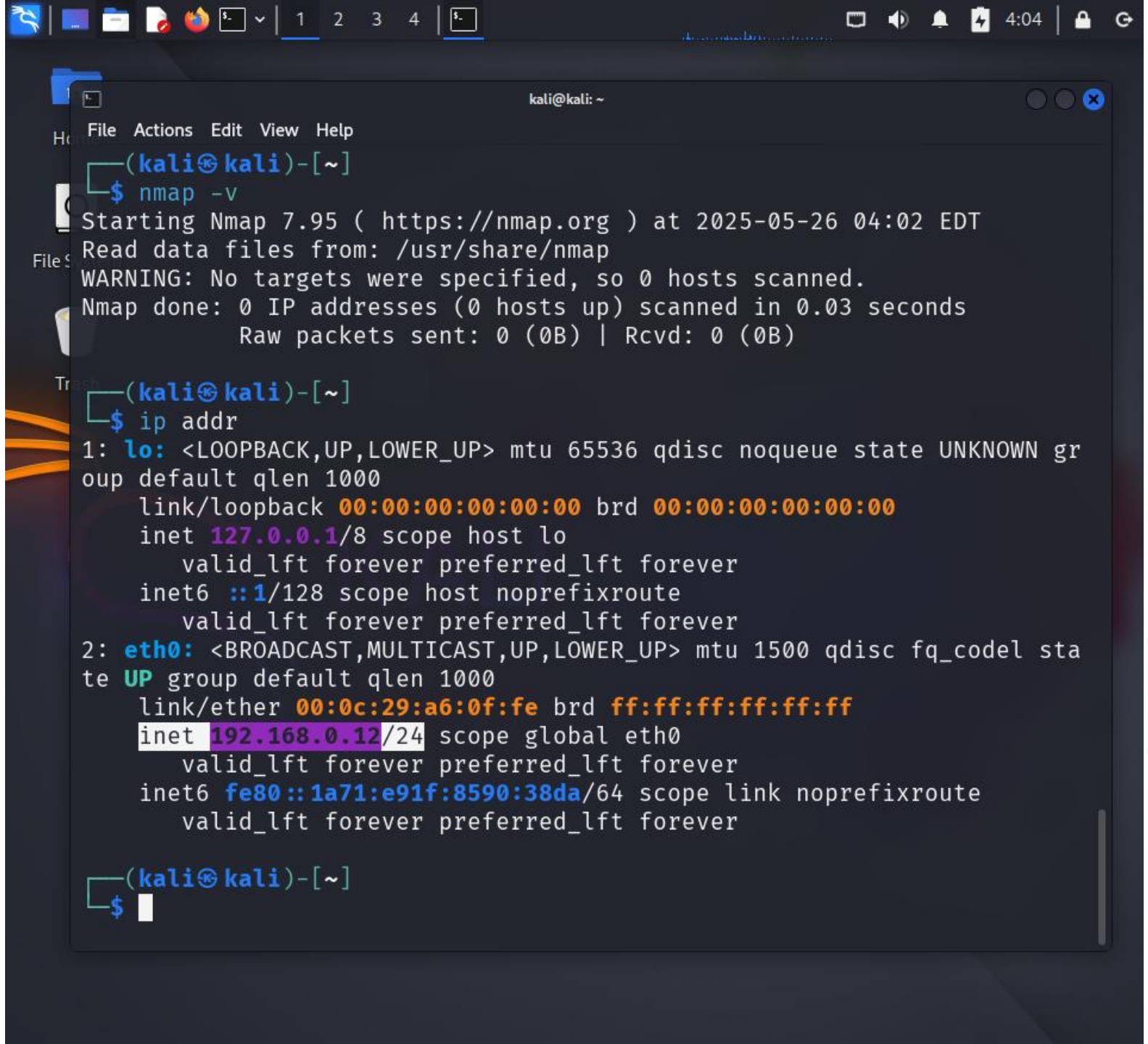
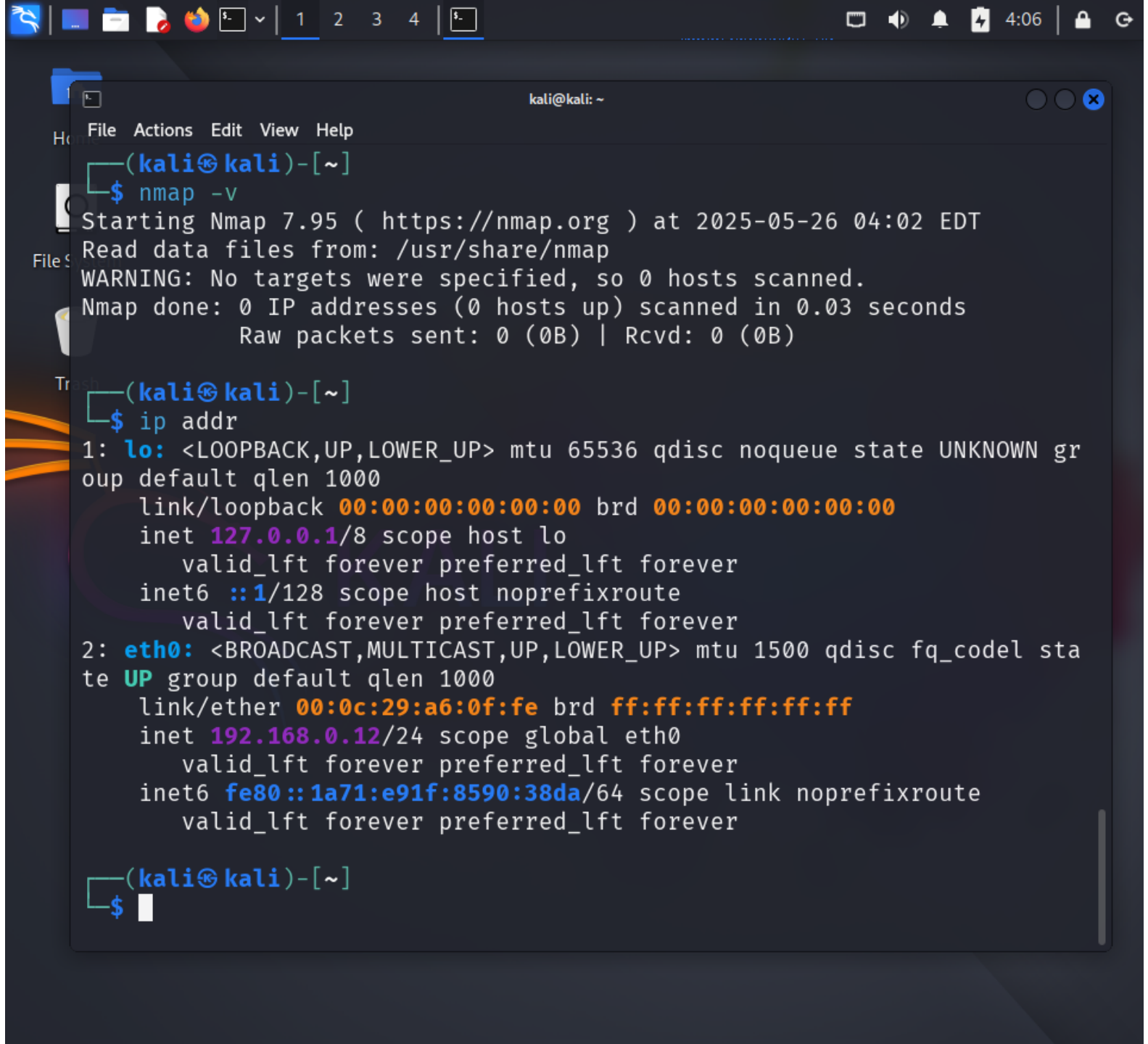
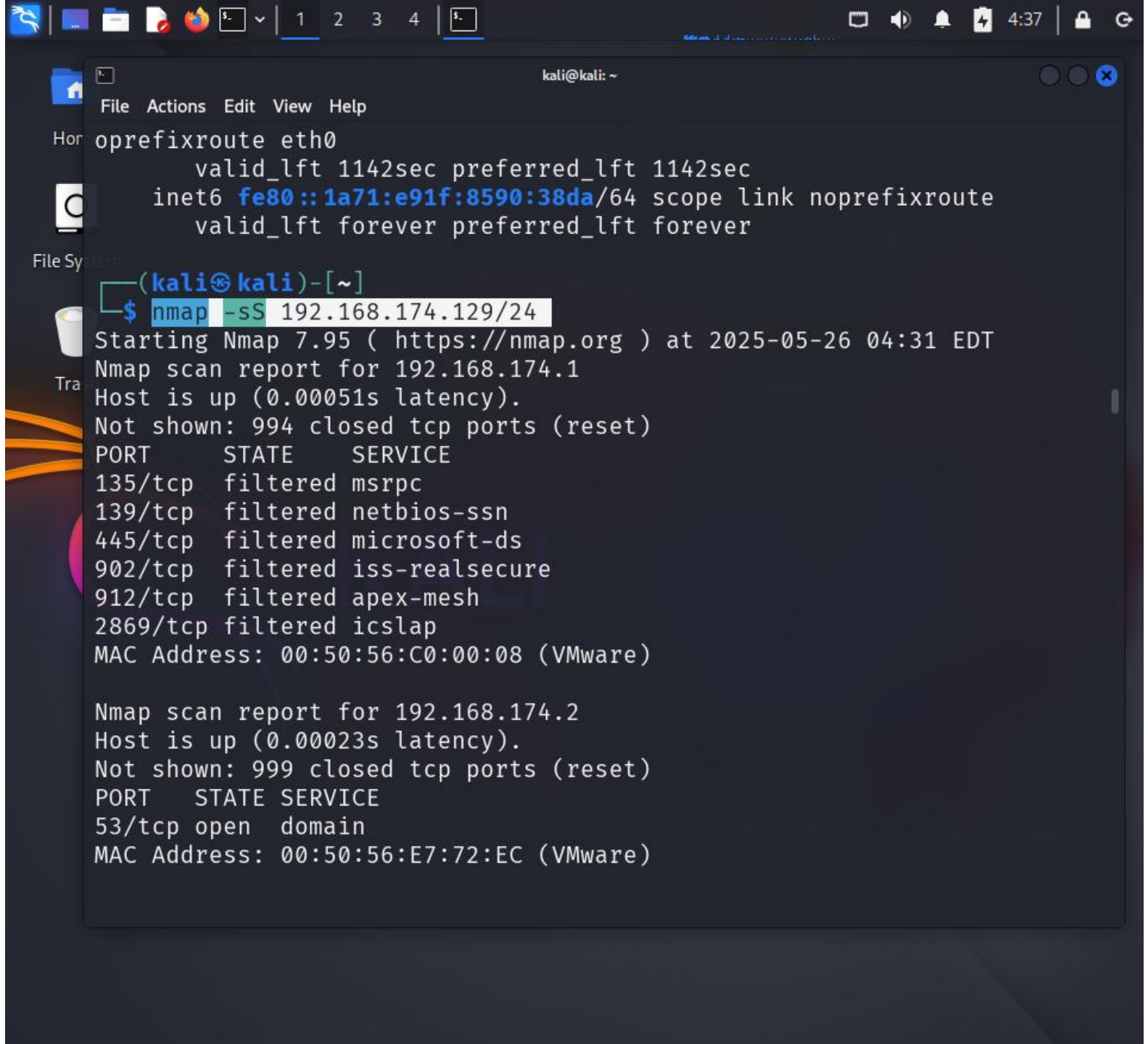
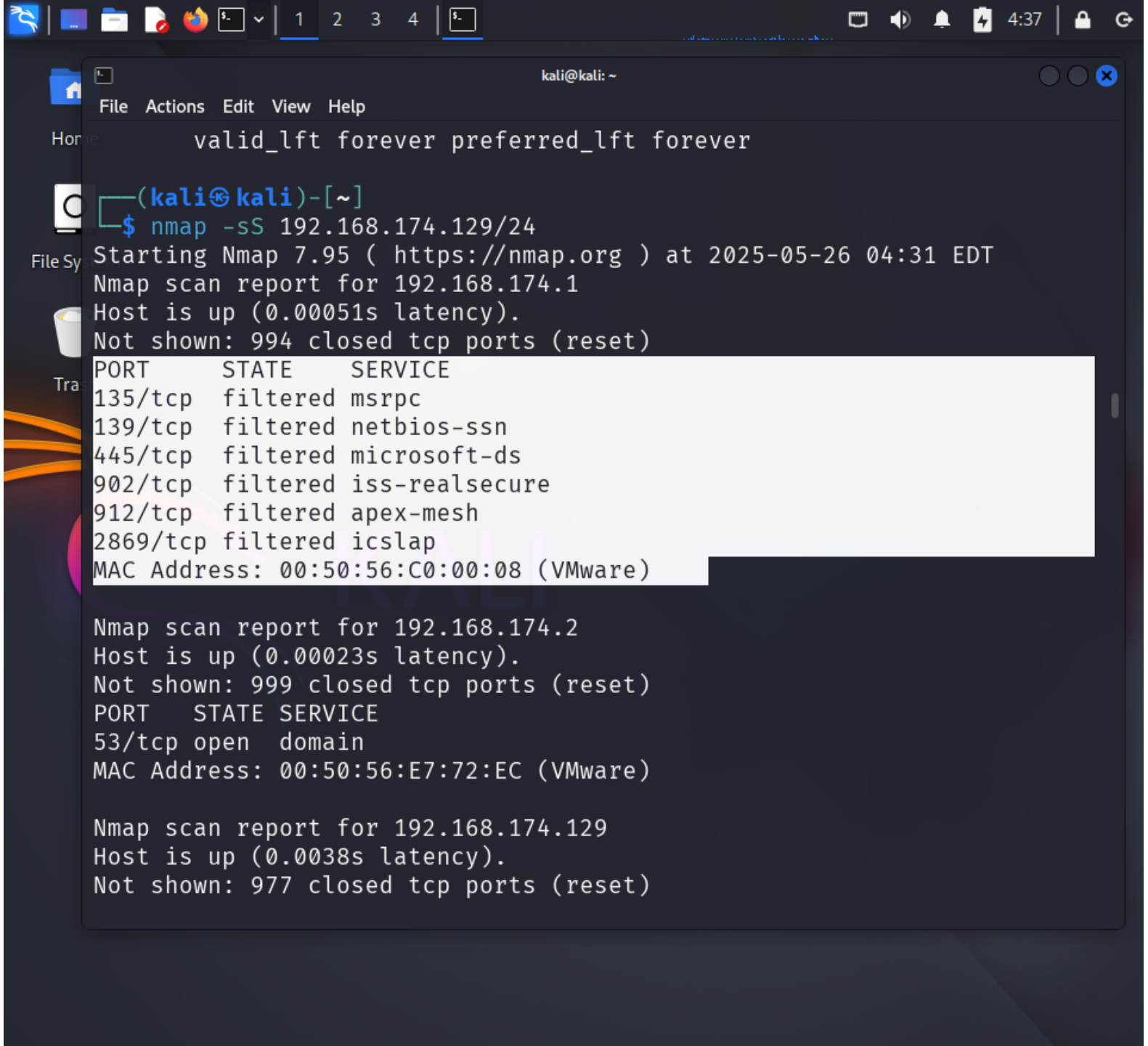
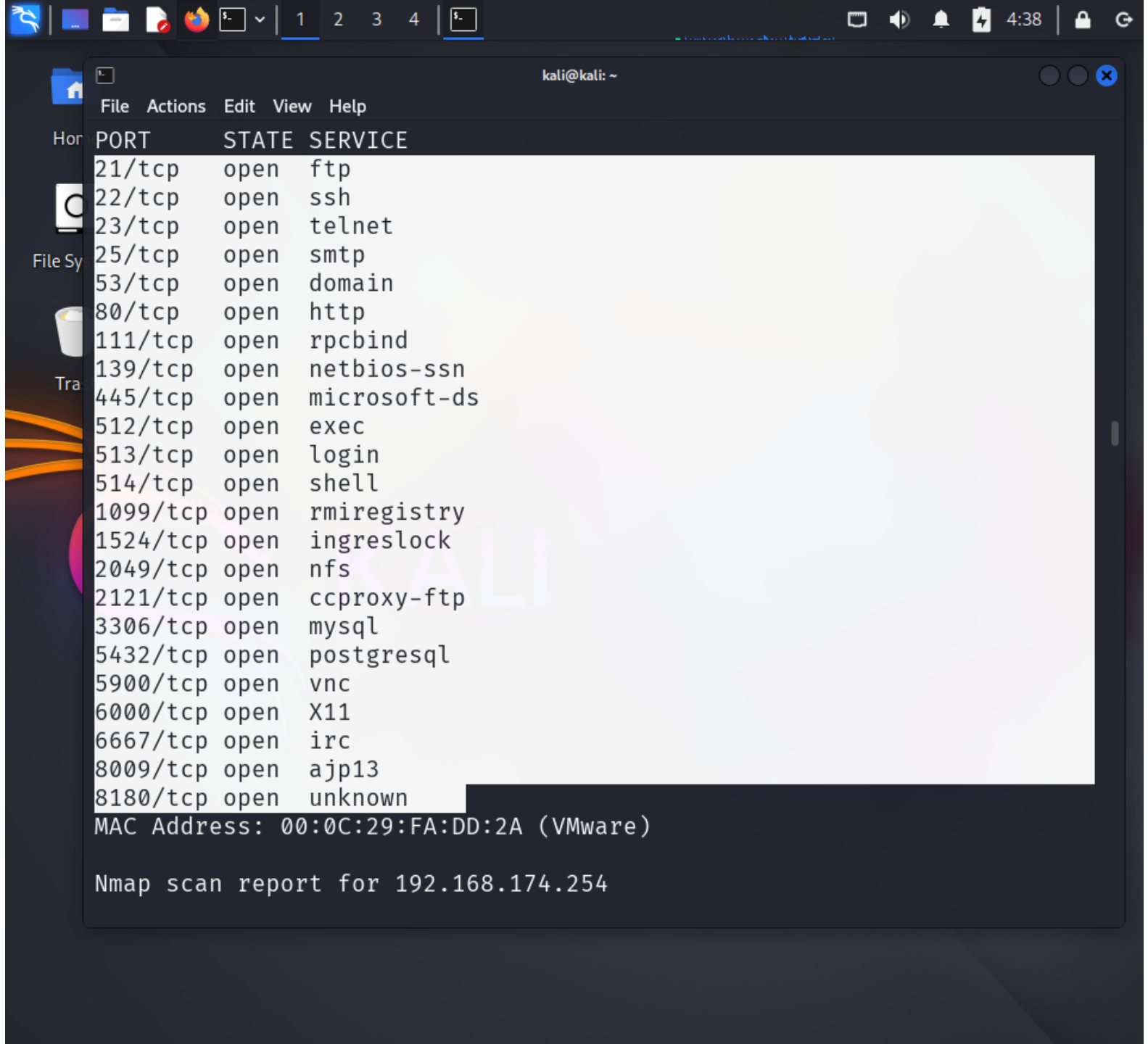
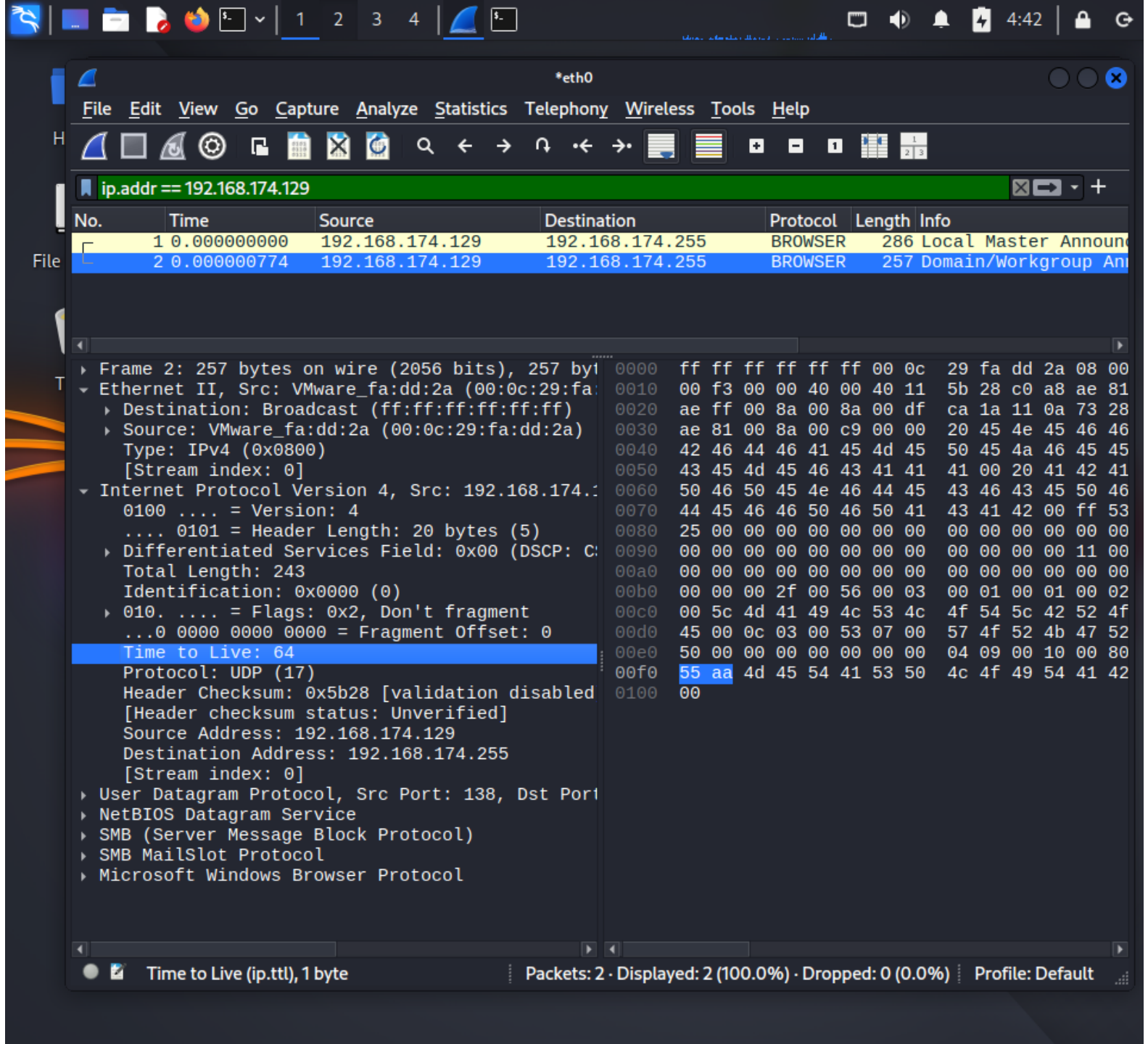

1 2 3 4
4:04
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -v
Starting Nmap 7.95 (https://nmap.org) at 2025-05-26 04:02 EDT
Read data files from: /usr/share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
(kali㉿kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 00:0c:29:a6:0f:fe brd ff:ff:ff:ff:ff:ff
inet 192.168.0.12/24 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::1a71:e91f:8590:38da/64 scope link noprefixroute
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$

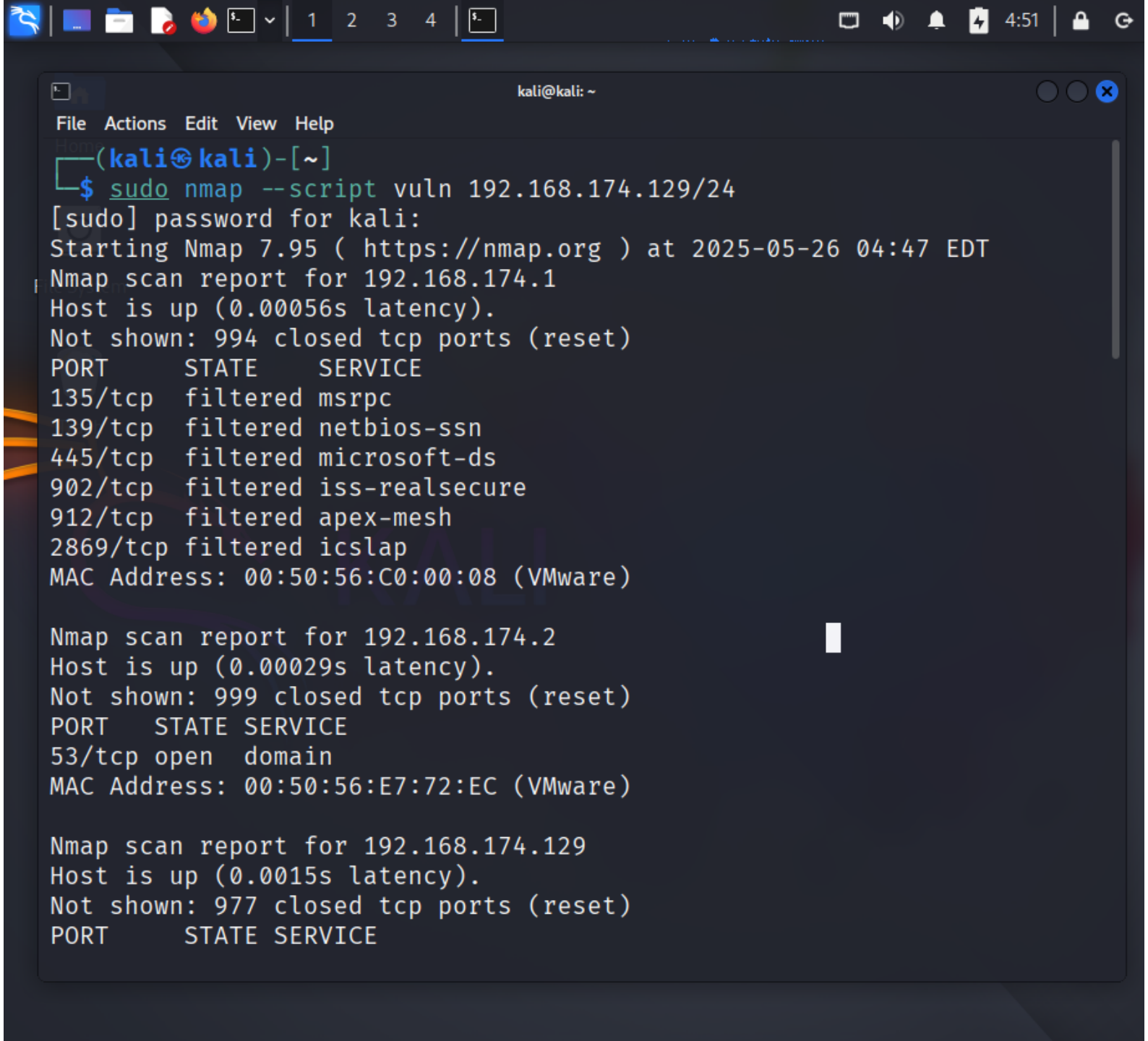

1 2 3 4
4:06
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -v
Starting Nmap 7.95 (https://nmap.org) at 2025-05-26 04:02 EDT
Read data files from: /usr/share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 00:0c:29:a6:0f:fe brd ff:ff:ff:ff:ff:ff
inet 192.168.0.12/24 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::1a71:e91f:8590:38da/64 scope link noprefixroute
valid_lft forever preferred_lft forever
┌──(kali㉿kali)-[~]
└─$

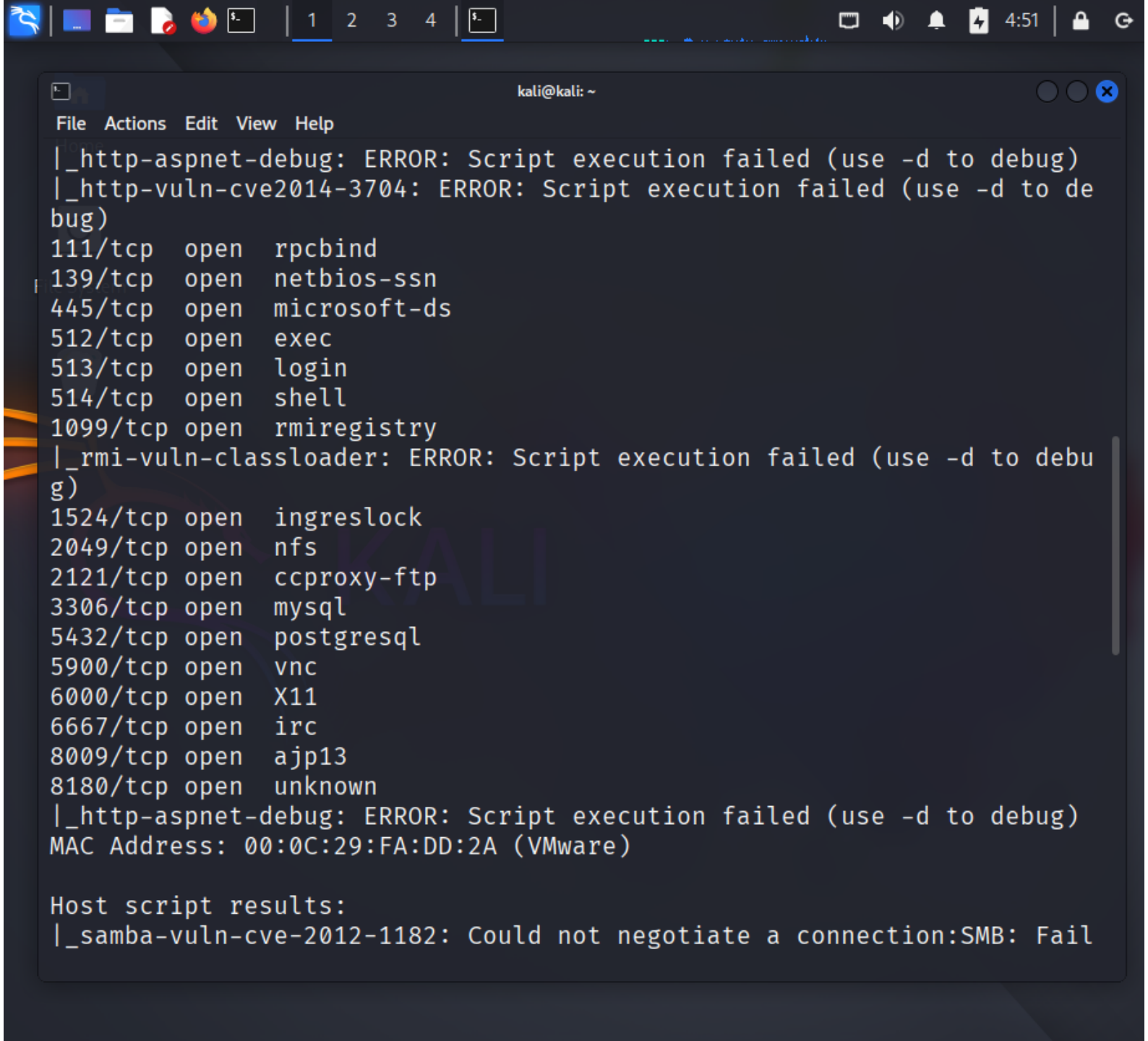

1 2 3 4
4:37
kali@kali: ~
File Actions Edit View Help
oprefixroute eth0
valid_lft 1142sec preferred_lft 1142sec
inet6 fe80::1a71:e91f:8590:38da/64 scope link noprefixroute
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$ nmap -sS 192.168.174.129/24
Starting Nmap 7.95 (https://nmap.org) at 2025-05-26 04:31 EDT
Nmap scan report for 192.168.174.1
Host is up (0.00051s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
902/tcp filtered iss-realsecure
912/tcp filtered apex-mesh
2869/tcp filtered icslap
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.174.2
Host is up (0.00023s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 00:50:56:E7:72:EC (VMware)

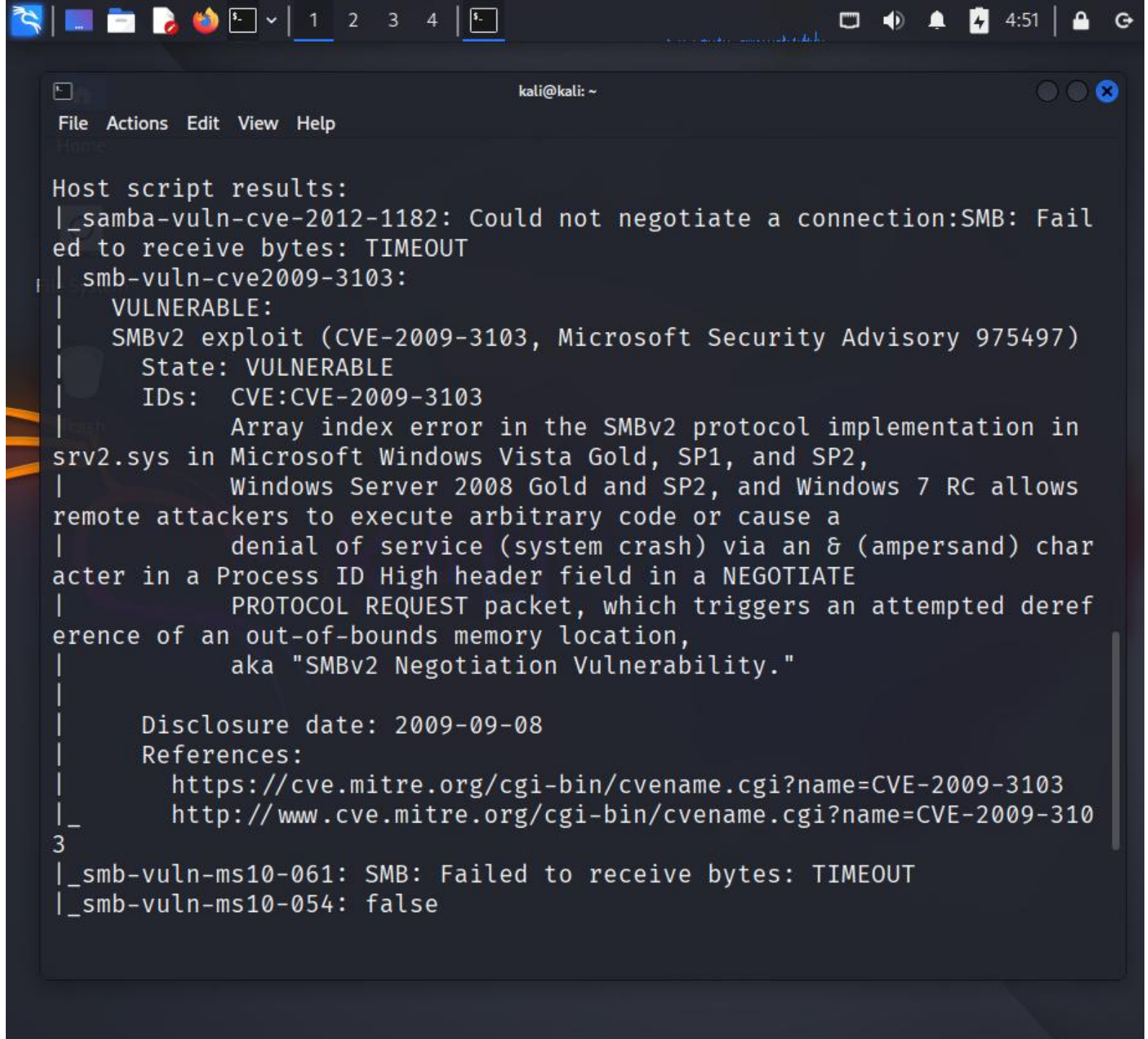

kali@kali: ~
File Actions Edit View Help
valid_lft forever preferred_lft forever
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.174.129/24
Starting Nmap 7.95 (https://nmap.org) at 2025-05-26 04:31 EDT
Nmap scan report for 192.168.174.1
Host is up (0.00051s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
902/tcp filtered iss-realsecure
912/tcp filtered apex-mesh
2869/tcp filtered icslap
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.174.2
Host is up (0.00023s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 00:50:56:E7:72:EC (VMware)
Nmap scan report for 192.168.174.129
Host is up (0.0038s latency).
Not shown: 977 closed tcp ports (reset)


1 2 3 4
4:38
kali@kali: ~
File Actions Edit View Help
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 192.168.174.254


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.174.129
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.174.129 192.168.174.255 BROWSER 286 Local Master Announ
2 0.000000774 192.168.174.129 192.168.174.255 BROWSER 257 Domain/Workgroup An
Frame 2: 257 bytes on wire (2056 bits), 257 by
Ethernet II, Src: VMware_fa:dd:2a (00:0c:29:fa
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: VMware_fa:dd:2a (00:0c:29:fa:dd:2a)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.174.
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: C
Total Length: 243
Identification: 0x0000 (0)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x5b28 [validation disabled
[Header checksum status: Unverified]
Source Address: 192.168.174.129
Destination Address: 192.168.174.255
[Stream index: 0]
User Datagram Protocol, Src Port: 138, Dst Port
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
0000 ff ff ff ff ff ff 00 0c 29 fa dd 2a 08 00
0010 00 f3 00 00 40 00 40 11 5b 28 c0 a8 ae 81
0020 ae ff 00 8a 00 8a 00 df ca 1a 11 0a 73 28
0030 ae 81 00 8a 00 c9 00 00 20 45 4e 45 46 46
0040 42 46 44 46 41 45 4d 45 50 45 4a 46 45 45
0050 43 45 4d 45 46 43 41 41 41 00 20 41 42 41
0060 50 46 50 45 4e 46 44 45 43 46 43 45 50 46
0070 44 45 46 46 50 46 50 41 43 41 42 00 ff 53
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 11 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 2f 00 56 00 03 00 01 00 01 00 02
00c0 00 5c 4d 41 49 4c 53 4c 4f 54 5c 42 52 4f
00d0 45 00 0c 03 00 53 07 00 57 4f 52 4b 47 52
00e0 50 00 00 00 00 00 00 00 04 09 00 10 00 80
00f0 55 aa 4d 45 54 41 53 50 4c 4f 49 54 41 42
0100 00
Time to Live (ip.ttl), 1 byte
Packets: 2 · Displayed: 2 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


1 2 3 4
4:51
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script vuln 192.168.174.129/24
[sudo] password for kali:
Starting Nmap 7.95 (https://nmap.org) at 2025-05-26 04:47 EDT
Nmap scan report for 192.168.174.1
Host is up (0.00056s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
902/tcp filtered iss-realsecure
912/tcp filtered apex-mesh
2869/tcp filtered icslap
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.174.2
Host is up (0.00029s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 00:50:56:E7:72:EC (VMware)
Nmap scan report for 192.168.174.129
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE


1 2 3 4
4:51
kali@kali: ~
File Actions Edit View Help
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to de
bug)
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
|_rmi-vuln-classloader: ERROR: Script execution failed (use -d to debu
g)
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Fail


1 2 3 4
4:51
kali@kali: ~
File Actions Edit View Help
Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Fail
ed to receive bytes: TIMEOUT
| smb-vuln-cve2009-3103:
| VULNERABLE:
| SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
| State: VULNERABLE
| IDs: CVE:CVE-2009-3103
| Array index error in the SMBv2 protocol implementation in
srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
| Windows Server 2008 Gold and SP2, and Windows 7 RC allows
remote attackers to execute arbitrary code or cause a
| denial of service (system crash) via an & (ampersand) char
acter in a Process ID High header field in a NEGOTIATE
| PROTOCOL REQUEST packet, which triggers an attempted deref
erence of an out-of-bounds memory location,
| aka "SMBv2 Negotiation Vulnerability."
|
| Disclosure date: 2009-09-08
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_ http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-310
3
|_smb-vuln-ms10-061: SMB: Failed to receive bytes: TIMEOUT
|_smb-vuln-ms10-054: false