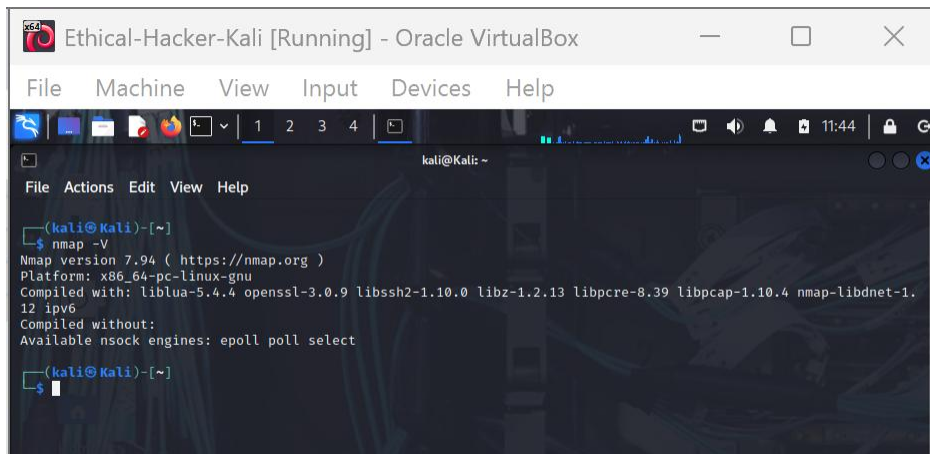


Ethical Hacker Lab: 3.2.6

Step 1: Log into Kali Linux and verify the environment.



Screenshot Description: Shows the command `nmap -V` being executed in Kali Linux, displaying the installed Nmap version.

Key Information Provided:

1. Version number (critical for exploit compatibility)
2. Compilation details (shows supported features)
3. Underlying libraries (openssl, libssh2, etc.)

Why This Matters for Ethical Hackers:

1. Exploit Reliability:

- Certain vulnerabilities (e.g., EternalBlue detection) require specific Nmap versions
- Scripts in NSE (Nmap Scripting Engine) may need minimum version requirements

2. Feature Verification:

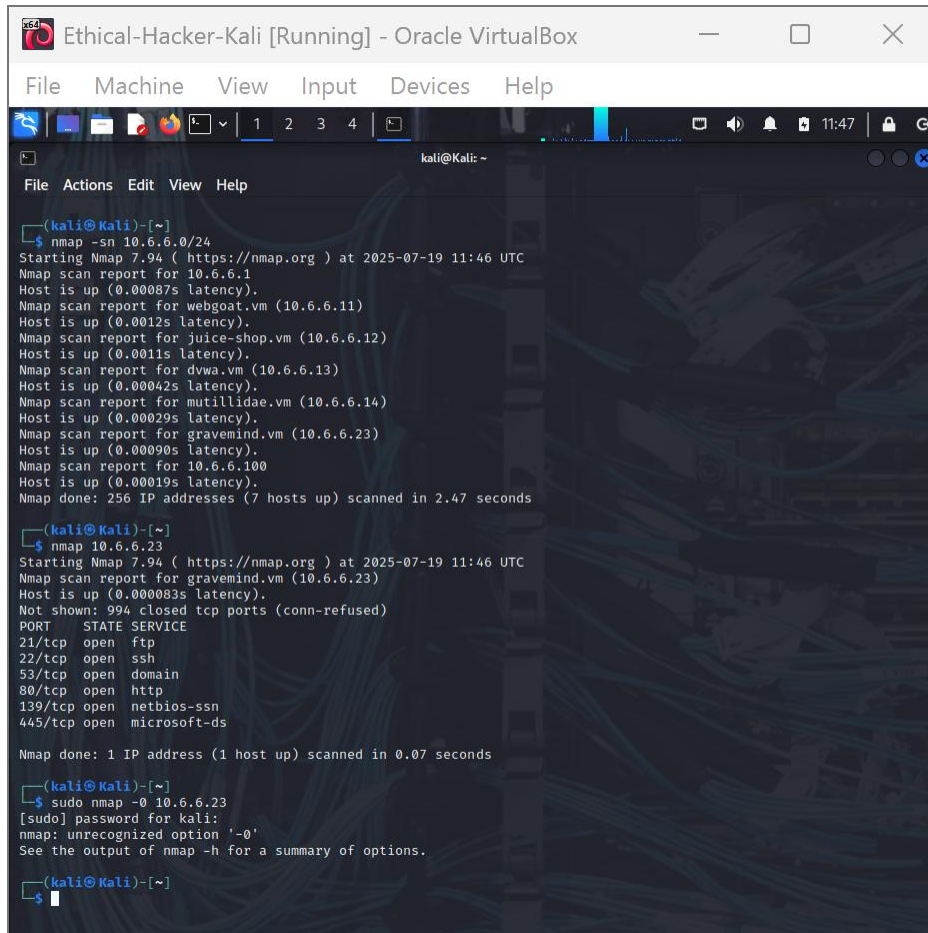
- Confirms if compiled with key capabilities like:
 - SSL scanning (openssl)
 - SSH brute-force support (libssh2)
 - Packet capture (libpcap - shown if missing in this example)

3. Reporting Requirements:

- Professional pentest reports must document tool versions

- Provides evidence of using updated tools for legal defensibility

Step 2: Initiate a basic Nmap scan of the target computer.



The screenshot shows a Kali Linux terminal window titled "Ethical-Hacker-Kali [Running] - Oracle VirtualBox". The terminal displays the output of an Nmap scan. The first command is `nmap -sn 10.6.6.0/24`, which scans the entire 10.6.6.0/24 network. The output lists several hosts that are up, including `10.6.6.1`, `10.6.6.11`, `10.6.6.12`, `10.6.6.13`, `10.6.6.14`, `10.6.6.23`, and `10.6.6.100`. The second command is `nmap 10.6.6.23`, which performs a detailed scan on the host 10.6.6.23. The output shows that the host is up and lists several open ports: 21/tcp (ftp), 22/tcp (ssh), 53/tcp (domain), 80/tcp (http), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds). The third command is `sudo nmap -0 10.6.6.23`, which results in an error: `nmmap: unrecognized option '-0'`.

```
(kali@kali)-[~]
$ nmap -sn 10.6.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-07-19 11:46 UTC
Nmap scan report for 10.6.6.1
Host is up (0.00087s latency).
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.0012s latency).
Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.0011s latency).
Nmap scan report for dvwa.vm (10.6.6.13)
Host is up (0.00042s latency).
Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.00029s latency).
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00090s latency).
Nmap scan report for 10.6.6.100
Host is up (0.00019s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.47 seconds

(kali@kali)-[~]
$ nmap 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-07-19 11:46 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00083s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

(kali@kali)-[~]
$ sudo nmap -0 10.6.6.23
[sudo] password for kali:
nmmap: unrecognized option '-0'
See the output of nmap -h for a summary of options.

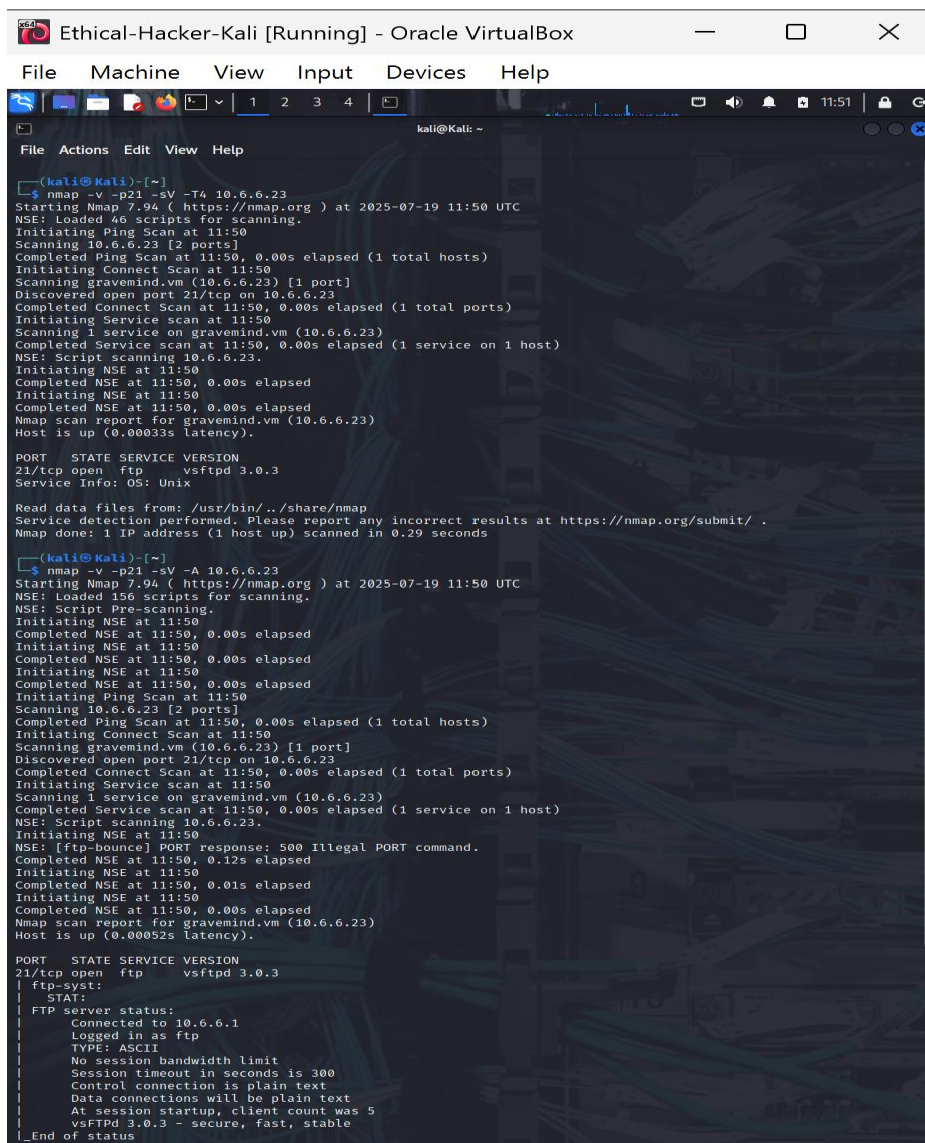
(kali@kali)-[~]
$
```

Screenshot Description: Demonstrates a basic nmap scan (e.g., `nmap 192.168.1.100`).

Explanation:

- **Command:** `nmap [target_IP]`
- **Output Includes:**
 - Open Ports: Lists accessible ports (e.g., 22/tcp SSH, 80/tcp HTTP).
 - Service Versions: Detects running services (e.g., Apache 2.4.29).
- **Use Case:**
 - Identifies live hosts and entry points for further exploitation.
 - Maps the attack surface of a target

Step 3: Obtain additional information about the host and services.



```
(kali@kali)~$ nmap -v -p21 -sV -T4 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-07-19 11:50 UTC
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 11:50
Scanning 10.6.6.23 [2 ports]
Completed Ping Scan at 11:50, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 11:50
Scanning gravemind.vm (10.6.6.23) [1 port]
Discovered open port 21/tcp on 10.6.6.23
Completed Connect Scan at 11:50, 0.00s elapsed (1 total ports)
Initiating Service scan at 11:50
Scanning 1 service on gravemind.vm (10.6.6.23)
Completed Service scan at 11:50, 0.00s elapsed (1 service on 1 host)
NSE: Script scanning 10.6.6.23.
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00033s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
Service Info: OS: Unix

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds

(kali@kali)~$ nmap -v -p21 -sV -A 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-07-19 11:50 UTC
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Initiating Ping Scan at 11:50
Scanning 10.6.6.23 [2 ports]
Completed Ping Scan at 11:50, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 11:50
Scanning gravemind.vm (10.6.6.23) [1 port]
Discovered open port 21/tcp on 10.6.6.23
Completed Connect Scan at 11:50, 0.00s elapsed (1 total ports)
Initiating Service scan at 11:50
Scanning 1 service on gravemind.vm (10.6.6.23)
Completed Service scan at 11:50, 0.00s elapsed (1 service on 1 host)
NSE: Script scanning 10.6.6.23.
Initiating NSE at 11:50
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 11:50, 0.12s elapsed
Initiating NSE at 11:50
Completed NSE at 11:50, 0.01s elapsed
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00052s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 10.6.6.1
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 5
|_vsFTPD 3.0.3 - secure, fast, stable
|_End of status
```

Screenshot Description: Shows two advanced Nmap scans targeting FTP services on 10.6.6.23:

1. `nmap -v -p21 -sV -T4 10.6.6.23`
2. `nmap -v -p21 -sV -A 10.6.6.23`

Commands Breakdown & Tactical Applications

1. Fast Version Detection Scan

Command: `nmap -v -p21 -sV -T4 10.6.6.23`

Flags Explained:

Flag	Purpose	Ethical Hacking Value
-v	Verbose output	Tracks scan progress in real-time
-p21	Targets FTP control port	Focuses on high-value service
-sV	Service version detection	Identifies vulnerable FTP implementations
-T4	Aggressive timing	Faster scans during time-sensitive engagements

When To Use:

- Initial vulnerability assessment
- Time-constrained engagements
- When you need quick verification of service versions

2. Comprehensive FTP Analysis

Command: nmap -v -p21 -sV -A 10.6.6.23

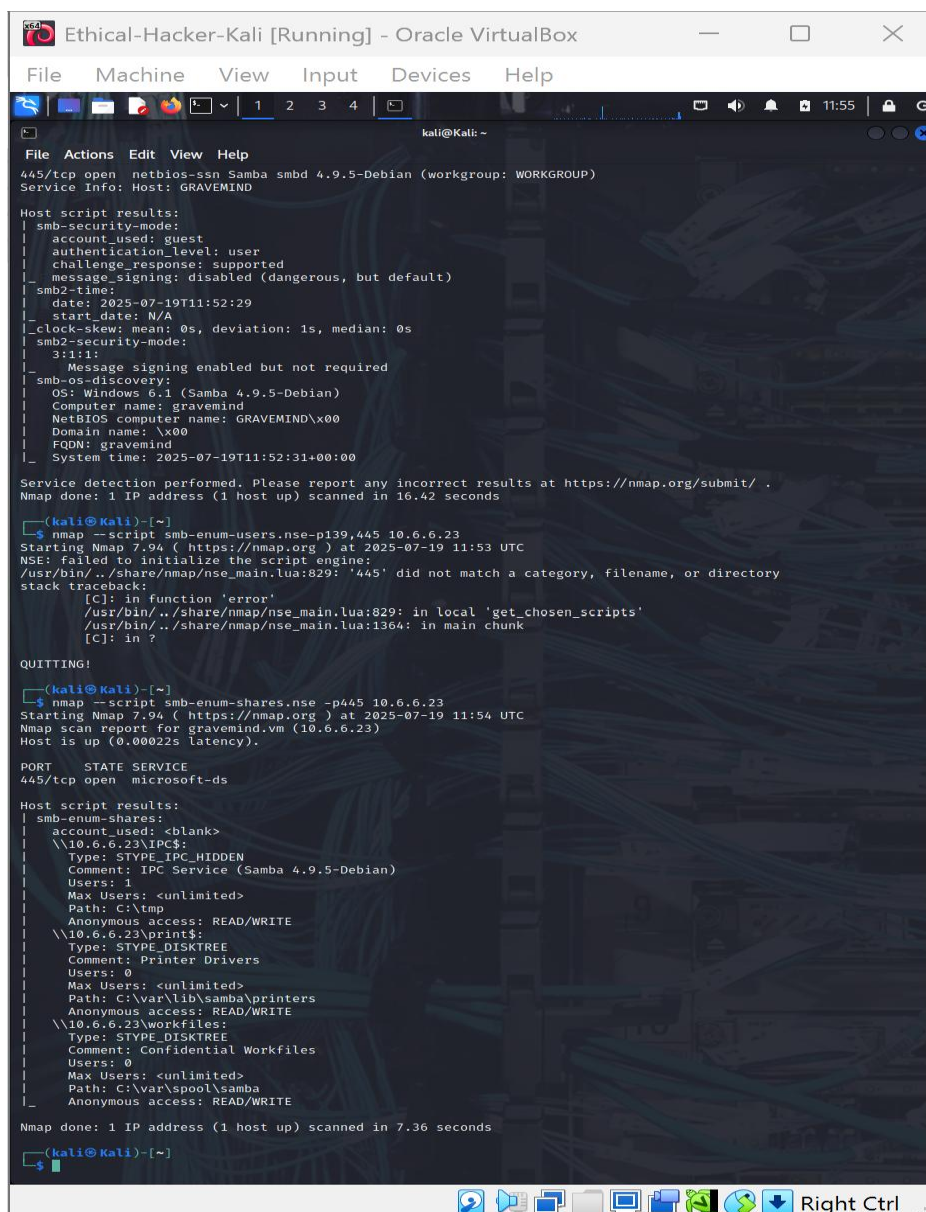
Enhanced Flags:

Flag	Additional Capabilities	Security Value
-A	Enables:	
	• OS detection (-O)	Identifies underlying system
	• Script scanning (-sC)	Runs default NSE scripts
	• Traceroute	Maps network path

When To Use:

- Full service enumeration
- Discovering misconfigurations (e.g., anonymous login)
- Comprehensive penetration tests

Step 4: Investigate SMB Services with Scripts



```
Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help

kali@Kali: ~
File Actions Edit View Help
445/tcp open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
Service Info: Host: GRAVEMIND

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_  smb2-time:
|     date: 2025-07-19T11:52:29
|     start_date: N/A
|_  clock-skew: mean: 0s, deviation: 1s, median: 0s
|_  smb2-security-mode:
|     3.1.1:
|       Message signing enabled but not required
|_  smb-os-discovery:
|     OS: Windows 6.1 (Samba 4.9.5-Debian)
|     Computer name: gravemind
|     NetBIOS computer name: GRAVEMIND\x00
|     Domain name: \x00
|     FQDN: gravemind
|_  System time: 2025-07-19T11:52:31+00:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.42 seconds

(kali@Kali)-[~]
$ nmap --script smb-enum-users.nse-p139,445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-07-19 11:53 UTC
NSE: failed to initialize the script engine:
/usr/bin/./share/nmap/nse_main.lua:829: '445' did not match a category, filename, or directory
stack traceback:
  [C]: in function 'error'
  /usr/bin/./share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
  /usr/bin/./share/nmap/nse_main.lua:1364: in main chunk
  [C]: in ?

QUITTING!

(kali@Kali)-[~]
$ nmap --script smb-enum-shares.nse -p445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-07-19 11:54 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00022s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\10.6.6.23\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba 4.9.5-Debian)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\10.6.6.23\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: READ/WRITE
|   \\10.6.6.23\workfiles:
|     Type: STYPE_DISKTREE
|     Comment: Confidential Workfiles
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\spool\samba
|_  Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 7.36 seconds

(kali@Kali)-[~]
```

Targeted SMB Service Investigation

Screenshot Description: Demonstrates two critical Nmap SMB enumeration scripts against target 10.6.6.23:

- 1. nmap --script smb-enum-users.nse -p139,445 10.6.6.23
- 2. nmap --script smb-enum-shares.nse -p445 10.6.6.23

Command Breakdown & Strategic Value

1. User Account Enumeration

Command: nmap --script smb-enum-users.nse -p139,445 10.6.6.23

Key Flags:

Component	Purpose	Attack Surface Value
smb-enum-users.nse	Enumerates domain/local users	Identifies potential usernames for brute-force
-p139,445	Targets NetBIOS and SMB ports	Covers both legacy and modern SMB

Tactical Applications:

- Builds username wordlists for password spraying
- Identifies service accounts (e.g., backup, www-data)
- Reveals default/common accounts (e.g., admin, guest)

2. Share Discovery

Command: nmap --script smb-enum-shares.nse -p445 10.6.6.23

Key Flags:

Component	Purpose	Attack Surface Value
smb-enum-shares.nse	Lists accessible shares	Finds data repositories

Component	Purpose	Attack Surface Value
-p445	Focuses on modern SMB	Avoids legacy NetBIOS noise