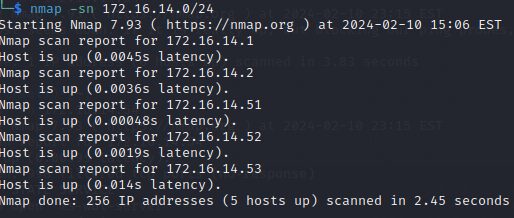
**Project: Network Administration**

**Subject:** Network Security Assessment Completed

Dear LHL Manager,

I am pleased to present the findings from our recently completed network security assessment. The primary goal was to identify any open ports and verify the configurations of service ports on all our servers. The assessment’s key insights are as follows:



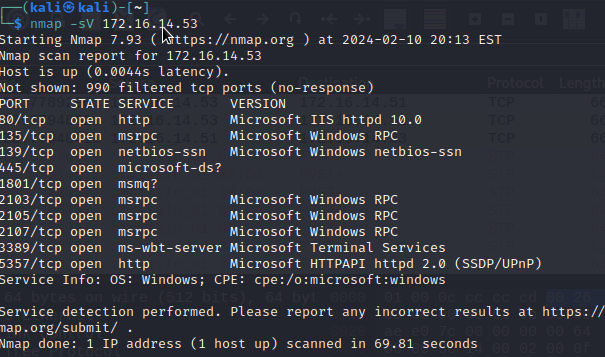
* Active hosts validated: The assessment confirmed the operational status of the following hosts: Windows 1 Server (172.16.14.50), Windows 2 Server (172.14.54), Linux Server (172.16.14.52), KaliOpenVas (172.16.14.51), and lastly WinServer1 (172.16.14.53)
* Critical open ports: Open ports identified on our Windows Servers that require immediate attention due to the high vulnerabilities
* Irregular Network Patterns: The first part of the report was traffic analysis and there were some irregular ARP patterns that led me to start scanning the network

Please see the attached report which includes detailed findings and all the documents of the steps taken during this whole assessment. I have added screenshots and traffic logs.

I’ve used the command -nmap -sV to scan the ports for both linux and winserver, but for the Windows1 server I’ve used -nmap -pN to scan for the ports.

Port Scans

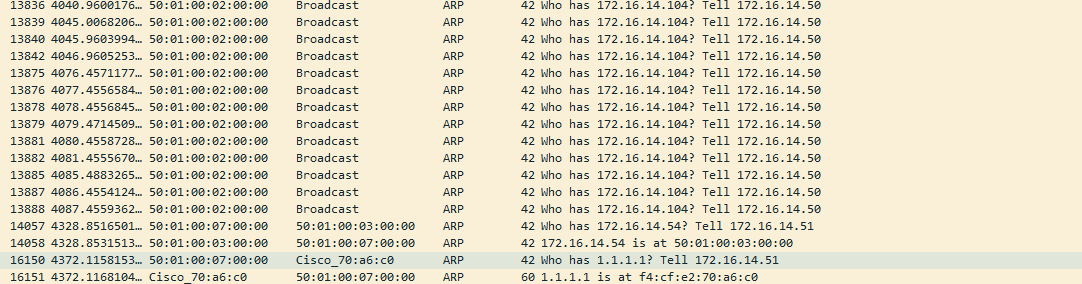
1. **WinsServer1 (172.16.14.53)**



Based on the nmap scan shown on my screenshot, 172.16.14.53 - Winserver1, the following open ports and services are:

1. *80/tcp*: open and active, running HTTP service. This can be exploited if HTTP is not required for this server’s operations
2. *135/tcp*: Open, running on Microsoft Windows RPC. I believe this is standard on all Windows. This would still be monitored as it can be vulnerable to attacks if exposed to the internet.
3. *139/tcp and 445/tcp*: Open, running Microsoft-DS and netbios-ssn. NetBIOS over TCP/IP presents risk if not properly secured
4. *1801/tcp*: Open, associated with msmq (Microsoft Messaage Queuing).
5. *2103/tcp*, 2105/tcp, 2107/tcp: All open, running msrpc (Microsoft Windows RPC). Multiple ports open for RPC can mean that different services or multiple endpoints.
6. *3389/tcp*: open, running ms-wbt-server (Microsoft Terminal Services). This port is used for RDP (Remote Desktop Protocol)

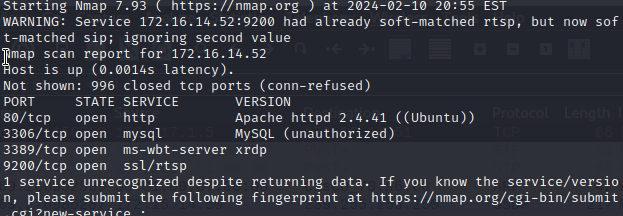
Wireshark Captures for Winserver1



Based on the Wireshark capture provided:

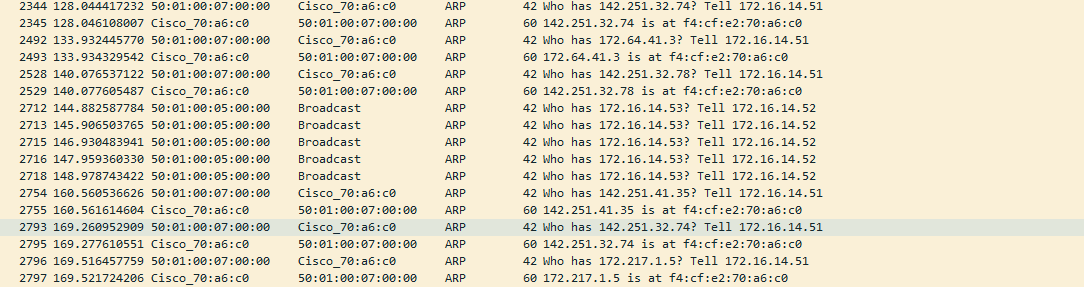
1. Requests for **172.16.104**: ARP requests broadcasted by **172.16.14.50**, looking for the device with IP **172.16.14.104**
2. Requests for **172.16.14.54**: ARP request made by **172.16.14.51**, which is the Kali machine itself which is performing the actual scan, asking for the MAC address of **172.16.14.54**
3. Reply from **172.16.14.54**: The device with IP **172.16.14.54** replied with its MAC address **50:01:00:07:07:00**
4. Other replies identified: At the bottom of the capture, we see two more ARP replies indicating that the other device with the IP address, **1.1.1.1** has the MAC address **fc:4f:e2:70:a6:c0** and **00:1a:11:fa:a1:c2**

2. Linux Server Port Scan:



1. *Port 80/tcp:* Active and hosting Apache **HTTP** server version 2.4.41 (Ubuntu), a commonplace setup for serving web content. Should this server not be designated for web hosting duties, an open port 80 is superfluous and presents a potential vulnerability.
2. *Port 3306/tcp*: This port is open and hosting a **MySQL** service that's labeled as "unauthorized," suggesting that while the service is operational, the scan was unable to verify its authenticity. Should there be no requirement for network-wide accessibility to the MySQL database, its exposure poses a security threat. It's advisable to fortify the database's security or limit its accessibility to explicitly trusted hosts.
3. *Port 3389/tcp*: Found to be active with **xrdp**, a Linux-based implementation of the Windows Remote Desktop Protocol. Its presence implies the server is set to receive RDP connections, likely to simplify administrative tasks. This configuration is unusual for Linux systems and, unless secured diligently, introduces a vector for potential security breaches.
4. *Port 9200/tcp*: This port is active with **SSL/rtsp service**, commonly associated with streaming or Elasticsearch functionalities. Should this relate to an Elasticsearch service, it is imperative to secure it thoroughly to prevent any instances of data exposure.

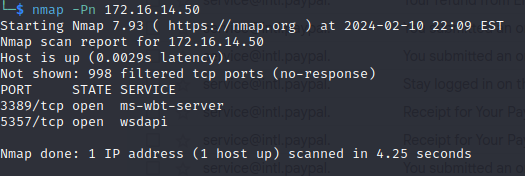
Wireshark Capture for Linux



Based on the wireshark capture:

* The Originating IP Address: This is the IP address of the device initiating the ARP is **172.16.14.51**.
* The Originating MAC Address: This refers to the hardware address of the device sending out the ARP inquiry.
* The Queried IP Address: These are the IP addresses that the originating device is attempting to discover on the network, such as **142.251.32.74** and **172.16.14.53**.
* The Queried MAC Address: This is the hardware address that corresponds to the IP address being looked up in the ARP request. For instance, the IP addresses **142.251.32.74** and **172.16.14.53** are associated with the MAC address `**fc:4f:e2:70:a6:c0.**

3. Windows1/ Windows2 server nmap scan:



1. *Port 3389/tcp****:*** Service is **ms-wbt-server** is running on this port, which is used for RDP (Windows Remote Desktop Protocol). This is required on Windows. If this port is not used for RDP, this opened port is a security risk.
2. *Port 5357/tcp*: Service is **wsdapi** and running on this port, associated with the Web Services on Devices API, used by Windows. This should be filtered or closed to prevent exploits.

**Immediate Recommendations:**

* Conduct a thorough security review of the open ports, especially those on the Windows server
* Investigate the main cause of the strange ARP traffic to exclude any unauthorized scans

Kindly examine the comprehensive report provided, with the data and traffic logs and screenshots and let me know your availability for a meeting to further explore the remediation strategy.

I suggest we convene to discuss the remediation plan in greater detail. Your guidance on the next steps would be crucial so please inform me of your availability to have a meeting.

**Warm regards,**

**Reniel Villahermosa**

**APA Citations:**

IANA Port Numbers registry:

Internet Assigned Numbers Authority. (n.d.). Service Name and Transport Protocol Port Number Registry. (2024, January 1). https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Oracle Corporation. (n.d.). MySQL Documentation. (2024). https://dev.mysql.com/doc/

Apache Software Foundation. (n.d.). Apache HTTP Server Documentation. (1997-2023) https://httpd.apache.org/docs/

National Institute of Standards and Technology. (n.d.). National Vulnerability Database. Retrieved (2024, February 7). https://nvd.nist.gov/

Microsoft. (2022). Windows Server documentation. (2024). https://learn.microsoft.com/en-us/windows-server/