Penetration Test Report Lab Week #8

Jordan Torres
03-NOV-2024

Penetration Testing LLC

Upson II Room 366
243 Centennial Dr Stop 7165
Grand Forks, ND 58202
United States of America

Tel: 1-701-777-2180
Fax: We still use these :)
Email: jordan.torres@und.edu
Web: http://www.penetrationtestingllc.com

Table of Contents

Version Control

Version	Title	Author	Description	Date
0.1	Initial Report	Jordan Torres	Report Template Created	10-OCT-2024
1.0	Penetration Test Lab Report Week #8	Jordan Torres	Created new report, screenshots, and edited report	02-NOV-2024

Point of Contact

Contractor

Jordan Torres

Upson II Room 366
243 Centennial Dr Stop 7165
Grand Forks, ND 58202
United States of America
Email: jordan.torres@und.edu
Tel: 1-701-777-2180

Client

CSCI 487 Penetration Testing

Project Details

Project Objectives

Module 5, Exercise 1: Exploring and Auditing a Machine Using Nmap

Module 5, Exercise 2: Accessing Misconfigured FTP Connection on a Remote Machine

Scope of Work

Complete the tasks in EC-Council's lab by working through module 5. After finishing, compile findings into a report and submit it for grading.

Period of Testing

27-OCT-2024 to 03-NOV-2024

Executive Summary

This lab provides essential skills in network scanning, vulnerability analysis, and network security maintenance, in conducting comprehensive network assessments. The exercise includes identifying live systems and open ports and OS fingerprinting, analyzing network vulnerabilities, mapping vulnerable hosts, and performing penetration tests to assess network weaknesses.

The lab centers on external penetration testing, simulating real-world scenarios in which an external attacker might exploit network vulnerabilities to compromise security. By identifying issues such as weak authentication and unnecessary services we can gain insight into the key weaknesses that could compromise network confidentiality, integrity, or availability.

A primary focus is the detection of FTP servers with anonymous access enabled, which poses a critical security risk by allowing unrestricted access to sensitive files. We conduct port and network scanning, vulnerability identification, and mapping, simulating penetration testing tasked with identifying and mitigating security threats in an organization's network.

Upon completion, we will have a foundational understanding of penetration testing and the ability to recognize and address common vulnerabilities, enhancing the security posture of any organization they support.

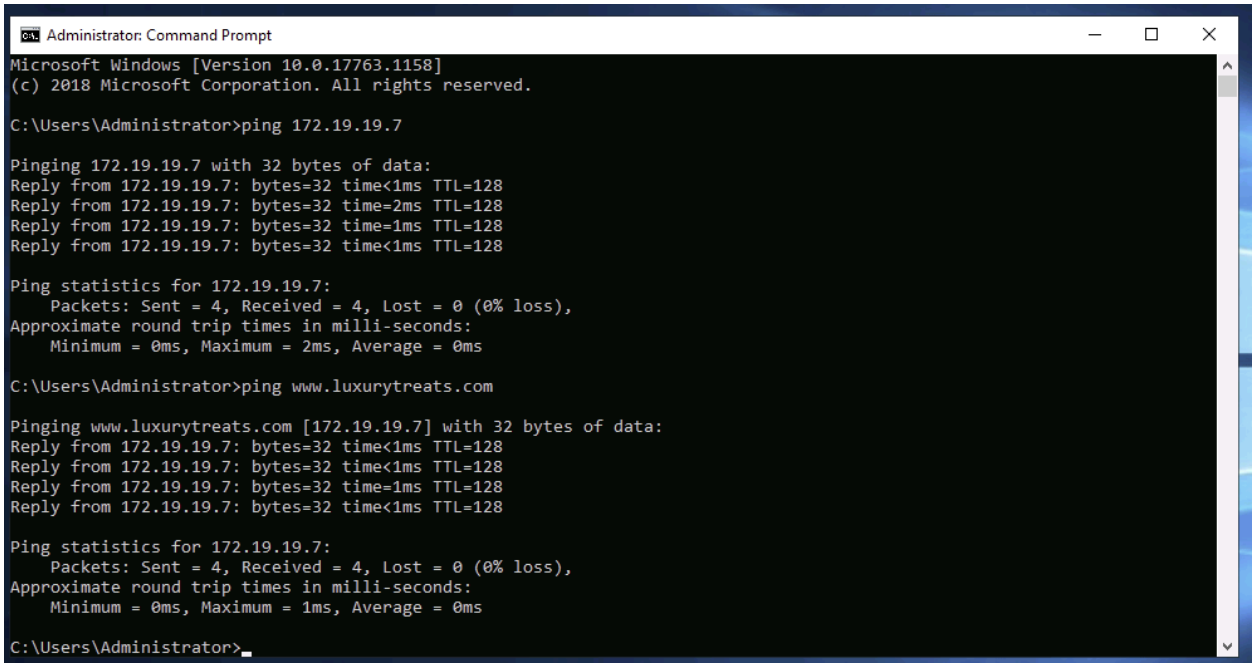
Exercise 1 - ZenMap (Nmap)

https://nmap.org/zenmap/

Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.[1]

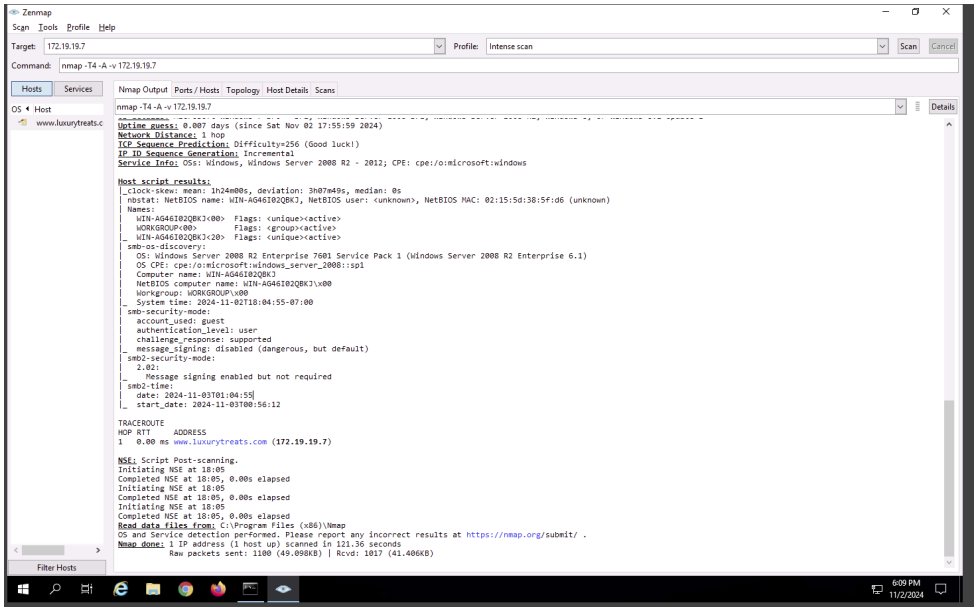
This exercise we will analyze all IP addresses, open and closed ports, services and protocols during the scan of www.luxurytreats.com.

Finding IP addresses

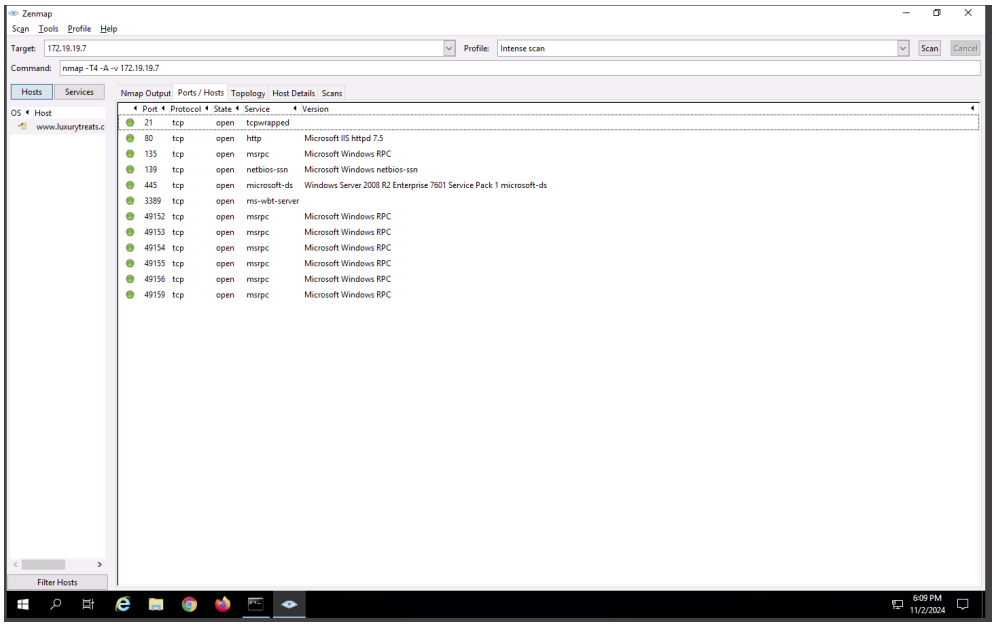


[1] https://nmap.org/zenmap/

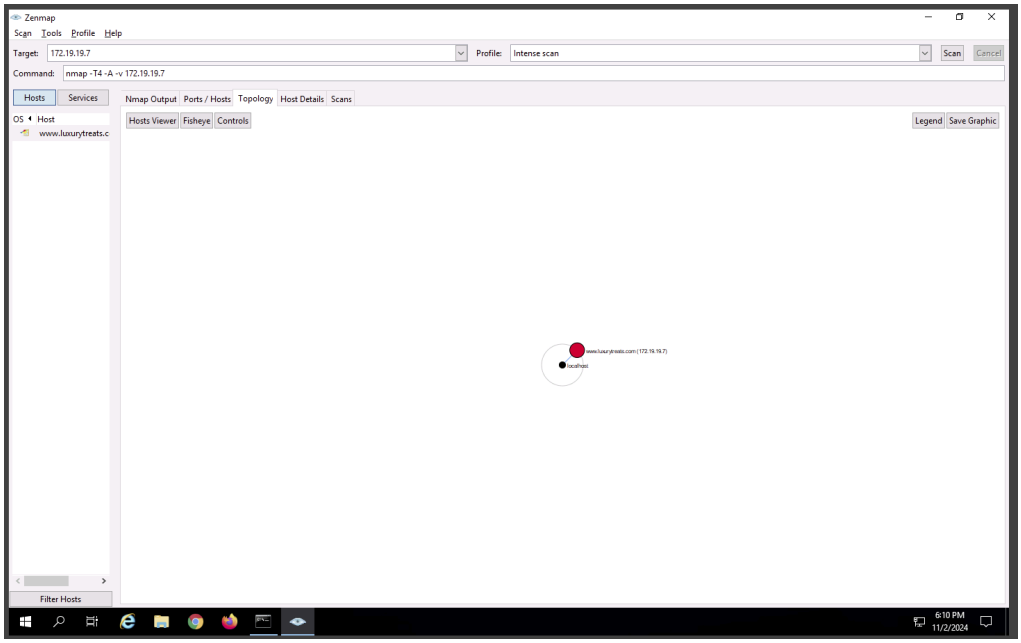
Run Scan



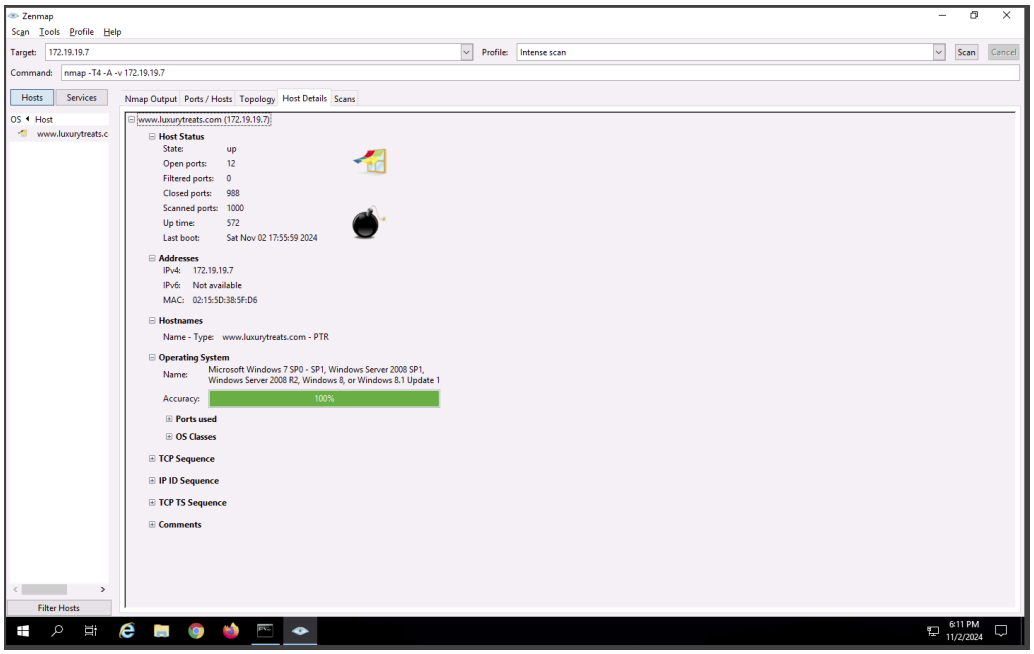
Found hosts and ports



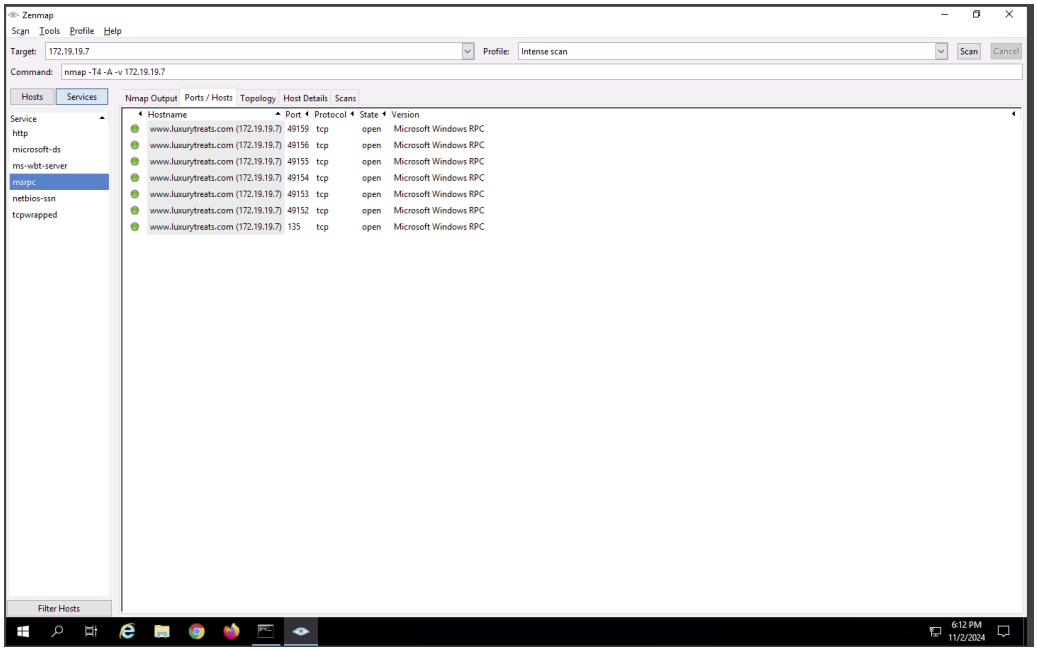
Topology Display



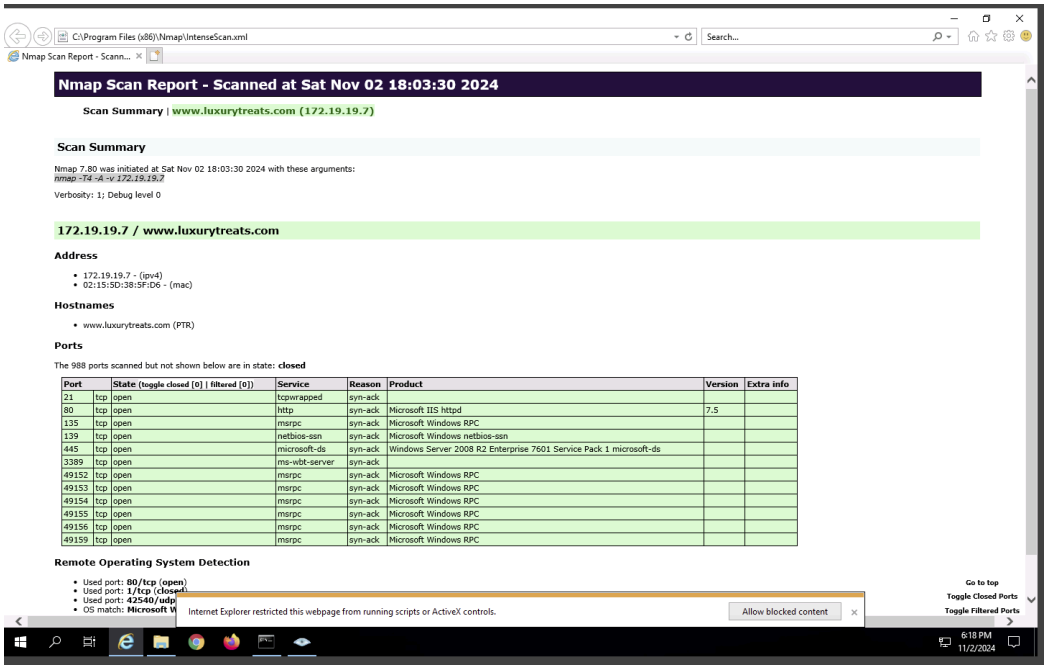
Host Detail



Host Services - MSRPC



Nmap Scan Report



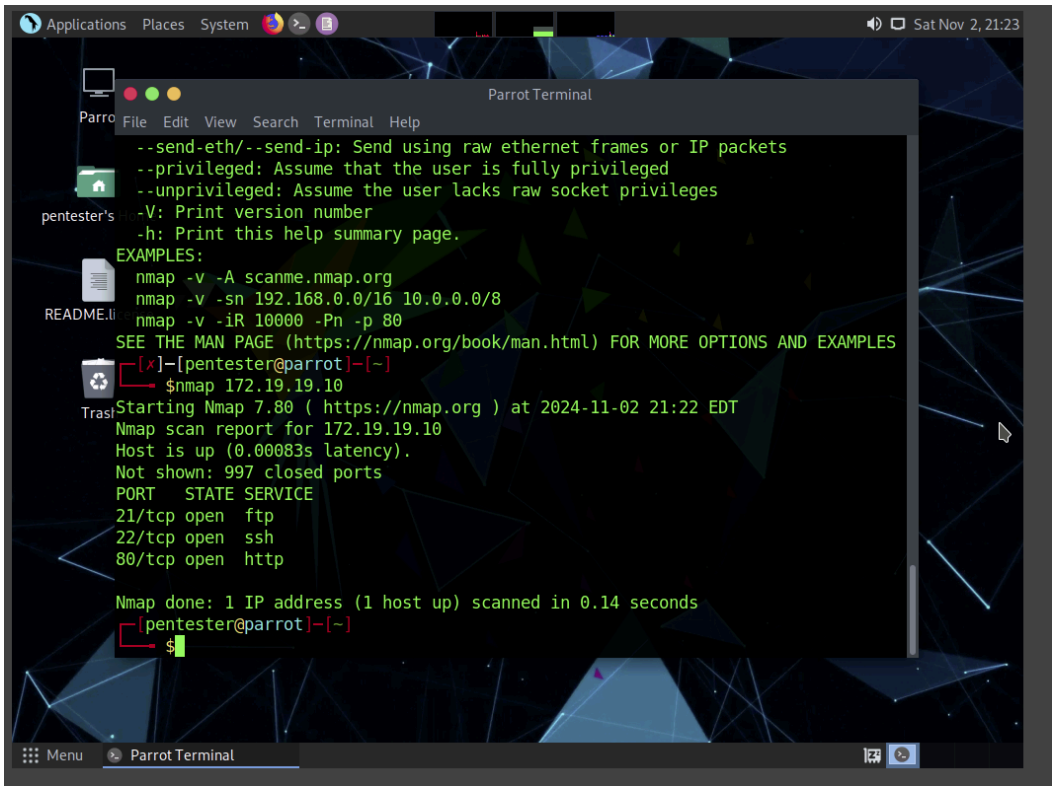
Exercise 2 - Parrot Terminal - Nmap - FTP

https://nmap.org/

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.[2]

Checking for open ports

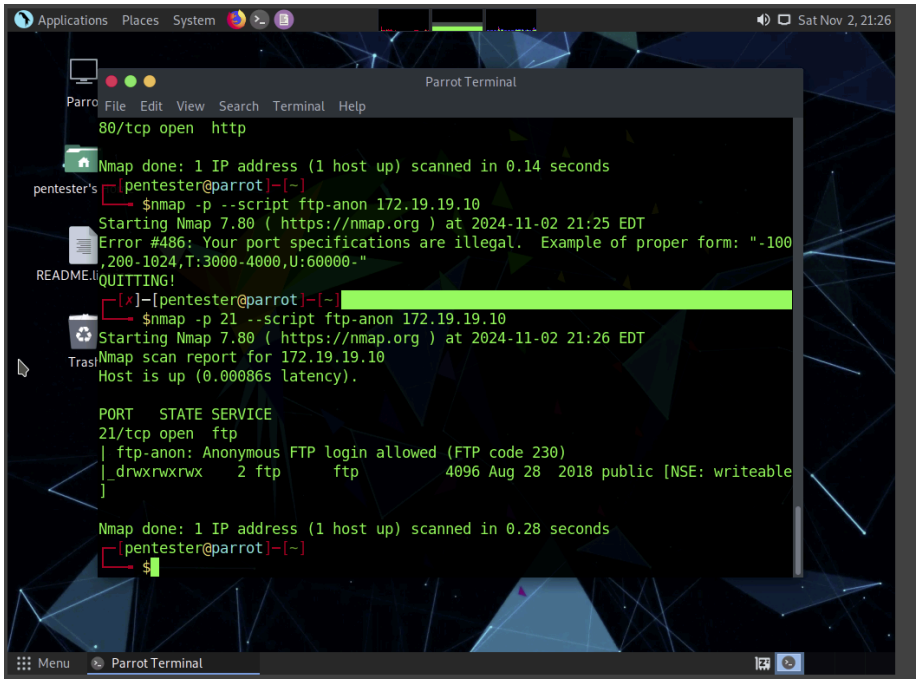
- Nmap on terminal for IP address 172.19.19.10



[2] https://nmap.org/

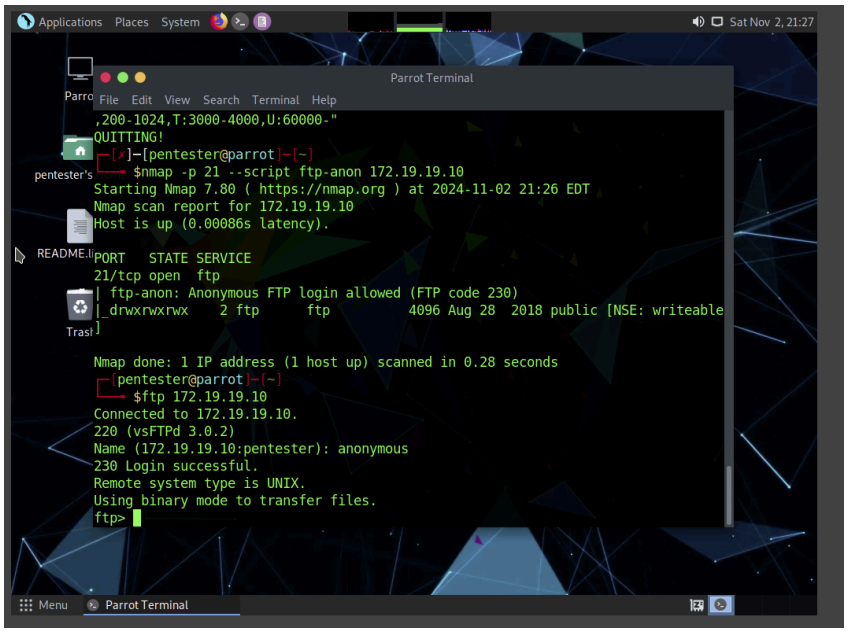
Check if FTP is Anonymous

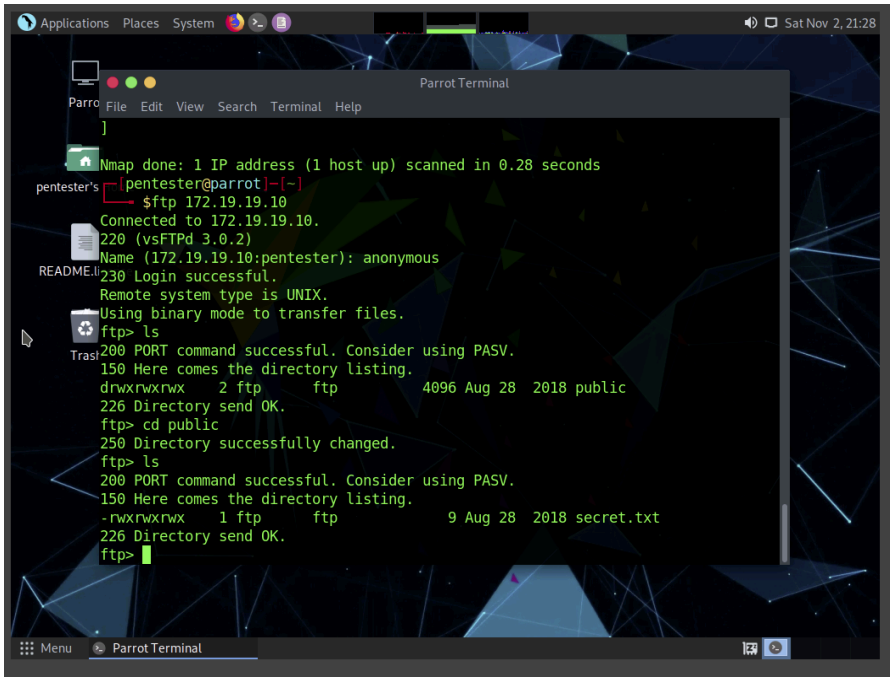
- Command - nmap -p 21 –script ftp-anon 172.19.19.10

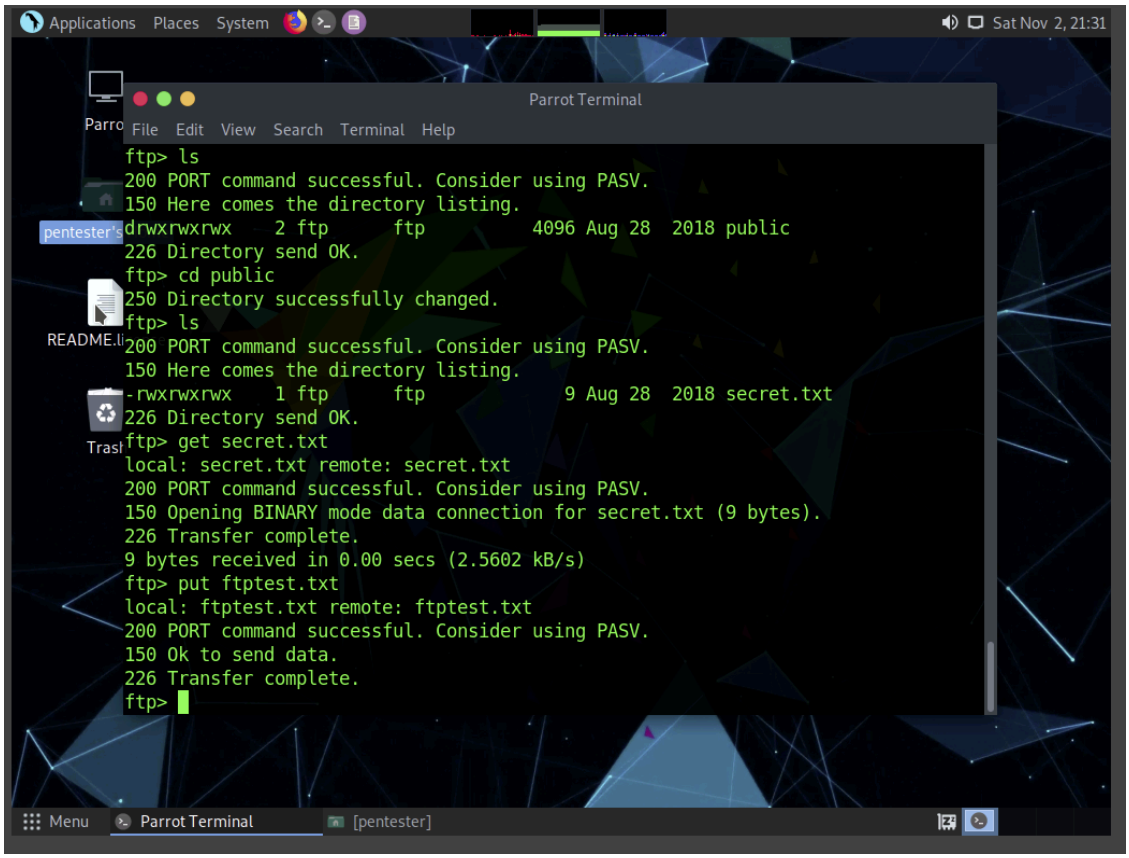


FTP anonymous active

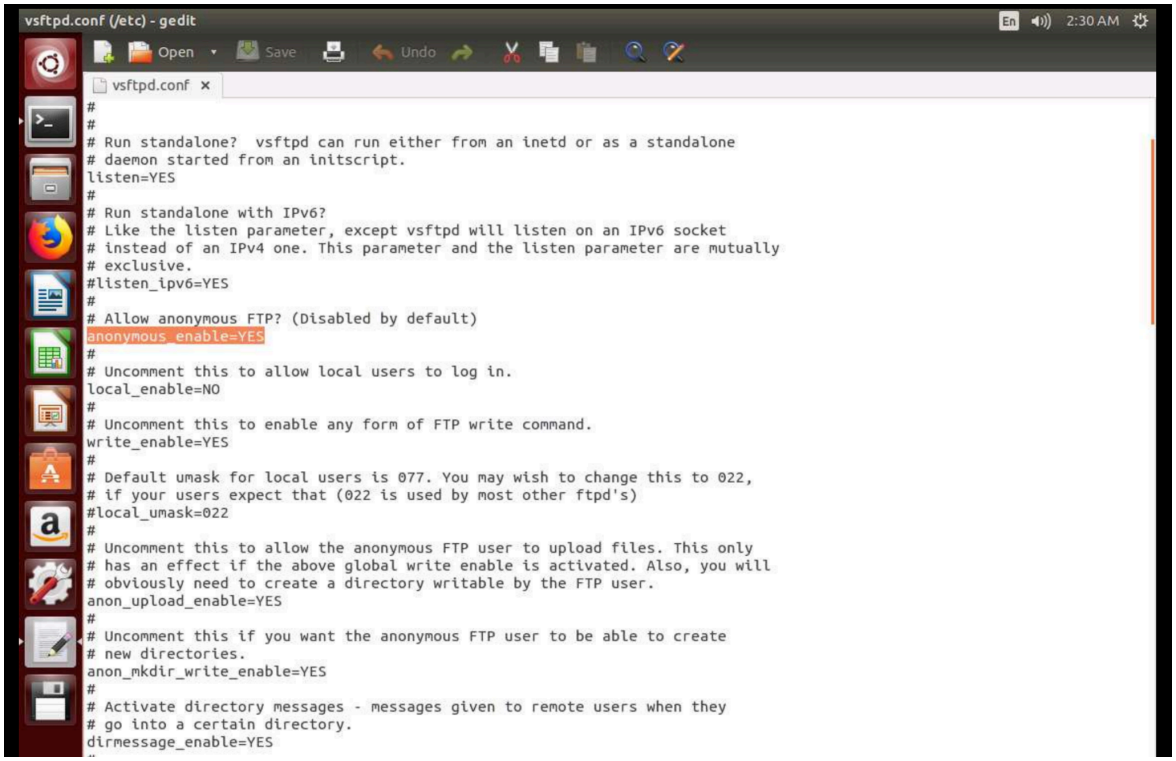
- Able to login, download, and upload files

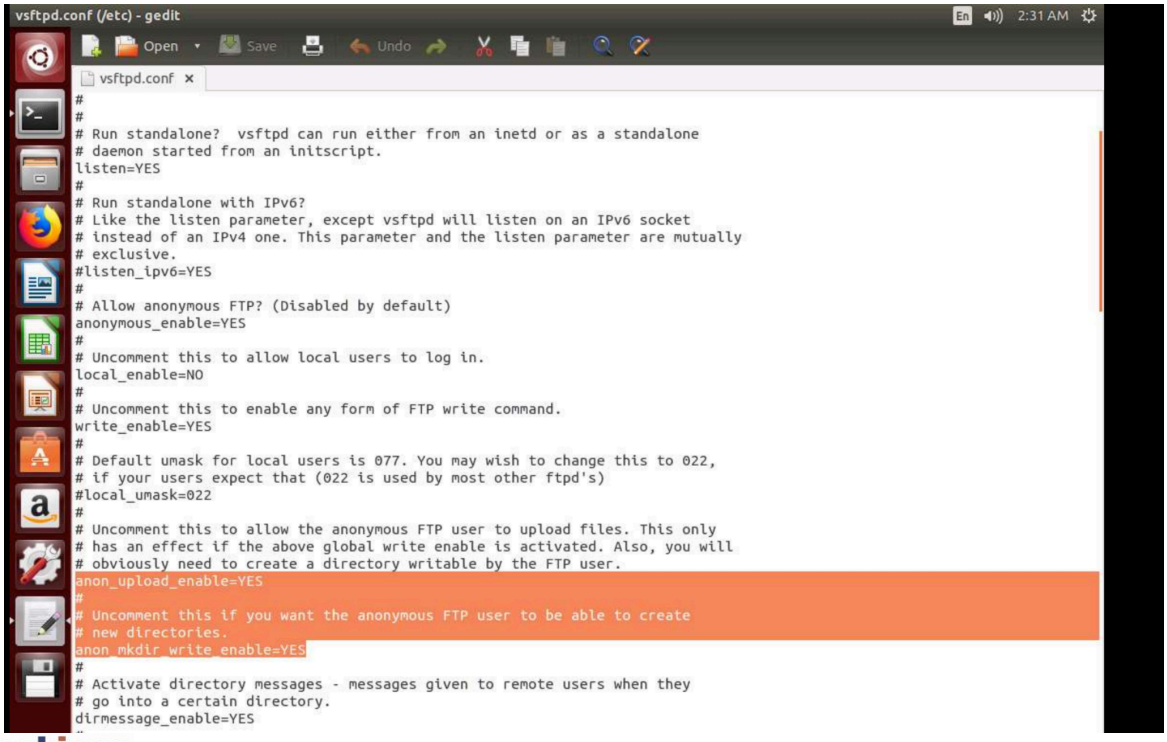






Configuration File





Conclusion

This lab provided a comprehensive hands-on experience in network scanning, vulnerability analysis, and network security maintenance, all critical skills for both network security administrators and penetration testers. By using tools such as Zenmap and Nmap, we gained the ability to identify live hosts, open ports, and the services running on those ports. Key tasks included performing banner grabbing, OS fingerprinting, and network topology mapping, essential steps in assessing the security posture of a network.

Through **e**xercise 1, we successfully analyzed network hosts and cataloged open and closed ports, services, and protocols, which are foundational steps in vulnerability assessment. This exercise emphasized network layout and identifying potential points of attack.

Exercise 2 introduced the specific challenge of identifying FTP servers allowing anonymous access. By connecting to these servers, we were able to see firsthand how easily misconfigured services can compromise data confidentiality and increase exposure to unauthorized access.

Overall, this lab underscored the importance of proactive security measures, including closing unnecessary ports, enforcing strong authentication, and conducting regular vulnerability scans. These actions are essential in maintaining a secure network environment and protecting organizational data from external threats.

Recommendations

Disable anonymous FTP access or restrict it only to users with a legitimate need. For any FTP access, use more secure alternatives like SFTP (Secure File Transfer Protocol) or FTPS (FTP Secure) to encrypt data in transit. Also, close unnecessary ports to minimize the attack surface, restrict access to essential ports using firewalls, only allowing trusted IP ranges. Regularly update and patch services on open ports to reduce vulnerabilities. Use intrusion detection systems (IDS) to monitor and log access attempts on critical ports.

Risk Rating

Anonymous FTP Access

Risk Level: High

Impact: Allowing anonymous access on FTP servers poses a significant security risk, as it enables any user, without authentication, to access, upload, and potentially download files on the server. This access could expose sensitive information to unauthorized users, create an opportunity for data exfiltration, or allow an attacker to plant malicious files. Additionally, attackers could exploit this access to gather information about the network or use the server as a platform to distribute malware.

Likelihood: Moderate to High
Many attackers routinely scan networks for servers with open FTP ports (usually port 21) and test for anonymous access. Anonymous FTP is known to be an insecure setup, so any FTP server configured this way is at high risk of exploitation.

Open Ports

Risk Level: Varies (Low to High)

Impact: Open ports provide entry points into the network and allow potential attackers to interact with exposed services. The risk associated with each open port depends on the service running and its configuration. For instance:

- Low Risk: Ports used for well-secured internal services or encrypted communications with strict access control.
- Moderate to High Risk: Ports associated with outdated or vulnerable services (e.g., Telnet on port 23, SMB on port 445), especially if accessible from outside the network, as they can be exploited for unauthorized access, data breaches, or service disruption.

Likelihood: Moderate to High
Attackers commonly scan networks for open ports as part of their reconnaissance. Open ports with misconfigured or vulnerable services are especially attractive targets. For example, open ports without strong authentication or encryption invite brute force attacks and information leaks.

Reflection

Addressing anonymous FTP access and open ports is essential in a secure network environment. By controlling access to FTP servers and managing open ports carefully, organizations can significantly reduce the risk of unauthorized access, data leakage, and other malicious activities

Appendix A: About Penetration Testing LLC

Penetration Testing LLC is a specialized network security firm dedicated to safeguarding businesses from potential cyber threats. We offer comprehensive penetration testing services that identify vulnerabilities within networks, applications, and systems. Our team of certified ethical hackers utilizes cutting-edge tools and techniques to simulate real-world cyberattacks, helping organizations fortify their defenses. By delivering detailed reports and actionable recommendations, Penetration Testing LLC ensures that businesses remain resilient against emerging threats, while also maintaining compliance with industry standards and regulations. Our commitment to security excellence empowers clients to proactively protect their digital assets and maintain business continuity.