

## Lab 2: Performing a Vulnerability Assessment

Osamudiamen Eweka

Cyb-605-Z2 Principles of Cybersecurity

Utica University

## **Introduction**

In this lab, we will be simulating a penetration test and vulnerability assessment of a networked environment. Vulnerability assessments and penetration testing are essential for identifying and mitigating potential weaknesses in information security systems (Kim, 2021). The primary goal of this exercise is to identify potential vulnerabilities and security weaknesses within the target network and to provide recommendations for remediation. We will be using various tools and techniques, such as Nmap, Nessus, and OpenVAS, to conduct scans, identify vulnerabilities, and generate detailed reports based on our findings.

The lab is divided into three sections, each focusing on different aspects of the penetration test and vulnerability assessment process. In the first section, we will use Zenmap and Nessus to scan and assess the security posture of a network, while in the second section, we will conduct external vulnerability scans using Nmap and OpenVAS. Finally, in the third section, we will analyze the findings from the scans and prepare a comprehensive penetration test report for the target network.

Throughout the lab, we will emphasize the importance of understanding the purpose and scope of the penetration test, as well as the severity of identified vulnerabilities. We will also explore the process of researching and analyzing CVE entries to gain a deeper understanding of the identified vulnerabilities and their potential impact on the target network. Overall, this lab will provide valuable hands-on experience in conducting vulnerability assessments and penetration tests, essential skills for any aspiring cybersecurity professional.

## **Objective**

The objective of this lab is to simulate a real-world scenario where a penetration test and vulnerability assessment are conducted in a networked environment. The lab aims to familiarize students with the tools and techniques used in these activities, such as Nmap, Nessus, and OpenVAS, and to provide hands-on experience in identifying and analyzing vulnerabilities, as well as generating detailed reports based on the findings. By completing the lab, students will gain practical knowledge and skills in conducting security assessments, understanding the cyber kill chain, and recommending mitigation strategies for identified vulnerabilities.

### **LAB Setup**

The lab setup for this exercise includes the use of virtual machines and specific software and tools to conduct a vulnerability assessment and penetration test. The hardware used for the lab setup is not explicitly mentioned in the uploaded material, but it can be inferred that virtual machines are being utilized for the exercises.

**Hardware:**

- vWorkstation (Windows: Server 2022)
- Switch01 (Linux: Debian 11)
- FileServer01 (FreeBSD)
- pfSense-office (FreeBSD)
- pfSense-dc (FreeBSD)
- DomainController01 (Windows: Server 2019)
- WebServer01 (Linux: Ubuntu 20)
- AttackLinux01 (Linux: Kali)
- GSM (Linux: Greenbone OS)

**Software and Tools:**

- Nmap/Zenmap
- Nessus
- OpenVAS/Greenbone Security Manager
- Kali Linux distribution
- Zenmap GUI
- Nessus vulnerability scanner
- Nmap command line version

## Section 1: Hands-On Demonstration

### Part 1:

#### *Scan The Network with Zenmap*

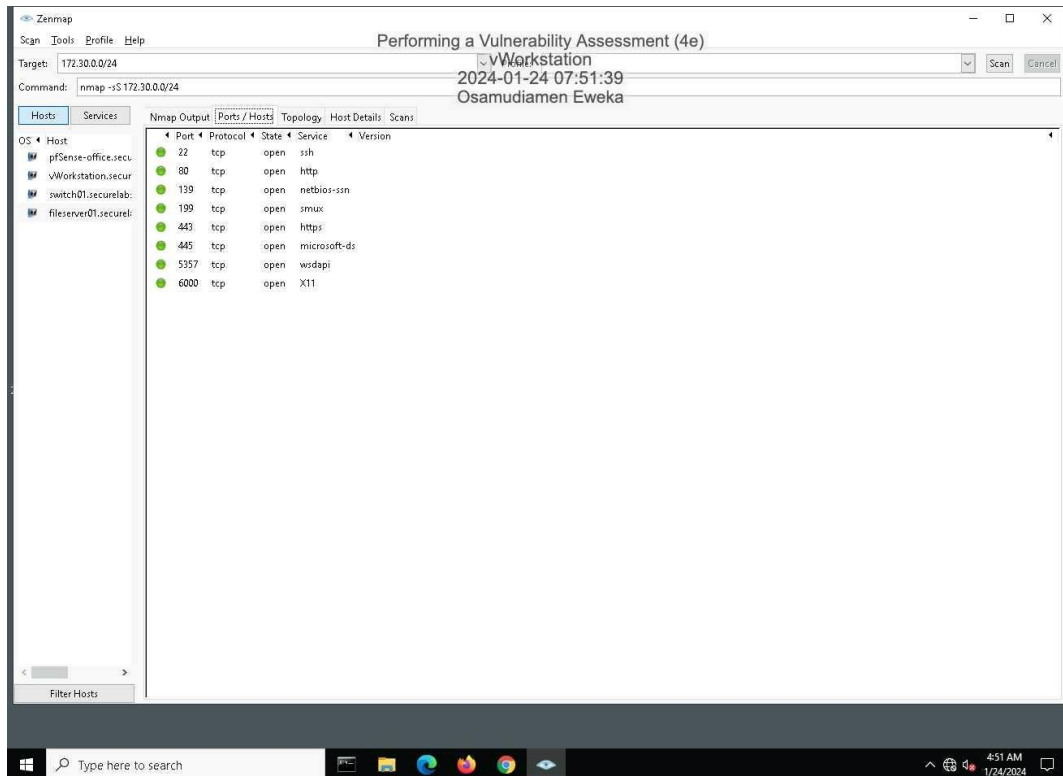
In Hands-On Demonstration, the process begins with using the Zenmap application to scan the local area network at the Secure Labs on Demand office LAN. The target field is set to specify the 172.30.0.0/24 subnet, and a Ping scan is selected from the Profile menu to initiate the scan. The scan returns four results representing the different machines detected on the specified target network segment. The host fileserver01.securelabsondemand.com is selected, and the Host Details tab is clicked to view an organized summary of the information gathered during the scan.

The next step involves interacting with multiple ports on each host, and a Service scan is initiated on the network by using the -O and -sV switches in the Command box. After the scan is complete, the Ports/Hosts tab is clicked to display the ports and services detected by the Service scan. The scan reveals the versions of the services running on the TCP protocol, such as the Nginx web server software running at port 80 on the fileserver01 host. The scan results are then saved to a new folder on the vWorkstation Desktop, and the Zenmap window is closed.

In summary, the process involves using Zenmap to conduct a network scan, identify hosts and their services, and gather detailed information about the operating systems and versions running on the network. The screen capture requested in Figure 1 (Eweka, 2024), is of the contents of the Ports/Hosts tab from the SYN scan for fileserver01.securelabsondemand.com.

**Figure 1**

*Make a screen capture showing the contents of the Ports/Hosts tab from the SYN scan for fileserver01.securelabsondemand.com.*

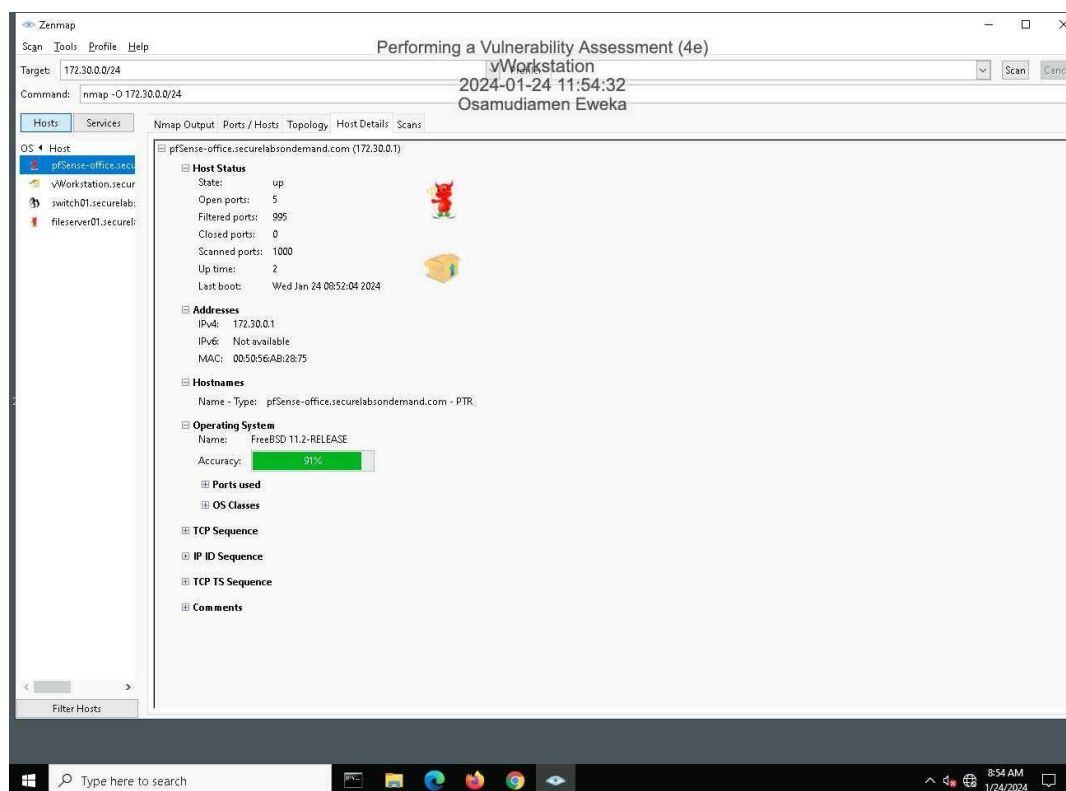


in the next step, the user engages in configuring and executing an Operating System (OS) detection scan through Zenmap. They start by modifying the command in Zenmap to incorporate the -O switch, aimed at detecting the operating system of the target host. Upon initiating the scan, the user attentively reviews the generated results to discern and analyze the potential operating systems of the hosts scanned. This OS detection scan yields insights by comparing the responses from the targeted system to a database of known OS signatures, thereby estimating the likelihood of specific operating systems running on each host. This analysis is pivotal for a deeper understanding of the target environment, setting the stage for subsequent vulnerability assessments or the development of mitigation strategies. The user meticulously examines each identified host within the Host Details tab, evaluating Zenmap's operating system predictions alongside other critical details such as open ports and active

services. To conclude this phase, the user captures a screenshot of the Host Details tab for a particular target, `fileserver01.securelabsondemand.com`. This screenshot shown in Figure 2 (Eweka, 2024), documents the scan's findings regarding the operating system and open ports, serving as essential documentation for further analysis or reporting purposes.

**Figure 2**

*Make a screen capture showing the contents of the Host Details tab from the OS scan for `fileserver01.securelabsondemand.com`.*



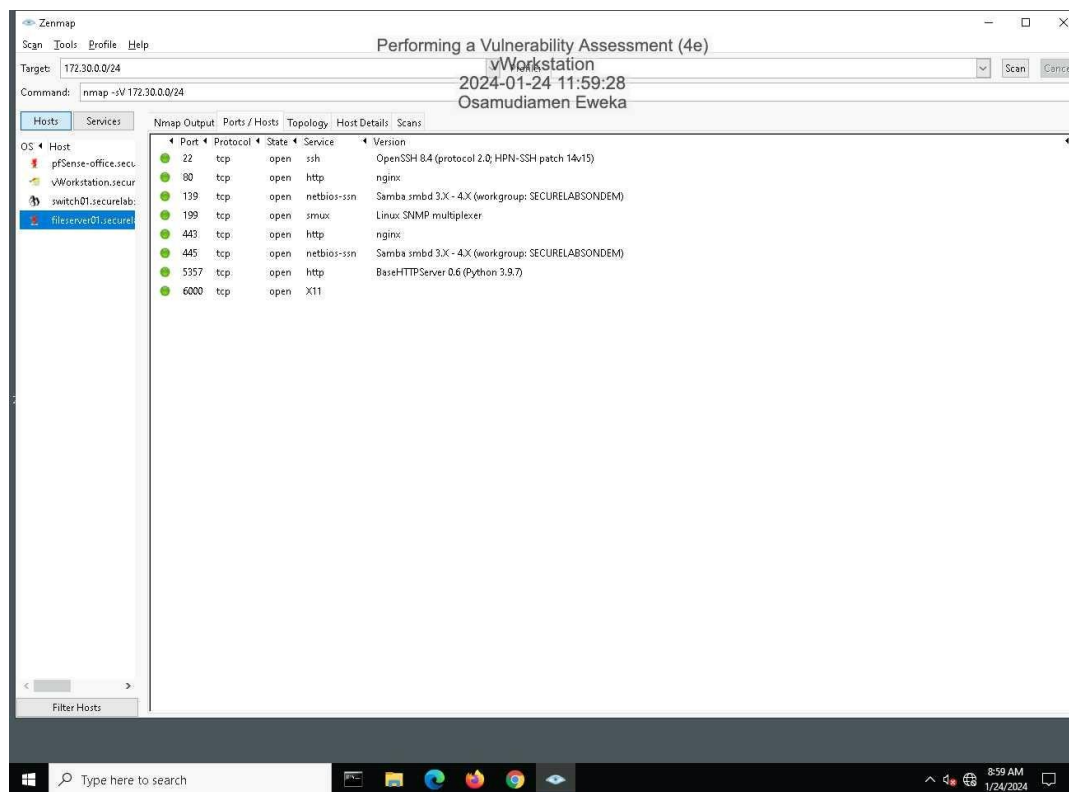
Next the following steps focus is on utilizing Zenmap for a Service scan on "fileserver01.securelabsondemand.com" to pinpoint service versions on active TCP ports. This step, leveraging the `-sV` command, is pivotal for identifying precise software versions of operational services, essential for recognizing specific vulnerabilities linked to these versions. The culmination of this process involves examining and documenting the findings in the Ports/Hosts tab for the targeted machine, illustrating a detailed list of ports, services, and their

respective versions. This crucial information aids in evaluating the security stance of the scanned system, setting the stage for further vulnerability analysis and mitigation strategies.

Figure 3 shows the result of the step (Eweka, 2024)

**Figure 3**

*Make a screen capture showing the details in the Ports/Hosts tab from the Service scan for fileserver01.securelabsondemand.com.*





## Section 1: Hands-On Demonstration

### Part 2:

#### *Conduct A Vulnerability Scan With Nessus*

In this part, the process involves conducting a vulnerability scan using Nessus, a widely recognized vulnerability scanning tool, on a network. This part of the lab is critical for identifying and understanding the security weaknesses that could potentially be exploited in a networked environment. The process is carried out through a series of steps designed to familiarize students with the practical aspects of vulnerability assessment using Nessus.

1. **Starting Nessus:** The process begins with launching the Nessus web application by navigating to `https://localhost:8834/` in a web browser. This URL accesses the Nessus service running locally on the machine, providing a user interface for conducting scans.
2. **Security Warning Bypass:** Since Nessus uses a self-signed SSL certificate for its web interface, a security warning is presented by the browser. The user must bypass this warning by selecting "Proceed to localhost (unsafe)" to move forward. This step is common with local security tools that use HTTPS for their web interfaces.
3. **Login:** Upon reaching the Nessus login page, the user is required to enter their credentials. In this lab setup, a predefined username and password are provided, which the student uses to authenticate and access the Nessus dashboard.
4. **Navigating Nessus:** After logging in, the user may encounter a welcome dialog box or tutorial, which they can close to proceed to the main dashboard of Nessus.
5. **Initiating a New Scan:** To begin the vulnerability scanning process, the user clicks on the "New Scan" button, which opens the Scan Library. This library contains various pre-configured scan types tailored for different objectives.

6. **Selecting Scan Type:** From the Scan Library, the user selects the "Basic Network Scan" option. This scan type is designed to perform a comprehensive assessment of the network for vulnerabilities.
7. **Configuring the Scan:** The user is then required to fill in details about the scan, including a name, description, and most importantly, the target IP range or specific devices to be scanned. This information directs Nessus to focus the scan on the intended targets within the network.
8. **Saving the Scan Configuration:** After entering all necessary information, the scan configuration is saved. This action creates a scan task within Nessus, ready to be executed.
9. **Launching the Scan:** With the scan configured, the user initiates the scan process by selecting the configured scan from the list and launching it. Nessus then begins assessing the specified targets for vulnerabilities.
10. **Monitoring Scan Progress:** The user can monitor the progress of the scan through the Nessus interface. The tool provides real-time feedback on the scan status, including completion percentage and any vulnerabilities detected thus far.
11. **Reviewing Scan Results:** Upon completion of the scan, the user reviews the results presented in Nessus. The tool categorizes vulnerabilities based on their severity, providing detailed information about each identified issue.
12. **Exporting the Report:** For documentation and further analysis, the user can export the scan results. Nessus allows exporting in various formats; in this lab, the HTML format is chosen for its readability and ease of sharing.
13. **Saving and Accessing the Report:** The exported report is saved to the local machine. The user is guided through the process of saving the file and then locating it in the designated folder, typically the Downloads folder or a specified location.



## Section 1: Hands-On Demonstration

### Part 3:

#### *Evaluate Your Findings*

##### **Result and analysis:**

**Question:** Summarize the vulnerability you selected, including the CVSS risk score, and **recommend** a mitigation strategy.

##### **Answer:**

##### **1. Vulnerability selected:**

IP address 172.30.0.2

Severity HIGH, CVSSv3.0 (7.5), Plugin (42873), Name (SSL Medium Strength Cipher Suites Supported (SWEET32))

##### **2. Description:**

The remote host supports the use of SSL ciphers that offer medium-strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

##### **3. Mitigation Strategy:**

Reconfigure the affected application if possible to avoid use of medium-strength ciphers. Recommended practice To help protect against this vulnerability, you need to disable some older cyphers in the registry, e.g (Disable 3DES)

## Section 2: Applied Learning

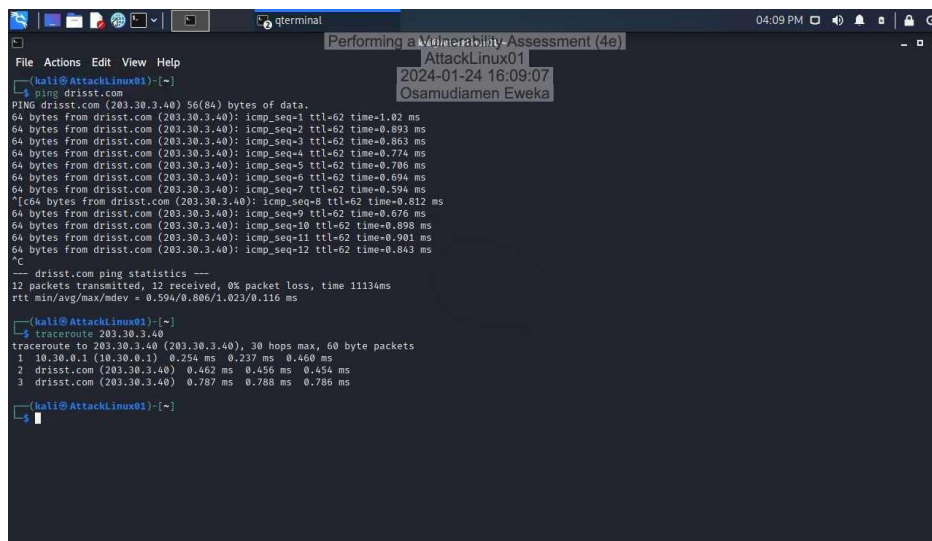
### Part 1:

#### *Scan The Network With Nmap*

In Section 2: Applied Learning, Part 1 of the lab, the student is introduced to penetration testing with a focus on network scanning using Nmap, a tool integral to cybersecurity practices. The student begins by logging into a Kali Linux system, a platform equipped with an array of penetration testing tools. They then proceed to use the terminal to execute a **traceroute** command to the target domain, which in this case is 'drisst.com.' This command maps the route that data packets take from the origin to the destination, providing insight into the network's structure. The student documents this process by capturing the traceroute results as illustrated below in Figure 4 (Eweka, 2024), a crucial step in maintaining a record of the penetration testing activities. The next phase involves using Nmap to conduct a comprehensive network scan, identifying open ports and services on the target network, which could potentially be exploited by an attacker. This hands-on exercise is designed to enhance the student's practical skills in identifying network vulnerabilities.

**Figure 4**

*Make a screen capture showing the results of the traceroute command.*



```

kali@AttackLinux01:~$ ping drisst.com
PING drisst.com (203.30.3.40) 56(84) bytes of data:
64 bytes from drisst.com (203.30.3.40): icmp_seq=1 ttl=62 time=1.02 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=2 ttl=62 time=0.893 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=3 ttl=62 time=0.863 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=4 ttl=62 time=0.774 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=5 ttl=62 time=0.786 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=6 ttl=62 time=0.694 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=7 ttl=62 time=0.594 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=8 ttl=62 time=0.212 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=9 ttl=62 time=0.676 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=10 ttl=62 time=0.898 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=11 ttl=62 time=0.901 ms
64 bytes from drisst.com (203.30.3.40): icmp_seq=12 ttl=62 time=0.843 ms
^C
--- drisst.com ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11134ms
rtt min/avg/max/mdev = 0.594/0.886/1.023/0.116 ms

kali@AttackLinux01:~$ traceroute 203.30.3.40
traceroute to 203.30.3.40 (203.30.3.40), 30 hops max, 60 byte packets
 1 10.30.0.1 (10.30.0.1) 0.254 ms 0.237 ms 0.460 ms
 2 drisst.com (203.30.3.40) 0.462 ms 0.456 ms 0.454 ms
 3 drisst.com (203.30.3.40) 0.787 ms 0.788 ms 0.786 ms

kali@AttackLinux01:~$

```

In this step, the student engages in advanced network scanning techniques using Nmap, a powerful network scanning tool favored by cybersecurity professionals. Initially, the student conducts a default Nmap scan of the target web server's IP address, which checks the most common 1000 TCP and UDP ports. This quick scan is designed to identify widely-used open ports, and in this case, it reveals that ports 21 (FTP), 22 (SSH), 80 (HTTP), 3000 (commonly used for web servers), and 3306 (MySQL) are open on the web server. Notably, while port 80 is expected to be open for a web server, the openness of the other ports, especially port 22, presents potential security risks, as it could allow unauthorized SSH access to the server.

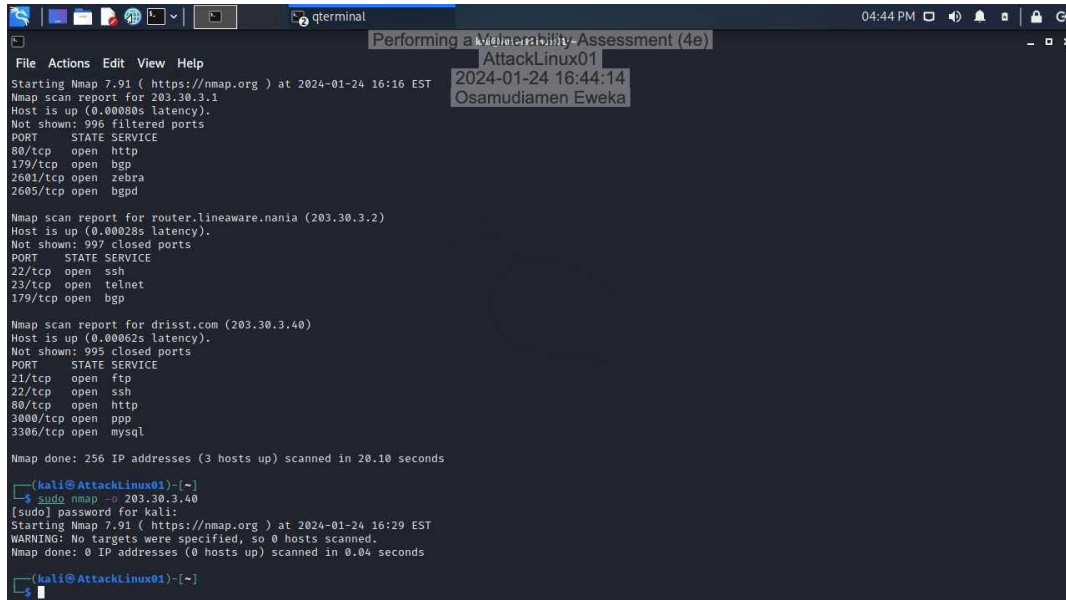
Subsequently, the student expands the scan to include a broader range of IP addresses within the network segment, discovering additional devices, including a router and a firewall. This broader scan provides further context about the network's infrastructure and potential points of vulnerability.

In the following step, the student delves deeper by executing an Nmap scan with the OS detection switch (-O). This scan sends specially crafted packets to the web server to analyze the responses, aiming to identify the operating system based on unique network characteristics. The results from this OS detection scan are not definitive but offer an educated guess, suggesting a Linux operating system based on the TCP/IP fingerprint observed.

Finally, the student is instructed to capture the screen showing the results of the Nmap scan with OS detection activated as illustrated in Figure 5 (Eweka, 2024). This screen capture is a crucial part of documenting the scanning process, providing a visual record of the scan findings, which may include the open ports and the guessed operating system, enriching the assessment with actionable intelligence for further security analysis or reporting purposes.

**Figure 5**

*Make a screen capture showing the results of the Nmap scan with OS detection activated.*



```
Performing a Vulnerability Assessment (4e)
AttackLinux01
2024-01-24 16:44:14
Osamudiamen Eweka

File Actions Edit View Help
Starting Nmap 7.91 ( https://nmap.org ) at 2024-01-24 16:16 EST
Nmap scan report for 203.30.3.1
Host is up (0.00080s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
179/tcp   open  bgp
2601/tcp  open  zebra
2605/tcp  open  bgpd

Nmap scan report for router.lineaware.nania (203.30.3.2)
Host is up (0.00028s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
179/tcp   open  bgp

Nmap scan report for drisst.com (203.30.3.40)
Host is up (0.00062s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
3000/tcp  open  ppp
3306/tcp  open  mysql

Nmap done: 256 IP addresses (3 hosts up) scanned in 20.10 seconds

kali@AttackLinux01:~$
$ sudo nmap -v 203.30.3.40
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2024-01-24 16:29 EST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds

kali@AttackLinux01:~$
```

## Section 2: Applied Learning

### Part 2:

#### *Conduct a Vulnerability Scan with Openvas*

In the "Performing a Vulnerability Assessment" lab, the student transitions to utilizing the OpenVAS vulnerability scanner paired with the Greenbone Security Manager (GSM) interface. This part of the lab is designed to introduce and train the student on conducting a comprehensive vulnerability assessment using this robust, open-source alternative to commercial tools like Nessus.

Starting within the Kali Linux environment, the student launches a web browser from the AttackLinux01 system. They then navigate to the GSM by entering the appropriate IP address. The browser may present a security warning due to the self-signed certificate used by the GSM, which the student is instructed to bypass, understanding that it's a common occurrence in security tools not yet configured with a certificate from a trusted authority.

Upon accessing the GSM login page, the student enters the provided administrative credentials, allowing them to reach the GSM dashboard. This is the operational heart of OpenVAS, where vulnerability scanning tasks are managed. With no existing tasks displayed, the student proceeds to create a new one by selecting the 'New Task' option. This new task is aptly named 'drisst.com scan,' indicating its target—the specified web server IP address.

After saving the new scan configuration, the student initiates the vulnerability scan by clicking the 'Start' icon. OpenVAS begins its work, with the scan's progress reflected in the status updates on the GSM dashboard, initially displayed as 'Requested,' then advancing through a percentage completion metric.

Once the scan concludes, the student examines the results by accessing the report linked under the 'Reports' header. The OpenVAS report lists all detected vulnerabilities, providing a succinct description and a severity rating for each. The report also includes the



Quality of Detection (QoD) score, which gauges the reliability of the finding, alongside the associated IP address, port, and the timestamp of when each vulnerability was detected.

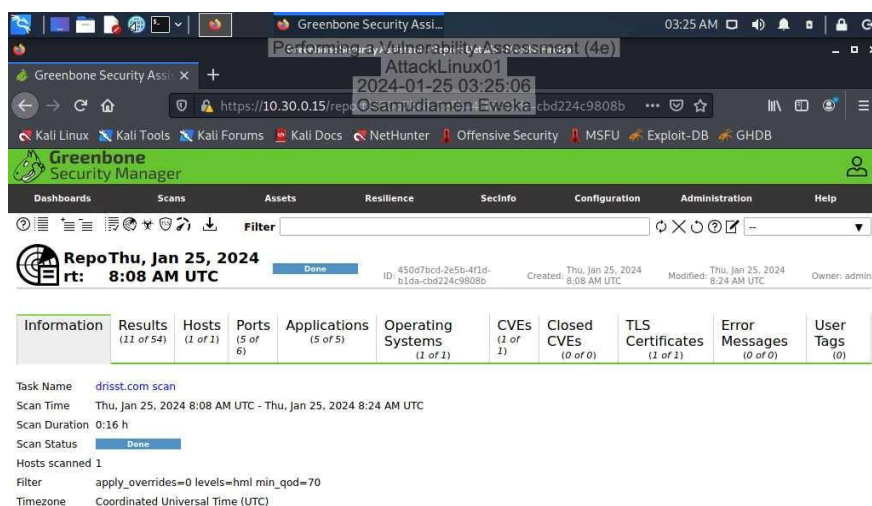
To delve deeper into the analysis, the student clicks on the timestamp within the scan report, bringing up more granular details about each vulnerability. This step is critical for understanding the full context and potential impact of each security issue uncovered during the scan.

In the final step, the student captures a screenshot of the detailed OpenVAS scan results shown below in Figure 6 (Eweka, 2024). This screenshot serves as tangible proof of the vulnerabilities discovered and is a crucial part of the documentation process. It not only provides a visual record for immediate analysis but also becomes a part of the permanent record that can inform future security decisions and actions.

Through this exercise, the student gains hands-on experience with the OpenVAS and GSM platforms, learning to configure and execute a vulnerability scan, interpret the results, and understand the significance of meticulous documentation in the field of cybersecurity.

**Figure 6**

*Make a screen capture showing the detailed OpenVAS scan results.*



## Section 2: Applied Learning

### Part 3:

#### *Prepare a Penetration Test Report*

##### **Result and analysis:**

**Target:** The focus of this penetration test is the web server at drisst.com, with the specific aim of performing a vulnerability scan for the identification of possible security vulnerabilities.

**Completed By:** Osamudiamen Eweka

**ON:** Thursday, January 25, 2024

**Purpose:** The purpose of this penetration test is to identify potential security vulnerabilities in the drisst.com web server and assess the security posture of the organization. This test will help identify potential security weaknesses and suggest measures to improve the security posture of the organization.

**Scope:** The scope of this penetration test is limited to a vulnerability scan of the drisst.com web server. The penetration tester is allowed to scan the web server for vulnerabilities using Nmap and OpenVAS but is not authorized to conduct any potentially destructive scans or tests. The penetration test is limited to the web server and does not include any other systems or networks within the organization.

**Summary Of Findings:** Identify and summarize each of the three high-severity vulnerabilities identified during your penetration test. For each vulnerability, identify the severity, describe the issue, and recommend a remediation.

## 1. Vulnerability 1: MVSOL MariaDB Weak Password

Severity: 9.0 (High)

- **Description:** The MariaDB service is using a weak password, which can be easily guessed or brute-forced by an attacker. This could lead to unauthorized access to the database and sensitive information being stolen.
- **Recommendation:** Change the MariaDB password to a stronger and more complex one, preferably using a combination of upper and lowercase letters, numbers, and special characters (Default Accounts : MySQL / MariaDB Weak Password, n.d.).

## 1. Vulnerability 2: VSFTPD Compromised Source Packages Backdoor

### Vulnerability

Severity: 7.5 (High)

- **Description:** The vsftpd service is using compromised source packages, which contain a backdoor vulnerability that can be exploited by an attacker to gain unauthorized access to the server.
- **Recommendation:** Update the vsftpd service to the latest version, which does not contain the backdoor vulnerability, and remove any compromised source packages from the system (Gain a Shell Remotely : Vsftpd Compromised Source Packages Backdoor Vulnerability, n.d.).

## 2. Vulnerability 3: VSFTPD Compromised Source Packages Backdoor

### Vulnerability

Severity: 7.5 (High)

- **Description:** The vsftpd service is using compromised source packages, which contain a backdoor vulnerability that can be exploited by an attacker to gain unauthorized access to the server.
- **Recommendation:** Update the vsftpd service to the latest version, which does not contain the backdoor vulnerability, and remove any compromised source packages from the system.

**Conclusion:** The penetration test revealed numerous vulnerabilities in the web server at drisst.com, with three of them being high-severity issues that present a substantial security threat to the organization.

Immediate action is required to rectify these vulnerabilities, as they could lead to unauthorized system access and compromise sensitive information. The organization should promptly apply the suggested remediation measures to enhance the security stance of the drisst.com web server and address the identified vulnerabilities. It is advisable to conduct regular vulnerability assessments and penetration tests to detect and mitigate potential security weaknesses in the organization's IT infrastructure.

## Section 3: Challenge And Analysis

### Part 1:

#### Scan The Domain Controller With Nmap

To conduct a penetration test targeting the Domain Controller within Secure Labs on Demand's protected network, the process involves several steps, utilizing tools like Nmap for scanning and enumeration. This process is crucial for identifying vulnerabilities that could potentially be exploited by attackers. Here's a breakdown of the steps involved:

##### Step 1: Preparing for the Scan

Before initiating the scan, ensure you have access to the vWorkstation and that Nmap is installed and ready to use. Given the Domain Controller's critical role in managing network security, permissions, and user data, it's essential to approach this test with caution, ensuring no disruptive scans are performed that might affect the network's operation.

##### Step 2: Conducting an Initial Service Scan

- Open a terminal on the vWorkstation.
- Run an initial Nmap scan using the Service Scan switch (-sV). This switch is used for version detection, enabling Nmap to identify software versions running on the open ports of the target system.
- The command structure is as follows: `nmap -sV [Domain Controller IP Address]`. Replace [Domain Controller IP Address] with the actual IP address of the DomainController01.
- This initial scan aims to identify all open ports and services running on the Domain Controller, with a specific lookout for the LDAP service, commonly running on port 389 or 636 for LDAP over SSL.

### **Step 3: Conducting a Targeted Scan on the LDAP Service Port**

- After identifying the LDAP service port from the initial scan, run a more focused scan on just this port. This targeted approach reduces the scan's footprint and focuses on gathering detailed information about the LDAP service.
- Use the -p option to specify the port. The command format is: `nmap -sV -p [LDAP Port] [Domain Controller IP Address]`.
- Replace [LDAP Port] with the port number identified in the initial scan (e.g., 389 or 636) and [Domain Controller IP Address] with the Domain Controller's IP address.

### **Step 4: Analyzing the Results**

- Review the Nmap output for the targeted scan on the LDAP port. This information will include the service version, which can be crucial for identifying known vulnerabilities associated with that version.
- Pay special attention to the service's configuration and any indications of weak security practices, such as default credentials, unnecessary services running, or outdated software versions.

### **Step 5: Documentation**

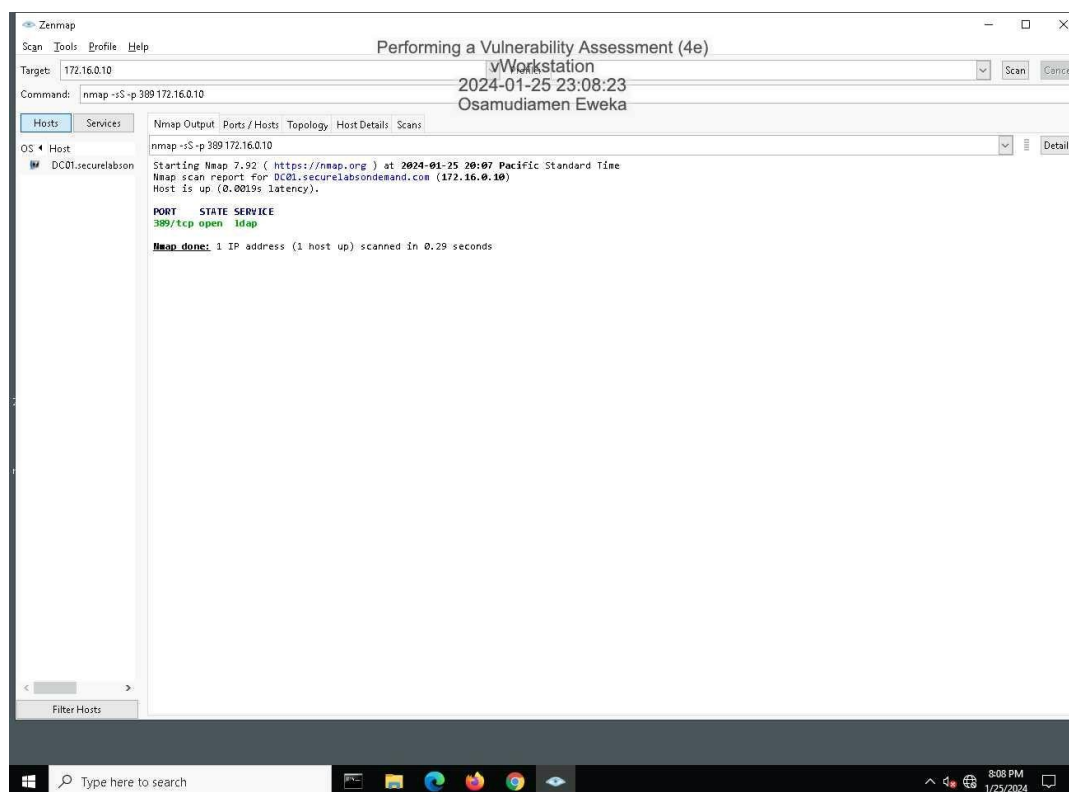
- Capture screenshots of the Nmap output, specifically the results of the targeted LDAP service port scan the screen capture is shown in Figure 7 below (Eweka, 2024), This documentation is crucial for the penetration test report, providing evidence of the findings and forming the basis for recommendations.
- Ensure the screenshots display the command used and the resulting output, highlighting any vulnerabilities or concerns identified during the scan.

## Conclusion and Recommendations

After completing the scans and documenting the findings, the next steps involve analyzing the information to understand the security posture of the Domain Controller. Any identified vulnerabilities or misconfigurations should be addressed in the penetration test report, along with recommendations for mitigating these risks. This may include patching outdated software, changing default credentials, or disabling unnecessary services. The goal is to enhance the security of the Domain Controller, thus strengthening the overall network security for Secure Labs on Demand.

Figure 7

**Make a screen capture showing the results of your targeted port scan on the domain controller.**



## Section 3: Challenge And Analysis

### Part 2:

#### Scan the Domain Controller with Nessus

**Figure 8**

Make a screen capture showing the Nessus report summary for the domain controller.

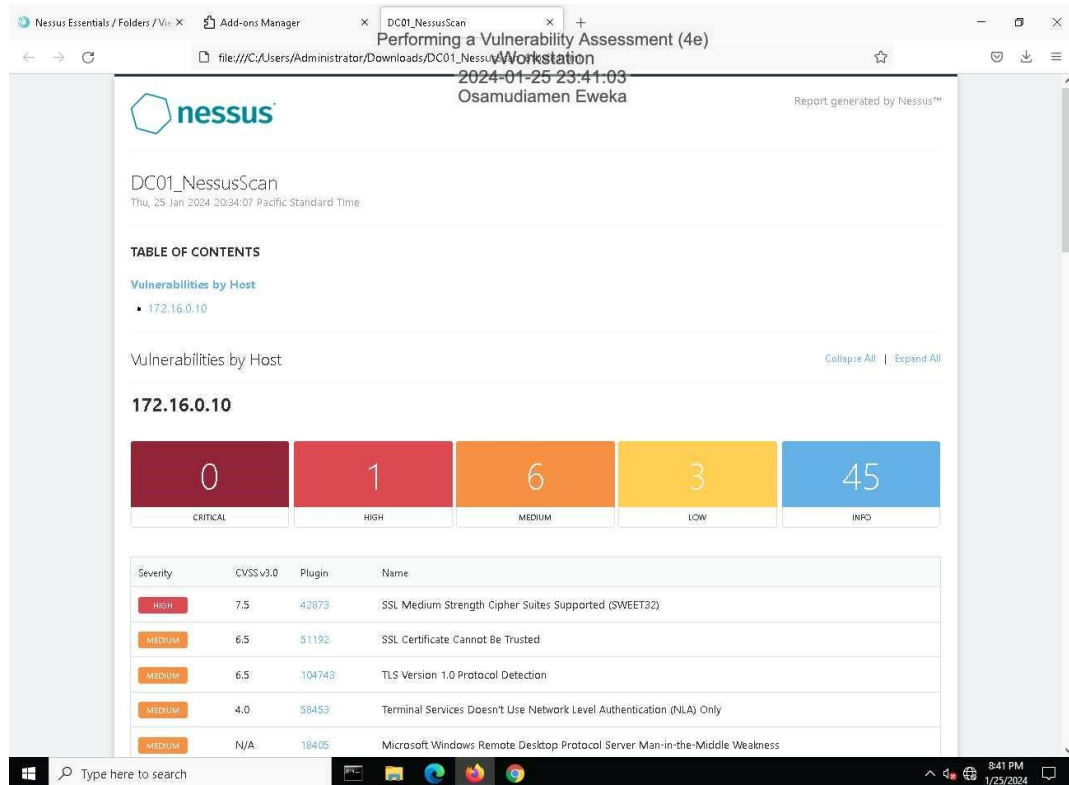


Figure 8 (Eweka, 2024) The process involves using the Nessus tool to conduct a vulnerability assessment scan of a domain controller. The goal of this scan is to identify and document any vulnerabilities present in the domain controller's system. The Nessus report summary provides an overview of the scan results, including the number and severity of vulnerabilities found. The screenshot of the Nessus report would typically show a bar chart or similar visual representation of the findings, breaking down the vulnerabilities by their severity levels, such as critical, high, medium, or low.



### **Part 3: Prepare a Penetration Test Report**

**Target:** Secure Labs on Demand Domain Controller (DomainController01)

**Completed By:** Osamudiamen Eweka

**On:** Thursdays, January 25, 2024

**Purpose:**

The goal of conducting this penetration test is to assess the security stance of the domain controller belonging to Secure Labs on Demand. The objective is to pinpoint and analyze potential vulnerabilities that could be exploited by malicious attackers.

**Scope:**

The scope of this penetration test involves performing Nmap scans to detect open ports and services on the domain controller. Additionally, a Nessus vulnerability scan will be carried out to pinpoint any recognized vulnerabilities.

**Summary Of Findings:** Identify and summarize each vulnerability identified during your penetration test. For each vulnerability, identify the severity, describe the issue, and recommend a remediation.

**Vulnerability 1:**

A critical vulnerability linked to the LDAP service (SSL Medium Strength Cipher Suites Supported (SWEET32)).

**Issue:** This vulnerability is connected to a recognized issue in the current version of the LDAP service on the domain controller, enabling unauthorized entry to confidential data.

Remediation: Mitigate the vulnerability by updating the LDAP service to the most recent version and implementing any required patches (SSL Medium Strength Cipher Suites Supported (SWEET32), n.d.).

**Conclusion:** In summary, based on the results from Nmap and Nessus scans, it's evident that the domain controller faces a vulnerability concerning unauthorized access due to an identified flaw in the LDAP service version. Secure Labs on Demand is advised to promptly upgrade the LDAP service and apply necessary patches to enhance the domain controller's security. The penetration test simulated an attack on the domain controller to assess its security and pinpoint potential vulnerabilities, with specific focus on Nmap scans for open ports and services, and a Nessus vulnerability scan. The latter identified a high-severity vulnerability linked to the LDAP service, emphasizing the urgency of remediation through service upgrade and patch application.

## **Conclusion**

In conclusion, Lab 2, "Performing a Vulnerability Assessment," provided an in-depth exploration into identifying and mitigating network vulnerabilities, utilizing Nmap and Nessus. This hands-on approach offered participants a nuanced understanding of vulnerability management, from detection through to remediation. The lab underscored the criticality of systematic vulnerability scanners in modern cybersecurity practices, highlighting their indispensable role in automating the detection process for enhanced network security. Through practical exercises, including targeted scans and vulnerability assessments, participants applied theoretical knowledge to real-world scenarios, gaining insights into attacker methodologies and enhancing defensive strategies. Moreover, the lab emphasized the development of analytical skills, encouraging a deeper comprehension of vulnerabilities and their mitigation. This comprehensive training serves as a cornerstone in cybersecurity education, preparing professionals to navigate the complexities of information security with a proactive and informed approach.

## Reference

Default Accounts: MySQL / MariaDB weak password. (n.d.). Wwww.securityspace.com.

<https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.10355>.

Eweka O. (2024). Performing a Vulnerability Assessment(Figure 1). *Jones and BartlettLearning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>

Eweka O. (2024). Performing a Vulnerability Assessment(Figure 2). *Jones and BartlettLearning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>

Eweka O. (2024). Performing a Vulnerability Assessment(Figure 3). *Jones and BartlettLearning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>

Eweka O. (2024). Performing a Vulnerability Assessment(Figure 4). *Jones and BartlettLearning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>

Eweka O. (2024). Performing a Vulnerability Assessment(Figure 5). *Jones and BartlettLearning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>

Eweka O. (2024). Performing a Vulnerability Assessment(Figure 6). *Jones and BartlettLearning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>

Eweka O. (2024). Performing a Vulnerability Assessment(Figure 7). *Jones and BartlettLearning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>

Eweka O. (2024). Performing a Vulnerability Assessment(Figure 8). *Jones and BartlettLearning Virtual Lab*. URL: <https://jbl-lti.hatsize.com/startlab>

Gain a shell remotely: vsftpd Compromised Source Packages Backdoor Vulnerability. (n.d.). Wwww.securityspace.com.

<https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.10318>.

Kim, D. (2021). *Fundamentals Of Information Systems Security + Cloud Labs*. Jones & Bartlett Learning Lab2 Performing a Vulnerability Assessment<https://jbl-lti.hatsize.com/startlab>

*SSL Medium Strength Cipher suites supported (SWEET32)*. (n.d.). Tenable®.

<https://www.tenable.com/plugins/nessus/42873>