

Nmap and Wireshark

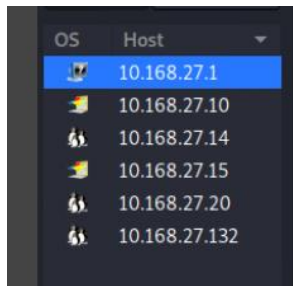





Mahdi Ghaznawy

A. Network Topology

Screenshots of running Nmap.

A scan on Zenmap reveals a star topology of hosts linked to a central switch or router. The network appears based on a single subnet (10.168.27.0/24), a local LAN where every host gets an IP address in this range. As all scanned hosts are in this particular subnet and show single-hop latency, they're probably connected through a central network device (switch or router). The advantages of the Star topology consist of easy scalability, centralized management, and high reliability due to the fact that every device has a dedicated connection, which lessens congestion and simplifies troubleshooting. The disadvantages include the presence associated with a central switch, which is a single point of failure, more cabling, and greater price than some other topologies.

IP Address	Operating System
10.168.27.10	Windows Server 2012
10.168.27.14	Linux Kernel 2.6.32
10.168.27.15	Windows 8.1 Pro
10.168.27.20	Linux (Unspecified)
10.168.27.132	Linux Kernel 2.6.32
10.168.27.1	Unknown

OS	Host
	10.168.27.1
	10.168.27.10
	10.168.27.14
	10.168.27.15
	10.168.27.20
	10.168.27.132

10.168.27.10 - Open Ports: 135, 139, 389, 445, 636, 49152, 49154, 49155, 49157, 49161

10.168.27.14 - Open Ports: 22, 9090

10.168.27.15 - Open Ports: 7, 9, 13, 17, 19, 21, 80, 135, 139, 445, 49154, 49155, 49158

10.168.27.20 - Open Ports: 22

10.168.27.132 - Open Ports: 22, 9090

10.168.27.1 - All Ports Closed

```
root@kali: ~ Zenmap
File Actions Edit View Help
root@kali ~
# nmap 10.168.27.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-08 06:46 MST
Nmap scan report for 10.168.27.10
Host is up (0.00013s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
389/tcp    open  ldap
445/tcp    open  microsoft-ds
636/tcp    open  ldaps
49152/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49157/tcp  open  unknown
49161/tcp  open  unknown
MAC Address: 00:0C:29:FB:2F:35 (VMware)

Nmap scan report for 10.168.27.14
Host is up (0.000031s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9090/tcp  open  zeus-admin
MAC Address: 00:0C:29:40:9B:C7 (VMware)

Nmap scan report for 10.168.27.15
Host is up (0.00011s latency).
Not shown: 987 filtered ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
21/tcp    open  ftp
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49154/tcp  open  unknown
49155/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 00:15:5D:01:80:07 (Microsoft)

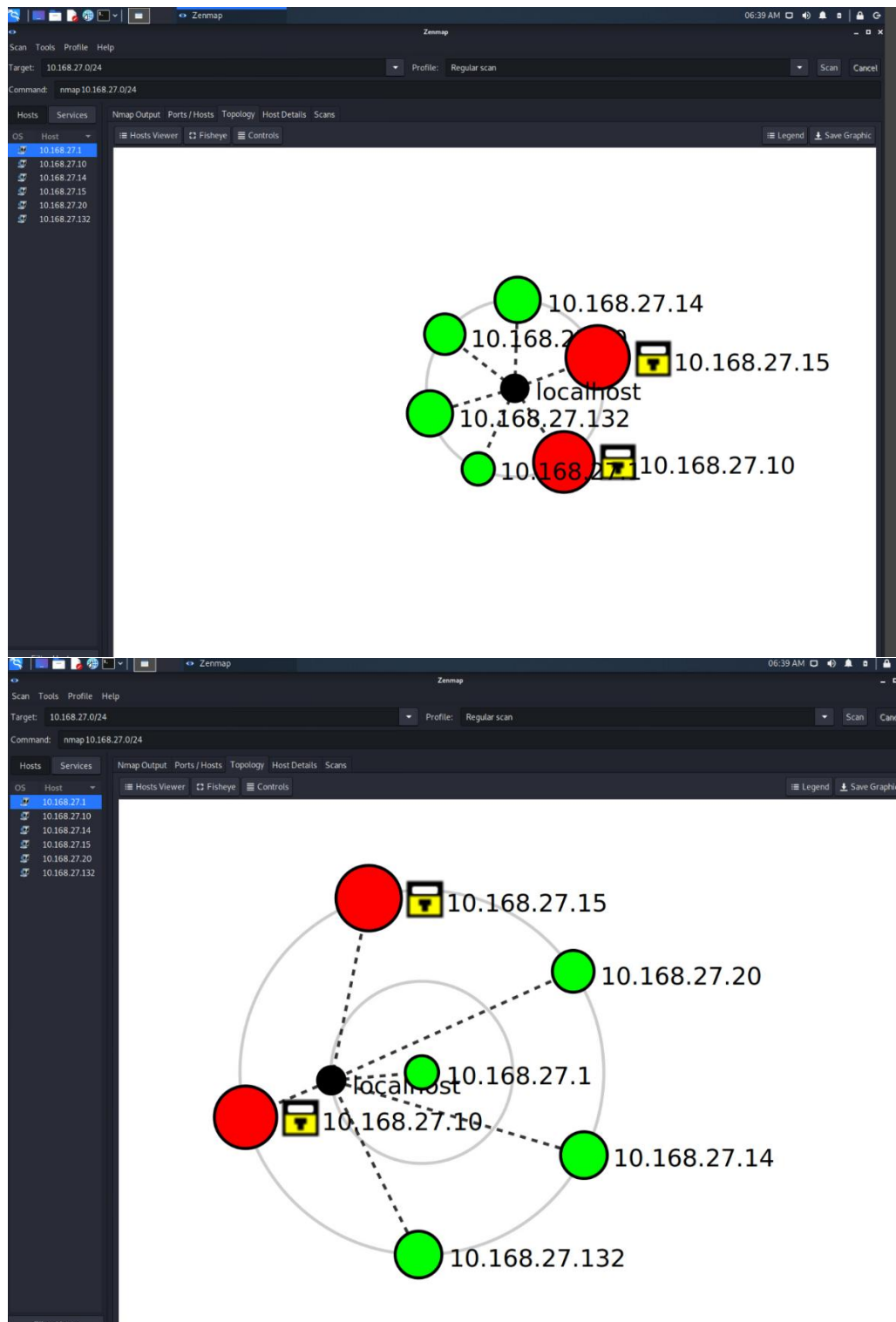
Nmap scan report for 10.168.27.20
Host is up (0.000035s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:45:9B:21 (VMware)

Nmap scan report for 10.168.27.132
Host is up (0.000028s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9090/tcp  open  zeus-admin
MAC Address: 00:0C:29:87:8B:8E (VMware)

Nmap scan report for 10.168.27.1
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.168.27.1 are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 7.78 seconds
root@kali ~
```

Screenshot of Zenmap Topology



B Summary of Vulnerabilities and Implications

First vulnerability

Plaintext FTP Data Transmission (MITM Attack)

This packet capture File shows that a device at IP address 10.168.27.15 connects through FTP over TCP port 21. This is an outdated protocol. FTP sends data like login credentials and documents in plaintext and, therefore, is prone to a Man-In-The-Middle (MITM) attack. This means an attacker can intercept the traffic and modify the information being transferred between a server and a client. If nothing is done, the organization exposes login credentials along with other private documents to attackers. Attackers can intercept, alter, or exfiltrate data during transmission, allowing unauthorized access, information leaks, and possible breaches. An attacker could also inject malicious commands into FTP traffic.

Second vulnerability

HTTP Lack of Encryption & XSS Attacks

The Nmap scan shows that the device 10.168.27.15 runs a web service using HTTP on TCP port 80. HTTP doesn't support encryption, so all transmitted information like user credentials, session tokens, and other very sensitive data is sent in plaintext. Also, HTTP-based applications are in danger of Cross-Site Scripting (XSS) attacks, where a hacker injects harmful scripts into websites to execute arbitrary code on users' browsers. Not fixing this particular flaw means attackers could intercept and read sensitive communications, steal authentication cookies, and impersonate users. XSS attacks may enable malicious scripts to run in users' browsers, resulting in session hijacking, credential theft, and redirection to phishing sites. This might result in data breaches, financial losses, and reputational damage to the organization.

Third vulnerability

Outdated Windows Server (EternalBlue Exploit CVE-2017-0144)

The packet capture file shows that node 10.168.27.10 of the network is running Windows Server 2012 R2. This operating system has reached its EOL and no longer receives security patches or updates from Microsoft. Most important for this system is the EternalBlue attack (CVE-2017-0144) that exploits a flaw in SMBv1, enabling remote attackers to execute arbitrary code on susceptible machines. Leaving old Windows servers in production puts the organization in danger of remote code execution, ransomware infections (like WannaCry and NotPetya), and unauthorized system access. Attackers can exploit unpatched vulnerabilities to gain entry to the network, escalate privileges, and laterally attack other systems.

C. Wireshark Anomalies for

Analyzing PCAP4

First Anomaly

Unusual Port Scanning Behavior

Evidence: The packet capture file reveals a series of TCP packets coming from IP address 10.16.80.243 and targeting 10.168.27.10 across multiple ports, including key services like FTP (21), SSH (22), SMTP (25), HTTP (80), HTTPS (443), and RDP (3389). What stands out is the presence of TCP FIN, PSH, and URG flags in these packets,

which suggests an unusual scanning pattern rather than normal traffic. This activity occurs between packets 6 and 66, indicating a deliberate attempt to probe critical service ports.

Second Anomaly

Malformed DNS Queries

Evidence: The packet capture file shows a DNS request from 10.16.80.243 to 8.8.4.4, querying for the PTR record of 10.27.168.10. The response from the DNS server indicates "No such name" (packet 4-5). This suggests that the queried domain does not exist, which could indicate DNS tunneling attempts or misconfigured network settings.

Third Anomaly

Abnormal TCP Reset (RST) Responses

Evidence: Multiple packets in the capture file (16-66) show TCP RST (Reset) responses from 10.168.27.10 to 10.16.80.243. These frequent resets could indicate an attempted unauthorized connection to various ports, potentially suggesting an intrusion attempt or a misconfigured network device rejecting connections.

D. Implications of each Wireshark Anomaly

Implications of taking no action

If unaddressed, this behavior might lead to a full-blown attack involving service exploitation, credential theft, or unauthorized access. Permitting these sorts of scanning to go unchecked presents a risk of a security breach, information exfiltration, and service disruptions.

Implications of taking no action 2

If no action is taken, unresolved or malformed DNS queries can be leveraged for data exfiltration using DNS tunneling. Attackers may use DNS queries to encode and transmit information to an external server, bypassing traditional security controls. Additionally, frequent unresolved DNS queries may point to malware attempting to communicate with command-and-control (C2) servers.

Implications of taking no action 3

If nothing is done, frequent TCP RST responses might lead to slowed network performance, disrupted connections, and DoS scenarios. In case this activity is part of an attack, it might suggest that an adversary is attempting to stay away from detection by forcing session terminations or by flooding target services with reset packets.

E. Recommended Solutions

First Vulnerability

For best practice, replace FTP with a Secure alternative like safe file Transfer Protocol (SFTP) or File Transfer Protocol secure (FTPS). SFTP utilizes SSH (port 22) and encrypts authentication and file transfers to reduce the risk of MITM attacks. Organizations should stop using unsecured FTP and switch to encrypted transfer methods to maintain information confidentiality and integrity (Scarfone et al., 2010), according to the National Institute of Standards & Technology (NIST).

Second Vulnerability

Organizations should enforce HTTPS using Transport Layer Security (TLS) certificates to limit this risk. HTTPS encrypts web traffic to keep information private and protect against MITM attacks. In addition, applications should implement Content Security Policy (CSP) headers and appropriate input validation to avoid XSS attacks. The Open Web Application Security Project (OWASP, 2021) recommends disabling HTTP and forcing HTTPS with TLS 1.2 or 1.3 for secure communication (OWASP, 2021).

Third Vulnerability

The best mitigation strategy is upgrading to Windows Server-supported versions (Windows Server 2019 or 2022), which get regular security updates from Microsoft. If upgrading isn't immediately possible, organizations should turn off SMBv1, apply all readily available patches, and use network segmentation to isolate vulnerable systems. Disabling SMBv1 and utilizing SMBv3 lowers the risk of exploitation (Microsoft, 2020).

First Anomaly

An Intrusion Detection System (IDS) like Suricata or Snort can identify and block port scanning attempts in real time. Firewalls ought to restrict external access to only essential ports and use anomaly-based detection mechanisms. Intrusion detection and prevention systems (IDPS) are necessary to detect and prevent reconnaissance activities before they escalate into a breach (Scarfone and Mell, 2007).

Second Anomaly

Unresolved or malformed DNS queries can be leveraged for data exfiltration using DNS tunneling. Attackers may use DNS queries to encode and transmit information to an external server, bypassing traditional security controls (Antonakakis et al., 2012). Additionally, frequent unresolved DNS queries may point to malware attempting to communicate with command-and-control (C2) servers.

Third Anomaly

Network administrators must apply rate-limiting and anomaly detection on firewalls and intrusion prevention systems (IPS) to stop too many Reset (RST) packets used in attacks, including denial-of-service (DoS), or to interrupt connections. The NSA Cisco Firepower Hardening Guide (2023) suggests deep packet inspection (DPI) to identify suspicious behaviors. DPI monitors network traffic in real time and inspects headers and payloads for unusual patterns like unusual RST packet spikes. This combination of rate-limiting, anomaly detection, and DPI could defend against RST-based attacks.

References

Antonakakis, M., Perdisci, R., Nadji, Y., Vasiloglou, N., Abu-Nimeh, S., Lee, W., & Dagon, D. (2012). From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware. USENIX Security Symposium.

<https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final127.pdf>

Microsoft. (2020). Guidance for Customers about SMBv1 and CVE-2017-0144. Microsoft Security Response Center.

<https://docs.microsoft.com/en-us/windows-server/storage/file-server/smb-security>

National Security Agency. (2023). Cisco Firepower Hardening Guide.

https://media.defense.gov/2023/Aug/02/2003272858/-1/-1/0/CTR_CISCO_FIREPOWER_HARDENING_GUIDE.PDF

OWASP. (2021). Transport Layer Security Cheat Sheet. The Open Web Application Security Project.

https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Security_Cheat_Sheet.html

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2010). Guide to Secure Web Services. National Institute of Standards and Technology (NIST). <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf>

Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf>