Ping scan
    - Command: *nmap -sP <target>*, Example: nmap -sP 192.168.1.0/24
    - This command scan for the hosts that are running in the network.
- Operating System Detection

    - Command: *nmap -O <target>*, Example: nmap -O 192.168.1.121
- Service Version Detection
    - Command: nmap -sV <target>, Example: nmap -sV 192.168.1.121
    - Those two commands can help to check if any device is not up-to-date for a patch.

Reason to use Nmap:

- Nmap is very flexible because it supports many different advanced network mapping techniques.
- Very powerful, Nmap can scan very large networks.
- Free to use with all the functions, and the functions are improving daily since it's open-source.
- You can ask the community for help if there are any questions or problems with Nmap.
-

Potential drawbacks or limitations of Nmap: Some of the potential drawbacks of nmap are that it can crash some systems when performing scans that are a little heavy-duty. It can be considered hostile when scanning with nmap, so the user must always ask for permission before scanning. Also, nmap can be a dangerous tool if a system administrator turns on the company (Edward Snowden) or someone gets access by using stolen credentials. Also, Nmap can only be exported into XML format.

Tool/Resources 2: Gobuster

Description: Gobuster is a scanner tool that uses brute force to enumerate hidden directories and files of websites from a custom wordlist. Gobuster is also a tool that can help find the DNS subdomains and the virtual host names. It is written using the Go programming language that can be used in a command-line interface.

Ways to use Gobuster:

- DIR mode: used to enumerate URLs for directories and files. It will uncover hidden directories or files within the target domain or subdomain
- DNS mode: used to enumerate subdomains.
- VHOST mode: used to find virtual hosts within the domain. Virtual hosting is when a domain hosts other domain names on single or multiple servers.
- S3 mode: used to enumerate publicly available Amazon Web Service (AWS) S3 buckets.
- Fuzz mode: used to fuzz for parameters

Commands:

- DIR mode: gobuster dir --url [https://example.com/] --wordlist [path/to/file]
- DNS mode: gobuster dns --domain [example.com] --wordlist [path/to/file]
- VHOST mode: gobuster vhost --url [https://example.com/] --wordlist [path/to/file]
- S3 mode: gobuster s3 --wordlist [path/to/file]

- Fuzz mode/ value of a parameter: gobuster fuzz --url [https://example.com/?parameter=FUZZ] --wordlist [path/to/file]
- Fuzz mode/ name of a parameter: gobuster fuzz --url [https://example.com/?FUZZ=value] --wordlist [path/to/file]

Reason to use Gobuster:

- Gobuster has multiple extensive that can help with scanning.
- There is a function "-d" that discovers backup files.
- Gobuster has many modes (I mentioned above) to choose from and is easy to use.

Potential drawbacks or limitations of Gobuster:

- Gobuster can only use one wordlist at a time for scanning.
- Very loud and hostile, definitely will alert people when used.
- There is only one output format (.txt)

Tool/Resources 3: Angry IP Scanner

Description: An open-source and cross-platform network scanner. It is a scanner known for its speed of tasks, simplicity, and very user-friendly. The main purpose of the Angry IP scanner is to scan IP addresses and ports. It can ping network devices and export the scan results into CSV, TXT, XML, or IP-port list files.

Ways to use Angry IP Scanner:

- Scan local networks and the Internet.
- DNS lookup to find the host and domain name.
- Scan for TCP and UDP ports.
- Fetchers: IP address, Ping, TTL(time to live), MAC address, Ports, filtered ports, and version detection.
- Pingers: ICMP echo, Windows ICMP.DLL, UDP, TCP, and ARP.

Reason to use Angry IP Scanner:

- Free to use, open-source.
- The tool can be freely copied and used anywhere. Doesn't require installation.
- One of the easiest tools to use on the market from how simple the GUI is.
- Very good for smaller networks and home use.

Potential drawbacks or limitations of Angry IP Scanner:

- The interface of the tool doesn't scale well on enterprise-size networks.
- It doesn't have any graphing capabilities like other tools on the market.
- It doesn't provide the maximum amount of detailed report information.

Tool/Resources 4: Mitec Network Scanner

Description: Mitec Network Scanner is a free multi-threaded scanner. It is first designed to increase computer security. It can identify active devices on your network and keep them safe. It also ensures that only the ports you need are open.

Ways to use Mitec Network Scanner:

- Scans Active Directory, Network Neighbourhood, IP addresses, MAC addresses.
- Pings function (ICMP)
- Find out the device name and device domain/workgroup.
- Find out the operating system, BIOS, model, and CPU
- TCP and UDP port scanning.

Reason to use Mitec Network Scanner:

- Free to use
- Mitec Network Scanner has an event log that can be viewed for information.
- It can auto-detect the local IP range.
- It can perform several ping sweeps.
- Very simple interface and is user-friendly. Also easy to download.

Potential drawbacks or limitations of Mitec Network Scanner:

- It can only be saved as a CSV file.
- It only runs on Windows Operating System.

Tool/Resources 5: Lansweeper Network Scanner

Description: The Lansweeper Network Scanner is a free IP scanner that scans for all available ports to retrieve information from all devices on the user's network without any installations. It is well organized by all the discovered devices, which users can navigate easily to for information.

Ways to use Lansweeper Network Scanner:

- Scan IP ranges on demand or automatically.
    - Scanning tab > scanning type to (IP range), put in your IP start and end.
    - On the Scanning Credentials section, put SNMP credentials for read-only access.
    - Map those credentials to the created IP Range and press scan now.
- Users can discover a wide range of network protocols with just one click.
    - Firewalls, printers, switches, NAS devices, IP phones.

Reason to use Lansweeper Network Scanner:

- The user interface is easy to navigate to the information the user needs regarding easier tasks.

- Can set up a recurring scanning schedule to always have a completely updated overview of all the assets.
- Can remotely retrieve all sorts of hardware information, such as:
    - IP addresses, Asset type, Operating Systems, Domain, Manufacturer, Model, Hardware info and antivirus info, Network info, and Harddisk space of the device.
- It has a free one-month trial with a maximum of 5,000 quired devices.

Potential drawbacks or limitations of Lansweeper Network Scanner

- There is a limitation of customer service support and the helpdesk.
- The user interface can sometimes be confusing when a harder task is performed.
- It is not free after one month.