Phase 2. Identify Targets and Run Scans

Goal: Identify the tools and techniques to be used to perform host discovery and enumeration.
Procedure: List out the tools you plan on using to perform network scans, the purpose for using them, and how you will use them.
Deliverable: Provide a minimum 2-page description of the tools you plan on using for the network scans, your reasoning for selecting them, and how they will be used. Be sure to include any challenges and potential drawbacks or limitations. Deliverable should cover at least 5 tools/resources.

1. Nmap

   Purpose: Obtain information on host, ports, and operating systems. I picked nmap because it allows you to scan a network and discover everything connected to it and also services and hosts.

   Commands:
   Nmap <ip address> - Scans an IP address
   Nmap -O <ip address> - Determines the OS
   nmap -sU <ip address> - Scans for UDP ports
   Nmap sT <ip address> - Scans for TCP ports

2. Wget

   Purpose: Wget is a computer tool created by the GNU Project. I use this tool so I can retrieve content and files from various web servers. The name is a combination of World Wide Web and the word get. It supports downloads via FTP, SFTP, HTTP, and HTTPS.

   Commands:
   wget 192.168.0.15 -q -S

3. Aircrack-ng

   Purpose: Aircrack-ng is a wireless security software suite. It consists of a network packet analyzer, a WEP network cracker, and WPA / WPA2-PSK along with another set of wireless auditing tools.

   Commands:
   -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
   -e <essid> : target selection: network identifier
   -b <bssid> : target selection: access point's MAC

-p <nbcpu> : # of CPU to use (default: all CPUs)
-q : enable quiet mode (no status output)

4. nslookup

Purpose: Nslookup is a command line tool included with most operating systems that allows a user to look up a network name server, as well as return IP addresses and domain names for a network server.

Commands:
Dig artemis.com mx - DIG performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.

Whois artemis.com - WHOIS is an Internet utility that shows the user additional information about a domain, the registrar of the domain, and the IP address.

5. DIRD

Purpose: DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary-based attack against a web server and analyzing the response.

Commands:
-a <agent_string> : Specify your custom USER_AGENT.
-c <cookie_string> : Set a cookie for the HTTP request.
-f : Fine tunning of NOT_FOUND (404) detection.
-H <header_string> : Add a custom header to the HTTP request.
-i : Use case-insensitive search.
-l : Print “Location” header when found.
-N <nf_code>: Ignore responses with this HTTP code.
-o <output_file> : Save output to disk.
-p <proxy[:port]> : Use this proxy. (Default port is 1080)
-P <proxy_username:proxy_password> : Proxy Authentication.
-r : Don’t search recursively.
-R : Interactive recursion. (Asks for each directory)
-S : Silent Mode. Don’t show tested words. (For dumb terminals)
-t : Don’t force an ending ‘/’ on URLs.
-u <username:password> : HTTP Authentication.