SECURITY MAXIMALE

PENTESTING

# Penetration Testing Plan for Near-Earth Broadcast Network (NBN)

**Customer:**
NBN
2024-05-06
v0.0

**Contact:**
Yanyan Gao
2063518385
yg3099@nyu.edu

# Table of Contents

# Executive Summary

During the penetration testing conducted by Security Maximale GmbH, several vulnerabilities were identified across the target environment. The vulnerabilities were classified into different criticality levels, ranging from High to Info, indicating varying degrees of risk and potential impact on the security posture of the systems.

Founds:

1. one admin user and password;
2. one root shell;
3. client username and password
4. four flags;

The most critical vulnerability discovered was a Linux Privilege Escalation issue with a severity rating of High (8.0). This vulnerability allowed unprivileged users with UID > INT_MAX to escalate privileges and execute arbitrary systemctl commands, potentially leading to unauthorized access and system compromise.

Additionally, two Medium-level vulnerabilities were identified: Administrative credentials stored in cache memory and User Enumeration. The former posed a risk of retrieving administrative credentials from the system's cache memory, while the latter exposed the web application to user enumeration attacks, providing attackers with valuable information for follow-up attacks such as brute force or credential stuffing.

Furthermore, two Low-level vulnerabilities were found: Cracked weak credentials and FTP Anonymous Authentication. The former highlighted the risk of unauthorized access due to insufficient data validation and the low complexity of stored hashes, while the latter exposed the FTP service to potential attacks such as directory traversal, cross-site scripting, and brute force.

It is recommended that the identified vulnerabilities be addressed promptly to mitigate potential security risks and strengthen the overall security posture of the systems. Security measures such as patching vulnerable systems, implementing proper access controls, and conducting regular security assessments are recommended to prevent future exploitation and ensure the protection of sensitive information.

# Methodology and Scope

**Methodology and Scope:**

NBN has entrusted the consultant with two system images, referred to as "Targets," to be utilized at the onset of the penetration testing endeavor. These images encompass a comprehensive compilation of prevalent NBN applications and services. The examination scope will be strictly confined to these two designated images, with no testing permitted against any operational NBN systems. It is imperative to note that the targets must be deployed on systems provided by the Consultant for testing purposes exclusively. All testing endeavors are to be conducted remotely over the network, simulating the actions of an external adversary. The targets possess no local access, except for the initial setup. Any report incorporating vulnerabilities unearthed through local access to the machines would contravene the terms of this agreement, rendering the deliverables null and void.

**Penetration Test Target Details:**

1. NBN Server ("6573FinalServer.ova"): This server instance represents a developmental build of a cloud image intended for deployment. It serves as a platform for customer online account access and facilitates employee customer service interactions.
2. NBN Client ("6573FinalClient.ova"): The client workstation serves as a developmental build of an employee workstation. It is utilized by employees to access the server or execute other NBN customer service functions.

**Detailed Scope of Work:**

- Network Pen Testing: This segment entails the enumeration and evaluation of all external-facing hosts and services.
- Web App Pen Testing: Comprehensive assessment and testing of all external-facing web applications.
- Internal Pen Test: In the event that internal network access is attained, the assessment will continue to unearth additional vulnerabilities and ascertain potential impacts.
- Sensitive Data: The provided developmental images exclusively contain unclassified test data. The task involves identifying any insecurely stored sensitive information. Additionally, hidden "flags" representing sensitive data are dispersed throughout the targets, with the expectation to enumerate and document all discoveries. Furthermore, the cracking of any password hashes uncovered during the assessment is deemed essential.
- Out of Scope: Distributed Denial of Service (DDoS) attacks are explicitly excluded from the scope. Similarly, local access to the machines, including logging into the VM console, or any activity necessitating physical access is strictly prohibited.
- Severity: NBN prioritizes the identification of security flaws with a "medium" or higher security impact. However, all vulnerabilities or weaknesses, regardless of severity, are welcomed. It is important to note that attacks compromising a single account are categorized as "low" severity. Moreover, information-only findings, recommended best practices, and theoretical-only exploits fall under the "low" severity classification.
- Other Pen Testing: Apart from the delineated out-of-scope activities, the assessment extends to evaluating and scrutinizing any other available elements for potential security implications.

# Vulnerability Overview

In the course of this penetration test **1 High**, **2 Medium**, **2 Low** and **1 Info** vulnerabilities were identified:

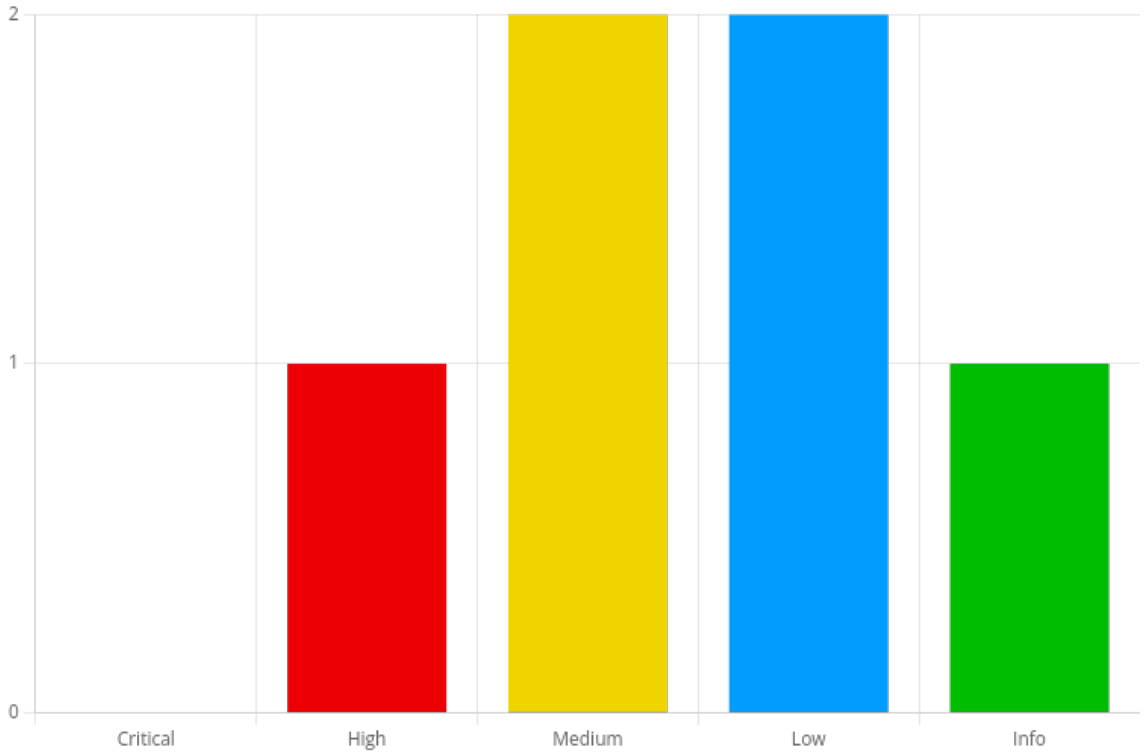



**Figure 1 - Distribution of identified vulnerabilities**

A tabular overview of all vulnerabilities identified:

| Vulnerability | Criticality |
|---|---|
| Linux Privilege Escalation | High |
| Administrative/client credentials stored in cache memory | Medium |
| User Enumeration | Medium |
| Cracked weak credentials | Low |
| FTP Anonymous Authentication | Low |
| Appendix | Info |

A list of all vulnerabilities including a brief description:

### 1. Linux Privilege Escalation (High: 8.0)

Affects: root
Some Linux versions were affected by a bug that allows users with UID > INT_MAX to escalate privileges. unprivileged users with UID > INT_MAX can successfully execute any systemctl command.

### 2. Administrative/client credentials stored in cache memory (Medium: 5.3)

It is possible to retrieve administrative credentials from the systems cache memory. Impact: Obtain functional credentials for privileged users.

### 3. User Enumeration (Medium: 5.3)

The web application was vulnerable to a user enumeration vulnerability. User enumeration is a common vulnerability in web applications that occurs when an attacker can use brute force techniques to determine valid user accounts in a system. Although user enumeration is a low risk in itself, it still provides an attacker with valuable information for follow-up attacks such as in brute force and credential stuffing attacks or in social engineering campaigns.

### 4. Cracked weak credentials (Low: 3.4)

Affects: Unauthorized access, or even the insufficient data validation can make the system vulnerable.
The low complexity of the hashes stored in the database considerably reduces the amount of time required to crack them. **Threat:** Authenticated attacker from the Internet with access to the hashes.

### 5. FTP Anonymous Authentication (Low: 3.4)

Affects:

- Directory Traversal Attack
- Cross-Site Scripting (XSS)
- Brute Force Attack
- Buffer Overflow
- Remote
- Local

FTP (File Transfer Protocol) is a service or so-called protocol for transferring files between computers via the Transmission Control Protocol / Internet Protocol (TCP / IP). It is considered as an Application Layer Protocol

FTP Anonymous Authentication -This Vulnerability is caused by system administrators misconfiguring FTP, and it doesn't require any specific version or application to exploit.

### 6. Appendix (Info: 0.0)

Founds: 4 flags; one admin user and password; one root shell; client username and password

# Vulnerability Details

## 1. Linux Privilege Escalation

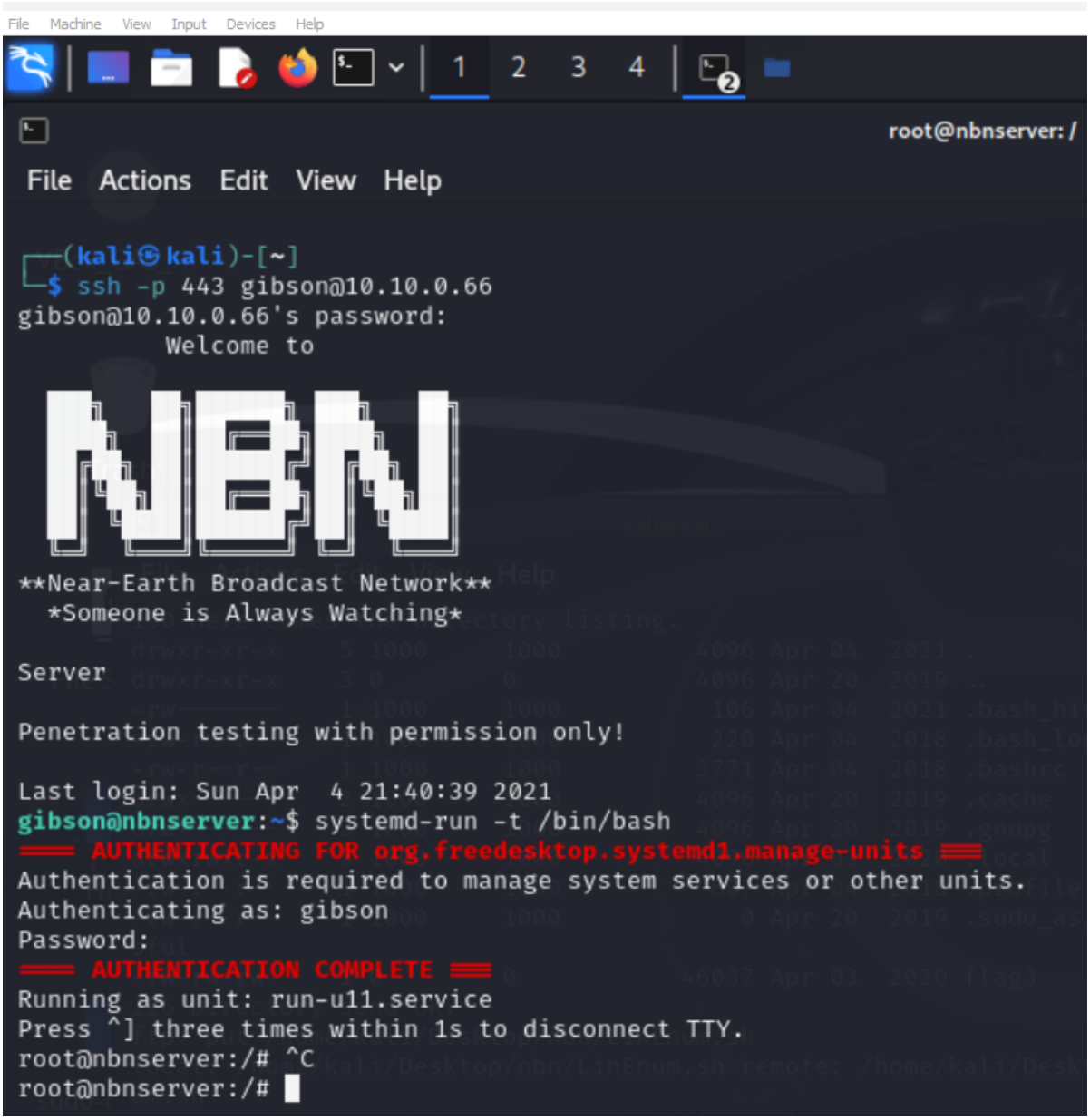
**Remediation Status:**
**Criticality:** High
**CVSS-Score:** 8.0
**Affects:** root

### Overview

Some Linux versions were affected by a bug that allows users with UID > INT_MAX to escalate privileges. unprivileged users with UID > INT_MAX can successfully execute any systemctl command.

### Description

gibson@nbnserver:~$ systemd-run -t /bin/bash




## Recommendation

- Patch and Update: Ensure that all affected Linux systems are promptly patched with the latest security updates provided by the respective Linux distribution vendors. These patches often include fixes for known vulnerabilities and security flaws, mitigating the risk of privilege escalation exploits.
- Implement User Privileges: Review and adjust user privileges and permissions to limit the ability of unprivileged users to execute systemctl commands. Consider implementing the principle of least privilege, granting users only the permissions necessary for their designated tasks.
- Security Hardening: Implement additional security measures and hardening techniques to reinforce the security posture of Linux systems. This may include enabling mandatory access control (MAC) mechanisms such as SELinux or AppArmor, which can provide additional layers of protection against unauthorized privilege escalation attempts.

- User Input Validation: Enhance input validation mechanisms to prevent potential exploitation of vulnerabilities related to user input handling. Validate user-supplied data thoroughly to prevent malicious input from being processed or executed by systemctl commands.
- Monitoring and Logging: Implement comprehensive monitoring and logging solutions to detect and track suspicious activities, including unauthorized attempts to execute systemctl commands. Regularly review system logs for any indications of privilege escalation attempts or unusual user behavior.
- User Awareness and Training: Educate users and system administrators about the risks associated with privilege escalation vulnerabilities and the importance of adhering to security best practices. Provide training on secure system configuration, user management, and incident response procedures to mitigate potential security risks effectively.
- Regular Security Assessments: Conduct regular security assessments, including penetration testing and vulnerability assessments, to identify and remediate security weaknesses proactively. Continuously monitor for new vulnerabilities and emerging threats, ensuring that systems remain protected against evolving security risks.

# 2. Administrative/client credentials stored in cache memory

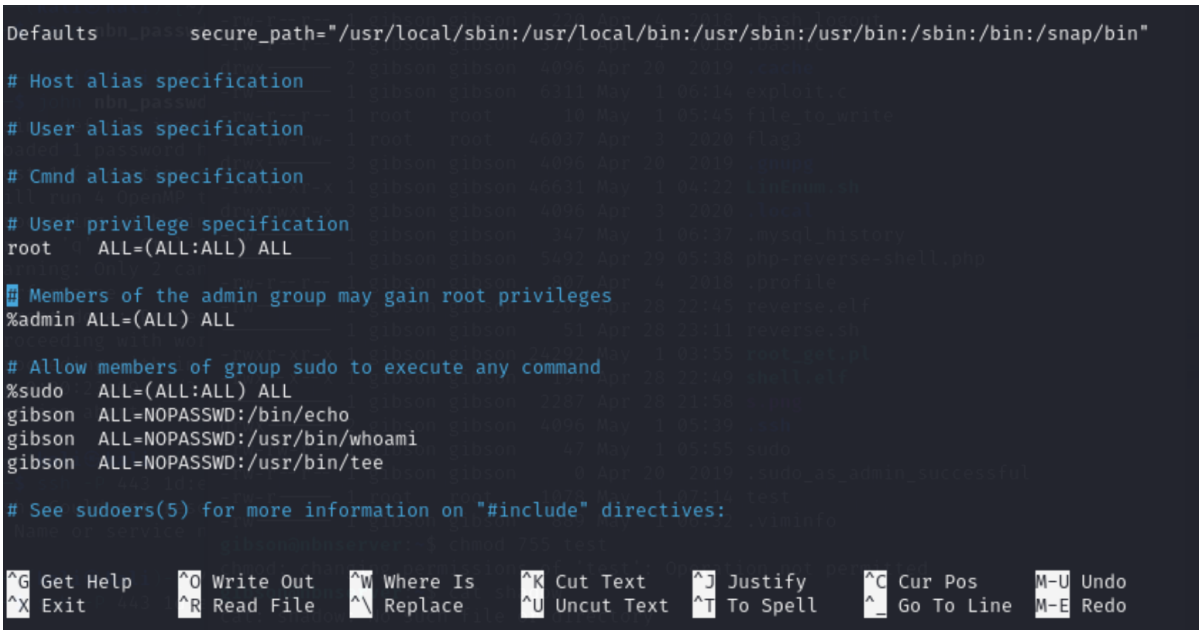
**Remediation Status:**
**Criticality:** Medium
**CVSS-Score:** 5.3

## Overview

It is possible to retrieve administrative credentials from the systems cache memory. Impact: Obtain functional credentials for privileged users.

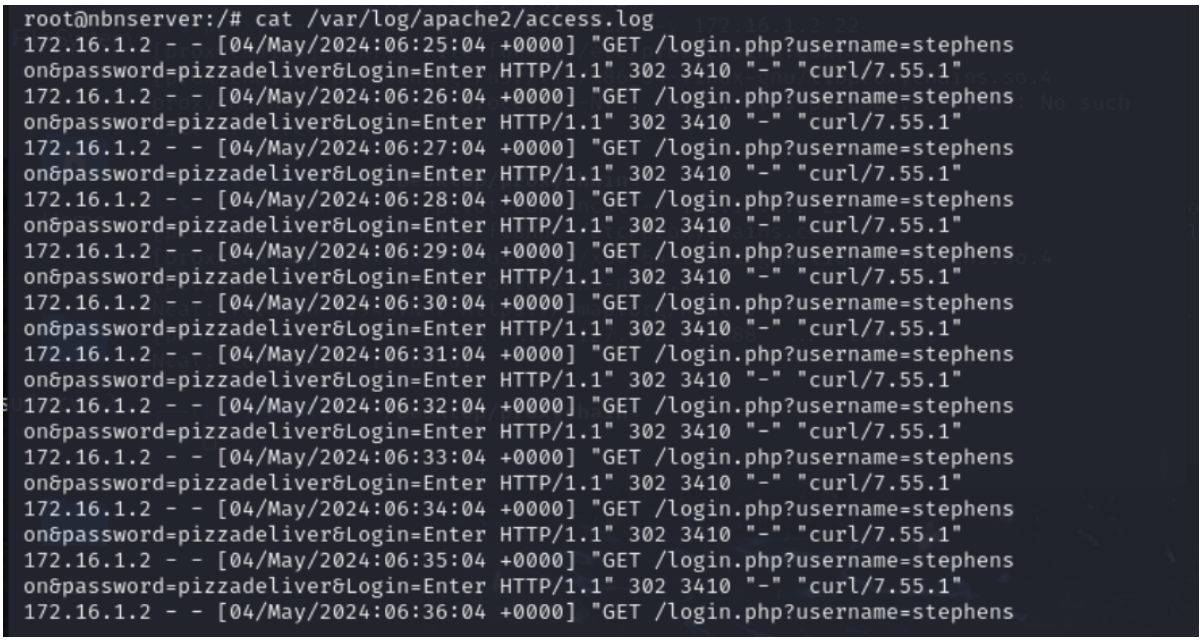
## Description

**We can increase Gibson's privilege as root by modifying the sudoers file, and also add other users and give them the root privilege.**

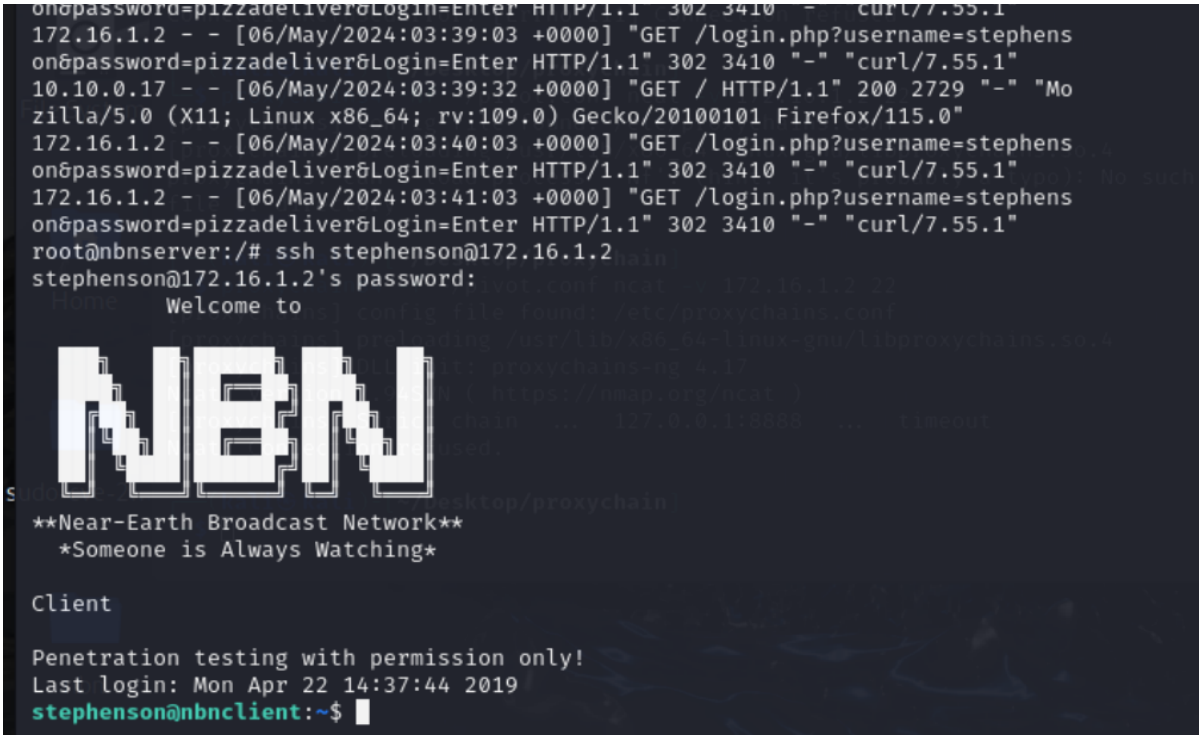



**I found that CEO.gibson,jpg, customer.list, stephenson.jpg file in /var/www/html/data, it provides me more information for the client exploitations.**


**I found client username and password in apache access log:**




**I use ssh login in client account:**




## Recommendation

Avoid the store of sensitive information in temporary files or cache.

# 3. User Enumeration

**Remediation Status:**
**Criticality:** Medium
**CVSS-Score:** 5.3
**Recommendation:** Identify all application attack surfaces relevant to User Enumeration and ensures that the web application always returns generic error messages when invalid credentials are entered.

## Overview

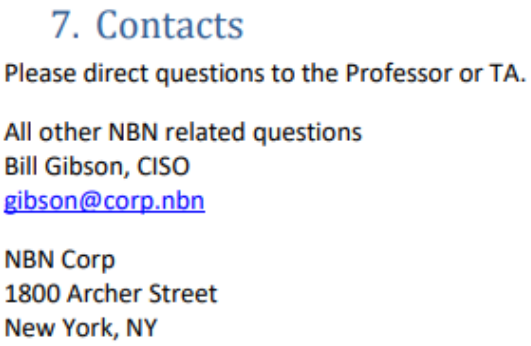
The web application was vulnerable to a user enumeration vulnerability. User enumeration is a common vulnerability in web applications that occurs when an attacker can use brute force techniques to determine valid user accounts in a system. Although user enumeration is a low risk in itself, it still provides an attacker with valuable information for follow-up attacks such as in brute force and credential stuffing attacks or in social engineering campaigns.

## Description

We were able to identify a user enumeration vulnerability in the web application, allowing us to determine valid user accounts using brute force techniques.

I found the user gibson from the contact information in the contracts, and then I use it for hydra password brute force, and got his login password.

Info in contract:



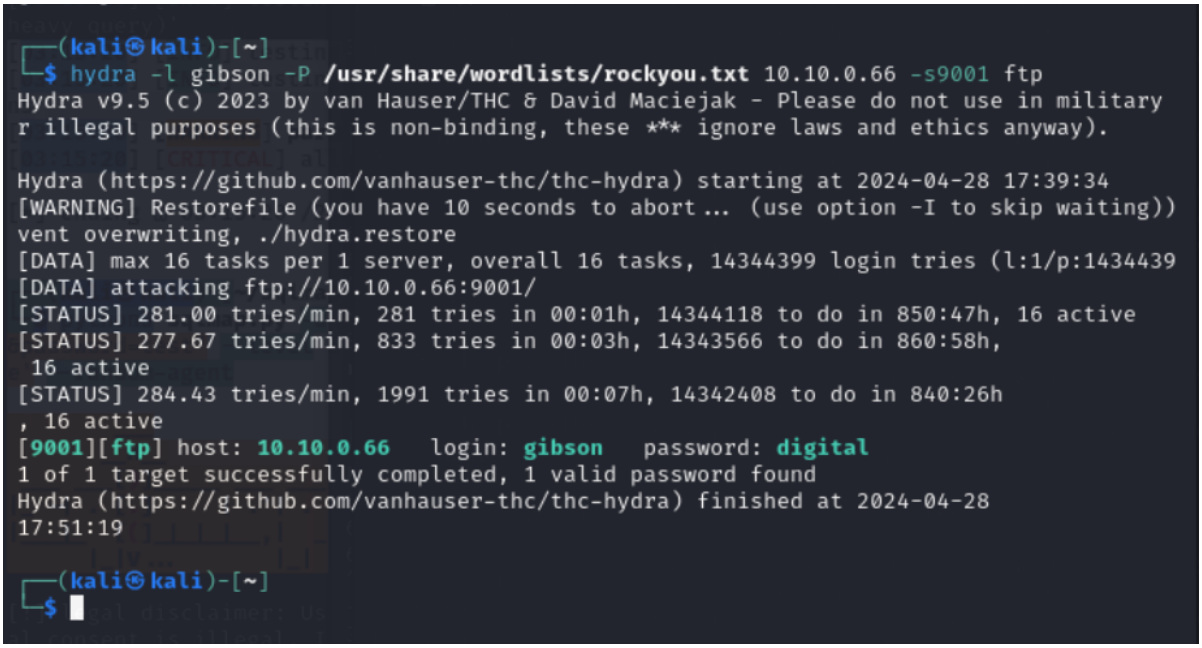
7. Contacts

Please direct questions to the Professor or TA.

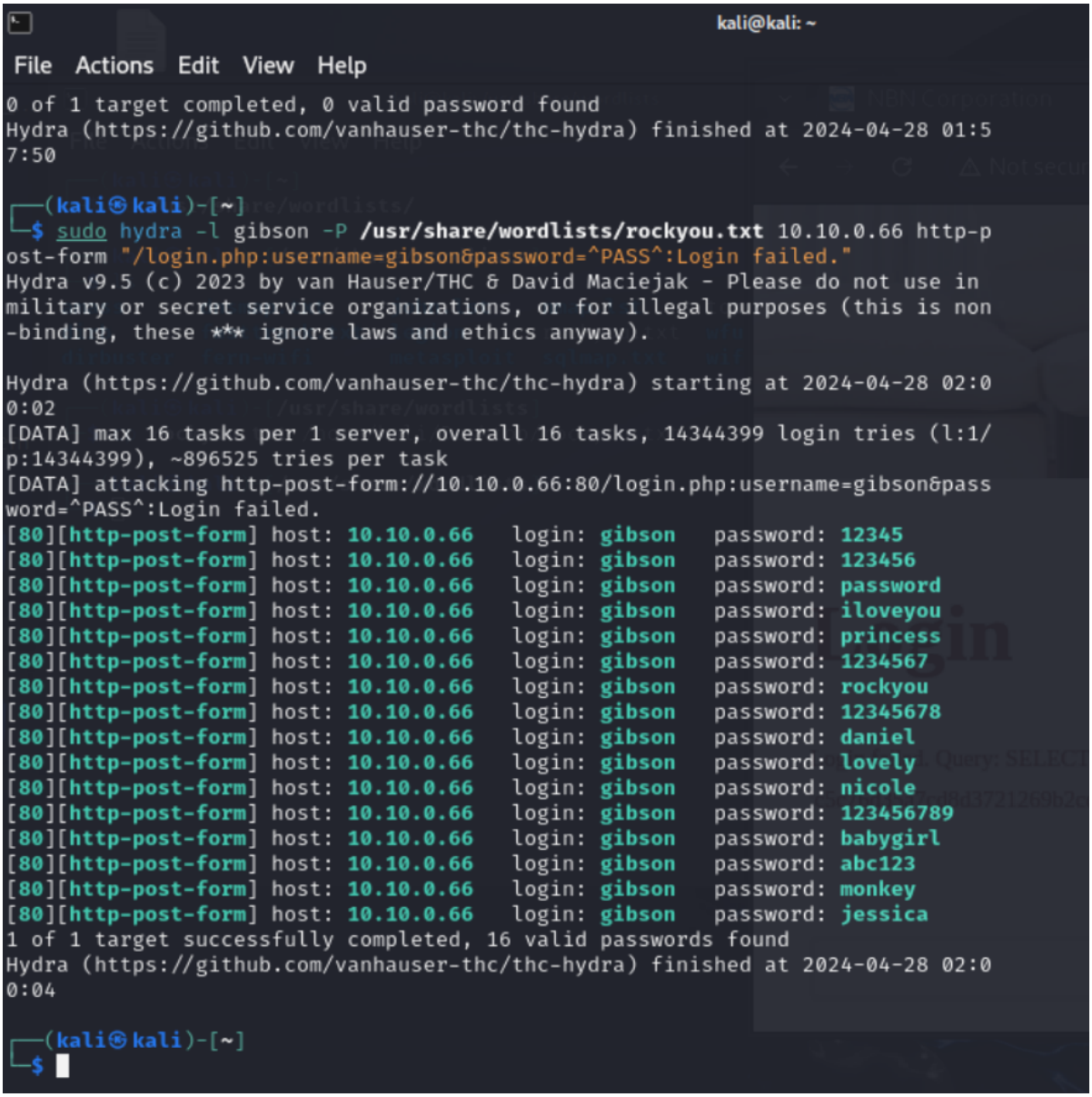
All other NBN related questions
Bill Gibson, CISO
gibson@corp.nbn

NBN Corp
1800 Archer Street
New York, NY

Brute force gibson's password: digital




I also found some inactive passwords:




Often, as a result of a faulty configuration or design decision, web applications indicate when a user already exists in the system. Two of the most common areas where this occurs are the login page or the "forgot password" feature of a web application. One example is when a user enters incorrect credentials, they receive information that the password they entered was incorrect. The information obtained can now be used by an attacker to determine whether or not a particular username already exists. By trial and error, an attacker can use it to determine a list of valid usernames.

Once an attacker has such a list, they can address these user accounts in new attacks to obtain valid credentials. In its simplest form, an attacker could perform a brute force attack. In this, an attacker tries to guess a user account's credentials by automatically trying through passwords. Often very large word lists containing frequently used passwords are used for this purpose. An attacker could also use determined usernames to search past data leaks for passwords. Credentials from data leaks, consisting of pairs of usernames and passwords, can be reused by an attacker in an automated attack. This particular form of brute force

attack, is also known as credential stuffing. Alternatively, an attacker can use usernames in the course of social engineering campaigns to contact users directly.

## Recommendation

- Ensure that the web application always returns generic error messages when invalid usernames, passwords, or other credentials are entered. Identifies all relevant attack surfaces of the application for this purpose.
- If the application defines usernames itself, user enumeration can be effectively prevented. The prerequisite for this is that user names are randomly generated so that they cannot be guessed.
- The application can also use email addresses as usernames. If the username is not yet registered, an email message will contain a unique URL that can be used to complete the registration process. If the username exists, the user receives an email message with a URL to reset the password. In either case, an attacker cannot infer valid user accounts.
- As an additional security measure, you could delete default system accounts as well as test accounts or rename them before releasing the system to production.

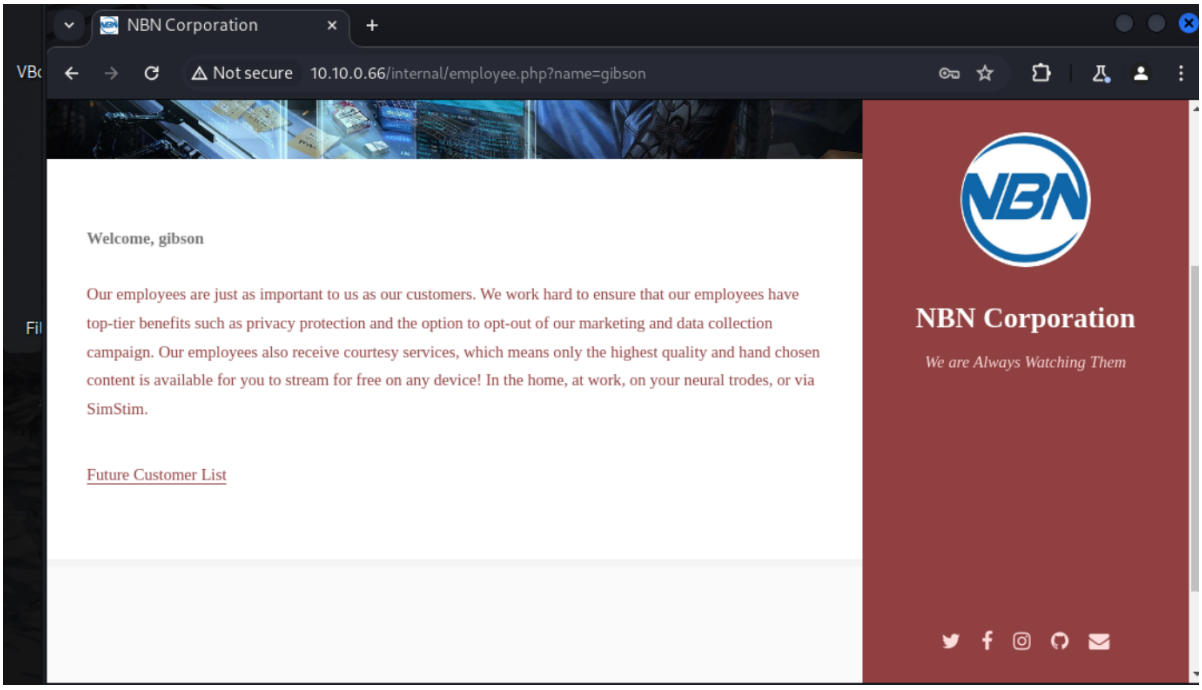
# 4. Cracked weak credentials

**Remediation Status:**
**Criticality:** Low
**CVSS-Score:** 3.4
**Affects:** Unauthorized access, or even the insufficient data validation can make the system vulnerable.

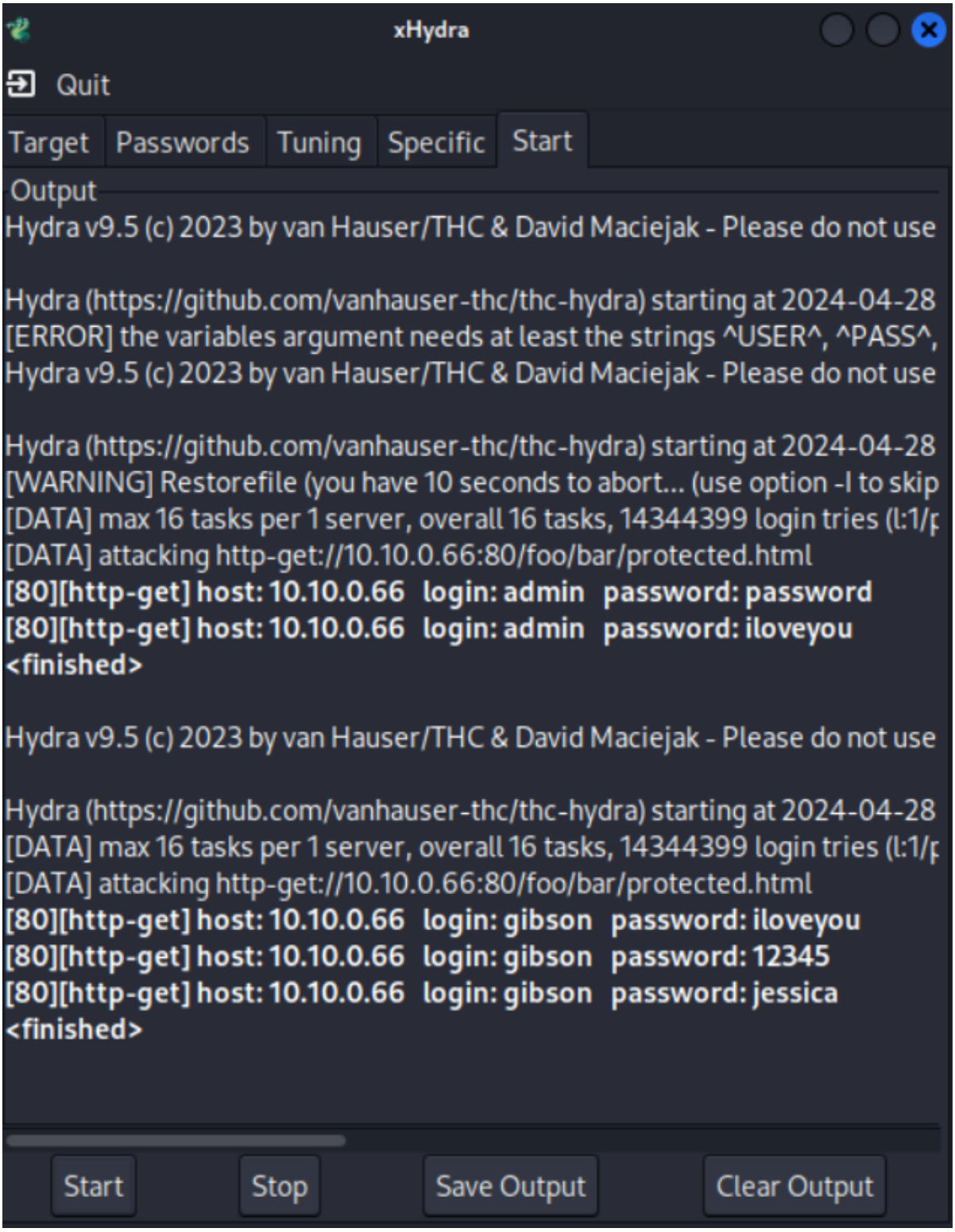
## Overview

The low complexity of the hashes stored in the database considerably reduces the amount of time required to crack them. **Threat:** Authenticated attacker from the Internet with access to the hashes.

## Description




The login session does not have a three-time unlocked-out mechanism, and the Same usernames may have the same passwords. Passwords may be weak and can be cracked using the Rockyou wordlist. All passwords came from Rockyou; there are no mangling rules.




It makes it easy for password brute force.

## Recommendation

Ensure that the functions of the password summary are 256 bits in size. MFA is also recommended to mitigate this vulnerability.

# 5. FTP Anonymous Authentication

**Remediation Status:**
**Criticality:** Low
**CVSS-Score:** 3.4
**Affects:**

- Directory Traversal Attack
- Cross-Site Scripting (XSS)
- Brute Force Attack
- Buffer Overflow
- Remote
- Local

## Overview

FTP (File Transfer Protocol) is a service or so-called protocol for transferring files between computers via the Transmission Control Protocol / Internet Protocol (TCP / IP). It is considered as an Application Layer Protocol

FTP Anonymous Authentication -This Vulnerability is caused by system administrators misconfiguring FTP, and it doesn't require any specific version or application to exploit.

## Description

Anonymous Exploitation Configuration

| **Attacker** | **Victim** | **VSFTPD (3.0.3)** |
|---|---|---|
| Kali Linux | NBNserver | Application |

Scanning As we can see in the result of nmap scan, Anonymous login is allowed.

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ nmap -sC -sV 10.10.0.66 -P 445 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 02:36 EDT
Nmap scan report for 10.10.0.66
Host is up (0.0029s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: NBN Corporation
|_http-server-header: Apache/2.4.29 (Ubuntu)
|8001/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_/internal/ /data/
443/tcp  open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1d:e1:40:6b:1c:a0:52:e5:97:6f:46:93:ba:ec:dd:8e (RSA)
|   256 75:6c:d6:39:ec:9b:0a:9a:87:e1:97:0e:a1:71:d4:77 (ECDSA)
|_  256 e0:fc:27:90:3a:c5:ab:f0:86:a5:99:49:a3:9f:2e:00 (ED25519)
8001/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_/internal/ /data/
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: NBN Corporation
9001/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.0.10
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    5 1000     1000         4096 Apr 04  2021 gibson
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 445 (0.0.1.189)
Host is up.int
All 1000 scanned ports on 445 (0.0.1.189) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

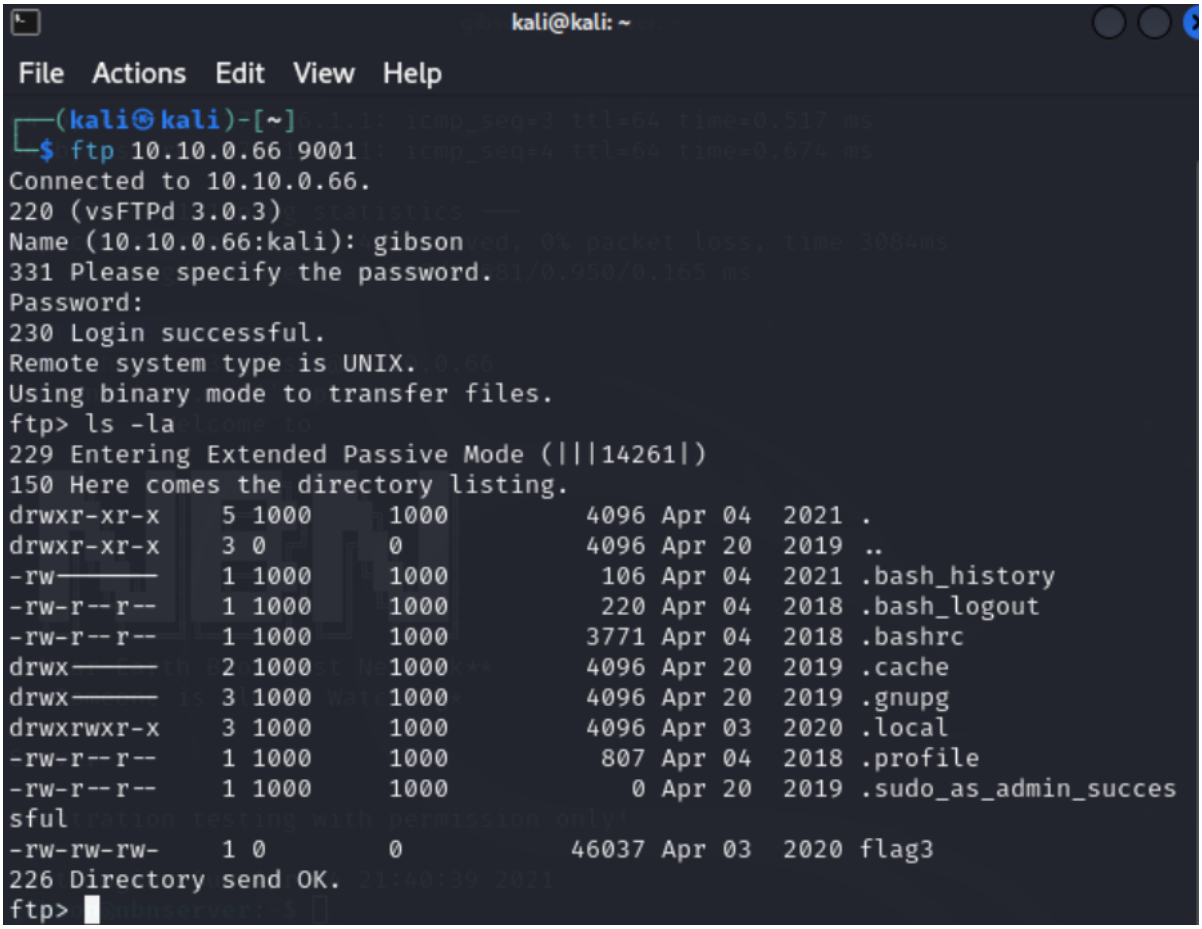
Exploitation For successful exploitation we will log in as anonymous user with blank password.

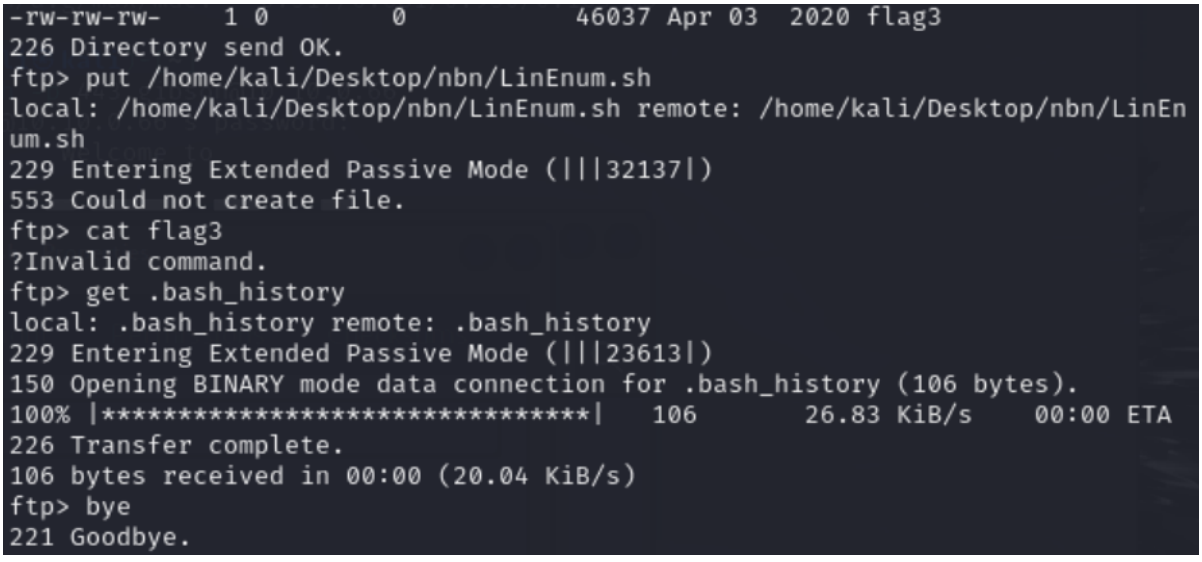
#ftp 10.0.0.66 #Name (10.0.0.66:root): anonymous #Password: Leave it Blank

```
┌──(kali㉿kali)-[~]
└─$ ftp anonymous@10.10.0.66 9001
Connected to 10.10.0.66.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password: admin
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||34831|)
150 Here comes the directory listing.
drwxr-xr-x    5 1000     1000         4096 Apr 04  2021 gibson
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||16493|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Apr 20  2019 .
drwxr-xr-x    3 0        0            4096 Apr 20  2019 ..
drwxr-xr-x    5 1000     1000         4096 Apr 04  2021 gibson
226 Directory send OK.
ftp> whoiam
?Invalid command.
ftp> get gibson
local: gibson remote: gibson
229 Entering Extended Passive Mode (|||47955|)
550 Failed to open file.
ftp> nc -lvnp 7000
?Invalid command.
ftp> cd gibson
421 Timeout.
ftp> exit
```

As you can tell, we can also get to know that the user gibson's user id is 1000, which means he is the admin user. We can do hydra password brute force from here too.

After I got gibson's password, I can login ftp with his credentials and I can do Upload a file, Download a file, Delete a file, Rename a file, Move and copy files.




## Recommendation

When it comes to anonymous FTP, security should be a top priority. While there are benefits to enabling anonymous file transfers, it is important to implement best practices to protect your network from potential threats. From an administrative point of view, the first step is to ensure the FTP server is properly configured and secure. This includes setting up firewalls,

restricting access to the server, and regularly updating the software to address any vulnerabilities. Additionally, it is recommended to use ssl/TLS encryption to ensure that data is transmitted securely.

Anonymous FTP can be a useful tool for sharing files, but it poses significant security risks that need to be mitigated. By using encryption protocols, limiting anonymous access, using strong passwords, monitoring and logging FTP activity, and regularly updating your FTP software, you can help secure your files and prevent data breaches and cyber attacks.

## Additional Information

- https://medium.com/@kubotortech/pentesting-exploiting-ftp-cba8ec81968e
- https://fastercapital.com/content/Anonymous-FTP--Unveiling-the-Pros-and-Cons-of-Anonymous-File-Transfers.html

# 6. Appendix

**Remediation Status:**
**Criticality: Info**
**CVSS-Score: 0.0**

## Overview

Founds: 4 flags; one admin user and password; one root shell; client username and password

## Description

**| machine | ip | tool | | ------- | ------- | ------- | | server | 172.16.1.1/10.10.0.66 | namp |**

**10.10.0.66**

**Address**

- 10.10.0.66 (ipv4)
- 08:00:27:38:85:7B - Oracle VirtualBox virtual NIC (mac)

**Ports**

The 996 ports scanned but not shown below are in state: **closed**

- 996 ports replied with: **reset**

| Port | | State (toggle closed [0] \| filtered [0]) | Service | Reason | Product | Version | Extra info |
|---|---|---|---|---|---|---|---|
| 80 | tcp | open | http | syn-ack | Apache httpd | 2.4.29 | (Ubuntu) |
| 443 | tcp | open | ssh | syn-ack | OpenSSH | 7.6p1 Ubuntu 4ubuntu0.3 | Ubuntu Linux; protocol 2.0 |
| 8001 | tcp | open | http | syn-ack | Apache httpd | 2.4.29 | (Ubuntu) |
| 9001 | tcp | open | ftp | syn-ack | vsftpd | 3.0.3 | |

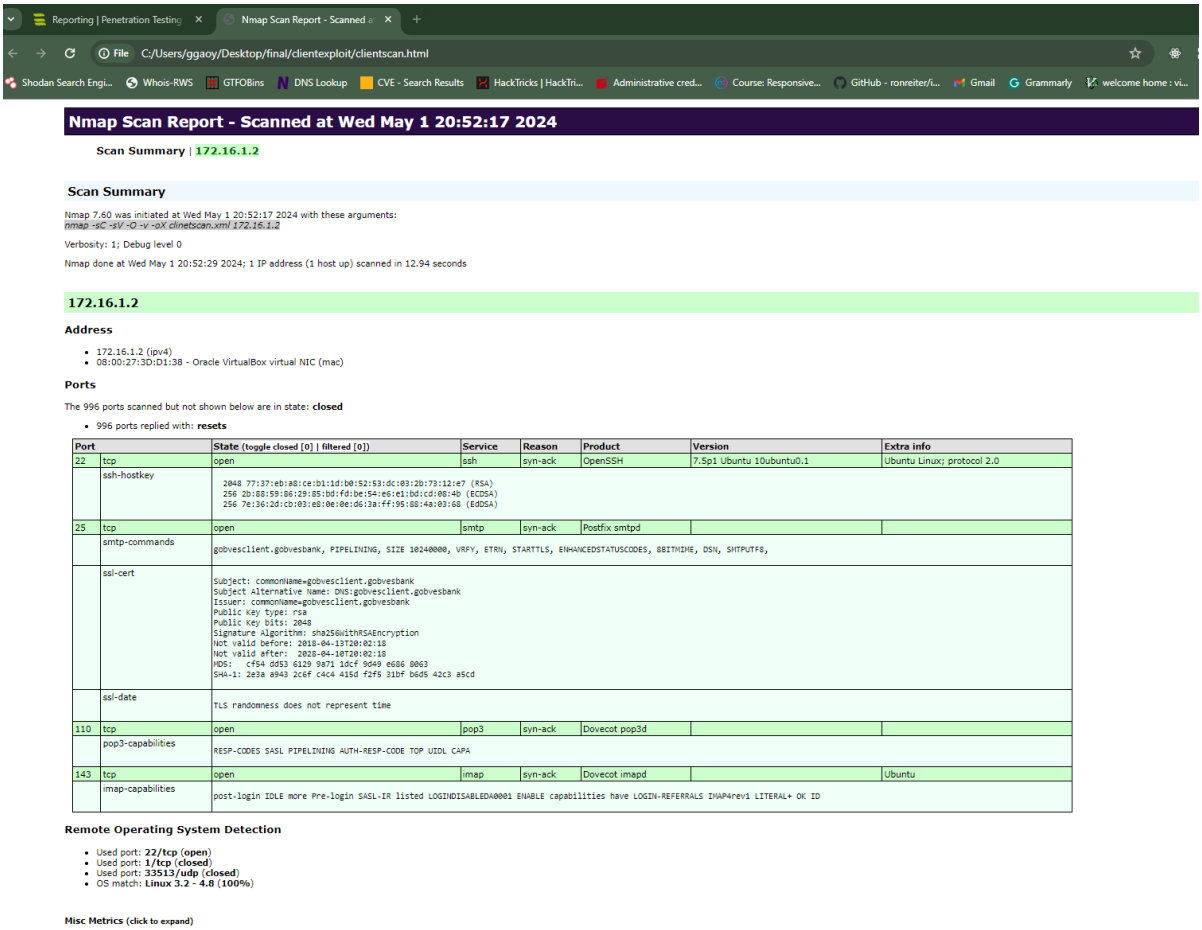
**Remote Operating System Detection**

- Used port: **80/tcp (open)**
- Used port: **1/tcp (closed)**
- Used port: **44770/udp (closed)**
- OS match: **Linux 3.2 - 4.9 (100%)**

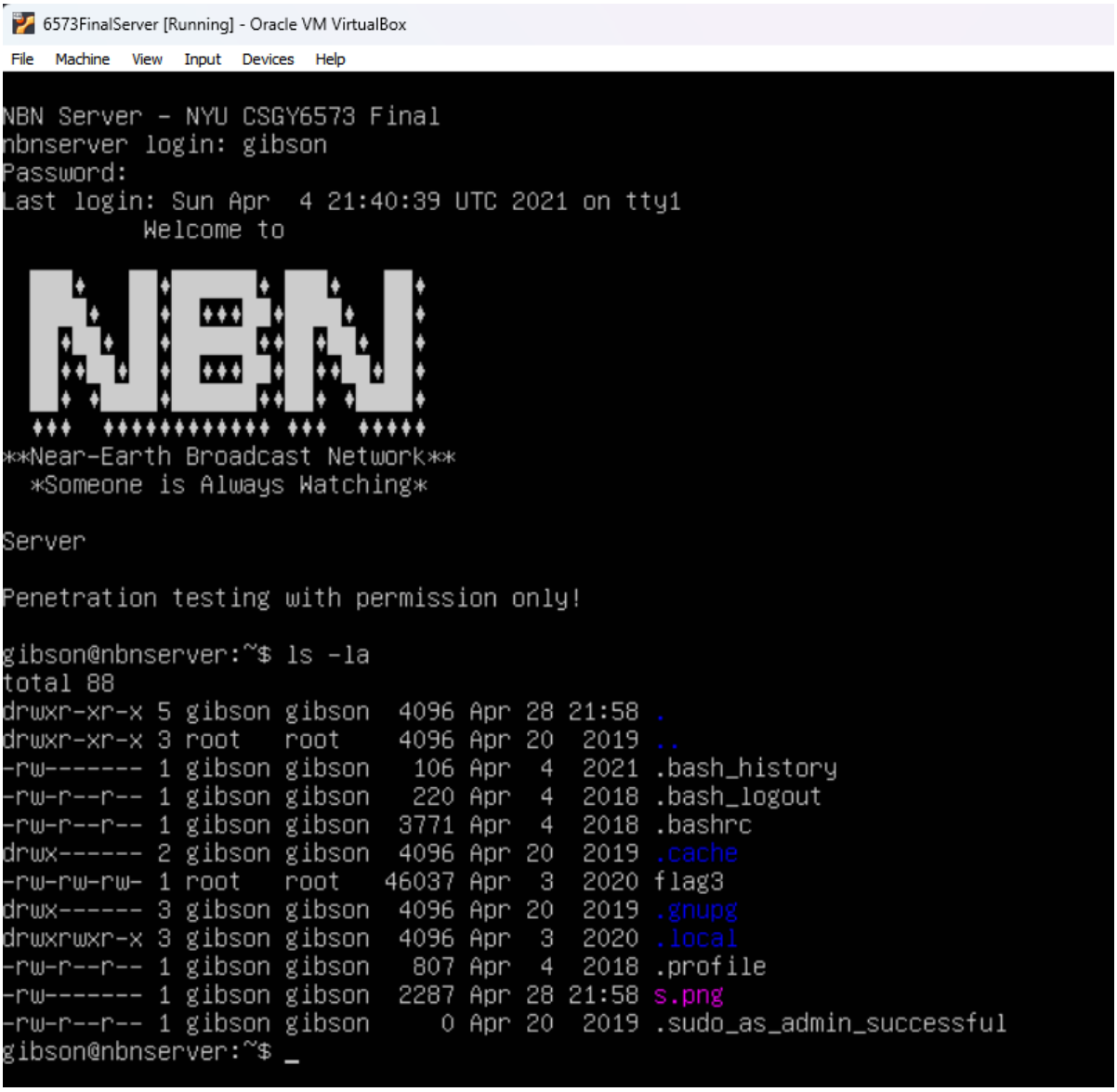
**Misc Metrics** (click to expand)

Go to top
Toggle Closed Ports
Toggle Filtered Ports

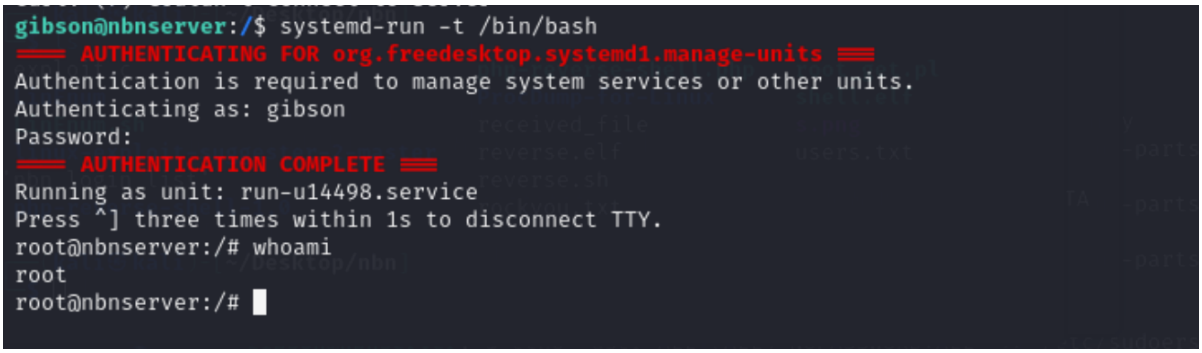
**| machine | ip | tool | | ------- | ------- | ------- | | client | 172.16.1.2 | namp && proxychains |**



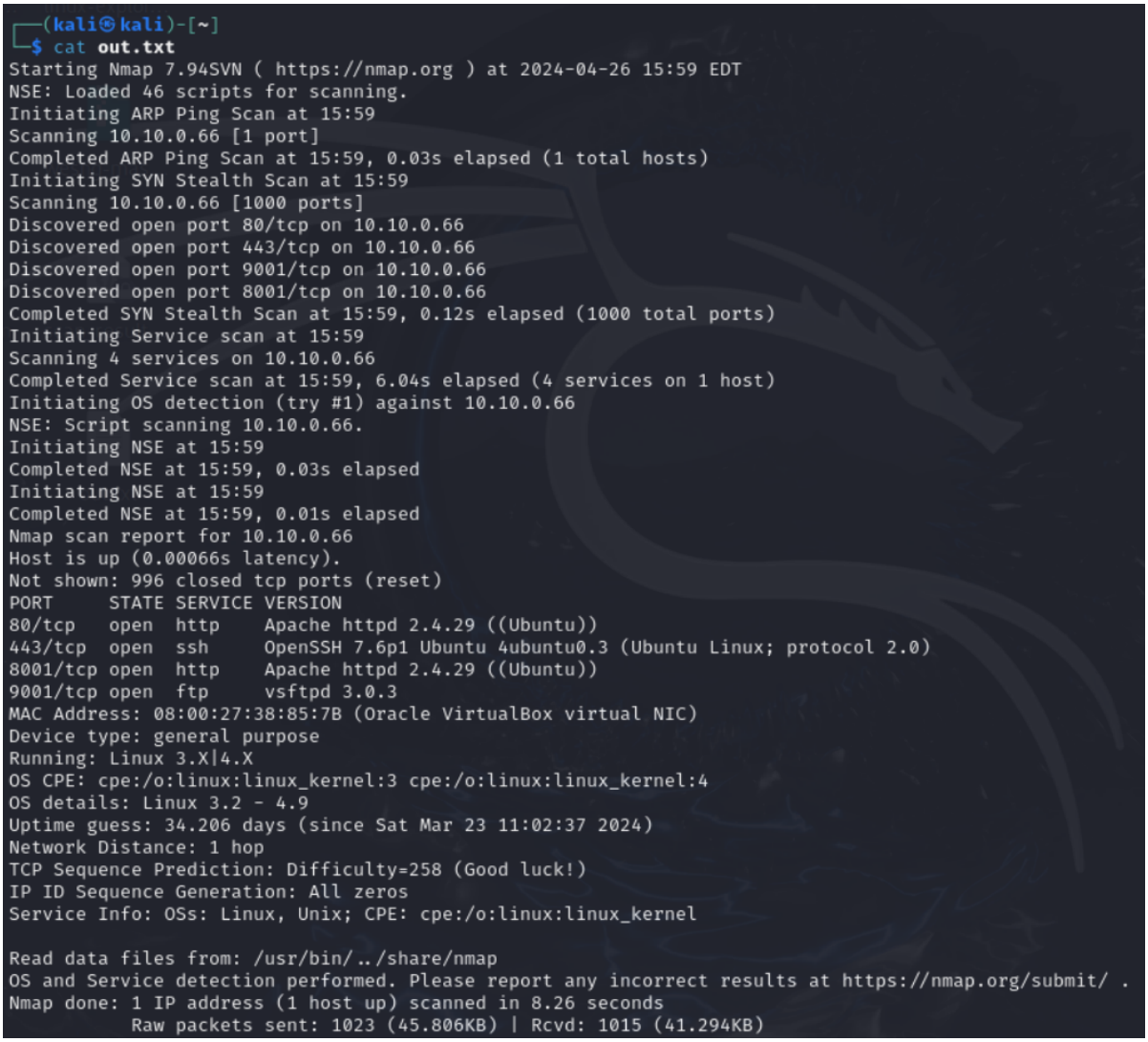

## Server shell login by gibson




**webserver privilege escalation **



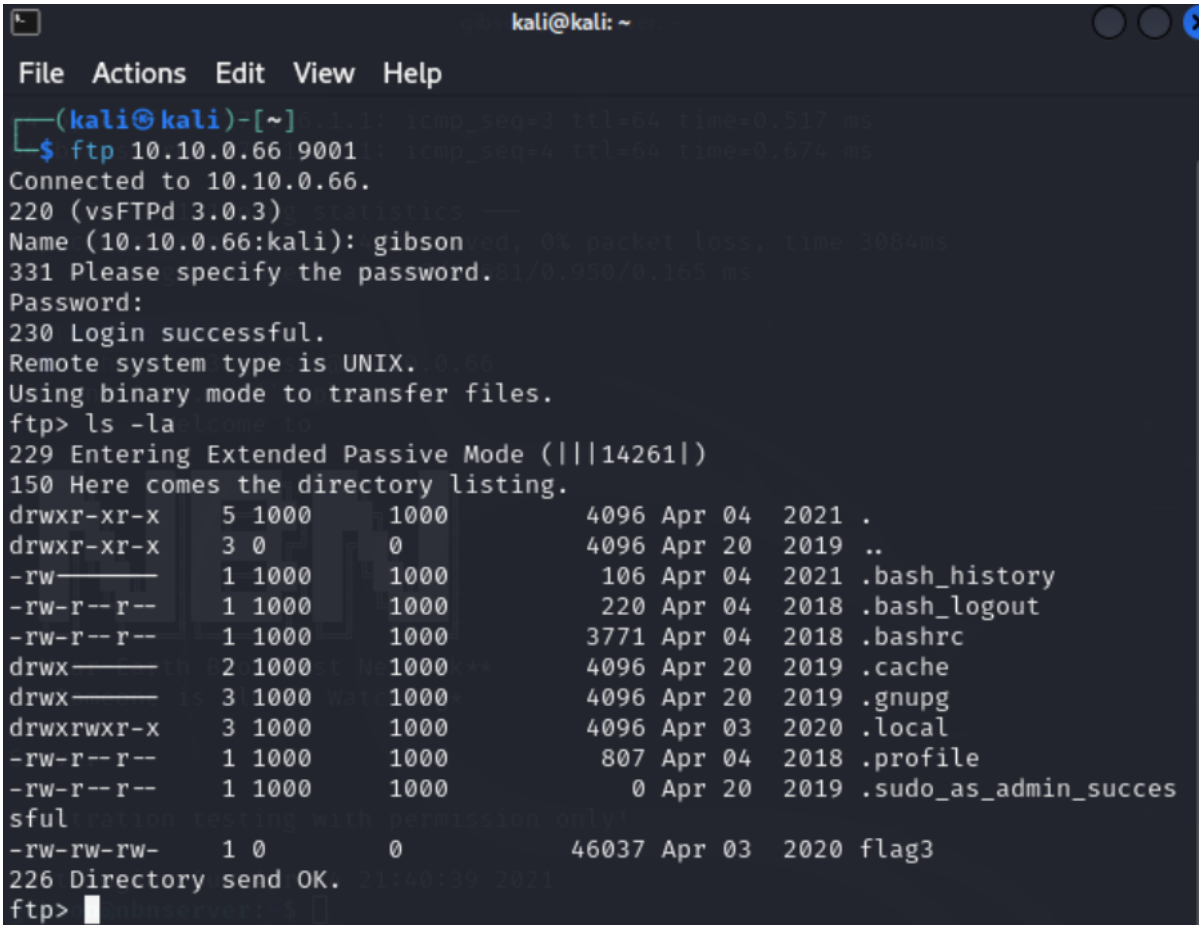

**nmap scan towards to webserver**



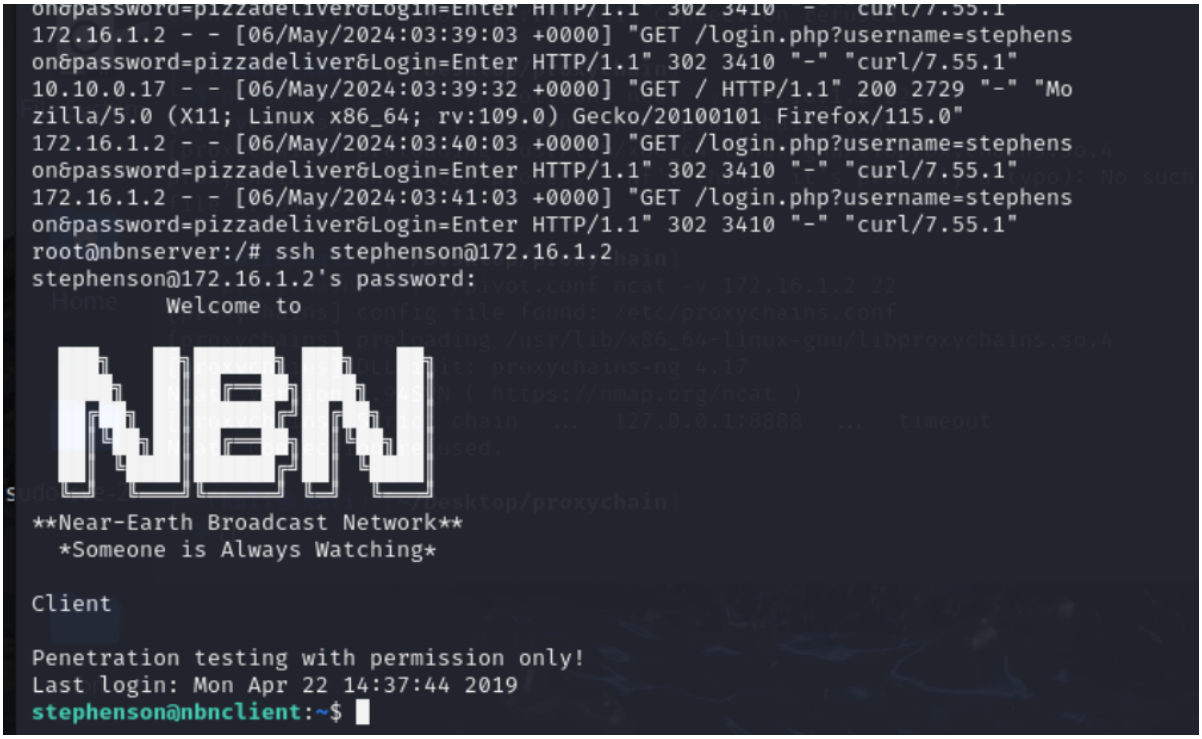
```
┌──(kali㉿kali)-[~]
└─$ cat out.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 15:59 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 15:59
Scanning 10.10.0.66 [1 port]
Completed ARP Ping Scan at 15:59, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 15:59
Scanning 10.10.0.66 [1000 ports]
Discovered open port 80/tcp on 10.10.0.66
Discovered open port 443/tcp on 10.10.0.66
Discovered open port 9001/tcp on 10.10.0.66
Discovered open port 8001/tcp on 10.10.0.66
Completed SYN Stealth Scan at 15:59, 0.12s elapsed (1000 total ports)
Initiating Service scan at 15:59
Scanning 4 services on 10.10.0.66
Completed Service scan at 15:59, 6.04s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 10.10.0.66
NSE: Script scanning 10.10.0.66.
Initiating NSE at 15:59
Completed NSE at 15:59, 0.03s elapsed
Initiating NSE at 15:59
Completed NSE at 15:59, 0.01s elapsed
Nmap scan report for 10.10.0.66
Host is up (0.00066s latency).
Not shown: 996 closed tcp ports (reset)
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
MAC Address: 08:00:27:38:85:7B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 34.206 days (since Sat Mar 23 11:02:37 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds
           Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.294KB)
```

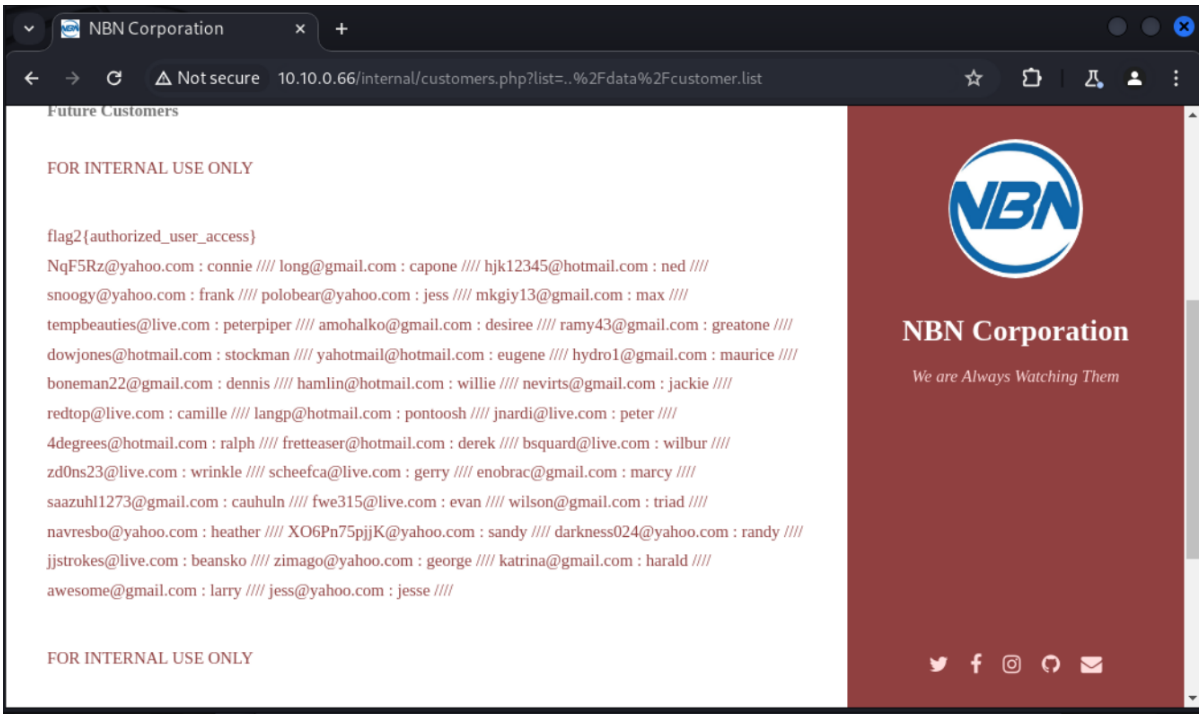
**ftp log**




**client login**

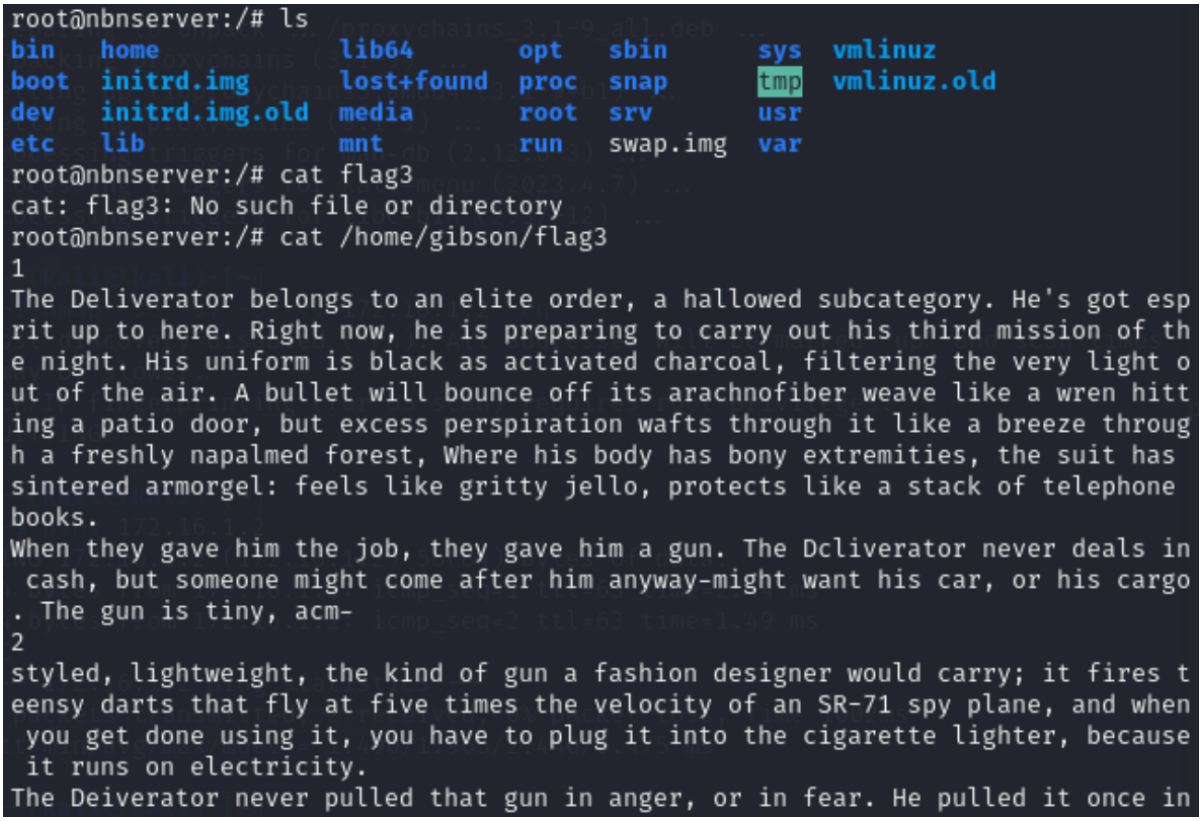


### internal customer and flag 2

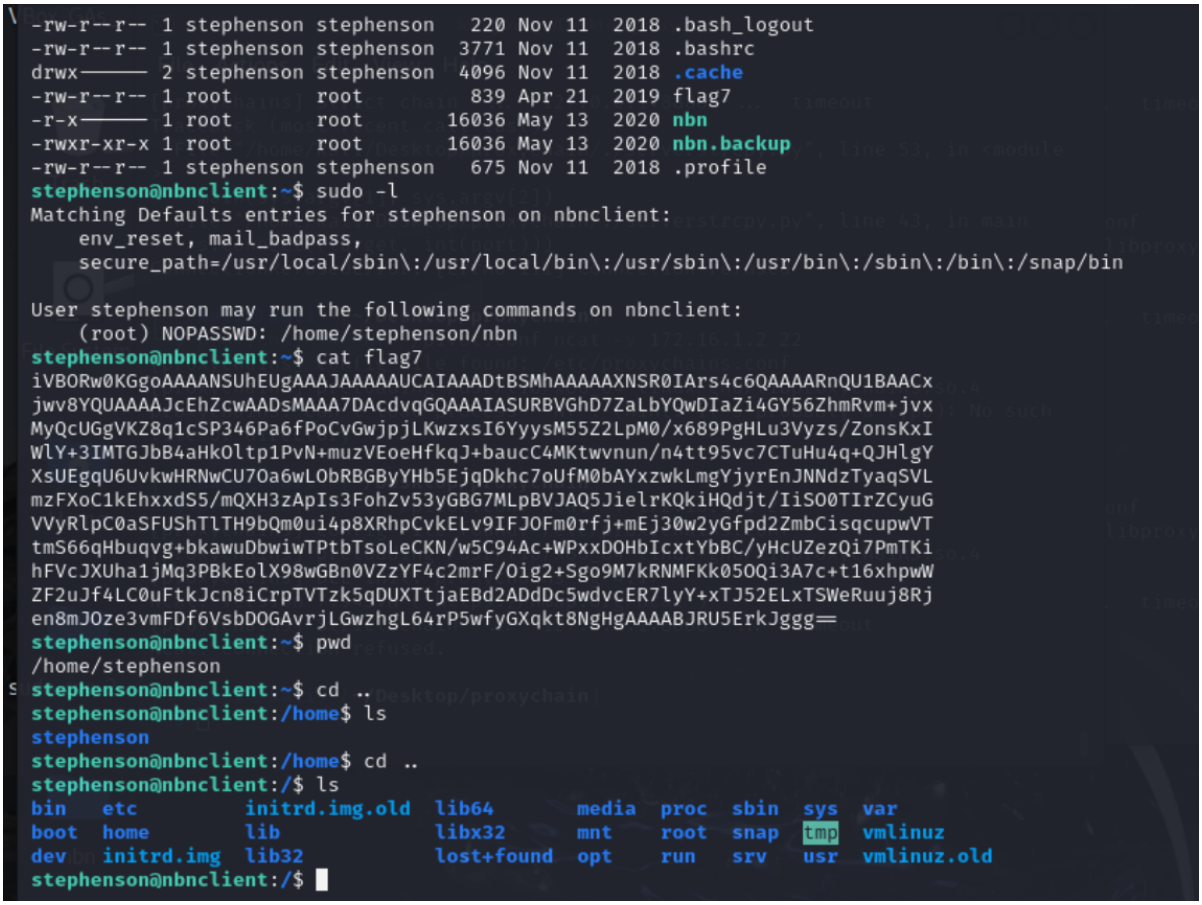



### flag 1


### flag 3


root@nbnserver:/# ls
bin home lib64 opt sbin sys vmlinuz
boot initrd.img lost+found proc snap tmp vmlinuz.old
dev initrd.img.old media root srv usr
etc lib mnt run swap.img var
root@nbnserver:/# cat flag3
cat: flag3: No such file or directory
root@nbnserver:/# cat /home/gibson/flag3
1
The Deliverator belongs to an elite order, a hallowed subcategory. He's got esp
rit up to here. Right now, he is preparing to carry out his third mission of th
e night. His uniform is black as activated charcoal, filtering the very light o
ut of the air. A bullet will bounce off its arachnofiber weave like a wren hitt
ing a patio door, but excess perspiration wafts through it like a breeze throug
h 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 t
eensy 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

**flag 7**




## Recommendation

I will continue to work on exploiting the client shell.

# Contact

Security Maximale GmbH
Example Street 47 | 4711 Example
FN 12345 v | District Court Example