

INTERNSHIP ASSIGNMENT REPORT

Title: Network Scanning and Security Analysis Using Nmap

Student Details

Name: Putta Honna

Tools Used: Nmap, Wireshark

Operating System: Windows 11

1. Introduction

Network security is a critical aspect of cybersecurity. Identifying active devices and open ports helps in understanding potential risks. This assignment focuses on using Nmap to analyze a local network.

2. Objective

- Install and use Nmap
- Identify live hosts
- Detect open ports and services
- Analyze network traffic
- Identify security risks

3. Tools Used

Nmap – Network scanning

Wireshark – Packet analysis

Command Prompt – Execution

4. Network Information

Local IP Address: 172.17.0.1

Subnet Mask: 255.255.0.0

Network Range: 172.17.0.1/24

22/tcp → SSH (remote shell)

23/tcp → Telnet (insecure remote shell)

21/tcp → FTP (file transfer)

80/tcp → HTTP (web server)

443/tcp → HTTPS (secure web server)

3389/tcp → RDP (Windows Remote Desktop)

445/tcp → SMB (file sharing / Windows shares)

3306/tcp → MySQL database

5432/tcp → PostgreSQL database

5. Methodology:-

Installed Nmap from the official website and verified installation.

Used ipconfig to find the local network range.

Performed a TCP SYN scan using nmap -sS.

Recorded discovered hosts and open ports.

6. 10 Nmap Commands:-

1. Basic Ping Scan :- nmap -sn 81.161.178.68

Checks if a host is up without scanning ports.

2. Full Port Scan (1-65535) :-nmap -p- 81.161.178.68

Scans all 65,535 ports on the host.

3. Scan Specific Ports :-nmap -p 22,80,443 81.161.178.68

Scans only the selected ports.

4. Service & Version Detection:-nmap -sV 81.161.178.68

Shows software version running on each open port.

5. Aggressive Scan:-nmap -A 81.161.178.68

Performs OS detection, version detection, traceroute, script scanning.

6. Operating System Detection:-nmap -O 81.161.178.68

Identifies the OS (Windows/Linux) of the target.

7. Stealth SYN Scan (Default Scan):-nmap -sS 81.161.178.68

Fast and less detectable by firewalls.

8. Scan an Entire Network:-nmap 81.161.178.68

Scans all 256 devices in the subnet.

9. Vulnerability Scan (Using NSE Scripts) :-nmap --script=vuln 81.161.178.68

Runs vulnerability detection scripts.

10. Output Scan Results to a File:-nmap -oN scan_result.txt 81.161.178.681

7. Results and Findings

Multiple hosts and services were discovered. Some open ports could pose security risks if not secured.

8. Conclusion

Nmap is an effective tool for understanding network exposure and improving security posture.

```
root@BK:home0k
HELP
Commands supported: AUTH HELO MAIL RCPT DATA BOAT NOOP QUIT RSET HELP
587/tcp open  smtp      Exin smtpd 4.98.2
| ssl-cert: Subject: commonName=mail.pesce.ac.in
| Subject Alternative Name: DNS:mail.pesce.ac.in, DNS:pesce.ac.in, DNS:pesceandanya.org, DNS:www.pesce.ac.in, DNS:www.pesceandanya.org
| Not valid before: 2025-10-09T08:09:45
| Not valid after: 2026-01-07T08:09:44
| ssl-date: TLS randomness does not represent time
smtp_commands: 81.161.178.68 host.secureserver.net Hello pesce.ac.in [152.57.137.185], SIZE 52428800, LIMITS MAILMAX=1000 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP
Commands supported: AUTH STARTTLS HELO MAIL RCPT DATA BOAT NOOP QUIT RSET HELP
631/tcp filtered ipp
993/tcp open  imap2
| ssl-cert: Subject: commonName=mail.pesce.ac.in
| Subject Alternative Name: DNS:mail.pesce.ac.in, DNS:pesce.ac.in, DNS:pesceandanya.org, DNS:www.pesce.ac.in, DNS:www.pesceandanya.org
| Not valid before: 2025-10-09T08:09:45
| Not valid after: 2025-02-09T08:09:44
| ssl-date: TLS randomness does not represent time
| imap-capabilities: more NAMESPACE SASL-IR listed Pre-login ID have AUTH=PLAIN ENABLE IDLE IMAP4rev1 OK capabilities AUTH=LOGIN AUTH=LITERAL+ LOGIN-REFERRALS post-login
995/tcp open  pop3s
| ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mail.pesce.ac.in
| Subject Alternative Name: DNS:mail.pesce.ac.in, DNS:pesce.ac.in, DNS:pesceandanya.org, DNS:www.pesce.ac.in, DNS:www.pesceandanya.org
| Not valid before: 2025-10-09T08:09:45
| Not valid after: 2026-01-07T08:09:44
| pop3-capabilities: UIDL SASL(PLAIN LOGIN) USER AUTH-RESP-CODE PIPELINING RESP-CODES TOP CAPA
1806/tcp open  mysql      MySQL (unauthorized)
53/udp open  domain     (generic dns response: REFUSED)
dns-nsid:
| NSID: 81.161.178.68 host.secureserver.net (38312e3136312e3137382e36382e686f73742e7365637572657365727665722e6e6574)
| id.server: 81.161.178.68 host.secureserver.net
fingerprint-strings:
| DNS-SD:
| _services
| _dns-sd
| _udp
| _local
| NBTSState:
| CXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
111/udp open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp rpcbind
| 100000 3,4 111/udp rpcbind
135/udp open|filtered msrpc
136/udp open|filtered profile
137/udp open|filtered netbios-ns
138/udp open|filtered netbios-dgm
139/udp open|filtered netbios-ssn
445/udp open|filtered microsoft-ds
631/udp open|filtered ipp
2 resources unaccounted despite returning data. If you know the exact function, please submit the following fingerprints at https://www.nmap.org/bn/bin/submit.cgi?name=cpuinfo
```

Dec 3 13:24

root@BK:home/bk

HELP

Commands supported: AUTH HELO EHLO MAIL RCPT DATA BOAT NOOP QUIT RSET HELP

587/tcp open smtp Exim smtpd 4.98.2

ssl-cert: Subject: commonName=mail.pesce.ac.in

Subject Alternative Name: DNS:mail.pesce.ac.in, DNS:pesce.ac.in, DNS:pesceandya.org, DNS:www.pesce.ac.in, DNS:www.pesceandya.org

Not valid before: 2025-10-09T08:09:45

Not valid after: 2026-01-07T08:09:44

ssl-date: TLS randomness does not represent time

smtp-commands: 81.161.178.68.host.secureserver.net Hello pesce.ac.in [152.57.137.185], SIZE 52428800, LIMITS MAILMAX=1000 RCPTMAX=50000, BSMTPIME, PIPELINING, PIPECONNECT, STARTTLS, HELP

Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BOAT NOOP QUIT RSET HELP

631/tcp filtered pop

993/tcp open pop3s

ssl-cert: Subject: commonName=mail.pesce.ac.in

Subject Alternative Name: DNS:mail.pesce.ac.in, DNS:pesce.ac.in, DNS:pesceandya.org, DNS:www.pesce.ac.in, DNS:www.pesceandya.org

Not valid before: 2025-10-09T08:09:45

Not valid after: 2026-01-07T08:09:44

ssl-date: TLS randomness does not represent time

imap-capabilities: more NAMESPACE SASL-IR Listed Pre-login ID have AUTH=PLAIN ENABLE IDLE IMAP4rev1 OK capabilities AUTH=LOGIN AUTH=LOGIN LITERAL+ LOGIN-REFERRALS post-login

995/tcp open pop3s

ssl-date: TLS randomness does not represent time

ssl-cert: Subject: commonName=mail.pesce.ac.in

Subject Alternative Name: DNS:mail.pesce.ac.in, DNS:pesce.ac.in, DNS:pesceandya.org, DNS:www.pesce.ac.in, DNS:www.pesceandya.org

Not valid before: 2025-10-09T08:09:45

Not valid after: 2026-01-07T08:09:44

ssl-date: TLS randomness does not represent time

pop3-capabilities: UIDL SASL=PLAIN LOGIN USER AUTH=RESP=CODE PIPELINING RESP-CODES TOP CAPA

3306/tcp open mysql MySQL (unauthorized)

53/udp open domain (generic dns response: REFUSED)

dns-nsd

NSID: 81.161.178.68.host.secureserver.net [18312e3136312e3137382e36382e686e473742e73656375726572766372766e6574]

id.server: 81.161.178.68.host.secureserver.net

fingerprint-strings:

DNS-SD:

services

_dns-sd

_udp

_local

NETStat:

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

111/udp open rcpbind 2-4 (RPC #100000)

rcpinfo:

program version port/proto service

100000 2-4 111/udp rcpbind

100000 2-4 111/udp rcpbind

100000 3-4 111/tcp rcpbind

100000 3-4 111/udp rcpbind

135/udp open/filtered ntp

136/udp open/filtered profile

137/udp open/filtered netbios-ns

138/udp open/filtered netbios-dgm

139/udp open/filtered netbios-ssn

445/udp open/filtered microsoft-ds

631/udp open/filtered ipsec

Services information: Details returning data. If you know the source/hostname, please submit the full/fingerprints at <https://www.nmap.org/bin/submit.cgi?how=service>.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter -> <Ctrl-F>

No. Time Source Destination Protocol Length Info

3057.16.150612950 2004:8808:4:100:1F: 2409:40F2:217A:9130: HTTP 94 80 - 52642 [SYN, ACK] Seq=150612950 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3058.16.150612953 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 52618 - 80 [ACK] Seq=150612953 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3059.16.150612957 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 52618 - 80 [ACK] Seq=150612957 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3060.16.150612961 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 80 - 52602 [ACK] Seq=150612961 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3061.16.150612965 2004:8808:4:100:1F: 2409:40F2:217A:9130: HTTP 947 HTTP/1.1 200 OK (text/css)

3062.16.150612969 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 52618 - 80 [ACK] Seq=150612969 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3063.16.150612973 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 80 - 54908 [FIN, ACK] Seq=150612973 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3064.16.150612977 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 80 - 54908 [FIN, ACK] Seq=150612977 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3065.16.150612981 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150612981 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3066.16.150612985 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150612985 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3067.16.150612989 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150612989 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3068.16.150612993 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150612993 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3069.16.150612997 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150612997 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3070.16.150613001 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613001 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3071.16.150613005 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613005 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3072.16.150613009 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613009 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3073.16.150613013 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613013 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3074.16.150613017 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613017 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3075.16.150613021 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613021 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3076.16.150613025 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613025 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3077.16.150613029 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613029 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3078.16.150613033 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613033 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3079.16.150613037 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613037 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3080.16.150613041 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613041 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3081.16.150613045 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613045 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3082.16.150613049 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613049 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3083.16.150613053 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613053 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3084.16.150613057 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613057 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3085.16.150613061 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613061 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3086.16.150613065 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613065 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3087.16.150613069 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613069 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3088.16.150613073 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613073 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3089.16.150613077 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613077 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3090.16.150613081 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613081 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3091.16.150613085 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613085 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3092.16.150613089 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613089 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3093.16.150613093 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613093 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3094.16.150613097 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613097 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3095.16.150613101 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613101 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3096.16.150613105 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613105 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3097.16.150613109 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613109 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3098.16.150613113 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613113 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3099.16.150613117 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613117 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3100.16.150613121 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613121 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3101.16.150613125 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613125 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3102.16.150613129 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613129 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3103.16.150613133 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613133 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3104.16.150613137 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613137 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3105.16.150613141 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613141 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3106.16.150613145 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613145 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3107.16.150613149 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613149 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3108.16.150613153 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613153 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3109.16.150613157 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613157 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3110.16.150613161 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613161 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3111.16.150613165 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613165 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3112.16.150613169 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613169 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3113.16.150613173 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613173 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3114.16.150613177 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613177 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3115.16.150613181 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613181 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3116.16.150613185 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613185 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3117.16.150613189 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613189 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3118.16.150613193 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613193 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3119.16.150613197 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613197 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3120.16.150613201 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613201 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3121.16.150613205 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613205 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3122.16.150613209 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613209 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3123.16.150613213 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613213 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3124.16.150613217 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613217 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3125.16.150613221 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613221 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3126.16.150613225 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613225 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3127.16.150613229 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613229 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3128.16.150613233 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613233 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3129.16.150613237 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613237 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3130.16.150613241 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613241 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3131.16.150613245 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613245 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3132.16.150613249 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613249 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3133.16.150613253 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613253 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3134.16.150613257 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613257 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3135.16.150613261 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613261 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3136.16.150613265 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613265 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3137.16.150613269 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613269 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=2328976952 WS=128

3138.16.150613273 2004:8808:4:100:1F: 2409:40F2:217A:9130: TCP 80 54908 - 80 [ACK] Seq=150613273 Win=0 MSS=1300 SACK_PERM TSval=255274805 TSecr=232