A screenshot of a computer

Description automatically generated with medium confidence

A.  Describe the network topology you found when running Nmap. Include screenshots as evidence of running Nmap.

The Topology I found was a Star Topology within the given scan of 10.168.27.0/24. It included 8 devices all connecting to a central point. 4 Systems including my own host running the Linux Operating system, and 2 running Windows.

A screenshot of a computer program

Description automatically generated with medium confidence

B.  Summarize the vulnerabilities on the network and their potential implications based on your Nmap results.

Investigating the Ports and Hosts on each system I found that http was open on port 80 on host 10.138.27.15 but no means of implementing https is seen. Https which is known to secure using encryption would be a better means of securing the network. Http could lead to a potential security breach on the network from an outside threat such as a Mitm attack. Also on host 10.138.27.15 I found that FTP was being used on tcp port 21. A more secure file transport system could be used in place instead such as a SFTP or FTPS. Again, this leaves a vulnerability and an opportunity for an attacker to packet sniff on unencrypted data or initiate Mitm attacks.

On host 10.168.27.10 we find that ldap is being used on tcp port 389, the use of ldap does not use any encryption method so using this could lease to a potential breach in security. If the attacker were to gain access to ldap components, then they could have the ability to find other appliances on the network including that of any internal servers. This could result in serious repercussions as it widens the attack surface of the network if not secured.

A screenshot of a computer program

Description automatically generated with medium confidence

C.  Describe the anomalies you found when running Wireshark, on the network capture file, and include evidence of the range of packets associated with each  anomaly.

I found that packets were being sent using HTTP which is known to be unsecured network protocol. This is associated with the host address of which include 10.168.27.132 , 10.168.27.1 , 10.168.27.14.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

I found FTP packets being sent from unknown devices residing on a different network to the current network of 10.168.27.0/24. LDAP packets were also found being used from sources outside of the network.

D. Summarize the potential implications of not addressing each  of the anomalies found when running Wireshark.

If these anomalies are not addressed then it exposes the network to great harm. Using unencrypted protocols such as HTTP, FTP, and LDAP could lead to an interception of traffic. With traffic between traversed across the network like this it could open up many paths of opportunity for an attacker to gain unauthorized access to the network. It could lead to MITM attacks and if they were to gain access to LDAP resources, they could gain knowledge of other devices residing on the network of 10.168.27.0/24. Being able to gain knowledge about other devices on the network broadens the attack surface on the network and leaves the attacker prone to more opportunity to try to gain access onto the network or harm system devices. Using HTTP could result in phishing attacks or leading the user onto spoofed websites where credentials can be harvested. FTP could falsely packets and could send malicious scripts and code to the system user which could open back doors within the system.

E.  Recommend solutions for eliminating or minimizing all identified vulnerabilities or anomalies from Wireshark and Nmap. Use current, industry-respected, reliable research and sources to support your recommendations for each vulnerability or anomaly.

With the use of these unsecured and unencrypted protocols we leave a lot of potential breaches to system. Using a means of encrypting traffic across and connections established outside of the network is the best way to ensure that the network is secured. The use of unsecure ports such as that associated with HTTP (80), FTP (20/21), LDAP (389) need to be closed and configured unusable on the network. These ports can be blocked within a firewall or manually configured on another management system. According to the National Institute of Standards and Technology (NIST) in a publication for *small Business Information Security, “*If in your business, you send sensitive documents or emails, you may want to consider encrypting those documents and/or emails. Many document, and email applications provide for this capability. Typically, the receiver will need to have the same application to de-crypt the message or document as you used to encrypt it. If you need to send them a password or key, give it to them via phone or other method. Never send it in the same email as the encrypted document.” The use of unencrypted protocols being used can pose a risk to MITM attacks and leave valuable information exposed to the attacker.

References

*Small Business Information Security - NIST*, nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf. Accessed 6 July 2023.