Nmap reports 6 active hosts on the 10.168.27.0/24 network.

10.168.27.10 – Notable open ports on this host are 389/636 which are LDAP and LDAPS ports, as well as port 445 (microsoft-ds) which is a Microsoft file sharing service. These ports being open indicate this host is a Windows server/domain controller, a Windows Server OS was detected.

10.168.27.14 – Open ports are 22 for SSH and 9090 which is identified as zeus-admin. This is a Linux host.

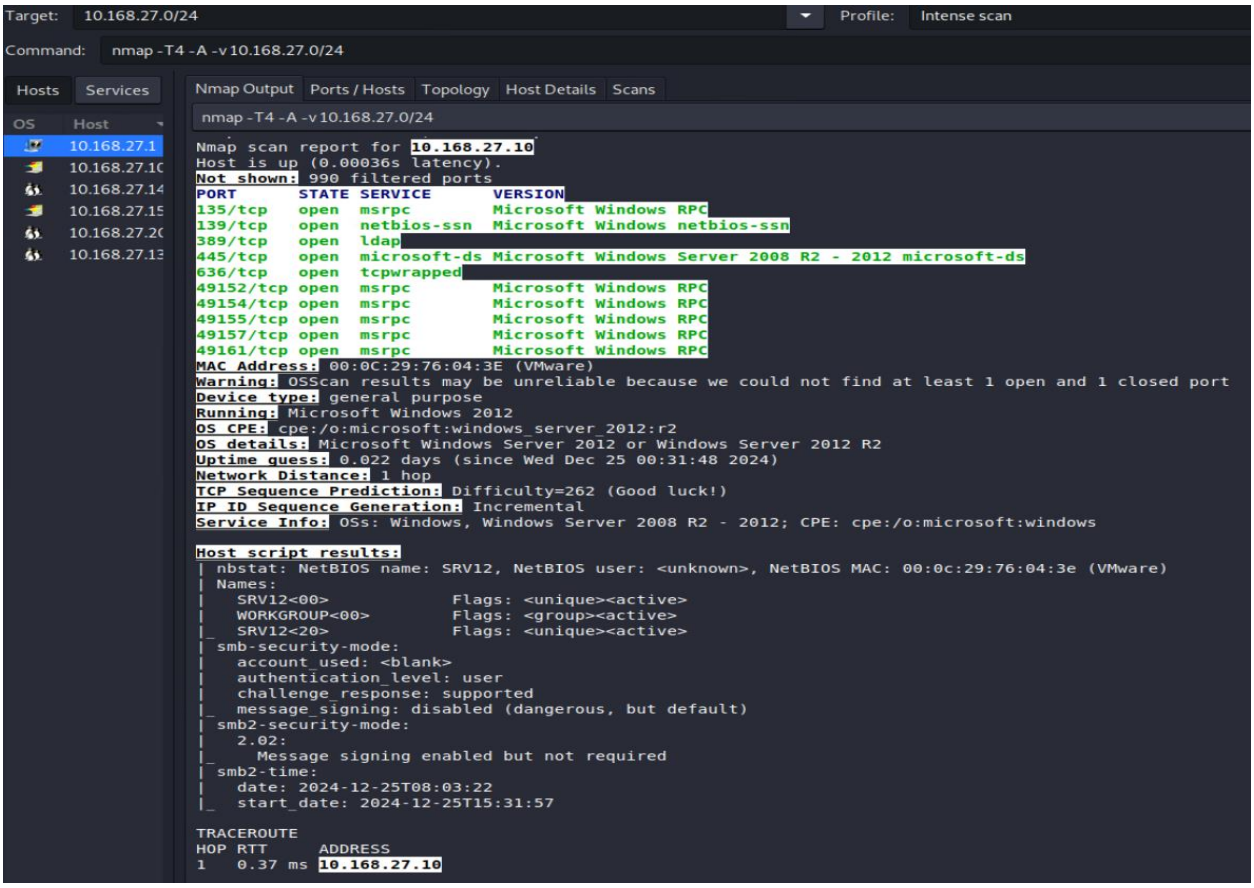
10.168.27.15 – This is a Windows host that is also open on ports 135 being msrpc, and 445 being microsoft-ds, this could be a server/workstation. This host has an FTP server open on port 21.

10.168.27.20 – This host only has one port open, 22 for SSH. No additional services could be found. This is a Linux host.

10.168.27.132 – This host also has ports 22 and 9090 open, the same as 10.167.27.14. This is also a Linux host.

10.168.27.1 – No open ports detected. This host is most likely the gateway.

To summarize, we have a gateway (10.168.27.1), a domain controller (10.168.27.10), a Windows server (10.168.27.15), and three Linux hosts. (10.168.27.14, 10.168.27.20, 10.168.27.132). Included is a screenshot of Zenmaps topology of the network, showing a star like shape with the scanning host at the center. All hosts responded to the scanning machine in one hop. This indicates that they are all on the same local subnet.



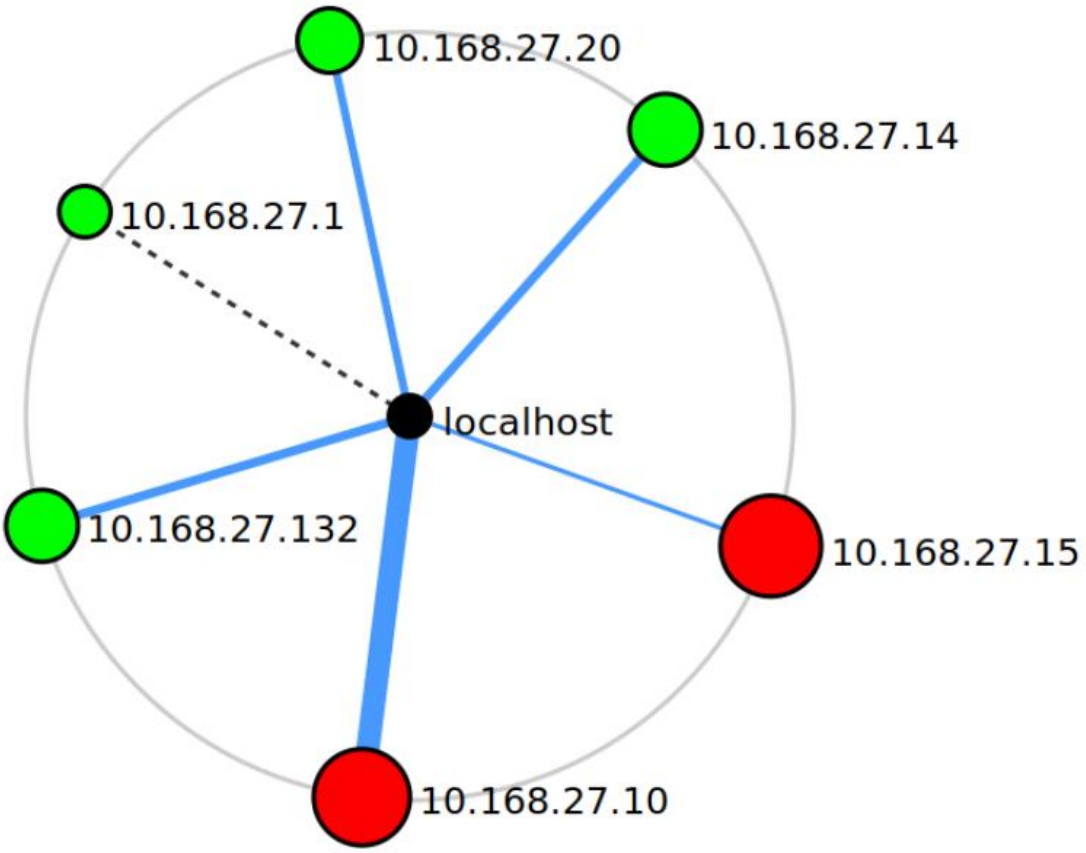

```
Nmap scan report for 10.168.27.14
Host is up (0.00029s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey:
|   1024 76:79:a0:26:2a:47:1e:e3:b8:4e:cc:1f:de:d8:0f:18 (DSA)
|_  2048 60:5e:4d:d6:85:0c:08:fb:66:df:62:80:e1:46:81:7f (RSA)
9090/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey:
|   1024 76:79:a0:26:2a:47:1e:e3:b8:4e:cc:1f:de:d8:0f:18 (DSA)
|_  2048 60:5e:4d:d6:85:0c:08:fb:66:df:62:80:e1:46:81:7f (RSA)
MAC Address: 00:0C:29:A1:62:07 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Uptime guess: 0.019 days (since Wed Dec 25 00:36:59 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.29 ms 10.168.27.14
```

```
Nmap scan report for 10.168.27.15
Host is up (0.0048s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE     VERSION
7/tcp     open  tcpwrapped
9/tcp     open  tcpwrapped
13/tcp    open  tcpwrapped
17/tcp    open  tcpwrapped
19/tcp    open  tcpwrapped
21/tcp    open  tcpwrapped
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   SYST: UNIX emulated by FileZilla
80/tcp    open  tcpwrapped
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
| http-title: IIS Windows
135/tcp   open  tcpwrapped
139/tcp   open  tcpwrapped
445/tcp   open  tcpwrapped Windows 8.1 Pro 9600 tcpwrapped
49155/tcp open  tcpwrapped
49158/tcp open  tcpwrapped
MAC Address: 00:15:5D:01:80:07 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|8|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 0.022 days (since Wed Dec 25 00:31:44 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental
```

```
Host script results:
|_clock-skew: mean: 2h39m59s, deviation: 4h37m08s, median: -1s
| nbstat: NetBIOS name: WIN8-TARGET, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:01:80:07 (Microsoft)
| Names:
|   WIN8-TARGET<20>      Flags: <unique><active>
|   WIN8-TARGET<00>      Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 8.1 Pro 9600 (Windows 8.1 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_8.1::-
|   Computer name: win8-target
|   NetBIOS computer name: WIN8-TARGET\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-12-25T00:03:22-08:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-12-25T08:03:22
|_  start_date: 2024-12-25T15:31:58

TRACEROUTE
HOP RTT     ADDRESS
1   4.79 ms 10.168.27.15
```

```
Nmap scan report for 10.168.27.20
Host is up (0.00024s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey:
|   1024 6e:4a:f1:68:b9:6a:68:fa:cb:06:8a:30:38:26:d1:aa (DSA)
|_  2048 70:8f:3c:87:ed:7f:a6:2e:20:98:08:f3:b9:69:da:71 (RSA)
MAC Address: 00:0C:29:7D:EB:8F (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Uptime guess: 0.019 days (since Wed Dec 25 00:36:31 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=253 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.24 ms 10.168.27.20

Nmap scan report for 10.168.27.132
Host is up (0.00026s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey:
|   1024 f1:b3:c0:cf:2e:ba:ea:bc:dd:b2:84:70:50:8a:b4:a1 (DSA)
|   2048 bc:01:82:d9:01:a5:8d:13:8e:ec:db:37:7b:88:82:4f (RSA)
9090/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey:
|   1024 f1:b3:c0:cf:2e:ba:ea:bc:dd:b2:84:70:50:8a:b4:a1 (DSA)
|   2048 bc:01:82:d9:01:a5:8d:13:8e:ec:db:37:7b:88:82:4f (RSA)
MAC Address: 00:0C:29:58:DF:90 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Uptime guess: 0.019 days (since Wed Dec 25 00:36:45 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.26 ms 10.168.27.132
```

```
Initiating SYN Stealth Scan at 01:04
Scanning 10.168.27.1 [1000 ports]
Completed SYN Stealth Scan at 01:04, 0.04s elapsed (1000 total ports)
Initiating Service scan at 01:04
Initiating OS detection (try #1) against 10.168.27.1
Retrying OS detection (try #2) against 10.168.27.1
NSE: Script scanning 10.168.27.1.
Initiating NSE at 01:04
Completed NSE at 01:04, 0.00s elapsed
Initiating NSE at 01:04
Completed NSE at 01:04, 0.00s elapsed
Initiating NSE at 01:04
Completed NSE at 01:04, 0.00s elapsed
Nmap scan report for 10.168.27.1
Host is up (0.000041s latency).
All 1000 scanned ports on 10.168.27.1 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

NSE: Script Post-scanning.
Initiating NSE at 01:04
Completed NSE at 01:04, 0.00s elapsed
Initiating NSE at 01:04
Completed NSE at 01:04, 0.00s elapsed
Initiating NSE at 01:04
Completed NSE at 01:04, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 111.00 seconds
           Raw packets sent: 8642 (379.366KB) | Rcvd: 5117 (213.231KB)
```



The Windows hosts have SMB/NetBIOS, microsoft-ds, and LDAP/LDAPS exposed to the external network. These are common attack targets and can be used for domain compromise. One of the Windows hosts has legacy ports open (echo, discard, daytime, etc.). These ports can be used in reflection attacks. Two of the Linux hosts are running an unknown service labeled ‘zeus-admin’, this could be a custom interface or service, but if it is misconfigured or not secure then it could be used as a target for an attack. SSH ports are open on all Linus hosts and can be open to brute force attacks if credentials are weak.

PCAP4 is the pcap file that was analyzed during the assessment. Some anomalies that were discovered were, there was a very high amount of connection reset (RST) and connection finish (FIN) activity happening in short bursts between 10.168.27.10 and 10.16.80.243. The Handshakes were incomplete or half open and were terminated almost immediately. There was no meaningful data being exchanged between the two addresses, and the connections were being made to a very wide range of ports. This activity shows that 10.16.80.243 may have been port scanning 10.168.27.10. Screenshots of the Wireshark data will also be attached.

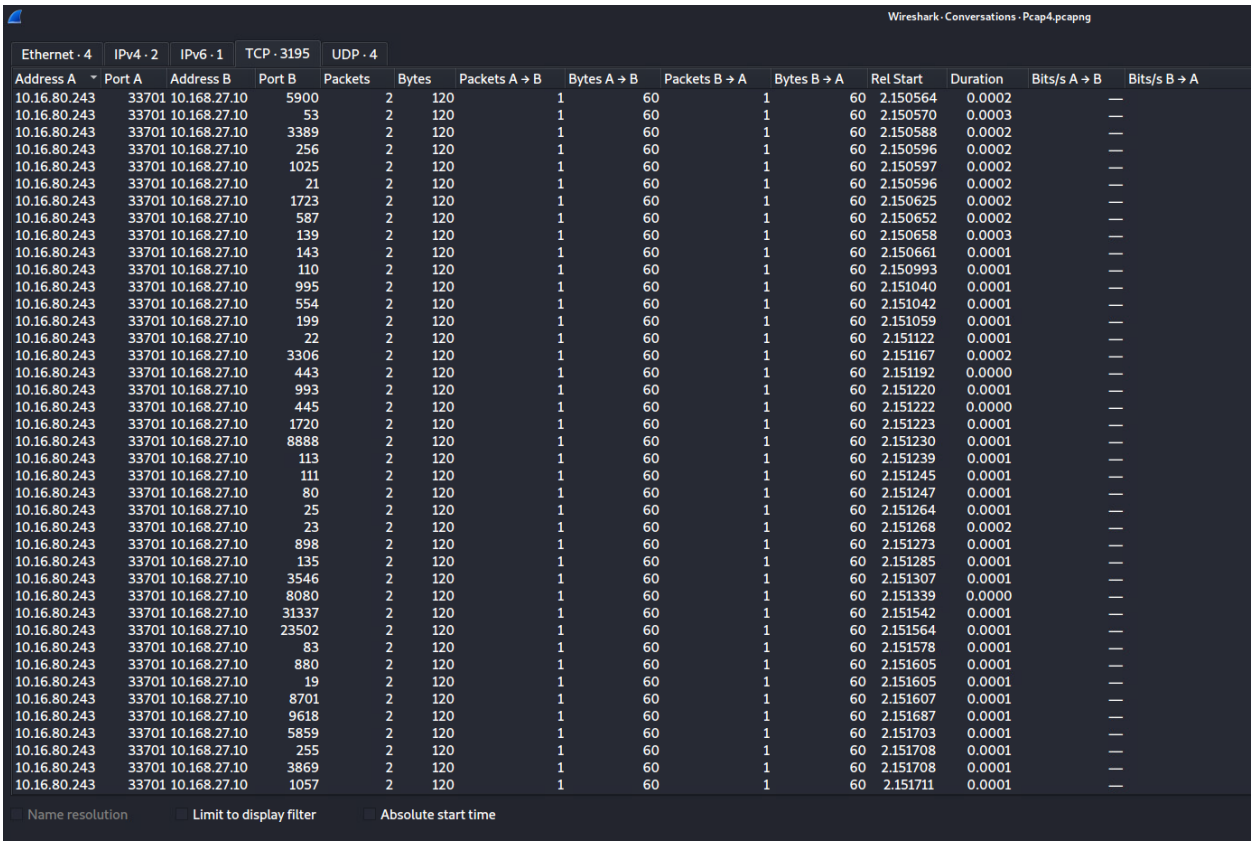
The short-lived TCP connections to a large range of ports indicates it is the activity of port scanning which can be used by attackers to discover open ports and weak services. Inaction could allow attackers to identify vulnerable services and ports to exploit. If not addressed, the spike of activity during the connection attempts could also lead to network performance issues in the short-term.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::bccb:d28:42a:…	ff02::1:2	DHCPv6	147	Solicit XID: 0x29bf43 CID: 0001000128cae9c000155d018006
2	2.046862290	Microsof_01:80:10	Broadcast	ARP	60	Who has 10.168.27.10? Tell 10.16.80.243
3	2.047052690	Microsof_01:80:06	Microsof_01:80:10	ARP	60	10.168.27.10 is at 00:15:5d:01:80:06
4	2.102397296	10.16.80.243	8.8.4.4	DNS	85	Standard query 0xddf4 PTR 10.27.168.10.in-addr.arpa
5	2.110589053	8.8.4.4	10.16.80.243	DNS	85	Standard query response 0xddf4 No such name PTR 10.27.168.10.in-addr.arpa
6	2.150564345	10.16.80.243	10.168.27.10	TCP	60	33701 → 5900 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7	2.150570343	10.16.80.243	10.168.27.10	TCP	60	33701 → 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
8	2.150588482	10.16.80.243	10.168.27.10	TCP	60	33701 → 3389 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
9	2.150596257	10.16.80.243	10.168.27.10	TCP	60	33701 → 256 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
10	2.150597405	10.16.80.243	10.168.27.10	TCP	60	33701 → 1025 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
11	2.150596499	10.16.80.243	10.168.27.10	TCP	60	33701 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
12	2.150624830	10.16.80.243	10.168.27.10	TCP	60	33701 → 1723 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
13	2.150652263	10.16.80.243	10.168.27.10	TCP	60	33701 → 587 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
14	2.150658089	10.16.80.243	10.168.27.10	TCP	60	33701 → 139 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
15	2.150661441	10.16.80.243	10.168.27.10	TCP	60	33701 → 143 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
16	2.150758909	10.168.27.10	10.16.80.243	TCP	60	5900 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
17	2.150760667	10.168.27.10	10.16.80.243	TCP	60	256 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
18	2.150760817	10.168.27.10	10.16.80.243	TCP	60	143 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
19	2.150762602	10.168.27.10	10.16.80.243	TCP	60	21 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
20	2.150762033	10.168.27.10	10.16.80.243	TCP	60	3389 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
21	2.150768379	10.168.27.10	10.16.80.243	TCP	60	1025 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
22	2.150817200	10.168.27.10	10.16.80.243	TCP	60	587 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
23	2.150852165	10.168.27.10	10.16.80.243	TCP	60	1723 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
24	2.150907340	10.168.27.10	10.16.80.243	TCP	60	53 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
25	2.150973148	10.168.27.10	10.16.80.243	TCP	60	139 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
26	2.150992683	10.16.80.243	10.168.27.10	TCP	60	33701 → 110 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
27	2.151040029	10.16.80.243	10.168.27.10	TCP	60	33701 → 995 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
28	2.151042162	10.16.80.243	10.168.27.10	TCP	60	33701 → 554 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
29	2.151057399	10.168.27.10	10.16.80.243	TCP	60	110 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
30	2.151059075	10.16.80.243	10.168.27.10	TCP	60	33701 → 199 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
31	2.151107976	10.168.27.10	10.16.80.243	TCP	60	995 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
32	2.151121967	10.16.80.243	10.168.27.10	TCP	60	33701 → 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
33	2.151166758	10.16.80.243	10.168.27.10	TCP	60	33701 → 3306 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
34	2.151171903	10.168.27.10	10.16.80.243	TCP	60	554 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
35	2.151173802	10.168.27.10	10.16.80.243	TCP	60	199 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
36	2.151191997	10.16.80.243	10.168.27.10	TCP	60	33701 → 443 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
37	2.151194152	10.168.27.10	10.16.80.243	TCP	60	22 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
38	2.151220468	10.16.80.243	10.168.27.10	TCP	60	33701 → 993 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
39	2.151221912	10.16.80.243	10.168.27.10	TCP	60	33701 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
40	2.151223292	10.16.80.243	10.168.27.10	TCP	60	33701 → 1720 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
41	2.151230426	10.16.80.243	10.168.27.10	TCP	60	33701 → 8888 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
42	2.151233489	10.168.27.10	10.16.80.243	TCP	60	443 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
43	2.151238691	10.168.27.10	10.16.80.243	TCP	60	113 → 33701 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
44	2.151245230	10.16.80.243	10.168.27.10	TCP	60	33701 → 111 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
45	2.151247033	10.16.80.243	10.168.27.10	TCP	60	33701 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
46	2.151263623	10.16.80.243	10.168.27.10	TCP	60	33701 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
47	2.151268182	10.16.80.243	10.168.27.10	TCP	60	33701 → 23 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
48	2.151270078	10.168.27.10	10.16.80.243	TCP	60	445 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
49	2.151272924	10.16.80.243	10.168.27.10	TCP	60	33701 → 898 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
50	2.151285339	10.168.27.10	10.16.80.243	TCP	60	135 → 33701 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
51	2.151307277	10.16.80.243	10.168.27.10	TCP	60	33701 → 3546 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

```
▸ Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: Microsof_01:80:06 (00:15:5d:01:80:06), Dst: Microsof_01:80:10 (00:15:5d:01:80:10)
▸ Internet Protocol Version 4, Src: 10.168.27.10, Dst: 10.16.80.243
▸ Transmission Control Protocol, Src Port: 5900, Dst Port: 33701, Seq: 1, Ack: 2, Len: 0
```

Wireshark · Expert Information · Pcap4.pcapng

Severity	Summary	Group	Protocol	Count
▸ Warning	Connection reset (RST)	Sequence	TCP	3000
▸ Chat	Connection finish (FIN)	Sequence	TCP	3195



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.16.80.243	33701	10.168.27.10	5900	2	120	1	60	1	60	2.150564	0.0002	—	
10.16.80.243	33701	10.168.27.10	53	2	120	1	60	1	60	2.150570	0.0003	—	
10.16.80.243	33701	10.168.27.10	3389	2	120	1	60	1	60	2.150588	0.0002	—	
10.16.80.243	33701	10.168.27.10	256	2	120	1	60	1	60	2.150596	0.0002	—	
10.16.80.243	33701	10.168.27.10	1025	2	120	1	60	1	60	2.150597	0.0002	—	
10.16.80.243	33701	10.168.27.10	21	2	120	1	60	1	60	2.150596	0.0002	—	
10.16.80.243	33701	10.168.27.10	1723	2	120	1	60	1	60	2.150625	0.0002	—	
10.16.80.243	33701	10.168.27.10	587	2	120	1	60	1	60	2.150652	0.0002	—	
10.16.80.243	33701	10.168.27.10	139	2	120	1	60	1	60	2.150658	0.0003	—	
10.16.80.243	33701	10.168.27.10	143	2	120	1	60	1	60	2.150661	0.0001	—	
10.16.80.243	33701	10.168.27.10	110	2	120	1	60	1	60	2.150993	0.0001	—	
10.16.80.243	33701	10.168.27.10	995	2	120	1	60	1	60	2.151040	0.0001	—	
10.16.80.243	33701	10.168.27.10	554	2	120	1	60	1	60	2.151042	0.0001	—	
10.16.80.243	33701	10.168.27.10	199	2	120	1	60	1	60	2.151059	0.0001	—	
10.16.80.243	33701	10.168.27.10	22	2	120	1	60	1	60	2.151122	0.0001	—	
10.16.80.243	33701	10.168.27.10	3306	2	120	1	60	1	60	2.151167	0.0002	—	
10.16.80.243	33701	10.168.27.10	443	2	120	1	60	1	60	2.151192	0.0000	—	
10.16.80.243	33701	10.168.27.10	993	2	120	1	60	1	60	2.151220	0.0001	—	
10.16.80.243	33701	10.168.27.10	445	2	120	1	60	1	60	2.151222	0.0000	—	
10.16.80.243	33701	10.168.27.10	1720	2	120	1	60	1	60	2.151223	0.0001	—	
10.16.80.243	33701	10.168.27.10	8888	2	120	1	60	1	60	2.151230	0.0001	—	
10.16.80.243	33701	10.168.27.10	113	2	120	1	60	1	60	2.151239	0.0001	—	
10.16.80.243	33701	10.168.27.10	111	2	120	1	60	1	60	2.151245	0.0001	—	
10.16.80.243	33701	10.168.27.10	80	2	120	1	60	1	60	2.151247	0.0001	—	
10.16.80.243	33701	10.168.27.10	25	2	120	1	60	1	60	2.151264	0.0001	—	
10.16.80.243	33701	10.168.27.10	23	2	120	1	60	1	60	2.151268	0.0002	—	
10.16.80.243	33701	10.168.27.10	898	2	120	1	60	1	60	2.151273	0.0001	—	
10.16.80.243	33701	10.168.27.10	135	2	120	1	60	1	60	2.151285	0.0001	—	
10.16.80.243	33701	10.168.27.10	3546	2	120	1	60	1	60	2.151307	0.0001	—	
10.16.80.243	33701	10.168.27.10	8080	2	120	1	60	1	60	2.151339	0.0000	—	
10.16.80.243	33701	10.168.27.10	31337	2	120	1	60	1	60	2.151542	0.0001	—	
10.16.80.243	33701	10.168.27.10	23502	2	120	1	60	1	60	2.151564	0.0001	—	
10.16.80.243	33701	10.168.27.10	83	2	120	1	60	1	60	2.151578	0.0001	—	
10.16.80.243	33701	10.168.27.10	880	2	120	1	60	1	60	2.151605	0.0001	—	
10.16.80.243	33701	10.168.27.10	19	2	120	1	60	1	60	2.151605	0.0001	—	
10.16.80.243	33701	10.168.27.10	8701	2	120	1	60	1	60	2.151607	0.0001	—	
10.16.80.243	33701	10.168.27.10	9618	2	120	1	60	1	60	2.151687	0.0001	—	
10.16.80.243	33701	10.168.27.10	5859	2	120	1	60	1	60	2.151703	0.0001	—	
10.16.80.243	33701	10.168.27.10	255	2	120	1	60	1	60	2.151708	0.0001	—	
10.16.80.243	33701	10.168.27.10	3869	2	120	1	60	1	60	2.151708	0.0001	—	
10.16.80.243	33701	10.168.27.10	1057	2	120	1	60	1	60	2.151711	0.0001	—	

Recommended solutions for vulnerabilities found in Nmap:

Apply the latest updates to address vulnerabilities in SMB and LDAP, this reduces the risk of known exploits targeting unpatched services (NIST, 2020). Implement LDAPS by securing LDAP with SSL/TLS to protect authentication traffic (Microsoft, 2024). Disable unnecessary legacy/diagnostic ports (echo, discard, daytime, qotd, chargen) (CIS, 2024). Replace FTP with SFTP to prevent cleartext credential exposure (SANS Institute, 2002). Linux hosts should disable root login via SSH and enforce key based authentication (CIS, 2024). Investigate the custom service labeled ‘zeus-admin’ for any vulnerabilities, if it is necessary then restrict access to a trusted network.

Recommended solutions for Wireshark anomalies:

Deploy a network-based IDS/IPS such as Snort or Suricata to detect port scans and block malicious hosts (SANS Institute, 2015) and configure alerting rules so that repeated half-open connections on ports trigger notifications and alerts (CIS, 2024). Implementing a firewall and adding rules to allow inbound traffic only on necessary ports, as well as blocking all others by default (NIST, 2020). Review and audit logs regularly for repeated RST/FIN bursts or any suspicious scanning (Microsoft, 2021).

References:

Center for Internet Security (CIS). (2024). *CIS Critical Security Controls Navigator* https://www.cisecurity.org/controls/cis-controls-navigator

Microsoft. (2024). *LDAP over SSL (LDAPS) Configuration*. https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/enable-ldap-over-ssl-3rd-certification-authority

Microsoft. (2021). *Windows Security Auditing* https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/security-auditing-overview

National Institute of Standards and Technology (NIST). (2020). *NIST SP 800-53 Rev. 5* https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

SANS Institute (2002). *Securing FTP Authentication*. https://www.sans.org/white-papers/374/

SANS Institute. (2015). *Following a Breach Simulating and Detecting a Common Attack* https://www.sans.org/white-papers/36157/