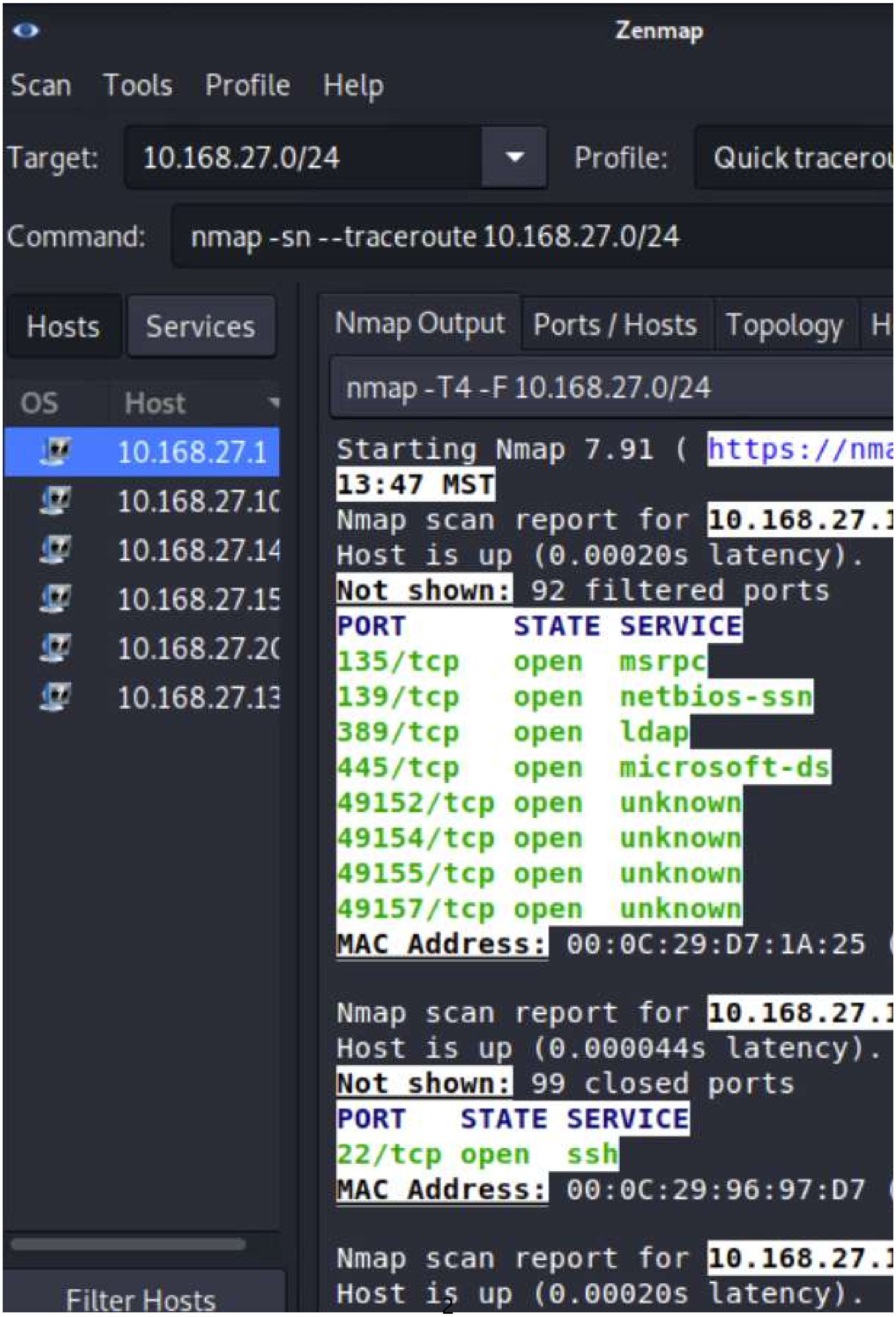
A. Network Topology

Screenshots of running nmap



Target: 10.168.27.0/24

Profile: Quick tracerou

Command: nmap -sn --traceroute 10.168.27.0/24

```
10.168.27.1
10.168.27.1(
10.168.27.14
10.168.27.15
10.168.27.2(
10.168.27.13
```

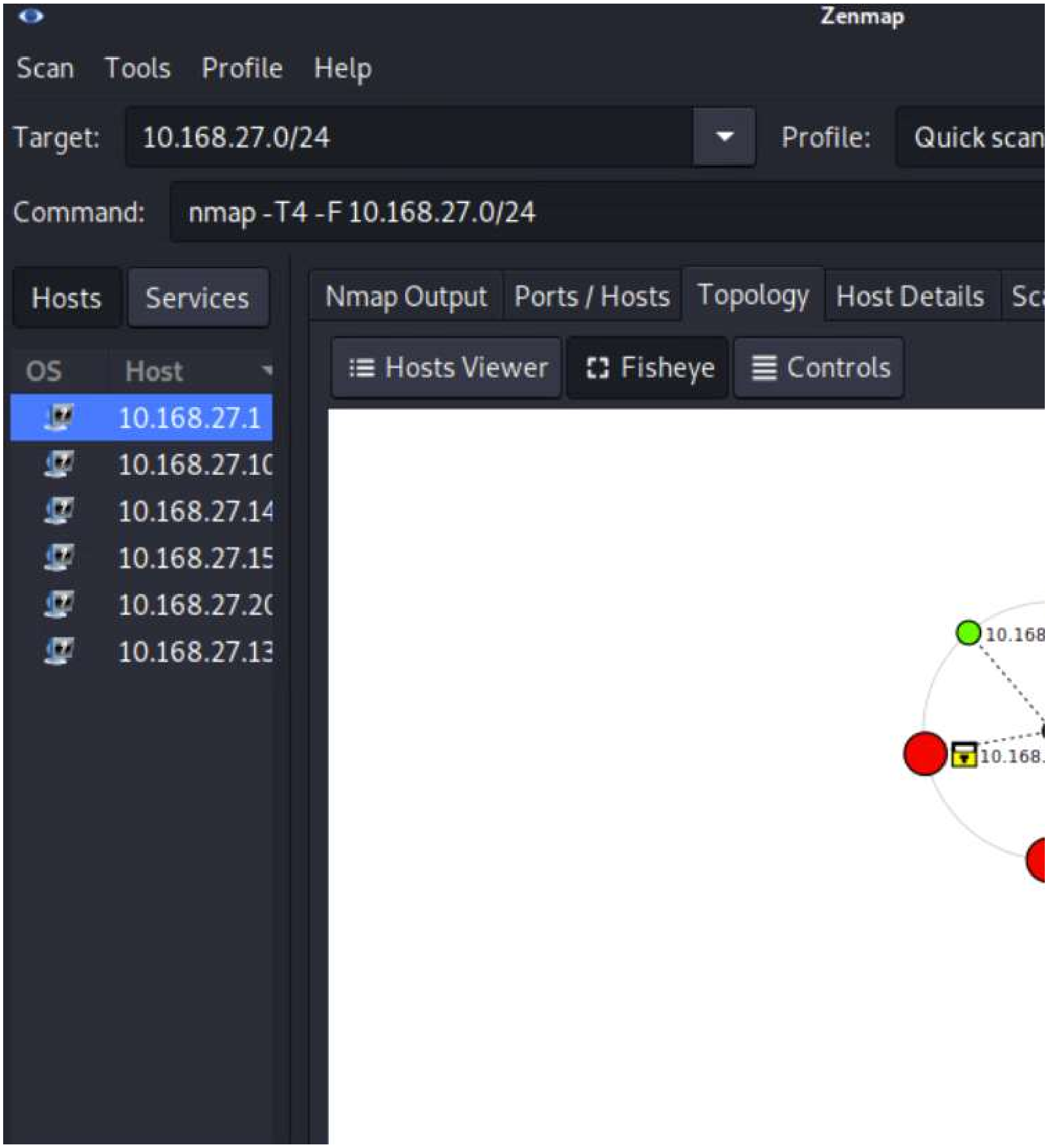
```
nmap -T4 -F 10.168.27.0/24
```

```
Starting Nmap 7.91 ( https://nma
13:47 MST
Nmap scan report for 10.168.27.1
Host is up (0.00020s latency).
Not shown: 92 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:D7:1A:25 (

Nmap scan report for 10.168.27.1
Host is up (0.000044s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:96:97:D7 (

Nmap scan report for 10.168.27.1
Host is up (0.00020s latency).
```

Screenshot of Zenmap Topology



Target: 10.168.27.0/24

Profile: Quick scan

```
Command: nmap -T4 -F 10.168.27.0/24
```

```
10.168.27.1
10.168.27.10
10.168.27.14
10.168.27.15
10.168.27.20
10.168.27.13
```

Topology: This Network is using a Star Topology. In a star setup, devices connect to a middle hub for easy control and growth. But, if that hub has problems or costs more, it could be a challenge.

B Summary of Vulnerabilities and Implications

First vulnerability

Host 10.168.27.15 has Port 21/ FTP opened. FTP doesn't encrypt data in transit, making it susceptible to man-in-the-middle attacks where attackers can intercept and modify data during transmission.

Second vulnerability

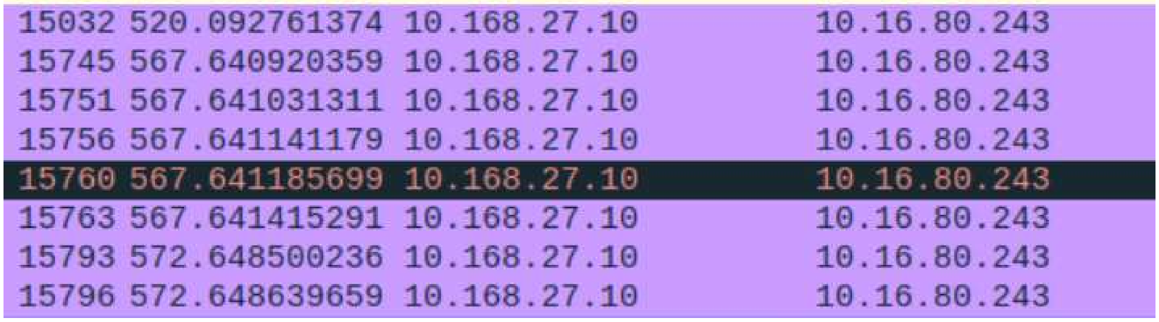
Host 10.168.27.14 has Port 80/HTTP opened. Open Port 80 can be targeted for DoS attacks, where attackers overwhelm the server with a high volume of requests, leading to service disruption and unavailability.

Third vulnerability

Host 10.168.27.10 has Port 9/Discard opened. Open ports, such as Port 9 associated with the Discard service, are vulnerable to network scanning by attackers seeking information. To lower the risk, it's advised to close unused ports, particularly if the Discard service isn't in active use. If necessary, limit access to trusted networks and monitor network traffic for enhanced security.

C. Wireshark Anomalies

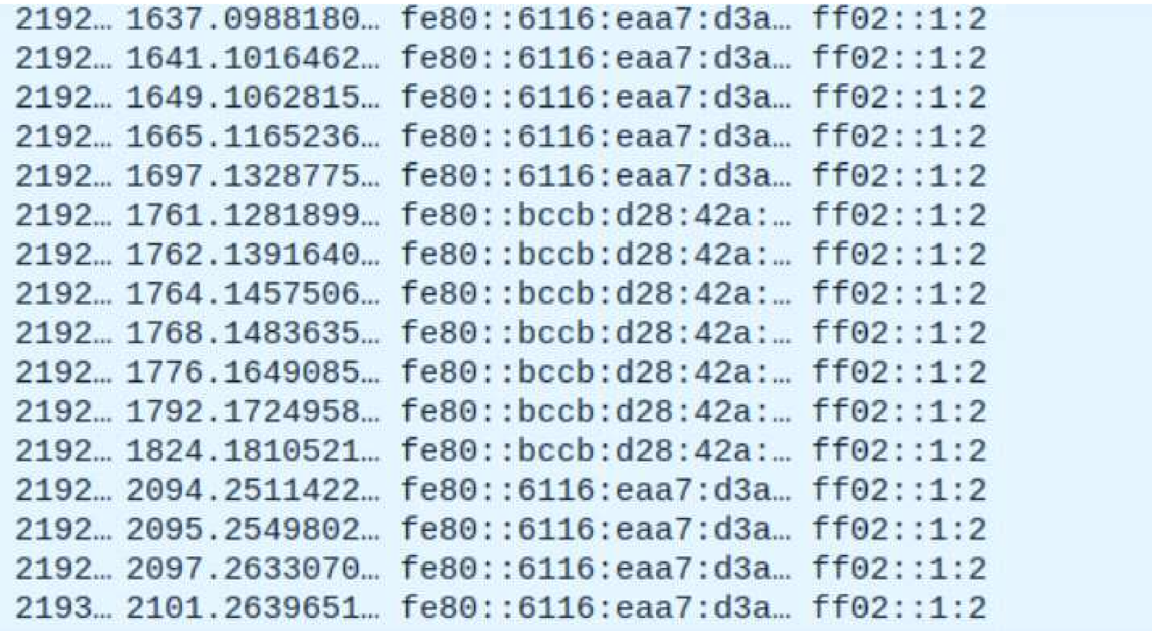
First Anomaly



```
15032 520.092761374 10.168.27.10          10.16.80.243
15745 567.640920359 10.168.27.10          10.16.80.243
15751 567.641031311 10.168.27.10          10.16.80.243
15756 567.641141179 10.168.27.10          10.16.80.243
15760 567.641185699 10.168.27.10          10.16.80.243
15763 567.641415291 10.168.27.10          10.16.80.243
15793 572.648500236 10.168.27.10          10.16.80.243
15796 572.648639659 10.168.27.10          10.16.80.243
```

The vulnerability is related to the DCERPC service used for communication between components in a VMware vCenter Server environment. It occurs during the interpreting stage of network packets. By manipulating certain fields in the packet header, an attacker can trick the system into accessing memory outside the intended boundaries. This manipulation allows an attacker to control pointers, potentially leading to unauthorized access and an authentication bypass.

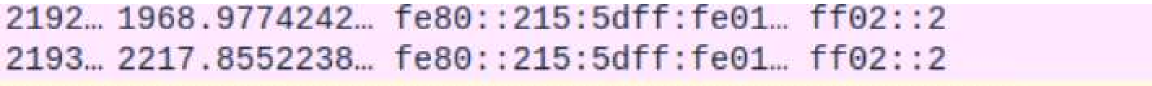
Second Anomaly



```
2192… 1637.0988180… fe80::6116:eaa7:d3a… ff02::1:2
2192… 1641.1016462… fe80::6116:eaa7:d3a… ff02::1:2
2192… 1649.1062815… fe80::6116:eaa7:d3a… ff02::1:2
2192… 1665.1165236… fe80::6116:eaa7:d3a… ff02::1:2
2192… 1697.1328775… fe80::6116:eaa7:d3a… ff02::1:2
2192… 1761.1281899… fe80::bccb:d28:42a:… ff02::1:2
2192… 1762.1391640… fe80::bccb:d28:42a:… ff02::1:2
2192… 1764.1457506… fe80::bccb:d28:42a:… ff02::1:2
2192… 1768.1483635… fe80::bccb:d28:42a:… ff02::1:2
2192… 1776.1649085… fe80::bccb:d28:42a:… ff02::1:2
2192… 1792.1724958… fe80::bccb:d28:42a:… ff02::1:2
2192… 1824.1810521… fe80::bccb:d28:42a:… ff02::1:2
2192… 2094.2511422… fe80::6116:eaa7:d3a… ff02::1:2
2192… 2095.2549802… fe80::6116:eaa7:d3a… ff02::1:2
2192… 2097.2633070… fe80::6116:eaa7:d3a… ff02::1:2
2193… 2101.2639651… fe80::6116:eaa7:d3a… ff02::1:2
```

A buffer overflow vulnerability is present in the processing of the DNS Servers option from a DHCPv6 Advertise message, posing a risk of unauthorized access and potential compromise of Confidentiality, Integrity, and/or Availability.

Third Anomaly



```
2192… 1968.9774242… fe80::215:5dff:fe01… ff02::2
2193… 2217.8552238… fe80::215:5dff:fe01… ff02::2
```

A vulnerability in Open vSwitch enables ICMPv6 Neighbor Advertisement packets to evade OpenFlow rules when exchanged between virtual machines. This flaw may be used a local attacker to create packets with a manipulated or forged target IP address, redirecting ICMPv6 traffic to unknown IP addresses.

.D. Implications of each Wireshark Anomaly

Implications of taking no action 1

Failing to fix DCERPC vulnerability in VMware vCenter Server risks an authentication bypass, enabling unauthorized access and potential compromise of sensitive data. Swift remediation is crucial to prevent operational disruptions, data breaches, and broader security implications.

Implications of taking no action 2

Failure to address the buffer overflow vulnerability in the DNS Servers option of a DHCPv6 Advertise message could result in unauthorized access and compromise of Confidentiality, Integrity, and/or Availability. This neglect increases the risk of security breaches, potential data exposure, and system instability.

Implications of taking no action 3

Failure to address ICMPv6 in Open vSwitch poses a risk. It allows local attackers to manipulate ICMPv6 Neighbor Advertisement packets, potentially redirecting traffic between virtual machines to arbitrary IP addresses, compromising communication integrity.

E. Recommended Solutions

First Vulnerability

To secure port 21 for FTP, consider implementing the following measures, Use FTPS (FTP Secure): FTPS is an extension to FTP that adds support for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) cryptographic protocols. This ensures that data transmitted over port 21 is encrypted, enhancing the security of FTP connections. (1)

Second Vulnerability

An alternative to port 80 for HTTP is port 443, which is used for secure HTTP (HTTPS). HTTPS encrypts the data transmitted between the client and the server, providing a secure communication channel. This encryption is particularly important for sensitive information, such as login credentials and personal data, as it helps protect against eavesdropping and man-in-the-middle attacks. (2)

Third Vulnerability

To implement this measure, disable unnecessary ICMPv6-related services after identifying and deactivating non-essential features. Regularly review and update configurations to align with security best practices, reducing exposure to potential vulnerabilities. (3)

First Anomaly

To mitigate vulnerabilities related to DCERPC, it is recommended to apply the patches and updates provided by the software vendor promptly. Additionally, organizations should consider implementing network segmentation and firewall configurations to restrict unauthorized access to vulnerable systems. (4)

Second Anomaly

Mitigate risks by promptly applying available patches for vulnerabilities 1-7, accessible here. These patches aim to address the vulnerabilities and will be integrated into the Feb 2024 release. For vulnerabilities 8 and 9, which lack patches, minimize exposure by avoiding PXE or HTTP boot on untrusted networks. Regular updates from the source are recommended for any developments regarding fixes for vulnerabilities 8 and 9. (5)

Third Anomaly

Users should install Open vSwitch (OVS) from RHEL Fast Datapath on Red Hat Enterprise Linux 7, avoiding the unsupported Optional repository. Red Hat OpenStack Platform 13/16 users are unaffected, and updates will be distributed through the Fast Datapath channel, emphasizing the importance of regular security updates for continued system integrity. (6)

References

(1) McIntyre, Jim. “Secure FTP: How to secure your FTP server”InfoWorld

(2) Shinder, D., & Shinder, T. (2003). Configuring ISA Server 2000: Building Firewalls for Windows 2000. Syngress

(3) RFC 7450: "Security Risks Related to IPv6 Deployment" provides insights into security considerations for IPv6, including ICMPv6.

(4) Dimitrios Tatsis. “VMware vCenter Server DCERPC save_sec_fragment out-of-bounds pointer vulnerability” JULY 13, 2023

(5) Mathews J.K . “Vulnerabilities in EDK2 NetworkPkg IP stack implementation” JAN 5 2024

(6) National Vulnerability Database (NVD) under CVE-2023-5366.