1. HTTP Interception

Part (b)

Table

Description automatically generated with medium confidence

Part (c)

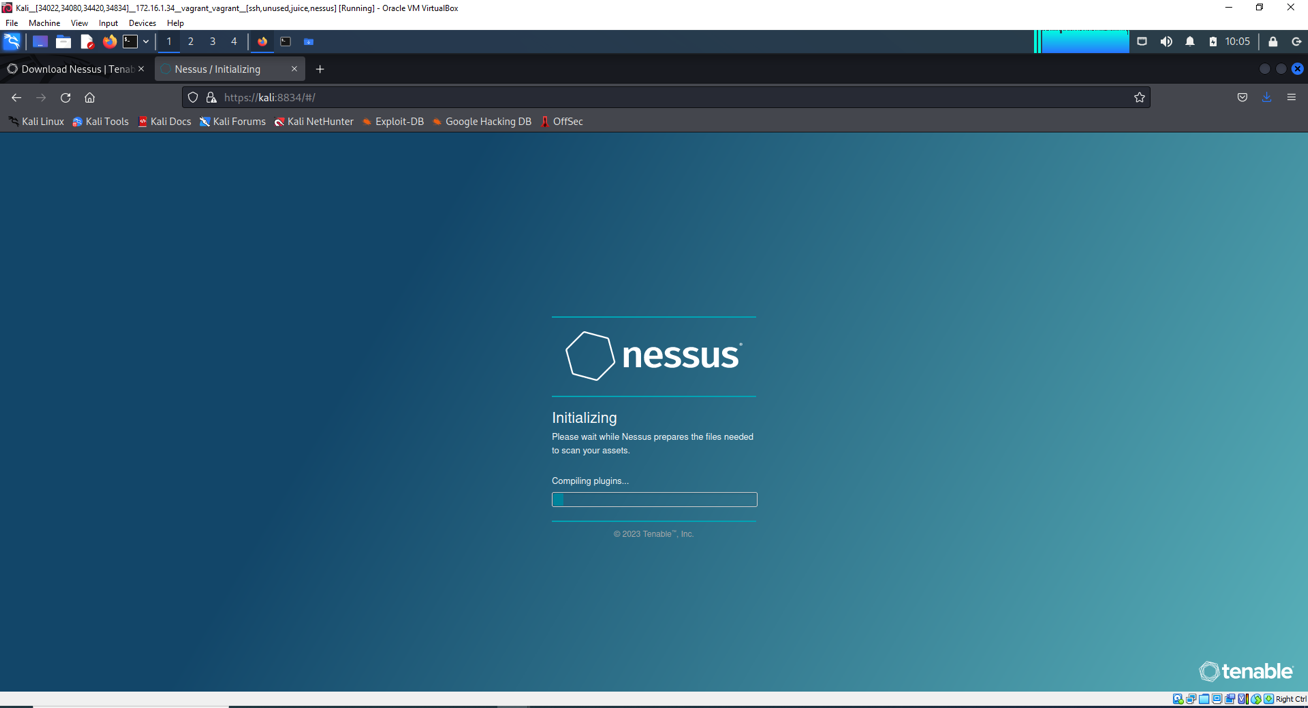
Within the capture file of this context, the bits that would be useful to an attacker would be the login credentials of the user, meaning the username and password, the user’s IP address, and the personal grades of the student in the session. For the login credentials, packet number 26 displays the username and password in the HTML Form URL Encoded section in Wireshark, which can compromise the login details, and an attacker can use that to access unauthorized data in the students account, or even run a malware encryption for ransomware. The attacker could also just erase or edit the data if they have a personal vendetta against the student.

Another data an attacker can get is the IP address, which can cause the most damage. As the attacker also has the login credentials of the student, they could access other information in the student portal, including the full name, address, phone number, email address, and date of birth. This information, paired with the IP address can help an attacker to perform identity theft, as this information paired together can be an authentication factor. Having an IP address can also help an attacker to **learn the student location, restrict their access to some services, execute a DDoS attack, or even sell their information.**

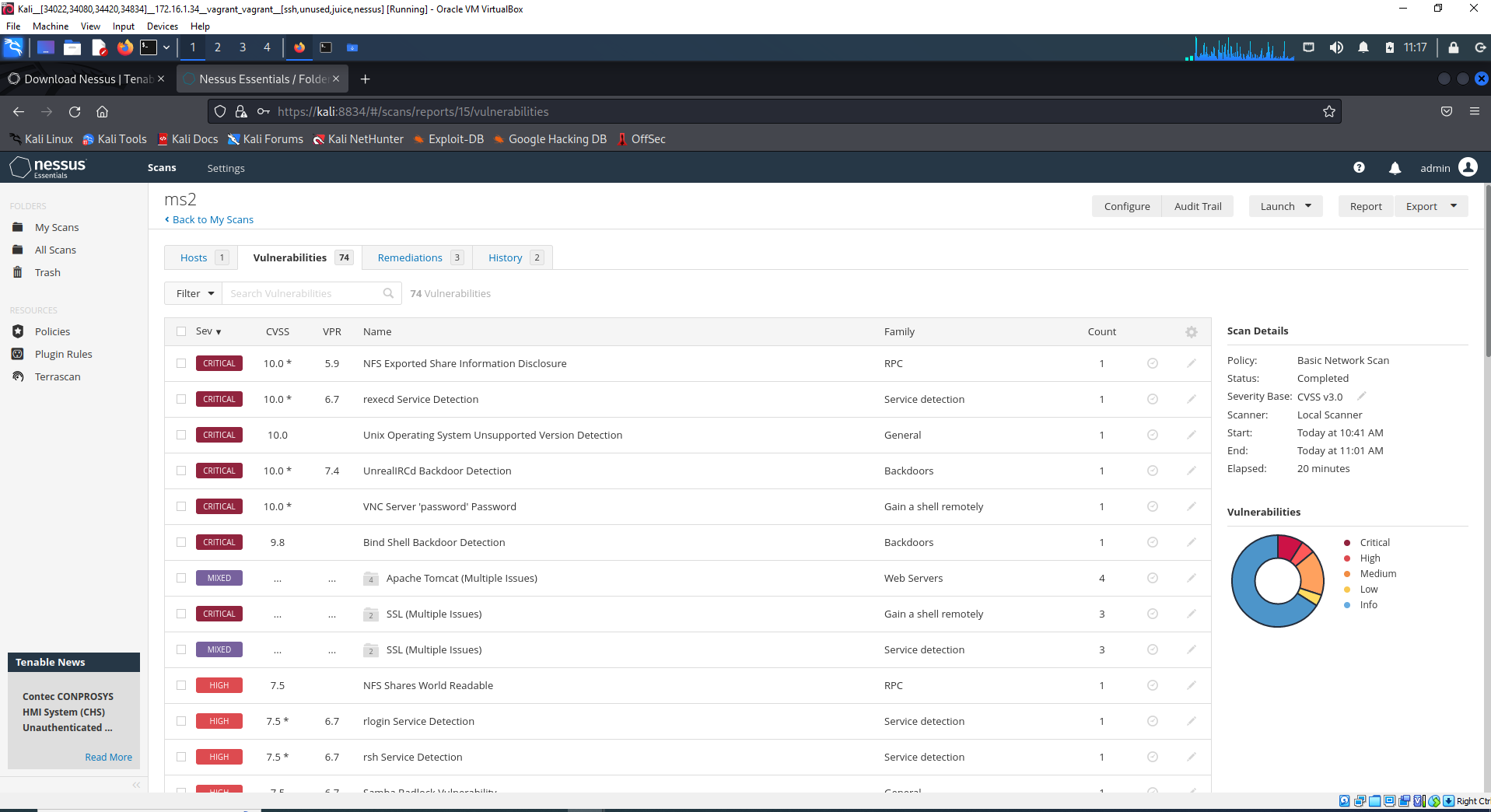
Another compromised data, the student’s grades can be viewed in packet number 59, which is from the server, viewing the student’s grades. This data can be seen in the html text data in Wireshark. While not as sensitive as the others mentioned, the grades are meant to be accessed by only the student and the authorized university faculty, therefore, an attacker is not authorized and could leak them.

1. Vulnerability analysis using Nessus

Part (a)



Part (b)



Part (c)

There were 11 critical vulnerabilities in ms2:

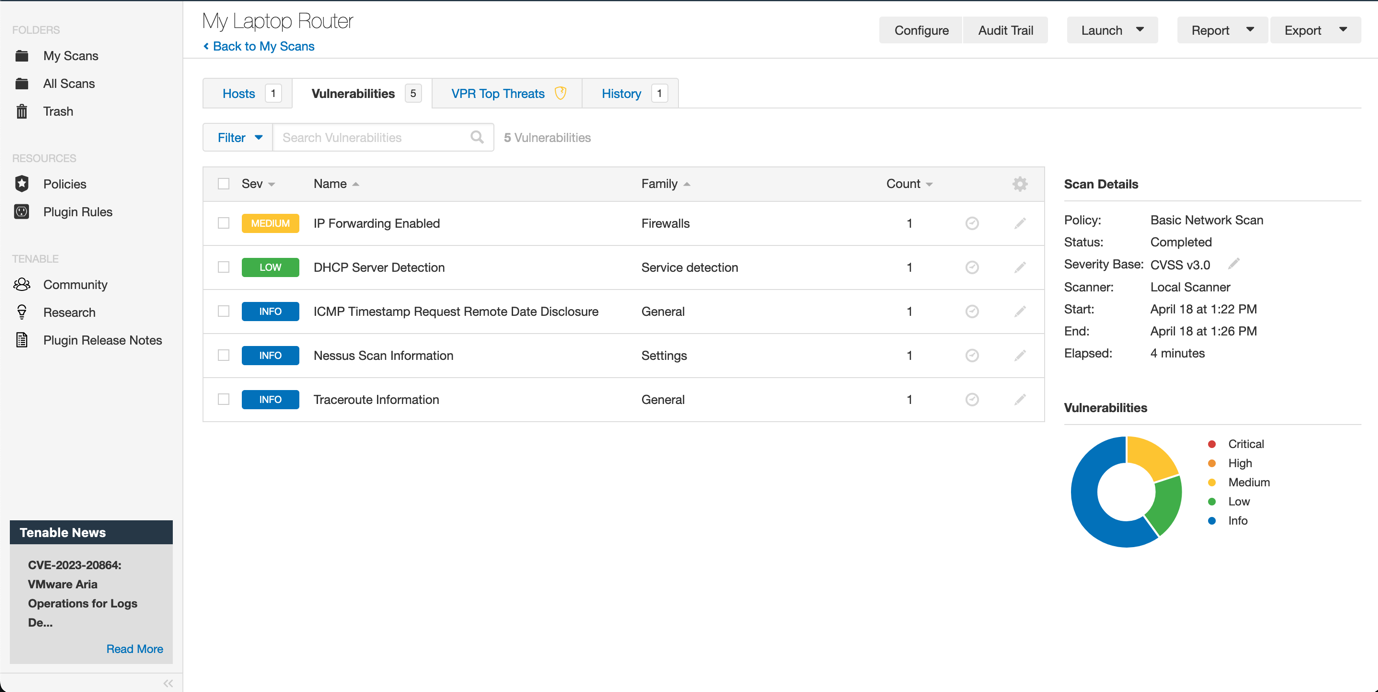
1. Apache Tomcat A JP Connector Request Injection (Ghostcat)
2. Bind Shell Backdoor Detection
3. SSL Version 2 and 3 Protocol Detection
4. Apache Tomcat Web Server SEoL (<= 5.5.x)
5. Unix Operating System Unsupported Version Detection
6. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
7. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
8. NFS Exported Share Information Disclosure
9. UnrealIRCd Backdoor Detection
10. VNC Server 'password' Password
11. rexecd Service Detection

Part (d)

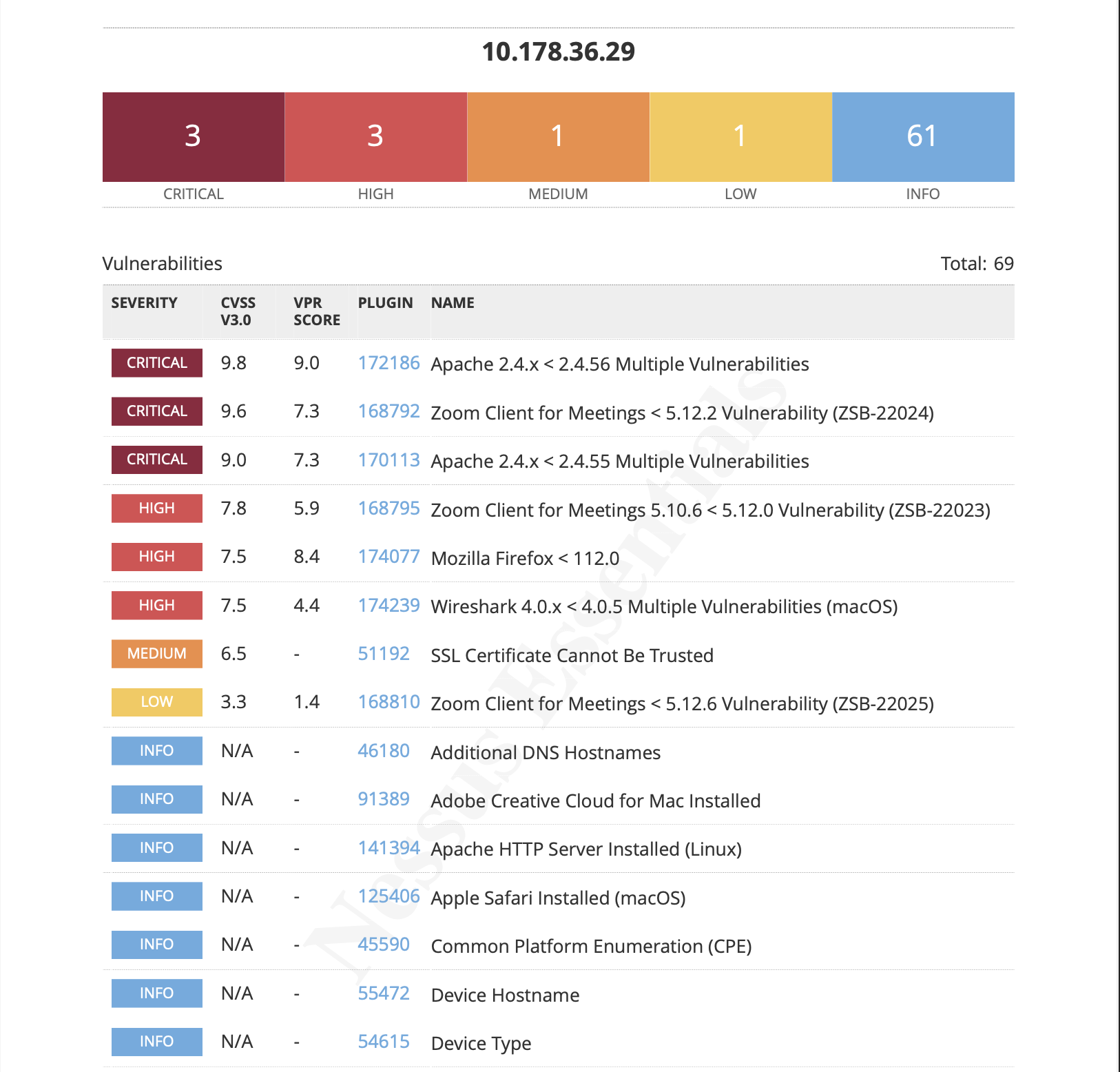
The first two screenshots include vulnerabilities from my personal laptop, while the third screenshot include my router vulnerability.

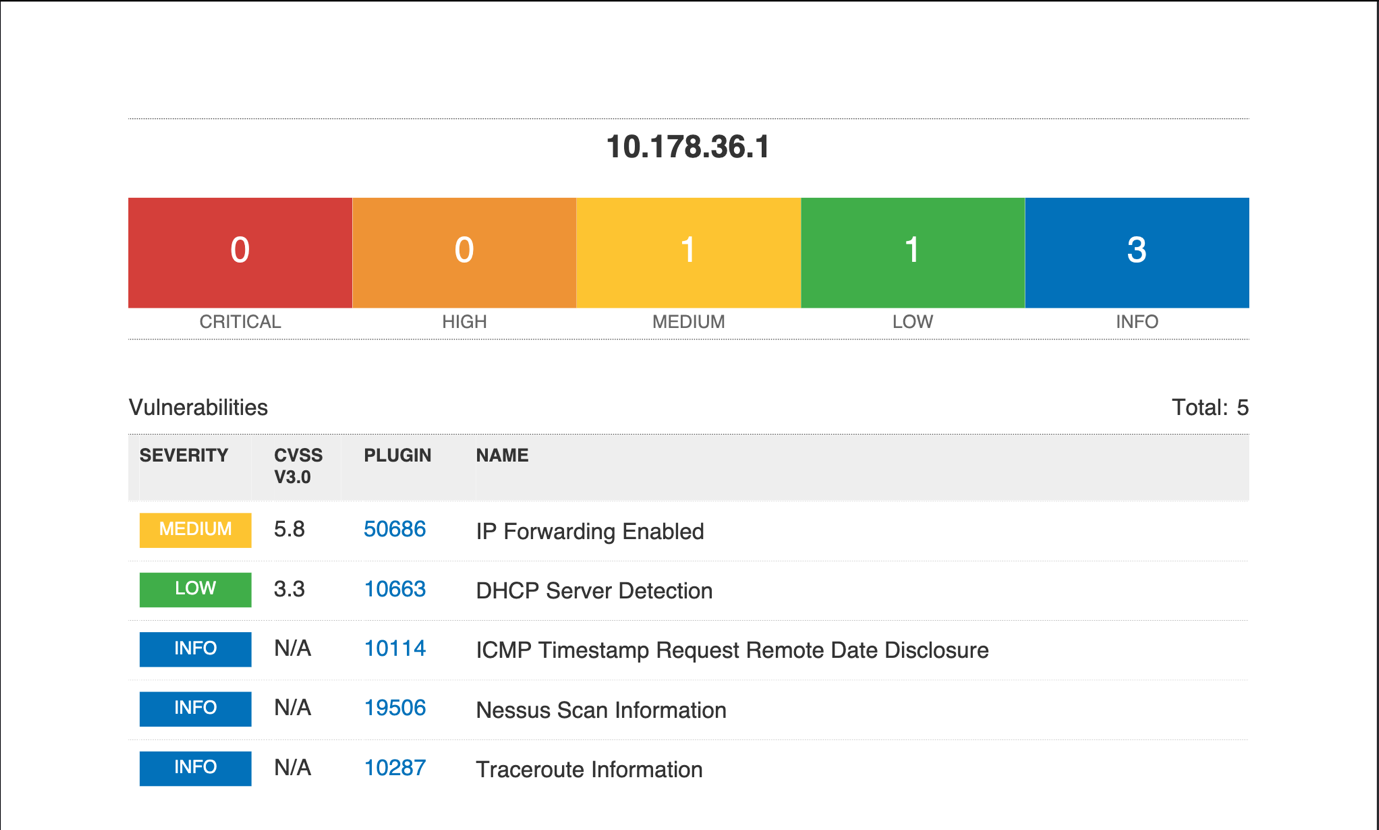
Graphical user interface, text, application, email

Description automatically generated



The following screenshots are from documentation from those scans.





Part (e)

The most critical vulnerabilities arise from my laptop. One came from Zoom, the video conferencing app, stating that I have an outdated version, where I am more susceptible to URL parsing via malicious links sent.

Another was from Apache which had multiple vulnerabilities, stating the outdated version may lead to threats of memory reading, and inconsistent HTTP requests, meaning an attacker may be able to smuggle requests through my device.

A third “high” threat was from Mozilla, claiming I have an outdated version of Firefox which can lead an attacker to trick Mozilla Maintenance Service into applying an unsigned update file not authorized by me. There are also other vulnerabilities regarding full screen notification obscurement, which are more a bug than a vulnerability.

1. Cryptography

Part (a)

Unable to decrypt.

Part (b)

The decryption of ciphered key and IV files in order to decrypt the final message file was difficult to plan out, despite the encryption process going smoothly. I also had to redo most of my encryptions as I accidentally created a 32 bit IV instead of 16, along with encrypting the message file with –aes-128-cbc instead of –aes-256-cbc. The main issue I faced was the inability to be able to decrypt my partners files. The other parts went smoothly as can be seen in the files submitted and the screenshots. However, I was unable to decrypt them

Part (c)

My private key, while encoded, was first created as a text file, which still exists on my device. None of the steps asked to delete it, once encoded, therefore, anyone with access to my private key can hack into any data that heads my way, as my public key will be known anyway.

1. Ransomware Research

Part (a)

Ransomware is an attack on a computer, where an attacker uses a software (malware) to encrypt the files of the computer. Encryption is a process that turns data into code that can not be accessed by anyone except the person who has a decryption key to that code. Encryption is usually a good security method and is used widely. For example, when you send a text-message to someone, that message is encrypted and can only be decrypted by the person you sent it to, keeping your message safe from attackers. However, hackers/attackers can use this for harmful means such as ransomware, where the malware encrypts all the personal files of the computer and makes it inaccessible by the owner of the computer. The attacker is the only one who has the key to decrypt the data, and they can use that as leverage to get ransom (money) from the owner of the computer, hence the word ransomware. They may also threaten to delete or leak the data if their demands are not met within a certain time. The malware can be installed to a computer or network in many ways.

A real-life example is WannaCry ransomware attack that took place in 2017 where over 300,000 computers running Microsoft Windows OS in over 150 countries were infected. The attack lasted for four days, and the attackers demanded $300-$600 US worth of Bitcoins per ransom.

Part (b)

One of most common methods of ransomware infecting a computer with ransomware attacks is by using phishing techniques, where an attacker deceives the user into clicking a link or downloading a file, which then installs the malware into the user’s device, encrypting their device and halting access to all their data. Another way is by accessing a compromised website, which can directly install the malware to a device. Another method could be via downloading a software, which could be compromised. Another way of having malware installed is through remote desktop access, where an attacker can get remote access of a person’s device due to a weak or non-existent password. Lastly, a malware could also be sent through suspicious wireless networks such as free Wi-Fi.

Cryptographic techniques include symmetric encryption algorithms, such as Advanced Encryption Standard (AES) to encrypt user data. Asymmetric encryption methods such as RSA can also be used to perform the same function.

The main way of obtaining ransoms is through cryptocurrency such as Bitcoin and Ethereum, as these cannot be tracked back to the attacker. Attackers also use anonymous networks such as Tor to hide their details such as location and addresses.

Ransomware uses strong encryption algorithms that can be difficult to break. Attackers also use complex obfuscation techniques to hide the code. Furthermore, attackers constantly update their ransomware tools and techniques and improve encryption methods, making it harder to catch up. Oftentimes, these attackers can also be state-sponsored which means they have a lot more tools on their hands as opposed to small time hackers who may be doing it through smaller networks.

Part (c)

The following are the ways that can help prevent ransomware:

* Have multiple backups of data, both in the cloud and hard drives, while routinely backing it up
* Keep software and OS updated with the latest security patches.
* Use strong passwords along with two-factor authentication to make devices safe from Remote Desktop Protocol (RDP) attacks.
* Have anti-virus/anti-malware software installed on devices to detect and prevent ransomware attacks.
* Be wary of the websites visited, checking the domain name for http/https or the lock symbol in the domain bar.
* Be vary of links emailed, specifically ones claiming a prize.

\*The screenshots journaling this assignment are in the shared OneDrive folder called “Assessment 1.”