CS581 (Computer & Network Security)

Lab-01

Date: 10/12/2015

Group No.: 05
Group Members:
01. Rajnish Kumar (CIN: 304470392)
02. Jay Purohit (CIN: 304455065)
03. Rupal Jaiswal (CIN: 304442169)
04. Gaurav Prajapati (CIN: 304470132)

Port Scanning

Install nmap (or nmapfe) (http://nmap.org) port scanner onto your laptop or home computer and perform a TCP port scan and a UDP port scan of another computer. Submit reports generated by nmap (or Zenmap) containing list of open TCP & UDP ports. Also submit output of "netstat –na" command on computer that was scanned. Be sure to temporarily turn off any host-based firewall software if needed so that outputs of nmap and "netstat –na" indicate the same number of open ports.

We, Group No. 5, going to perform this lab in below steps:

Step 1: Base Machine IP Configuration

Step 2: Virtual Machine Setting Change

Step 3: Virtual Machine IP Configuration

Step 4: Downloading & Installing nmap software on Virtual Machine

Step 5: TCP Port Scanning

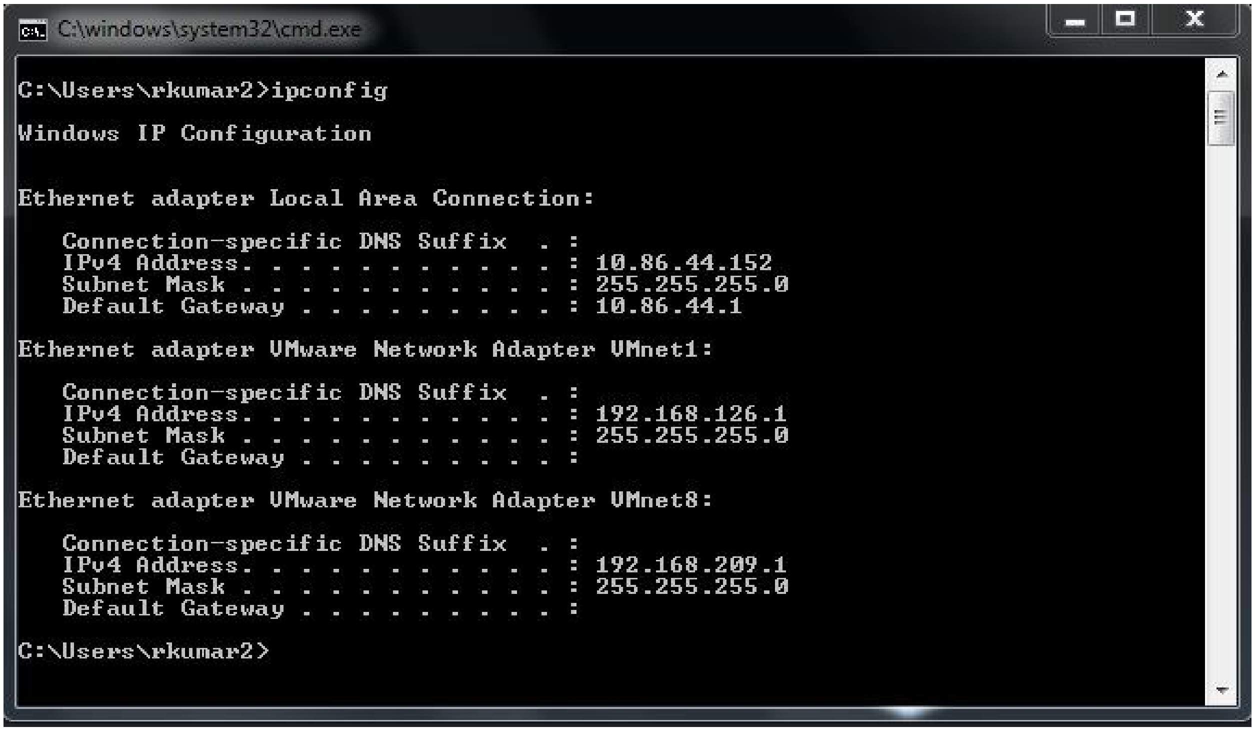
Step 6: UDP Port Scanning

Step 7: Temporarily Turned off Firewall on Virtual Machine

Step 8: Submitting output of "netstat -na" for TCP Port

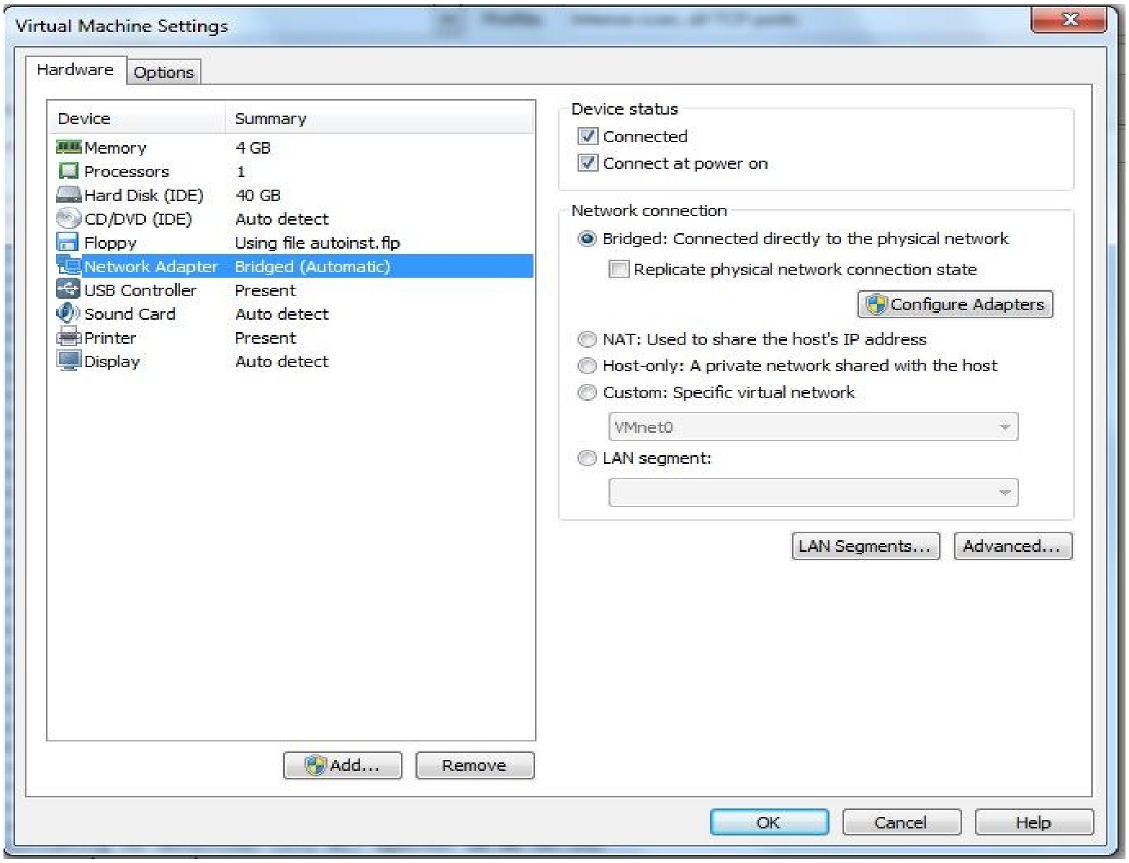
Step 9: Submitting output of "netstat -na" for UDP Port

Step 1: Base Machine IP Configuration



```
C:\Users\rkumar2>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.86.44.152
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.86.44.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.126.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.209.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\rkumar2>
```

Step 2: Virtual Machine Setting Change



Device	Summary
Memory	4 GB
Processors	1
Hard Disk (IDE)	40 GB
CD/DVD (IDE)	Auto detect
Floppy	Using file autoinst.flp
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

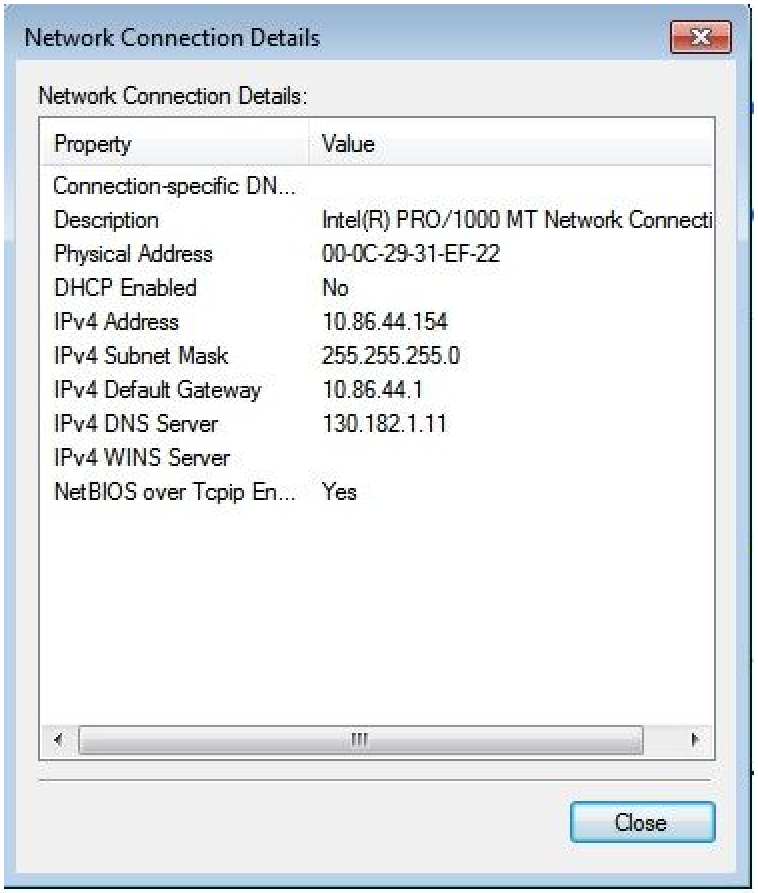
○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0

○ LAN segment:

Step 3: Virtual Machine IP Configuration



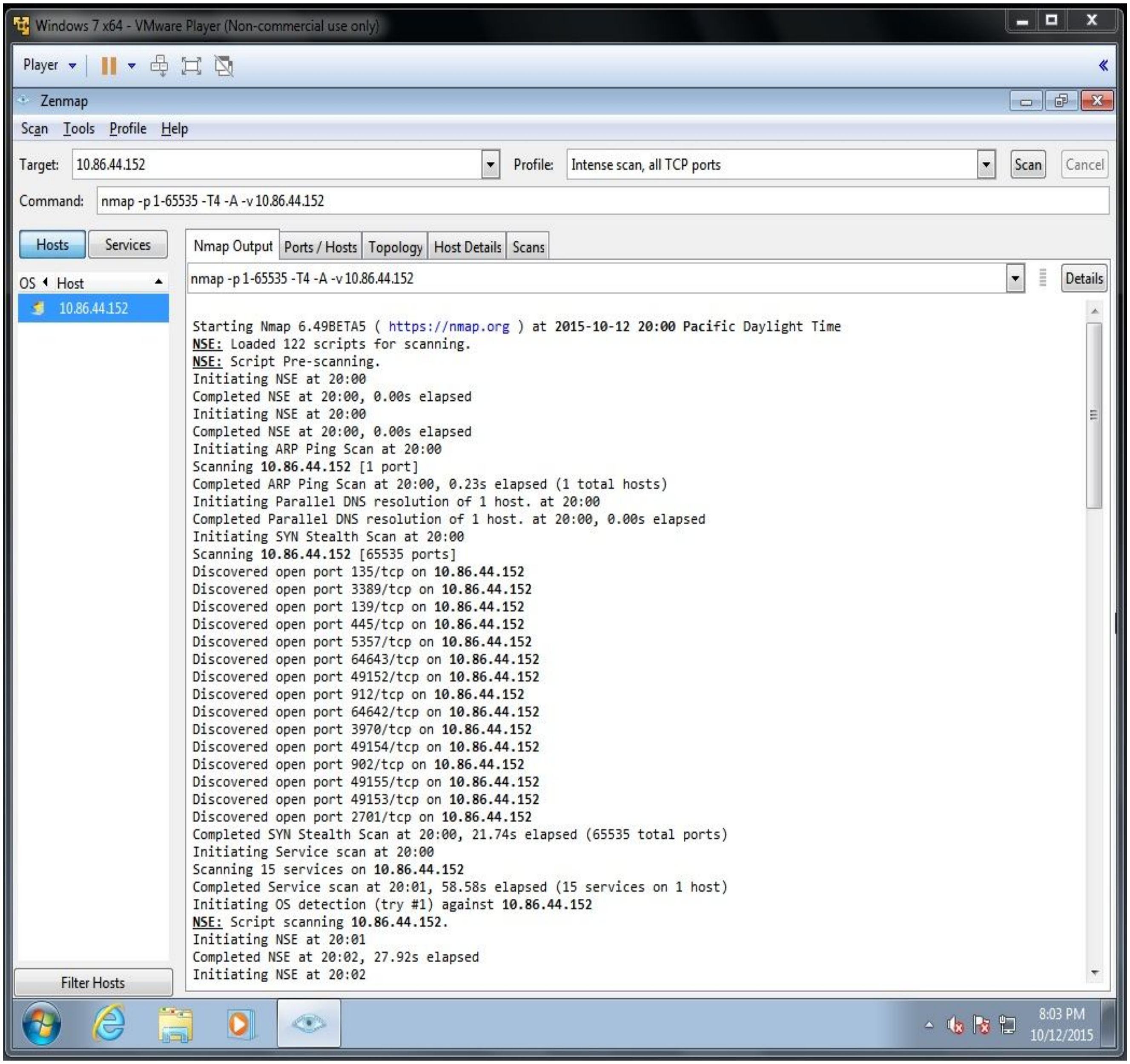
Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) PRO/1000 MT Network Connecti
Physical Address	00-0C-29-31-EF-22
DHCP Enabled	No
IPv4 Address	10.86.44.154
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.86.44.1
IPv4 DNS Server	130.182.1.11
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes

Step 4: Downloading & Installing nmap software on Virtual Machine

- ➔ We downloaded the nmap software from www.nmap.org
- ➔ nmap software version: nmap-6.49BETA5-setup-xp.exe
- ➔ and then, we installed this software

Step 5: TCP Port Scanning

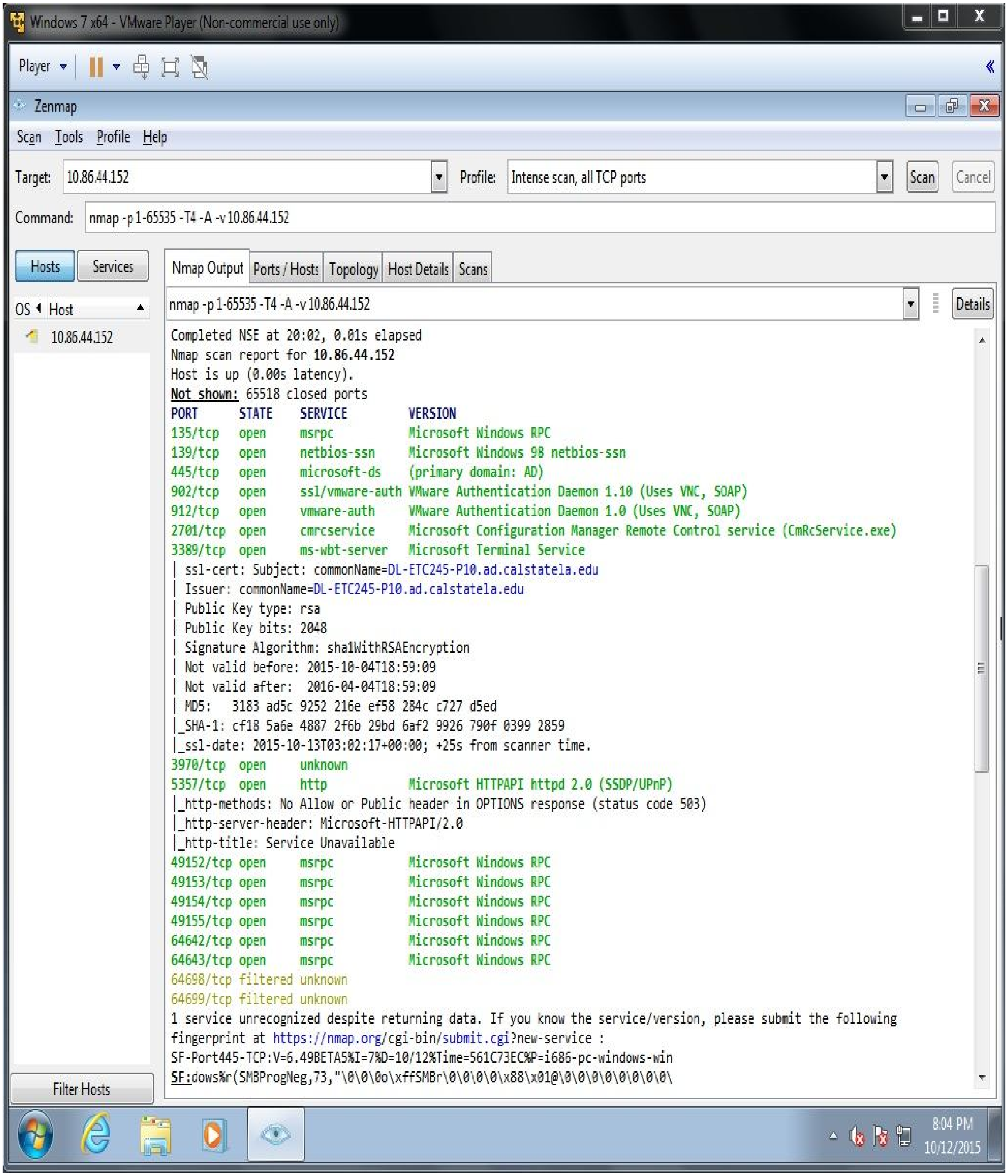


Target: 10.86.44.152

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 10.86.44.152

```
nmap -p 1-65535 -T4 -A -v 10.86.44.152

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-10-12 20:00 Pacific Daylight Time
NSE: Loaded 122 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:00
Completed NSE at 20:00, 0.00s elapsed
Initiating NSE at 20:00
Completed NSE at 20:00, 0.00s elapsed
Initiating ARP Ping Scan at 20:00
Scanning 10.86.44.152 [1 port]
Completed ARP Ping Scan at 20:00, 0.23s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:00
Completed Parallel DNS resolution of 1 host. at 20:00, 0.00s elapsed
Initiating SYN Stealth Scan at 20:00
Scanning 10.86.44.152 [65535 ports]
Discovered open port 135/tcp on 10.86.44.152
Discovered open port 3389/tcp on 10.86.44.152
Discovered open port 139/tcp on 10.86.44.152
Discovered open port 445/tcp on 10.86.44.152
Discovered open port 5357/tcp on 10.86.44.152
Discovered open port 64643/tcp on 10.86.44.152
Discovered open port 49152/tcp on 10.86.44.152
Discovered open port 912/tcp on 10.86.44.152
Discovered open port 64642/tcp on 10.86.44.152
Discovered open port 3970/tcp on 10.86.44.152
Discovered open port 49154/tcp on 10.86.44.152
Discovered open port 902/tcp on 10.86.44.152
Discovered open port 49155/tcp on 10.86.44.152
Discovered open port 49153/tcp on 10.86.44.152
Discovered open port 2701/tcp on 10.86.44.152
Completed SYN Stealth Scan at 20:00, 21.74s elapsed (65535 total ports)
Initiating Service scan at 20:00
Scanning 15 services on 10.86.44.152
Completed Service scan at 20:01, 58.58s elapsed (15 services on 1 host)
Initiating OS detection (try #1) against 10.86.44.152
NSE: Script scanning 10.86.44.152.
Initiating NSE at 20:01
Completed NSE at 20:02, 27.92s elapsed
Initiating NSE at 20:02
```



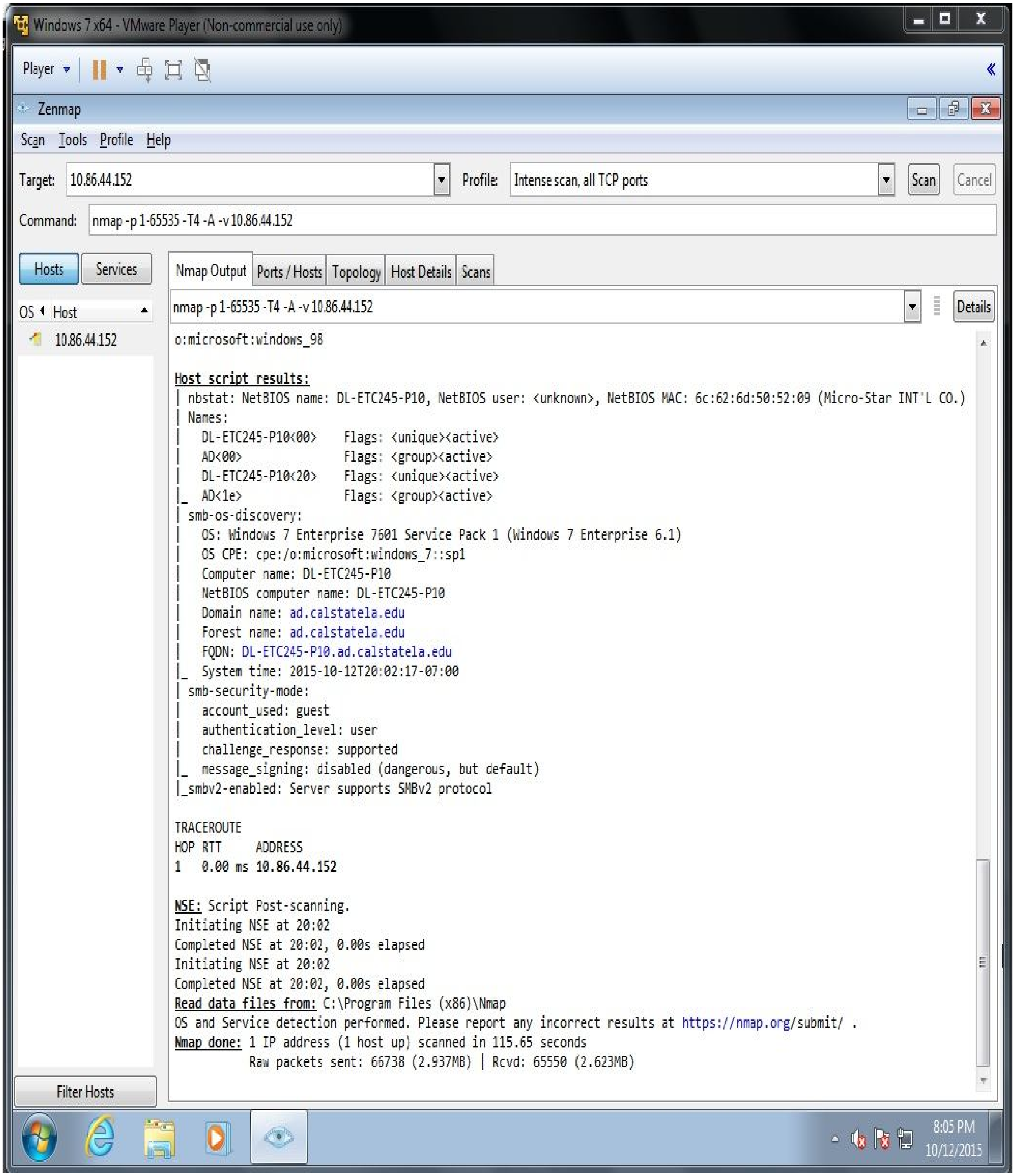
Target: 10.86.44.152

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 10.86.44.152

```
nmap -p 1-65535 -T4 -A -v 10.86.44.152
```

```
Completed NSE at 20:02, 0.01s elapsed
Nmap scan report for 10.86.44.152
Host is up (0.00s latency).
Not shown: 65518 closed ports
PORT      STATE    SERVICE         VERSION
135/tcp   open     msrpc           Microsoft Windows RPC
139/tcp   open     netbios-ssn     Microsoft Windows 98 netbios-ssn
445/tcp   open     microsoft-ds    (primary domain: AD)
902/tcp   open     ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open     vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
2701/tcp  open     cmrcservice     Microsoft Configuration Manager Remote Control service (CmRcService.exe)
3389/tcp  open     ms-wbt-server   Microsoft Terminal Service
| ssl-cert: Subject: commonName=DL-ETC245-P10.ad.calstatela.edu
| Issuer: commonName=DL-ETC245-P10.ad.calstatela.edu
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-10-04T18:59:09
| Not valid after:  2016-04-04T18:59:09
| MD5:   3183 ad5c 9252 216e ef58 284c c727 d5ed
|_SHA-1: cf18 5a6e 4887 2f6b 29bd 6af2 9926 790f 0399 2859
|_ssl-date: 2015-10-13T03:02:17+00:00; +25s from scanner time.
3970/tcp  open     unknown
5357/tcp  open     http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open     msrpc           Microsoft Windows RPC
49153/tcp open     msrpc           Microsoft Windows RPC
49154/tcp open     msrpc           Microsoft Windows RPC
49155/tcp open     msrpc           Microsoft Windows RPC
64642/tcp open     msrpc           Microsoft Windows RPC
64643/tcp open     msrpc           Microsoft Windows RPC
64698/tcp filtered unknown
64699/tcp filtered unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port445-TCP:V=6.49BETA5%I=7%D=10/12%Time=561C73EC%P=i686-pc-windows-win
SF:dows%r(SMBProgNeg,73,"\0\0\0o\xffSMBr\0\0\0\0\x88\x01@\0\0\0\0\0\0\0\0\
```



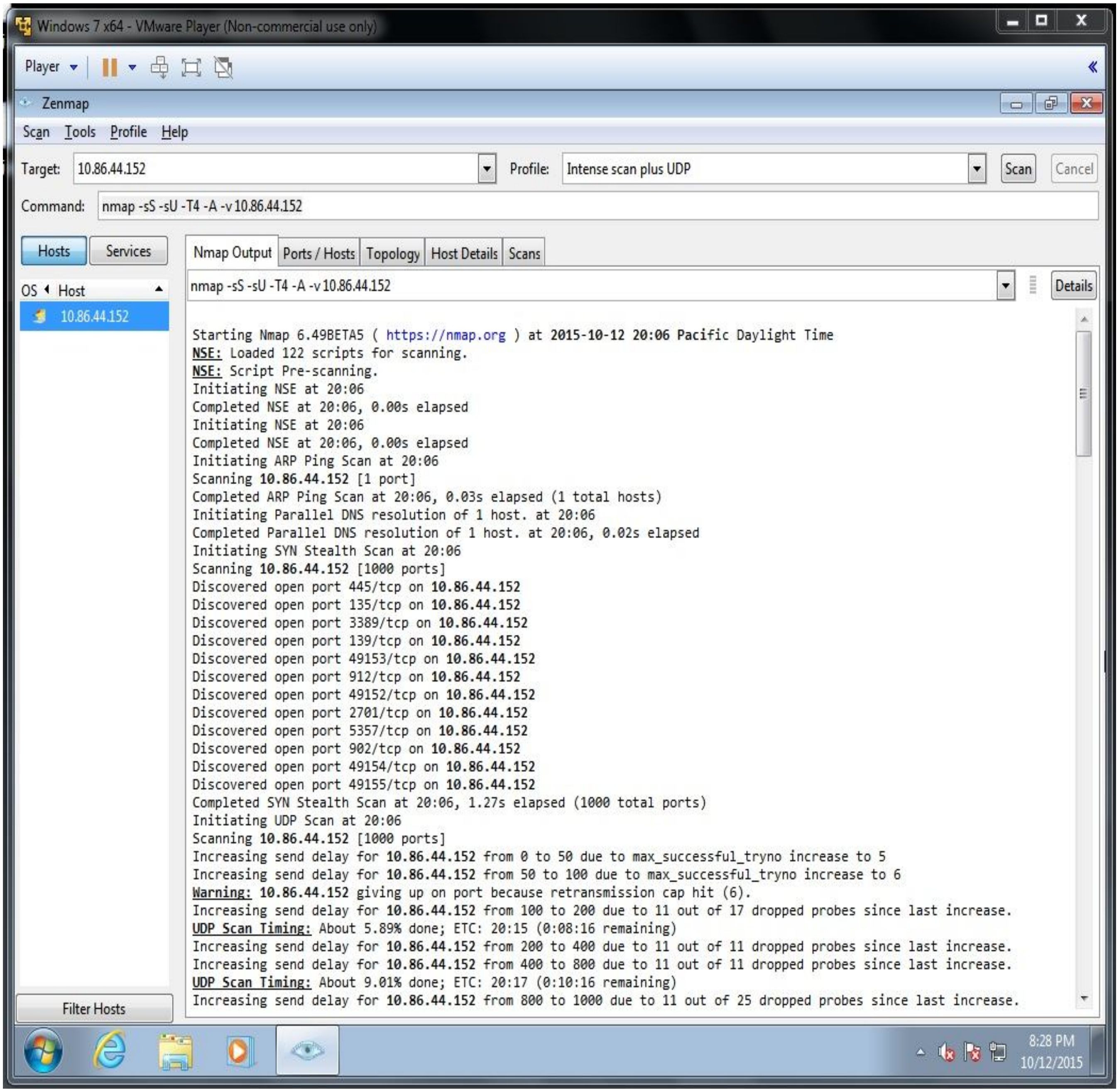
Target: 10.86.44.152

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 10.86.44.152

```
nmap -p 1-65535 -T4 -A -v 10.86.44.152
o:microsoft:windows_98

Host script results:
| nbstat: NetBIOS name: DL-ETC245-P10, NetBIOS user: <unknown>, NetBIOS MAC: 6c:62:6d:50:52:09 (Micro-Star INT'L CO.)
| Names:
|   DL-ETC245-P10<00>    Flags: <unique><active>
|   AD<00>               Flags: <group><active>
|   DL-ETC245-P10<20>    Flags: <unique><active>
|_  AD<1e>               Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: DL-ETC245-P10
|   NetBIOS computer name: DL-ETC245-P10
|   Domain name: ad.calstatela.edu
|   Forest name: ad.calstatela.edu
|   FQDN: DL-ETC245-P10.ad.calstatela.edu
|_  System time: 2015-10-12T20:02:17-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   0.00 ms 10.86.44.152

NSE: Script Post-scanning.
Initiating NSE at 20:02
Completed NSE at 20:02, 0.00s elapsed
Initiating NSE at 20:02
Completed NSE at 20:02, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 115.65 seconds
           Raw packets sent: 66738 (2.937MB) | Rcvd: 65550 (2.623MB)
```

Step 6: UDP Port Scanning

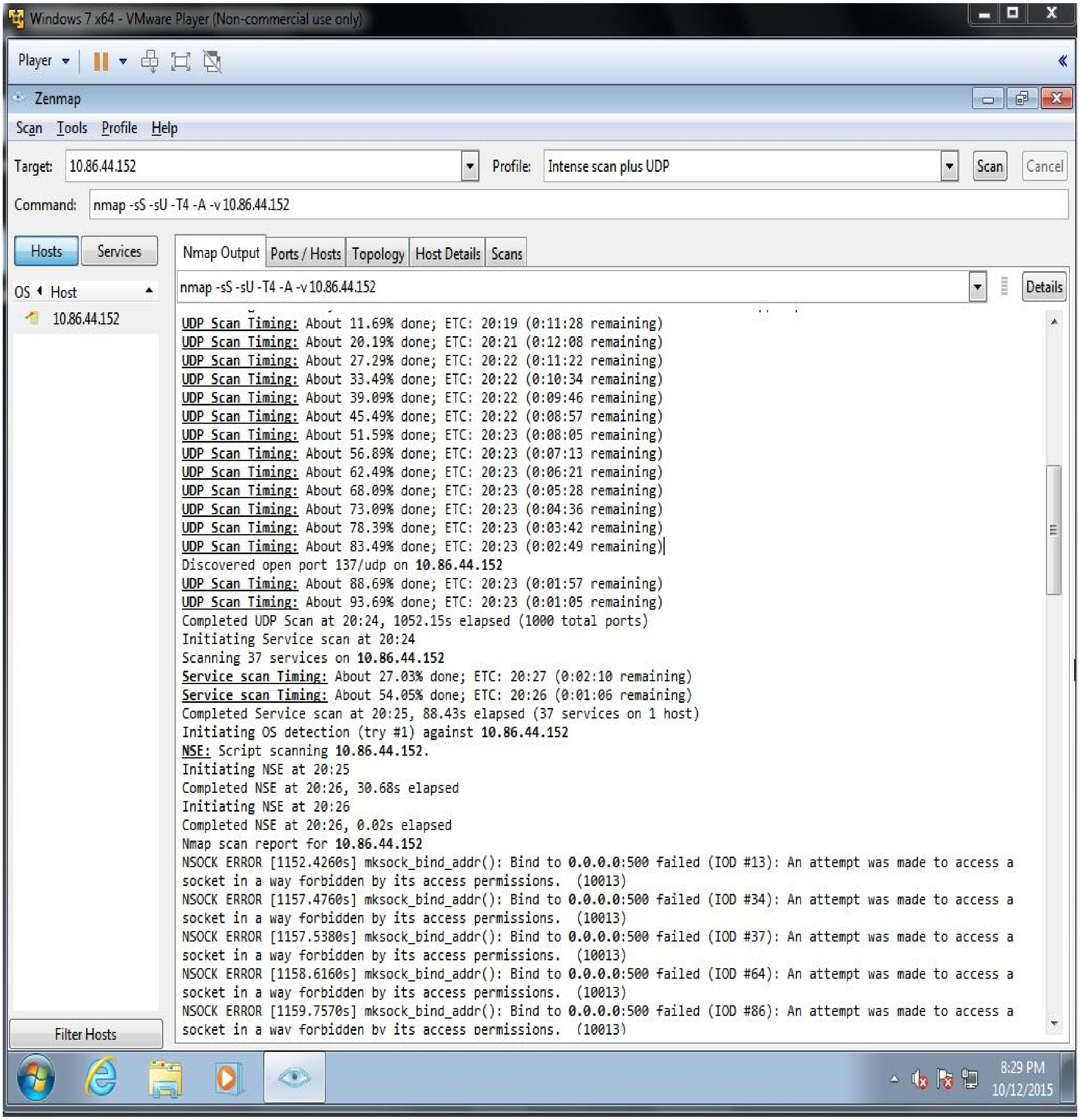


Target: 10.86.44.152

Profile: Intense scan plus UDP

Command: nmap -sS -sU -T4 -A -v 10.86.44.152

```
Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-10-12 20:06 Pacific Daylight Time
NSE: Loaded 122 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:06
Completed NSE at 20:06, 0.00s elapsed
Initiating NSE at 20:06
Completed NSE at 20:06, 0.00s elapsed
Initiating ARP Ping Scan at 20:06
Scanning 10.86.44.152 [1 port]
Completed ARP Ping Scan at 20:06, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:06
Completed Parallel DNS resolution of 1 host. at 20:06, 0.02s elapsed
Initiating SYN Stealth Scan at 20:06
Scanning 10.86.44.152 [1000 ports]
Discovered open port 445/tcp on 10.86.44.152
Discovered open port 135/tcp on 10.86.44.152
Discovered open port 3389/tcp on 10.86.44.152
Discovered open port 139/tcp on 10.86.44.152
Discovered open port 49153/tcp on 10.86.44.152
Discovered open port 912/tcp on 10.86.44.152
Discovered open port 49152/tcp on 10.86.44.152
Discovered open port 2701/tcp on 10.86.44.152
Discovered open port 5357/tcp on 10.86.44.152
Discovered open port 902/tcp on 10.86.44.152
Discovered open port 49154/tcp on 10.86.44.152
Discovered open port 49155/tcp on 10.86.44.152
Completed SYN Stealth Scan at 20:06, 1.27s elapsed (1000 total ports)
Initiating UDP Scan at 20:06
Scanning 10.86.44.152 [1000 ports]
Increasing send delay for 10.86.44.152 from 0 to 50 due to max_successful_tryno increase to 5
Increasing send delay for 10.86.44.152 from 50 to 100 due to max_successful_tryno increase to 6
Warning: 10.86.44.152 giving up on port because retransmission cap hit (6).
Increasing send delay for 10.86.44.152 from 100 to 200 due to 11 out of 17 dropped probes since last increase.
UDP Scan Timing: About 5.89% done; ETC: 20:15 (0:08:16 remaining)
Increasing send delay for 10.86.44.152 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 10.86.44.152 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 9.01% done; ETC: 20:17 (0:10:16 remaining)
Increasing send delay for 10.86.44.152 from 800 to 1000 due to 11 out of 25 dropped probes since last increase.
```



Target: 10.86.44.152

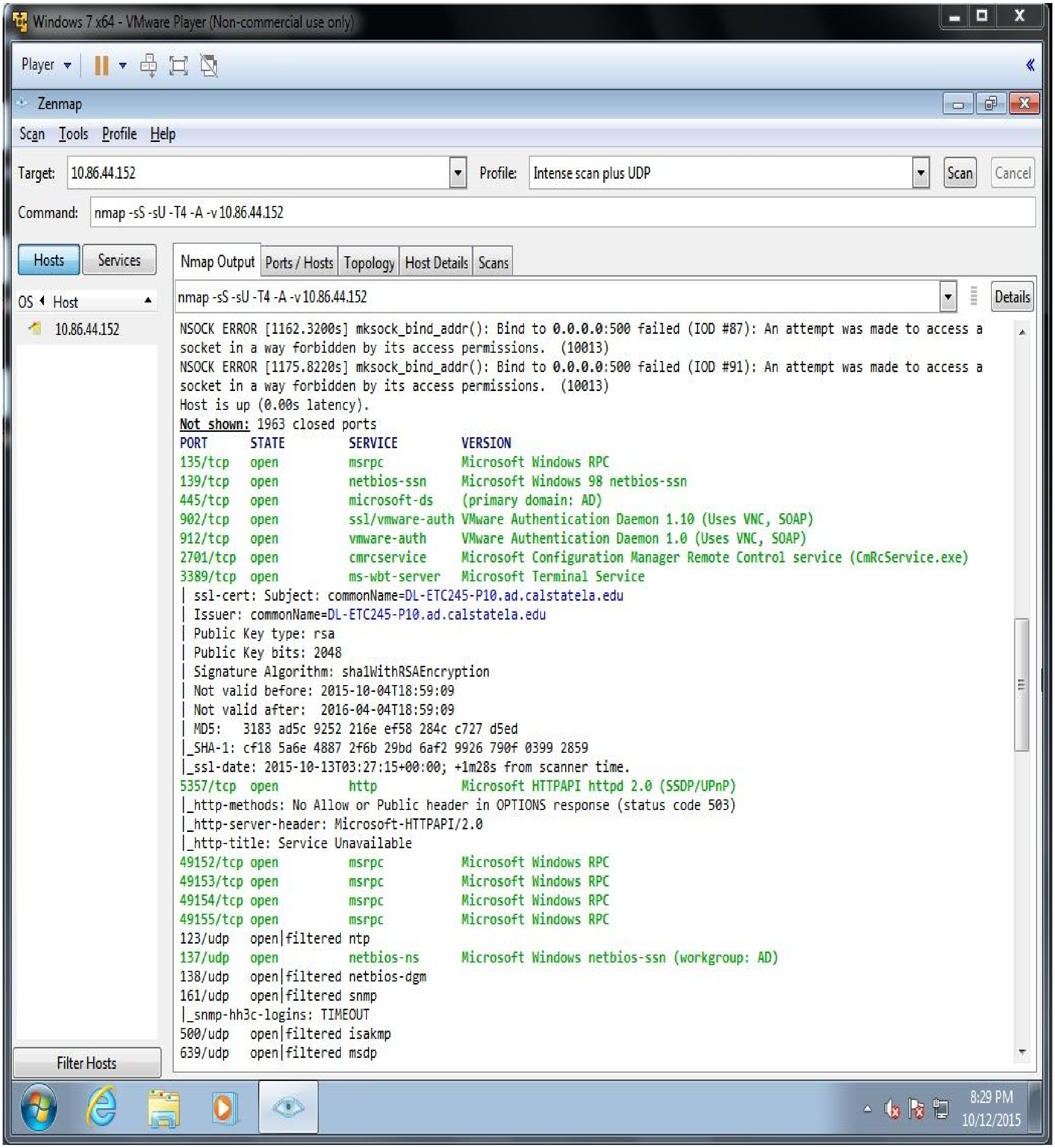
Profile: Intense scan plus UDP

Command: nmap -sS -sU -T4 -A -v 10.86.44.152

10.86.44.152

nmap -sS -sU -T4 -A -v 10.86.44.152

```
UDP Scan Timing: About 11.69% done; ETC: 20:19 (0:11:28 remaining)
UDP Scan Timing: About 20.19% done; ETC: 20:21 (0:12:08 remaining)
UDP Scan Timing: About 27.29% done; ETC: 20:22 (0:11:22 remaining)
UDP Scan Timing: About 33.49% done; ETC: 20:22 (0:10:34 remaining)
UDP Scan Timing: About 39.09% done; ETC: 20:22 (0:09:46 remaining)
UDP Scan Timing: About 45.49% done; ETC: 20:22 (0:08:57 remaining)
UDP Scan Timing: About 51.59% done; ETC: 20:23 (0:08:05 remaining)
UDP Scan Timing: About 56.89% done; ETC: 20:23 (0:07:13 remaining)
UDP Scan Timing: About 62.49% done; ETC: 20:23 (0:06:21 remaining)
UDP Scan Timing: About 68.09% done; ETC: 20:23 (0:05:28 remaining)
UDP Scan Timing: About 73.09% done; ETC: 20:23 (0:04:36 remaining)
UDP Scan Timing: About 78.39% done; ETC: 20:23 (0:03:42 remaining)
UDP Scan Timing: About 83.49% done; ETC: 20:23 (0:02:49 remaining)
Discovered open port 137/udp on 10.86.44.152
UDP Scan Timing: About 88.69% done; ETC: 20:23 (0:01:57 remaining)
UDP Scan Timing: About 93.69% done; ETC: 20:23 (0:01:05 remaining)
Completed UDP Scan at 20:24, 1052.15s elapsed (1000 total ports)
Initiating Service scan at 20:24
Scanning 37 services on 10.86.44.152
Service scan Timing: About 27.03% done; ETC: 20:27 (0:02:10 remaining)
Service scan Timing: About 54.05% done; ETC: 20:26 (0:01:06 remaining)
Completed Service scan at 20:25, 88.43s elapsed (37 services on 1 host)
Initiating OS detection (try #1) against 10.86.44.152
NSE: Script scanning 10.86.44.152.
Initiating NSE at 20:25
Completed NSE at 20:26, 30.68s elapsed
Initiating NSE at 20:26
Completed NSE at 20:26, 0.02s elapsed
Nmap scan report for 10.86.44.152
NSOCK ERROR [1152.4260s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #13): An attempt was made to access a
socket in a way forbidden by its access permissions.  (10013)
NSOCK ERROR [1157.4760s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #34): An attempt was made to access a
socket in a way forbidden by its access permissions.  (10013)
NSOCK ERROR [1157.5380s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #37): An attempt was made to access a
socket in a way forbidden by its access permissions.  (10013)
NSOCK ERROR [1158.6160s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #64): An attempt was made to access a
socket in a way forbidden by its access permissions.  (10013)
NSOCK ERROR [1159.7570s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #86): An attempt was made to access a
socket in a wav forbidden bv its access permissions.  (10013)
```



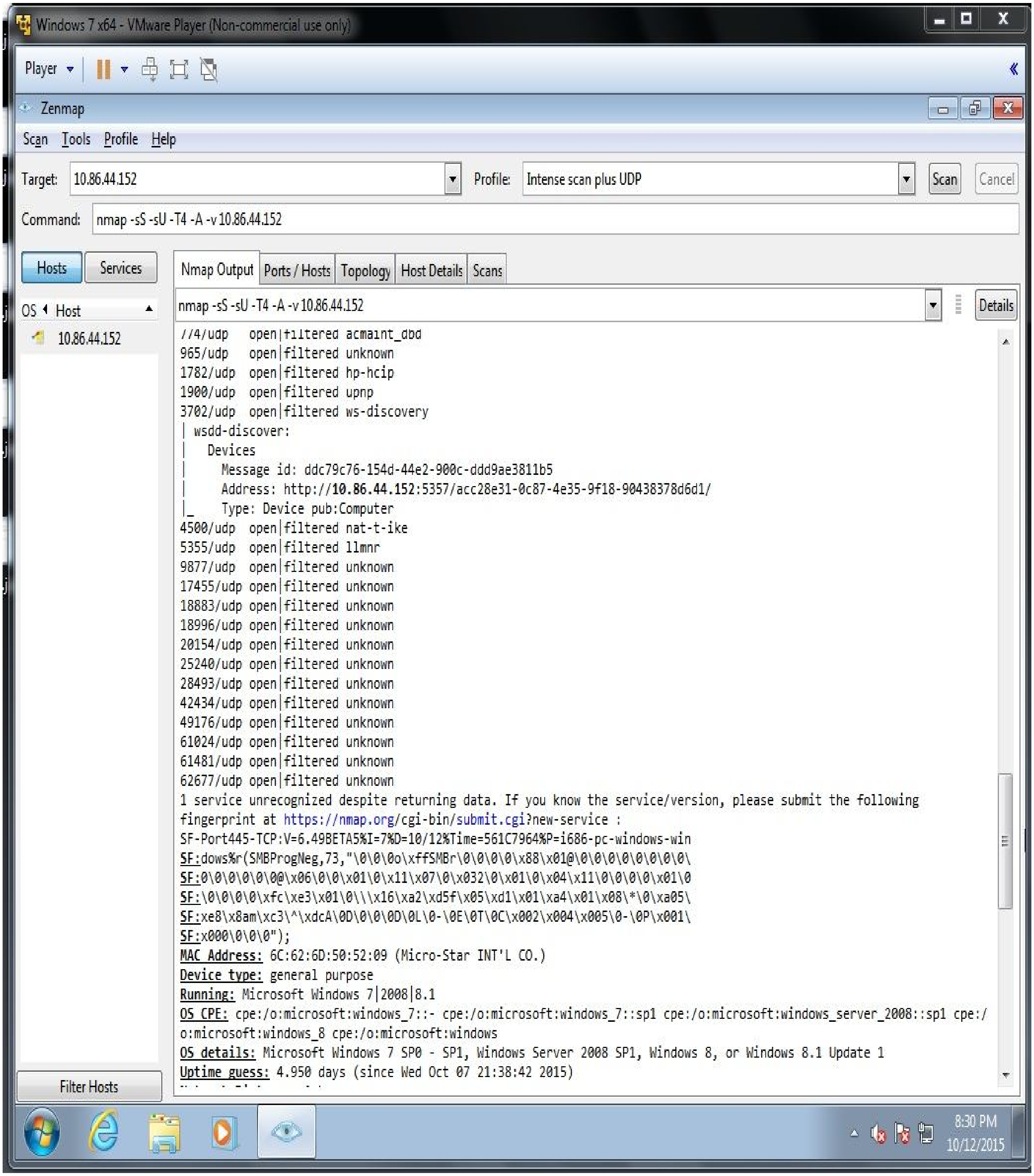
Target: 10.86.44.152

Profile: Intense scan plus UDP

Command: nmap -sS -sU -T4 -A -v 10.86.44.152

```
nmap -sS -sU -T4 -A -v 10.86.44.152
```

```
NSOCK ERROR [1162.3200s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #87): An attempt was made to access a
socket in a way forbidden by its access permissions.  (10013)
NSOCK ERROR [1175.8220s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #91): An attempt was made to access a
socket in a way forbidden by its access permissions.  (10013)
Host is up (0.00s latency).
Not shown: 1963 closed ports
PORT      STATE         SERVICE         VERSION
135/tcp   open          msrpc           Microsoft Windows RPC
139/tcp   open          netbios-ssn     Microsoft Windows 98 netbios-ssn
445/tcp   open          microsoft-ds    (primary domain: AD)
902/tcp   open          ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open          vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
2701/tcp  open          cmrcservice     Microsoft Configuration Manager Remote Control service (CmRcService.exe)
3389/tcp  open          ms-wbt-server   Microsoft Terminal Service
| ssl-cert: Subject: commonName=DL-ETC245-P10.ad.calstatela.edu
| Issuer: commonName=DL-ETC245-P10.ad.calstatela.edu
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-10-04T18:59:09
| Not valid after:  2016-04-04T18:59:09
| MD5:   3183 ad5c 9252 216e ef58 284c c727 d5ed
|_SHA-1: cf18 5a6e 4887 2f6b 29bd 6af2 9926 790f 0399 2859
|_ssl-date: 2015-10-13T03:27:15+00:00; +1m28s from scanner time.
5357/tcp  open          http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open          msrpc           Microsoft Windows RPC
49153/tcp open          msrpc           Microsoft Windows RPC
49154/tcp open          msrpc           Microsoft Windows RPC
49155/tcp open          msrpc           Microsoft Windows RPC
123/udp   open|filtered ntp
137/udp   open          netbios-ns      Microsoft Windows netbios-ssn (workgroup: AD)
138/udp   open|filtered netbios-dgm
161/udp   open|filtered snmp
|_snmp-hh3c-logins: TIMEOUT
500/udp   open|filtered isakmp
639/udp   open|filtered msdp
```

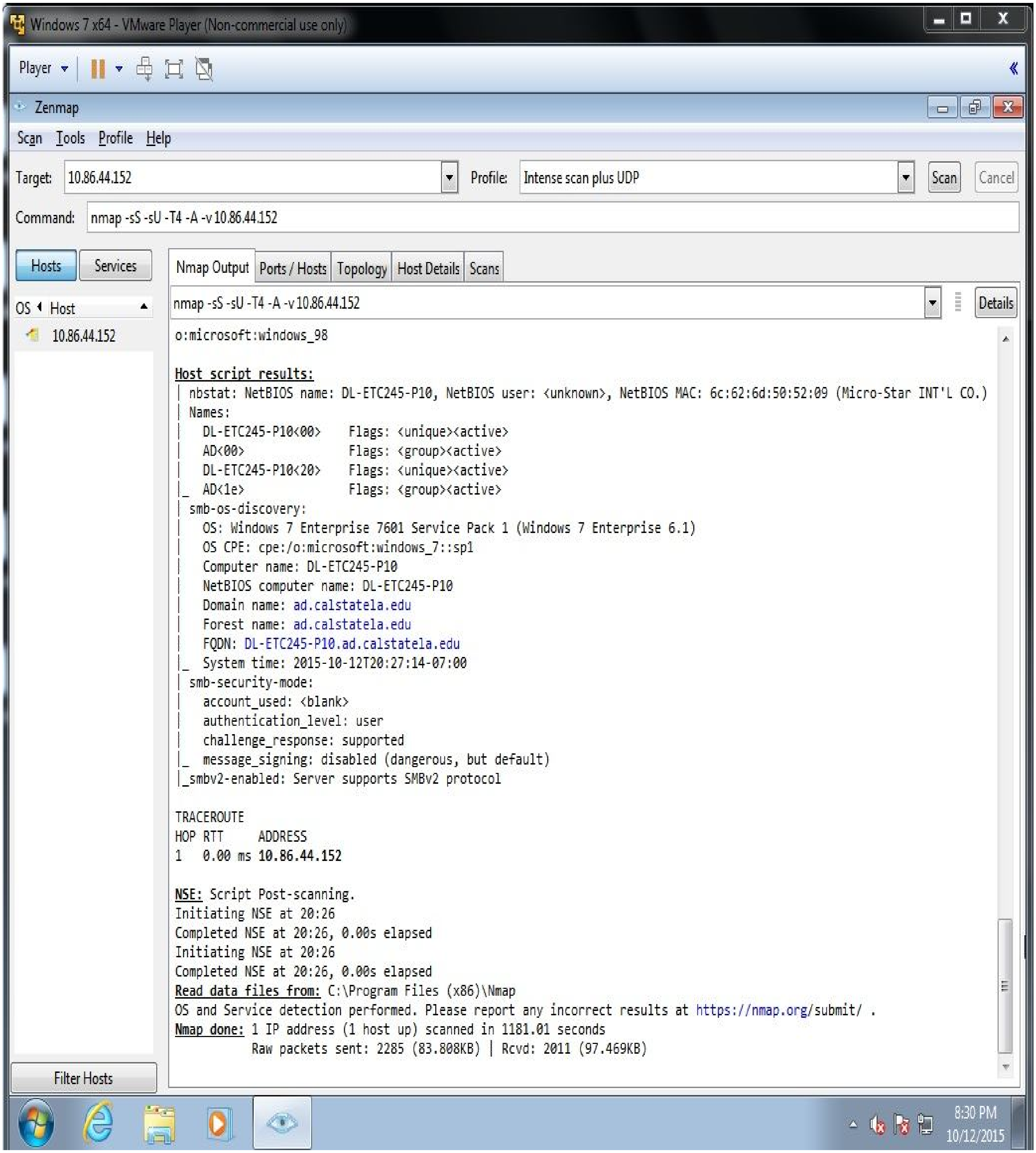


Target: 10.86.44.152

Profile: Intense scan plus UDP

Command: nmap -sS -sU -T4 -A -v 10.86.44.152

```
nmap -sS -sU -T4 -A -v 10.86.44.152
774/udp   open|filtered acmaint_dbd
965/udp   open|filtered unknown
1782/udp  open|filtered hp-hcip
1900/udp  open|filtered upnp
3702/udp  open|filtered ws-discovery
| wsdd-discover:
|   Devices
|     Message id: ddc79c76-154d-44e2-900c-ddd9ae3811b5
|     Address: http://10.86.44.152:5357/acc28e31-0c87-4e35-9f18-90438378d6d1/
|_    Type: Device pub:Computer
4500/udp  open|filtered nat-t-ike
5355/udp  open|filtered llmnr
9877/udp  open|filtered unknown
17455/udp open|filtered unknown
18883/udp open|filtered unknown
18996/udp open|filtered unknown
20154/udp open|filtered unknown
25240/udp open|filtered unknown
28493/udp open|filtered unknown
42434/udp open|filtered unknown
49176/udp open|filtered unknown
61024/udp open|filtered unknown
61481/udp open|filtered unknown
62677/udp open|filtered unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port445-TCP:V=6.49BETA5%I=7%D=10/12%Time=561C7964%P=i686-pc-windows-win
SF:dows%r(SMBProgNeg,73,"\0\0\0o\xffSMBr\0\0\0\0\x88\x01@\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0@\x06\0\0\x01\0\x11\x07\0\x032\0\x01\0\x04\x11\0\0\0\0\x01\0
SF:\0\0\0\0\xfc\xe3\x01\0\\\x16\xa2\xd5f\x05\xd1\x01\xa4\x01\x08\*\0\xa05\
SF:xe8\x8am\xc3\^\xdcA\0D\0\0\0D\0L\0-\0E\0T\0C\x002\x004\x005\0-\0P\x001\
SF:x000\0\0\0");
MAC Address: 6C:62:6D:50:52:09 (Micro-Star INT'L CO.)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/
o:microsoft:windows_8 cpe:/o:microsoft:windows
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Windows 8.1 Update 1
Uptime guess: 4.950 days (since Wed Oct 07 21:38:42 2015)
```



Target: 10.86.44.152

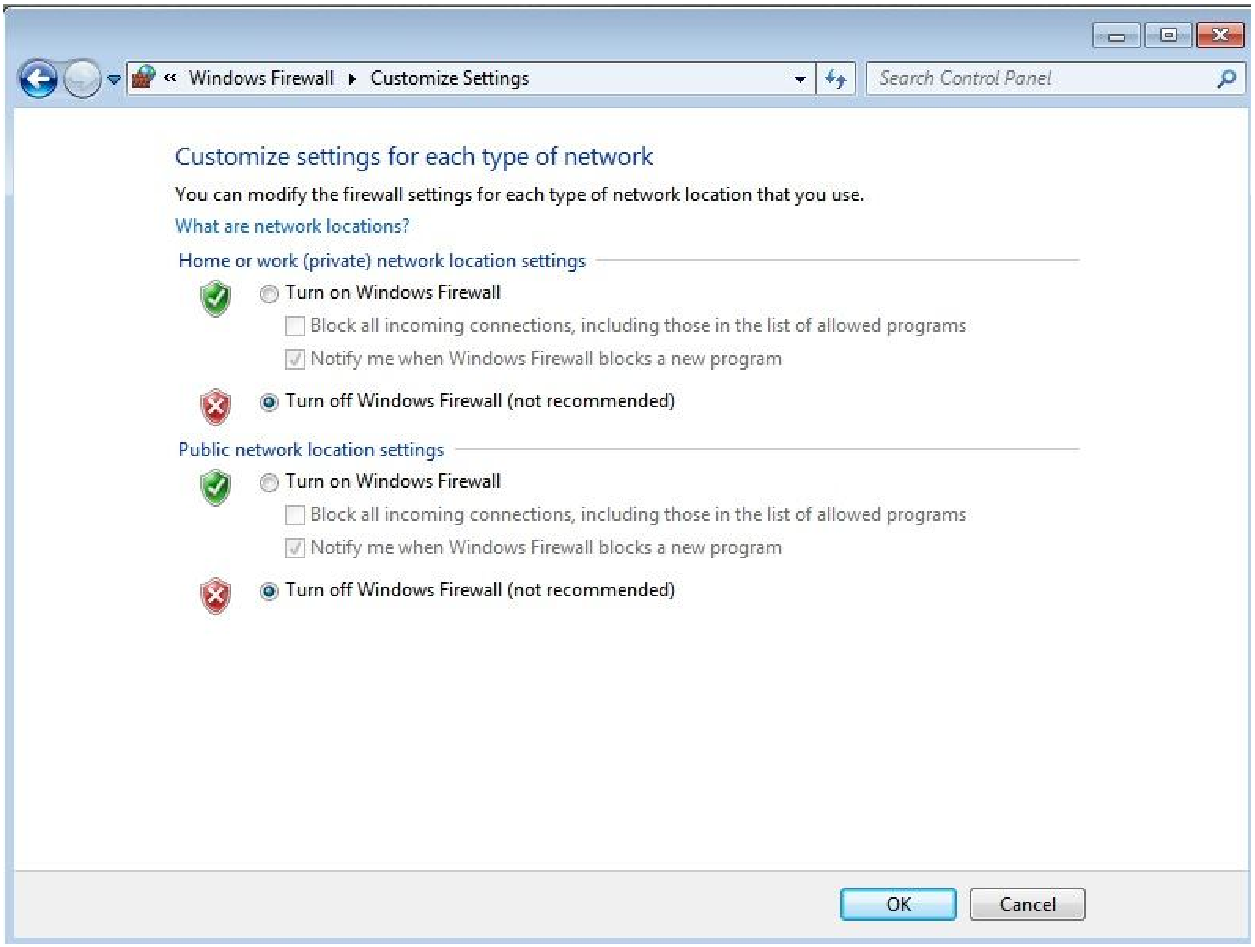
Profile: Intense scan plus UDP

Command: nmap -sS -sU -T4 -A -v 10.86.44.152

nmap -sS -sU -T4 -A -v 10.86.44.152

```
o:microsoft:windows_98

Host script results:
| nbstat: NetBIOS name: DL-ETC245-P10, NetBIOS user: <unknown>, NetBIOS MAC: 6c:62:6d:50:52:09 (Micro-Star INT'L CO.)
| Names:
|   DL-ETC245-P10<00>    Flags: <unique><active>
|   AD<00>               Flags: <group><active>
|   DL-ETC245-P10<20>    Flags: <unique><active>
|_  AD<1e>               Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: DL-ETC245-P10
|   NetBIOS computer name: DL-ETC245-P10
|   Domain name: ad.calstatela.edu
|   Forest name: ad.calstatela.edu
|   FQDN: DL-ETC245-P10.ad.calstatela.edu
|_  System time: 2015-10-12T20:27:14-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   0.00 ms 10.86.44.152

NSE: Script Post-scanning.
Initiating NSE at 20:26
Completed NSE at 20:26, 0.00s elapsed
Initiating NSE at 20:26
Completed NSE at 20:26, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1181.01 seconds
           Raw packets sent: 2285 (83.808KB) | Rcvd: 2011 (97.469KB)
```

Step 7: Temporarily Turned off Firewall on Virtual Machine



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

Public network location settings

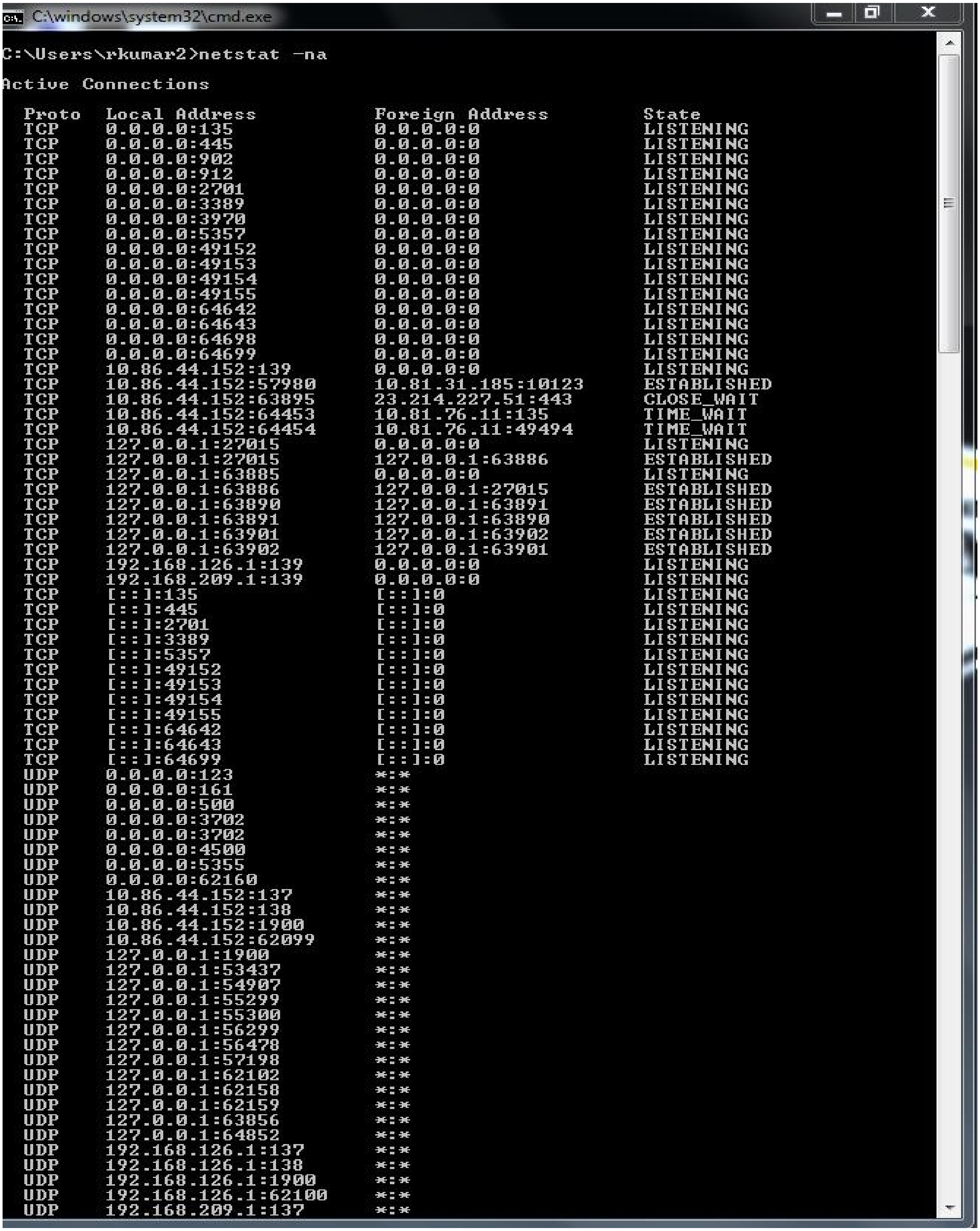
○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

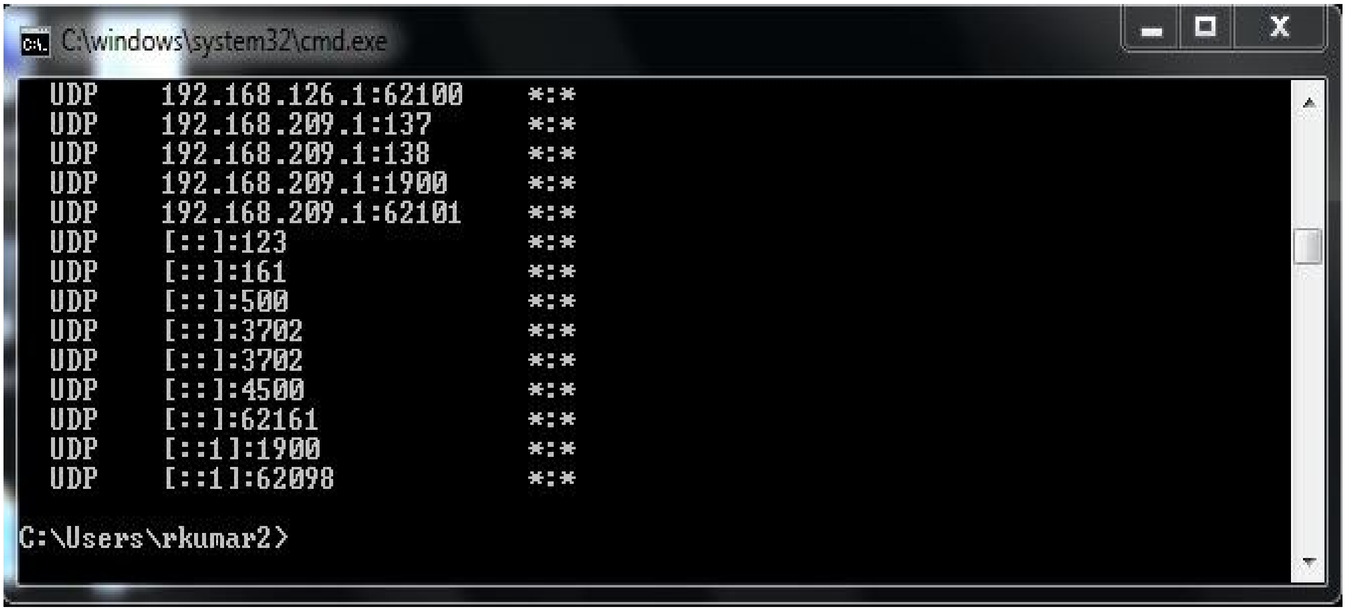
☑ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

Step 8: Submitting output of “netstat -na” for TCP Port

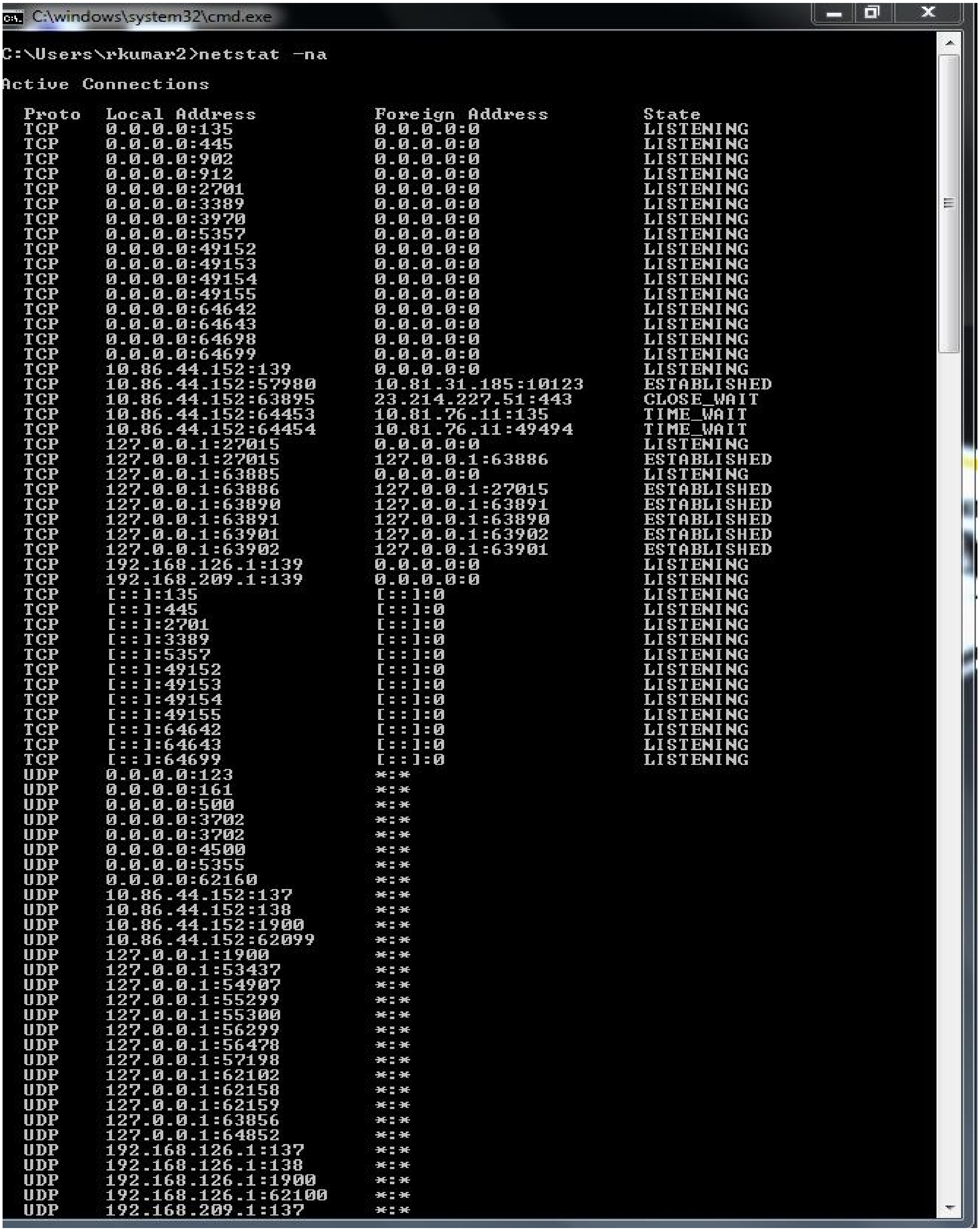


```
C:\Users\rkumar2>netstat -na

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2701           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3970           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:64642          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:64643          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:64698          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:64699          0.0.0.0:0              LISTENING
  TCP    10.86.44.152:139       0.0.0.0:0              LISTENING
  TCP    10.86.44.152:57980     10.81.31.185:10123     ESTABLISHED
  TCP    10.86.44.152:63895     23.214.227.51:443      CLOSE_WAIT
  TCP    10.86.44.152:64453     10.81.76.11:135        TIME_WAIT
  TCP    10.86.44.152:64454     10.81.76.11:49494      TIME_WAIT
  TCP    127.0.0.1:27015        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:27015        127.0.0.1:63886        ESTABLISHED
  TCP    127.0.0.1:63885        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:63886        127.0.0.1:27015        ESTABLISHED
  TCP    127.0.0.1:63890        127.0.0.1:63891        ESTABLISHED
  TCP    127.0.0.1:63891        127.0.0.1:63890        ESTABLISHED
  TCP    127.0.0.1:63901        127.0.0.1:63902        ESTABLISHED
  TCP    127.0.0.1:63902        127.0.0.1:63901        ESTABLISHED
  TCP    192.168.126.1:139      0.0.0.0:0              LISTENING
  TCP    192.168.209.1:139      0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:2701              [::]:0                 LISTENING
  TCP    [::]:3389              [::]:0                 LISTENING
  TCP    [::]:5357              [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:64642             [::]:0                 LISTENING
  TCP    [::]:64643             [::]:0                 LISTENING
  TCP    [::]:64699             [::]:0                 LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:161            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:62160          *:*
  UDP    10.86.44.152:137       *:*
  UDP    10.86.44.152:138       *:*
  UDP    10.86.44.152:1900      *:*
  UDP    10.86.44.152:62099     *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:53437        *:*
  UDP    127.0.0.1:54907        *:*
  UDP    127.0.0.1:55299        *:*
  UDP    127.0.0.1:55300        *:*
  UDP    127.0.0.1:56299        *:*
  UDP    127.0.0.1:56478        *:*
  UDP    127.0.0.1:57198        *:*
  UDP    127.0.0.1:62102        *:*
  UDP    127.0.0.1:62158        *:*
  UDP    127.0.0.1:62159        *:*
  UDP    127.0.0.1:63856        *:*
  UDP    127.0.0.1:64852        *:*
  UDP    192.168.126.1:137      *:*
  UDP    192.168.126.1:138      *:*
  UDP    192.168.126.1:1900     *:*
  UDP    192.168.126.1:62100    *:*
  UDP    192.168.209.1:137      *:*
```

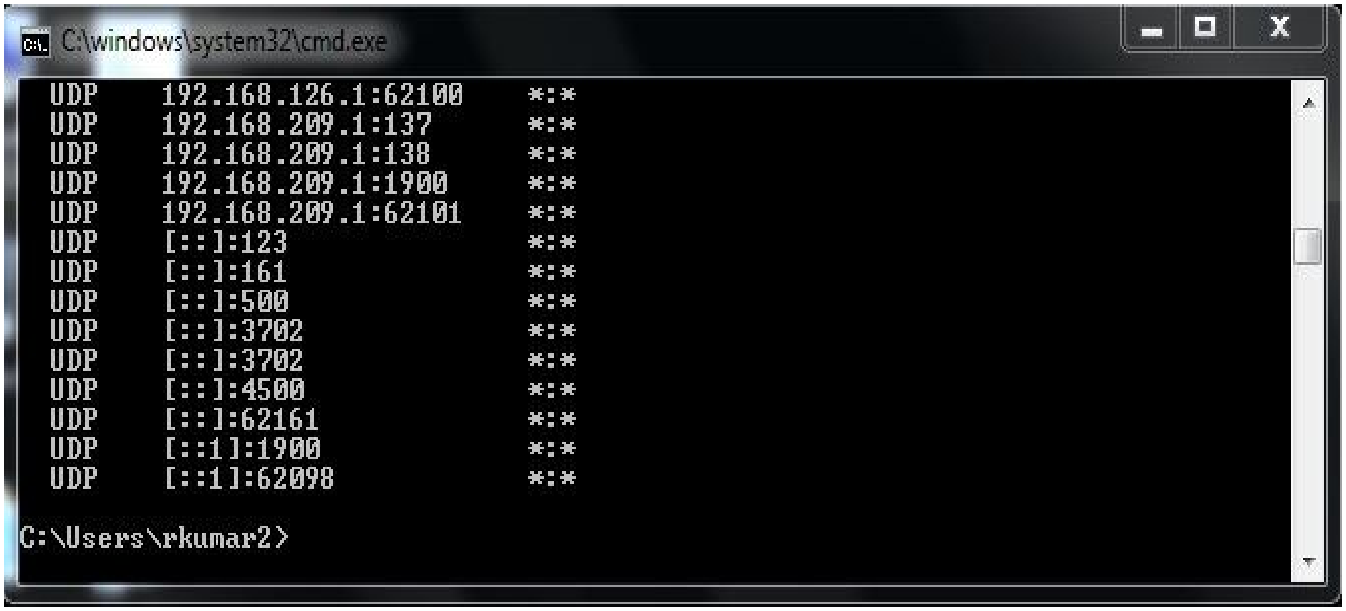


```
  UDP    192.168.126.1:62100    *:*
  UDP    192.168.209.1:137      *:*
  UDP    192.168.209.1:138      *:*
  UDP    192.168.209.1:1900     *:*
  UDP    192.168.209.1:62101    *:*
  UDP    [::]:123               *:*
  UDP    [::]:161               *:*
  UDP    [::]:500               *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:4500              *:*
  UDP    [::]:62161             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:62098            *:*

C:\Users\rkumar2>
```

Step 9: Submitting output of “netstat -na” for UDP Port



```
C:\Users\rkumar2>netstat -na

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2701           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3970           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:64642          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:64643          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:64698          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:64699          0.0.0.0:0              LISTENING
  TCP    10.86.44.152:139       0.0.0.0:0              LISTENING
  TCP    10.86.44.152:57980     10.81.31.185:10123     ESTABLISHED
  TCP    10.86.44.152:63895     23.214.227.51:443      CLOSE_WAIT
  TCP    10.86.44.152:64453     10.81.76.11:135        TIME_WAIT
  TCP    10.86.44.152:64454     10.81.76.11:49494      TIME_WAIT
  TCP    127.0.0.1:27015        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:27015        127.0.0.1:63886        ESTABLISHED
  TCP    127.0.0.1:63885        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:63886        127.0.0.1:27015        ESTABLISHED
  TCP    127.0.0.1:63890        127.0.0.1:63891        ESTABLISHED
  TCP    127.0.0.1:63891        127.0.0.1:63890        ESTABLISHED
  TCP    127.0.0.1:63901        127.0.0.1:63902        ESTABLISHED
  TCP    127.0.0.1:63902        127.0.0.1:63901        ESTABLISHED
  TCP    192.168.126.1:139      0.0.0.0:0              LISTENING
  TCP    192.168.209.1:139      0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:2701              [::]:0                 LISTENING
  TCP    [::]:3389              [::]:0                 LISTENING
  TCP    [::]:5357              [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:64642             [::]:0                 LISTENING
  TCP    [::]:64643             [::]:0                 LISTENING
  TCP    [::]:64699             [::]:0                 LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:161            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:62160          *:*
  UDP    10.86.44.152:137       *:*
  UDP    10.86.44.152:138       *:*
  UDP    10.86.44.152:1900      *:*
  UDP    10.86.44.152:62099     *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:53437        *:*
  UDP    127.0.0.1:54907        *:*
  UDP    127.0.0.1:55299        *:*
  UDP    127.0.0.1:55300        *:*
  UDP    127.0.0.1:56299        *:*
  UDP    127.0.0.1:56478        *:*
  UDP    127.0.0.1:57198        *:*
  UDP    127.0.0.1:62102        *:*
  UDP    127.0.0.1:62158        *:*
  UDP    127.0.0.1:62159        *:*
  UDP    127.0.0.1:63856        *:*
  UDP    127.0.0.1:64852        *:*
  UDP    192.168.126.1:137      *:*
  UDP    192.168.126.1:138      *:*
  UDP    192.168.126.1:1900     *:*
  UDP    192.168.126.1:62100    *:*
  UDP    192.168.209.1:137      *:*
```



```
  UDP    192.168.126.1:62100    *:*
  UDP    192.168.209.1:137      *:*
  UDP    192.168.209.1:138      *:*
  UDP    192.168.209.1:1900     *:*
  UDP    192.168.209.1:62101    *:*
  UDP    [::]:123               *:*
  UDP    [::]:161               *:*
  UDP    [::]:500               *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:4500              *:*
  UDP    [::]:62161             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:62098            *:*

C:\Users\rkumar2>
```