Nishant Baruah

A053

70022100516

Experiment 2 – NMAP and its various functionalities

What is NMAP?

Nmap (Network Mapper) is a free and open-source command-line tool essential for network discovery, enumeration, and security auditing within the Kali Linux operating system. It's renowned for its versatility, flexibility, and array of features that equip security professionals, network administrators, and ethical hackers with the necessary insights to:

- Identify active hosts: Determine the presence of devices on a network, revealing their IP addresses and availability.
- Enumerate services: Uncover the services running on identified devices, including the ports they're using and the corresponding protocols.
- Detect operating systems: Employ advanced techniques to infer the operating systems or devices hosting discovered services, aiding in vulnerability assessments.
- Perform vulnerability scans: While nmap itself shouldn't be used for unauthorized exploitation, understanding the services and operating systems involved can guide further vulnerability scanning with dedicated tools.

Key Usage Considerations:

- Always obtain explicit permission: It's paramount to have written or verbal authorization from the network owner or administrator before conducting any scans, as unauthorized scanning can be illegal and have severe consequences.
- Start with basic scans: Begin with non-aggressive scans like TCP SYN scans (e.g., nmap -sS target_ip) to avoid triggering intrusion detection systems or causing disruptions.
- Respect ethical boundaries: Utilize nmap solely for authorized security assessments and vulnerability management, never for malicious purposes.

Beyond Basic Usage:

While the information above covers nmap's core functionalities, its capabilities extend far beyond:

- Advanced scanning techniques: Stealth scans, service version detection, OS fingerprinting, and more provide intricate details about a network's composition and potential vulnerabilities.
- Scripting and automation: Automate repetitive tasks through nmap scripting, streamlining and scaling network assessments.
- Visualization and output customization: Tailor nmap's output to fit your needs, using graphical interfaces or customizing text formats for clear interpretation.

What are the functionalities of NMAP?

Nmap, short for Network Mapper, is a free and open-source network scanning tool known for its flexibility and vast feature set. Here's a breakdown of its key functionalities:

Host Discovery:

- Identify live hosts on a network using techniques like ping sweeps, TCP SYN scans, and UDP scans.
- Discover the number of hosts and their IP addresses.

Port Scanning:

- Identify open ports on discovered hosts, revealing the services running on them.
- Scan specific ports or port ranges.
- Employ various scan techniques like TCP SYN scans, TCP Connect scans, UDP scans, and more, each offering different advantages and stealth levels.

Service and Version Detection:

- Identify the services running on open ports by analyzing responses.
- Determine the version of running services, which can be crucial for vulnerability assessments.
- Support for a wide range of popular services and protocols.

Operating System (OS) Detection:

- Analyze packet responses and other characteristics to infer the operating system of a device.
- Provides valuable information for understanding the potential attack surface.

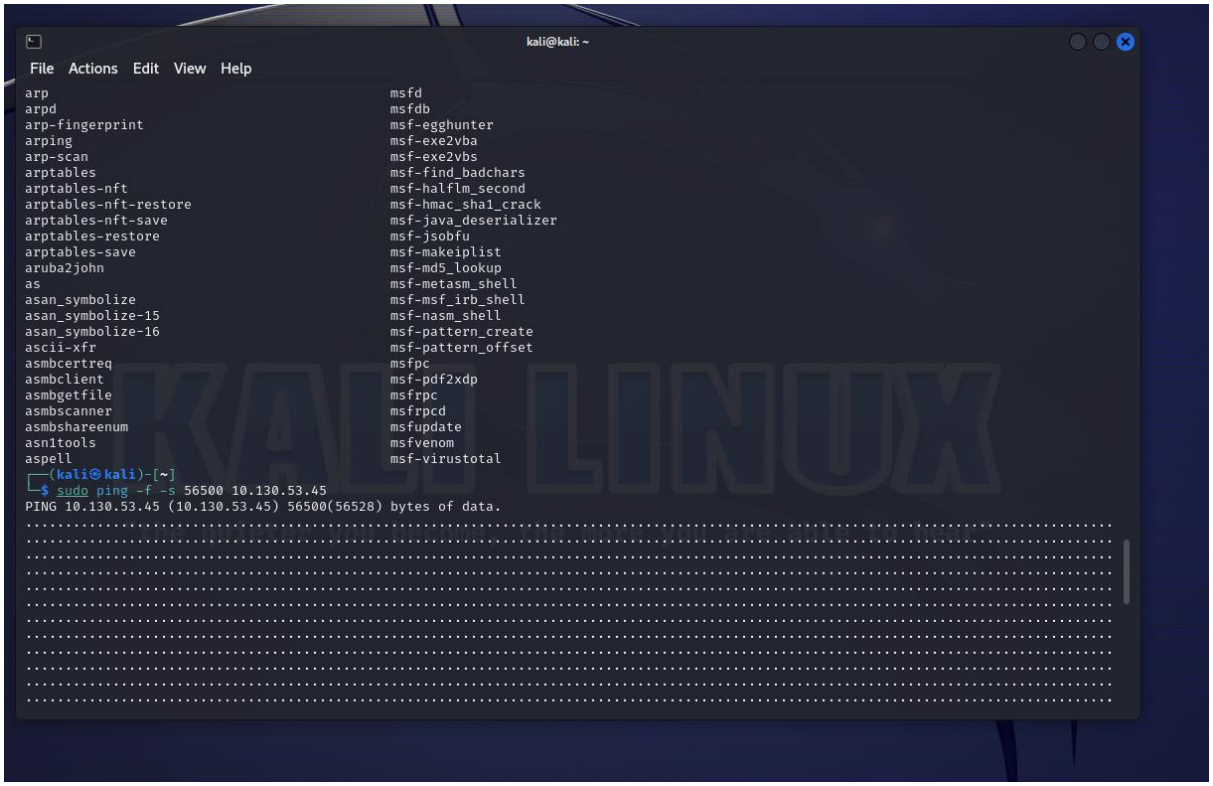
Script Scanning:

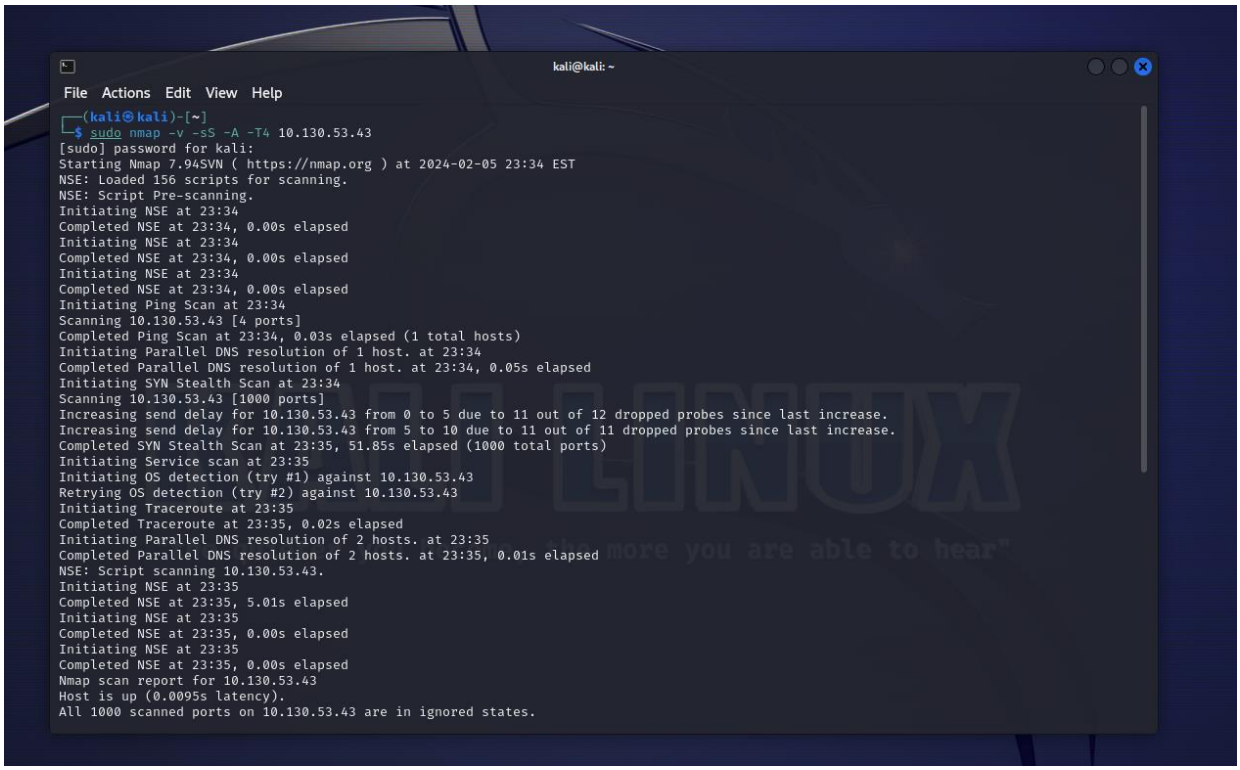
- Execute custom scripts to gather specific information or perform advanced tasks beyond basic scanning.
- Explore vulnerabilities, identify specific applications, and more.
- Requires scripting knowledge and careful usage to avoid unintended consequences.

Other Functionalities:

- Traceroute to map the path packets take to reach a host.
- DNS resolution to obtain hostnames for IP addresses.
- Output customization for various formats like text, XML, and graphical interfaces.
- Scheduling and automation of scans.

Some Basic Commands:


kali@kali: ~
File Actions Edit View Help
arp
arpd
arp-fingerprint
arping
arp-scan
arptables
arptables-nft
arptables-nft-restore
arptables-nft-save
arptables-restore
arptables-save
aruba2john
as
asan_symbolize
asan_symbolize-15
asan_symbolize-16
ascii-xfr
asmbcertreq
asmbclient
asmbgetfile
asmbscanner
asmbshareenum
asn1tools
aspell
msfd
msfdb
msf-egghunter
msf-exe2vba
msf-exe2vbs
msf-find_badchars
msf-halflm_second
msf-hmac_sha1_crack
msf-java_deserializer
msf-jsobfu
msf-makeiplist
msf-md5_lookup
msf-metasm_shell
msf-msf_irb_shell
msf-nasm_shell
msf-pattern_create
msf-pattern_offset
msfpc
msf-pdf2xdp
msfrpc
msfrpcd
msfupdate
msfvenom
msf-virustotal
┌──(kali㉿kali)-[~]
└─$ sudo ping -f -s 56500 10.130.53.45
PING 10.130.53.45 (10.130.53.45) 56500(56528) bytes of data.


kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -sS -A -T4 10.130.53.43
[sudo] password for kali:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-05 23:34 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:34
Completed NSE at 23:34, 0.00s elapsed
Initiating NSE at 23:34
Completed NSE at 23:34, 0.00s elapsed
Initiating NSE at 23:34
Completed NSE at 23:34, 0.00s elapsed
Initiating Ping Scan at 23:34
Scanning 10.130.53.43 [4 ports]
Completed Ping Scan at 23:34, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:34
Completed Parallel DNS resolution of 1 host. at 23:34, 0.05s elapsed
Initiating SYN Stealth Scan at 23:34
Scanning 10.130.53.43 [1000 ports]
Increasing send delay for 10.130.53.43 from 0 to 5 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.130.53.43 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Completed SYN Stealth Scan at 23:35, 51.85s elapsed (1000 total ports)
Initiating Service scan at 23:35
Initiating OS detection (try #1) against 10.130.53.43
Retrying OS detection (try #2) against 10.130.53.43
Initiating Traceroute at 23:35
Completed Traceroute at 23:35, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 23:35
Completed Parallel DNS resolution of 2 hosts. at 23:35, 0.01s elapsed
NSE: Script scanning 10.130.53.43.
Initiating NSE at 23:35
Completed NSE at 23:35, 5.01s elapsed
Initiating NSE at 23:35
Completed NSE at 23:35, 0.00s elapsed
Initiating NSE at 23:35
Completed NSE at 23:35, 0.00s elapsed
Nmap scan report for 10.130.53.43
Host is up (0.0095s latency).
All 1000 scanned ports on 10.130.53.43 are in ignored states.