Goal: Identify the tools and techniques to be used to perform host discovery and enumeration.

Deliverables should cover at least 5 tools/resources.

- Tool: **Nmap.** Purpose: Obtain information on hosts and the services and operating systems they are running.
  - Commands:
    - Base scan (no flags)
      - nmap <ip address or range of ip addresses>
      - For example: nmap 196.168.1.1 or nmap 196.168.1.0/24
        - This scan will provide the port # that is open, with the state, and service of that port
        - For example:
          - 80/tcp open http
    - Quick host discovery scan (host discovery only)
      - nmap -sn <ip address or range of ip addresses:>
      - For example: nmap -sn 196.168.1.1 or nmap 196.168.1.0/24
        - This scan will provide whether the host/s are up (meaning that they are responding to icmp requests)
        - For example:
          - Nmap scan report for 192.168.1.1
          - Host is up (0.0032s latency)
    - The two above scans will generally bring up the host discovery and base needs requested for Phase 2. However, I've included the flags below just in case.

        - -A Enables OS detection, version detection, script scanning, and traceroute
        - -T0-T5 Changes the speed and intensity of the scan
        - - O Remote OS detection using TCP/IP stack fingerprinting
        - -sV –version-all Enable intensity level 9. Higher possibility of correctness. Slower
        - -f Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters
        - -D Send scans from spoofed IPs
        - -oG Grepable output to the file grep.file
        - Combined example:
            - nmap -p80 -sV -oG – –open 192.168.1.1/24 | grep open
            - Scan for web servers and grep to show which IPs are running web servers
    - Drawbacks:
        - These scans can take a significant amount of time
        - Aggressive scans can overwhelm the network and take down a service
        - If the client is not made aware ahead of time how the scans will affect their network, scans can throw false positives and other disruptions that could cause a negative experience for them during the penetration test. Always look to avoid this.
- Tool: **Dig.** Purpose: Enumerate and obtain information about the DNS servers.
    - Commands:
        - dig <global server> OR <host (ip address) local server>
            - Look up the “A” record for the domain/server

        - Output example:
            - ;;QUESTION SECTION:
            - ;<server> IN   A
            - ;; ANSWER SECTION:
            - <server> 300 IN A 103.15.32.5 (MADE UP IP)
            - ;; AUTHORITY SECTION:
            - <server> 53058 IN NS dde.ns.cloudflare.com
            - ;; ADDITIONAL SECTION:
            - Dde.ns.cloudflare.com 65838 IN A 173.245.43.12 (MADE UP IP)
    - dig <global server> OR <host (ip address) local server> -t mx
        - Look up the “MX” (mail server record) for the domain/server
        - Output example:
            - ;;QUESTION SECTION:
            - ;<server> IN   MX
            - ;; ANSWER SECTION:
            - <server> 300 IN MX 10 mx.stackmail.com (MADE UP IP)
            - ;; AUTHORITY SECTION:
            - <server> 53058 IN NS dde.ns.cloudflare.com
            - ;; ADDITIONAL SECTION:
            - Dde.ns.cloudflare.com 65838 IN A 173.245.43.12 (MADE UP IP)
    - dig <global server> OR <host (ip address) local server> -t ns
        - Look up the “NS” (name server record) for the domain/server
        - Output example:

- ◆ ;;QUESTION SECTION:
- ◆ ;<server> IN NS
- ◆ ;; ANSWER SECTION:
- ◆ <server> 300 IN NS 10 dde.ns.cloudflare.com (MADE UP IP)
- ◆ ;; AUTHORITY SECTION:
- ◆ <server> 53058 IN NS dde.ns.cloudflare.com
- ◆ ;; ADDITIONAL SECTION:
- ◆ Dde.ns.cloudflare.com 65838 IN A 173.245.43.12 (MADE UP IP)

➢ Drawbacks:

- ■ This tool can be blocked or misled to a point by the servers in question.
- ■ This tool brings up very simple and general lookups

❖ Tool: **DirBuster.** Purpose: Enumerate and obtain information about files and directories of a server.

➢ Commands within application:

- ■ Place URL of the target in the Target URL input
- ■ Example: Target URL
  - ● http://192.168.1.11/wordpress/
- ■ Select Work Method
  - ● Use Get requests only: will be faster but less accurate
  - ● Auto Switch (HEAD and GET): will be slower and more thorough
- ■ Number of Threads
  - ● The resource allocation of the computer to the scan

        - Be careful to not set this too high as it may crash or dramatically slow down your computer or worse; the server being tested
            - Best practice would be to check the Go Faster box if you want the optimal/highest speed, but work with the client to make sure the server isn't pushed into failure during the scan.
    - Select List based brute force and use the tried and tested lists you have or use the provided lists that come with the tool/platform being used (i.e. Kali)
    - Select the options:
        - Brute Force Dirs
        - Brute Force Files
        - Be Recursive << VERY IMPORTANT TO BE ABLE TO SEE DIRECTORIES WITHIN DIRECTORIES.
        - Dir to start with: /wordpress/ << with the example sever given above
        - File Extension: php << change as needed
- The directories and files will be mapped out from the starting/root folder chosen.
- From here you'll be able to place these URLs in the browser and be able to see folders and files you normally wouldn't know existed.
    - However, some of these files and directories may need escalated privileges to view/access.
- Drawbacks:
    - Scans can disrupt or take down servers if the servers are not well configured or are running on low resources.

        - Even if you find files and folders you didn't know existed, they can be restricted and could require admin privileges to access them.

- Tool: **Bloodhound** Purpose: Enumerate and obtain information about an active directory.
    - Commands:
        - Bloodhound-python -u <username> -p <password> -ns <domain controller ip> -d <domain name> -c <collection request>
        - Example:
            - Bloodhound-python -u testUser -p red&7IPsec@21cU -192.168.1.34 -d conda.local -c All (get everything you can)
        - 4 json files should appear
            - Computers.json
            - Domain.json
            - Groups.json
            - Users.json
        - Take these 4 files and place them within the bloodhound UI
        - From here, you can map out the other groups and users that branch off of the domain in question (strictly relating to the user chosen).
    - Drawbacks:
        - This tool is not even remotely stealthy and will raise a lot of alerts.
        - Any changes or updates to the active directory will require bloodhound to be run again
        - The data received is limited to what the user chosen is attached to
            - Different users will show different information based on privileges and inclusion of groups

- Tool: **nbtstat** Purpose: Enumerate and obtain information about protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP.
    - Commands:
        - nbtstat -A 192.168.1.24
            - This will output the Name Type & Status of the machine and groups attached to it, along with the machine's MAC address
        - nbtstat -S 192.168.1.24
            - This will output the sessions table with the destination IP addresses
    - Drawbacks:
        - Very simple tool for NetBIOS enumeration
        - Limited information, but works as defined.

References

15 best network scanning tools (network and IP scanner) of 2022. Software Testing Help. (2022, May 4). Retrieved May 9, 2022, from https://www.softwaretestinghelp.com/network-scanning-tools/

YouTube. (2018, October 21). NetBIOS and SMB enumeration - nbtstat & smbclient. YouTube. Retrieved May 19, 2022, from https://www.youtube.com/watch?v=sXqT95eIAjo

YouTube. (2020, November 27). *Attacking active directory - bloodhound*. YouTube. Retrieved May 19, 2022, from https://www.youtube.com/watch?v=aJqjH3MsbLM

YouTube. (2018, August 2). *Web app penetration testing - #12 - DirBuster*. YouTube. Retrieved May 19, 2022, from https://www.youtube.com/watch?v=Hnz1d4WmD5Y

YouTube. (2019, March 19). *DNS enumeration tutorial - dig, NSLOOKUP & Host*. YouTube. Retrieved May 19, 2022, from https://www.youtube.com/watch?v=rQ-dc5kwRtU

DIG commands Cheatsheet. Never Ending Security. (2015, April 13). Retrieved May 19, 2022, from https://neverendingsecurity.wordpress.com/2015/04/13/dig-commands-cheatsheet/

YouTube. (2017, March 16). *Nmap tutorial for beginners - 1 - what is nmap?* YouTube. Retrieved May 19, 2022, from https://www.youtube.com/watch?v=5MTZdN9TEO4

House, N., & About Nathan HouseNathan House is the founder and CEO of Station X a cyber security training and consultancy company. He has over 25 years experience in cyber security where he has advised some of largest companies in the world. (2022, May 12).

Nmap cheat sheet. StationX. Retrieved May 19, 2022, from https://www.stationx.net/nmap-cheat-sheet/