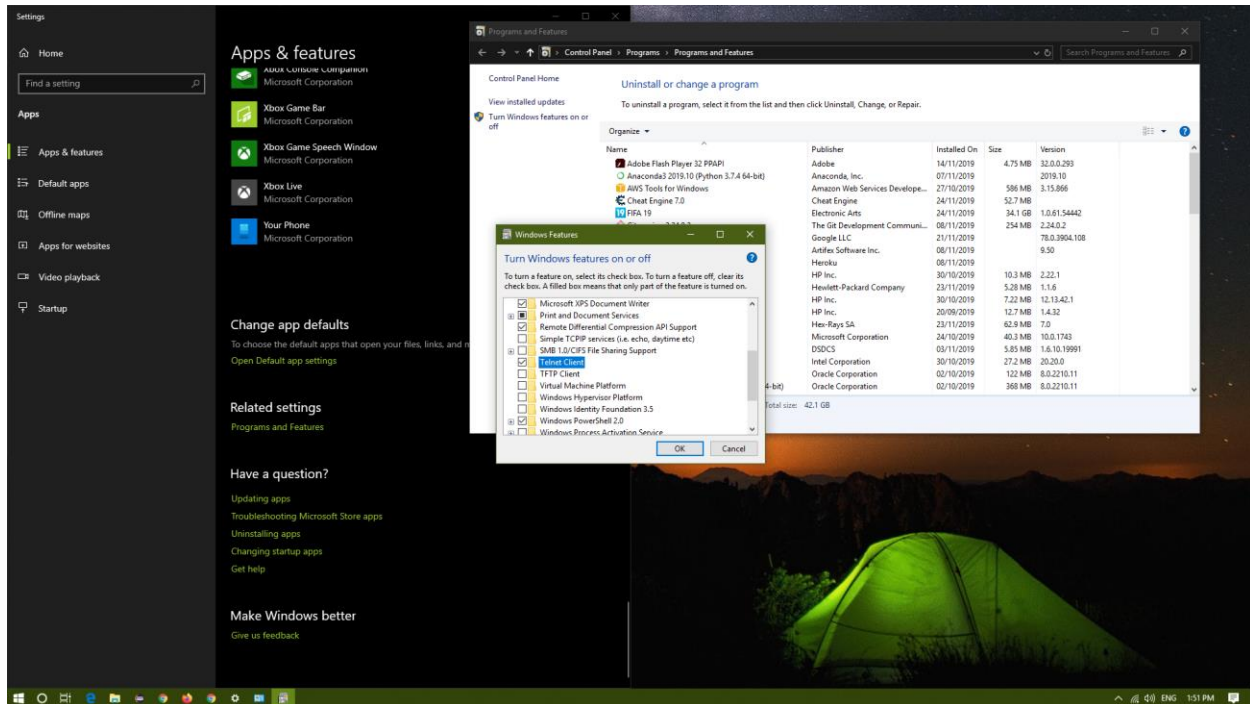


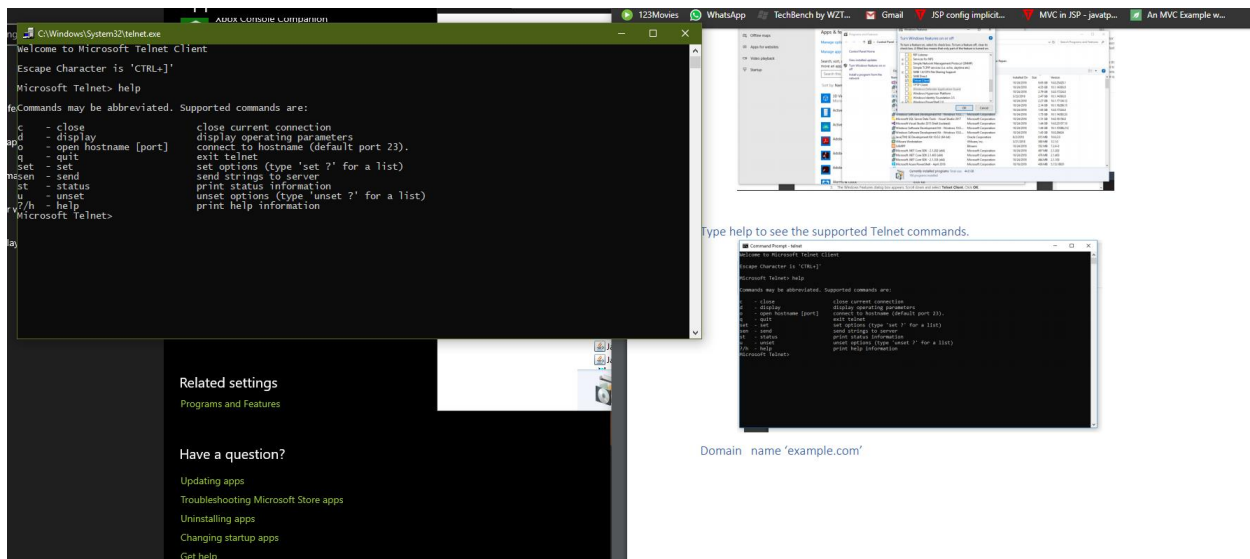
COMP 307 – Lab 07 – Supporting Info 1

Bashkar Sampath | 300987283

Select Telnet Client in Windows Features



Supported Telnet Commands



Domain: example.com

Zenmap

Scan Tools Profile Help

Target: example.com Profile: Intense scan [Scan] [Cancel]

Command: nmap -T4 -A -v example.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

example.com (93.184.216.34)

nmap -T4 -A -v example.com

Details

```

_ ECS (ord/573A)
|_ http-title: Example Domain
|_ ssl-cert: Subject: commonName=www.example.org/organizationName=Internet Corporation for Assigned Names
and Numbers/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:www.example.org, DNS:example.com, DNS:example.edu, DNS:example.net,
DNS:example.org, DNS:www.example.com, DNS:www.example.edu, DNS:www.example.net
| Issuer: commonName=DigiCert SHA2 Secure Server CA/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-11-28T00:00:00
| Not valid after: 2020-12-02T12:00:00
| MD5: 3510 c21c 66bd 6201 0fc5 47d3 cd3f 0ce6
|_ SHA-1: 7bb6 9838 6970 363d 2919 cc57 7284 6984 ffd4 a889
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|   h2
|_ http/1.1
|_ tls-nextprotoneg:
|   h2
|_ http/1.1
|_ http/1.0
1119/tcp closed bnetgame
1935/tcp closed rtmp
Device type: printer|general purpose|specialized
Running (JUST GUESSING): HP embedded (86%), OpenBSD 4.X (86%), FreeBSD 7.X (85%), Crestron 2-Series (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.3 cpe:/o:freebsd:freebsd:7.0 cpe:/o:crestron:2_series
Aggressive OS guesses: HP PSC 2400-series Photosmart printer (86%), OpenBSD 4.3 (86%), FreeBSD 7.0-STABLE
(85%), OpenBSD 4.0 (x86) (85%), Crestron XPanel control system (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.000 days (since Sun Dec 01 13:58:50 2019)
Network Distance: 11 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Randomized

TRACEROUTE (using port 1935/tcp)
HOP RTT ADDRESS
1 4.00 ms 192.168.1.1
2 7.00 ms 192.168.30.10
3 7.00 ms 204.197.191.165
4 8.00 ms 207.35.12.105
5 17.00 ms tcore1-torontotxn_be5.net.bell.ca (64.230.97.180)
6 29.00 ms tcore4-toronto12_bundle-ether22.net.bell.ca (64.230.51.157)
7 30.00 ms tcore4-chicagocp_hundredgige0-4-0-0.net.bell.ca (64.230.79.157)
8 19.00 ms bx6-chicagodt_0-6-0-0.net.bell.ca (64.230.79.85)
9 20.00 ms edgecast_chicago.net.bell.ca (184.150.181.53)
10 26.00 ms 192.229.225.133
11 19.00 ms 93.184.216.34

NSE: Script Post-scanning.
Initiating NSE at 13:58
Completed NSE at 13:58, 0.00s elapsed
Initiating NSE at 13:58
Completed NSE at 13:58, 0.00s elapsed
Initiating NSE at 13:58
Completed NSE at 13:58, 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 28.14 seconds
Raw packets sent: 2078 (94.820KB) | Rcvd: 69 (4.268KB)

```

Filter Hosts

Domain: 127.0.0.1

Zenmap

Scan Tools Profile Help

Target: 127.0.0.1 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 127.0.0.1

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

example.com (93.11) localhost (127.0.0.1)

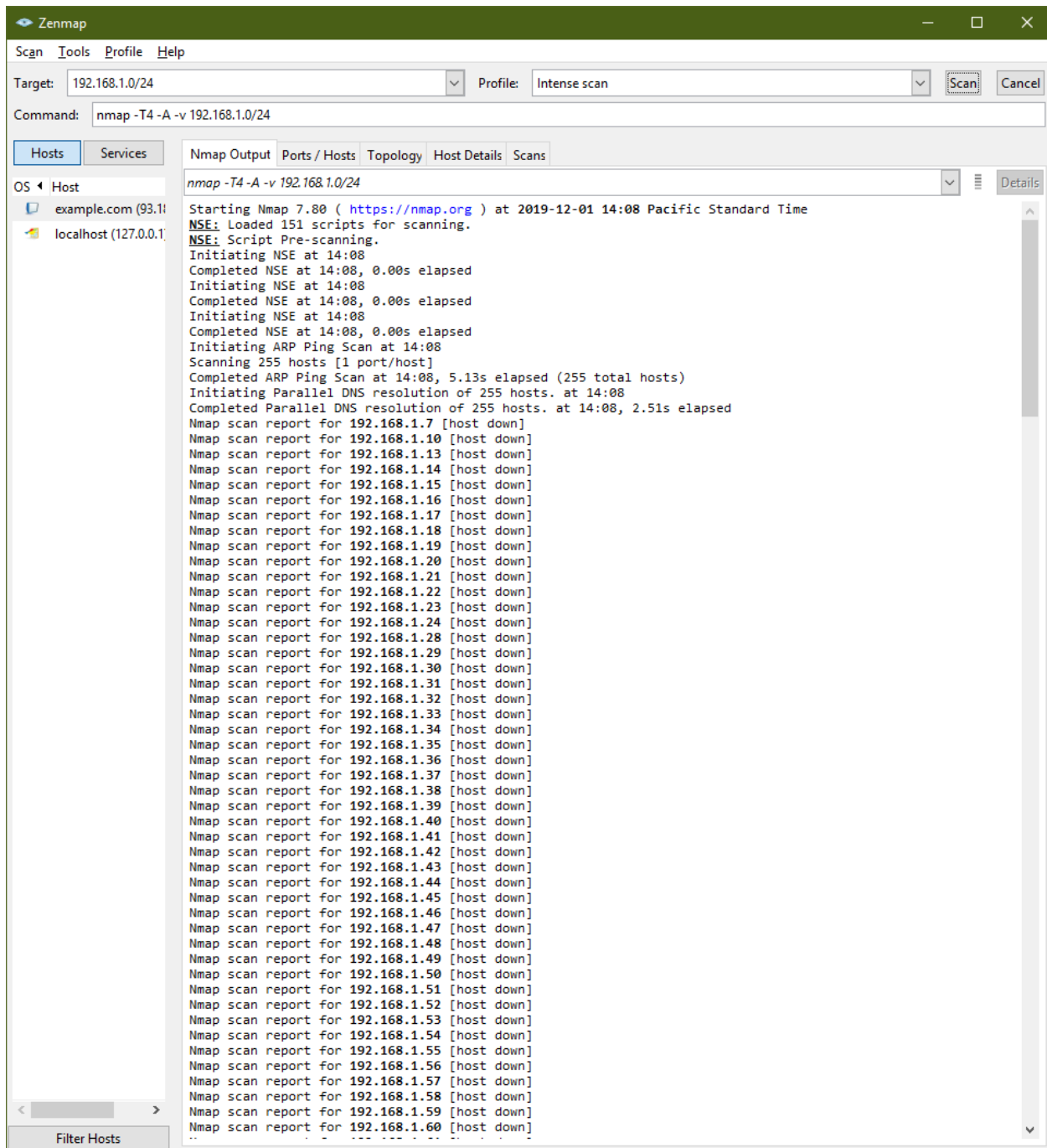
nmap -T4 -A -v 127.0.0.1

Starting Nmap 7.80 (<https://nmap.org>) at 2019-12-01 14:00 Pacific Standard Time
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:00
Completed NSE at 14:00, 0.00s elapsed
Initiating NSE at 14:00
Completed NSE at 14:00, 0.00s elapsed
Initiating NSE at 14:00
Completed NSE at 14:00, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 14:00
Completed Parallel DNS resolution of 1 host. at 14:00, 0.01s elapsed
Initiating SYN Stealth Scan at 14:00
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 5357/tcp on 127.0.0.1
Completed SYN Stealth Scan at 14:00, 0.10s elapsed (1000 total ports)
Initiating Service scan at 14:00
Scanning 3 services on localhost (127.0.0.1)
Completed Service scan at 14:00, 11.02s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against localhost (127.0.0.1)
Retrying OS detection (try #2) against localhost (127.0.0.1)
Retrying OS detection (try #3) against localhost (127.0.0.1)
Retrying OS detection (try #4) against localhost (127.0.0.1)
Retrying OS detection (try #5) against localhost (127.0.0.1)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 14:00
Completed NSE at 14:00, 30.07s elapsed
Initiating NSE at 14:00
Completed NSE at 14:00, 0.05s elapsed
Initiating NSE at 14:00
Completed NSE at 14:00, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000050s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=12/1%OT=135%CT=1%CU=31513%PV=N%DS=0%DC=L%G=Y%TM=5DE438
OS:17%P=i686-pc-windows-windows)SEQ(SP=FA%GCD=1%ISR=100%TI=I%CI=I%II=I%TS=U
OS:1)OPS(O1=MFFD7NW8NNS%O2=MFFD7NW8NNS%O3=MFFD7NW8%O4=MFFD7NW8NNS%O5=MFFD7NW
OS:8NNS%O6=MFFD7NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN
OS:(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=O
OS:AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80
OS:%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=O
OS:1)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=Z%A
OS:A=O%F=AR%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%
OS:DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=O
OS:80%CD=Z)

Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=250 (Good luck!)
IP ID Sequence Generation: Incrementing by 2
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

Domain: 192.168.1.0/24



Zenmap

Scan Tools Profile Help

Target: 192.168.1.0/24 Profile: Intense scan [Scan] [Cancel]

Command: nmap -T4 -A -v 192.168.1.0/24

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

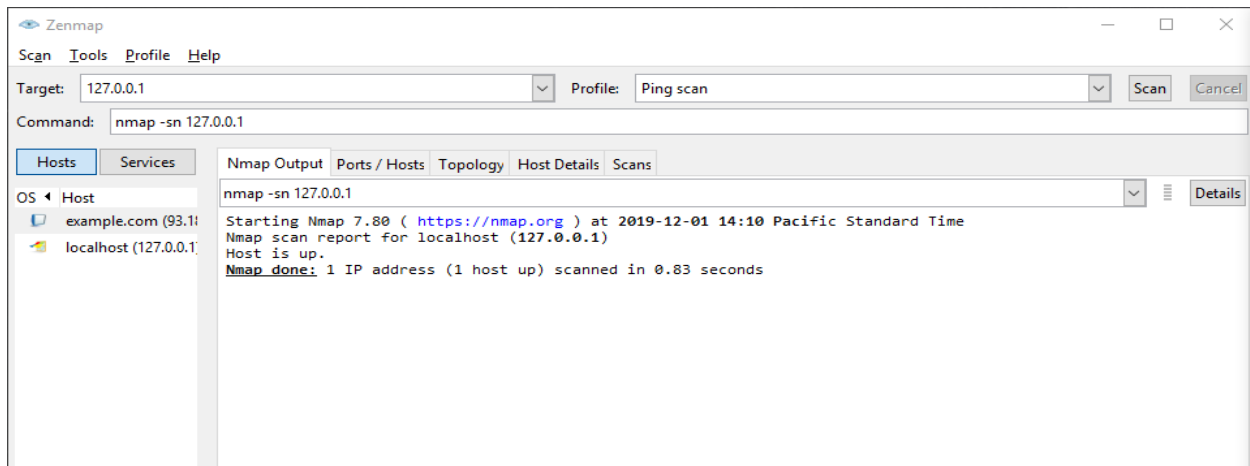
- example.com (93.111.111.111)
- localhost (127.0.0.1)

nmap -T4 -A -v 192.168.1.0/24

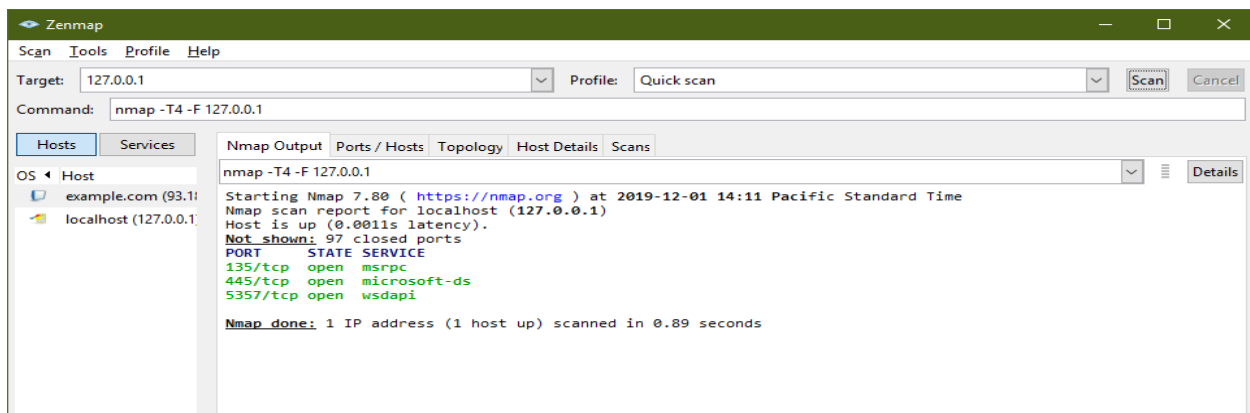
Starting Nmap 7.80 (<https://nmap.org>) at 2019-12-01 14:08 Pacific Standard Time
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:08
Completed NSE at 14:08, 0.00s elapsed
Initiating NSE at 14:08
Completed NSE at 14:08, 0.00s elapsed
Initiating NSE at 14:08
Completed NSE at 14:08, 0.00s elapsed
Initiating ARP Ping Scan at 14:08
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 14:08, 5.13s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 14:08
Completed Parallel DNS resolution of 255 hosts. at 14:08, 2.51s elapsed
Nmap scan report for 192.168.1.7 [host down]
Nmap scan report for 192.168.1.10 [host down]
Nmap scan report for 192.168.1.13 [host down]
Nmap scan report for 192.168.1.14 [host down]
Nmap scan report for 192.168.1.15 [host down]
Nmap scan report for 192.168.1.16 [host down]
Nmap scan report for 192.168.1.17 [host down]
Nmap scan report for 192.168.1.18 [host down]
Nmap scan report for 192.168.1.19 [host down]
Nmap scan report for 192.168.1.20 [host down]
Nmap scan report for 192.168.1.21 [host down]
Nmap scan report for 192.168.1.22 [host down]
Nmap scan report for 192.168.1.23 [host down]
Nmap scan report for 192.168.1.24 [host down]
Nmap scan report for 192.168.1.28 [host down]
Nmap scan report for 192.168.1.29 [host down]
Nmap scan report for 192.168.1.30 [host down]
Nmap scan report for 192.168.1.31 [host down]
Nmap scan report for 192.168.1.32 [host down]
Nmap scan report for 192.168.1.33 [host down]
Nmap scan report for 192.168.1.34 [host down]
Nmap scan report for 192.168.1.35 [host down]
Nmap scan report for 192.168.1.36 [host down]
Nmap scan report for 192.168.1.37 [host down]
Nmap scan report for 192.168.1.38 [host down]
Nmap scan report for 192.168.1.39 [host down]
Nmap scan report for 192.168.1.40 [host down]
Nmap scan report for 192.168.1.41 [host down]
Nmap scan report for 192.168.1.42 [host down]
Nmap scan report for 192.168.1.43 [host down]
Nmap scan report for 192.168.1.44 [host down]
Nmap scan report for 192.168.1.45 [host down]
Nmap scan report for 192.168.1.46 [host down]
Nmap scan report for 192.168.1.47 [host down]
Nmap scan report for 192.168.1.48 [host down]
Nmap scan report for 192.168.1.49 [host down]
Nmap scan report for 192.168.1.50 [host down]
Nmap scan report for 192.168.1.51 [host down]
Nmap scan report for 192.168.1.52 [host down]
Nmap scan report for 192.168.1.53 [host down]
Nmap scan report for 192.168.1.54 [host down]
Nmap scan report for 192.168.1.55 [host down]
Nmap scan report for 192.168.1.56 [host down]
Nmap scan report for 192.168.1.57 [host down]
Nmap scan report for 192.168.1.58 [host down]
Nmap scan report for 192.168.1.59 [host down]
Nmap scan report for 192.168.1.60 [host down]
..

Filter Hosts

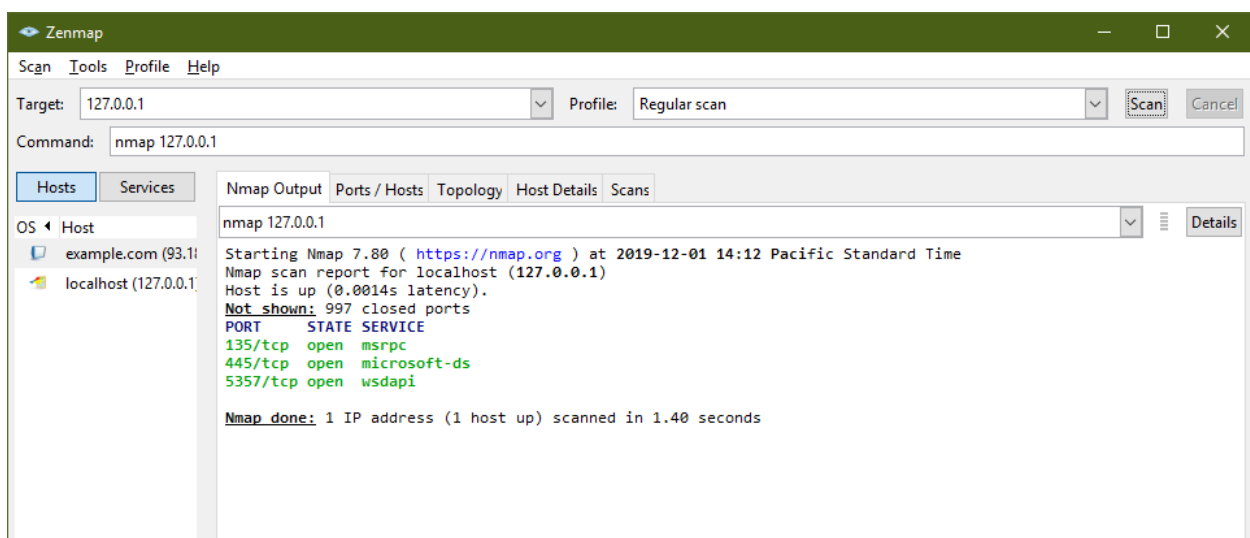
Domain: 127.0.0.1 Profile: Ping Scan



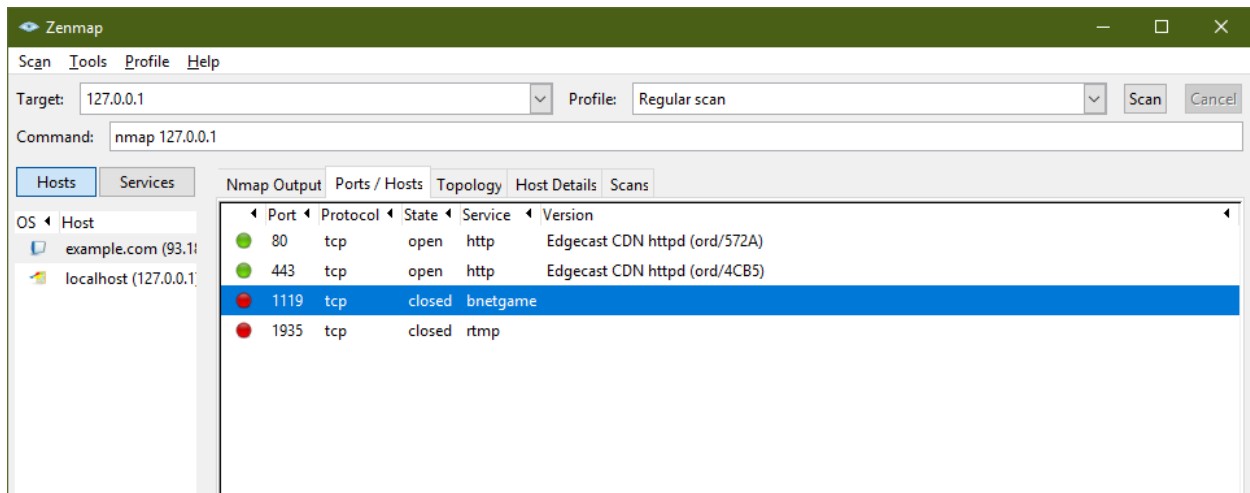
Domain: 127.0.0.1 Profile: Quick Scan



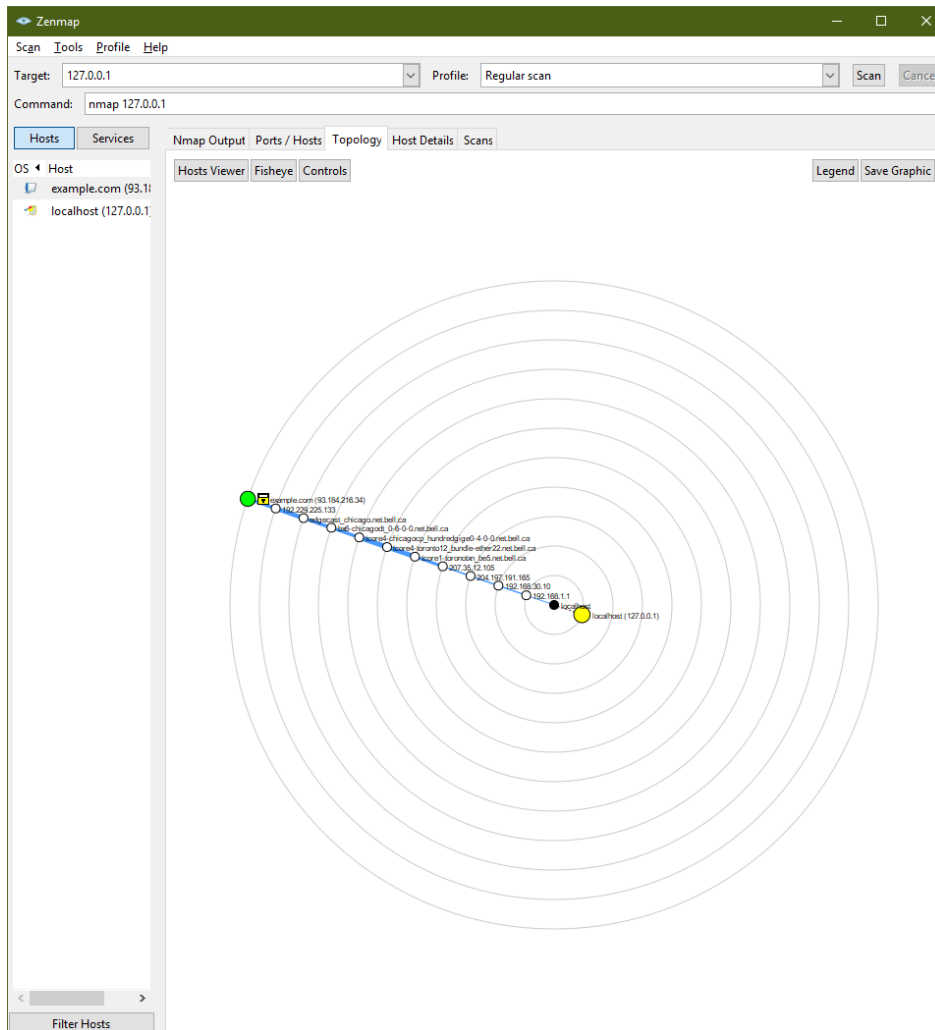
Domain: 127.0.0.1 Profile: Regular Scan



Ports/Host



Topology:



Host Details:

Zenmap

Scan Tools Profile Help

Target: 127.0.0.1 Profile: Regular scan Scan Cancel

Command: nmap 127.0.0.1

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

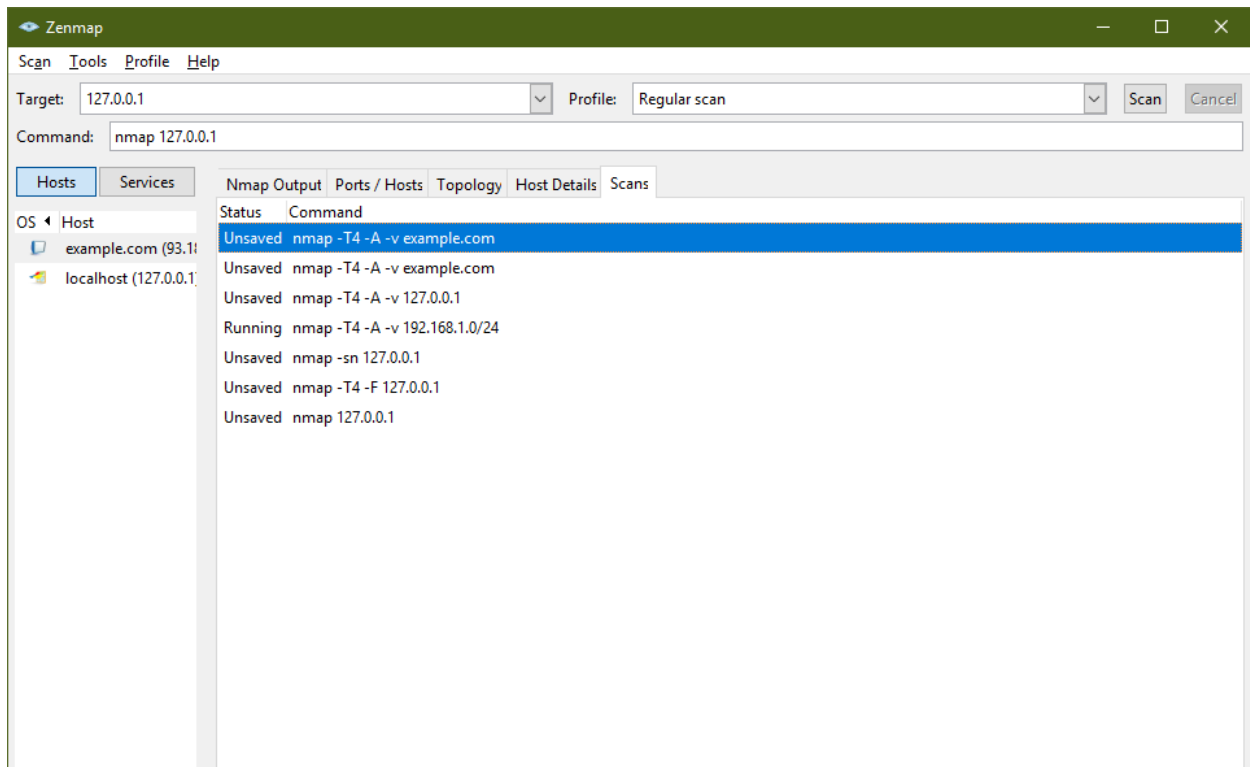
- example.com (93.184.216.34)
- localhost (127.0.0.1)

example.com (93.184.216.34)

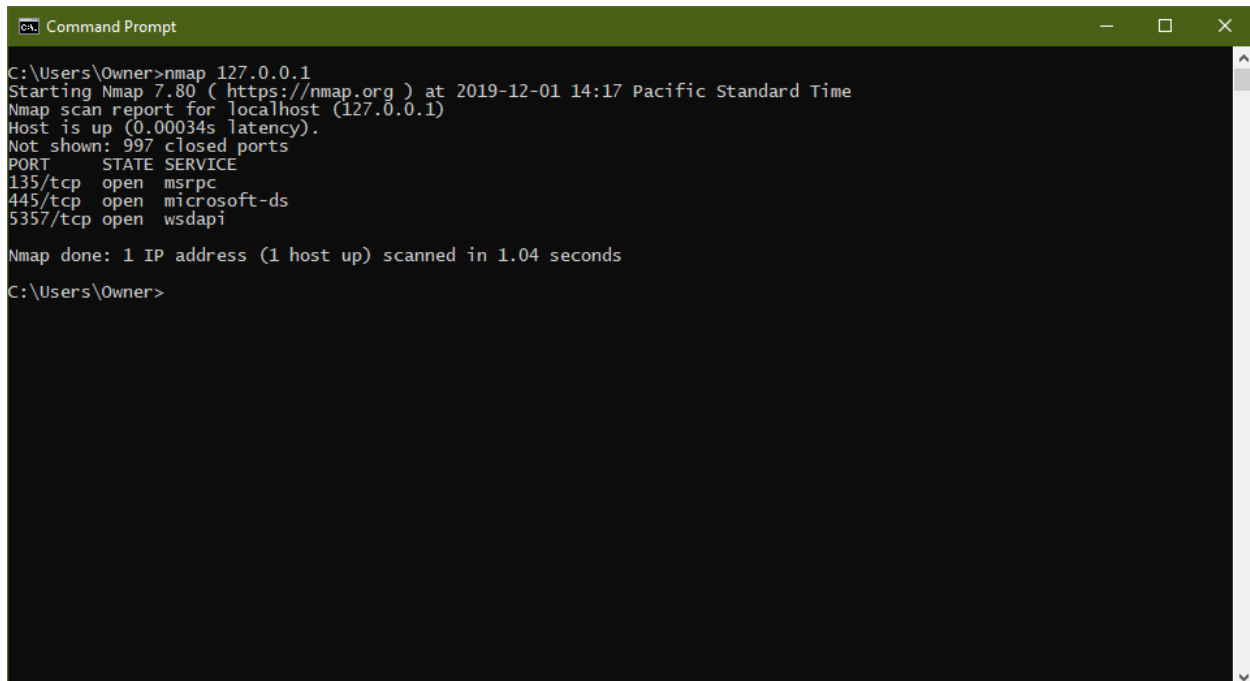
- Host Status**
 - State: up
 - Open ports: 2
 - Filtered ports: 996
 - Closed ports: 2
 - Scanned ports: 1000
 - Up time: 5
 - Last boot: Sun Dec 01 13:58:50 2019
- Addresses**
 - IPv4: 93.184.216.34
 - IPv6: Not available
 - MAC: Not available
- Hostnames**
 - Name - Type: example.com - user
- Operating System**
 - Name: HP PSC 2400-series Photosmart printer
 - Accuracy: 86%
- Ports used**
- OS Classes**
- TCP Sequence**
- IP ID Sequence**
- TCP TS Sequence**
- Comments**

Filter Hosts

Scans:



Scan of target's ports:



NMAP -sS 127.0.0.1

```
Command Prompt
C:\Users\Owner>nmap 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-01 14:17 Pacific Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00034s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
5357/tcp  open  wsapi

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds

C:\Users\Owner>nmap -sS 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-01 14:17 Pacific Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
5357/tcp  open  wsapi

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds

C:\Users\Owner>
```

NMAP -sn 127.0.0.1

```
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
5357/tcp  open  wsapi

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds

C:\Users\Owner>nmap -sn 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-01 14:18 Pacific Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.85 seconds

C:\Users\Owner>
```

NMAP -O 127.0.0.1

```
Command Prompt
C:\Users\Owner>nmap -O 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-01 14:20 Pacific Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000080s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=12/1%OT=135%CT=1%CU=31224%PV=N%DS=0%DC=L%G=Y%TM=5DE43C
OS:B1%P=i686-pc-windows-windows)SEQ(SP=103%GCD=1%ISR=10D%TI=I%CI=I%II=I%TS=
OS:U)OPS(O1=MFFD7NW8NNS%O2=MFFD7NW8NNS%O3=MFFD7NW8%O4=MFFD7NW8NNS%O5=MFFD7N
OS:W8NNS%O6=MFFD7NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)EC
OS:N(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+%F
OS:=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=8
OS:0%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A=0%F=R%O=%RD=0%Q
OS:=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A
OS:=0%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)U1(R=Y
OS:%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T
OS:=80%CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.86 seconds

C:\Users\Owner>
```

NMAP -A 127.0.0.1

```
Command Prompt
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Owner>nmap -A 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-01 14:23 Pacific Standard Time
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.51% done; ETC: 14:24 (0:00:00 remaining)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00040s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
445/tcp    open  microsoft-ds?
5357/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Aggressive OS guesses: Microsoft Windows Longhorn (93%), Microsoft Windows 10 1607 (92%), Microsoft Windows 10 1703 (91%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows 8.1 Update 1 (91%), Microsoft Windows Vista SP1 (91%), Microsoft Windows 10 1511 (90%), Microsoft Windows 7 Enterprise SP1 (90%), Microsoft Windows 7 SP1 (90%), Microsoft Windows 8 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2019-12-01T22:24:07
|_ start_date: N/A

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 58.43 seconds
```

NMAP -F 127.0.0.1

```
CA: Command Prompt

C:\Users\Owner>nmap -F 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-01 14:25 Pacific Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0016s latency).
Not shown: 97 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
5357/tcp  open  wsapi

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
C:\Users\Owner>
```

NMAP -v 127.0.0.1

```
CA: Command Prompt

C:\Users\Owner>nmap -v 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-01 14:26 Pacific Standard Time
Initiating Parallel DNS resolution of 1 host. at 14:26
Completed Parallel DNS resolution of 1 host. at 14:26, 0.01s elapsed
Initiating SYN Stealth Scan at 14:26
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 5357/tcp on 127.0.0.1
Completed SYN Stealth Scan at 14:26, 0.24s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0017s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
5357/tcp  open  wsapi

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 2003 (84.132KB)
C:\Users\Owner>
```

COMP 307 – Lab 07 – Supporting Info 2

Header information from web server centennialcollege.ca using telnet

```
Command Prompt
C:\Users\Owner>telnet centennialcollege.ca 80
```

```
Command Prompt

HTTP/1.1 400 Bad Request
Server: nginx
Date: Sun, 01 Dec 2019 19:38:44 GMT
Content-Type: text/html
Content-Length: 150
Connection: close

<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

Server – nginx

Scan using nmap

Intense Scan:

The screenshot shows the Zenmap application window. The 'Target' field is set to 'centennialcollege.ca' and the 'Profile' is set to 'Intense scan'. The 'Command' field displays 'nmap -T4 -A -v centennialcollege.ca'. The 'Hosts' tab is selected, showing a list of hosts including 'example.com (93.111.111.111)', 'localhost (127.0.0.1)', and several IP addresses in the 192.168.1.x range. The 'Nmap Output' tab is active, displaying the scan results for 'centennialcollege.ca (199.212.27.206)'. The output includes details about the NSE scripts, the SYN Stealth Scan, the Service Scan, and the OS detection. It also shows the results of the 'http' and 'ssl' scripts, including supported methods, titles, and certificates.

OS Host

- example.com (93.111.111.111)
- localhost (127.0.0.1)
- 192.168.1.1
- 192.168.1.3
- 192.168.1.4
- 192.168.1.5
- 192.168.1.8
- 192.168.1.9
- 192.168.1.11
- 192.168.1.12
- 192.168.1.25
- 192.168.1.26
- 192.168.1.27
- centennialcollege.ca

Nmap Output

nmap -T4 -A -v centennialcollege.ca

NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:42
Completed NSE at 14:42, 0.00s elapsed
Initiating NSE at 14:42
Completed NSE at 14:42, 0.00s elapsed
Initiating NSE at 14:42
Completed NSE at 14:42, 0.00s elapsed
Initiating Ping Scan at 14:42
Scanning centennialcollege.ca (199.212.27.206) [4 ports]
Completed Ping Scan at 14:42, 0.47s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:42
Completed Parallel DNS resolution of 1 host. at 14:42, 0.12s elapsed
Initiating SYN Stealth Scan at 14:42
Scanning centennialcollege.ca (199.212.27.206) [1000 ports]
Discovered open port 443/tcp on 199.212.27.206
Discovered open port 80/tcp on 199.212.27.206
Completed SYN Stealth Scan at 14:42, 4.92s elapsed (1000 total ports)
Initiating Service scan at 14:42
Scanning 2 services on centennialcollege.ca (199.212.27.206)
Completed Service scan at 14:42, 12.09s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against centennialcollege.ca (199.212.27.206)
Initiating Traceroute at 14:42
Completed Traceroute at 14:43, 3.03s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 14:43
Completed Parallel DNS resolution of 9 hosts. at 14:43, 0.09s elapsed
NSE: Script scanning 199.212.27.206.
Initiating NSE at 14:43
Completed NSE at 14:43, 2.86s elapsed
Initiating NSE at 14:43
Completed NSE at 14:43, 0.34s elapsed
Initiating NSE at 14:43
Completed NSE at 14:43, 0.00s elapsed
Nmap scan report for centennialcollege.ca (199.212.27.206)
Host is up (0.020s latency).
Other addresses for centennialcollege.ca (not scanned): 199.212.27.207
rDNS record for 199.212.27.206: www.centennialcollege.ca
Not shown: 998 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http nginx
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Did not follow redirect to https://www.centennialcollege.ca/
443/tcp open ssl/http nginx
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Did not follow redirect to https://www.centennialcollege.ca/
|_ ssl-cert: Subject: commonName=*.centennialcollege.ca/organizationName=Centennial College of Applied Arts and Technology/stateOrProvinceName=Ontario/countryName=CA
| Subject Alternative Name: DNS:*.centennialcollege.ca, DNS:centennialcollege.ca
| Issuer: commonName=DigiCert SHA2 High Assurance Server CA/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-11-23T00:00:00
| Not valid after: 2021-02-11T12:00:00
| MD5: c671 9d60 0fea 56ec 41a0 17f5 2369 bcab
|_ SHA-1: f01a a5bc 7223 876c 7f22 37e2 960c ee57 bc11 a3a3
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
| h2

Filter Hosts

Zenmap

Scan Tools Profile Help

Target: Profile:

Command:

Hosts Services

OS Host

- example.com (93.11)
- localhost (127.0.0.1)
- 192.168.1.1
- 192.168.1.3
- 192.168.1.4
- 192.168.1.5
- 192.168.1.8
- 192.168.1.9
- 192.168.1.11
- 192.168.1.12
- 192.168.1.25
- 192.168.1.26
- 192.168.1.27
- centennialcollege.ca

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v centennialcollege.ca

Details

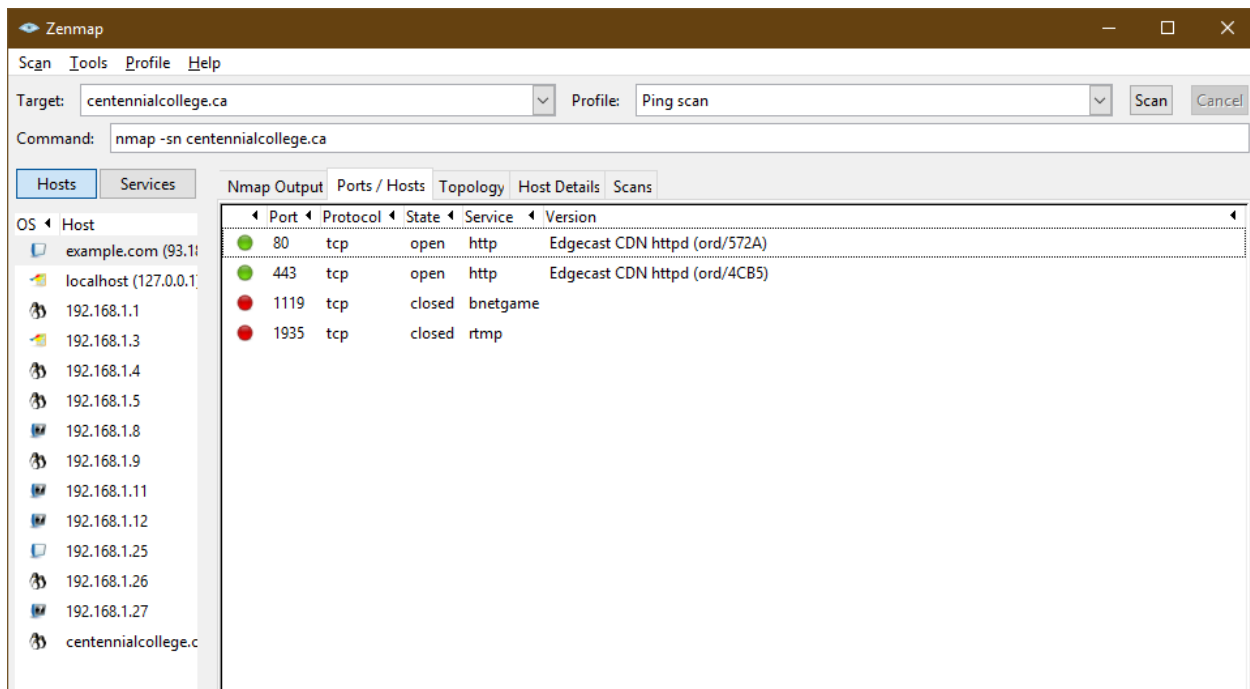
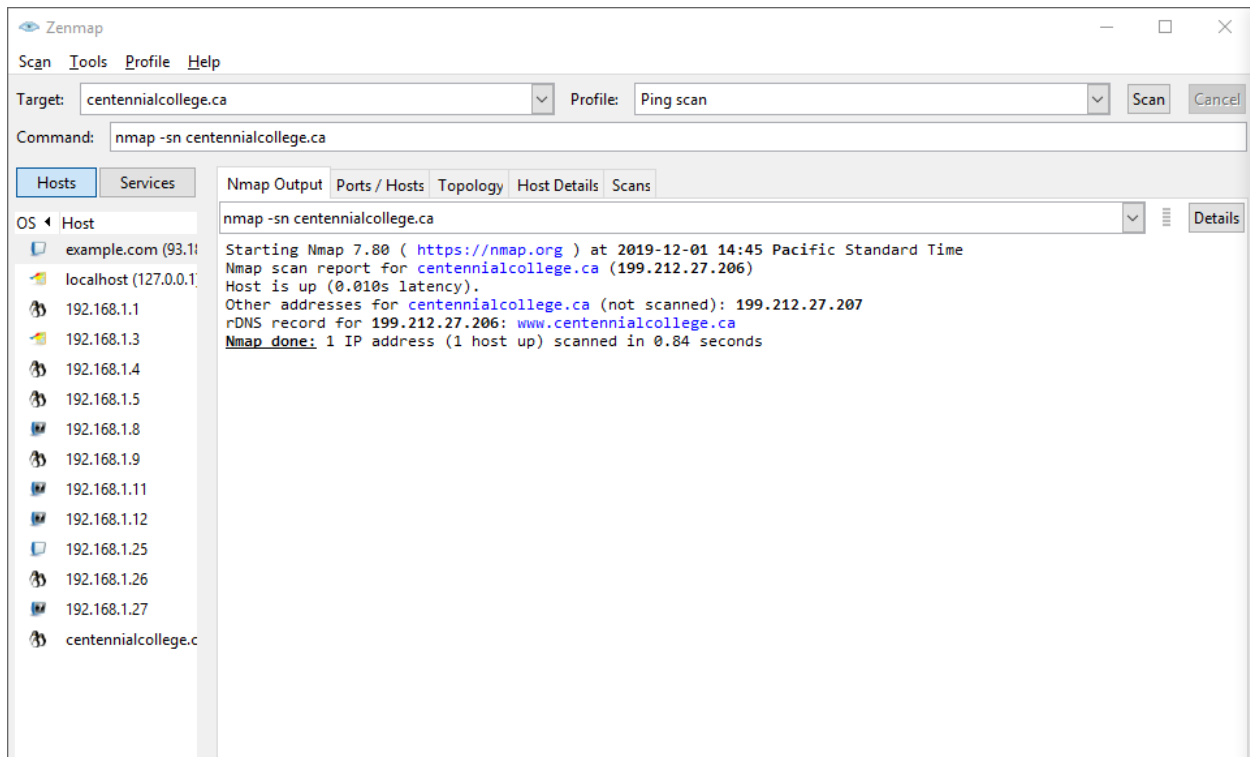
```
80/tcp open  http    nginx
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Did not follow redirect to https://www.centennialcollege.ca/
443/tcp open  ssl/http nginx
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Did not follow redirect to https://www.centennialcollege.ca/
|_ ssl-cert: Subject: commonName=*.centennialcollege.ca/organizationName=Centennial College of Applied Arts
and Technology/stateOrProvinceName=Ontario/countryName=CA
|_   Subject Alternative Name: DNS:*.centennialcollege.ca, DNS:centennialcollege.ca
|_   Issuer: commonName=DigiCert SHA2 High Assurance Server CA/organizationName=DigiCert Inc/countryName=US
|_   Public Key type: rsa
|_   Public Key bits: 2048
|_   Signature Algorithm: sha256WithRSAEncryption
|_   Not valid before: 2017-11-23T00:00:00
|_   Not valid after:  2021-02-11T12:00:00
|_   MD5:  c671 9d60 0fea 56ec 41a0 17f5 2369 bcab
|_   _SHA-1: f01a a5bc 7223 876c 7f22 37e2 960c ee57 bc11 a3a3
|_   _ssl-date: TLS randomness does not represent time
|_   tls-alpn:
|_     h2
|_     http/1.1
|_   _tls-nextprotoneg:
|_     h2
|_   _http/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4.9
OS details: Linux 3.10 - 3.16, Linux 4.9
Uptime guess: 27.708 days (since Sun Nov 03 21:43:15 2019)
Network Distance: 10 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

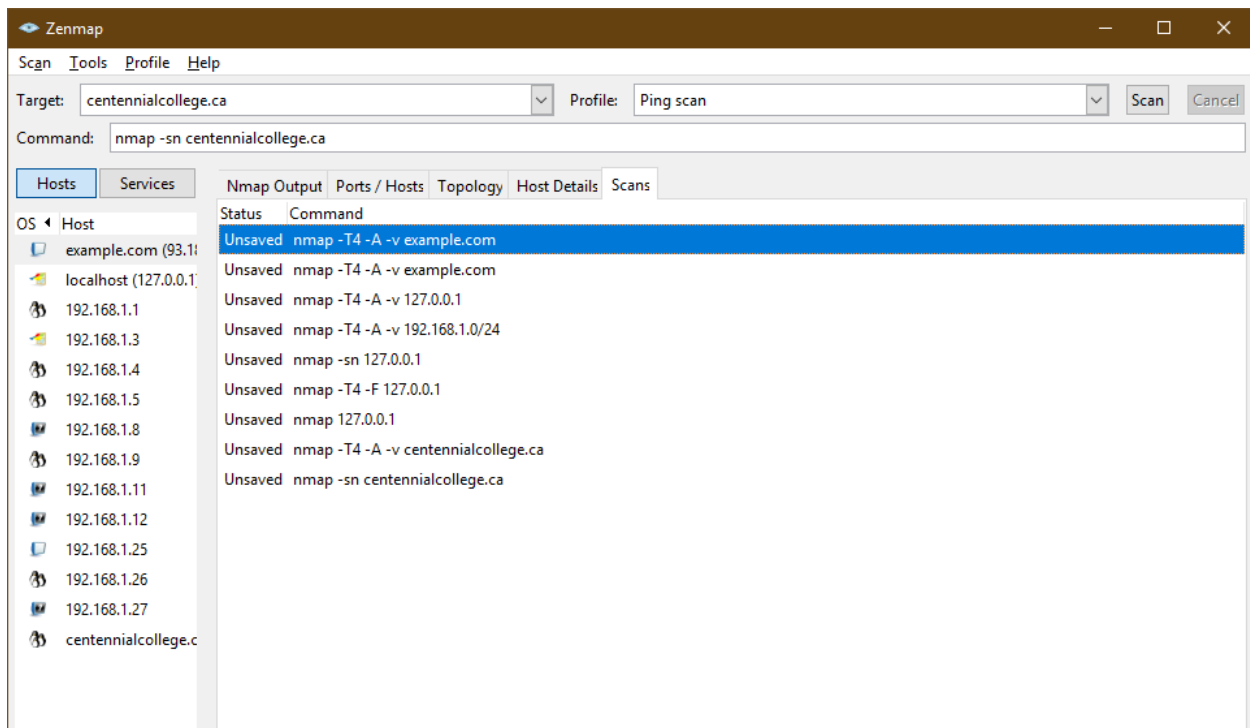
TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1  7.00 ms  192.168.1.1
2  16.00 ms 192.168.30.10
3  27.00 ms 204.197.191.165
4  28.00 ms te0-0-1-14.ccr31.yyz02.atlas.cogentco.com (38.104.158.9)
5  32.00 ms te0-0-2-0.rcr13.b011027-3.yyz02.atlas.cogentco.com (66.28.4.166)
6  35.00 ms 38.104.251.82
7  59.00 ms york-hub-ut-hub-100g-if.gtinet.ca (205.211.94.22)
8  69.00 ms cencol-york-hub-if-internet.gtinet.ca (205.211.95.142)
9  ...
10 82.00 ms www.centennialcollege.ca (199.212.27.206)

NSE: Script Post-scanning.
Initiating NSE at 14:43
Completed NSE at 14:43, 0.00s elapsed
Initiating NSE at 14:43
Completed NSE at 14:43, 0.00s elapsed
Initiating NSE at 14:43
Completed NSE at 14:43, 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 27.93 seconds
Raw packets sent: 2056 (92.606KB) | Rcvd: 49 (2.972KB)
```

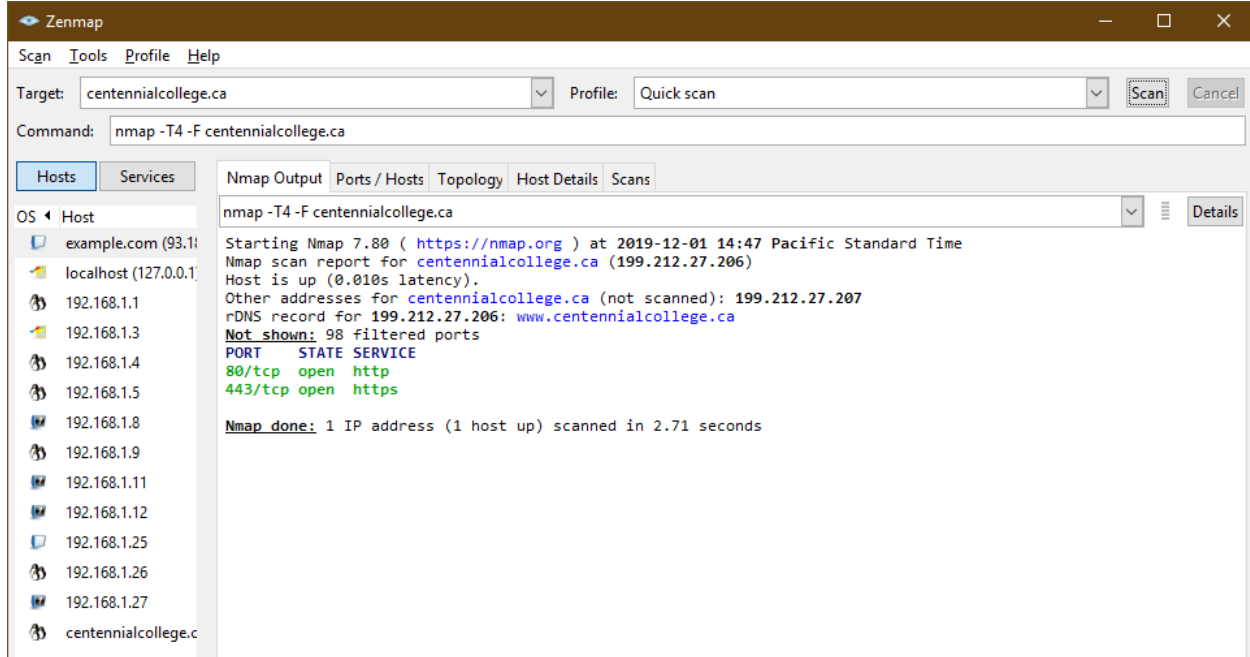
Filter Hosts

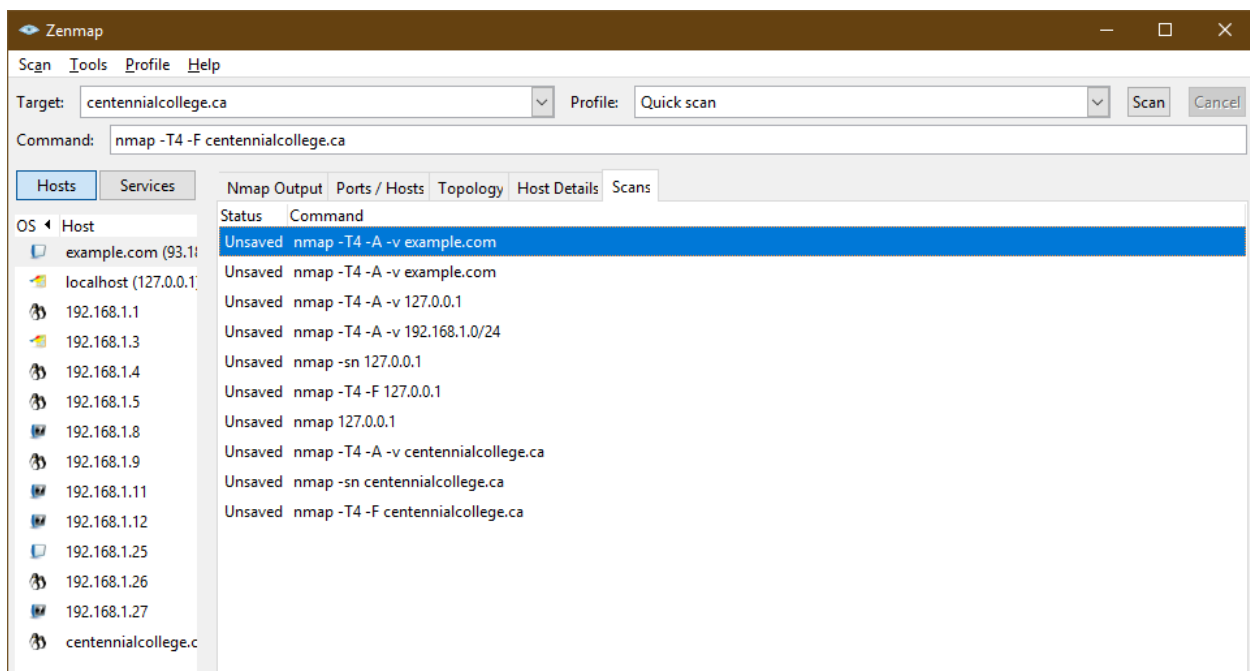
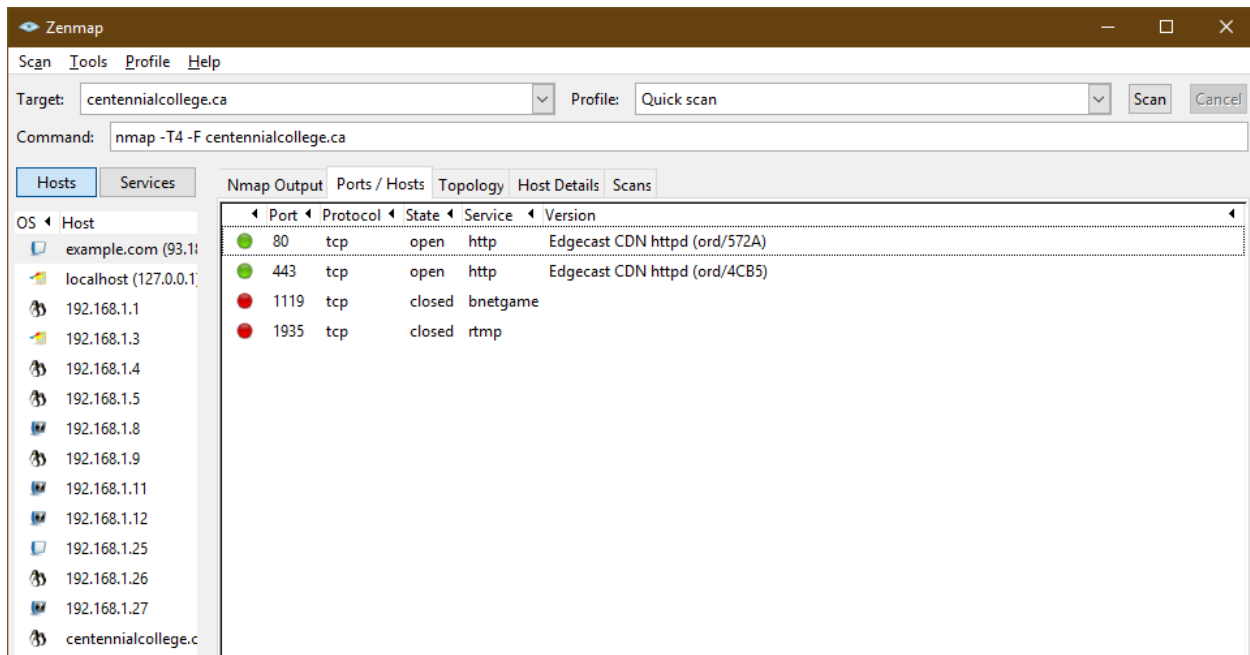
Ping scan:



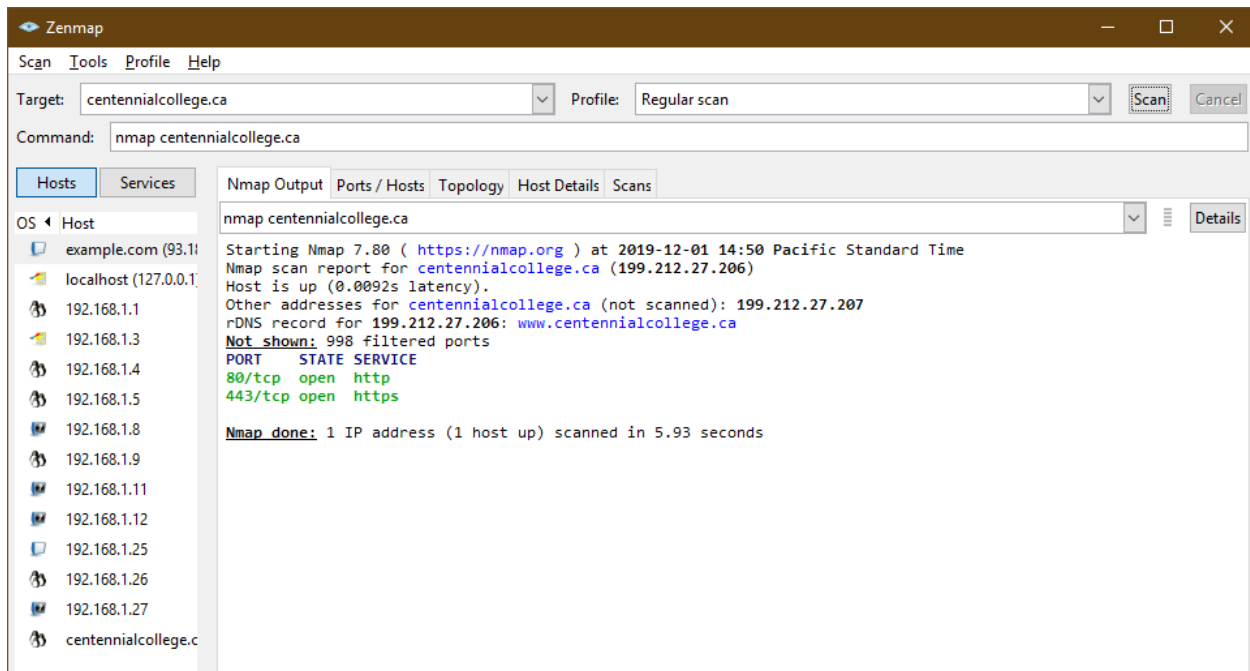


Quick Scan:





Regular Scan:



Zenmap interface showing a regular scan of `centennialcollege.ca`. The **Hosts** tab is selected, displaying a list of hosts. The **Nmap Output** tab is also selected, showing the scan results for `centennialcollege.ca`.

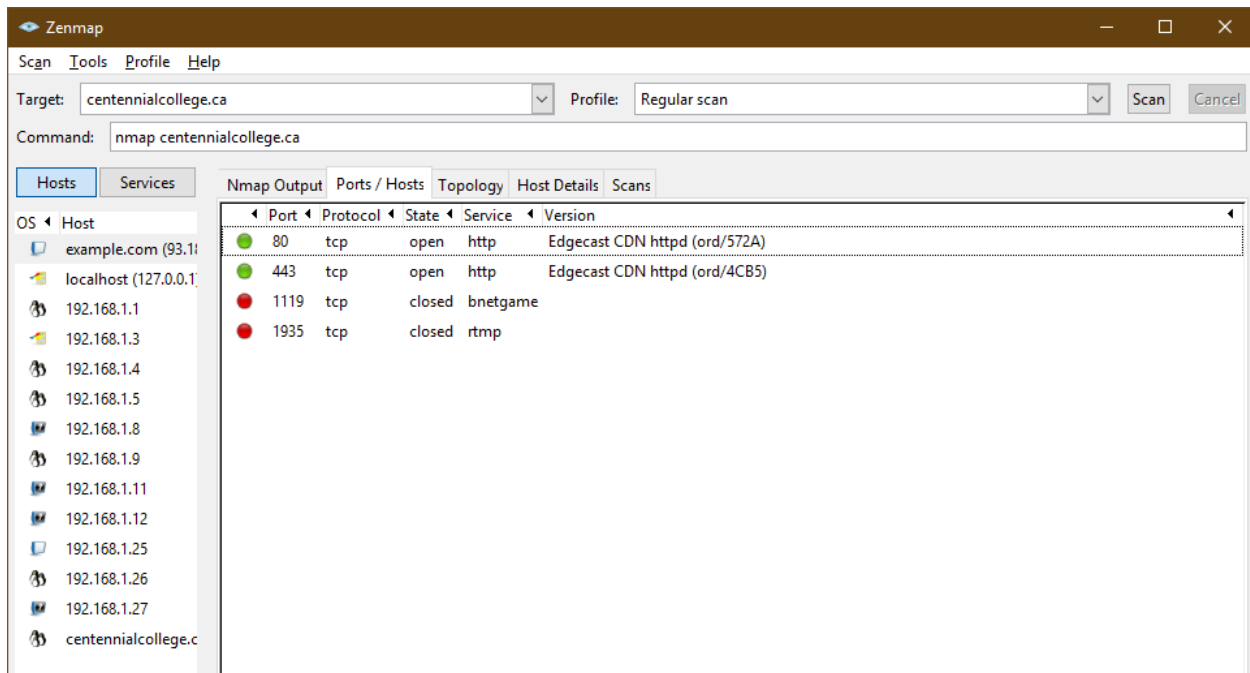
Target: `centennialcollege.ca` Profile: `Regular scan` Command: `nmap centennialcollege.ca`

Hosts:

- example.com (93.111.160.10)
- localhost (127.0.0.1)
- 192.168.1.1
- 192.168.1.3
- 192.168.1.4
- 192.168.1.5
- 192.168.1.8
- 192.168.1.9
- 192.168.1.11
- 192.168.1.12
- 192.168.1.25
- 192.168.1.26
- 192.168.1.27
- centennialcollege.ca (199.212.27.206)

Nmap Output:

```
nmap centennialcollege.ca
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-01 14:50 Pacific Standard Time
Nmap scan report for centennialcollege.ca (199.212.27.206)
Host is up (0.0092s latency).
Other addresses for centennialcollege.ca (not scanned): 199.212.27.207
rDNS record for 199.212.27.206: www.centennialcollege.ca
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
Nmap done: 1 IP address (1 host up) scanned in 5.93 seconds
```



Zenmap interface showing a regular scan of `centennialcollege.ca`. The **Hosts** tab is selected, displaying a list of hosts. The **Nmap Output** tab is also selected, showing the scan results for `centennialcollege.ca` in a table format.

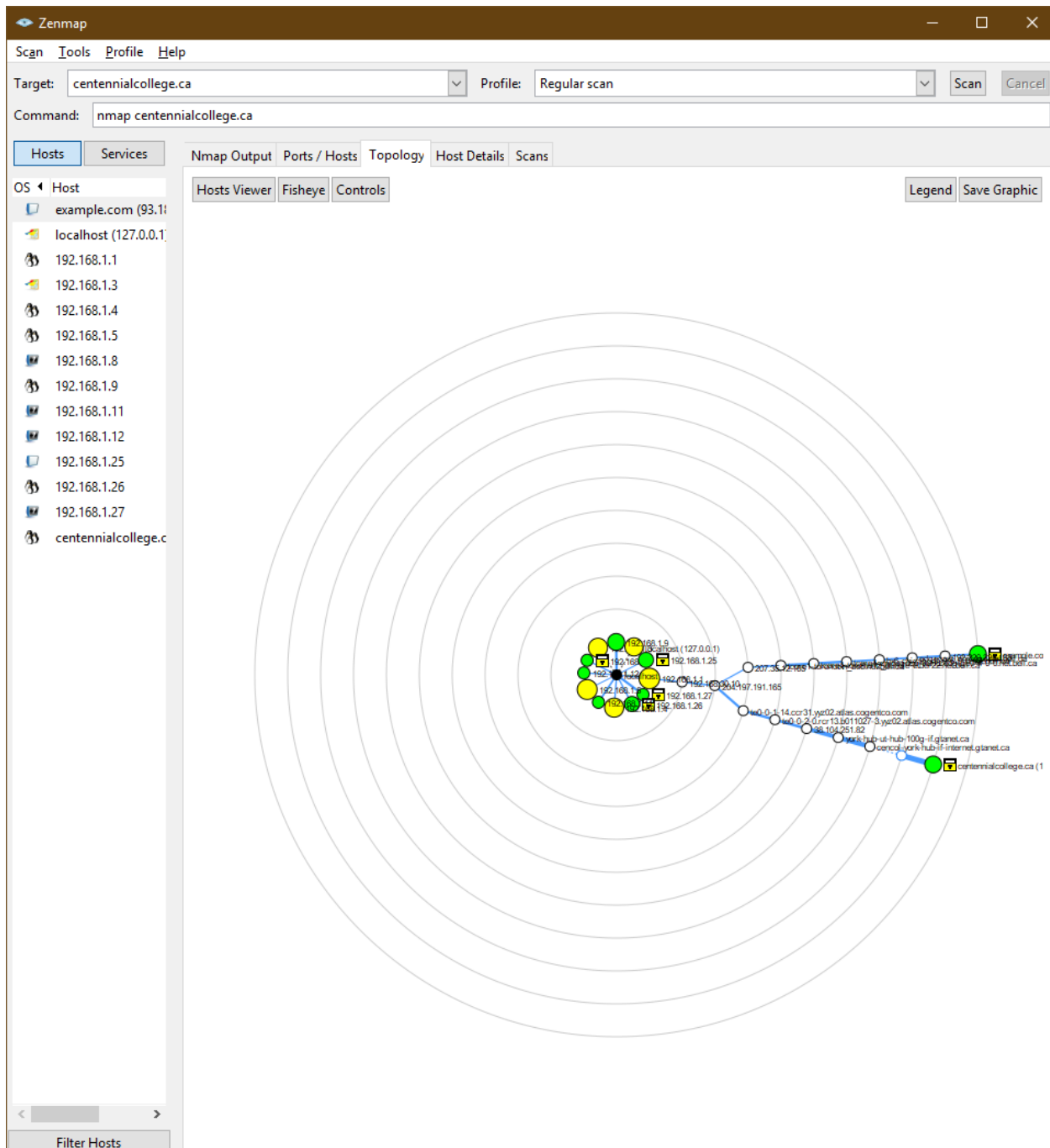
Target: `centennialcollege.ca` Profile: `Regular scan` Command: `nmap centennialcollege.ca`

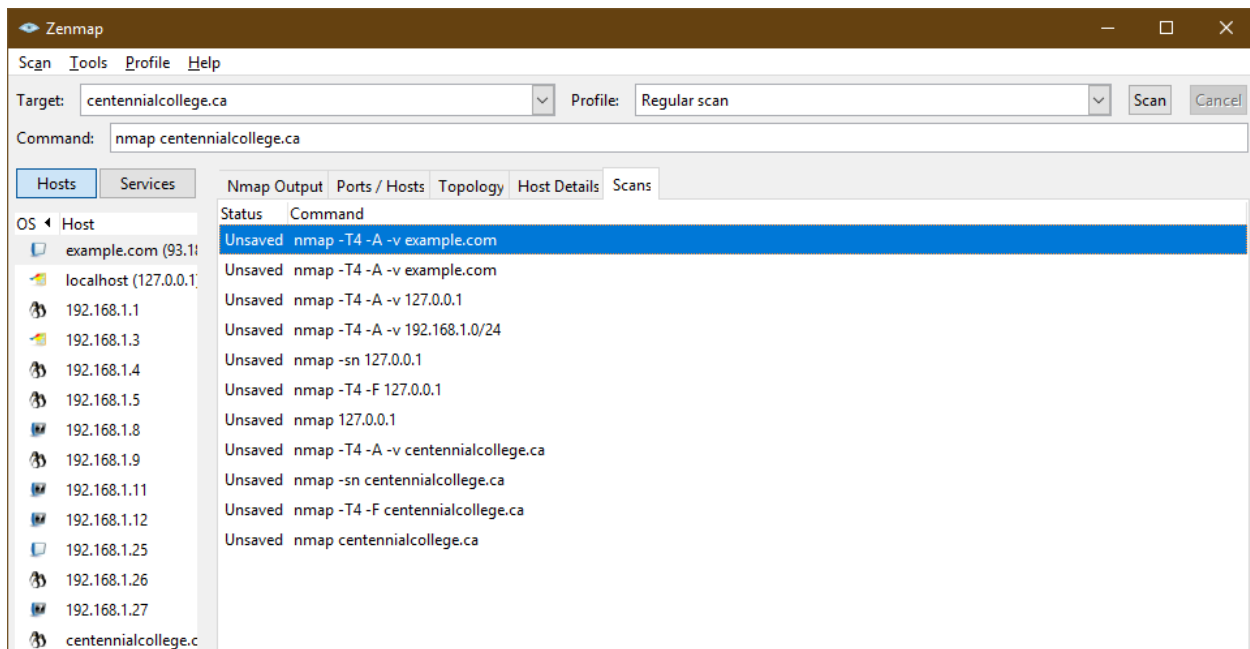
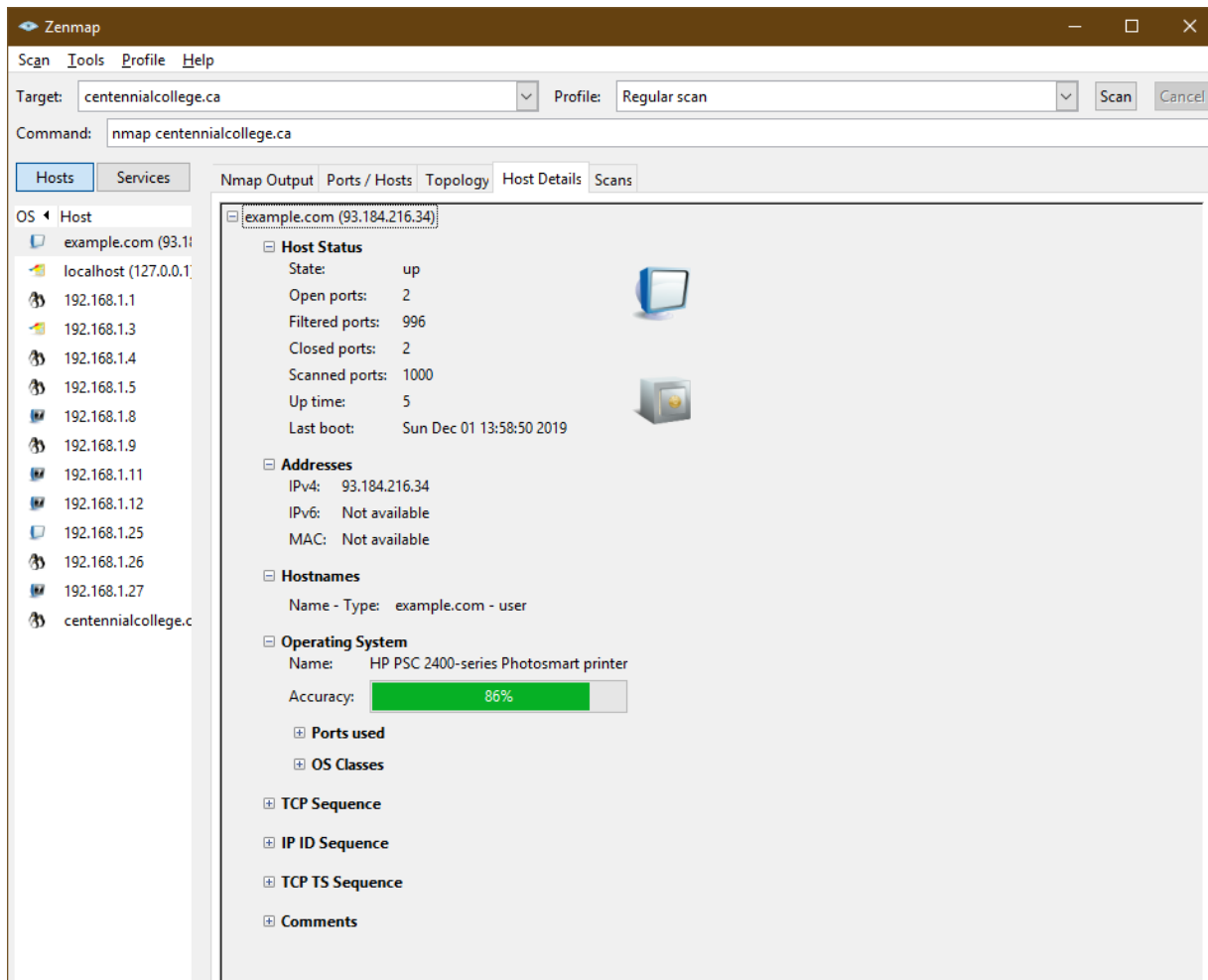
Hosts:

- example.com (93.111.160.10)
- localhost (127.0.0.1)
- 192.168.1.1
- 192.168.1.3
- 192.168.1.4
- 192.168.1.5
- 192.168.1.8
- 192.168.1.9
- 192.168.1.11
- 192.168.1.12
- 192.168.1.25
- 192.168.1.26
- 192.168.1.27
- centennialcollege.ca (199.212.27.206)

Nmap Output:

| Port | Protocol | State | Service | Version |
|------|----------|--------|----------|-------------------------------|
| 80 | tcp | open | http | Edgecast CDN httpd (ord/572A) |
| 443 | tcp | open | http | Edgecast CDN httpd (ord/4CB5) |
| 1119 | tcp | closed | bnetgame | |
| 1935 | tcp | closed | rtmp | |





Automatic fingerprinting - HttpRecon

httprecon 7.3 - http://centennialcollege.ca:80/

File Configuration Fingerprinting Reporting Help






















Target (Microsoft IIS 6.0)

http:// centennialcollege.ca : 80

GET existing GET long request GET non-existing GET wrong protocol HEAD existing OPTIONS con

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 01 Dec 2019 19:55:27 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Set-Cookie: wwwsrv=e7abc5bf3c2bd39fe9e816cddb8e5701; expires=Sun, 01-Dec-19 20:55:26 GMT; max-age=3600; domain=www.centennialcollege.ca; path=/
Cache-Control: private
Set-Cookie: centcont=CA; expires=Tue, 31-Dec-2019 19:55:26 GMT; path=/
Set-Cookie: BannerHomeCookieCount=2; path=/
Set-Cookie: BannerHomeCookieCurrentIndex=0; path=/
Access-Control-Allow-Origin: *
Strict-Transport-Security: max-age=63072000; includeSubdomains;
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Backend-Server: 2
```

Matchlist (352 Implementations) Fingerprint Details Report Preview

| Name | Hits | Match % |
|--------------------------------------------------------------------------------------------------------------------|------|----------|
|  Sun ONE Web Server 6.1 | 36 | 81.81... |
|  Zeus 4.3 | 36 | 81.81... |
|  Apache 2.0.54 | 35 | 79.54... |
|  Apache 2.2.2 | 35 | 79.54... |
|  Sun Java System Web Server 7.0 | 35 | 79.54... |
|  Apache 2.0.55 | 34 | 77.27... |
|  Apache 2.2.4 | 34 | 77.27... |
|  Cherokee 0.6.0 | 34 | 77.27... |
|  Hiawatha 6.2 | 34 | 77.27... |
|  Apache 2.0.45 | 33 | 75 |
|  Mongrel 1.0 | 33 | 75 |
|  nginx 0.5.19 | 33 | 75 |
|  nginx 0.5.30 | 33 | 75 |
|  nginx 0.5.32 | 33 | 75 |
|  nginx 0.6.13 | 33 | 75 |
|  Zope 2.8.4 | 33 | 75 |
|  Zope 2.8.6 | 33 | 75 |
|  Zope 2.9.6 | 33 | 75 |
|  and-httpd 0.99.11 | 32 | 72.72... |
|  Apache 1.3.34 | 32 | 72.72... |
|  Apache 2.2.11 | 32 | 72.72... |
| nginx 0.5.35 | 32 | 72.72... |
| nginx 0.5.16 | 32 | 72.72... |

Ready

Automatic Fingerprinting - Netcraft


LAB 7-Supporting_Info_2 - 19f

Site report for www.centennialcollege.ca

Free Software Downloads and S...

toolbarnetcraft.com/site_report?url=https://www.centennialcollege.ca

123Movies WhatsApp TechBench by WZT... Gmail JSP config implic... MVC in JSP - jstnp... An MVC Example w... Handling HTML for... software risk mana... GitHub - casuvm... IPA tutorial: Mappl... IPA CRUD example... Configuring Eclipse...



Site report for www.centennialcollege.ca

Search

Netcraft Extension

Home

Download Now!

Report a Phish

Site Report

Top Reporters

Incentives for reporters

Phishiest TLDs

Phishiest Countries

Phishiest Hosters

Phishiest Certificate Authorities

Phishing Map

Takedown Map

Most Popular Websites

Branded Extensions

Tell a Friend

Phishing & Fraud

Phishing Site Feed

Hosting Phishing Alerts

SSL CA Phishing Alerts

Protection for TLDs against Phishing and Malware

Deceptive Domain Score

Bank Fraud Detection

Phishing Site Countermeasures

Extension Support

FAQ

Glossary






Contact Us

Report a Bug

Tutorials

Installing the Extension











Lookup another URL:
Enter a URL here

Share:     

Background

| | | | |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-------------|
| Site title | Centennial College Community Colleges in Toronto, Canada | Date first seen | August 2000 |
| Site rank | 103100 | Primary language | English |
| Description | Centennial College (342)200(223 Toronto)342(200)231s first Community College offers Degree Programs in Business, Communication, Engineering Technology, Health Community courses.. | | |
| Keywords | community college, community colleges, continuing education, college degrees, college courses, degree programs, college course, college programs, Canadian college, distance learning, college education, continuing education college, community college degree, Toronto college, Toronto education, Toronto degree, Toronto, Canada | | |
| Netcraft Risk Rating [FAQ] | 0/10 <div></div> | | |

Network

| Site | https://www.centennialcollege.ca | | | Netblock Owner | Centennial College | | | | | | | | | | | | | | | | | | | | |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------------------------------------|-------------------------|-------------------------------|----------|---------|------|-------------|-------------------------|-----|----------|------------------------------|-----------------------------|-------------------------------------------------------------------------------------------------|--------|----------------------------------------|-------------------------------|------------------------------------------------------------------------------------------|------------|--------------------|------------------|------------------------------------------------------------------------------------------|------------|--------------------|
| Domain | centennialcollege.ca | | | Nameserver | ns1.centennialcollege.ca | | | | | | | | | | | | | | | | | | | | |
| IP address | 199.212.27.206 (view full) | | | DNS admin | dnsadmin@centennialcollege.ca | | | | | | | | | | | | | | | | | | | | |
| IPv6 address | Not Present | | | Reverse DNS | www.centennialcollege.ca | | | | | | | | | | | | | | | | | | | | |
| Domain registrar | cira.ca | | | Nameserver organisation | whols.cira.ca | | | | | | | | | | | | | | | | | | | | |
| Organisation | unknown | | | Hosting company | centennialcollege.ca | | | | | | | | | | | | | | | | | | | | |
| Top Level Domain | Canada (.ca) | | | DNS Security Extensions | unknown | | | | | | | | | | | | | | | | | | | | |
| Hosting country |  CA | | | | | | | | | | | | | | | | | | | | | | | | |
| IP delegation | <div>IPv4 address (199.212.27.206)</div> <table><thead><tr><th>IP range</th><th>Country</th><th>Name</th><th>Description</th></tr></thead><tbody><tr><td>0.0.0.0-255.255.255.255</td><td>N/A</td><td>IANA-BLK</td><td>The whole IPv4 address space</td></tr><tr><td>~ 199.0.0.0-199.255.255.255</td><td> United States</td><td>NET199</td><td>American Registry for Internet Numbers</td></tr><tr><td>~ 199.212.26.0-199.212.27.255</td><td> Canada</td><td>IDC-CENCOL</td><td>Centennial College</td></tr><tr><td>~ 199.212.27.206</td><td> Canada</td><td>IDC-CENCOL</td><td>Centennial College</td></tr></tbody></table> | | | | | IP range | Country | Name | Description | 0.0.0.0-255.255.255.255 | N/A | IANA-BLK | The whole IPv4 address space | ~ 199.0.0.0-199.255.255.255 |  United States | NET199 | American Registry for Internet Numbers | ~ 199.212.26.0-199.212.27.255 |  Canada | IDC-CENCOL | Centennial College | ~ 199.212.27.206 |  Canada | IDC-CENCOL | Centennial College |
| IP range | Country | Name | Description | | | | | | | | | | | | | | | | | | | | | | |
| 0.0.0.0-255.255.255.255 | N/A | IANA-BLK | The whole IPv4 address space | | | | | | | | | | | | | | | | | | | | | | |
| ~ 199.0.0.0-199.255.255.255 |  United States | NET199 | American Registry for Internet Numbers | | | | | | | | | | | | | | | | | | | | | | |
| ~ 199.212.26.0-199.212.27.255 |  Canada | IDC-CENCOL | Centennial College | | | | | | | | | | | | | | | | | | | | | | |
| ~ 199.212.27.206 |  Canada | IDC-CENCOL | Centennial College | | | | | | | | | | | | | | | | | | | | | | |

SSL/TLS

| | |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| SSLv3/POODLE | This site does not support the SSL version 3 protocol. More information about SSL version 3 and the POODLE vulnerability. |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------|

| Certificate transparency | Signed Certificate Timestamps (SCTs) | | | |
|------------------------------------|--------------------------------------|-----|-----------|------------------------|
| | Source | Log | Timestamp | Signature Verification |
| No SCTs received or issuer unknown | | | | |

SSL Certificate Chain

| | | | |
|--------------|------------------------------------|---------------------|-------------------------------|
| Common name | DigiCert High Assurance EV Root CA | Organisational unit | www.digicert.com |
| Organisation | DigiCert Inc | Validity period | From 2006-11-10 to 2031-11-10 |



| | | | |
|--------------|----------------------------------------|---------------------|-------------------------------|
| Common name | DigiCert SHA2 High Assurance Server CA | Organisational unit | www.digicert.com |
| Organisation | DigiCert Inc | Validity period | From 2013-10-22 to 2028-10-22 |

Hosting History

| Netblock owner | IP address | OS |
|------------------------------------------------------------------|----------------|---------------------|
| Centennial College 941 Progress Avenue Scarborough ON CA M1K-5E9 | 199.212.27.207 | Linux |
| Centennial College 941 Progress Avenue Scarborough ON CA M1K-5E9 | 199.212.27.206 | Linux |
| Centennial College 941 Progress Avenue Scarborough ON CA M1K-5E9 | 199.212.27.207 | Linux |
| Centennial College 941 Progress Avenue Scarborough ON CA M1K-5E9 | 199.212.27.206 | Linux |
| Centennial College 941 Progress Avenue Scarborough ON CA M1K-5E9 | 199.212.60.207 | Windows Server 2008 |

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of [rules](#). Each rule consists of a qualifier for this qualifier to. For more information please see [openspf.org](#).

Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be method to set policy and to give reporting of failures. For more information please see [dmarc.org](#).

This host does not have a DMARC record.

Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individuals from these trackers are primarily used for advertising or analytics purposes.

4 known trackers were identified.

Companies



Categories

