# Penetration Testing Rules Of Engagement

## Team Primary Contact

Primary Contact: John Doe

Mobile Phone: 123-456-7890

Pager: 987-654-3210

## Team Secondary Contact

Secondary Contact: Jane Smith

Secondary Phone: 098-765-4321

Secondary Pager: 654-321-0987

## Target Primary Contact

Target Primary Contact: Alice Johnson

Target Phone: 555-123-4567

Target Pager: 555-765-4321

## Target Secondary Contact

Target Secondary Contact: Bob Brown

Target Secondary Phone: 555-987-6543

Target Secondary Pager: 555-345-6789

## Debriefing Information

Debrief Frequency: Daily

Debrief Location: Conference Room A

## Test Dates and Times

Start Date: 2024-10-01

End Date: 2024-10-05

Test Times: 9 AM to 5 PM

## Testing Parameters

Announced Test: yes

Shun IP: no

Automatic Shun: None

Shun Steps: Notify IT

## Test Continuation Information

Conclude Test: no

Continue Test: Use backup systems

## Attack and Policy Information

Attack IPs: 192.168.1.100, 192.168.1.101

Black Box: yes

Viewing Policy: Only if necessary

Observing Team: yes

## Signature Information

Target Signature:

Target Date: 2024-10-01

Pen Test Leader Signature:

Leader Date: 2024-10-01

Tester Signatures:

Team Member 1, Team Member 2

# Passive Reconnaissance Scanning Result

NSLOOKUP SCANNING RESULT
TARGET DOMAIN: saskpolytech.ca

---------- A ----------
A: 142.99.246.34
---

---------- NS ----------
NS: azuredns1.
NS: ns2.d-zone.ca.
NS: ns1.d-zone.ca.
---

---------- CNAME ----------
Reason: The DNS response does not contain an answer to the question: saskpolytech.ca. IN CNAME
---

---------- AAAA ----------
Reason: The DNS response does not contain an answer to the question: saskpolytech.ca. IN AAAA
---

---------- MX ----------
MX: 5 saskpolytech-ca.mail.protection.outlook.com.
---

---------- SOA ----------
SOA: azuredns1. hostmaster. 1305 900 600 2592000 3600
---

---------- PTR ----------
Reason: The DNS response does not contain an answer to the question: saskpolytech.ca. IN PTR
---

---------- TXT ----------
TXT: "ms-domain-verification=5335518d-4ff5-443f-a119-491b29927a13"
TXT: "v=spf1 ip4:174.90.127.252 ip4:142.99.240.232 ip4:108.63.20.35 ip4:206.191.49.128/25 "
"ip4:209.217.89.253 ip4:74.91.86.65 ip4:199.244.78.221/24 ip4:74.91.86.73 ip4:74.91.86.77
ip4:52.31.29.196 " "ip4:205.139.105.50/24 ip4:172.21.8.6 ip4:162.244.239.26/27 ip4:216.243.142.142
ip4:142.3.152.69 ip4:142.3.100.254 " "ip4:206.191.23.156 ip4:54.240.37.1 ip4:56.60.142.64
ip4:184.173.105.143 ip4:216.146.32.161 ip4:216.146.32.188 " "ip4:216.146.32.187 ip4:216.146.32.186
ip4:216.146.32.185 ip4:81.93.173.201 ip4:81.93.164.103 ip4:192.68.72.46 " "ip4:192.68.72.47
ip4:161.47.143.129 ip4:161.47.143.131 ip4:161.47.143.133 ip4:192.190.92.0/23 ip4:198.97.238.0/23 "
"ip4:204.239.0.0/24 ip4:198.207.147.224/27 ip4:204.239.0.224/27 ip4:166.78.70.104 ip4:198.61.255.245 "
"ip4:198.61.255.238 ip4:52.60.142.64 ip4:69.167.138.236 ip4:205.201.128.0/20 ip4:148.105.8.0/21 "
"ip4:149.96.5.7 ip4:199.91.140.28 ip4:149.96.6.6 ip4:149.96.6.3 ip4:149.96.5.6 ip4:149.96.5.3
ip4:149.96.6.2 " "ip4:149.96.6.7 ip4:199.91.136.28 ip4:149.96.5.2 ip4:69.167.139.85 ip4:142.3.100.94
ip4:207.138.59.82 " "ip4:142.99.241.46 ip4:142.99.18.12 ip4:35.182.71.56 ip4:205.139.104.0/22
ip4:149.72.161.246 ip4:149.72.190.43 " "ip4:149.72.227.21 ip4:167.89.111.77 ip4:168.245.22.106
ip4:168.245.23.37 ip4:168.245.61.128 ip4:168.245.125.167 " "ip4:172.25.24.83 ip4:149.72.40.131
ip4:52.60.116.9 ip4:52.60.157.49 " "ip4:216.235.196.0/22 ip4:216.235.200.0/21 ip4:206.79.6.0/24
ip4:216.235.195.0/24 ip4:205.139.105.48/29 " "ip4:206.79.6.128/26 ip4:208.40.241.140/30
ip4:216.37.18.6 ip4:204.8.10.114 ip4:216.235.197.198 ip4:64.209.141.221 " "ip4:198.2.128.0/18
ip4:148.105.0.0/16 ip4:176.31.145.254 ip4:208.117.49.214/32 ip4:69.27.105.10 " "ip4:64.110.233.142
ip4:184.107.80.100 ip4:184.107.80.111 ip4:184.107.80.101 ip4:184.107.80.123 ip4:184.107.80.119 "
"ip4:184.107.63.100 ip4:174.142.116.50 ip4:174.142.116.51 ip4:174.142.116.39 ip4:174.142.116.40

ip4:216.230.14.224/27 " "ip4:64.74.237.230/31 ip4:216.147.212.20/30 ip4:139.60.152.0/22 ip4:64.69.212.0/24 ip4:162.247.216.0/22 ip4:35.182.104.93 ip4:99.79.84.236 ip4:52.60.171.2 " "ip4:98.97.248.0/21 ip4:142.99.241.241/31 ip4:3.64.88.217 ip4:3.68.40.83 ip4:3.68.17.221 ip4:3.67.235.98 ip4:52.60.156.213 ip4:3.68.38.23 " "ip4:3.64.131.199 ip4:3.64.142.243 ip4:142.99.246.40 ip4:142.99.246.85 ip4:18.198.149.19 ip4:147.253.212.171 ip4:18.198.18.157 ip4:198.245.53.9 ip4:66.116.119.146 ip4:52.20.131.1 ip4:52.204.119.75 " "ip4:205.139.105.140 ip4:205.139.105.10 ip4:205.139.105.11 ip4:52.60.141.24 ip4:52.60.221.41 ip4:52.60.41.154 include:spf.protection.outlook.com include:sendgrid.net include:amazonses.com include:mailgun.org ~all"
TXT: "bcn=7A8C471E-7C96-11ED-B622-81D0F6BACC47"
TXT: "apple-domain-verification=VIKPxwXBa2dlWr87"
TXT: "google-site-verification=P5wY59rRfyGhRMIxTcdlYtEnIj3T7I5Zdv9iK1XZ6jA"
---

---------- DNSKEY ----------
Reason: The DNS response does not contain an answer to the question: saskpolytech.ca. IN DNSKEY
---

---------- AXFR ----------
Reason: DNS metaqueries are not allowed.
---

# Target Domain: scanme.nmap.org

| Port ID | Protocol | State | Reason | Service |
|---|---|---|---|---|
| 21 | tcp | closed | reset | ftp |
| 22 | tcp | open | syn-ack | ssh |
| 23 | tcp | filtered | no-response | telnet |
| 25 | tcp | closed | reset | smtp |
| 80 | tcp | open | syn-ack | http |
| 110 | tcp | closed | reset | pop3 |
| 139 | tcp | closed | reset | netbios-ssn |
| 443 | tcp | closed | reset | https |
| 445 | tcp | closed | reset | microsoft-ds |
| 3389 | tcp | closed | reset | ms-wbt-server |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 22 | open | 95499236-C9FE-56A6-9D7D-E943A24B633A | 10.0 | https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A | true |
| 45.33.32.156 | tcp | 22 | open | 2C119FFA-ECE0-5E14-A4A4-354A2C38071A | 10.0 | https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A | true |
| 45.33.32.156 | tcp | 22 | open | 5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A | 8.1 | https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A | true |
| 45.33.32.156 | tcp | 22 | open | PACKETSTORM:140070 | 7.8 | https://vulners.com/packetstorm/PACKETSTORM:140070 | true |
| 45.33.32.156 | tcp | 22 | open | EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 | 7.8 | https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 | true |
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-26494 | 7.8 | https://vulners.com/zdt/1337DAY-ID-26494 | true |
| 45.33.32.156 | tcp | 22 | open | SSV:92579 | 7.5 | https://vulners.com/seebug/SSV:92579 | true |
| 45.33.32.156 | tcp | 22 | open | PACKETSTORM:173661 | 7.5 | https://vulners.com/packetstorm/PACKETSTORM:173661 | true |
| 45.33.32.156 | tcp | 22 | open | F0979183-AE88-53B4-86CF-3AF0523F3807 | 7.5 | https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:40888 | 7.5 | https://vulners.com/exploitdb/EDB-ID:40888 | true |
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-26576 | 7.5 | https://vulners.com/zdt/1337DAY-ID-26576 | true |
| 45.33.32.156 | tcp | 22 | open | SSV:92582 | 7.2 | https://vulners.com/seebug/SSV:92582 | true |
| 45.33.32.156 | tcp | 22 | open | SSV:92580 | 6.9 | https://vulners.com/seebug/SSV:92580 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-26577 | 6.9 | https://vulners.com/zdt/1337DAY-ID-26577 | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:46516 | 6.8 | https://vulners.com/exploitdb/EDB-ID:46516 | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:46193 | 6.8 | https://vulners.com/exploitdb/EDB-ID:46193 | true |
| 45.33.32.156 | tcp | 22 | open | C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 | 6.8 | https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 | true |
| 45.33.32.156 | tcp | 22 | open | 10213DBE-F683-58BB-B6D3-353173626207 | 6.8 | https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207 | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:40858 | 6.4 | https://vulners.com/exploitdb/EDB-ID:40858 | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:40119 | 6.4 | https://vulners.com/exploitdb/EDB-ID:40119 | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:39569 | 6.4 | https://vulners.com/exploitdb/EDB-ID:39569 | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:40136 | 5.9 | https://vulners.com/exploitdb/EDB-ID:40136 | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:40113 | 5.9 | https://vulners.com/exploitdb/EDB-ID:40113 | true |
| 45.33.32.156 | tcp | 22 | open | EXPLOITPACK:98FE96309F9524B8C84C508837551A19 | 5.8 | https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19 | true |
| 45.33.32.156 | tcp | 22 | open | EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 | 5.8 | https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 | true |
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-32328 | 5.8 | https://vulners.com/zdt/1337DAY-ID-32328 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-32009 | 5.8 | https://vulners.com/zdt/1337DAY-ID-32009 | true |
| 45.33.32.156 | tcp | 22 | open | SSV:91041 | 5.5 | https://vulners.com/seebug/SSV:91041 | true |
| 45.33.32.156 | tcp | 22 | open | PACKETSTORM:140019 | 5.5 | https://vulners.com/packetstorm/PACKETSTORM:140019 | true |
| 45.33.32.156 | tcp | 22 | open | PACKETSTORM:136234 | 5.5 | https://vulners.com/packetstorm/PACKETSTORM:136234 | true |
| 45.33.32.156 | tcp | 22 | open | EXPLOITPACK:F92411A645D85F05BDBD274FD222226F | 5.5 | https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05BDBD274FD222226F | true |
| 45.33.32.156 | tcp | 22 | open | EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 | 5.5 | https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 | true |
| 45.33.32.156 | tcp | 22 | open | EXPLOITPACK:1902C998CBF9154396911926B4C3B330 | 5.5 | https://vulners.com/exploitpack/EXPLOITPACK:1902C998CBF9154396911926B4C3B330 | true |
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-25388 | 5.5 | https://vulners.com/zdt/1337DAY-ID-25388 | true |
| 45.33.32.156 | tcp | 22 | open | PACKETSTORM:181223 | 5.3 | https://vulners.com/packetstorm/PACKETSTORM:181223 | true |
| 45.33.32.156 | tcp | 22 | open | MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- | 5.3 | https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:45939 | 5.3 | https://vulners.com/exploitdb/EDB-ID:45939 | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:45233 | 5.3 | https://vulners.com/exploitdb/EDB-ID:45233 | true |
| 45.33.32.156 | tcp | 22 | open | SSH_ENUM | 5.0 | https://vulners.com/canvas/SSH_ENUM | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 22 | open | PACKETSTORM:150621 | 5.0 | https://vulners.com/packetstorm/PACKETSTORM:150621 | true |
| 45.33.32.156 | tcp | 22 | open | EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 | 5.0 | https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 | true |
| 45.33.32.156 | tcp | 22 | open | EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 | 5.0 | https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 | true |
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-31730 | 5.0 | https://vulners.com/zdt/1337DAY-ID-31730 | true |
| 45.33.32.156 | tcp | 22 | open | EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF | 4.3 | https://vulners.com/exploitpack/EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF | true |
| 45.33.32.156 | tcp | 22 | open | EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF | 4.3 | https://vulners.com/exploitpack/EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF | true |
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-25440 | 4.3 | https://vulners.com/zdt/1337DAY-ID-25440 | true |
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-25438 | 4.3 | https://vulners.com/zdt/1337DAY-ID-25438 | true |
| 45.33.32.156 | tcp | 22 | open | SSV:92581 | 2.1 | https://vulners.com/seebug/SSV:92581 | true |
| 45.33.32.156 | tcp | 22 | open | PACKETSTORM:151227 | 0.0 | https://vulners.com/packetstorm/PACKETSTORM:151227 | true |
| 45.33.32.156 | tcp | 22 | open | PACKETSTORM:140261 | 0.0 | https://vulners.com/packetstorm/PACKETSTORM:140261 | true |
| 45.33.32.156 | tcp | 22 | open | PACKETSTORM:138006 | 0.0 | https://vulners.com/packetstorm/PACKETSTORM:138006 | true |
| 45.33.32.156 | tcp | 22 | open | PACKETSTORM:137942 | 0.0 | https://vulners.com/packetstorm/PACKETSTORM:137942 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 22 | open | EDB-ID:45210 | 0.0 | https://vulners.com/exploitdb/EDB-ID:45210 | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:40963 | 0.0 | https://vulners.com/exploitdb/EDB-ID:40963 | true |
| 45.33.32.156 | tcp | 22 | open | EDB-ID:40962 | 0.0 | https://vulners.com/exploitdb/EDB-ID:40962 | true |
| 45.33.32.156 | tcp | 22 | open | B8190CDB-3EB9-5631-9828-8064A1575B23 | 0.0 | https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 | true |
| 45.33.32.156 | tcp | 22 | open | 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 | 0.0 | https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 | true |
| 45.33.32.156 | tcp | 22 | open | 8AD01159-548E-546E-AA87-2DE89F3927EC | 0.0 | https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC | true |
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-30937 | 0.0 | https://vulners.com/zdt/1337DAY-ID-30937 | true |
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-26468 | 0.0 | https://vulners.com/zdt/1337DAY-ID-26468 | true |
| 45.33.32.156 | tcp | 22 | open | 1337DAY-ID-25391 | 0.0 | https://vulners.com/zdt/1337DAY-ID-25391 | true |
| 45.33.32.156 | tcp | 22 | open | 0221525F-07F5-5790-912D-F4B9E2D1B587 | 0.0 | https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587 | true |
| 45.33.32.156 | tcp | 80 | open | 95499236-C9FE-56A6-9D7D-E943A24B633A | 10.0 | https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A | true |
| 45.33.32.156 | tcp | 80 | open | 2C119FFA-ECE0-5E14-A4A4-354A2C38071A | 10.0 | https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A | true |
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:181114 | 9.8 | https://vulners.com/packetstorm/PACKETSTORM:181114 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5 | 9.8 | https://vulners.com/githubexploit/F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5 | true |
| 45.33.32.156 | tcp | 80 | open | F607361B-6369-5DF5-9B29-E90FA29DC565 | 9.8 | https://vulners.com/githubexploit/F607361B-6369-5DF5-9B29-E90FA29DC565 | true |
| 45.33.32.156 | tcp | 80 | open | EDB-ID:51193 | 9.8 | https://vulners.com/exploitdb/EDB-ID:51193 | true |
| 45.33.32.156 | tcp | 80 | open | EDB-ID:50512 | 9.8 | https://vulners.com/exploitdb/EDB-ID:50512 | true |
| 45.33.32.156 | tcp | 80 | open | EDB-ID:50446 | 9.8 | https://vulners.com/exploitdb/EDB-ID:50446 | true |
| 45.33.32.156 | tcp | 80 | open | EDB-ID:50406 | 9.8 | https://vulners.com/exploitdb/EDB-ID:50406 | true |
| 45.33.32.156 | tcp | 80 | open | C94CBDE1-4CC5-5C06-9D18-23CAB216705E | 9.8 | https://vulners.com/githubexploit/C94CBDE1-4CC5-5C06-9D18-23CAB216705E | true |
| 45.33.32.156 | tcp | 80 | open | A5425A79-9D81-513A-9CC5-549D6321897C | 9.8 | https://vulners.com/githubexploit/A5425A79-9D81-513A-9CC5-549D6321897C | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-39214 | 9.8 | https://vulners.com/zdt/1337DAY-ID-39214 | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-37777 | 9.8 | https://vulners.com/zdt/1337DAY-ID-37777 | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-36952 | 9.8 | https://vulners.com/zdt/1337DAY-ID-36952 | true |
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:181038 | 7.5 | https://vulners.com/packetstorm/PACKETSTORM:181038 | true |
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:176334 | 7.5 | https://vulners.com/packetstorm/PACKETSTORM:176334 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:171631 | 7.5 | https://vulners.com/packetstorm/PACKETSTORM:171631 | true |
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:164941 | 7.5 | https://vulners.com/packetstorm/PACKETSTORM:164941 | true |
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:164629 | 7.5 | https://vulners.com/packetstorm/PACKETSTORM:164629 | true |
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:164609 | 7.5 | https://vulners.com/packetstorm/PACKETSTORM:164609 | true |
| 45.33.32.156 | tcp | 80 | open | F8A7DE57-8F14-5B3C-A102-D546BDD8D2B8 | 7.5 | https://vulners.com/githubexploit/F8A7DE57-8F14-5B3C-A102-D546BDD8D2B8 | true |
| 45.33.32.156 | tcp | 80 | open | EDB-ID:50383 | 7.5 | https://vulners.com/exploitdb/EDB-ID:50383 | true |
| 45.33.32.156 | tcp | 80 | open | EDB-ID:42745 | 7.5 | https://vulners.com/exploitdb/EDB-ID:42745 | true |
| 45.33.32.156 | tcp | 80 | open | EDB-ID:40961 | 7.5 | https://vulners.com/exploitdb/EDB-ID:40961 | true |
| 45.33.32.156 | tcp | 80 | open | E81474F6-6DDC-5FC2-828A-812A8815E3B4 | 7.5 | https://vulners.com/githubexploit/E81474F6-6DDC-5FC2-828A-812A8815E3B4 | true |
| 45.33.32.156 | tcp | 80 | open | E59A01BE-8176-5F5E-BD32-D30B009CDBDA | 7.5 | https://vulners.com/githubexploit/E59A01BE-8176-5F5E-BD32-D30B009CDBDA | true |
| 45.33.32.156 | tcp | 80 | open | E-739 | 7.5 | https://vulners.com/dsquare/E-739 | true |
| 45.33.32.156 | tcp | 80 | open | E-738 | 7.5 | https://vulners.com/dsquare/E-738 | true |
| 45.33.32.156 | tcp | 80 | open | B81BC21D-818E-5B33-96D7-062C14102874 | 7.5 | https://vulners.com/githubexploit/B81BC21D-818E-5B33-96D7-062C14102874 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | A3F15BCE-08AD-509D-AE63-9D3D8E402E0B | 7.5 | https://vulners.com/githubexploit/A3F15BCE-08AD-509D-AE63-9D3D8E402E0B | true |
| 45.33.32.156 | tcp | 80 | open | 9D511461-7D24-5402-8E2A-58364D6E758F | 7.5 | https://vulners.com/githubexploit/9D511461-7D24-5402-8E2A-58364D6E758F | true |
| 45.33.32.156 | tcp | 80 | open | 7C40F14D-44E4-5155-95CF-40899776329C | 7.5 | https://vulners.com/githubexploit/7C40F14D-44E4-5155-95CF-40899776329C | true |
| 45.33.32.156 | tcp | 80 | open | 6BCBA83C-4A4C-58D7-92E4-DF092DFEF267 | 7.5 | https://vulners.com/githubexploit/6BCBA83C-4A4C-58D7-92E4-DF092DFEF267 | true |
| 45.33.32.156 | tcp | 80 | open | 68A13FF0-60E5-5A29-9248-83A940B0FB02 | 7.5 | https://vulners.com/githubexploit/68A13FF0-60E5-5A29-9248-83A940B0FB02 | true |
| 45.33.32.156 | tcp | 80 | open | 4051D2EF-1C43-576D-ADB2-B519B31F93A0 | 7.5 | https://vulners.com/githubexploit/4051D2EF-1C43-576D-ADB2-B519B31F93A0 | true |
| 45.33.32.156 | tcp | 80 | open | 2A177215-CE4A-5FA7-B016-EEAF332D165C | 7.5 | https://vulners.com/githubexploit/2A177215-CE4A-5FA7-B016-EEAF332D165C | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-38427 | 7.5 | https://vulners.com/zdt/1337DAY-ID-38427 | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-37030 | 7.5 | https://vulners.com/zdt/1337DAY-ID-37030 | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-36937 | 7.5 | https://vulners.com/zdt/1337DAY-ID-36937 | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-36897 | 7.5 | https://vulners.com/zdt/1337DAY-ID-36897 | true |
| 45.33.32.156 | tcp | 80 | open | 0C28A0EC-7162-5D73-BEC9-B034F5392847 | 7.5 | https://vulners.com/githubexploit/0C28A0EC-7162-5D73-BEC9-B034F5392847 | true |
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:127546 | 6.8 | https://vulners.com/packetstorm/PACKETSTORM:127546 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 | 6.8 | https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 | true |
| 45.33.32.156 | tcp | 80 | open | 4427DEE4-E1E2-5A16-8683-D74750941604 | 6.8 | https://vulners.com/githubexploit/4427DEE4-E1E2-5A16-8683-D74750941604 | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-22451 | 6.8 | https://vulners.com/zdt/1337DAY-ID-22451 | true |
| 45.33.32.156 | tcp | 80 | open | 0095E929-7573-5E4A-A7FA-F6598A35E8DE | 6.8 | https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE | true |
| 45.33.32.156 | tcp | 80 | open | 45F0EB7B-CE04-5103-9D40-7379AE4B6CDD | 5.8 | https://vulners.com/githubexploit/45F0EB7B-CE04-5103-9D40-7379AE4B6CDD | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-33577 | 5.8 | https://vulners.com/zdt/1337DAY-ID-33577 | true |
| 45.33.32.156 | tcp | 80 | open | SSV:96537 | 5.0 | https://vulners.com/seebug/SSV:96537 | true |
| 45.33.32.156 | tcp | 80 | open | SSV:62058 | 5.0 | https://vulners.com/seebug/SSV:62058 | true |
| 45.33.32.156 | tcp | 80 | open | SSV:61874 | 5.0 | https://vulners.com/seebug/SSV:61874 | true |
| 45.33.32.156 | tcp | 80 | open | EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 | 5.0 | https://vulners.com/exploitpack/EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 | true |
| 45.33.32.156 | tcp | 80 | open | EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D | 5.0 | https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-28573 | 5.0 | https://vulners.com/zdt/1337DAY-ID-28573 | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-26574 | 5.0 | https://vulners.com/zdt/1337DAY-ID-26574 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | SSV:87152 | 4.3 | https://vulners.com/seebug/SSV:87152 | true |
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:127563 | 4.3 | https://vulners.com/packetstorm/PACKETSTORM:127563 | true |
| 45.33.32.156 | tcp | 80 | open | FFE89CAE-FAA6-5E93-9994-B5F4D0EC2197 | 4.3 | https://vulners.com/githubexploit/FFE89CAE-FAA6-5E93-9994-B5F4D0EC2197 | true |
| 45.33.32.156 | tcp | 80 | open | F893E602-F8EB-5D23-8ABF-920890DB23A3 | 4.3 | https://vulners.com/githubexploit/F893E602-F8EB-5D23-8ABF-920890DB23A3 | true |
| 45.33.32.156 | tcp | 80 | open | F463914D-1B20-54CA-BF87-EA28F3ADE2A3 | 4.3 | https://vulners.com/githubexploit/F463914D-1B20-54CA-BF87-EA28F3ADE2A3 | true |
| 45.33.32.156 | tcp | 80 | open | ECD5D758-774C-5488-B782-C8996208B401 | 4.3 | https://vulners.com/githubexploit/ECD5D758-774C-5488-B782-C8996208B401 | true |
| 45.33.32.156 | tcp | 80 | open | E9FE319B-26BF-5A75-8C6A-8AE55D7E7615 | 4.3 | https://vulners.com/githubexploit/E9FE319B-26BF-5A75-8C6A-8AE55D7E7615 | true |
| 45.33.32.156 | tcp | 80 | open | DF57E8F1-FE21-5EB9-8FC7-5F2EA267B09D | 4.3 | https://vulners.com/githubexploit/DF57E8F1-FE21-5EB9-8FC7-5F2EA267B09D | true |
| 45.33.32.156 | tcp | 80 | open | D7922C26-D431-5825-9897-B98478354289 | 4.3 | https://vulners.com/githubexploit/D7922C26-D431-5825-9897-B98478354289 | true |
| 45.33.32.156 | tcp | 80 | open | C26A395B-9695-59E4-908F-866A561936E9 | 4.3 | https://vulners.com/githubexploit/C26A395B-9695-59E4-908F-866A561936E9 | true |
| 45.33.32.156 | tcp | 80 | open | C068A003-5258-51DC-A3C0-786638A1B69C | 4.3 | https://vulners.com/githubexploit/C068A003-5258-51DC-A3C0-786638A1B69C | true |
| 45.33.32.156 | tcp | 80 | open | B8198D62-F9C8-5E03-A301-9A3580070B4C | 4.3 | https://vulners.com/githubexploit/B8198D62-F9C8-5E03-A301-9A3580070B4C | true |
| 45.33.32.156 | tcp | 80 | open | B4483895-BA86-5CFB-84F3-7C06411B5175 | 4.3 | https://vulners.com/githubexploit/B4483895-BA86-5CFB-84F3-7C06411B5175 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | A6753173-D2DC-54CC-A5C4-0751E61F0343 | 4.3 | https://vulners.com/githubexploit/A6753173-D2DC-54CC-A5C4-0751E61F0343 | true |
| 45.33.32.156 | tcp | 80 | open | A1FF76C0-CF98-5704-AEE4-DF6F1E434FA3 | 4.3 | https://vulners.com/githubexploit/A1FF76C0-CF98-5704-AEE4-DF6F1E434FA3 | true |
| 45.33.32.156 | tcp | 80 | open | 8FB9E7A8-9A5B-5D87-9A44-AE4A1A92213D | 4.3 | https://vulners.com/githubexploit/8FB9E7A8-9A5B-5D87-9A44-AE4A1A92213D | true |
| 45.33.32.156 | tcp | 80 | open | 8A14FEAD-A401-5B54-84EB-2059841AD1DD | 4.3 | https://vulners.com/githubexploit/8A14FEAD-A401-5B54-84EB-2059841AD1DD | true |
| 45.33.32.156 | tcp | 80 | open | 7248BA4C-3FE5-5529-9E4C-C91E241E8AA0 | 4.3 | https://vulners.com/githubexploit/7248BA4C-3FE5-5529-9E4C-C91E241E8AA0 | true |
| 45.33.32.156 | tcp | 80 | open | 6E104766-2F7A-5A0A-A24B-61D9B52AD4EE | 4.3 | https://vulners.com/githubexploit/6E104766-2F7A-5A0A-A24B-61D9B52AD4EE | true |
| 45.33.32.156 | tcp | 80 | open | 6C0C909F-3307-5755-97D2-0EBD17367154 | 4.3 | https://vulners.com/githubexploit/6C0C909F-3307-5755-97D2-0EBD17367154 | true |
| 45.33.32.156 | tcp | 80 | open | 628A345B-5FD8-5A2F-8782-9125584E4C89 | 4.3 | https://vulners.com/githubexploit/628A345B-5FD8-5A2F-8782-9125584E4C89 | true |
| 45.33.32.156 | tcp | 80 | open | 5D88E443-7AB2-5034-910D-D52A5EFFF5FC | 4.3 | https://vulners.com/githubexploit/5D88E443-7AB2-5034-910D-D52A5EFFF5FC | true |
| 45.33.32.156 | tcp | 80 | open | 500CE683-17EB-5776-8EF6-85122451B145 | 4.3 | https://vulners.com/githubexploit/500CE683-17EB-5776-8EF6-85122451B145 | true |
| 45.33.32.156 | tcp | 80 | open | 4E4BAF15-6430-514A-8679-5B9F03584B71 | 4.3 | https://vulners.com/githubexploit/4E4BAF15-6430-514A-8679-5B9F03584B71 | true |
| 45.33.32.156 | tcp | 80 | open | 4B46EB21-DF1F-5D84-AE44-9BCFE311DFB9 | 4.3 | https://vulners.com/githubexploit/4B46EB21-DF1F-5D84-AE44-9BCFE311DFB9 | true |
| 45.33.32.156 | tcp | 80 | open | 4B44115D-85A3-5E62-B9A8-5F336C24673F | 4.3 | https://vulners.com/githubexploit/4B44115D-85A3-5E62-B9A8-5F336C24673F | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | 4013EC74-B3C1-5D95-938A-54197A58586D | 4.3 | https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D | true |
| 45.33.32.156 | tcp | 80 | open | 3C5B500C-1858-5834-9D23-38DBE44AE969 | 4.3 | https://vulners.com/githubexploit/3C5B500C-1858-5834-9D23-38DBE44AE969 | true |
| 45.33.32.156 | tcp | 80 | open | 3B159471-590A-5941-ADED-20F4187E8C63 | 4.3 | https://vulners.com/githubexploit/3B159471-590A-5941-ADED-20F4187E8C63 | true |
| 45.33.32.156 | tcp | 80 | open | 3AE03E90-26EC-5F91-B84E-F04AF6239A9F | 4.3 | https://vulners.com/githubexploit/3AE03E90-26EC-5F91-B84E-F04AF6239A9F | true |
| 45.33.32.156 | tcp | 80 | open | 37A9128D-17C4-50FF-B025-5FC3E0F3F338 | 4.3 | https://vulners.com/githubexploit/37A9128D-17C4-50FF-B025-5FC3E0F3F338 | true |
| 45.33.32.156 | tcp | 80 | open | 3749CB78-BE3A-5018-8838-CA693845B5BD | 4.3 | https://vulners.com/githubexploit/3749CB78-BE3A-5018-8838-CA693845B5BD | true |
| 45.33.32.156 | tcp | 80 | open | 27108E72-8DC1-53B5-97D9-E869CA13EFF7 | 4.3 | https://vulners.com/githubexploit/27108E72-8DC1-53B5-97D9-E869CA13EFF7 | true |
| 45.33.32.156 | tcp | 80 | open | 24ADD37D-C8A1-5671-A0F4-378760FC69AC | 4.3 | https://vulners.com/githubexploit/24ADD37D-C8A1-5671-A0F4-378760FC69AC | true |
| 45.33.32.156 | tcp | 80 | open | 1E6E9010-4BDF-5C30-951C-79C280B90883 | 4.3 | https://vulners.com/githubexploit/1E6E9010-4BDF-5C30-951C-79C280B90883 | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-36854 | 4.3 | https://vulners.com/zdt/1337DAY-ID-36854 | true |
| 45.33.32.156 | tcp | 80 | open | 1337DAY-ID-33575 | 4.3 | https://vulners.com/zdt/1337DAY-ID-33575 | true |
| 45.33.32.156 | tcp | 80 | open | 04E3583E-DFED-5D0D-BCF2-1C1230EB666D | 4.3 | https://vulners.com/githubexploit/04E3583E-DFED-5D0D-BCF2-1C1230EB666D | true |
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:164501 | 0.0 | https://vulners.com/packetstorm/PACKETSTORM:164501 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:164418 | 0.0 | https://vulners.com/packetstorm/PACKETSTORM:164418 | true |
| 45.33.32.156 | tcp | 80 | open | PACKETSTORM:140265 | 0.0 | https://vulners.com/packetstorm/PACKETSTORM:140265 | true |
| 45.33.32.156 | tcp | 80 | open | MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE- | 0.0 | https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE- | true |
| 45.33.32.156 | tcp | 80 | open | MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED- | 0.0 | https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED- | true |
| 45.33.32.156 | tcp | 80 | open | MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH- | 0.0 | https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH- | true |
| 45.33.32.156 | tcp | 80 | open | FF610CB4-801A-5D1D-9AC9-ADFC287C8482 | 0.0 | https://vulners.com/githubexploit/FF610CB4-801A-5D1D-9AC9-ADFC287C8482 | true |
| 45.33.32.156 | tcp | 80 | open | FDF4BBB1-979C-5320-95EA-9EC7EB064D72 | 0.0 | https://vulners.com/githubexploit/FDF4BBB1-979C-5320-95EA-9EC7EB064D72 | true |
| 45.33.32.156 | tcp | 80 | open | FCAF01A0-F921-5DB1-BBC5-850EC2DC5C46 | 0.0 | https://vulners.com/githubexploit/FCAF01A0-F921-5DB1-BBC5-850EC2DC5C46 | true |
| 45.33.32.156 | tcp | 80 | open | F7F6E599-CEF4-5E03-8E10-FE18C4101E38 | 0.0 | https://vulners.com/githubexploit/F7F6E599-CEF4-5E03-8E10-FE18C4101E38 | true |
| 45.33.32.156 | tcp | 80 | open | F41EE867-4E63-5259-9DF0-745881884D04 | 0.0 | https://vulners.com/githubexploit/F41EE867-4E63-5259-9DF0-745881884D04 | true |
| 45.33.32.156 | tcp | 80 | open | EDB-ID:47689 | 0.0 | https://vulners.com/exploitdb/EDB-ID:47689 | true |
| 45.33.32.156 | tcp | 80 | open | EDB-ID:47688 | 0.0 | https://vulners.com/exploitdb/EDB-ID:47688 | true |
| 45.33.32.156 | tcp | 80 | open | EDB-ID:34133 | 0.0 | https://vulners.com/exploitdb/EDB-ID:34133 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | E7B177F6-FA62-52FE-A108-4B8FC8112B7F | 0.0 | https://vulners.com/githubexploit/E7B177F6-FA62-52FE-A108-4B8FC8112B7F | true |
| 45.33.32.156 | tcp | 80 | open | E796A40A-8A8E-59D1-93FB-78EF4D8B7FA6 | 0.0 | https://vulners.com/githubexploit/E796A40A-8A8E-59D1-93FB-78EF4D8B7FA6 | true |
| 45.33.32.156 | tcp | 80 | open | E6B39247-8016-5007-B505-699F05FCA1B5 | 0.0 | https://vulners.com/githubexploit/E6B39247-8016-5007-B505-699F05FCA1B5 | true |
| 45.33.32.156 | tcp | 80 | open | E5C174E5-D6E8-56E0-8403-D287DE52EB3F | 0.0 | https://vulners.com/githubexploit/E5C174E5-D6E8-56E0-8403-D287DE52EB3F | true |
| 45.33.32.156 | tcp | 80 | open | DBF996C3-DC2A-5859-B767-6B2FC38F2185 | 0.0 | https://vulners.com/githubexploit/DBF996C3-DC2A-5859-B767-6B2FC38F2185 | true |
| 45.33.32.156 | tcp | 80 | open | DB6E1BBD-08B1-574D-A351-7D6BB9898A4A | 0.0 | https://vulners.com/githubexploit/DB6E1BBD-08B1-574D-A351-7D6BB9898A4A | true |
| 45.33.32.156 | tcp | 80 | open | D10426F3-DF82-5439-AC3E-6CA0A1365A09 | 0.0 | https://vulners.com/githubexploit/D10426F3-DF82-5439-AC3E-6CA0A1365A09 | true |
| 45.33.32.156 | tcp | 80 | open | D0E79214-C9E8-52BD-BC24-093970F5F34E | 0.0 | https://vulners.com/githubexploit/D0E79214-C9E8-52BD-BC24-093970F5F34E | true |
| 45.33.32.156 | tcp | 80 | open | D0368327-F989-5557-A5C6-0D9ACDB4E72F | 0.0 | https://vulners.com/githubexploit/D0368327-F989-5557-A5C6-0D9ACDB4E72F | true |
| 45.33.32.156 | tcp | 80 | open | CF47F8BF-37F7-5EF9-ABAB-E88ECF6B64FE | 0.0 | https://vulners.com/githubexploit/CF47F8BF-37F7-5EF9-ABAB-E88ECF6B64FE | true |
| 45.33.32.156 | tcp | 80 | open | CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 | 0.0 | https://vulners.com/githubexploit/CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 | true |
| 45.33.32.156 | tcp | 80 | open | CD48BD40-E52A-5A8B-AE27-B57C358BB0EE | 0.0 | https://vulners.com/githubexploit/CD48BD40-E52A-5A8B-AE27-B57C358BB0EE | true |
| 45.33.32.156 | tcp | 80 | open | CC15AE65-B697-525A-AF4B-38B1501CAB49 | 0.0 | https://vulners.com/githubexploit/CC15AE65-B697-525A-AF4B-38B1501CAB49 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B | 0.0 | https://vulners.com/githubexploit/C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B | true |
| 45.33.32.156 | tcp | 80 | open | C8C7BBD4-C089-5DA7-8474-A5B2B7DC5E79 | 0.0 | https://vulners.com/githubexploit/C8C7BBD4-C089-5DA7-8474-A5B2B7DC5E79 | true |
| 45.33.32.156 | tcp | 80 | open | C879EE66-6B75-5EC8-AA68-08693C6CCAD1 | 0.0 | https://vulners.com/githubexploit/C879EE66-6B75-5EC8-AA68-08693C6CCAD1 | true |
| 45.33.32.156 | tcp | 80 | open | C8799CA3-C88C-5B39-B291-2895BE0D9133 | 0.0 | https://vulners.com/githubexploit/C8799CA3-C88C-5B39-B291-2895BE0D9133 | true |
| 45.33.32.156 | tcp | 80 | open | C5A61CC6-919E-58B4-8FBB-0198654A7FC8 | 0.0 | https://vulners.com/githubexploit/C5A61CC6-919E-58B4-8FBB-0198654A7FC8 | true |
| 45.33.32.156 | tcp | 80 | open | C0380E16-C468-5540-A427-7FE34E7CF36B | 0.0 | https://vulners.com/githubexploit/C0380E16-C468-5540-A427-7FE34E7CF36B | true |
| 45.33.32.156 | tcp | 80 | open | BF9B0898-784E-5B5E-9505-430B58C1E6B8 | 0.0 | https://vulners.com/githubexploit/BF9B0898-784E-5B5E-9505-430B58C1E6B8 | true |
| 45.33.32.156 | tcp | 80 | open | BD3652A9-D066-57BA-9943-4E34970463B9 | 0.0 | https://vulners.com/githubexploit/BD3652A9-D066-57BA-9943-4E34970463B9 | true |
| 45.33.32.156 | tcp | 80 | open | BC027F41-02AD-5D71-A452-4DD62B0F1EE1 | 0.0 | https://vulners.com/githubexploit/BC027F41-02AD-5D71-A452-4DD62B0F1EE1 | true |
| 45.33.32.156 | tcp | 80 | open | B946B2A1-2914-537A-BF26-94B48FC501B3 | 0.0 | https://vulners.com/githubexploit/B946B2A1-2914-537A-BF26-94B48FC501B3 | true |
| 45.33.32.156 | tcp | 80 | open | B9151905-5395-5622-B789-E16B88F30C71 | 0.0 | https://vulners.com/githubexploit/B9151905-5395-5622-B789-E16B88F30C71 | true |
| 45.33.32.156 | tcp | 80 | open | B5E74010-A082-5ECE-AB37-623A5B33FE7D | 0.0 | https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D | true |
| 45.33.32.156 | tcp | 80 | open | B58E6202-6D04-5CB0-8529-59713C0E13B8 | 0.0 | https://vulners.com/githubexploit/B58E6202-6D04-5CB0-8529-59713C0E13B8 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | B53D7077-1A2B-5640-9581-0196F6138301 | 0.0 | https://vulners.com/githubexploit/B53D7077-1A2B-5640-9581-0196F6138301 | true |
| 45.33.32.156 | tcp | 80 | open | B02819DB-1481-56C4-BD09-6B4574297109 | 0.0 | https://vulners.com/githubexploit/B02819DB-1481-56C4-BD09-6B4574297109 | true |
| 45.33.32.156 | tcp | 80 | open | B0208442-6E17-5772-B12D-B5BE30FA5540 | 0.0 | https://vulners.com/githubexploit/B0208442-6E17-5772-B12D-B5BE30FA5540 | true |
| 45.33.32.156 | tcp | 80 | open | AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C | 0.0 | https://vulners.com/githubexploit/AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C | true |
| 45.33.32.156 | tcp | 80 | open | ACD5A7F2-FDB2-5859-8D23-3266A1AF6795 | 0.0 | https://vulners.com/githubexploit/ACD5A7F2-FDB2-5859-8D23-3266A1AF6795 | true |
| 45.33.32.156 | tcp | 80 | open | A9C7FB0F-65EC-5557-B6E8-6AFBBF8F140F | 0.0 | https://vulners.com/githubexploit/A9C7FB0F-65EC-5557-B6E8-6AFBBF8F140F | true |
| 45.33.32.156 | tcp | 80 | open | A90ABEAD-13A8-5F09-8A19-6D9D2D804F05 | 0.0 | https://vulners.com/githubexploit/A90ABEAD-13A8-5F09-8A19-6D9D2D804F05 | true |
| 45.33.32.156 | tcp | 80 | open | A8616E5E-04F8-56D8-ACB4-32FDF7F66EED | 0.0 | https://vulners.com/githubexploit/A8616E5E-04F8-56D8-ACB4-32FDF7F66EED | true |
| 45.33.32.156 | tcp | 80 | open | A820A056-9F91-5059-B0BC-8D92C7A31A52 | 0.0 | https://vulners.com/githubexploit/A820A056-9F91-5059-B0BC-8D92C7A31A52 | true |
| 45.33.32.156 | tcp | 80 | open | A66531EB-3C47-5C56-B8A6-E04B54E9D656 | 0.0 | https://vulners.com/githubexploit/A66531EB-3C47-5C56-B8A6-E04B54E9D656 | true |
| 45.33.32.156 | tcp | 80 | open | A2D97DCC-04C2-5CB1-921F-709AA8D7FD9A | 0.0 | https://vulners.com/githubexploit/A2D97DCC-04C2-5CB1-921F-709AA8D7FD9A | true |
| 45.33.32.156 | tcp | 80 | open | A0F268C8-7319-5637-82F7-8DAF72D14629 | 0.0 | https://vulners.com/githubexploit/A0F268C8-7319-5637-82F7-8DAF72D14629 | true |
| 45.33.32.156 | tcp | 80 | open | 9EE3F7E3-70E6-503E-9929-67FE3F3735A2 | 0.0 | https://vulners.com/githubexploit/9EE3F7E3-70E6-503E-9929-67FE3F3735A2 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | 9CEA663C-6236-5F45-B207-A873B971F988 | 0.0 | https://vulners.com/githubexploit/9CEA663C-6236-5F45-B207-A873B971F988 | true |
| 45.33.32.156 | tcp | 80 | open | 9B4F4E4A-CFDF-5847-805F-C0BAE809DBD5 | 0.0 | https://vulners.com/githubexploit/9B4F4E4A-CFDF-5847-805F-C0BAE809DBD5 | true |
| 45.33.32.156 | tcp | 80 | open | 987C6FDB-3E70-5FF5-AB5B-D50065D27594 | 0.0 | https://vulners.com/githubexploit/987C6FDB-3E70-5FF5-AB5B-D50065D27594 | true |
| 45.33.32.156 | tcp | 80 | open | 9814661A-35A4-5DB7-BB25-A1040F365C81 | 0.0 | https://vulners.com/githubexploit/9814661A-35A4-5DB7-BB25-A1040F365C81 | true |
| 45.33.32.156 | tcp | 80 | open | 907F28D0-5906-51C7-BAA3-FEBD5E878801 | 0.0 | https://vulners.com/githubexploit/907F28D0-5906-51C7-BAA3-FEBD5E878801 | true |
| 45.33.32.156 | tcp | 80 | open | 8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 | 0.0 | https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 | true |
| 45.33.32.156 | tcp | 80 | open | 8A57FAF6-FC91-52D1-84E0-4CBBAD3F9677 | 0.0 | https://vulners.com/githubexploit/8A57FAF6-FC91-52D1-84E0-4CBBAD3F9677 | true |
| 45.33.32.156 | tcp | 80 | open | 89732403-A14E-5A5D-B659-DD4830410847 | 0.0 | https://vulners.com/githubexploit/89732403-A14E-5A5D-B659-DD4830410847 | true |
| 45.33.32.156 | tcp | 80 | open | 88EB009A-EEFF-52B7-811D-A8A8C8DE8C81 | 0.0 | https://vulners.com/githubexploit/88EB009A-EEFF-52B7-811D-A8A8C8DE8C81 | true |
| 45.33.32.156 | tcp | 80 | open | 8713FD59-264B-5FD7-8429-3251AB5AB3B8 | 0.0 | https://vulners.com/githubexploit/8713FD59-264B-5FD7-8429-3251AB5AB3B8 | true |
| 45.33.32.156 | tcp | 80 | open | 866E26E3-759B-526D-ABB5-206B2A1AC3EE | 0.0 | https://vulners.com/githubexploit/866E26E3-759B-526D-ABB5-206B2A1AC3EE | true |
| 45.33.32.156 | tcp | 80 | open | 86360765-0B1A-5D73-A805-BAE8F1B5D16D | 0.0 | https://vulners.com/githubexploit/86360765-0B1A-5D73-A805-BAE8F1B5D16D | true |
| 45.33.32.156 | tcp | 80 | open | 831E1114-13D1-54EF-BDE4-F655114CDC29 | 0.0 | https://vulners.com/githubexploit/831E1114-13D1-54EF-BDE4-F655114CDC29 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | 805E6B24-8DF9-51D8-8DF6-6658161F96EA | 0.0 | https://vulners.com/githubexploit/805E6B24-8DF9-51D8-8DF6-6658161F96EA | true |
| 45.33.32.156 | tcp | 80 | open | 7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2 | 0.0 | https://vulners.com/githubexploit/7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2 | true |
| 45.33.32.156 | tcp | 80 | open | 7E615961-3792-5896-94FA-1F9D494ACB36 | 0.0 | https://vulners.com/githubexploit/7E615961-3792-5896-94FA-1F9D494ACB36 | true |
| 45.33.32.156 | tcp | 80 | open | 789B6112-E84C-566E-89A7-82CC108EFCD9 | 0.0 | https://vulners.com/githubexploit/789B6112-E84C-566E-89A7-82CC108EFCD9 | true |
| 45.33.32.156 | tcp | 80 | open | 788F7DF8-01F3-5D13-9B3E-E4AA692153E6 | 0.0 | https://vulners.com/githubexploit/788F7DF8-01F3-5D13-9B3E-E4AA692153E6 | true |
| 45.33.32.156 | tcp | 80 | open | 78787F63-0356-51EC-B32A-B9BD114431C3 | 0.0 | https://vulners.com/githubexploit/78787F63-0356-51EC-B32A-B9BD114431C3 | true |
| 45.33.32.156 | tcp | 80 | open | 749F952B-3ACF-56B2-809D-D66E756BE839 | 0.0 | https://vulners.com/githubexploit/749F952B-3ACF-56B2-809D-D66E756BE839 | true |
| 45.33.32.156 | tcp | 80 | open | 6E484197-456B-55DF-8D51-C2BB4925F45C | 0.0 | https://vulners.com/githubexploit/6E484197-456B-55DF-8D51-C2BB4925F45C | true |
| 45.33.32.156 | tcp | 80 | open | 6CAA7558-723B-5286-9840-4DF4EB48E0AF | 0.0 | https://vulners.com/githubexploit/6CAA7558-723B-5286-9840-4DF4EB48E0AF | true |
| 45.33.32.156 | tcp | 80 | open | 6A0A657E-8300-5312-99CE-E11F460B1DBF | 0.0 | https://vulners.com/githubexploit/6A0A657E-8300-5312-99CE-E11F460B1DBF | true |
| 45.33.32.156 | tcp | 80 | open | 68E78C64-D93A-5E8B-9DEA-4A8D826B474E | 0.0 | https://vulners.com/githubexploit/68E78C64-D93A-5E8B-9DEA-4A8D826B474E | true |
| 45.33.32.156 | tcp | 80 | open | 6758CFA9-271A-5E99-A590-E51F4E0C5046 | 0.0 | https://vulners.com/githubexploit/6758CFA9-271A-5E99-A590-E51F4E0C5046 | true |
| 45.33.32.156 | tcp | 80 | open | 674BA200-C494-57E6-B1B4-1672DDA15D3C | 0.0 | https://vulners.com/githubexploit/674BA200-C494-57E6-B1B4-1672DDA15D3C | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | 64D31BF1-F977-51EC-AB1C-6693CA6B58F3 | 0.0 | https://vulners.com/githubexploit/64D31BF1-F977-51EC-AB1C-6693CA6B58F3 | true |
| 45.33.32.156 | tcp | 80 | open | 61075B23-F713-537A-9B84-7EB9B96CF228 | 0.0 | https://vulners.com/githubexploit/61075B23-F713-537A-9B84-7EB9B96CF228 | true |
| 45.33.32.156 | tcp | 80 | open | 5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9 | 0.0 | https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9 | true |
| 45.33.32.156 | tcp | 80 | open | 5A864BCC-B490-5532-83AB-2E4109BB3C31 | 0.0 | https://vulners.com/githubexploit/5A864BCC-B490-5532-83AB-2E4109BB3C31 | true |
| 45.33.32.156 | tcp | 80 | open | 5A54F5DA-F9C1-508B-AD2D-3E45CD647D31 | 0.0 | https://vulners.com/githubexploit/5A54F5DA-F9C1-508B-AD2D-3E45CD647D31 | true |
| 45.33.32.156 | tcp | 80 | open | 5312D04F-9490-5472-84FA-86B3BBDC8928 | 0.0 | https://vulners.com/githubexploit/5312D04F-9490-5472-84FA-86B3BBDC8928 | true |
| 45.33.32.156 | tcp | 80 | open | 52E13088-9643-5E81-B0A0-B7478BCF1F2C | 0.0 | https://vulners.com/githubexploit/52E13088-9643-5E81-B0A0-B7478BCF1F2C | true |
| 45.33.32.156 | tcp | 80 | open | 4E5A5BA8-3BAF-57F0-B71A-F04B4D066E4F | 0.0 | https://vulners.com/githubexploit/4E5A5BA8-3BAF-57F0-B71A-F04B4D066E4F | true |
| 45.33.32.156 | tcp | 80 | open | 4C79D8E5-D595-5460-AA84-18D4CB93E8FC | 0.0 | https://vulners.com/githubexploit/4C79D8E5-D595-5460-AA84-18D4CB93E8FC | true |
| 45.33.32.156 | tcp | 80 | open | 4B14D194-BDE3-5D7F-A262-A701F90DE667 | 0.0 | https://vulners.com/githubexploit/4B14D194-BDE3-5D7F-A262-A701F90DE667 | true |
| 45.33.32.156 | tcp | 80 | open | 495E99E5-C1B0-52C1-9218-384D04161BE4 | 0.0 | https://vulners.com/githubexploit/495E99E5-C1B0-52C1-9218-384D04161BE4 | true |
| 45.33.32.156 | tcp | 80 | open | 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 | 0.0 | https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 | true |
| 45.33.32.156 | tcp | 80 | open | 44E43BB7-6255-58E7-99C7-C3B84645D497 | 0.0 | https://vulners.com/githubexploit/44E43BB7-6255-58E7-99C7-C3B84645D497 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | 4373C92A-2755-5538-9C91-0469C995AA9B | 0.0 | https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B | true |
| 45.33.32.156 | tcp | 80 | open | 41F0C2DA-2A2B-5ACC-A98D-CAD8D5AAD5ED | 0.0 | https://vulners.com/githubexploit/41F0C2DA-2A2B-5ACC-A98D-CAD8D5AAD5ED | true |
| 45.33.32.156 | tcp | 80 | open | 40F21EB4-9EE8-5ED1-B561-0A2B8625EED3 | 0.0 | https://vulners.com/githubexploit/40F21EB4-9EE8-5ED1-B561-0A2B8625EED3 | true |
| 45.33.32.156 | tcp | 80 | open | 3F17CA20-788F-5C45-88B3-E12DB2979B7B | 0.0 | https://vulners.com/githubexploit/3F17CA20-788F-5C45-88B3-E12DB2979B7B | true |
| 45.33.32.156 | tcp | 80 | open | 3CF66144-235E-5F7A-B889-113C11ABF150 | 0.0 | https://vulners.com/githubexploit/3CF66144-235E-5F7A-B889-113C11ABF150 | true |
| 45.33.32.156 | tcp | 80 | open | 379FCF38-0B4A-52EC-BE3E-408A0467BF20 | 0.0 | https://vulners.com/githubexploit/379FCF38-0B4A-52EC-BE3E-408A0467BF20 | true |
| 45.33.32.156 | tcp | 80 | open | 37634050-FDDF-571A-90BB-C8109824B38D | 0.0 | https://vulners.com/githubexploit/37634050-FDDF-571A-90BB-C8109824B38D | true |
| 45.33.32.156 | tcp | 80 | open | 36618CA8-9316-59CA-B748-82F15F407C4F | 0.0 | https://vulners.com/githubexploit/36618CA8-9316-59CA-B748-82F15F407C4F | true |
| 45.33.32.156 | tcp | 80 | open | 365CD0B0-D956-59D6-9500-965BF4017E2D | 0.0 | https://vulners.com/githubexploit/365CD0B0-D956-59D6-9500-965BF4017E2D | true |
| 45.33.32.156 | tcp | 80 | open | 30293CDA-FDB1-5FAF-9622-88427267F204 | 0.0 | https://vulners.com/githubexploit/30293CDA-FDB1-5FAF-9622-88427267F204 | true |
| 45.33.32.156 | tcp | 80 | open | 2E98EA81-24D1-5D5B-80B9-A8D616BF3C3F | 0.0 | https://vulners.com/githubexploit/2E98EA81-24D1-5D5B-80B9-A8D616BF3C3F | true |
| 45.33.32.156 | tcp | 80 | open | 2B4FEB27-377B-557B-AE46-66D677D5DA1C | 0.0 | https://vulners.com/githubexploit/2B4FEB27-377B-557B-AE46-66D677D5DA1C | true |
| 45.33.32.156 | tcp | 80 | open | 2B3110E1-BEA0-5DB8-93AD-1682230F3E19 | 0.0 | https://vulners.com/githubexploit/2B3110E1-BEA0-5DB8-93AD-1682230F3E19 | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | 249A954E-0189-5182-AE95-31C866A057E1 | 0.0 | https://vulners.com/githubexploit/249A954E-0189-5182-AE95-31C866A057E1 | true |
| 45.33.32.156 | tcp | 80 | open | 23079A70-8B37-56D2-9D37-F638EBF7F8B5 | 0.0 | https://vulners.com/githubexploit/23079A70-8B37-56D2-9D37-F638EBF7F8B5 | true |
| 45.33.32.156 | tcp | 80 | open | 22DCCD26-B68C-5905-BAC2-71D10DE3F123 | 0.0 | https://vulners.com/githubexploit/22DCCD26-B68C-5905-BAC2-71D10DE3F123 | true |
| 45.33.32.156 | tcp | 80 | open | 2108729F-1E99-54EF-9A4B-47299FD89FF2 | 0.0 | https://vulners.com/githubexploit/2108729F-1E99-54EF-9A4B-47299FD89FF2 | true |
| 45.33.32.156 | tcp | 80 | open | 1C39E10A-4A38-5228-8334-2A5F8AAB7FC3 | 0.0 | https://vulners.com/githubexploit/1C39E10A-4A38-5228-8334-2A5F8AAB7FC3 | true |
| 45.33.32.156 | tcp | 80 | open | 1B75F2E2-5B30-58FA-98A4-501B91327D7F | 0.0 | https://vulners.com/githubexploit/1B75F2E2-5B30-58FA-98A4-501B91327D7F | true |
| 45.33.32.156 | tcp | 80 | open | 18AE455A-1AA7-5386-81C2-39DA02CEFB57 | 0.0 | https://vulners.com/githubexploit/18AE455A-1AA7-5386-81C2-39DA02CEFB57 | true |
| 45.33.32.156 | tcp | 80 | open | 17C6AD2A-8469-56C8-BBBE-1764D0DF1680 | 0.0 | https://vulners.com/githubexploit/17C6AD2A-8469-56C8-BBBE-1764D0DF1680 | true |
| 45.33.32.156 | tcp | 80 | open | 11813536-2AFF-5EA4-B09F-E9EB340DDD26 | 0.0 | https://vulners.com/githubexploit/11813536-2AFF-5EA4-B09F-E9EB340DDD26 | true |
| 45.33.32.156 | tcp | 80 | open | 1145F3D1-0ECB-55AA-B25D-A26892116505 | 0.0 | https://vulners.com/githubexploit/1145F3D1-0ECB-55AA-B25D-A26892116505 | true |
| 45.33.32.156 | tcp | 80 | open | 108A0713-4AB8-5A1F-A16B-4BB13ECEC9B2 | 0.0 | https://vulners.com/githubexploit/108A0713-4AB8-5A1F-A16B-4BB13ECEC9B2 | true |
| 45.33.32.156 | tcp | 80 | open | 0C47BCF2-EA6F-5613-A6E8-B707D64155DE | 0.0 | https://vulners.com/githubexploit/0C47BCF2-EA6F-5613-A6E8-B707D64155DE | true |
| 45.33.32.156 | tcp | 80 | open | 0BC014D0-F944-5E78-B5FA-146A8E5D0F8A | 0.0 | https://vulners.com/githubexploit/0BC014D0-F944-5E78-B5FA-146A8E5D0F8A | true |

# Target Domain: scanme.nmap.org

| Host | Protocol | Port | State | CPE | CVE Score | URL | Is Exploit |
|---|---|---|---|---|---|---|---|
| 45.33.32.156 | tcp | 80 | open | 0AA6A425-25B1-5D2A-ABA1-2933D3E1DC56 | 0.0 | https://vulners.com/githubexploit/0AA6A425-25B1-5D2A-ABA1-2933D3E1DC56 | true |
| 45.33.32.156 | tcp | 80 | open | 07AA70EA-C34E-5F66-9510-7C265093992A | 0.0 | https://vulners.com/githubexploit/07AA70EA-C34E-5F66-9510-7C265093992A | true |
| 45.33.32.156 | tcp | 80 | open | 06076ECD-3FB7-53EC-8572-ABBB20029812 | 0.0 | https://vulners.com/githubexploit/06076ECD-3FB7-53EC-8572-ABBB20029812 | true |
| 45.33.32.156 | tcp | 80 | open | 05403438-4985-5E78-A702-784E03F724D4 | 0.0 | https://vulners.com/githubexploit/05403438-4985-5E78-A702-784E03F724D4 | true |
| 45.33.32.156 | tcp | 80 | open | 0486EBEE-F207-570A-9AD8-33269E72220A | 0.0 | https://vulners.com/githubexploit/0486EBEE-F207-570A-9AD8-33269E72220A | true |
| 45.33.32.156 | tcp | 80 | open | 00EC8F03-D8A3-56D4-9F8C-8DD1F5ACCA08 | 0.0 | https://vulners.com/githubexploit/00EC8F03-D8A3-56D4-9F8C-8DD1F5ACCA08 | true |

# Target Domain: saskpolytech.ca

| SubDomain | IP Address |
|---|---|
| ssb.saskpolytech.ca | 10.34.60.21 |
| webapi.saskpolytech.ca | 10.34.60.42 |
| alumninetwork.saskpolytech.ca | 3.164.255.95 |
| foodservices.saskpolytech.ca | 10.34.60.42 |
| sbc01.saskpolytech.ca | 10.33.7.11 |
| webprod.saskpolytech.ca | |
| acano.saskpolytech.ca | 142.99.4.35 |
| banssb2test3.saskpolytech.ca | 10.34.60.61 |
| timetorise.saskpolytech.ca | 20.151.119.96 |
| baneiscloudtest.saskpolytech.ca | 10.34.60.88 |
| libraries.saskpolytech.ca | 10.26.60.76 |
| pem.saskpolytech.ca | 10.26.60.15 |
| development.saskpolytech.ca | 10.34.60.45 |
| vaxxprooftest.saskpolytech.ca | |
| canarieidp.saskpolytech.ca | 10.34.56.246 |
| mobilechoicetest.saskpolytech.ca | 10.27.2.12 |
| anyconnect.saskpolytech.ca | |
| libdev.saskpolytech.ca | 10.34.60.45 |
| www.library.saskpolytech.ca | |
| surveys.saskpolytech.ca | |
| reportstest.saskpolytech.ca | 10.34.60.97 |
| smr.saskpolytech.ca | |

# Target Domain: saskpolytech.ca

| SubDomain | IP Address |
|---|---|
| www-myrxtx-ca.ezproxy.saskpolytech.ca | 132.174.254.110 |
| appsany-paging01.saskpolytech.ca | 10.34.56.115 |
| scholarships.saskpolytech.ca | 10.26.60.35 |
| appsanywhere.saskpolytech.ca | 10.34.60.83 |
| www.timetorise.saskpolytech.ca | |
| skypepool01-ext.saskpolytech.ca | |
| av.saskpolytech.ca | |
| janus.saskpolytech.ca | |
| learnlinc.saskpolytech.ca | |
| webtest.saskpolytech.ca | 10.26.60.85 |
| m.saskpolytech.ca | 142.99.18.51 |
| analytics.saskpolytech.ca | 4.206.210.215 |
| www.saskpolytech.ca | 10.34.60.42 |
| mymail2.saskpolytech.ca | |
| projectentapps.saskpolytech.ca | 10.26.60.71 |
| files.saskpolytech.ca | 10.34.60.15 |
| medianet.saskpolytech.ca | |
| testportal.saskpolytech.ca | 10.34.60.48 |
| apps.saskpolytech.ca | 10.34.60.57 |
| library.saskpolytech.ca | 10.34.60.42 |
| discussions.saskpolytech.ca | |
| ltdevt.saskpolytech.ca | 10.34.60.57 |

# Target Domain: saskpolytech.ca

| SubDomain | IP Address |
|---|---|
| hirecoop.saskpolytech.ca | 20.175.241.128 |
| libraryprod.saskpolytech.ca | |
| outraining.saskpolytech.ca | 10.26.60.37 |
| rdsgateway.saskpolytech.ca | 10.26.60.122 |
| bistest.saskpolytech.ca | 10.34.60.68 |
| ohs.saskpolytech.ca | |
| webpay.saskpolytech.ca | 10.34.60.96 |
| tem2.saskpolytech.ca | 10.26.60.93 |
| banadmin.saskpolytech.ca | 10.34.60.19 |
| sprite3.saskpolytech.ca | |
| mymail3.saskpolytech.ca | |
| streams.saskpolytech.ca | |
| elibrarytest.saskpolytech.ca | |
| banint.saskpolytech.ca | 10.26.60.60 |
| outside.saskpolytech.ca | |
| ltdevs.saskpolytech.ca | 10.34.60.57 |
| citrix.saskpolytech.ca | 10.34.56.63 |
| mypath.saskpolytech.ca | 10.34.60.46 |
| secured.saskpolytech.ca | |
| banadmintest4.saskpolytech.ca | 10.34.60.63 |
| persico.saskpolytech.ca | |
| tproxy.saskpolytech.ca | |

# Target Domain: saskpolytech.ca

| SubDomain | IP Address |
|---|---|
| www5.saskpolytech.ca | 20.151.7.109 |
| librariesnew.saskpolytech.ca | 10.26.60.37 |
| ourcollaborate.saskpolytech.ca | |
| appsdev.saskpolytech.ca | 10.34.60.57 |
| petrilli.saskpolytech.ca | |
| wlc-4402.saskpolytech.ca | |
| purvis.saskpolytech.ca | |
| wac.saskpolytech.ca | 10.26.60.38 |
| alumni.saskpolytech.ca | 20.151.119.96 |
| platoweb.saskpolytech.ca | |
| sspreset.saskpolytech.ca | |
| fastprod.saskpolytech.ca | |
| testportal51.saskpolytech.ca | |
| www.alumni.saskpolytech.ca | |
| russo1.saskpolytech.ca | |
| sspreg.saskpolytech.ca | |
| cnt-cisco-p01.saskpolytech.ca | |
| mysearch.saskpolytech.ca | |
| videos.saskpolytech.ca | 162.159.136.91 |
| curio-ca.ezproxy.saskpolytech.ca | 132.174.254.110 |
| learningtechnologies.saskpolytech.ca | 10.26.60.76 |
| tocco.saskpolytech.ca | |

# Target Domain: saskpolytech.ca

| SubDomain | IP Address |
|---|---|
| eis.saskpolytech.ca | 10.26.60.61 |
| apply.saskpolytech.ca | 20.48.202.163 |
| prod.saskpolytech.ca | |
| autodiscover.saskpolytech.ca | 10.34.60.103 |
| servicegateway.saskpolytech.ca | 40.82.185.39 |
| regexpresse.saskpolytech.ca | 10.27.2.1 |
| printingservices.saskpolytech.ca | 18.191.115.230 |
| online.saskpolytech.ca | 15.157.115.229 |
| reports.saskpolytech.ca | 10.34.60.98 |
| signagedev.saskpolytech.ca | 10.26.60.37 |
| ltxr.saskpolytech.ca | 10.34.60.57 |
| sbc02.saskpolytech.ca | 10.25.7.11 |
| borden.saskpolytech.ca | |
| myrobotrumble.saskpolytech.ca | 10.26.60.76 |
| cnt-super-p01.saskpolytech.ca | 10.34.60.77 |
| webresources.saskpolytech.ca | 10.26.60.22 |
| legacy.saskpolytech.ca | |
| meet.saskpolytech.ca | |
| portal.saskpolytech.ca | 10.34.60.25 |
| password.saskpolytech.ca | 10.26.60.17 |
| sip.saskpolytech.ca | |
| mymail.saskpolytech.ca | 10.26.60.5 |

# Target Domain: saskpolytech.ca

| SubDomain | IP Address |
|---|---|
| careers.saskpolytech.ca | 35.183.248.176 |
| www2.saskpolytech.ca | |
| calendar.saskpolytech.ca | 54.148.217.175 |
| mymail4.saskpolytech.ca | |
| personalprinting.saskpolytech.ca | 18.191.115.230 |
| scholarshipstest.saskpolytech.ca | 10.27.2.63 |
| test-analytics.saskpolytech.ca | |
| pressbooks.saskpolytech.ca | 3.164.255.32 |
| appsany-paging02.saskpolytech.ca | 10.34.56.116 |
| mymail5.saskpolytech.ca | |
| www1.saskpolytech.ca | 10.27.2.20 |
| forms.saskpolytech.ca | |
| netman.saskpolytech.ca | |
| ssbtest.saskpolytech.ca | 10.34.60.41 |
| ssbtest2.saskpolytech.ca | 10.34.60.44 |
| rabbitmq.saskpolytech.ca | 10.26.60.64 |
| cdpmt.saskpolytech.ca | |
| ltdevprod.saskpolytech.ca | 10.34.60.57 |
| schiro.saskpolytech.ca | |
| helpdesk.saskpolytech.ca | 10.26.60.9 |
| myfitandrec.saskpolytech.ca | 52.60.223.198 |
| ltdevt2.saskpolytech.ca | 10.34.60.57 |

# Target Domain: saskpolytech.ca

| SubDomain | IP Address |
|---|---|
| my.saskpolytech.ca | 10.34.60.104 |
| hybrid1.saskpolytech.ca | |
| mail.saskpolytech.ca | |
| banadmintest.saskpolytech.ca | 10.34.60.40 |
| secure.saskpolytech.ca | |
| pay4print.saskpolytech.ca | 10.34.60.53 |
| programsdev.saskpolytech.ca | 10.26.60.76 |
| testrecruiter.saskpolytech.ca | |
| myworkspace.saskpolytech.ca | 10.34.56.101 |
| ftp.saskpolytech.ca | 10.34.60.43 |
| oari.saskpolytech.ca | 10.26.60.76 |
| banadmintest3.saskpolytech.ca | 10.34.60.60 |
| login.ezproxy.saskpolytech.ca | 132.174.254.110 |
| smtp.saskpolytech.ca | 10.34.57.6 |
| videosdev.saskpolytech.ca | 162.159.135.91 |
| jackson.saskpolytech.ca | |
| librarynew.saskpolytech.ca | 10.26.60.37 |
| baneis.saskpolytech.ca | 10.34.60.17 |
| siastban.saskpolytech.ca | |
| mywebapps.saskpolytech.ca | |
| banssb1.saskpolytech.ca | 10.34.60.22 |
| nursing-unboundmedicine-com.ezproxy.saskpolytech.ca | 132.174.254.110 |

# Target Domain: saskpolytech.ca

| SubDomain | IP Address |
|---|---|
| techservices.saskpolytech.ca | 10.34.60.102 |
| bis.saskpolytech.ca | 10.34.60.67 |
| lamp.saskpolytech.ca | |
| banssb2.saskpolytech.ca | 10.34.60.20 |
| rabbitmqtest.saskpolytech.ca | 10.26.60.62 |
| dialin.saskpolytech.ca | |
| l4future.saskpolytech.ca | |
| russo.saskpolytech.ca | |
| templates.saskpolytech.ca | 10.26.60.76 |
| deross.saskpolytech.ca | |
| barnes.saskpolytech.ca | |
| collabtest.saskpolytech.ca | |
| signage.saskpolytech.ca | 10.34.60.42 |
| opac.saskpolytech.ca | |
| cloudowa.saskpolytech.ca | 52.96.223.50 |
| fms.saskpolytech.ca | |
| mypathtest.saskpolytech.ca | 10.34.60.47 |
| mysites.saskpolytech.ca | |
| l4test.saskpolytech.ca | |
| sites.saskpolytech.ca | 10.26.60.76 |
| bookstore.saskpolytech.ca | 52.142.31.64 |
| solano.saskpolytech.ca | |

# Target Domain: saskpolytech.ca

| SubDomain | IP Address |
|---|---|
| scholar-google-com.ezproxy.saskpolytech.ca | 132.174.254.110 |
| passwordreset.saskpolytech.ca | 10.26.60.47 |
| moss.saskpolytech.ca | |
| yale.saskpolytech.ca | |
| adfed.saskpolytech.ca | |
| lyncweb.saskpolytech.ca | |
| ssbtest3.saskpolytech.ca | 10.34.60.55 |
| engage.saskpolytech.ca | |
| ldap.saskpolytech.ca | 10.34.60.18 |
| programs.saskpolytech.ca | 10.26.60.76 |
| owa.saskpolytech.ca | |
| collaborate.saskpolytech.ca | |
| cnt-super-p02.saskpolytech.ca | 10.34.60.78 |
| think.saskpolytech.ca | 10.34.60.42 |
| apis-google-com.ezproxy.saskpolytech.ca | 132.174.254.110 |
| fastportal.saskpolytech.ca | 10.34.60.24 |
| ltdevtest.saskpolytech.ca | 10.34.60.57 |
| banssb1test3.saskpolytech.ca | 10.34.60.62 |
| avmweb.saskpolytech.ca | |
| hybrid2.saskpolytech.ca | |
| ltdevp.saskpolytech.ca | 10.34.60.57 |
| testalumni.saskpolytech.ca | 20.151.119.96 |

# Target Domain: saskpolytech.ca

| SubDomain | IP Address |
|---|---|
| ezproxy.saskpolytech.ca | 132.174.254.110 |
| testluminis.saskpolytech.ca | |
| virtualtour.saskpolytech.ca | 35.71.150.51 |
| ftpdev.saskpolytech.ca | 10.26.60.58 |
| preview.saskpolytech.ca | 10.34.60.45 |
| webconf.saskpolytech.ca | |
| ltprime.saskpolytech.ca | 10.34.60.57 |
| m.mypathtest.saskpolytech.ca | |
| skypeedge.saskpolytech.ca | |
| snapp.saskpolytech.ca | 10.34.60.71 |
| gillis.saskpolytech.ca | 10.27.2.81 |
| passwordenrol.saskpolytech.ca | 10.26.60.48 |
| lyncdiscover.saskpolytech.ca | |
| learningcentre.saskpolytech.ca | |
| robotrumble.saskpolytech.ca | 10.34.60.42 |

# Volatility Memory Analysis Result

Volatility 3 Framework 2.11.0

PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime File output

1732 1028 wuauclt.exe 0x10c3da0 7 189 0 False 2010-08-11 06:07:44.000000 UTC N/A Disabled
468 1028 wuauclt.exe 0x10f7588 4 142 0 False 2010-08-11 06:09:37.000000 UTC N/A Disabled
1028 676 svchost.exe 0x1122910 88 1424 0 False 2010-08-11 06:06:24.000000 UTC N/A Disabled
856 676 svchost.exe 0x115b8d8 29 336 0 False 2010-08-11 06:06:24.000000 UTC N/A Disabled
4 0 System 0x1214660 58 379 N/A False N/A N/A Disabled
1968 676 TPAutoConnSvc.e 0x211ab28 5 106 0 False 2010-08-11 06:06:39.000000 UTC N/A Disabled
1084 1968 TPAutoConnect.e 0x49c15f8 1 68 0 False 2010-08-11 06:06:52.000000 UTC N/A Disabled
1724 1708 explorer.exe 0x4a065d0 13 326 0 False 2010-08-11 06:09:29.000000 UTC N/A Disabled
452 1724 VMwareUser.exe 0x4b5a980 8 207 0 False 2010-08-11 06:09:32.000000 UTC N/A Disabled
432 1724 VMwareTray.exe 0x4be97e8 1 60 0 False 2010-08-11 06:09:31.000000 UTC N/A Disabled
888 1028 wscntfy.exe 0x4c2b310 1 40 0 False 2010-08-11 06:06:49.000000 UTC N/A Disabled
544 4 smss.exe 0x5471020 3 21 N/A False 2010-08-11 06:06:21.000000 UTC N/A Disabled
216 676 alg.exe 0x5f027e0 8 120 0 False 2010-08-11 06:06:39.000000 UTC N/A Disabled
688 632 lsass.exe 0x5f47020 21 405 0 False 2010-08-11 06:06:24.000000 UTC N/A Disabled
676 632 services.exe 0x6015020 16 288 0 False 2010-08-11 06:06:24.000000 UTC N/A Disabled
1088 676 svchost.exe 0x61ef558 7 93 0 False 2010-08-11 06:06:25.000000 UTC N/A Disabled
124 1668 cmd.exe 0x6238020 0 - 0 False 2010-08-15 19:17:55.000000 UTC 2010-08-15 19:17:56.000000 UTC Disabled
844 676 vmacthlp.exe 0x6384230 1 37 0 False 2010-08-11 06:06:24.000000 UTC N/A Disabled
936 676 svchost.exe 0x63c5560 11 288 0 False 2010-08-11 06:06:24.000000 UTC N/A Disabled
1148 676 svchost.exe 0x6499b80 15 217 0 False 2010-08-11 06:06:26.000000 UTC N/A Disabled
1788 676 VMUpgradeHelper 0x655fc88 5 112 0 False 2010-08-11 06:06:38.000000 UTC N/A Disabled
632 544 winlogon.exe 0x66f0978 24 536 0 False 2010-08-11 06:06:23.000000 UTC N/A Disabled
608 544 csrss.exe 0x66f0da0 10 410 0 False 2010-08-11 06:06:23.000000 UTC N/A Disabled
1432 676 spoolsv.exe 0x6945da0 14 145 0 False 2010-08-11 06:06:26.000000 UTC N/A Disabled
1944 124 VMip.exe 0x69a7328 0 - 0 False 2010-08-15 19:17:55.000000 UTC 2010-08-15 19:17:56.000000 UTC Disabled
1668 676 vmtoolsd.exe 0x69d5b28 5 225 0 False 2010-08-11 06:06:35.000000 UTC N/A Disabled