TANDON RED SECURITY

TANDON RED SECURITY

NBN Report Penetration Testing Services

Abraz Bashar
atb429@nyu.edu

Date: Nov. 5th, 2023
CS GY 6573: Penetration Testing

TANDON RED SECURITY

Table of Contents

1. Executive Summary

1.1) Purpose of Report

Tandon Red Security (TRSec) has secured a contract to engage proficient cybersecurity consultants for the execution of penetration testing services on a designated portion of NBN's IT infrastructure. This report outlines the penetration test findings, emphasizing NBN's cybersecurity vulnerability to external threats, and provides recommendations on mitigating this risk.

1.2) Major Flaws Identified

1. Anonymous FTP Login Reporting – vulnerable port 9001
2. Web App 19 items with medium and low alerts
3. XSS DOM based
4. XSS Persistent (Customer list exposed!)
5. XSS Reflected
6. Remote OS command injection
7. SSH access to NBN Gateway/Server (shell access)

1.3) List of Immediate Actions or Fixes

The findings of 1, 4 and 7 are recommended for immediate change. The findings and their respective recommended solution are mentioned below:

1. Anonymous FTP Login Reporting – vulnerable port 9001: Anonymous login must be disabled to prevent this problem.

4. XSS Persistent (Customer list exposed!) – Page data and customer lists should both be encrypted.

7. SSH access to NBN Gateway/Server (shell access) – Enforce a corporation-wide password policy and password strength training.

For the remaining cases, even though they are critical, we advise a comprehensive review of the web application architecture. This process, although time-consuming, is essential to prevent vulnerabilities, particularly in the context of Cross Site Scripting (XSS) and Remote OS command injection.

2. Web App 19 items with medium and low alerts (e.g., lack of encryption in NBN Web App)

3. XSS DOM based

5. XSS Reflected

6. Remote OS command injection

1.4) Overall security rating / score

1. OpenVAS Scan Discovery — CVSS Score 8.2
2. Hydra Password cracking) — CVSS Score 9.4
3. ZAP Scan Discovery — CVSS Score 6.8
4. XSS Persistent (Customer list exposed!) — CVSS Score 6.5
5. CEO Image Metadata Leak — CVSS Score 9.4
6. Information Leak/Bad Auth — CVSS Score 7.6

The Overall security score is the highest vulnerability: System CVSS Score 9.4

2. Preamble

2.1) Consultant name, title and contact information

TRSec consists of (1) consultants who will be working full-time during the entire duration of the penetration test (from November 15th, 2023, to December 15th, 2023). Details of employee(s):

Name: Abraz Bashar

Title: Security Consultant

Contact Information: atb429@nyu.edu | +1-929-316-1794

Company Address: 123 Silicon Valley

2.2) Subject

Tandon Red Security (TRSec) is a consulting and professional services entity. This document will provide a brief overview we have conducted a thorough penetration test based on NBN's RFP. The primary goal is to enhance the security posture of NBN by identifying vulnerabilities in both external and internal networks, as well as the external web application.

2.3) Date

2.4) Table of Contents

3. Introduction and Summary

3.1) Test Goals and Objectives

From November 15th, 2023, to December 15th, 2023, will conduct a thorough penetration test on NBN's networks and applications in order to assess the security posture of its infrastructure in alignment with current industry standards. The evaluation will incorporate both external and internal networks, as well as the external web application as per NBN's RFP scope.

3.2) Overall Approach

The testing procedures adhere to the guidelines outlined in *the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment*, as well as the *OWASP Testing Guide (v4)*.

The stages of penetration testing activities consist of the following:

1. Reconnaissance:

   The first phase is reconnaissance, where the tester gathers information about the target system, including network topology and user accounts.

2. Scanning:

   After reconnaissance, scanning is conducted to identify open ports and assess network traffic.

3. Vulnerability Assessment:

   The third phase involves a vulnerability assessment using data from reconnaissance and scanning to identify and evaluate potential vulnerabilities.

4. Exploitation:

   After identifying vulnerabilities, the tester attempts to exploit them using tools like Metasploit, Nmap, Burp Suite etc.

5. Reporting:

The final phase is reporting, where the tester creates a document detailing the findings of the pene tration test.

3.3) Schedule

November 15th, 2023: RFP Response and acceptance.

November 16th, 2023: Research and Reconnaissance

November 20th, 2023: Network Scanning (1/2)

Day 5: November 21st, 2023: Network Scanning (2/2)

November 25th – 28th, 2023: Exploitation Cycles

November 29th - 30th, 2023: Post-exploitation attacks

December 1st – 15th, 2023: Report completion

3.4) Roles and Responsibility of Organization

TRSec will bring its own hardware and software to carry out the complete penetration test.

There will only be one employee working on this project – Security Consultant, Abraz Bashar.

Any potential disturbance to bisuness critical infrastructure, TRSec will immediately halt the test in order to prevent any disruptions in NBN's operations.

3.5) Overall Security Ratings/Scoring

The following table defines levels of severity and corresponding CVSS pdf score range that are used throughout the document to assess vulnerability and risk impact. [2]

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

4. Methodology

4.1) TRSec Methodology

In accordance with the Cyber Kill Chain Framework (CKCF), we advocate allocating a significant portion of Pen Test time to the Reconnaissance phase, with a suggested emphasis of over 50%. This strategic approach is derived from our practical experience, recognizing that a comprehensive understanding of the environment is pivotal for successful exploitation and ultimately ensuring the security of a resilient system.

Moreover, by embracing the DevOps culture and employing Continuous Integration/Continuous Deployment (CI/CD) methods, our methodology proposes multiple succinct cycles of "equivalent" CKCF. These cycles are intricately linked to a consistent Reconnaissance phase, bolstered by thorough documentation steps.

4.2) How risk was scored

We relied on the Common Vulnerability Scoring System (CVSS) as a benchmark for determining our risk score. Our process involved initially identifying a vulnerability, followed by an investigation to ascertain its recognition within the industry. If the vulnerability was widely known, we took into account the conventional score assigned by the cybersecurity community/industry. In cases where it was not well-known, we employed the CVSS calculator provided in the Appendix below. In both scenarios, we took into consideration the specific characteristics of NBN's IT systems.

4.3) Tools Used

VM VirtualBox Manager, Google, LinkedIn TCPdump, nmap, ncat, OpenVAS (Greenbone/GVM), OWASP ZAP, FileZilla, VSTPD Tool Rapid7 Database, CVE, GitHub, THC-hydra, rockyou wordlist, Microsoft Word, Excel, Firefox Web Browser, Windows 10 and Kali Linux OS.

5. Findings

5.1) OpenVAS Scan Findings

a) How we found it

The automated tool OpenVAS (Greenbone/GVM) was used in order to scan the server 10.10.0.66 for vulnerabilities and ports that could be exploited. Two mid-levels vulnerabilities were found, which include Anonymous FTP Login Reporting and FTP Unencrypted Cleartext Login.

Vulnerability	Severity ▾	QoD	Host IP	Host Name	Location
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	10.10.0.66		9001/tcp
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	10.10.0.66		9001/tcp
TCP timestamps	2.6 (Low)	80 %	10.10.0.66		general/tcp
SSH Server type and version	0.0 (Log)	80 %	10.10.0.66		443/tcp
OpenSSH Detection Consolidation	0.0 (Log)	80 %	10.10.0.66		general/tcp
SSH Protocol Algorithms Supported	0.0 (Log)	80 %	10.10.0.66		443/tcp
SSH Protocol Versions Supported	0.0 (Log)	95 %	10.10.0.66		443/tcp
OS Detection Consolidation and Reporting	0.0 (Log)	80 %	10.10.0.66		general/tcp

Figure 1. Result of OpenVAS scan on 10.10.0.66

Ports 80 and 8001, hosting Apache httpd 2.4.29 ((Ubuntu)), and port 443/tcp, featuring OpenSSH 7.6p1, were found to be relatively secure, lacking any known vulnerabilities (referenced below).

We then further enumerated the ports of 10.10.0.66 with *nmap* default scripts (*-sC*) and version detection (*-sV*). This also confirmed what we found earlier with OpenVAS.

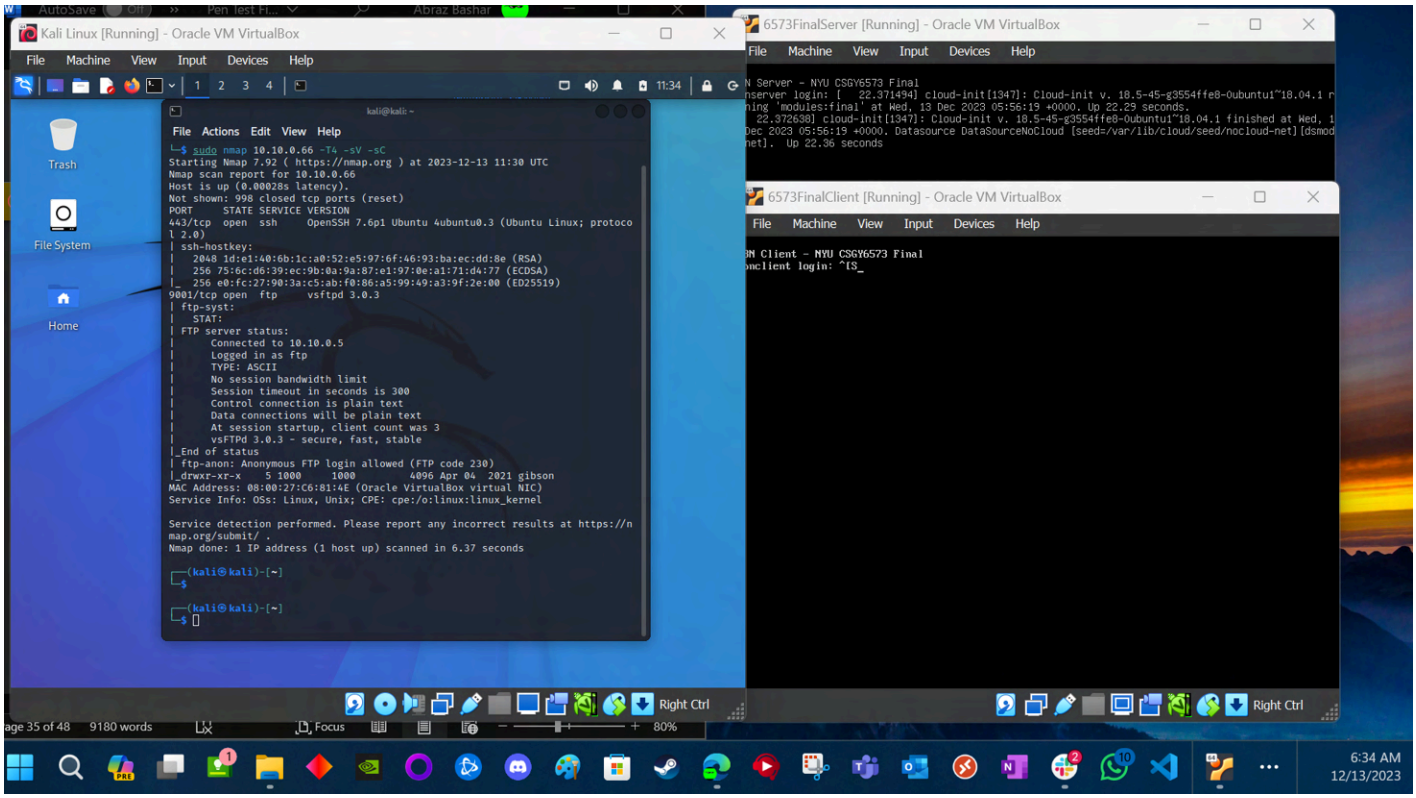


Figure 2. Using └─$ sudo nmap 10.10.0.66 -T4 -sV -sC

The relevant parts to focus on would be :

9001/tcp open ftp vsftpd 3.0.3

.

.

.

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|_drwxr-xr-x 5 1000 1000 4096 Apr 04 2021 gibson

b) How we exploited it

Consequently, our focus shifted to port 9001 utilizing the FTP protocol vsftpd 3.0.3. Notably, this port was configured to permit Anonymous FTP login (FTP code 230). Subsequently, we exploited this port using the vsftpd and FileZilla tool.

We have made the relevant changes to the *vsftpd.conf* file in order for the anonymous connection to work. We set up and additional windows VM with FileZilla, which was used to successfully log into the 10.10.0.6 server. A flag was also captured from the server (flag3. More details about recreating this in the Appendix).

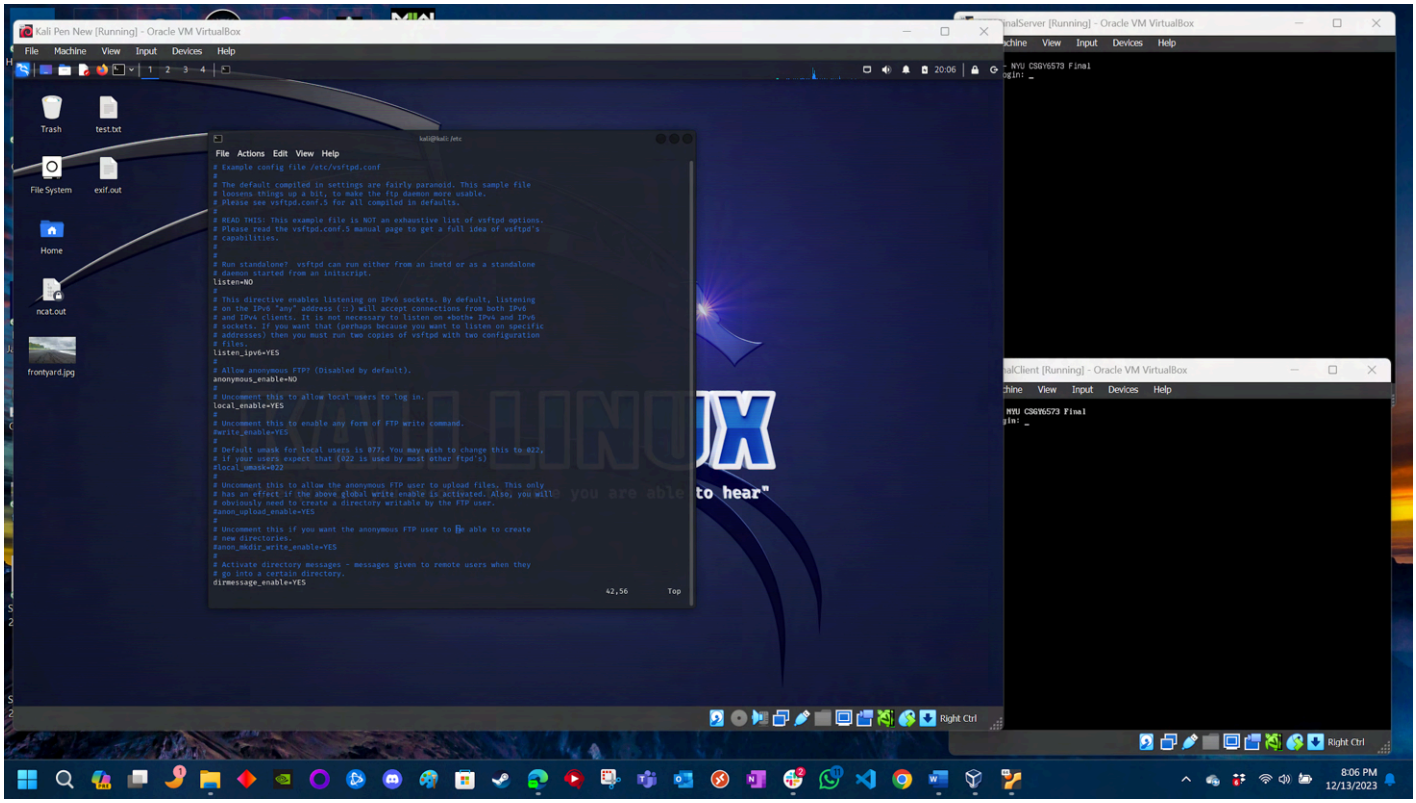
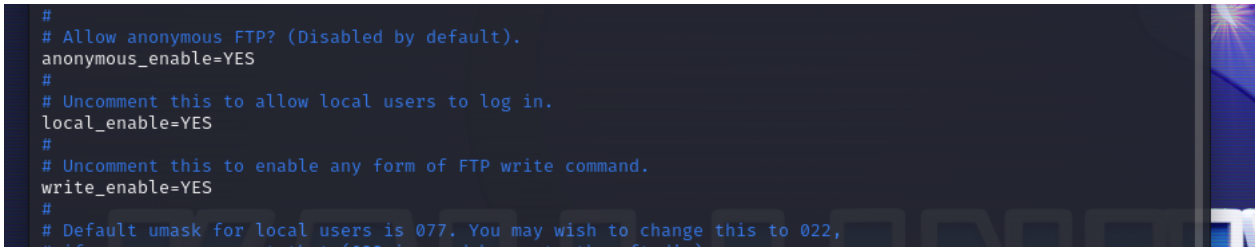


Figure 3. Unchanged */etc/vsftpd.config* file.



```
#chroot_local_user=YES
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
#
```

Figure 4. Relevant fields that were changed in order to accomplish the exploit.

References:

https://shadowmaster98.medium.com/source-680accc2d2d1

https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b

https://www.youtube.com/watch?v=MF-3iocKsEc

https://agyacorp.com/Pen%20Test%20Final%20Report%20to%20NBN%20AGYA%20v%203.0.pdf

This vulnerability/exploit led to Flag 3. Please Check the Appendix

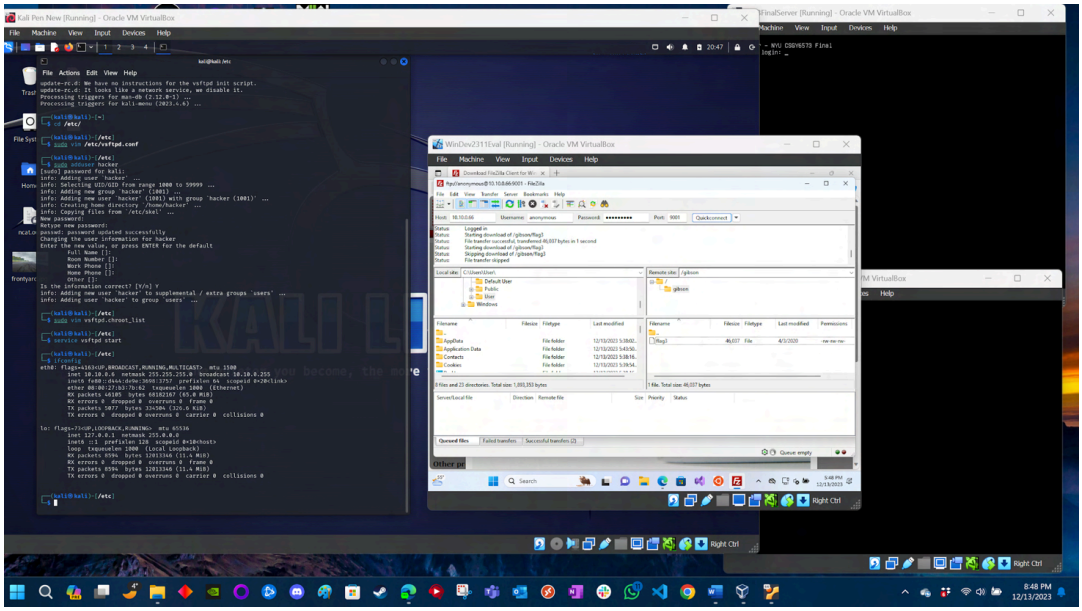


Figure 5. Using *FileZilla* in a Windows VM within the 10.10.0.0/24 subnet to connect to 10.10.0.66.

c) Risk Score and why

From CVSS table calculator (reference in the Appendix), this has a risk score of **8.2**.

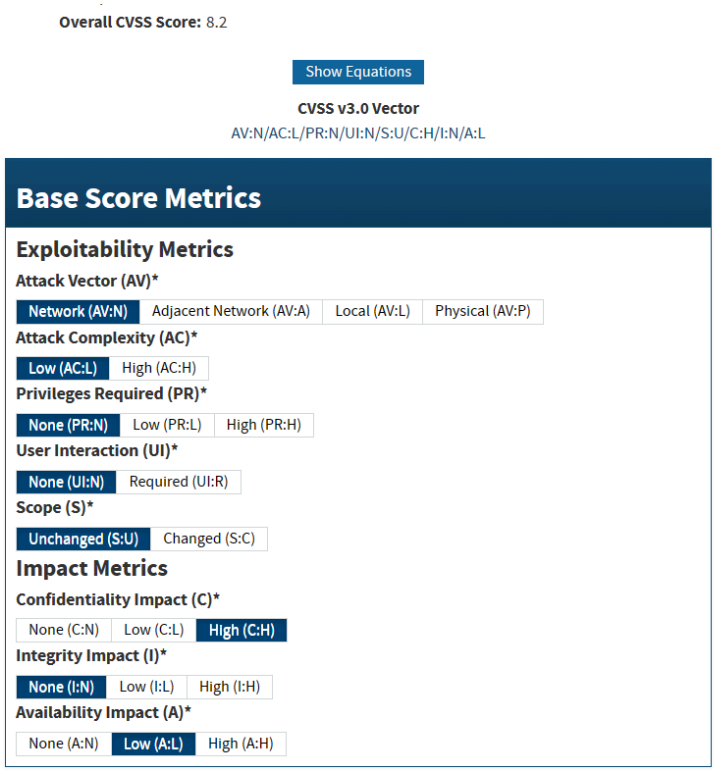


Figure 6. The CVSS Score of Finding **5.1)**.

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

d) How to fix this

The fix for this issue is fairly simple: Within the *vsftpd* config file(*/etc/vsftpd.conf*), disable Anonymous FTP. Set up the flag anonymous_enable = NO.

5.2) Password Brute Force with Hydra/Server SSH access Findings

a) How we found it

From the *nmap* scan (refer to **Figure 2.** In section **5.1)**) that was completed during the previous finding, we discovered that the ssh port 443 was open. We took advantage of the open vulnerable port of 9001 and used it to brute-force crack the password of the username we acquired from finding **5.1)**, “gibson”.

b) How we exploited it

Hydra is a tool used to brute-force crack username and password combinations. This means that it tries every possible combination of characters for a possible password. However, this task because very simple once we have a known username, as well as an easy/common password to deal with.

Hydra was used in combination with the wordlist file *rockyou.txt.gz*, which contains a list of commonly recurring passwords. The command is as follows:

└─$ *hydra -l gibson -P /usr/share/wordlists/rockyou.txt -vV 10.10.0.66 -s 9001 ftp*

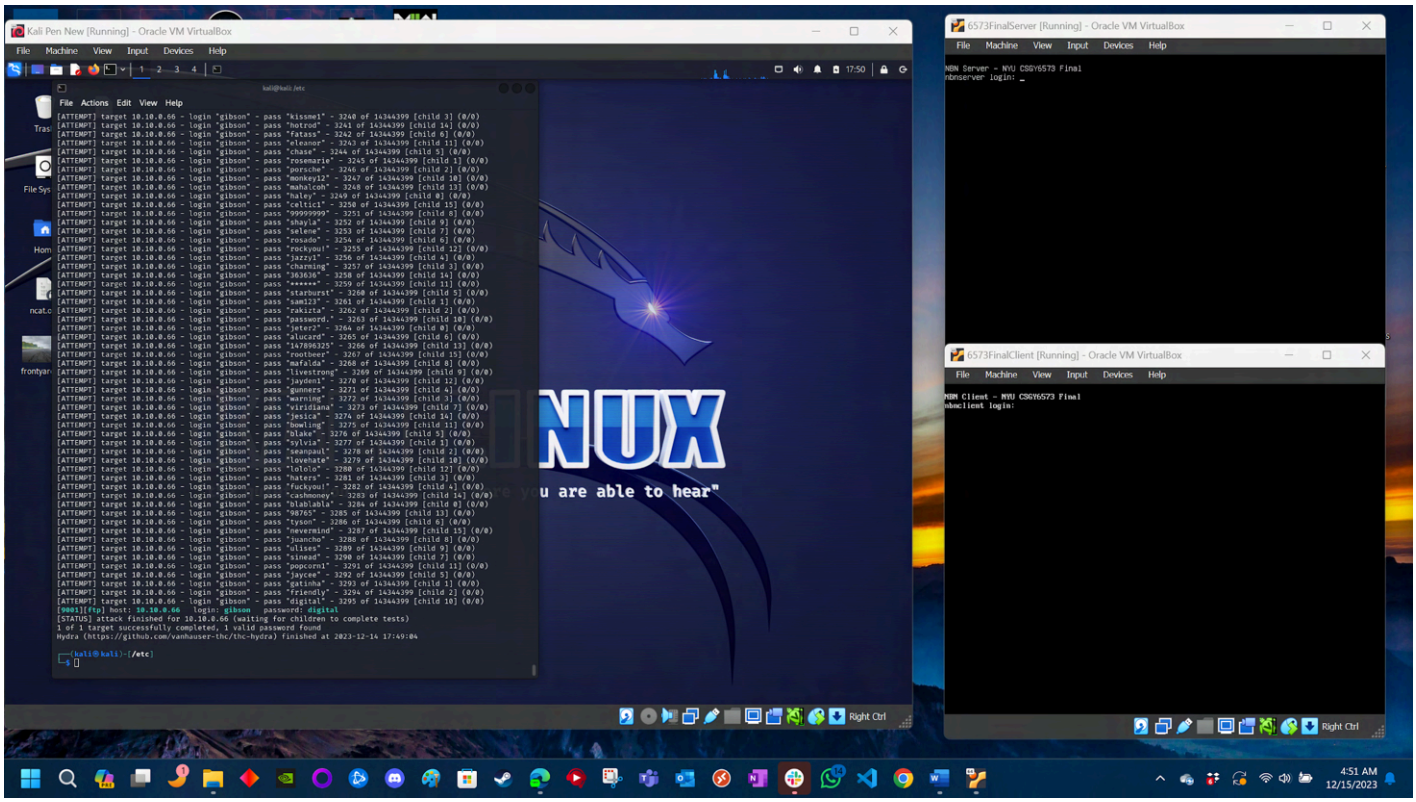


Figure 7. Using *Hydra* with *rockyou.txt* to crack user “gibson” password. Password = **digital**

Now that the password has been cracked, we can use the port 443 to log in to NBN’s server with user gibson’s credentials.

The following was entered from the *kali* machine:

└─$ ssh -p 443 10.10.0.66 -l gibson

└─$ password: digital

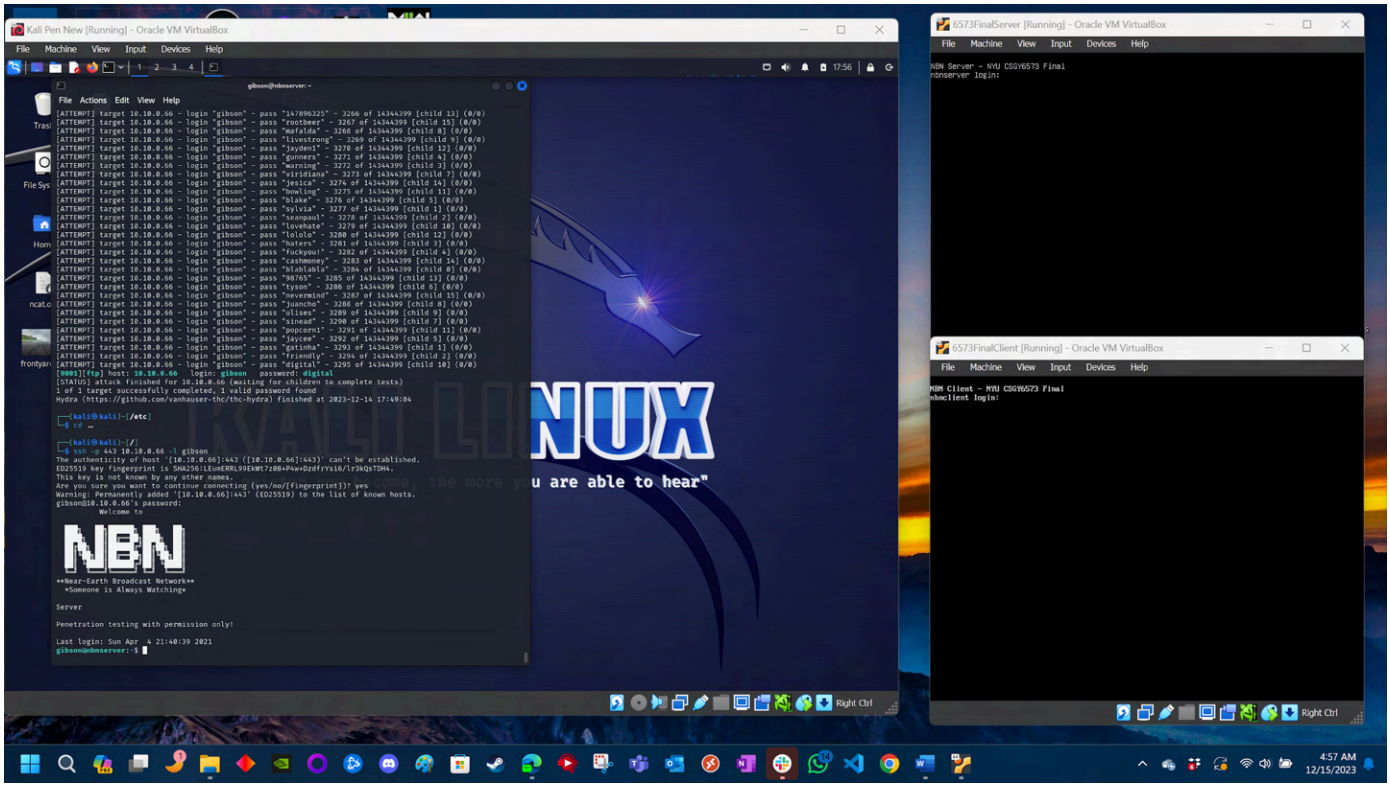


Figure 8. Successfully using user “gibson” and password “digital” to create a ssh to 10.10.0.66.

c) Risk Score and why

From CVSS table calculator, this has a risk score of **9.4.**

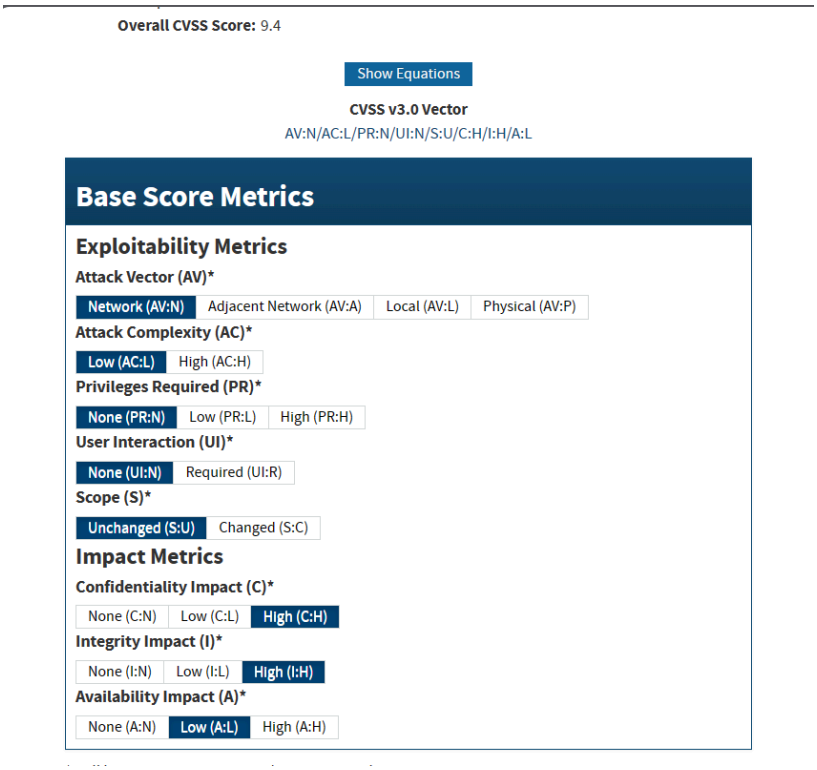


Figure 9. The CVSS Score of Finding **5.2)**.

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

d) How to fix

Implement comprehensive Password Policy within the company. This may include resetting passwords over a certain period of time, setting a specific character length for the password, as well as forcing users to add special characters, numbers and a mixture of upper and lowercase characters. MFA should also be adopted by all the staff, and password safety training should also be provided.

5.3) ZAP Scan Findings

a) How we found it

We performed a Man-in-the-middle (MitM) attack using OWASP ZAP on 10.10.0.66 NBN Server. There were a total of 23 alerts that came up as a result of the attack, out of which 4 were high and 19 were mid to low.

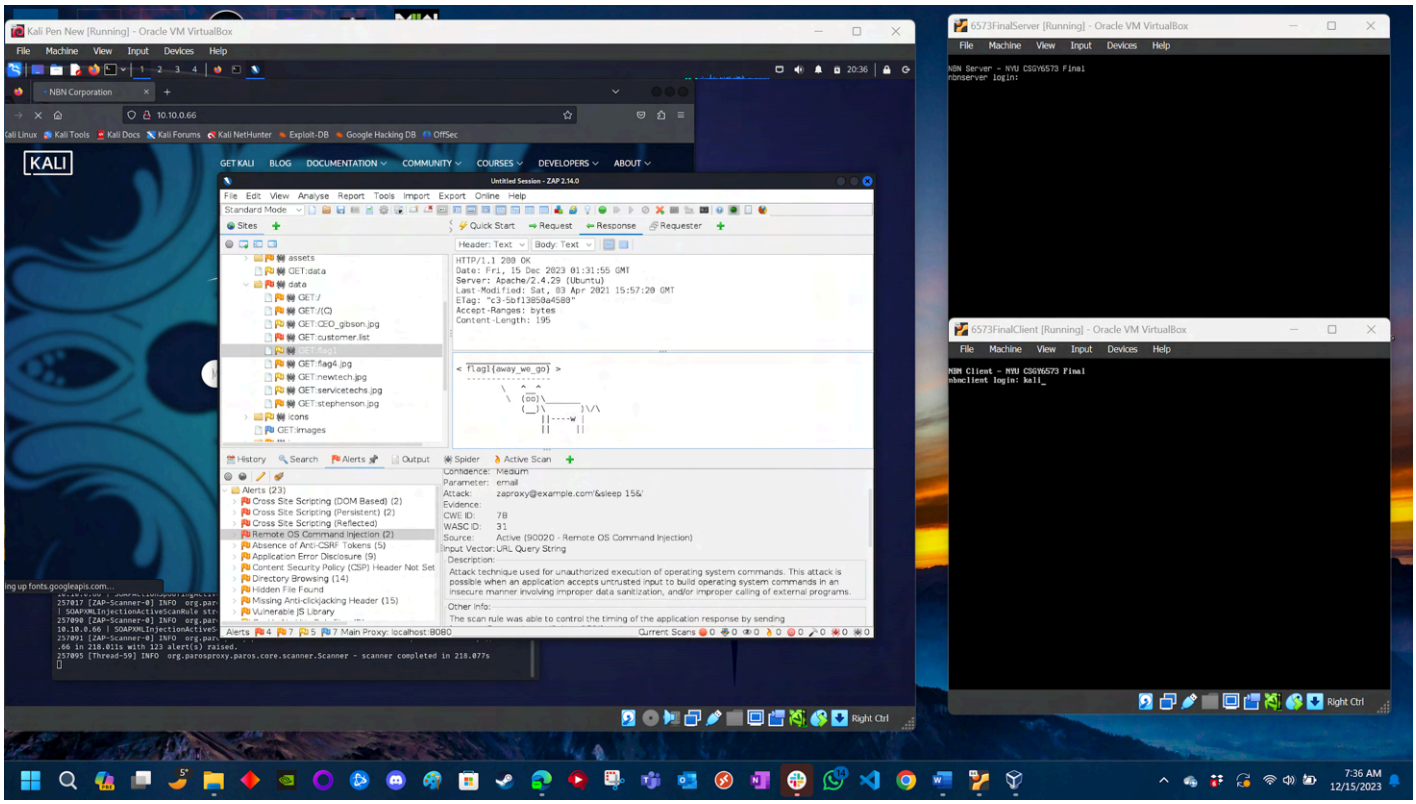


Figure 10. The usage of ZAP. The four red flags indicate the high-priority alerts.

This tool let us browse directories of the web app as well as give an alert of how the web app can be exploited based on a high to low alert priority categorization.

b) How we exploited it

The MitM attack itself is a great method to not only exploit the system, but to further find out more exploits. Amongst the further vulnerabilities found were Cross-site Scripting, unsafe developer comments, CEO image metadata, unsafe html comment. All of these are listed as separate findings below.

c) Risk Score and why

All 23 of the different vulnerabilities have different scores. I will only show the score of the highest one:

Absence of Anti-CSRF Token: 7.3

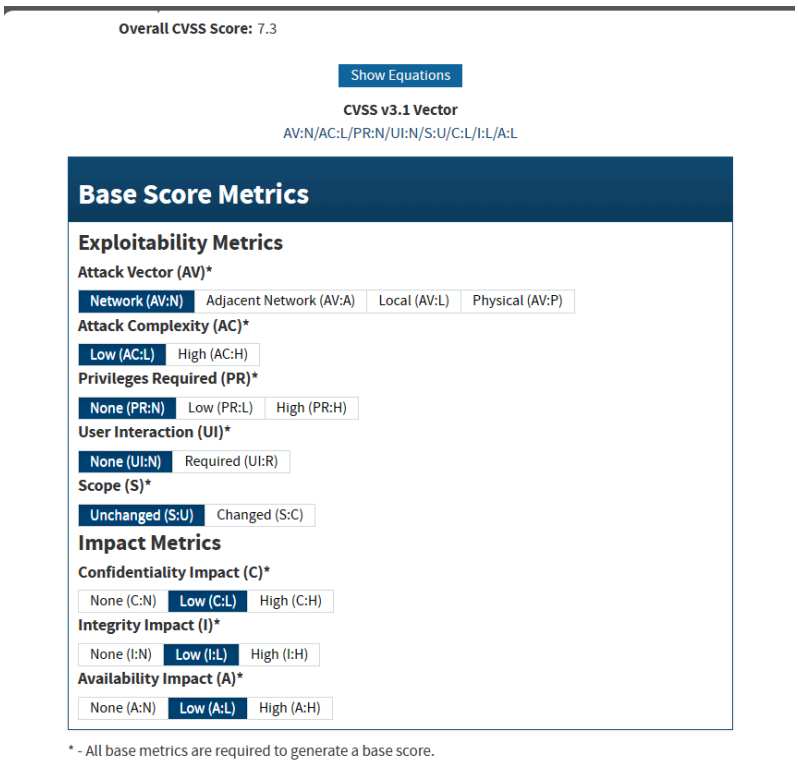


Figure 11. Score for Anti CSRF Token

d) How to fix it

The usage of the Anti-CSRF Token is to make sure there is no sort of forgery within the web app. NBN must make sure that its web app traffic is encrypted (SSL/TLS instead of just http).

5.4) CEO Image Metadata

a) How we found it

Through the ZAP MitM attack in 5.3, we found a poorly hidden note by NBN's developers.

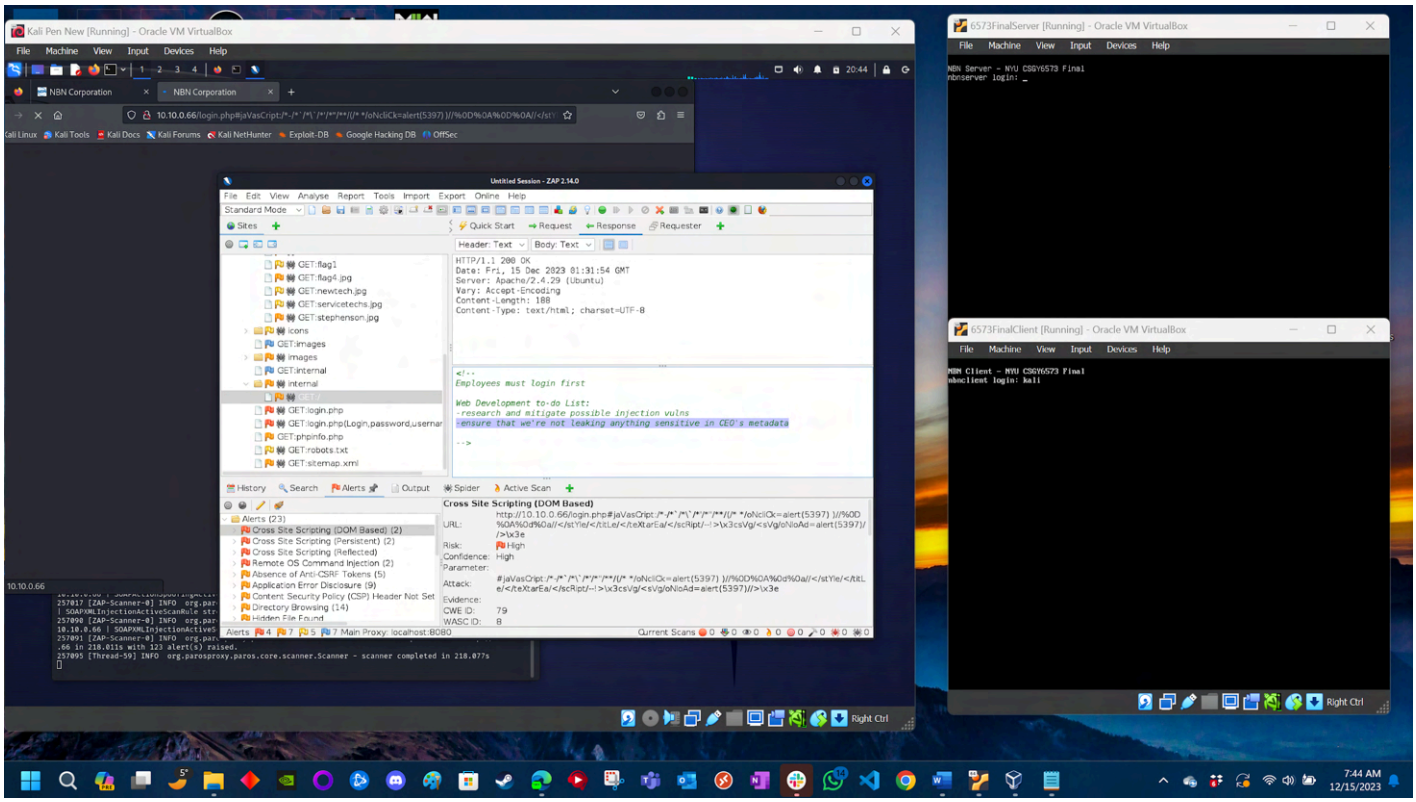


Figure 12. Poorly hidden comment by NBN developers.

The comments read "*-ensure that we're not leaking anything sensitive in the CEO's metadata*"

b) How we exploited it

We were able to navigate to the picture of the ceo in */data/GET:CEO_gibson.png.* We used the command └─*$ exiftool CEO_gibson.jpg > CEO.out* to export the metadata of the png file which revealed the password of the CEO to be "digital".

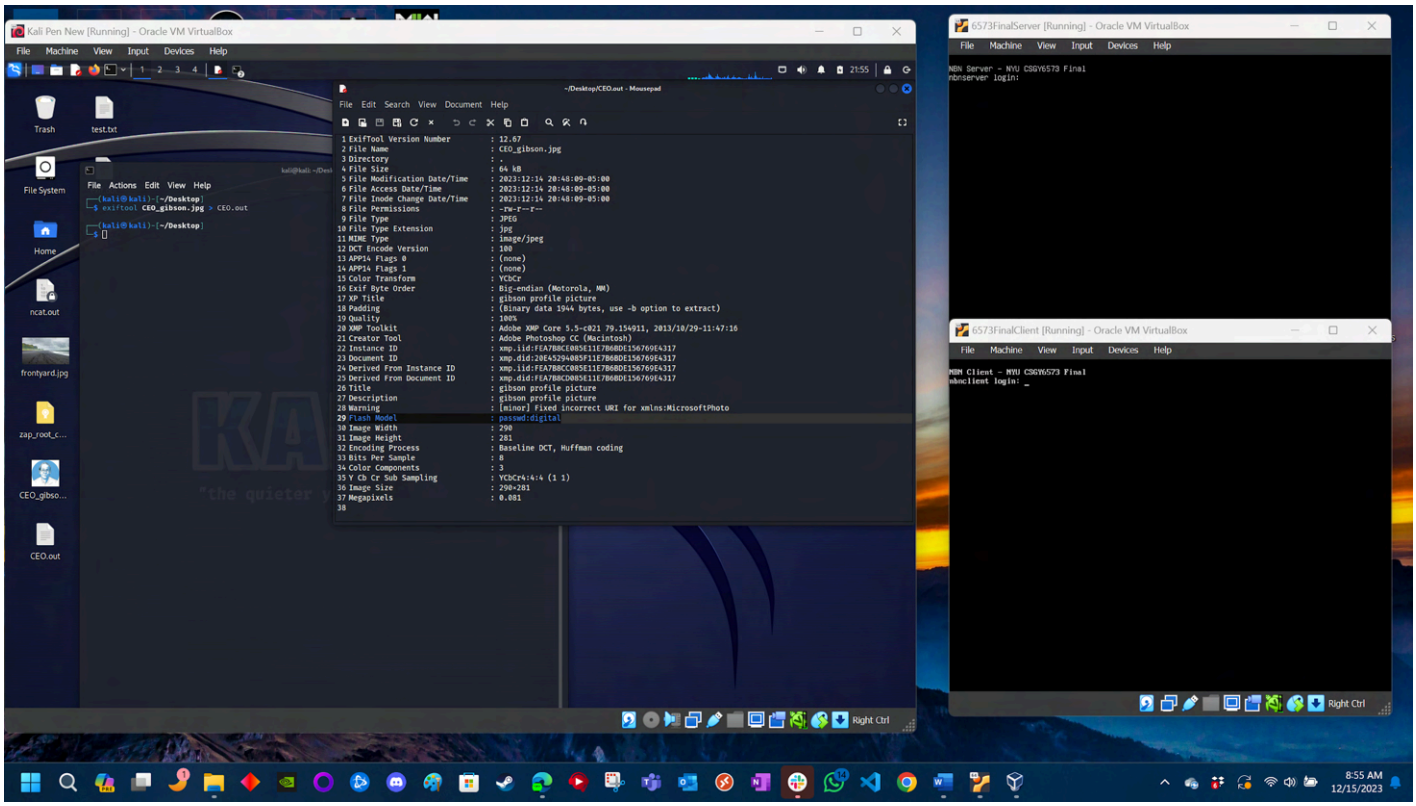


Figure 12. CEO's image metadata revealing the password of the CEO ("digital")

c) Risk Score and why

Similar to the score of the finding **5.2)**, this one is also a 9.4

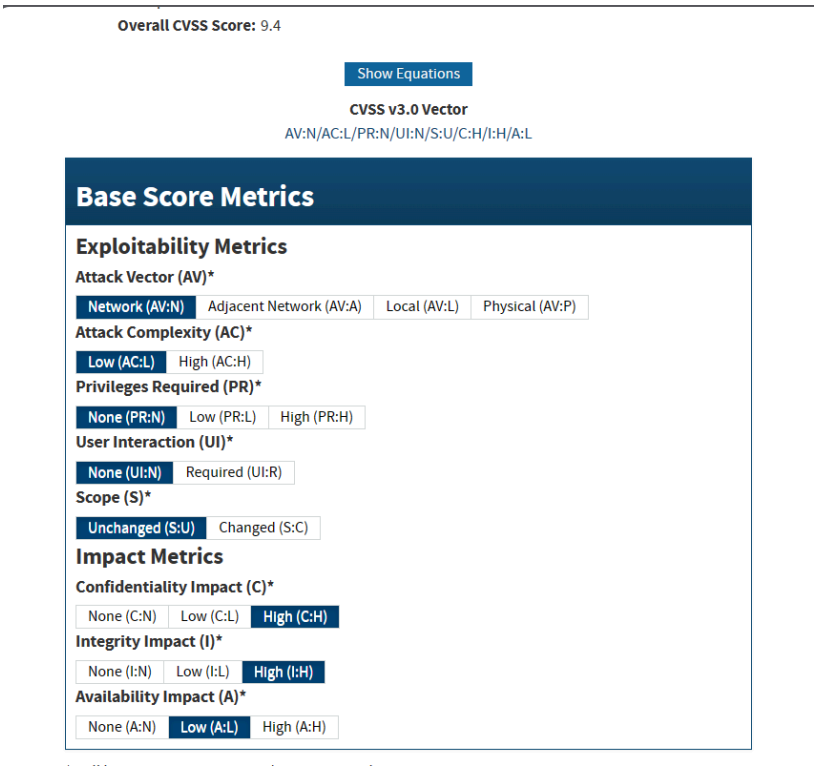


Figure 13. The CVSS Score of the CEO's password leak.

d) How to fix it

There has to be a security phase in the DevOps lifecycle that ensures no unsafe comments by developers on production, external facing code. Also, avoiding putting such metadata into PNG files. Fix such errors immediately before any compromise occurs.

5.5) Cross-Site Scripting

a) How we found it

We were able to find a highly sensitive link which contains all the customer personal data through the ZAP MitM investigation, as well as through poor site html commenting discovered through *Firefox* inspect element tool.

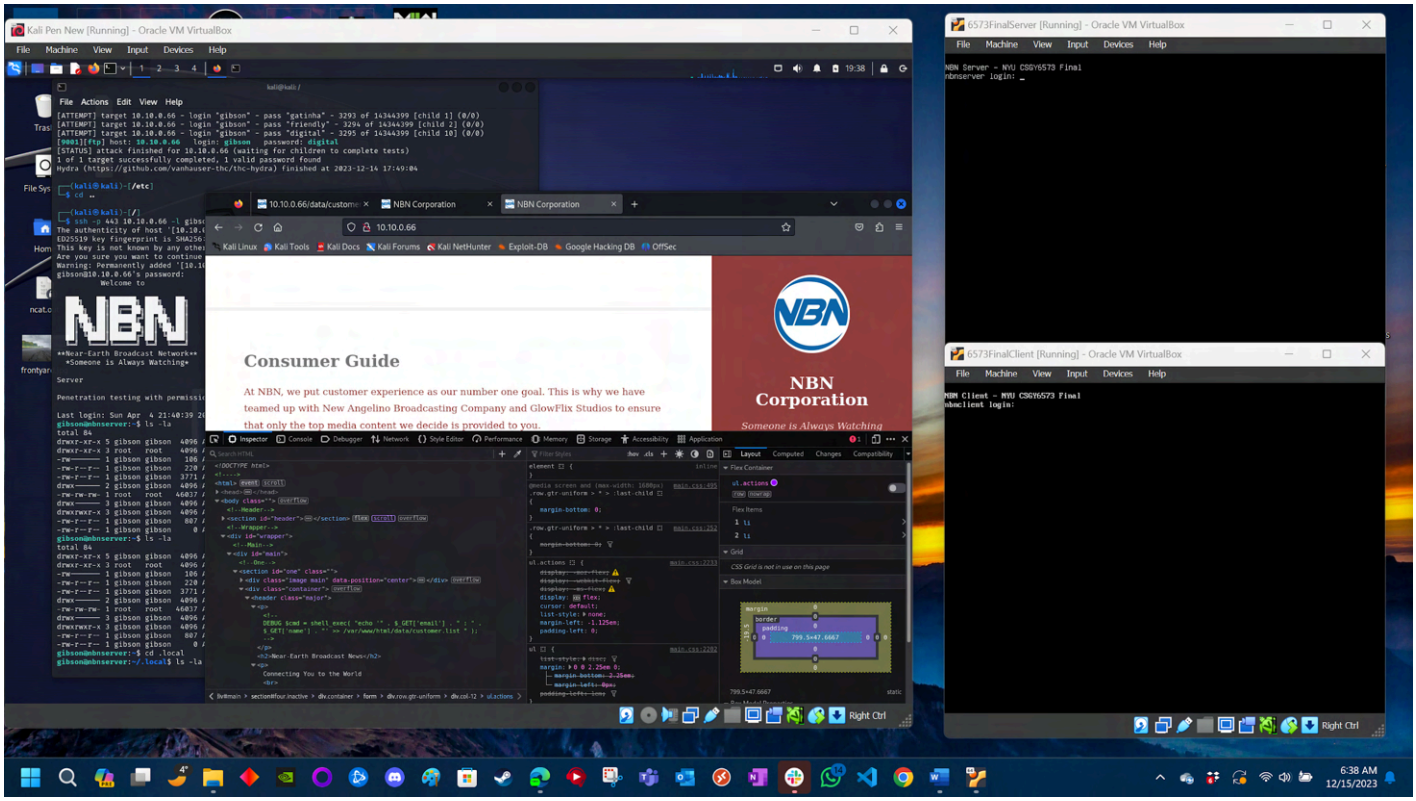


Figure 14. Web page dev's left a comment in the html that is extremely risky.

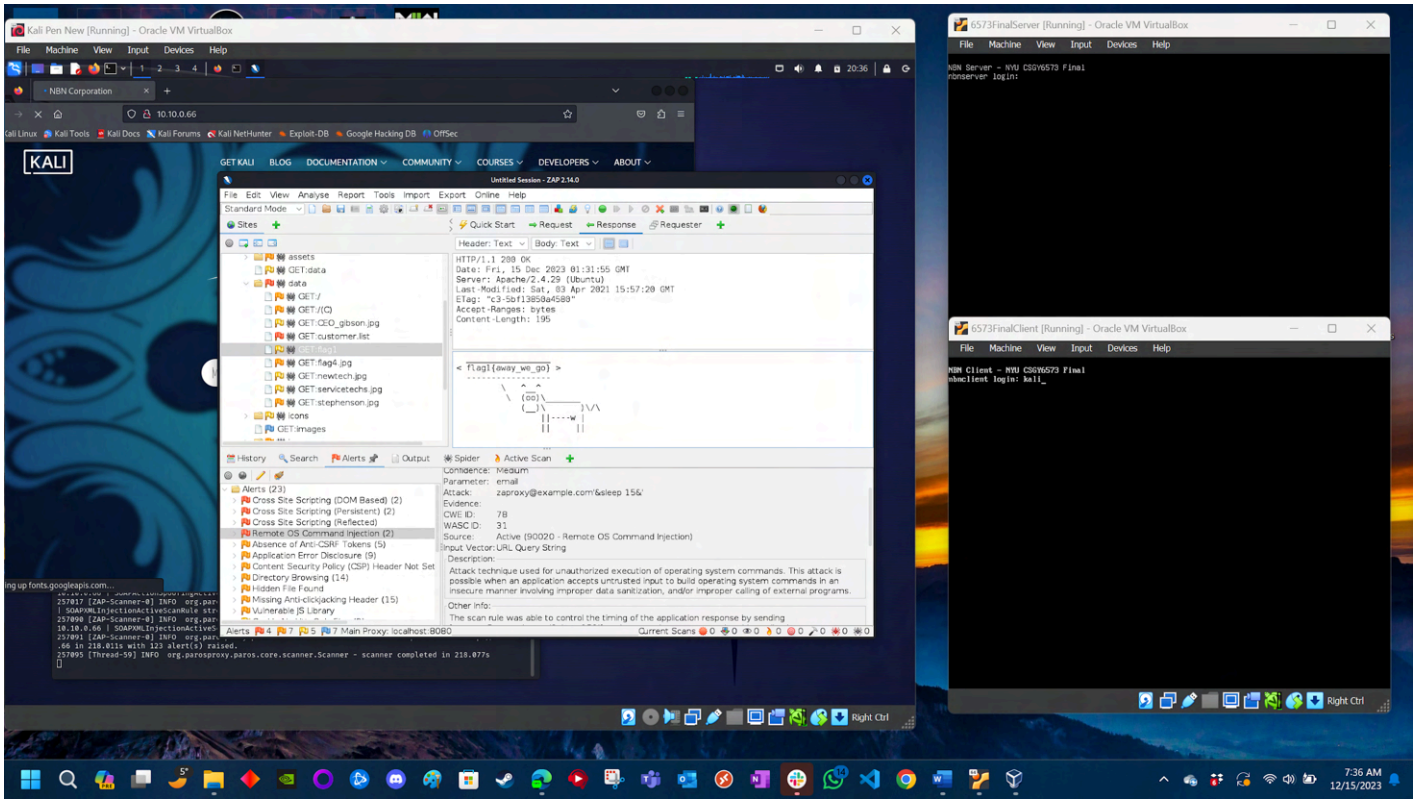


Figure 15. The alert "*Cross Site Scripting (Persistent)*" leads us to the *customer.list* file.

b) How we exploited it

We were easily able to access the document by just going to the link *http://10.10.0.66/data/customer.list*.

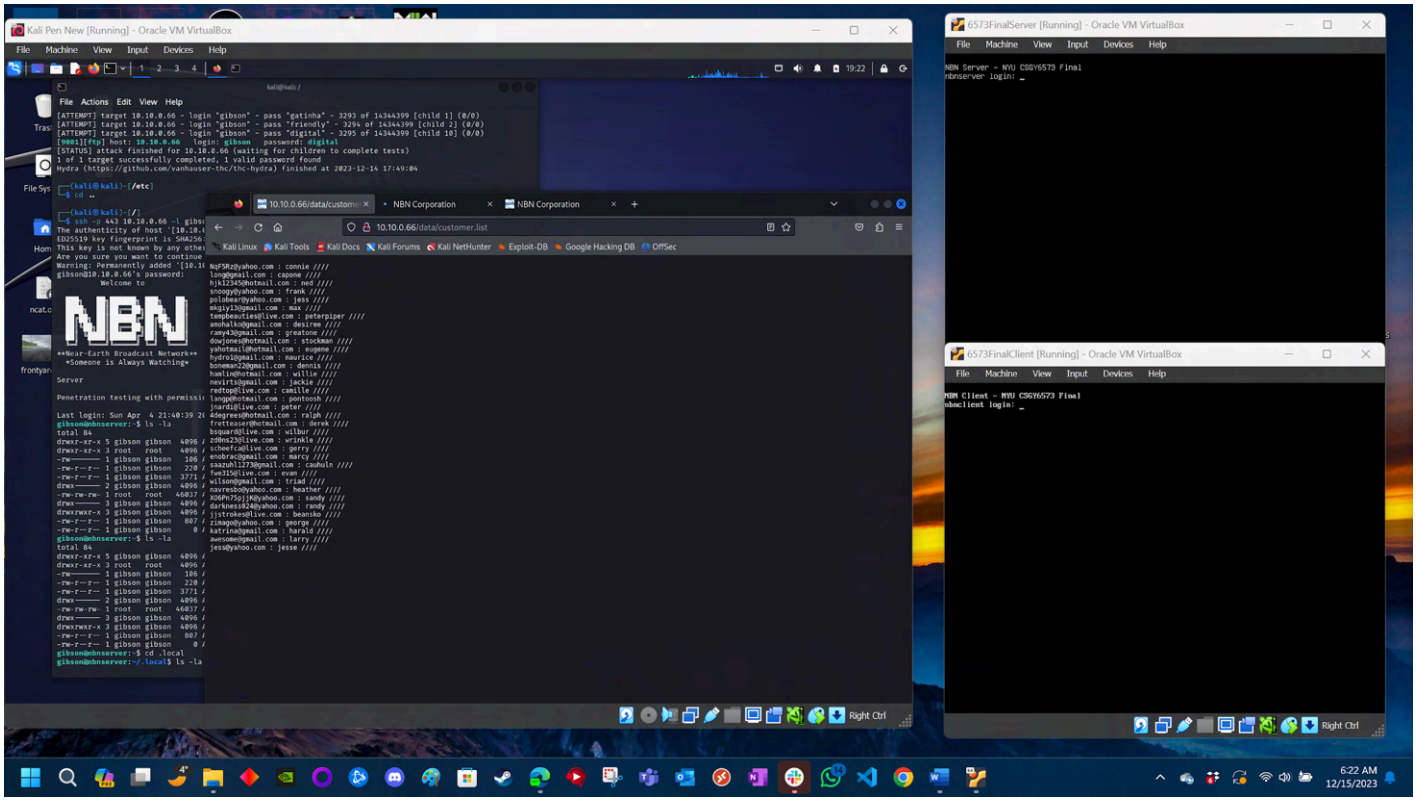


Figure 16. View of the sensitive file *customer.list*.

c) Risk Score and why

Cross Site Scripting (persistent): 7.3

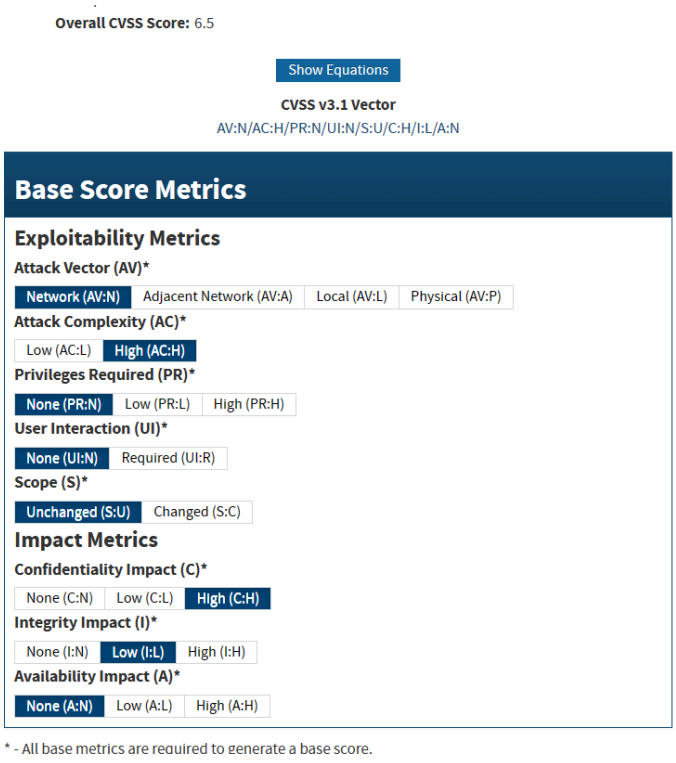


Figure 17. Score for Cross Site Scripting (persistent)

d) How to fix it

There has to be a security phase in the DevOps lifecycle that ensures no unsafe comments by developers on production, external facing code. Avoid releasing debugging comments into the production code. Dev's must also learn transmitting data using proper encoding to prevent Cross Site Scripting.

5.6) Bad Authentication/Authorization Mechanisms, Information Leakage

e) How we found it

Entering any SQL code show's the internal SQL variable names. Any log in attempt also show the credentials in plaintext on the URL.

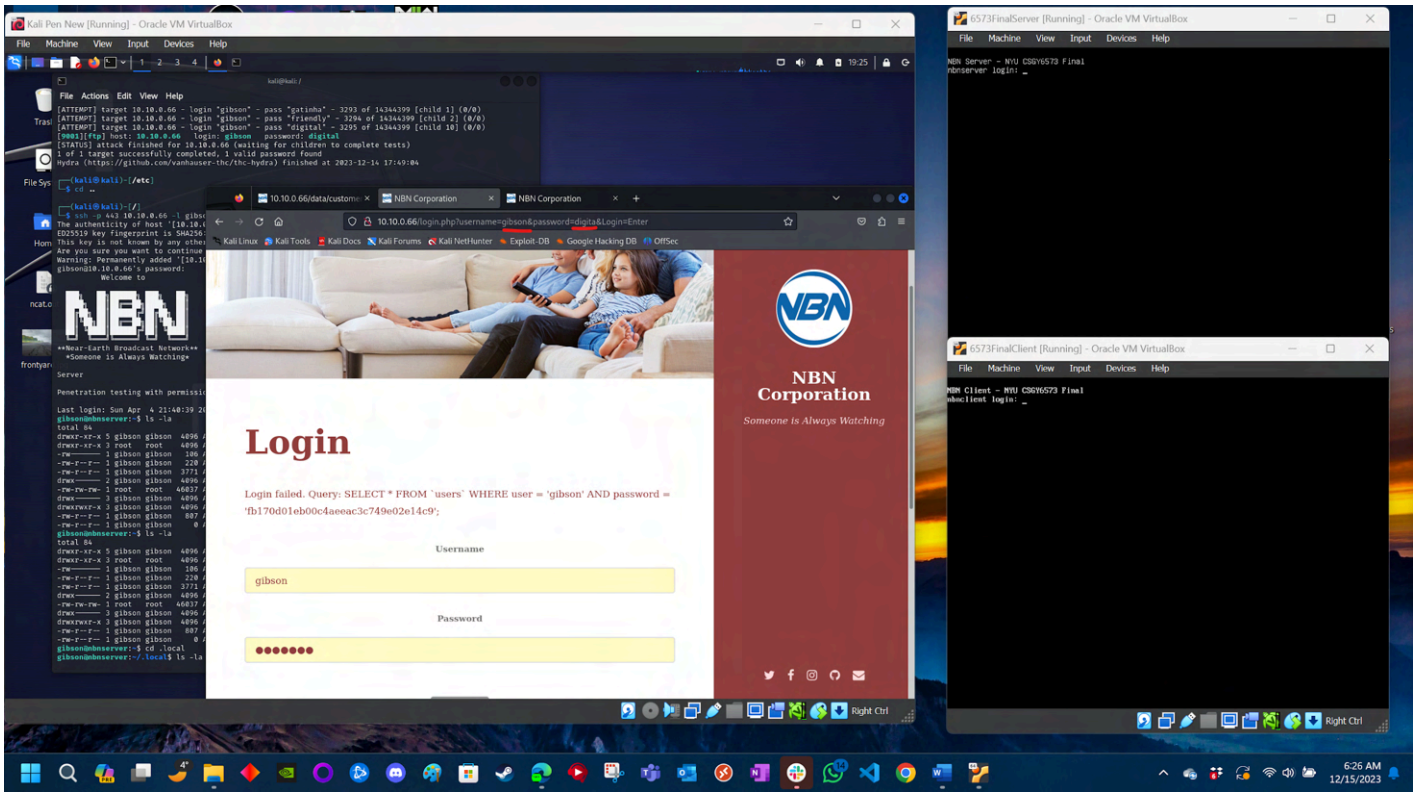


Figure 18. Credentials visible in url

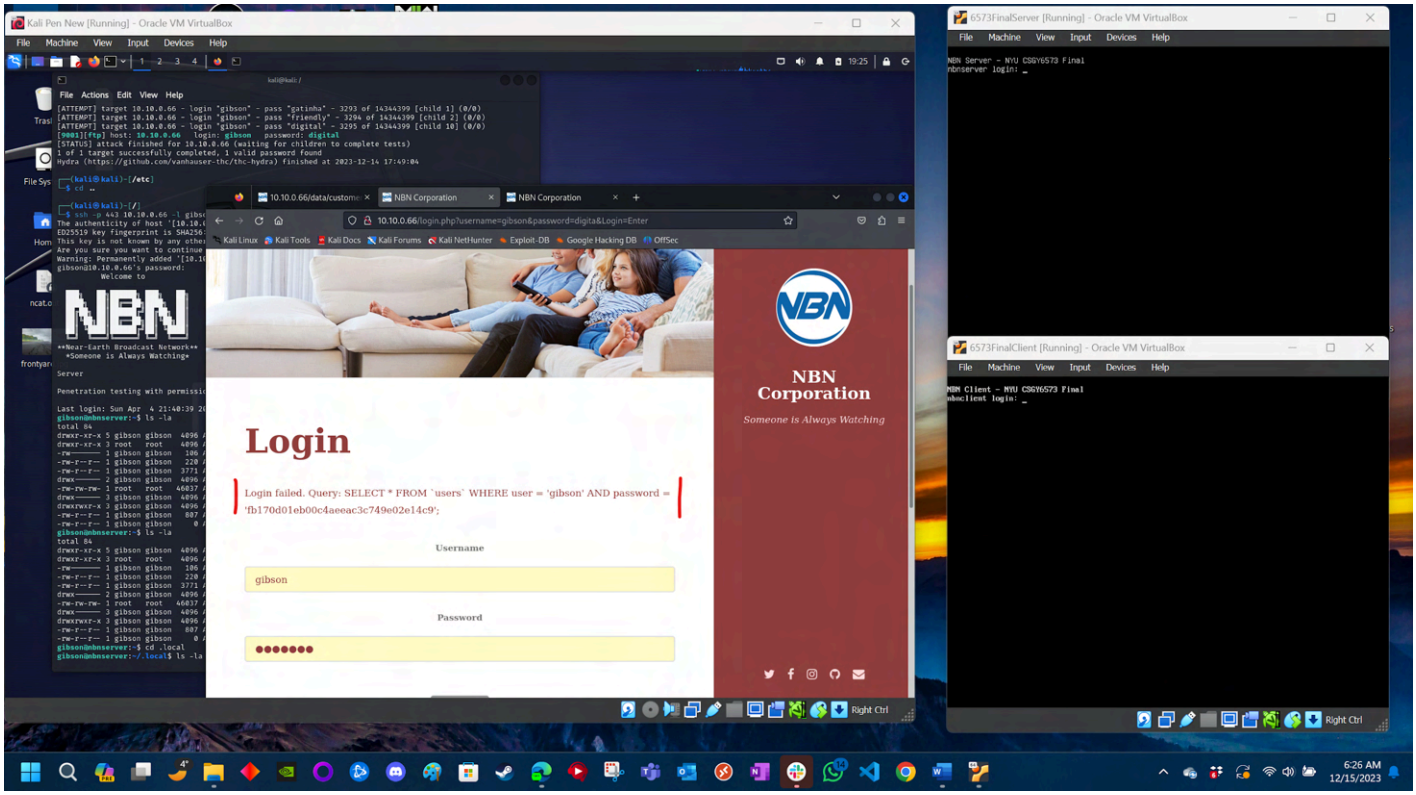


Figure 19. SQL variable names clearly visible.

f) How we exploited it

An successful log in reveals the credentials via the URL line. Additionally, SQL injections are made easier as well.

g) Risk Score and why

Score: 7.6

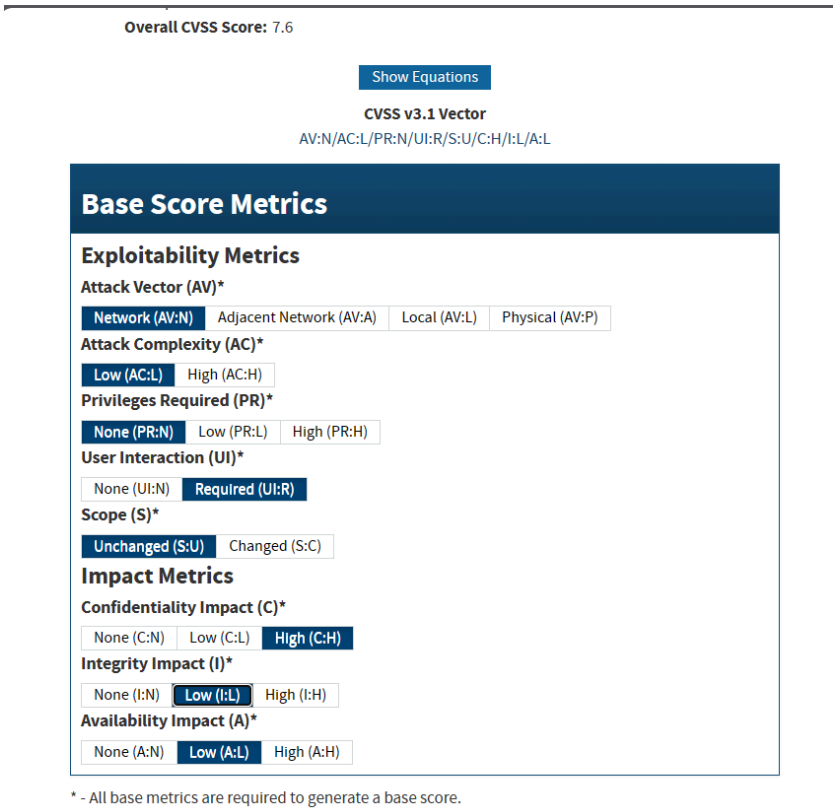


Figure 20. Information leakage score.

h) How to fix it

The developers can create separate variables for the credentials and send the variables via the URL instead of the actual variables. Also, they can make sure that the SQL errors do not show up to the webpage where it in clear view.

6. Conclusion

6.1) Test Goals

Tandon Red Security (TRSec) has secured a contract to engage proficient cybersecurity consultants for the execution of penetration testing services on a designated portion of NBN's IT infrastructure. This report outlines the penetration test findings, emphasizing NBN's cybersecurity vulnerability to external threats, and provides recommendations on mitigating this risk.

6.2) Results

1. OpenVAS Scan Discovery — CVSS Score 8.2
2. Hydra Password cracking) — CVSS Score 9.4
3. ZAP Scan Discovery — CVSS Score 6.8
4. XSS Persistent (Customer list exposed!) — CVSS Score 6.5
5. CEO Image Metadata Leak — CVSS Score 9.4
6. Information Leak/Bad Auth — CVSS Score 7.6

The Overall security score is the highest vulnerability: System CVSS Score 9.4

6.3) Targets

The following scope was considered:

- External Network Pen Testing (Enumeration and assessment of all external facing hosts and services.)
- External Web App Pen Testing (Assessment and exploitation of all external facing Web Apps.)
- Internal Network Pen Test (Post-exploitation suggested as future work.)
- Severity. Only “medium”, “high” and “critical” severities were presented (above 4.0 in the CVSS score

scale).

6.4) Immediate Fixes

We suggest immediate actions on items 1, 2, 4 and 5, as follows.
1 – OpenWAS Finding – REMOVE ANONYMOUS LOGIN
2 – Hydra Brute Force – ENFORCE COMPANY-WIDE PASSWORD POLICY
4 - XSS Persistent (Customer list exposed!) – ENCRYPT PAGE DATA/CUSTOMER.LIST
5 – CEO IMAGE METADATA – CHANGE CEO PASSWORD AND CLEAN UP METADATA AND DEV COMMENTS

6.5) Future Work

This work will be followed up by a post-exploitation, with privilege escalation.

6.6) Final Acceptance and Payment

Please contact atb429@nyu.edu from TRSec for a comprehensive invoice.

Appendix

a. Links, References, and Outside Resources

https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf https://csrc.nist.gov/publications/detail/sp/800-115/final
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html https://www.nist.gov/privacy-framework/nist-sp-800-30
https://www.first.org/cvss/
https://github.com/juliocesarfort/public-pentesting-reports https://nvd.nist.gov/vuln-metrics/cvss
https://www.cvedetails.com/cve/CVE-2001-0794/
https://www.cvedetails.com/cve/CVE-2017-14092/
https://www.invicti.com/blog/web-security/protecting-website-using-anti-csrf-token/
https://www.zaproxy.org/
https://www.cvedetails.com/cve/CVE-2017-14219/
https://www.cvedetails.com/cve/CVE-2022-29095/
https://www.dc864.org/2022/06/tryhackme-writeup-agent-sudo/

https://www.sherweb.com/blog/security/password-policies/
https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

b. Ports, Protocols, and Services

WEB SERVER AND GATEWAY (172.16.1.1 and 10.10.0.66)

PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
443/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0) 8001/tcp open http Apache httpd 2.4.29 ((Ubuntu))
9001/tcp open ftp vsftpd 3.0.3
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

CLIENT (172.16.1.2)
Starting Nmap 7.93 (https://nmap.org) at 2022-11-16 16:33
EST Nmap scan report for 172.16.1.2
Host is up (0.0018s latency).
All 1000 scanned ports on 172.16.1.2 are in ignored states. Not shown: 1000 filtered tcp ports (no-response)

c. Sensitive Data Enumeration (e.g. flags, passwords)

Bill Gibson, CISO
gibson@corp.nbn
NBN Corp
1800 Archer Street
New York, NY

SERVER LOGIN

host: 10.10.0.66
login: gibson
password: digital

NBN Clients information:

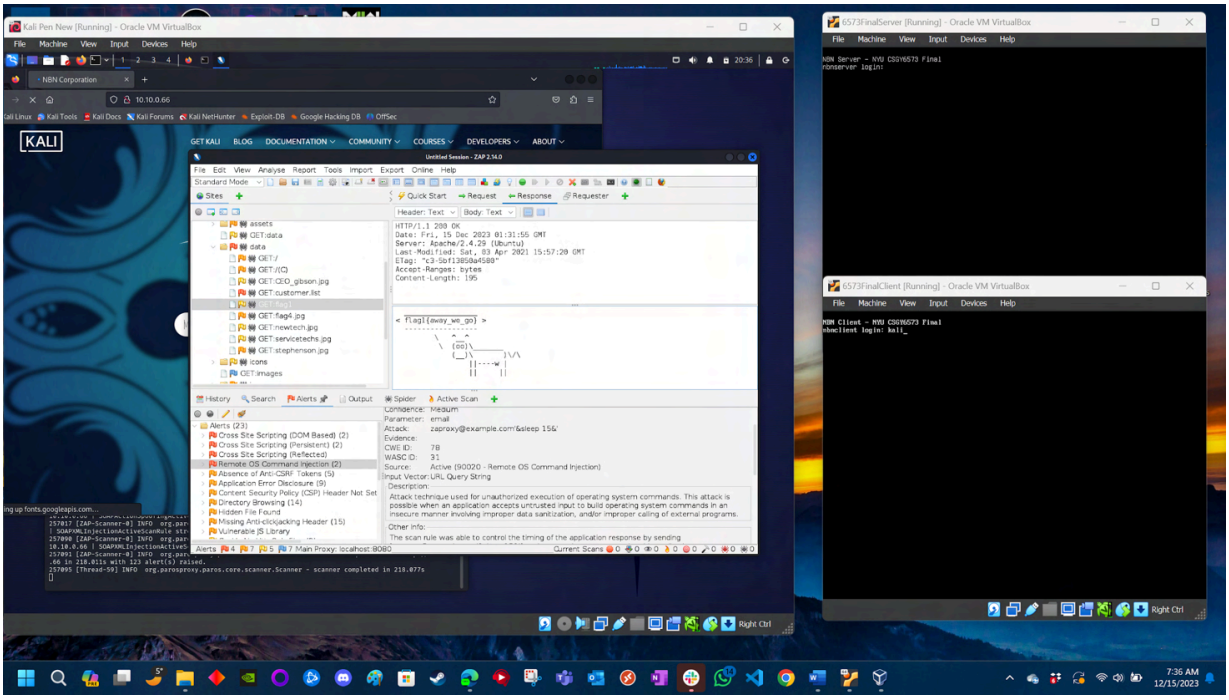
NqF5Rz@yahoo.com : connie ////
long@gmail.com : capone ////
hjk12345@hotmail.com : ned ////
snoogy@yahoo.com : frank ////
polobear@yahoo.com : jess ////
mkgiy13@gmail.com : max ////
tempbeauties@live.com : peterpiper ////
amohalko@gmail.com : desiree ////
ramy43@gmail.com : greatone ////
dowjones@hotmail.com : stockman ////
yahotmail@hotmail.com : eugene ////
hydro1@gmail.com : maurice ////
boneman22@gmail.com : dennis ////
hamlin@hotmail.com : willie ////
nevirts@gmail.com : jackie ////
redtop@live.com : camille ////
langp@hotmail.com : pontoosh ////
jnardi@live.com : peter ////
4degrees@hotmail.com : ralph ////

fretteaser@hotmail.com : derek ////
bsquard@live.com : wilbur ////
zd0ns23@live.com : wrinkle ////
scheefca@live.com : gerry ////
enobrac@gmail.com : marcy ////
saazuhl1273@gmail.com : cauhuln ////
fwe315@live.com : evan ////
wilson@gmail.com : triad ////
navresbo@yahoo.com : heather ////
XO6Pn75pjjK@yahoo.com : sandy ////
darkness024@yahoo.com : randy ////
jjstrokes@live.com : beansko ////

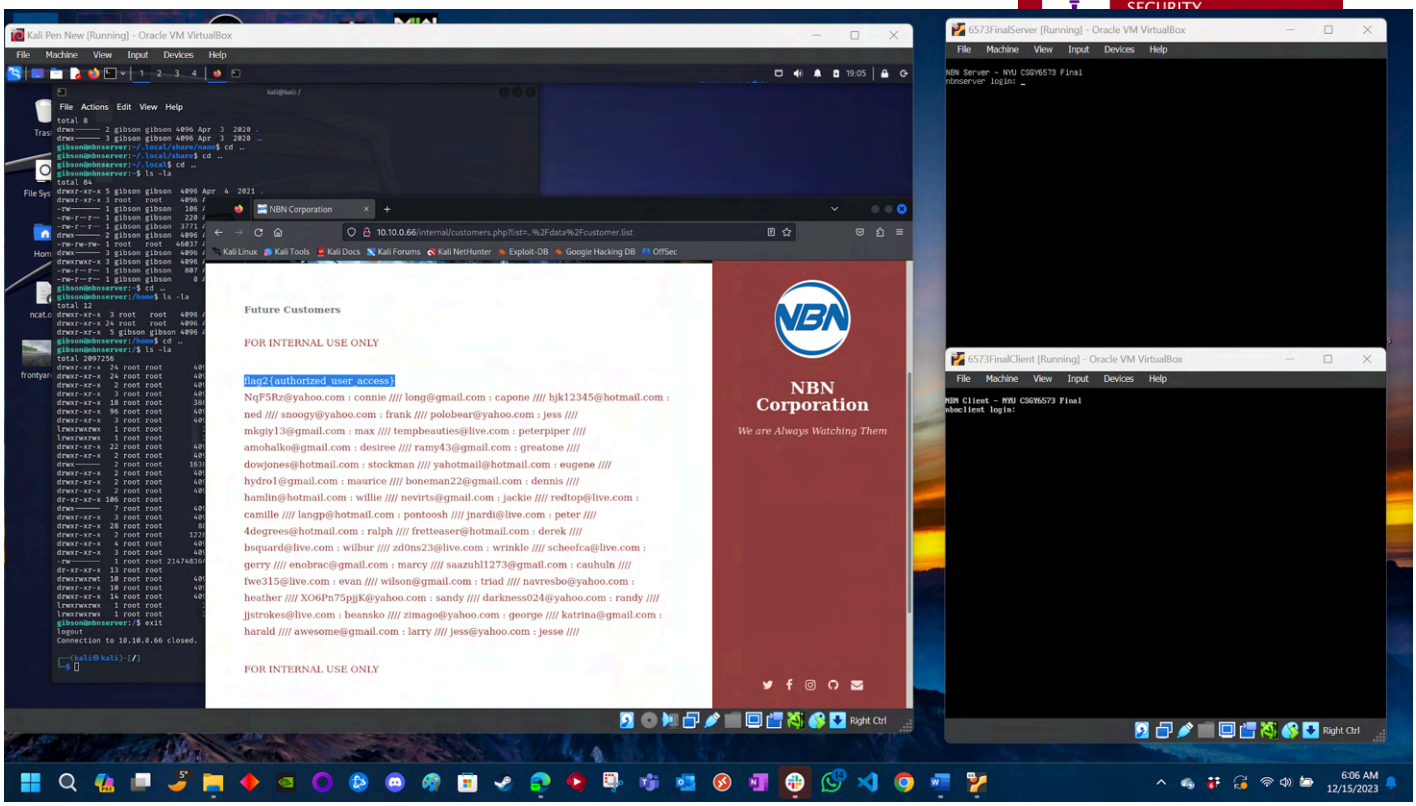
zimago@yahoo.com : george ////
katrina@gmail.com : harald ////
awesome@gmail.com : larry ////
jess@yahoo.com : jesse ////

FLAGS: 1,2 and 3

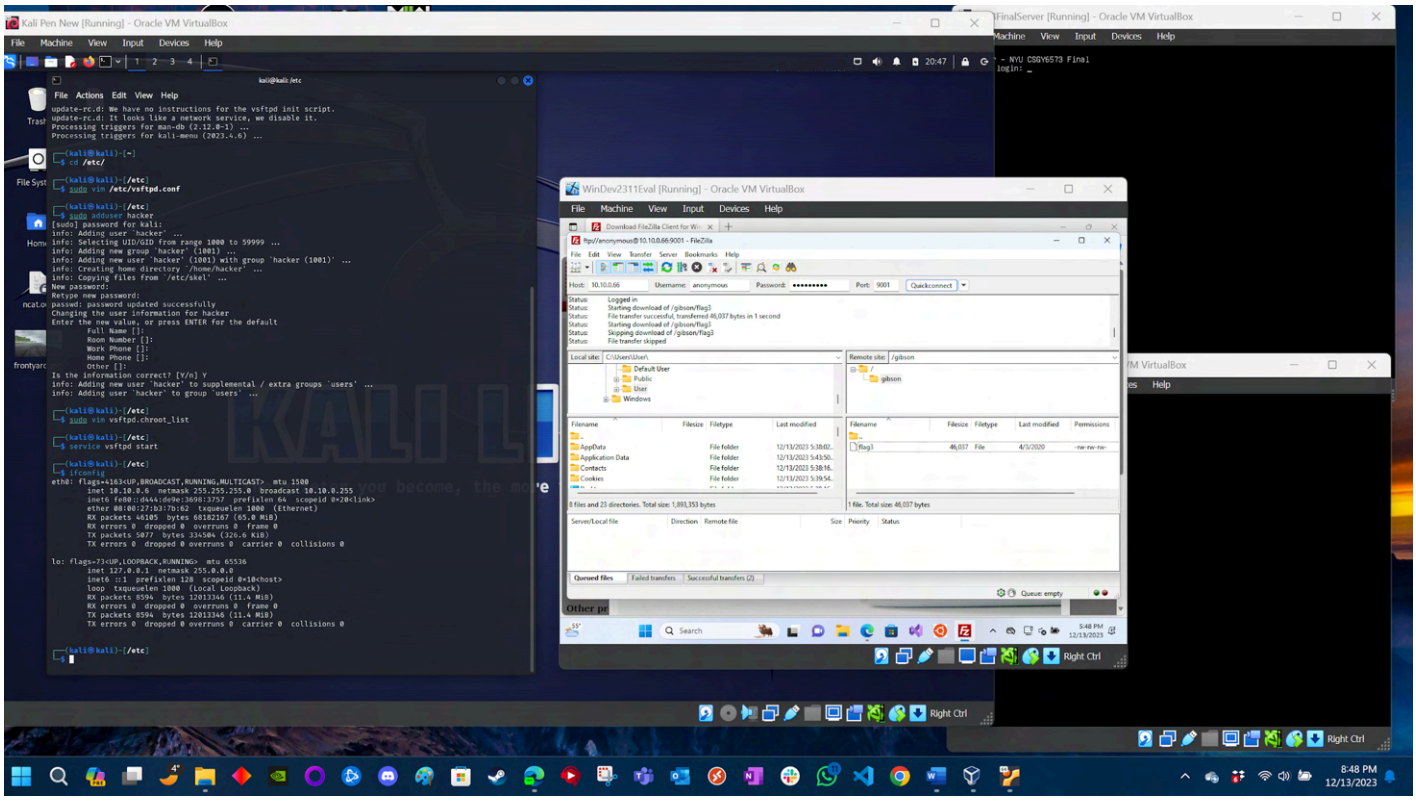
FLAG 1: flag1{away_we_go}

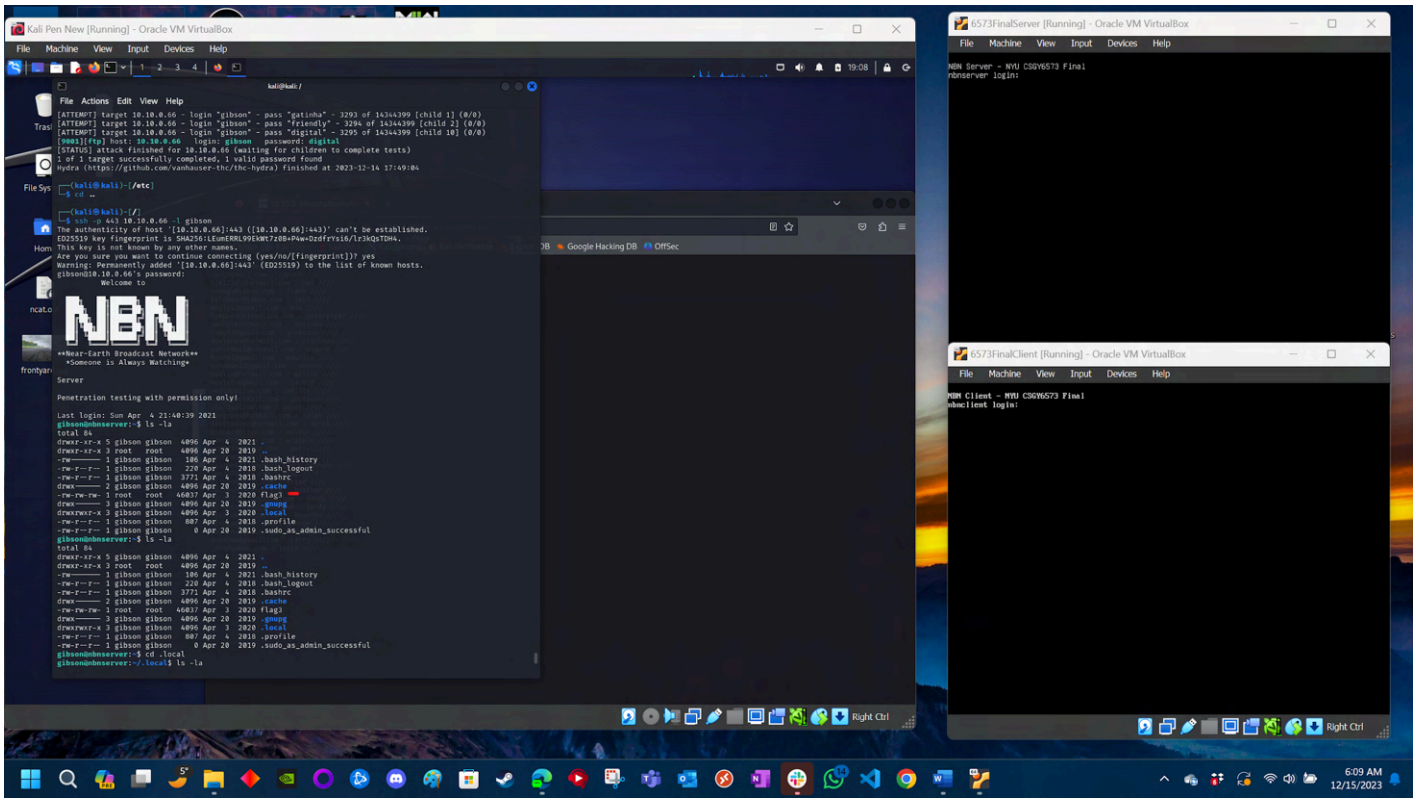


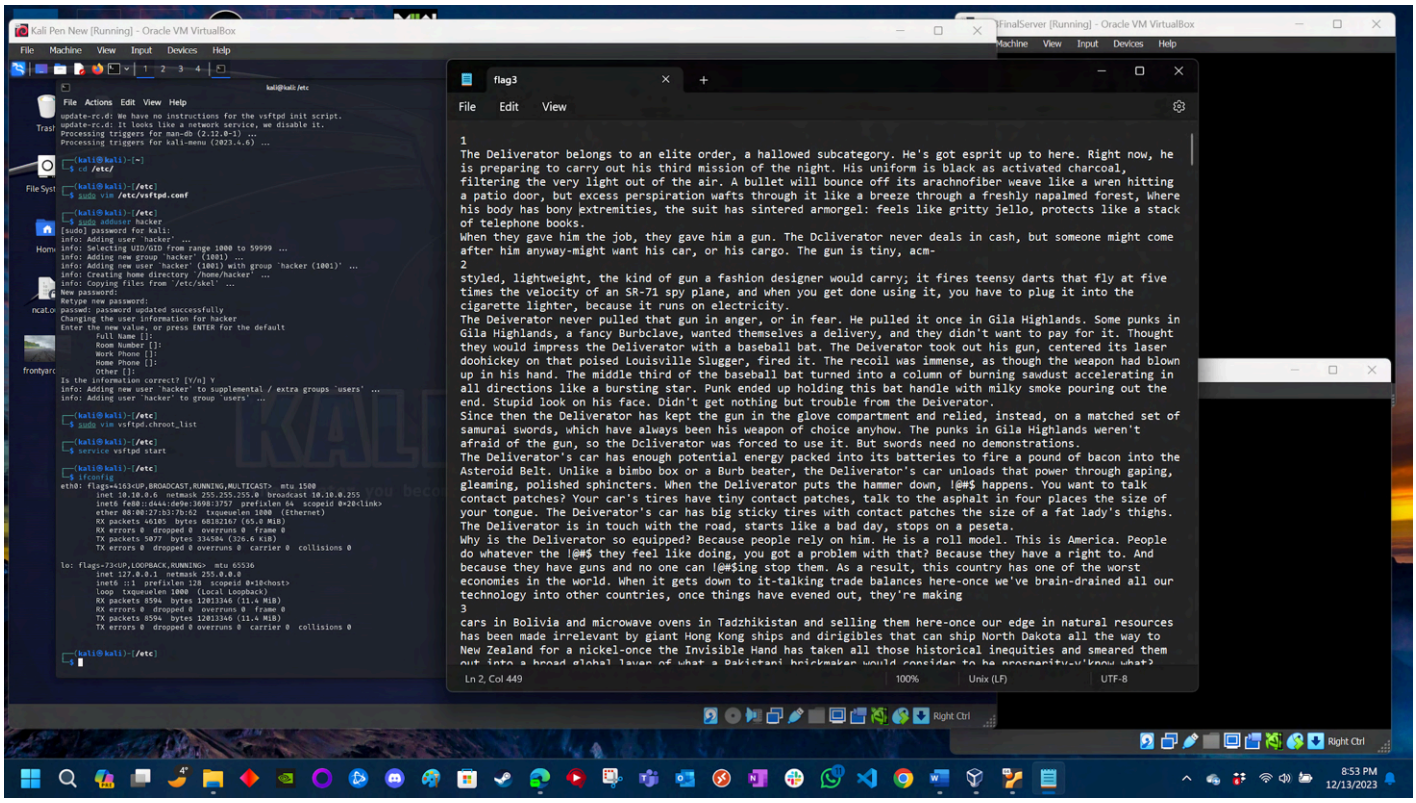
FLAG 2:
flag2{authorized_user_access}


Kali Pen New [Running] - Oracle VM VirtualBox
6573FinalServer [Running] - Oracle VM VirtualBox
6573FinalClient [Running] - Oracle VM VirtualBox
NBN Corporation
10.10.0.66/internal/customers.php?list=..%2Fdata%2Fcustomer.list
Future Customers
FOR INTERNAL USE ONLY
flag2{authorized_user_access}
NqF5Rz@yahoo.com : connie //// long@gmail.com : capone //// hjk12345@hotmail.com :
ned //// snoogy@yahoo.com : frank //// polobear@yahoo.com : jess ////
mkgiy13@gmail.com : max //// tempbeauties@live.com : peterpiper ////
amohalko@gmail.com : desiree //// ramy43@gmail.com : greatone ////
dowjones@hotmail.com : stockman //// yahotmail@hotmail.com : eugene ////
hydro1@gmail.com : maurice //// boneman22@gmail.com : dennis ////
hamlin@hotmail.com : willie //// nevirts@gmail.com : jackie //// redtop@live.com :
camille //// langp@hotmail.com : pontoosh //// jnardi@live.com : peter ////
4degrees@hotmail.com : ralph //// fretteaser@hotmail.com : derek ////
bsquard@live.com : wilbur //// zd0ns23@live.com : wrinkle //// scheefca@live.com :
gerry //// enobrac@gmail.com : marcy //// saazuhl1273@gmail.com : cauhuln ////
fwe315@live.com : evan //// wilson@gmail.com : triad //// navresbo@yahoo.com :
heather //// XO6Pn75pjjK@yahoo.com : sandy //// darkness024@yahoo.com : randy ////
jjstrokes@live.com : beansko //// zimago@yahoo.com : george //// katrina@gmail.com :
harald //// awesome@gmail.com : larry //// jess@yahoo.com : jesse ////
FOR INTERNAL USE ONLY
NBN Corporation
We are Always Watching Them
Right Ctrl
6:06 AM
12/15/2023

FLAG 3:


Kali Pen New [Running] - Oracle VM VirtualBox
WinDev2311Eval [Running] - Oracle VM VirtualBox
6573FinalServer [Running] - Oracle VM VirtualBox


Kali Pen New [Running] - Oracle VM VirtualBox
6573FinalServer [Running] - Oracle VM VirtualBox
6573FinalClient [Running] - Oracle VM VirtualBox
NBN
Near-Earth Broadcast Network
Someone is Always Watching


Kali Pen New [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
flag3
File Edit View
1
The Deliverator belongs to an elite order, a hallowed subcategory. He's got esprit up to here. Right now, he is preparing to carry out his third mission of the night. His uniform is black as activated charcoal, filtering the very light out of the air. A bullet will bounce off its arachnofiber weave like a wren hitting a patio door, but excess perspiration wafts through it like a breeze through a freshly napalmed forest, Where his body has bony extremities, the suit has sintered armorgel: feels like gritty jello, protects like a stack of telephone books.
When they gave him the job, they gave him a gun. The Dcliverator never deals in cash, but someone might come after him anyway-might want his car, or his cargo. The gun is tiny, acm-
2
styled, lightweight, the kind of gun a fashion designer would carry; it fires teensy darts that fly at five times the velocity of an SR-71 spy plane, and when you get done using it, you have to plug it into the cigarette lighter, because it runs on electricity.
The Deiverator never pulled that gun in anger, or in fear. He pulled it once in Gila Highlands. Some punks in Gila Highlands, a fancy Burbclave, wanted themselves a delivery, and they didn't want to pay for it. Thought they would impress the Deliverator with a baseball bat. The Deiverator took out his gun, centered its laser doohickey on that poised Louisville Slugger, fired it. The recoil was immense, as though the weapon had blown up in his hand. The middle third of the baseball bat turned into a column of burning sawdust accelerating in all directions like a bursting star. Punk ended up holding this bat handle with milky smoke pouring out the end. Stupid look on his face. Didn't get nothing but trouble from the Deiverator.
Since then the Deliverator has kept the gun in the glove compartment and relied, instead, on a matched set of samurai swords, which have always been his weapon of choice anyhow. The punks in Gila Highlands weren't afraid of the gun, so the Dcliverator was forced to use it. But swords need no demonstrations.
The Deliverator's car has enough potential energy packed into its batteries to fire a pound of bacon into the Asteroid Belt. Unlike a bimbo box or a Burb beater, the Deliverator's car unloads that power through gaping, gleaming, polished sphincters. When the Deliverator puts the hammer down, !@#$ happens. You want to talk contact patches? Your car's tires have tiny contact patches, talk to the asphalt in four places the size of your tongue. The Deiverator's car has big sticky tires with contact patches the size of a fat lady's thighs.
The Deliverator is in touch with the road, starts like a bad day, stops on a peseta.
Why is the Deliverator so equipped? Because people rely on him. He is a roll model. This is America. People do whatever the !@#$ they feel like doing, you got a problem with that? Because they have a right to. And because they have guns and no one can !@#$ing stop them. As a result, this country has one of the worst economies in the world. When it gets down to it-talking trade balances here-once we've brain-drained all our technology into other countries, once things have evened out, they're making
3
cars in Bolivia and microwave ovens in Tadzhikistan and selling them here-once our edge in natural resources has been made irrelevant by giant Hong Kong ships and dirigibles that can ship North Dakota all the way to New Zealand for a nickel-once the Invisible Hand has taken all those historical inequities and smeared them
Ln 2, Col 449
100%
Unix (LF)
UTF-8
Right Ctrl
8:53 PM
12/13/2023