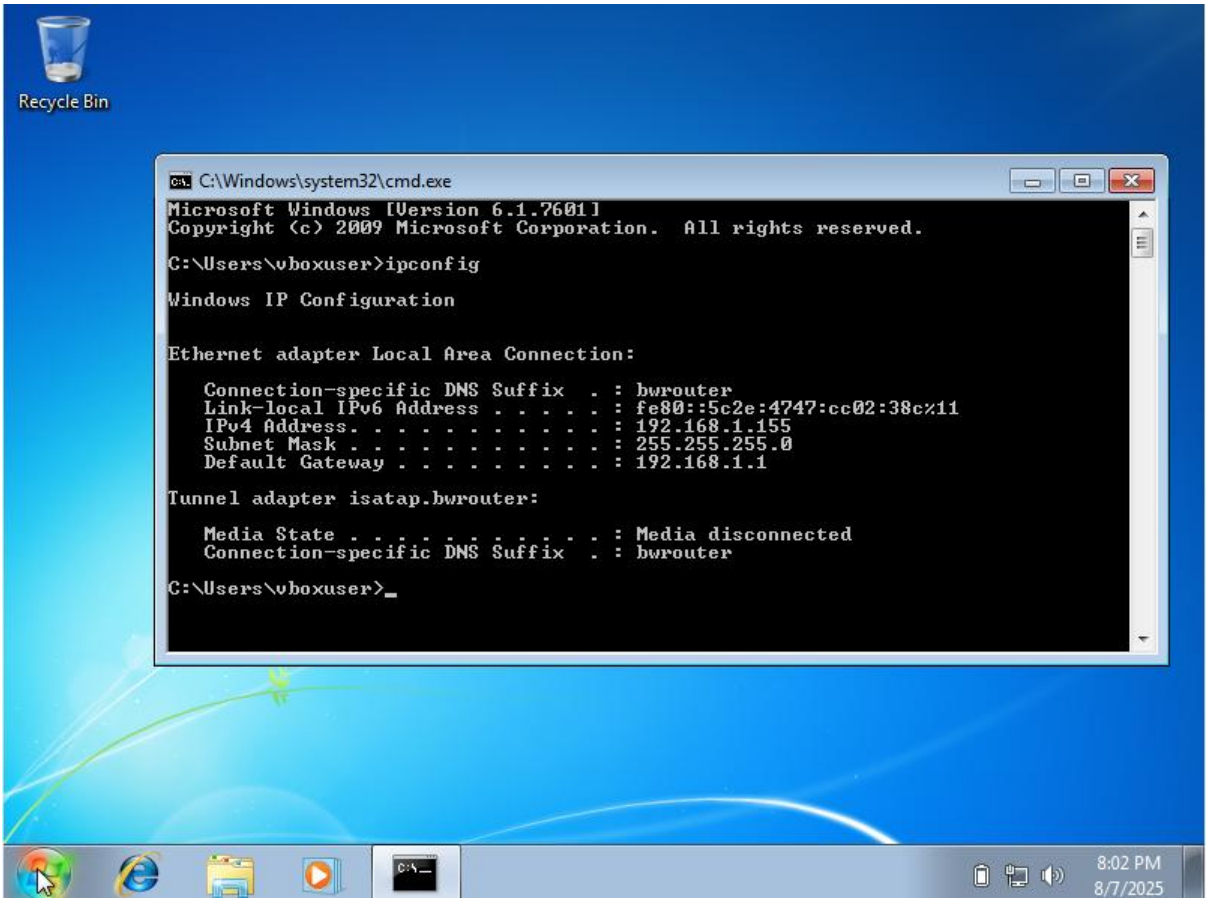
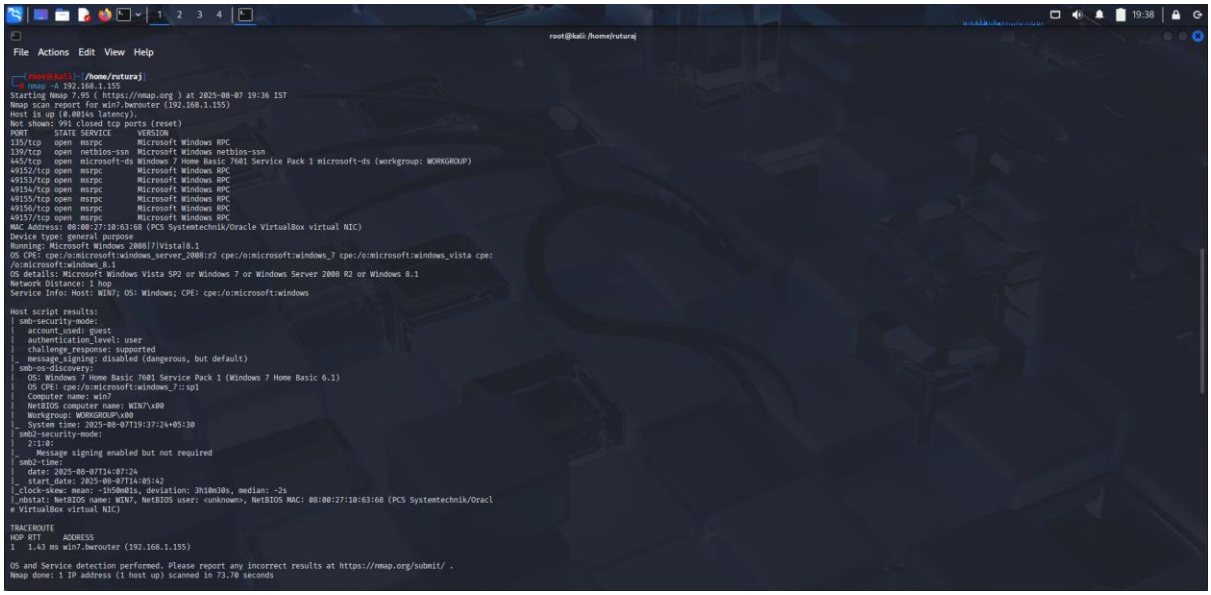
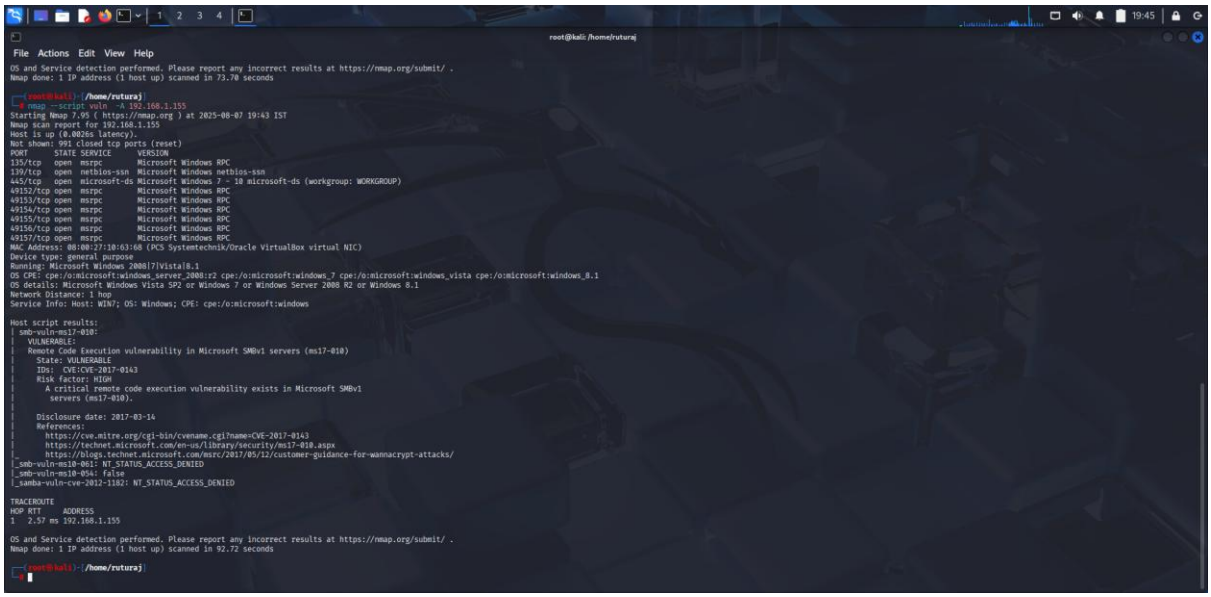
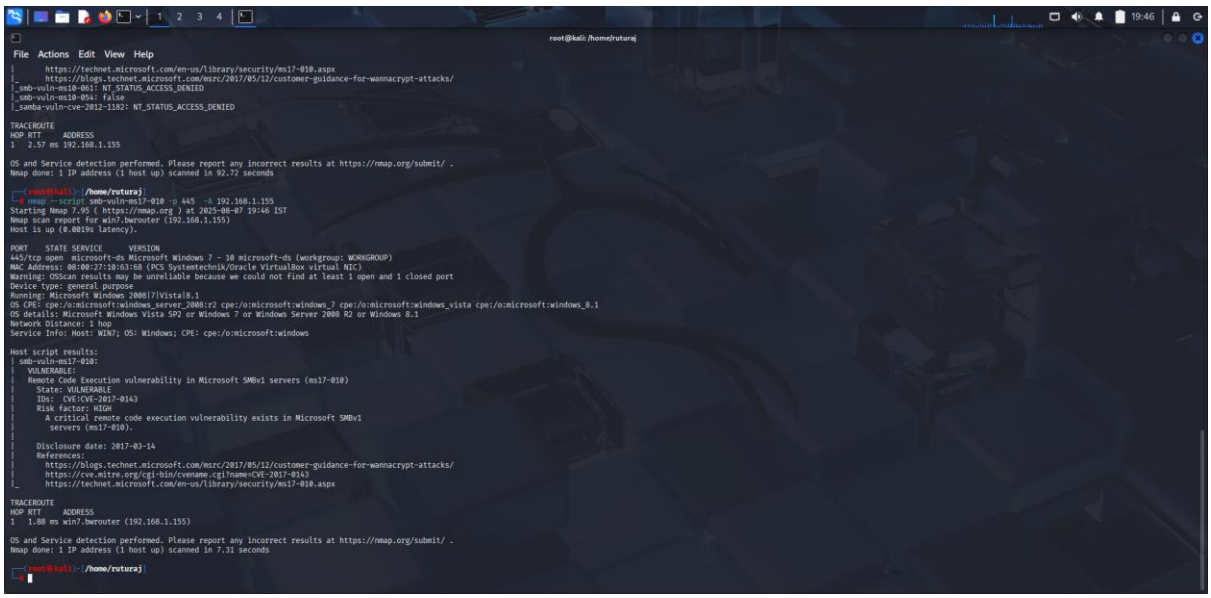
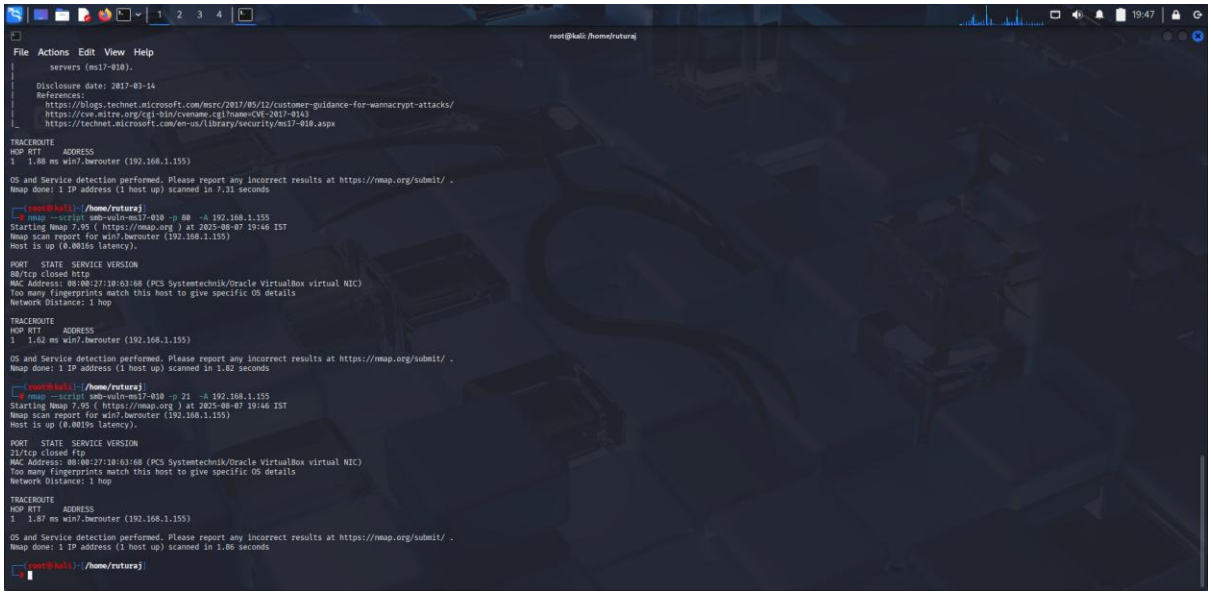
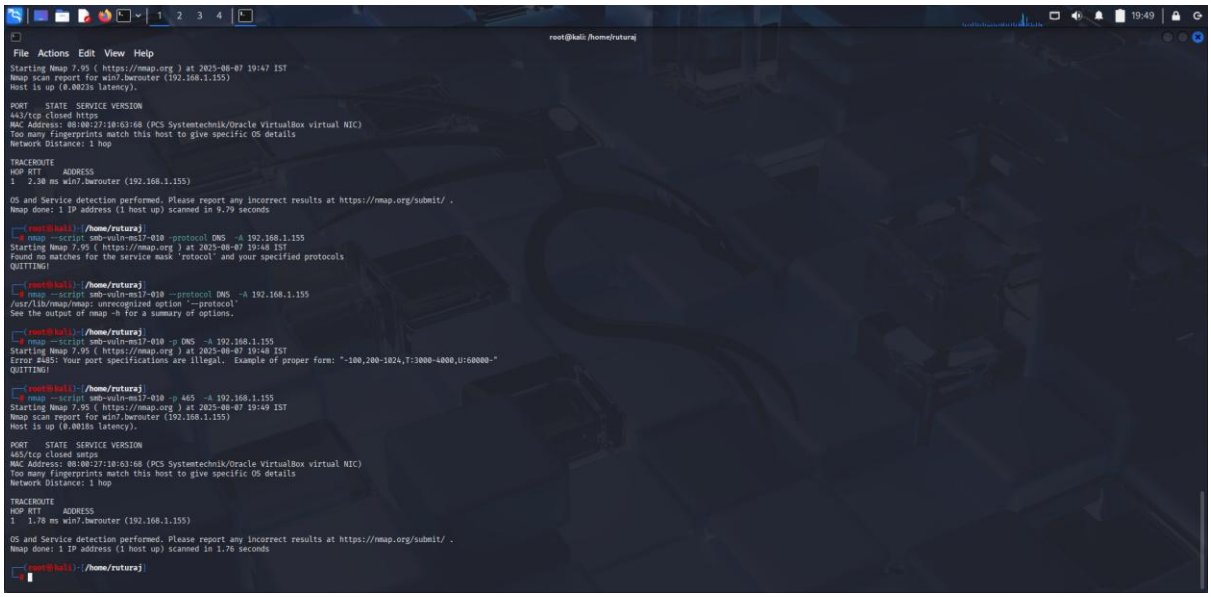

Recycle Bin
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\vboxuser>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : bwrouter
Link-local IPv6 Address . . . . . : fe80::5c2e:4747:cc02:38c%11
IPv4 Address. . . . . : 192.168.1.155
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Tunnel adapter isatap.bwrouter:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : bwrouter
C:\Users\vboxuser>_
8:02 PM
8/7/2025

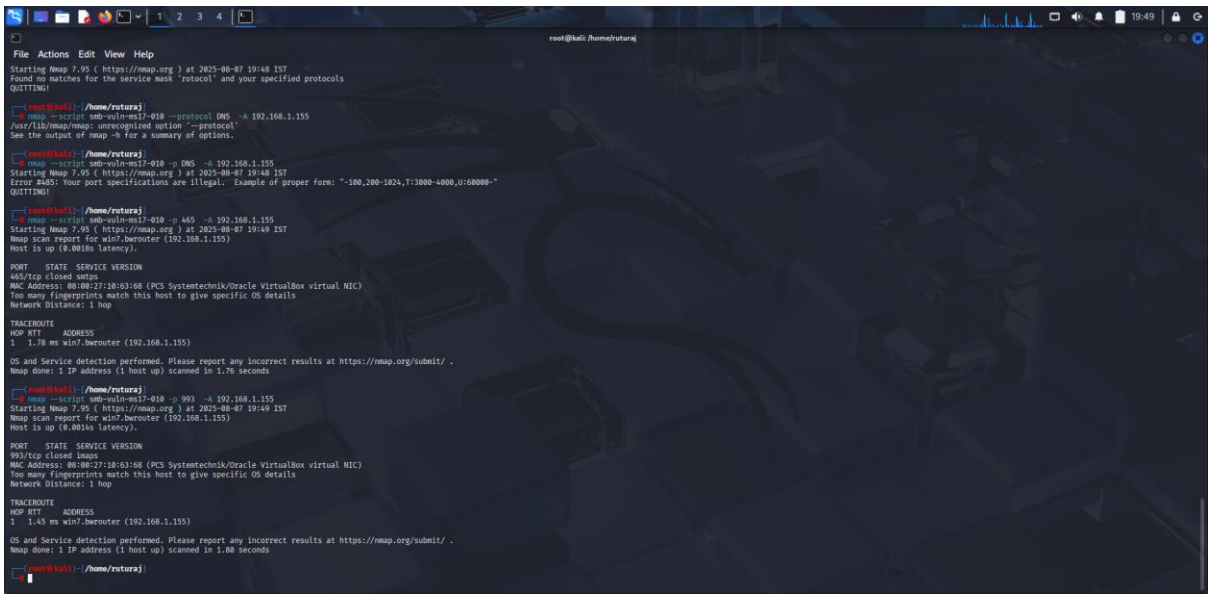

root@kali: /home/ruturaj
File Actions Edit View Help
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:36 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0014s latency).
Not shown: 991 closed tcp ports (reset)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc Microsoft Windows RPC
49157/tcp open msrpc Microsoft Windows RPC
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:
/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 1 hop
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
| OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
| OS CPE: cpe:/o:microsoft:windows_7::sp1
| Computer name: win7
| NetBIOS computer name: WIN7\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2025-08-07T19:37:24+05:30
| smb2-security-mode:
| 2:1:0:
|_ Message signing enabled but not required
| smb2-time:
| date: 2025-08-07T14:07:24
|_ start_date: 2025-08-07T14:05:42
|_clock-skew: mean: -1h50m01s, deviation: 3h10m30s, median: -2s
|_nbstat: NetBIOS name: WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:10:63:68 (PCS Systemtechnik/Oracl
e VirtualBox virtual NIC)
TRACEROUTE
HOP RTT ADDRESS
1 1.43 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.70 seconds

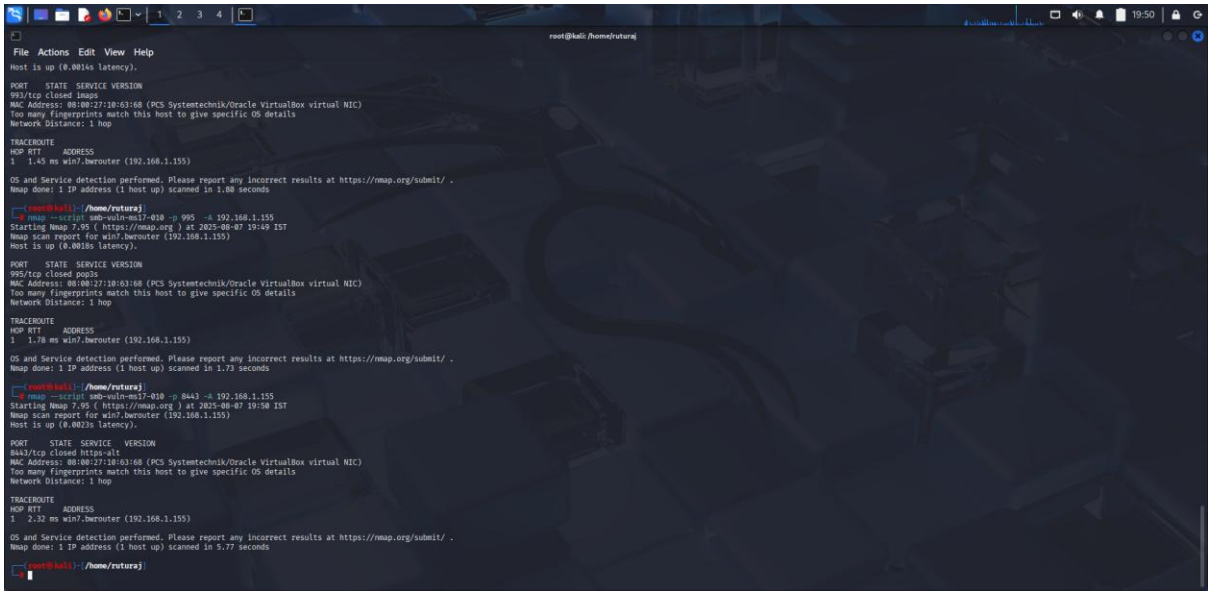

root@kali: /home/ruturaj
File Actions Edit View Help
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.70 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script vuln -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:43 IST
Nmap scan report for 192.168.1.155
Host is up (0.0026s latency).
Not shown: 991 closed tcp ports (reset)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc Microsoft Windows RPC
49157/tcp open msrpc Microsoft Windows RPC
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 1 hop
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
TRACEROUTE
HOP RTT ADDRESS
1 2.57 ms 192.168.1.155
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 92.72 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─#

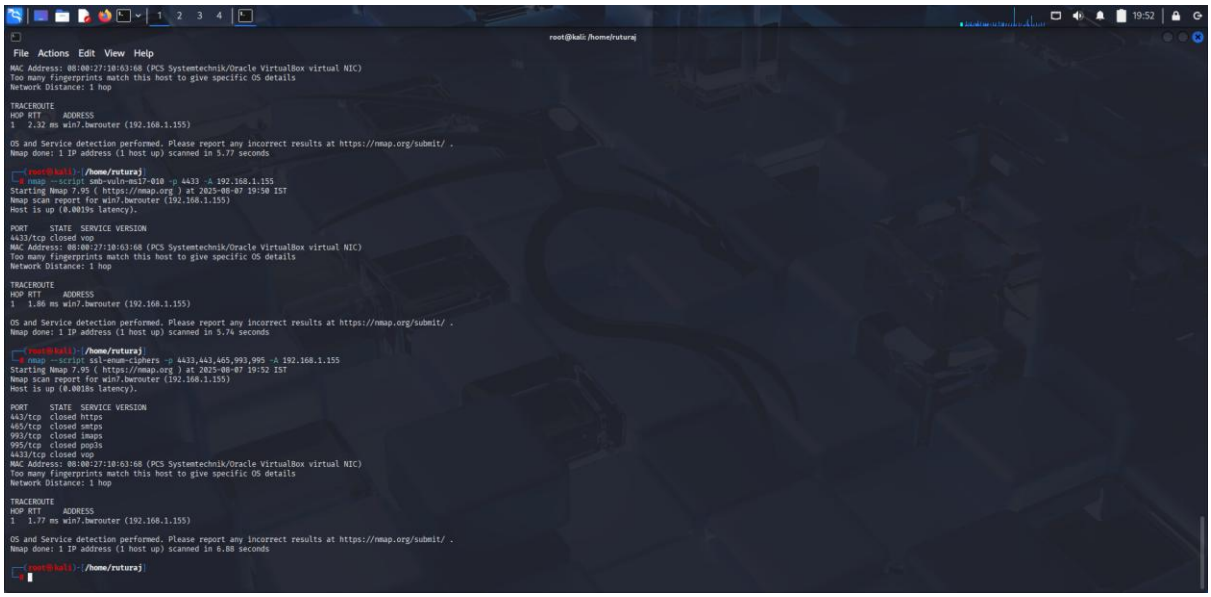

root@kali: /home/ruturaj
File Actions Edit View Help
| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
TRACEROUTE
HOP RTT ADDRESS
1 2.57 ms 192.168.1.155
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 92.72 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -p 445 -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:46 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0019s latency).
PORT STATE SERVICE VERSION
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 1 hop
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References:
| https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_ https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
TRACEROUTE
HOP RTT ADDRESS
1 1.88 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.31 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─#


root@kali: /home/ruturaj
File Actions Edit View Help
servers (ms17-010).
Disclosure date: 2017-03-14
References:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
TRACEROUTE
HOP RTT ADDRESS
1 1.88 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.31 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -p 80 -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:46 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0016s latency).
PORT STATE SERVICE VERSION
80/tcp closed http
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 1.62 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -p 21 -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:46 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0019s latency).
PORT STATE SERVICE VERSION
21/tcp closed ftp
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 1.87 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─#


root@kali: /home/ruturaj
File Actions Edit View Help
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:47 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0023s latency).
PORT STATE SERVICE VERSION
443/tcp closed https
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 2.38 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -protocol DNS -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:48 IST
Found no matches for the service mask 'rotocol' and your specified protocols
QUITTING!
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 --protocol DNS -A 192.168.1.155
/usr/lib/nmap/nmap: unrecognized option '--protocol'
See the output of nmap -h for a summary of options.
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -p DNS -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:48 IST
Error #485: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -p 465 -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:49 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0018s latency).
PORT STATE SERVICE VERSION
465/tcp closed smtps
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 1.78 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─#


root@kali: /home/ruturaj
File Actions Edit View Help
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:48 IST
Found no matches for the service mask 'rotocol' and your specified protocols
QUITTING!
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 --protocol DNS -A 192.168.1.155
/usr/lib/nmap/nmap: unrecognized option '--protocol'
See the output of nmap -h for a summary of options.
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -p DNS -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:48 IST
Error #485: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -p 465 -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:49 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0018s latency).
PORT STATE SERVICE VERSION
465/tcp closed smtps
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 1.78 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -p 993 -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:49 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0014s latency).
PORT STATE SERVICE VERSION
993/tcp closed imaps
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 1.45 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─#


root@kali: /home/ruturaj
File Actions Edit View Help
Host is up (0.0014s latency).
PORT STATE SERVICE VERSION
993/tcp closed imaps
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 1.45 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -p 995 -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:49 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0016s latency).
PORT STATE SERVICE VERSION
995/tcp closed pop3s
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 1.78 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -p 8443 -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:50 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0023s latency).
PORT STATE SERVICE VERSION
8443/tcp closed https-alt
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 2.32 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.77 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─#


root@kali: /home/ruturaj
File Actions Edit View Help
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 2.32 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.77 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script smb-vuln-ms17-010 -p 4433 -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:50 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0019s latency).
PORT STATE SERVICE VERSION
4433/tcp closed vop
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 1.86 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.74 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─# nmap --script ssl-enum-ciphers -p 4433,443,465,993,995 -A 192.168.1.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 19:52 IST
Nmap scan report for win7.bwrouter (192.168.1.155)
Host is up (0.0018s latency).
PORT STATE SERVICE VERSION
443/tcp closed https
465/tcp closed smtps
993/tcp closed imaps
995/tcp closed pop3s
4433/tcp closed vop
MAC Address: 08:00:27:10:63:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 1.77 ms win7.bwrouter (192.168.1.155)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds
┌──(root㉿kali)-[/home/ruturaj]
└─#