Quinton Green

Emerging Technologies in Cybersecurity - C844

GRP1 TASK 1: NMAP AND WIRESHARK

The network topology found in NMAP was a star topology and contains 6 hosts. Here is a list of the IP addresses, open ports, and operating systems:

* Host 1: 10.168.27.1 – 0 open ports- no OS running.
* Host 2- 10.168.27.10 – 8 ports- Microsoft Windows Server 2012
* Host 3- 10.168.27.14- 1 port- Linux 2.6.32
* Host 4 – 10.168.27.15 – 10 ports – Microsoft Windows Server 2008 R2 or Windows 8.1
* Host 5 – 10.168.27.20 – 1 port – Linux 2.6.32
* Host 6 – 10.168.27.132 – 1 port – Linux 2.6.32

The vulnerabilities found on the network were FTP, HTTP, and a Windows 7 OS running. The implications of FTP running are that it is an insecure protocol relies on plain text usernames and passwords for authentication, which makes it vulnerable to sniffing, spoofing, and brute force attacks (Jethva, 2022). FTP leaves your confidential information open to eavesdropping and security breaches. The implications of HTTP on the network are that it is insecure, lacks encryption, open to man in the middle attacks, SQL Injection, cross-site scripting, and cross-site request forgery attacks. The attacker can alter the database, reconfigure files and directories affecting integrity, take over sessions affecting authentication and nonrepudiation and access user information or change credentials (PureVPN n.d.). The implications of Windows 7 OS running are that it reached its end-of-life support from Microsoft in 2015 and no longer receives security updates, patches for bug, or support. This leaves the outdated OS open to malware and security risks. Even if you use antivirus software the system is still open to newer malware types. The outdated OS also makes your system non-compliant with current regulations and security standards (Chris 2022).

For Wireshark, I used Pcap file #1 and found the following anomalies or vulnerabilities: LDAP, SMB Session Setup AndX response, Error: STATUS\_ACCOUNT\_DENIED, and HTTP GET/HTTP/1.0. In the range of packets in the screenshot it is showing the same source 10.16.80.243 and destination 10.168.27.10 over and over trying to send requests, get responses, and extend requests from the searchResEntry, bindRequest, and extendedResp codes showing. This appears to be an LDAP injection attack. According to cve.mitre.org, LDAP has a Denial-of-Service vulnerability which are caused by LDAP injection attacks (Mitre Corporation, 2022). The implications of not addressing LDAP are that it is insecure and open to be exploited by attackers with many other malicious attacks. LDAP is also susceptible to man in the middle attacks, eavesdropping over the network, packet interception, and packet integrity modifications due to the lack of encryption (Rublon Authors, 2022). All of these issues leak sensitive data, and can corrupt or alter important files (Dahan, 2022). The SMB anomaly is showing someone trying to gain access to file sharing from a guest account by sending authentication requests that are responding as a disabled account thus denying access. The implications of not addressing SMB are data exfiltration if the attacker can gain access and possible and remote code execution. SMB does have a remote code execution vulnerability according (Mitre Corporation 2022). The implications of not addressing HTTP anomaly GET/HTTP/1.0 are that it is insecure, and The HTTP GET request is commonly used to retrieve information from a web server by specifying a URL. Cyber attackers can take advantage of HTTP GET requests to obtain confidential information from the servers. Attackers can cause DOS attacks by sending abnormal amounts of GET requests to the web server. HTTP also leaves the system vulnerable to SQL injection, sensitive data exposure, security misconfiguration, cross-site scripting, broken authentication, and session management (Farid, 2023).

For the FTP vulnerability in NMAP, I recommend disabling FTP by closing ports 20 and 21 and switching to FTPS port 989 or SFTP port 22, use strong passwords, and strong encryption (Jethva, 2022). For the HTTP vulnerability close port 80 and enable port 443 for HTTPS which provides secure encryption for data transmitted over the network. For the Windows 7 OS issue you can upgrade to Windows 10 or 11 or move to a newer device that supports the minimum specifications for the newer OS (Chris, 2022). The newer OS will be supported for security, bug patches, updates, and have faster speeds.

For the LDAP vulnerability found in Wireshark, I recommend disabling port 389 and switching to LDAPS on port 636. LDAPS is secure, encrypts all data, and prevents data modifications maintaining integrity, and prevents network eavesdropping because it uses TLS encryption. (Rublon Authors, 2022). Also enforce input validation, implement the principle of least privilege, and escape input with encoding (Dahan, 2022). I recommend upgrading SMB to the latest version SMB Version 3.1.1 with AES-128 encryption and blocking TCP port 445 at the enterprise perimeter firewall and install patch updates (Jain, 2020). It is backwards compatible with the older versions and provides more security against cyber-attacks (Bhardwaj, 2023). For the HTTP vulnerability close port 80 and enable port 443 for HTTPS which provides secure encryption for data transmitted over the network. Implement the principle of least privilege, CSRF protection, security headers, X-XSS protection, validate untrusted data entry points from cookies, GET parameters, request headers, POST parameters, and use strict transport security (Srinivas, 2020).

**Screenshots**

**Login in screen**

A screenshot of a computer

Description automatically generated with medium confidence

**Network Topology- Star**

**A screenshot of a computer

Description automatically generated**

**Host 1 - 10.168.27.1 – 0 open ports - no OS running**

**A screenshot of a computer

Description automatically generated**

**Host 2 - 10.168.27.10 – 8 ports - Microsoft Windows Server 2012**

**A screenshot of a computer

Description automatically generated**

**Host 3 - 10.168.27.14 - 1 port - Linux 2.6.32**

**A screenshot of a computer

Description automatically generated**

**Host 4 – 10.168.27.15 – 10 ports – Microsoft Windows Server 2008 R2 or Windows 8.1**

**A screenshot of a computer

Description automatically generated**

**Host 5 – 10.168.27.20 – 1 port – Linux 2.6.32**

**A screenshot of a computer

Description automatically generated**

**Host 6 – 10.168.27.132 – 1 port – Linux 2.6.32**

**A screenshot of a computer

Description automatically generated**

**NMAP Vulnerabilities: FTP, HTTP, Windows 7**

**A screenshot of a computer

Description automatically generated**

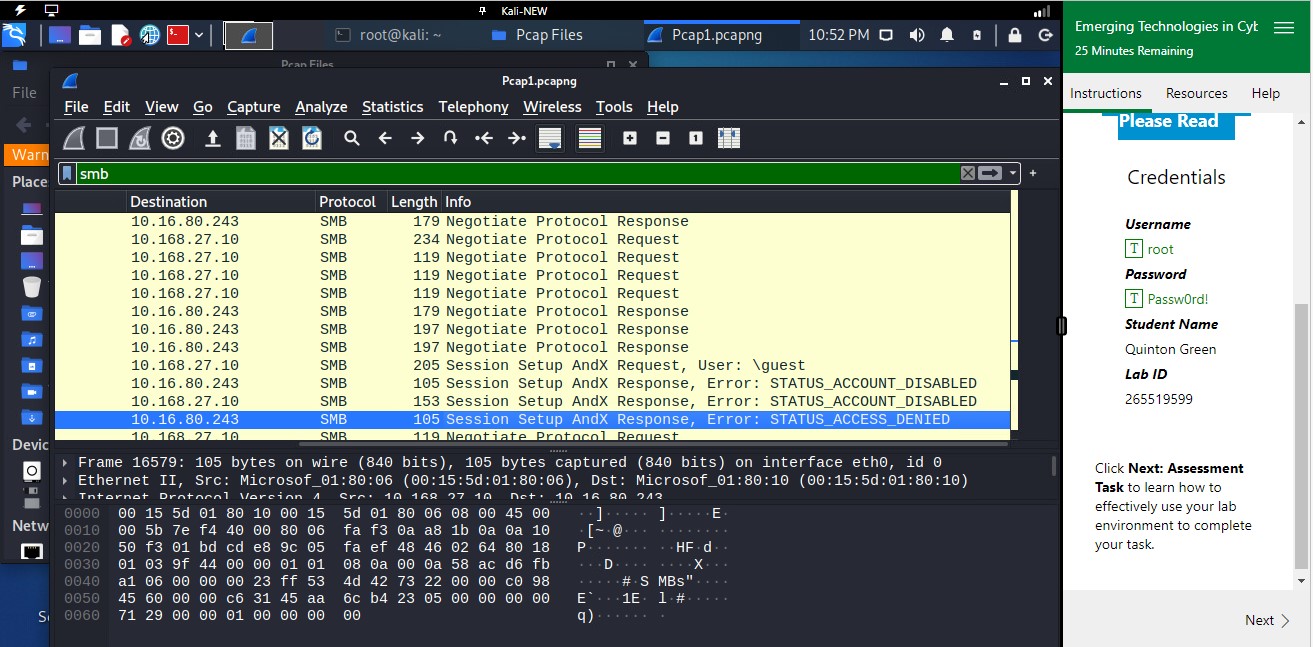
**Wireshark vulnerabilities/anomalies**

**LDAP**

**A computer screen shot of a computer

Description automatically generated with low confidence**

**SMB**

****

**HTTP**

**A screenshot of a computer

Description automatically generated**

**References:**

1. [Jethva, Hitesh. (2022, July 27), FTP Security Best Practices - FTP Vulnerabilities and Mitigation (cloudinfrastructureservices.co.uk)](https://cloudinfrastructureservices.co.uk/ftp-security-best-practices-ftp-vulnerabilities-and-mitigation/)
2. PureVPN. (n.d.). HTTP Vulnerability. PureVPN. Retrieved from <https://www.purevpn.com/ddos/http-vulnerability>
3. Chris, Lena (2022, October 20) [Windows 7 End of Life: Security Risks and Strategies (ubackup.com)](https://www.ubackup.com/windows-7/windows-7-end-of-life-risks-0040.html#:~:text=Windows%207%20end%20of%20life%20risks%3A%20you%20need%20to%20know,-As%20a%20matter&text=Among%20them%2C%20outdated%20software%20greatly,receiving%20security%20and%20feature%20updates.%22)
4. Rublon Authors (2022, November 21) [LDAP vs. LDAPS: What's the Difference? - Rublon](https://rublon.com/blog/ldap-ldaps-difference/#:~:text=The%20main%20difference%20between%20LDAP,over%20SSL%20or%20Secure%20LDAP.)
5. Bhardwaj, Pranav (2023, February 25) [SMB Protocol: How It Works and What Makes It Vulnerable (makeuseof.com)](https://www.makeuseof.com/what-is-smb-protocol-and-what-are-its-risks/#:~:text=SMB%20protocol%20is%20vulnerable%20to,to%20your%20files%20and%20data.)
6. Farid, Ammar Ahmad (2023) [What are HTTP protocol vulnerabilities? (educative.io)](https://www.educative.io/answers/what-are-http-protocol-vulnerabilities)
7. [The MITRE Corporation](https://www.mitre.org/) (2023 February 17) [CVE - CVE-2023-26044 (mitre.org)](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26044)
8. Portswigger LTD (n.d) [Exploiting HTTP request smuggling vulnerabilities | Web Security Academy (portswigger.net)](https://portswigger.net/web-security/request-smuggling/exploiting)
9. Srinivas (2020, December 8) [How to Mitigate Poor HTTP Usage Vulnerabilities | Infosec Resources (infosecinstitute.com)](https://resources.infosecinstitute.com/topic/how-to-mitigate-poor-http-usage-vulnerabilities/)
10. Dahn Marc (2022, June 19) [What are LDAP injection attacks and how to prevent them (comparitech.com)](https://www.comparitech.com/blog/information-security/prevent-ldap-injection-attacks/)
11. Microsoft (2[023 February 27) MS-SMB2]: Receiving an SMB2 SESSION\_SETUP Request | Microsoft Learn](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/e545352b-9f2b-4c5e-9350-db46e4f6755e)
12. Jain, Animesh (2020, March 11) [Microsoft Windows SMBv3 Remote Code Execution Vulnerability (CVE-2020-0796) | Qualys Security Blog](https://blog.qualys.com/vulnerabilities-threat-research/2020/03/11/microsoft-windows-smbv3-remote-code-execution-vulnerability-cve-2020-0796)