A logo of a university

Description automatically generated

**Western Governor’s University**

Emerging Technologies in Cybersecurity

C844

Joshua Lee

GRP1 Task 1: Nmap and Wireshark

1. **Describe the Network Topology**

A screenshot of a computer program

Description automatically generated

**A computer screen shot of a computer

Description automatically generated**

A diagram of a network

Description automatically generated

**Topology for this network is a Star Topology**

Being a Star Topology, this functions where the **localhost** is the central hub for the network. All the hosts connected to it sends messages out of network and to other hosts through the central node.

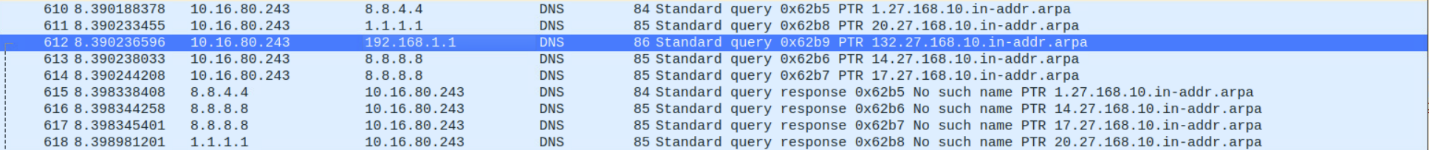
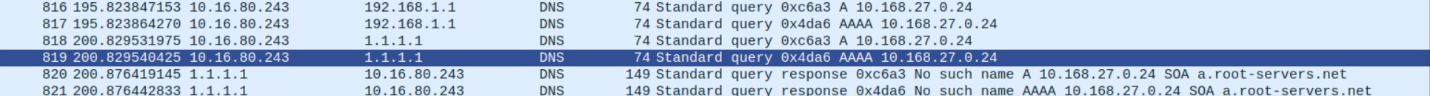
When performing a Quick Scan Plus through Zenmap with the provided network of 10.168.27.0/24, there were six hosts found. 10.168.27.1 was showing no open ports, but also did not give information on a operating system applied to the host or a MAC address associated with it. 10.168.27.10 was running either Microsoft Windows Server 2012 or Windows Server 2012 R2 and had 8 open ports. 10.168.27.15 was running Microsoft Windows Server 2008 R2 or Windows 8.1 and had 10 open ports. There were also three Linux systems running Kernel Version 2.6.32 and they all had 1 port running. Their addresses were 10.168.27.14, 10.168.27.20, and 10.168.27.132.

1. **Nmap Summary of Vulnerabilities and Implications**

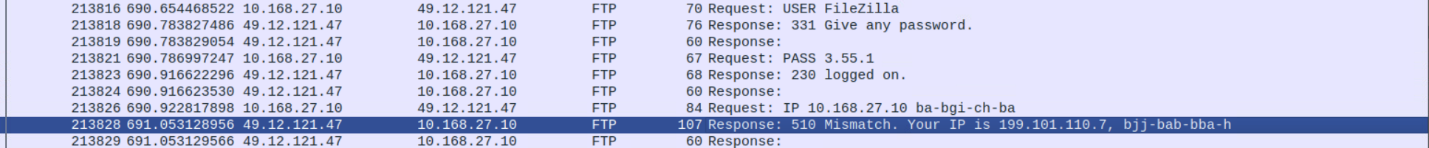
The first issue I noticed was at host 10.168.27.15 and it had to deal with the open port 21/tcp which is used for sending control information through FTP. Being that it is FTP and not SFTP, the information is susceptible to sniffing, spoofing and other types of attacks due to the information being sent in-the-clear (*What Is FTP Security?*, n.d.). This port is running Filezilla FTPD, which is a server oriented process for FTP, and there is a vulnerability where Filezilla Server can be susceptible to a buffer overflow attack. This will allow the threat actor to initiate a Denial of Service related to SSL/TLS packets (*CVE - CVE-2009-0884*, n.d.). The implications of a DoS attack would be to degrade or even interrupt services that are provided on this server and reduce Availability, which is a major part of the CIA Triad.  
  
Another issue was also prevalent on host 10.168.27.15. This now occurring on port 80/tcp, which is used for unencrypted HTTP traffic. HTTP messages are in-the-clear and can be easily accessed and read if a threat actor wanted to intercept them. This port is running Microsoft IIS HTTPD 8.5. The vulnerability to this is that the IP Security feature in this particular web server does not properly process Allow and Deny rules in the “IP Address and Domain Restrictions” list. This allows a threat actor to bypass rules set forth via a HTTP request and bypass security (*CVE - CVE-2014-4078*, n.d.). The implications of this would be that the threat actor would have access to data on the web server and could affect all three parts of the CIA Triad. They could get access to information not intended for public access which breaches Confidentiality. They could alter data on the web server which would affect Integrity. Finally, they could launch an attack from within the server to disrupt or interrupt service which would affect Availability.

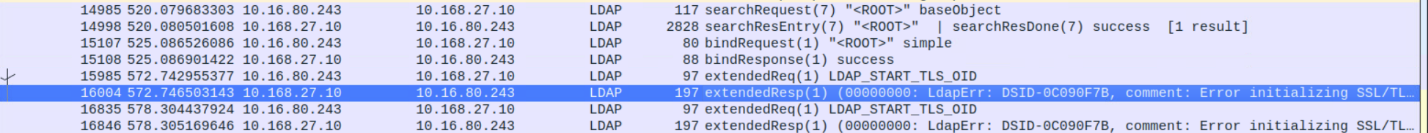
One more vulnerability has to deal with Linux Kernel Version 2.6.32 that is ran by hosts 10.168.27.14, 10.168.27.20, and 10.168.27.132. The vulnerability is that this version is that if a threat actor floods the diagnostic port 0x80, an exception can be triggered which can lead to kernel panic (*CVE - CVE-2017-1000407*, n.d.). Kernal panic is a term in which the OS determines that there might be a fatal error that can cause data loss or not be able to recover if it continues and enacts as a safety measure, similar to the Windows “Blue Screen of Death” (“Kernel Panic,” 2023). The implication of this is a Denial of Service and interruption in the Availability of the device.

1. **Anomalies in Wireshark**

One of the first anomalies I found was with frame 613. If you look at the range of frames from 610-618 (excluding 613). They are all going to common DNS servers for requests, such as Google’s Public DNS and Cloudflare DNS. Frame 613 is trying to get a response from 192.168.1.1 that is not a DNS server but a Class C private IP address. All the other requests got responses back saying the query response is not found except Frame 613. This is further validated in the second screenshot in frames 816-821 where the 10.16.80.243 is asking the same query for an A and AAAA DNS record and the Cloudflare DNS responds back but the Class C private address does not.



Another anomaly is through the above range frames from 213813-231829. The error on this is on frame 213828 where it is saying that there is an IP mismatch with IP 199.101.110.7. Which is valid since the request is coming from 49.12.121.47.  
  


One more anomaly shows up a couple times in the above frames 15985, 16004, 16835, 16846. If you look at the above frames in the screenshot, there were no issues with LDAP in the previous frames.

1. **Wireshark Anomaly Implications**

The implications for taking no action on the DNS requests going to a Class C Private address from a Class A network are some DNS queries are going to not being answered which lead to performance issues. This can lead to back up in productivity on host 10.16.80.243 when trying to access sites by name.

For taking no action on the Filezilla issue, the implications can be a couple things. If the person requesting to get into Filezilla is legitimate (maybe behind a VPN or proxy), they will not be able to get access to the FTP server. If this is a malicious intent and not checked after, they address could keep attempting to connect to the FTP if they are using a phished password and get through if they are able to do so from an approved IP address.

If no action is taken for the LDAP issue, the host/user will not be able to log in. This will create a delay in work and the user will not be able to access resources that are attached to their LDAP login.

1. **Solutions for Nmap Vulnerabilities and Wireshark Anomalies**

For the FTP and Filezilla vulnerability, it would be a two-prong solution. The first would be to use SFTP port 22/tcp instead of FTP port 21/tcp. The reason for this is instead of your data being sent in-the-clear, it encrypts the data in transit to keep threat actors from intercepting your data and allows authentication procedures (username and password) for that extra layer of security (Integrate.io, n.d.). For the Filezilla portion, the vulnerability is for versions of Filezilla Server before 0.9.31 (*CVE - CVE-2009-0884*, n.d.). You would make sure that the software is running a later version and if not make sure it gets updated to after the vulnerable version, preferably the latest stable version (*FileZilla Server SSL/TLS Denial of Service CVE-2009-0884 Vulnerability Report*, n.d.). One more thing to make sure this whole solution works is to make sure you are using the paid version of Filezilla Server, as the free version of Filezilla server does not support STFP (*Filezilla Server Using Port 22 - FileZilla Forums*, n.d.).

For the HTTP and Microsoft IIS 8.5 issue, it would also be a two-part solution. The first part would be to send the data over HTTPS instead of HTTP. This is similar to the FTP/STFP vulnerability above being that HTTP is sent in-the-clear and HTTPS allows encryption in transit and verification (*Why Is HTTP Not Secure?*, n.d.). The Microsoft IIS 8.5 vulnerability, you would make sure the Microsoft security update is applied in order to have it be resolved (BetaFred, 2023).

The hosts that are on Linux 2.6.32 that are susceptible to the vulnerability that can create kernal panic in the OS, it would be best to make sure the fix is run to correct the issue. The problem with this version would be that this versions End of Life was in March 2016, which means there is no more support (“Linux Kernel Version History,” 2023). It would be best to update to the newest version that the hardware can effectively handle and make sure up to date fixes are in place since the vulnerability is for 2.6.32 and later (*CVE - CVE-2017-1000407*, n.d.).

The DNS server for the Class A server should not be a Class C address. You can change it to the right default gateway address or a different DNS server through changing the default though command line with admin credentials by inputting “Nslookup IP\_Adress DNS\_Server” (Wasif, 2020). You can set it to your default gateway or one of the various reputable DNS servers, such as Google DNS or Cloudflare DNS (updated, 2022).

The Filezilla anomaly that Is allowing to access to the FTP server would be simple. You would want to make sure that your client and network is configured for Active Mode through Filezilla (*[Ubuntu] [SOLVED] Ftp / Ports / Lokkit [Archive] - Ubuntu Forums*, n.d.) By making sure the server and client are both set to Active, this should allow the IP address to resolve for Filezilla connectivity.

To fix the LDAP issue, is to see why the issue is taking place. This error is because the user changed their LDAP authentication to LDAP SSL authentication and it more than likely, on their side is saying the account is invalid. To fix this, the LDAP certificate needs to be configured before using LDAPS (*LDAP SSL - Invalid User Account-LdapErr-DSID-0C090FB4-Error-Initializing-SSL*, n.d.).

**References**

BetaFred. (2023, March 1). *Microsoft Security Bulletin MS14-076—Important*. <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-076>

Integrate.io. (n.d.). SFTP vs. FTP: Understanding the Difference. Integrate.Io. Retrieved November 4, 2023, from <https://www.integrate.io/blog/sftp-vs-ftp-understanding-the-difference/>

updated, M. W. last. (2022, January 26). *Best free and public DNS servers of 2023*. TechRadar. <https://www.techradar.com/news/best-dns-server>

Wasif. (2020, June 18). *Answer to “How do I change the default server for nslookup?”* Super User. <https://superuser.com/a/1561716>

*CVE - CVE-2009-0884*. (n.d.). Retrieved October 29, 2023, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0884>

*CVE - CVE-2014-4078*. (n.d.). Retrieved October 29, 2023, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4078>

*CVE - CVE-2017-1000407*. (n.d.). Retrieved October 29, 2023, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000407>

*FileZilla Server SSL/TLS denial of service CVE-2009-0884 Vulnerability Report*. (n.d.). Retrieved November 4, 2023, from <https://exchange.xforce.ibmcloud.com/vulnerabilities/exchange.xforce.ibmcloud.com/vulnerabilities/49107>

*Filezilla server using port 22—FileZilla Forums*. (n.d.). Retrieved November 4, 2023, from <https://forum.filezilla-project.org/viewtopic.php?t=55669>

*LDAP SSL - invalid user account-LdapErr-DSID-0C090FB4-Error-initializing-SSL*. (n.d.). Retrieved November 4, 2023, from <https://support.citrix.com/article/CTX222350/ldap-ssl-invalid-user-accountldaperrdsid0c090fb4errorinitializingssl>

*[ubuntu] [SOLVED] ftp / ports / lokkit [Archive]—Ubuntu Forums*. (n.d.). Retrieved November 4, 2023, from <https://ubuntuforums.org/archive/index.php/t-865915.html>

*What is FTP Security? Securing FTP Usage*. (n.d.). [Text]. Retrieved October 28, 2023, from <https://www.digitalguardian.com/blog/what-ftp-security-securing-ftp-usage>

*Why is HTTP not secure? | HTTP vs. HTTPS*. (n.d.). Cloudflare. Retrieved November 4, 2023, from <https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/>

Kernel panic. (2023). In *Wikipedia*. <https://en.wikipedia.org/w/index.php?title=Kernel_panic&oldid=1178158266>

Linux kernel version history. (2023). In *Wikipedia*. <https://en.wikipedia.org/w/index.php?title=Linux_kernel_version_history&oldid=1183335671>