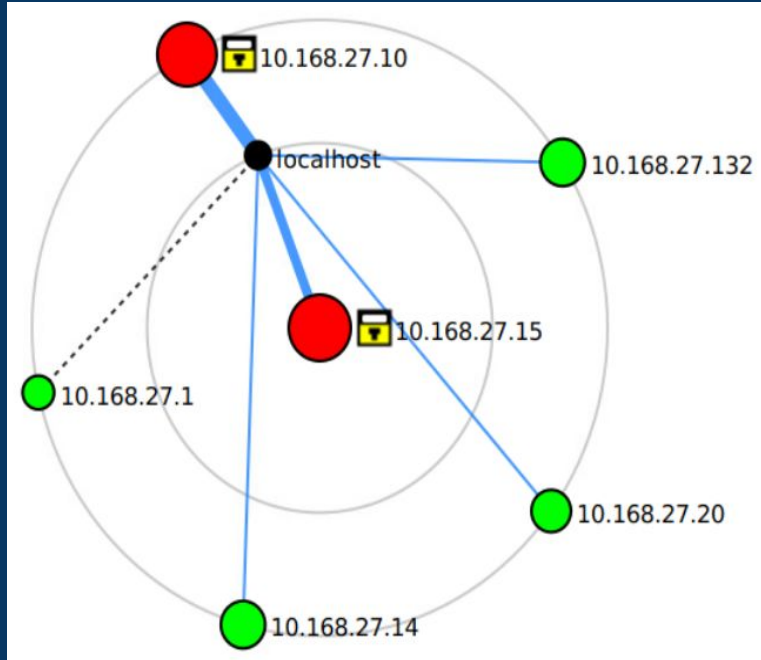


# Nmap Scan Results

## A: Topology



## Description

The scanned network appears to be using a star topology where five hosts are connected to a single central device totalling in six nodes, 10.168.27.1 which serves as the primary connection point and or gateway for each host, this can be assumed since all hosts take only one hop to reach this device.

The central device, which zenmap did not recognize as a switch or a router, seems to act as the core of the network, though it lacks identifiable routing capabilities or OS fingerprints. Connected to the network Two hosts, 10.168.27.10 and 10.168.27.15, exhibit a great security risk, with zenmap reporting that each host has more than six ports open including filtered ports, indicating only some security configurations have been made. The remaining three hosts report in as having fewer than three open ports, with no port filtering, which could suggest a less complex setup and fewer points of access.

This star topology allows each host to communicate through the central device, making it a potential single point of failure if compromised, and suggests a lack of advanced traffic management from a switch or router. Based on the lack of information zenmap is able to provide us we can assume the central device is either a hub, unmanaged switch, or a managed switch with little to no configuration .

# Nmap Scan Results

## B: Vulnerabilities: Unused IP Addresses

```
Nmap Output | Ports / Hosts | Topology | Host Details | Scans
nmap -T4 -A -v 10.168.27.0/24

Starting Nmap 7.91 ( https://nmap.org ) at 2024-10-29 22:48 MDT
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:48
Completed NSE at 22:48, 0.00s elapsed
Initiating NSE at 22:48
Completed NSE at 22:48, 0.00s elapsed
Initiating NSE at 22:48
Completed NSE at 22:48, 0.00s elapsed
Initiating ARP Ping Scan at 22:48
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 22:48, 1.95s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 5 hosts. at 22:48
Completed Parallel DNS resolution of 5 hosts. at 22:48, 0.00s elapsed
Nmap scan report for 10.168.27.0 [host down]
Nmap scan report for 10.168.27.2 [host down]
Nmap scan report for 10.168.27.3 [host down]
Nmap scan report for 10.168.27.4 [host down]
Nmap scan report for 10.168.27.5 [host down]
Nmap scan report for 10.168.27.6 [host down]
Nmap scan report for 10.168.27.7 [host down]
Nmap scan report for 10.168.27.8 [host down]
Nmap scan report for 10.168.27.9 [host down]
Nmap scan report for 10.168.27.11 [host down]
Nmap scan report for 10.168.27.12 [host down]
Nmap scan report for 10.168.27.13 [host down]
```

## Description

Upon scanning the network it was evident that the IP range is much larger than necessary given the fact that there is only 5 active hosts. Some of the vulnerabilities present in the network could be attributed to having a large range of unused IP addresses, which, if unmanaged, increases the network's attack surface (SparkNAV).

Unused IPs offer attackers more opportunities to assign unauthorized devices IPs within the network or impersonate legitimate hosts, enabling potential IP spoofing and man-in-the-middle attacks. Furthermore, these unused addresses aid attackers during reconnaissance, as they provide insights into the network's scope and infrastructure. This can lead to a clearer understanding of active devices and potential targets. Additionally, poor management of IP addresses can cause confusion in network monitoring, making it challenging to detect unauthorized devices and creating loopholes that serve as potential backdoors.

If these vulnerabilities are not addressed, attackers could gain unauthorized access, establish persistence in the network, and potentially exploit misconfigured or exposed services, jeopardizing data integrity and network security

# Nmap Scan Results

B: Vulnerabilities: Host 10.168.27.10

```
Nmap scan report for 10.168.27.10
Host is up (0.00032s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
636/tcp   open  tcpwrapped
49152/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49157/tcp open  msrpc            Microsoft Windows RPC
49161/tcp open  msrpc            Microsoft Windows RPC
MAC Address: 00:0C:29:07:8F:45 (VMware)
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 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Uptime guess: 0.014 days (since Tue Oct 29 22:31:06 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

## Description

The host system 10.168.27.10, operating Windows Server 2012 but also configured with a legacy Windows Server 2008 services, is highly vulnerable due to multiple open ports and outdated protocols.

This host has five open high-numbered dynamic ports (49152, 49154, 49155, 49157, 49161), all running Microsoft Windows RPC (MSRPC) services, along with exposed NetBIOS (port 139) and SMB (port 445). The open RPC ports increase the attack surface by potentially allowing unauthorized users to access or manipulate network services, while NetBIOS and SMB leave the system vulnerable to network enumeration and other known exploits. Given the likelihood of SMBv1 being active, this host is exposed to severe vulnerabilities like EternalBlue, which has been exploited in ransomware attacks such as WannaCry.

Additionally, because the system relies on outdated Windows Server 2008 components, it lacks recent security patches, making it susceptible to remote code execution, lateral movement, and data breaches (MITRE Corporation). Without strict access controls, firewall restrictions, or network segmentation, this host poses a substantial risk to its environment, leaving it open to both external and internal threats.

# Nmap Scan Results

## B: Vulnerabilities:

Hosts 10.168.27.14, 10.168.27.20 and, 10.168.27.132

```
Nmap scan report for 10.168.27.14
Host is up (0.00018s 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)
```

```
Nmap scan report for 10.168.27.20
Host is up (0.00018s 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)
```

```
Nmap scan report for 10.168.27.132
Host is up (0.00018s 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)
```

## Description

Hosts 10.168.27.14 & 10.168.27.132, with two open SSH ports (22 and 9090) and, Host 10.168.27.20 (port: 22) are all running an outdated OpenSSH 5.5p1 version, which all present several security vulnerabilities to both the clients and network. By exposing SSH on both the standard port 22 and an additional non-standard port 9090, both hosts double their attack surface, making them more susceptible to brute-force attacks and automated scans targeting SSH services.

Additionally, Nmap indicates that the RSA and DSA host keys are exactly the same across both instances where the client has multiple ports open, which compounds the risk; compromising one port could allow attackers to gain access to the other. The use of DSA keys, which are known to be weak by today's standards, further increases the network's security risks, since they're more vulnerable to computational attacks compared to modern key types.

Running this older version of OpenSSH also suggests a lack of recent patches, leaving the hosts open to known exploits targeting OpenSSH 5.5, which may permit unauthorized access or man-in-the-middle attacks. Upgrading OpenSSH, consolidating SSH access to a single, secure port, and removing outdated keys are crucial steps to reduce these vulnerabilities.



# Nmap Scan Results

B: Vulnerabilities: Host 10.168.27.15

```
Nmap scan report for 10.168.27.15
Host is up (0.00023s latency).
Not shown: 987 filtered ports
```

PORT	STATE	SERVICE	VERSION
7/tcp	open	echo	
9/tcp	open	discard?	
13/tcp	open	daytime	Microsoft Windows USA daytime
17/tcp	open	qotd	Windows qotd (English)
19/tcp	open	chargen	
21/tcp	open	ftp	FileZilla ftpd

```
| 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    http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| 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	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows 8.1 Pro 9600 microsoft-ds (workg
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC
49158/tcp	open	msrpc	Microsoft Windows RPC

## Description

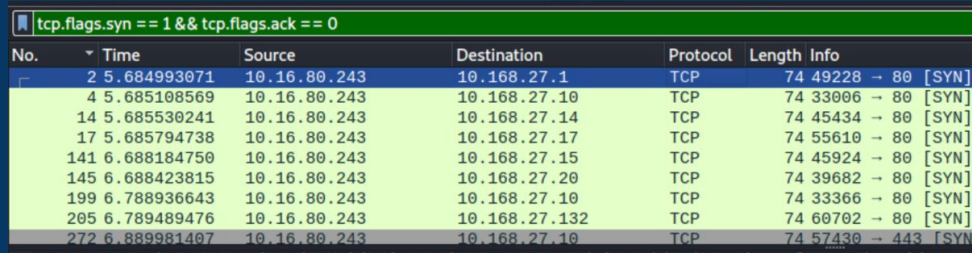
Host 10.168.27.15 is running either Windows 7, 8, or Vista, which is exposed to a range of significant security vulnerabilities due to the large number of open ports and services, many of which are outdated or risky. With port 7 (echo) open, the host is susceptible to ping flood and reflection attacks, where attackers can exploit the echo service to amplify traffic and cause denial-of-service (DoS). The presence of FTP on port 21 with anonymous login enabled (FTP code 230) further weakens security by allowing any user unrestricted access to potentially sensitive files stored on the client, a major entry point for unauthorized access and malicious activity.

The HTTP service on port 80, identified as Microsoft HTTPAPI httpd 2.0, supporting a range of methods (OPTIONS, TRACE, GET, HEAD, POST), TRACE, is of particular importance since it be leveraged in cross-site tracing (XST) attacks that reveal sensitive information in HTTP headers, making the host more vulnerable to client-side exploitation. Additionally, NetBIOS on port 139 opens the system to network enumeration, enabling attackers to gather details about shared resources, usernames, and other network assets.

The presence of three MSRPC services running on dynamic ports further increases the risk of remote code execution attacks, particularly in outdated systems like Windows 7, 8, or Vista, which are end-of-life OS and lack critical security patches. Combined, these risks create a substantial attack surface, making the host vulnerable to unauthorized access, data leakage, and exploitation.

# WireShark Pcap1 Analysis

## C:Anomalies: Port Scanning

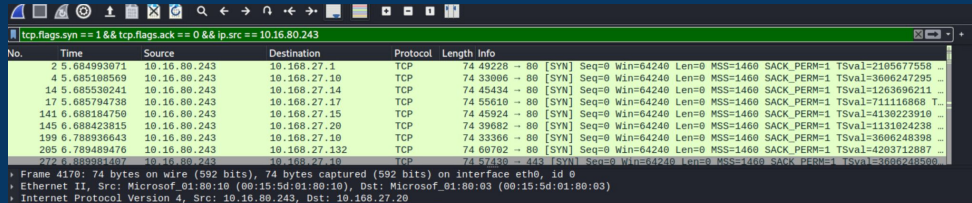


tcp.flags.syn == 1 && tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
2	5.684993071	10.16.80.243	10.168.27.1	TCP	74	49228 → 80 [SYN]
4	5.685108569	10.16.80.243	10.168.27.10	TCP	74	33006 → 80 [SYN]
14	5.685530241	10.16.80.243	10.168.27.14	TCP	74	45434 → 80 [SYN]
17	5.685794738	10.16.80.243	10.168.27.17	TCP	74	55610 → 80 [SYN]
141	6.688184750	10.16.80.243	10.168.27.15	TCP	74	45924 → 80 [SYN]
145	6.688423815	10.16.80.243	10.168.27.20	TCP	74	39682 → 80 [SYN]
199	6.788936643	10.16.80.243	10.168.27.10	TCP	74	33366 → 80 [SYN]
205	6.789489476	10.16.80.243	10.168.27.132	TCP	74	60702 → 80 [SYN]
272	6.889981407	10.16.80.243	10.168.27.10	TCP	74	57430 → 443 [SYN]

## Description

Analyzing file Pcap1 in Wireshark reveals many anomalies within this packet capture file, the first being port scanning. Using a few display filters like `tcp.flags.syn == 1 && tcp.flags.ack == 0` filters packets so that we may see SYN packets without ACK responses, which is a common sign of port scanning. This heavily suggests that the file recorded extensive port scanning on the network due to the large amount of packets meeting the filter's criteria, which gives us a range of 45,852/219,377 to be exact (Packet Range 2-219,346).



tcp.flags.syn == 1 && tcp.flags.ack == 0 && ip.src == 10.16.80.243

No.	Time	Source	Destination	Protocol	Length	Info
2	5.684993071	10.16.80.243	10.168.27.1	TCP	74	49228 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2105677558
4	5.685108569	10.16.80.243	10.168.27.10	TCP	74	33006 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3606247295
14	5.685530241	10.16.80.243	10.168.27.14	TCP	74	45434 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1263696211
17	5.685794738	10.16.80.243	10.168.27.17	TCP	74	55610 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=711116868
141	6.688184750	10.16.80.243	10.168.27.15	TCP	74	45924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4130223910
145	6.688423815	10.16.80.243	10.168.27.20	TCP	74	39682 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1131024238
199	6.788936643	10.16.80.243	10.168.27.10	TCP	74	33366 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3606248398
205	6.789489476	10.16.80.243	10.168.27.132	TCP	74	60702 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4263712807
272	6.889981407	10.16.80.243	10.168.27.10	TCP	74	57430 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3606248398

Frame 4170: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0  
Ethernet II, Src: Microsoft\_01:80:10 (00:15:5d:01:80:10), Dst: Microsoft\_01:80:03 (00:15:5d:01:80:03)  
Internet Protocol Version 4, Src: 10.16.80.243, Dst: 10.168.27.20

Further analysis also unveils that almost all of the port scanning traffic was generated by host 10.16.80.243, who was scanning multiple hosts on the network across many other network segments. 45,823 out of 45,852 packets were generated by this host when we add an additional filter to the originally used one above. By adding `&& ip.src == 10.16.80.243` We find out exactly how many packets (45,823) were sent by the host by using its IP address 10.16.80.243 to match it with packets displaying signs of port scanning (Packet Range 2-219,346).

# WireShark Pcap1 Analysis

C:**Anomalies**: Denial of Service or Network Loop

## Description

Ethernet · 9	IPv4 · 33	IPv6	TCP · 45781	UDP							
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	
10.16.80.243	10.168.27.1	1,002	74k	1,002	74k	0	0	5.684993	232.8292	2,547	
10.16.80.243	10.168.27.10	40,743	3,014k	40,743	3,014k	0	0	5.685109	1881.0778	12k	
10.16.80.243	10.168.27.14	1,011	74k	1,011	74k	0	0	5.685530	233.0691	2,567	
10.16.80.243	10.168.27.17	1,002	74k	1,002	74k	0	0	5.685795	232.8283	2,547	
10.16.80.243	10.168.27.15	8	592	8	592	0	0	6.688185	225.6374	20	
10.16.80.243	10.168.27.20	1,011	74k	1,011	74k	0	0	6.688424	232.0663	2,579	
10.16.80.243	10.168.27.132	1,013	74k	1,013	74k	0	0	6.789489	231.9650	2,585	
10.16.80.243	54.195.65.131	3	222	3	222	0	0	911.886707	51.0592	34	

While still using the filters from the previous slide,  
``tcp.flags.syn == 1 && tcp.flags.ack == 0 && ip.src == 10.16.80.243``

We can see from the Statistics> Conversations window that host 10.16.80.243 was able to access and pay special attention to a host on another network segment using the IP 10.168.27.10 . Address:A sent over 40,000 packets to Address:B totaling in only 12Kbits over 1880.07seconds or 31.3minutes.

These metrics allow us to safely assume one of two things is happening. First scenario is if host 10.16.80.243 is a known device on the network it could mean that it is misconfigured and might be experiencing a loop while trying to connect to 10.168.27.10 through an automated process. This however, seems unlikely given that host 10.16.80.243 generated 5k+ other packets matching the criteria of SYN=1/ACK=0 again, suggesting port scanning especially since the filter reports 10.16.80.243 sending this packets across almost every other IP in the network.

The second scenario and most likely is that host 10.16.80.243 was conducting a SYN Flood Attack as a form of DoS Attack, given the host's previous telemetry and its duration of 31minutes (Packet Range 2-219,346).

# WireShark Pcap1 Analysis

C:**Anomalies**: Traffic on Unsecured Ports

## Description

The network activity between Address A (10.16.80.243) and Address B (10.168.27.10) stands out due to repeated small bursts of traffic—1 to 10 packets each—sent over port 80 a total of 36 times.

This pattern is unusual since legitimate HTTP connections either establish longer sessions with larger data transfers like visiting a website or terminate after a brief exchange. These repetitive, low-packet connections could indicate that a automated web scanner is probing 10.168.27.10 for information or vulnerabilities without fully engaging in prolonged communication.

Alternatively, it may suggest intermittent connection failures, where 10.16.80.243 is attempting to reach a web service that's unresponsive or partially blocked. This anomaly warrants further analysis to determine whether it's part of legitimate testing/debugging activities or potentially malicious reconnaissance but, given the source address 10.16.80.243 and the history we've uncovered in previous analysis it is likely an unknown device on the network scanning and probing for information on devices native to the network (Packet Range 4-219,286).

tcp.port == 80    udp.port == 80 && ip.dst == 10.168.27.10					
No.	Time	Source	Destination	Protocol	
16280	573.066113077	10.16.80.243	10.168.27.10	HTTP	
16282	573.066183172	10.16.80.243	10.168.27.10	HTTP	
16284	573.066264347	10.16.80.243	10.168.27.10	HTTP	
16285	573.066319192	10.16.80.243	10.168.27.10	HTTP	
16294	573.068722905	10.16.80.243	10.168.27.10	TCP	
16298	573.069332756	10.16.80.243	10.168.27.10	TCP	
16306	573.089913049	10.16.80.243	10.168.27.10	TCP	
16307	573.090289733	10.16.80.243	10.168.27.10	TCP	
16312	573.090526806	10.16.80.243	10.168.27.10	TCP	

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	I
10.16.80.243	47088	10.168.27.10	80	1	74	1	74	0	1
10.16.80.243	47090	10.168.27.10	80	3	208	2	134	1	1
10.16.80.243	47120	10.168.27.10	80	4	280	3	206	1	1
10.16.80.243	49684	10.168.27.10	80	9	1,604	5	356	4	4
10.16.80.243	49984	10.168.27.10	80	10	1,340	6	564	4	4
10.16.80.243	49986	10.168.27.10	80	10	1,871	6	620	4	4
10.16.80.243	50004	10.168.27.10	80	10	1,488	6	712	4	4
10.16.80.243	50008	10.168.27.10	80	10	1,354	6	578	4	4
10.16.80.243	50010	10.168.27.10	80	10	1,419	6	569	4	4
10.16.80.243	50012	10.168.27.10	80	10	1,419	6	569	4	4
10.16.80.243	50014	10.168.27.10	80	10	1,053	6	558	4	4
10.16.80.243	50016	10.168.27.10	80	10	1,339	6	563	4	4
10.16.80.243	50022	10.168.27.10	80	10	1,053	6	558	4	4
10.16.80.243	50028	10.168.27.10	80	10	1,670	6	422	4	4
10.16.80.243	50034	10.168.27.10	80	10	1,340	6	564	4	4
10.16.80.243	50036	10.168.27.10	80	10	1,381	6	555	4	4
10.16.80.243	50038	10.168.27.10	80	10	1,111	6	616	4	4
10.16.80.243	50046	10.168.27.10	80	10	1,796	6	1,020	4	4
10.16.80.243	50050	10.168.27.10	80	10	1,341	6	565	4	4
10.16.80.243	50052	10.168.27.10	80	10	1,438	6	588	4	4
10.16.80.243	50054	10.168.27.10	80	10	1,335	6	559	4	4



# WireShark Pcap1 Analysis

## C:Anomalies: LDAPS Query Flood

Wireshark - Conversations - Pcap1.pcapng

Ethernet - 9	IPv4 - 33	IPv6	TCP - 45781	UDP							
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
10.16.80.243	54920	10.168.27.10	636	5	857	3	723	2	134 598.702497	0.0005	
10.16.80.243	54922	10.168.27.10	636	5	857	3	723	2	134 598.703110	0.0004	
10.16.80.243	54924	10.168.27.10	636	5	857	3	723	2	134 598.703608	0.0004	
10.16.80.243	54926	10.168.27.10	636	5	857	3	723	2	134 598.704120	0.0004	
10.16.80.243	54928	10.168.27.10	636	5	857	3	723	2	134 598.704645	0.0004	
10.16.80.243	54930	10.168.27.10	636	5	857	3	723	2	134 598.705119	0.0004	
10.16.80.243	54932	10.168.27.10	636	5	857	3	723	2	134 598.705604	0.0004	
10.16.80.243	54934	10.168.27.10	636	5	857	3	723	2	134 598.706079	0.0004	
10.16.80.243	54936	10.168.27.10	636	5	857	3	723	2	134 598.706574	0.0004	
10.16.80.243	54938	10.168.27.10	636	5	857	3	723	2	134 598.707052	0.0004	
10.16.80.243	54940	10.168.27.10	636	5	857	3	723	2	134 598.707516	0.0004	
10.16.80.243	54942	10.168.27.10	636	5	857	3	723	2	134 598.708019	0.0004	
10.16.80.243	54944	10.168.27.10	636	5	857	3	723	2	134 598.708490	0.0004	
10.16.80.243	54946	10.168.27.10	636	5	857	3	723	2	134 598.708980	0.0004	
10.16.80.243	54948	10.168.27.10	636	5	857	3	723	2	134 598.709448	0.0004	
10.16.80.243	54950	10.168.27.10	636	5	857	3	723	2	134 598.709931	0.0056	
10.16.80.243	54952	10.168.27.10	636	5	857	3	723	2	134 598.715606	0.0004	
10.16.80.243	54954	10.168.27.10	636	5	857	3	723	2	134 598.716091	0.0004	
10.16.80.243	54956	10.168.27.10	636	5	857	3	723	2	134 598.716587	0.0004	
10.16.80.243	54958	10.168.27.10	636	5	857	3	723	2	134 598.717057	0.0005	
10.16.80.243	54960	10.168.27.10	636	5	857	3	723	2	134 598.717602	0.0004	

## Description

Activity between host 10.16.80.243 and host 10.168.27.10 over port 636 highlights a concerning anomaly, with 39,000+ connection attempts over LDAPS (LDAP over SSL), each involving only 5 packets and an extremely brief duration of 0.0004 seconds. The excessive volume of LDAPS traffic is far beyond what's considered typical usage, even for automated directory queries, and suggests a possible attempt to exploit the directory service on 10.168.27.10. This volume of rapid, repeated connections may indicate a brute-force attack, credential stuffing, or a mass query attempt to extract sensitive directory data.

Furthermore, the fact that 10.16.80.243 was previously observed scanning other devices on the network raises the likelihood of malicious intent from this user. The combination of excessive traffic and previous reconnaissance behavior suggests that 10.16.80.243 may be engaged in an active directory exploitation attempt, or preparing for a larger attack both posing a significant risk to the directory server's availability, confidentiality, and integrity of its data (Packet Range 2-219,346).

# D:Implications of Anomalies

## Port Scanning Activity

Lack of remediation in response to the port scanning activity conducted by host 10.16.80.243, could have significant security implications. Firstly it increases network vulnerability exposure, port scanning is typically a precursor to more serious attacks, as it allows attackers to map out open and potentially vulnerable ports on network connected devices. By ignoring this behavior, an attacker may discover exploitable services on misconfigured devices and move forward with targeted attacks like unauthorized access, data exfiltration, or service disruptions.

Second, network performance and resource impact should be a major concern if this network is involved in operational processes as availability becomes an issue due to another anomaly found of a high volume of SYN packets without ACK responses can strain network resources and affect performance, especially when repeated over time. This results in a slow down of network resources, disrupts legitimate traffic, and even leads to denial-of-service (DoS) attacks.

Lastly, the scanning host could be engaging in reconnaissance efforts unchallenged, if left unchecked. Without addressing this anomaly, security teams might miss the opportunity to identify and mitigate risks early in the attack chain, allowing potential attackers to better understand and exploit vulnerabilities in the network's defenses.

In summary, failure to address this potentially malicious activity of port scanning could lead to escalated attacks, performance degradation, and a missed chance to preemptively secure the network.

# D:Implications of Anomalies

## DoS or Network Loop

Regarding traffic that suggests a potential SYN Flood Attack by host 10.16.80.243, there are a multitude of issues that are a concern for network security.

The first being Denial of Service (DoS) risk, a SYN Flood Attack, if allowed to continue, can overload the target system (in this case, 10.168.27.10), potentially leaving it unresponsive to legitimate incoming traffic. This could disrupt essential services and devices or critical network functions, causing downtime for users and impacting business operations that are reliant on the network's availability.

Activity of this sort on a network generally leads to broader network instability the high volume of packets generated by 10.16.80.243 can strain network resources, especially if it's scanning across multiple IPs and segments. This could degrade overall network performance and even spread disruptions if the attacker targets additional hosts, leading to a larger-scale DoS scenario. Ignoring this activity may embolden the attacker(s) to escalate their actions. Following reconnaissance and initial DoS attempts, the attacker might attempt further exploits or attacks on identified weak points since their unobtrusive generation of telemetry goes freely without security teams responding.

According to the Center for Internet Security, "EternalBlue is an exploit designed to attack SMB (Server Message Block) file and print sharing services on the affected Windows versions" which is running on host 10.168.27.10 (Center for Internet Security). This highlights the critical need to update or decommission legacy services to mitigate such vulnerabilities on the network.

The undetected malicious presence of 10.16.80.243 is very obviously an unauthorized or compromised device, leaving it unchecked allows the attacker to remain on the network indefinitely, which increases the likelihood of further attacks or persistence mechanisms being deployed. In summary, failing to act on this suspected SYN Flood Attack can lead to service disruptions, increased network instability, potential escalation of attacks, and prolonged unauthorized access by a potential attacker.

# D:Implications of Anomalies

## Network Activity Over Unsecured Ports

HTTP traffic from 10.16.80.243 to 10.168.27.10 has been identified to have suspicious qualities, there are several possible consequences to abstaining from action in response to this newly identified anomaly.

Repeated, low-data connections over HTTP (port 80) likely indicate reconnaissance efforts by an automated scanner controlled by a potential threat actor. If unaddressed, the probing could help the attacker identify exploitable vulnerabilities on 10.168.27.10, potentially leading to unauthorized access or further attacks targeting weaknesses uncovered during the attackers scans.

Exposure of sensitive information by automated web scanners is possible by the attackers and can reveal system details, service configurations, or even unprotected resources on web servers to them. If left unchecked, this reconnaissance activity might uncover valuable information about network configurations or vulnerabilities in web services that could be far more damaging and exploited later which presents a major issue for the network's confidentiality and integrity.

If 10.168.27.10 is an active web server, the repeated and constant connection attempts could disrupt normal service operations, especially if the probing increases in frequency or extends to additional hosts on the network. This could lead to slowdowns or intermittent accessibility issues for legitimate users.

All these issues increase the opportunity of enhanced attack vectors for the attackers by ignoring these anomalies it may give an attacker the freedom and information they need on a network to attempt more advanced tactics, such as SQL injection, cross-site scripting, or directory traversal attacks if they detect and exploit vulnerabilities through their probing. Failing to investigate or mitigate this repetitive malicious activity could expose the network to exploitation, service disruption, data leakage, and more complex attacks if the probing host succeeds in finding weak points.

# D:Implications of Anomalies

## LDAPS Query Flood

Excessive LDAPS activity from 10.16.80.243 to 10.168.27.10 could imply there has been an attempt at directory service disruption. The large volume of LDAPS connection attempts likely overloaded the directory server, potentially causing slowdowns and or making the service unavailable to authorized users. This could disrupt critical authentication and directory-based access management processes that are critical for resource accessibility.

If the activity turns out to be a brute-force or credential-stuffing attack, it could lead to unauthorized access to directory data. Successful exploitation could expose sensitive user information, permissions, and grant unauthorized access across other networked services and devices tied to the directory which will almost positively result in a catastrophic information security incident.

Given the observed reconnaissance and previous port scanning, this anomaly might allow an attacker to fine-tune future attacks. They may gain insights into this organization's network structure, user accounts, policies, and other assets, which could be exploited in privilege escalation attempts or lateral movement within the network.

The presence of the anomalous activity all points to the compromise of data integrity and confidentiality should the attacker succeed in querying or manipulating directory entries, they may compromise the integrity of directory data, impacting organizational security policies, group memberships, resource access rules, and the organization's reputation.



# E: Solutions for Network Security

The analysis of network activity from Wireshark revealed multiple alarming anomalies, each posing its own threat and distinct risks to the network's security. These include Identified port scanning, a suspected SYN Flood Attack, repeated HTTP probing, and excessive LDAPS traffic, indicative of directory exploitation attempts. To mitigate or eliminate these risks, several targeted actions are recommended. Port scanning, conducted by host 10.16.80.243, was detected with over 45,000 SYN packets and lacking any ACK responses. Port scanning is often a precursor to targeted attacks. To mitigate this it is recommended to deploy intrusion detection and prevention systems (IDS/IPS). IDS tools such as Snort or Suricata can identify and alert when port-scanning activity is taking place, while IPS can block suspicious traffic in real-time (Scarfone and Mell). Another recommended course of action is to implement network segmentation. This will prevent lateral movement across the network by isolating critical systems which reduces the scope of potential reconnaissance (Chapple et al.). Enforcing firewall rules can also help enhance security for example, stateful firewalls should block unsolicited traffic from hosts exhibiting scanning behavior like that of 10.16.80.243.

The SYN Flood Attack, recorded and identified within Wireshark is suspected due to 40,000+ packets targeting 10.168.27.10, seems to aim to overwhelm the host and disrupt services. In order to counteract this threat SYN cookies should be enabled. SYN cookies are a TCP mechanism that helps protect servers from SYN Floods by reducing the resources consumed by the TCP handshake process ("TCP SYN Flooding Attacks"). Rate-limit connections, configures network devices to limit the rate of connection attempts from individual IPs, reducing the impact and possibly preventing flooding attempts (Cisco Systems). Most importantly monitor and block malicious hosts security teams should actively track and block IP addresses like 10.16.80.243 if suspicious activity persists as well as have a list of all known device with their IPs and, MAC addresses so unknown or malicious devices are easier to identify.

Another anomaly detected within Wireshark was the repeated, low-packet HTTP connections over port 80. This suggests automated probing, which is likely reconnaissance for vulnerabilities on devices and services running on the network.. To mitigate this risk deploy web application firewalls (WAFs). Tools like ModSecurity can filter and block malicious probing traffic targeting web services (OWASP). Enabling HTTPS redirects HTTP traffic to secure HTTPS connections to encrypt data and deter unauthorized probing which is another method to bolster security in this vulnerable network. Conducting regular penetration testing on the networks will help in identifying and fixing web service vulnerabilities to reduce the attack surface for reconnaissance tools and threat actors.

# E: Solutions for Network Security II

The excessive LDAPS traffic found within the pcap file, involving over 39,000 rapid connection attempts, indicates the possibility of brute-force attacks or directory exploitation efforts. To prevent this security teams should be ready to strengthen authentication protocols and policies enforce strong passwords, multi-factor authentication (MFA), and account lockout policies for directory services (Microsoft). Implementing rate-limiting restricts the number of LDAP queries a single host can make from within a given timeframe in order to prevent abuse. Another useful methodology for analyzing LDAP traffic along a network is to audit and monitor this directory traffic using tools like Splunk or ELK Stack. Analysts should be tasked to look for unusual patterns and behaviors in order to be proactive with potential security threats. Isolating and hardening directory servers will restrict access to LDAPS access to only trusted IPs, ensuring unauthorized hosts like 10.16.80.243 cannot communicate with directory services.

The anomalies identified within the provided pcap1 file highlight significant risks and vulnerability to network security. Implementing robust monitoring, network segmentation, and access controls can help mitigate these threats as a very cost efficient solution. Proactive measures such as firewalls, intrusion prevention systems, and periodic security audits are also recommended for minimizing vulnerabilities and enhancing overall resilience against cyber threats.

# E: Solutions for Network Vulnerabilities

The Nmap scan on 10.168.27.0 network identified several critical vulnerabilities within the network, necessitating immediate action to improve upon overall security and reduce the attack surface. Key issues include an oversized and unused IP range, outdated systems with insecure protocols, misconfigured services, and weak cryptographic practices. Addressing these vulnerabilities requires network segmentation, system upgrades, and stringent access controls. An unnecessarily large IP range increases the network's attack surface by providing multiple potential entry points for unauthorized devices and facilitating IP spoofing or man-in-the-middle attacks like the range found in the 10.168.27.0 network. Reducing a large IP range to match the number of active hosts such as implementing a /28 subnet for the five hosts can minimize these risks. Implementing strict DHCP monitoring and disabling unused IP addresses through Access Control Lists further enhances security (Microsoft Azure).

A host running Windows Server 2012 with legacy Windows Server 2008 services like that of Host 10.168.27.10, is particularly vulnerable due to outdated patches and multiple open ports (InfoGuard Security). Upgrading to a current and supported operating system, such as Windows Server 2022, is crucial, since Microsoft no longer provides security patches for Server 2008 or 2012, leaving the host running these instances incredibly susceptible to exploits like EternalBlue. Implementing virtual patches through host-based intrusion prevention systems can also help mitigate risks. Additionally, disabling SMBv1 and closing unnecessary high-numbered RPC ports will reduce exposure to ransomware attacks like WannaCry.

Hosts 10.168.27.14, 10.168.27.132, and 10.168.27.20 are all running outdated versions of OpenSSH 5.5p1, which are lacking patches and updates for known vulnerabilities. Upgrading the host to a more up-to-date OpenSSH version is crucial. Consolidating SSH access to a single, secure port and implementing rate-limiting mechanisms might also help in preventing brute-force attacks (Control Audits). Another vulnerability these hosts share is the use of identical RSA and DSA keys across the separate instances. These keys should be replaced with unique, modern key types, such as Ed25519 or RSA 2048-bit keys, to enhance cryptographic security.

# E: Solutions for Network Vulnerabilities II

Running an end-of-life operating system on Host 10.168.27.15, puts it at high risk alongside the multiple open, misconfigured services like FTP with anonymous login enabled and HTTP supporting insecure methods like TRACE. Upgrading to a supported operating system is imperative (InfoSec Institute). FTP should be replaced with SFTP or disabled entirely if not compatible, while HTTP services should enforce HTTPS using SSL/TLS protocols. Disabling the TRACE method and limiting HTTP methods to just the bare essentials, such as GET and POST, will mitigate risks of cross-site tracing attacks. Echo services on port 7 should also be disabled to prevent ping flood or reflection attacks.

Implementing network-wide strategies can further bolster security. Network segmentation through VLANs can easily isolate sensitive resources and reduce IP ranges, and enabling firewalls to filter traffic based on strict rules can prevent unauthorized access that would otherwise be allowed on these vulnerable hosts. Deploying network intrusion detection systems can also help with detecting and preventing malicious activity like that of what was identified by nmap. Regular vulnerability scanning and patch management ensure that new threats are promptly addressed (Check Point Software). By addressing the oversized IP range, upgrading legacy systems, securing SSH configurations, and remediating host-specific vulnerabilities, the network can significantly enhance its defense against cyberattacks. Proactive measures such as subnetting, patching, and adopting modern cryptographic standards not only reduce the attack surface but also ensure governance and compliance with best practices in network security.