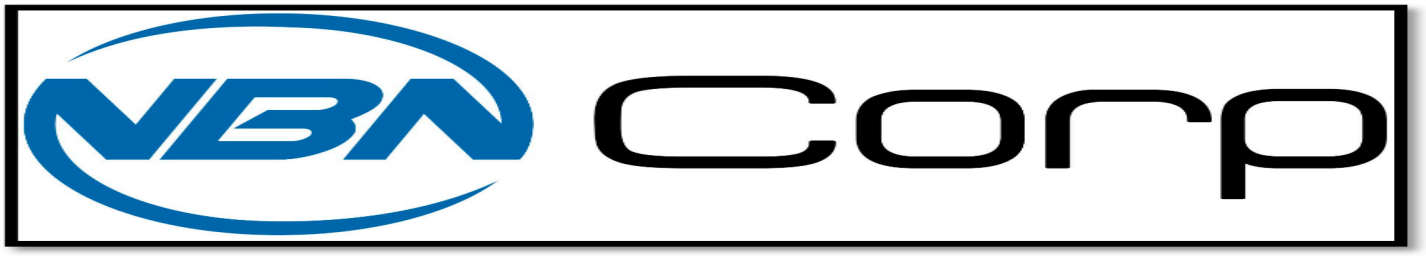
Penetration Testing Report

Hari Kishan Reddy Abbasani (ha2755)

ha2755@nyu.edu

Prepared for

Table of Contents



1.EXECUTIVE SUMMARY

This report presents a comprehensive security assessment prompted by a recent breach at NBN Corp. The primary aim was to identify vulnerabilities within the web servers through a rigorous approach involving network reconnaissance, vulnerability scanning, and targeted exploitation techniques. The examination unveiled critical security gaps, such as exploitable open ports, a login page vulnerability impacting both production and staging servers, and data exposure risks in certain directories. These findings highlight the urgent need to bolster the organization's security posture.

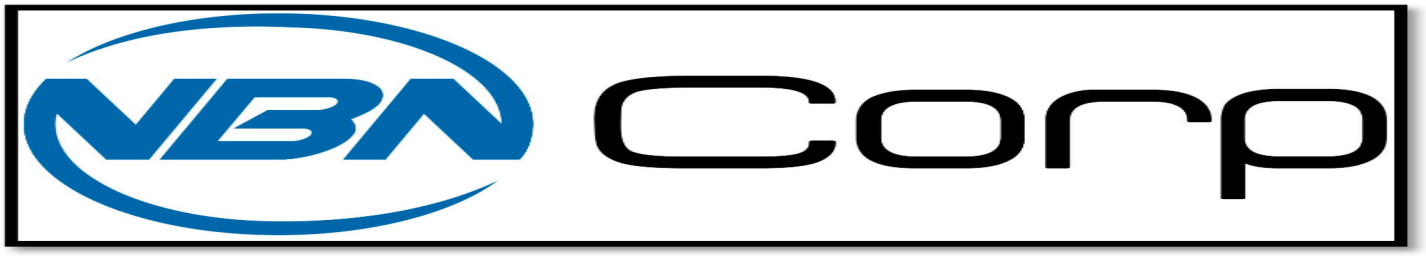
The testing methodology strictly adhered to the guidelines outlined in NIST SP 800-115, ensuring all assessments were conducted under controlled conditions. Throughout the process, the focus was on evaluating the resilience of the systems against security threats and understanding the potential impact of a breach. This executive summary outlines the assessment's purpose, methodology, and significant findings, providing a clear overview of the identified vulnerabilities, their potential consequences, and the pressing requirement for timely remediation efforts to fortify the organization's security stance.

Key Findings and Recommendations

The comprehensive testing revealed critical vulnerabilities within the web servers, indicating potential security threats. Initial Nmap scans uncovered open ports on the production and staging servers. Subsequent Nikto and script using nmap revealed potential exploits and a login page vulnerability on both servers. Further reconnaissance exposed sensitive data, including flag1, and hints of injection vulnerabilities, paving the way for exploitation.

In-depth analysis with SQLMap exposed vulnerabilities in the web application, particularly on the staging server, leading to the extraction of plaintext credentials for the user "gibson." Successful password guessing attacks using Hydra revealed the passwords "digital" for gibson and "pizzadeliver" for user "stephenson." These credentials enabled access to the web application, where exploiting an LFI vulnerability and XSS payloads led to the acquisition of flags 2 and 3. Privilege escalation involved exploiting a unique tee command capability, creating a new privileged user "test," and ultimately obtaining root access.

On the client side, login with stephenson" credentials revealed flag7. Examination identified a potential privilege escalation through sudo versions a linepeas.sh. Exploiting CVE-2021-3156 and CVE-2021-4034 allowed for root privilege escalation, enabling access to flag8. These findings underscore the importance of immediate remediation efforts, with specific recommendations outlined in the detailed report to fortify the organization's security posture.



2.INTRODUCTION

Goals and Purpose of the Test

Objective

The primary objective of the penetration test conducted for NBN Corporation is to assess the security posture of their external-facing web server and client machine. The test aims to identify vulnerabilities, potential attack vectors, and security weaknesses that malicious actors could exploit to gain unauthorized access or compromise sensitive data.

Specific Goals

Assess Security Posture: Evaluate the current security posture of NBN's external-facing web server and client machine to identify vulnerabilities and potential areas of exploitation.

Recommend Solutions: Provide actionable recommendations and immediate fixes to address identified vulnerabilities, enhance security controls, and reduce overall risk exposure.

Timelines/Schedules: The testing timeline adhered to the specified deadline, with the report submission scheduled for the evening of Sunday, May 12th EST.

Targets: The primary targets included the external-facing web server and client machine provided by NBN for assessment. (172.16.1.1, 172.16.1.2, 10.10.0.66)

Major Flaws Identified

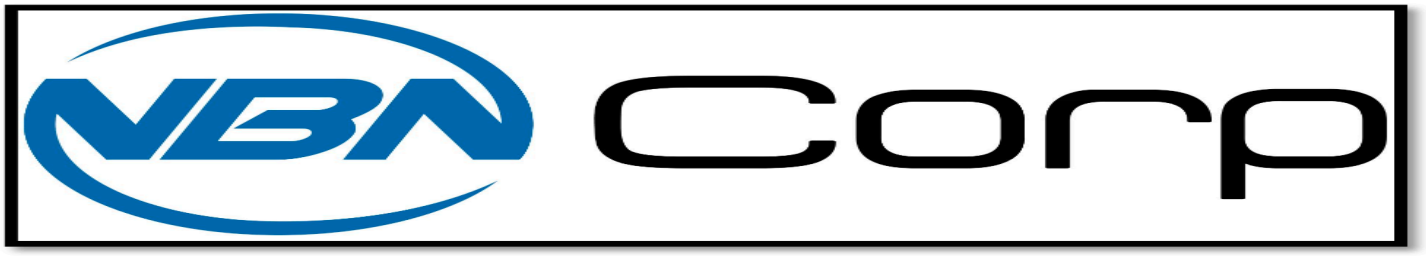
The engagement focused on identifying major flaws in the organization's security infrastructure which were XSS attacks, sqlmap attack, hydra, john the ripper attack and were vulnerable because of misconfigurations, older sudo versions for privilege escalations. The major flaws were.

Vulnerable to sqlmap,hydra,XSS attacks

Simple or basic password credentials of Gibson and Stephenson

FTP easy access allowed.

Older Sudo versions on nbn client and misconfigurations on nbnserver.



3.METHODOLOGY

The penetration testing methodology adopted followed a systematic and structured approach to uncover vulnerabilities within the target systems. The process commenced with an extensive reconnaissance phase aimed at gathering information about the production and staging servers (10.10.0.66 and 10.10.0.66:8001) using Nmap, a robust network scanning tool. This initial scan identified open ports and services, providing a foundational understanding for subsequent assessment steps.

Following reconnaissance, we utilized searchsploit to search for potential exploits based on the identified services and versions. Additionally, a Nikto scan was conducted to discover notable files and directories such as the login page (/login.php), data directory (/data), and internal hints (/internal). The login page discovery prompted further investigation for vulnerabilities and potential entry points.

The assessment progressed into an active exploitation phase, employing Hydra for password guessing attacks on the login page. SQLMap was then used to identify and exploit SQL injection vulnerabilities, resulting in the extraction of plaintext credentials. These credentials facilitated unauthorized access to the web application, where flags 1, 2, and 3 were discovered, highlighting data exposure risks. The methodology also included privilege escalation steps, involving the identification of SUID binaries, linpeas enumeration, and exploitation of CVE-2021-156 and CVE-2021-4034 to achieve root access.

Risk and criticality assessment were conducted using the Common Vulnerability Scoring System (CVSS), considering factors such as exploitability, impact, and affected users. Vulnerabilities were categorized into high, medium, and low risk levels, establishing a prioritized list for remediation efforts.

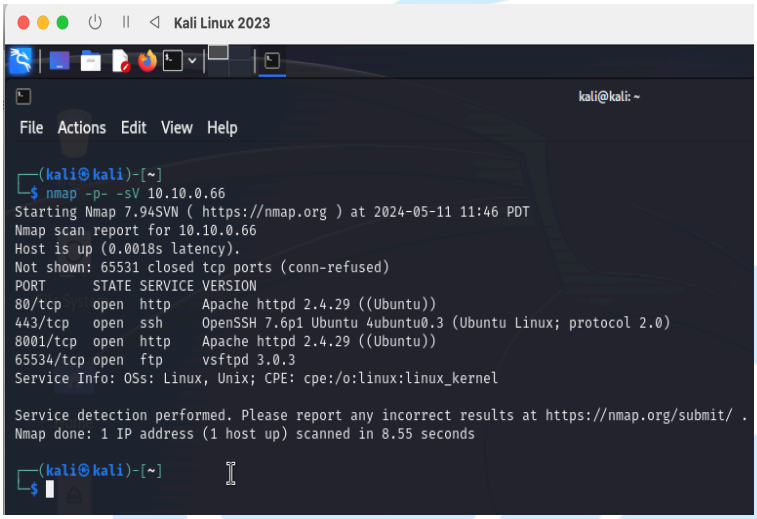
In summary, our methodology encompassed reconnaissance, vulnerability identification, exploitation, and privilege escalation. The tools utilized included Nmap, searchsploit, Nikto, Hydra, and SQLMap. Our risk scoring system facilitated a systematic prioritization of vulnerabilities, ensuring an effective and focused approach to remediation. The detailed steps provided offer transparency and reproducibility in our penetration testing process.

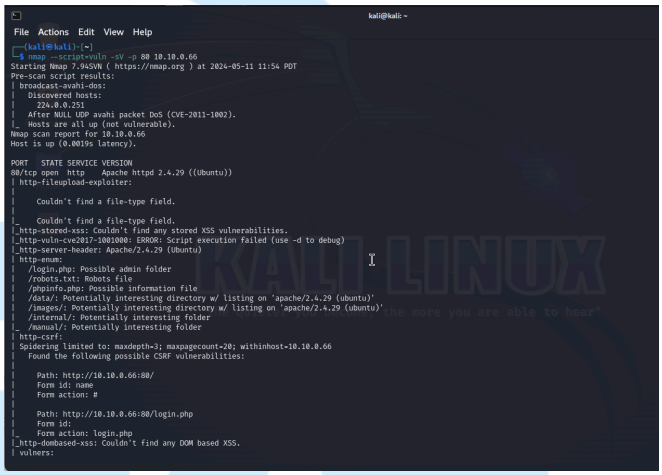
FINDINGS

ATTACK NARRATIVE

Using nmap:

I have started with nmap scanning.

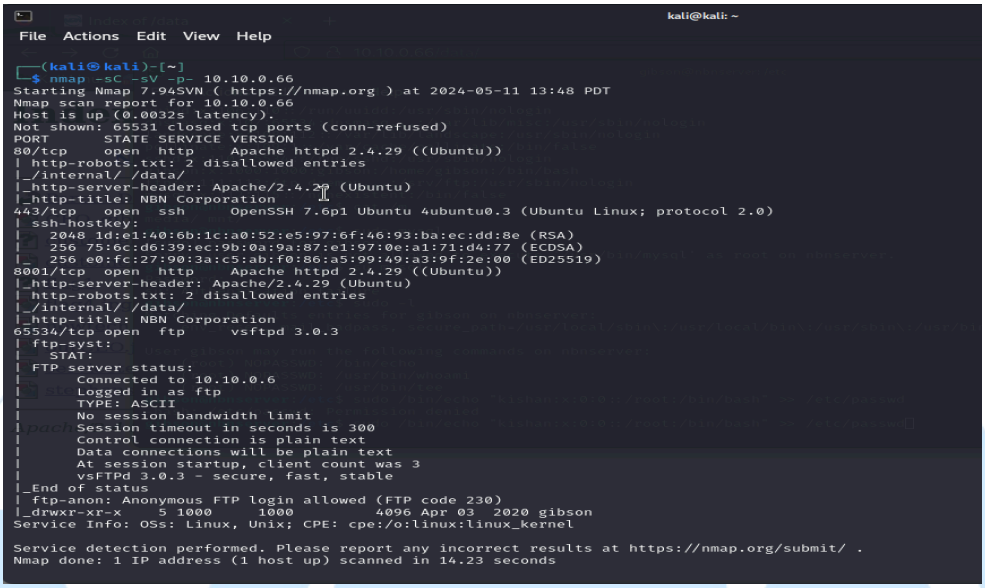




From the first screenshot we can see that 4 ports are running and are open on target 10.10.0.66.

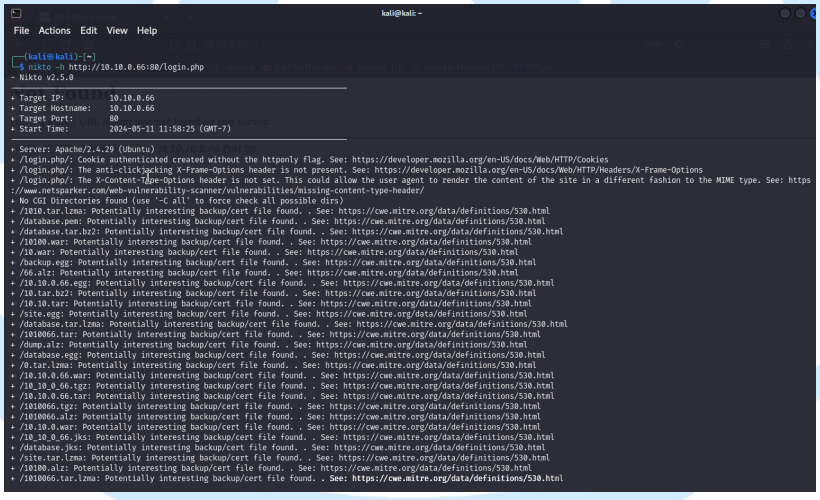
Port 80	http
Port 443	Ssh
Port 8001	http
Port 65534	ftp

From the second screenshot I have used --script=vuln for nmap scanning and the second scan looks interesting, and we can see that there is more interesting stuff. We need to explore login.php file and Robots.txt, data, images, internal, manual folders in the web page http://10.10.0.66.



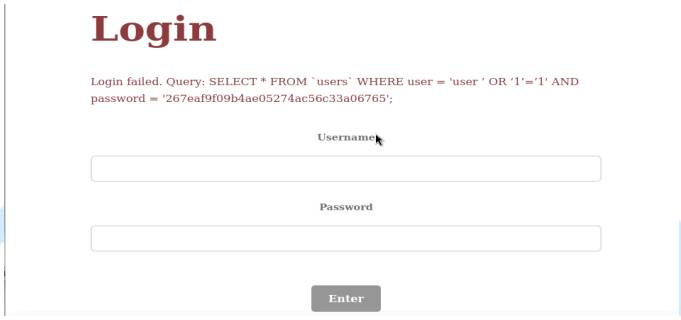
From the screenshot, we have seen that anonymous FTP login is allowed.Will keep this information and scan using other tools to get more information

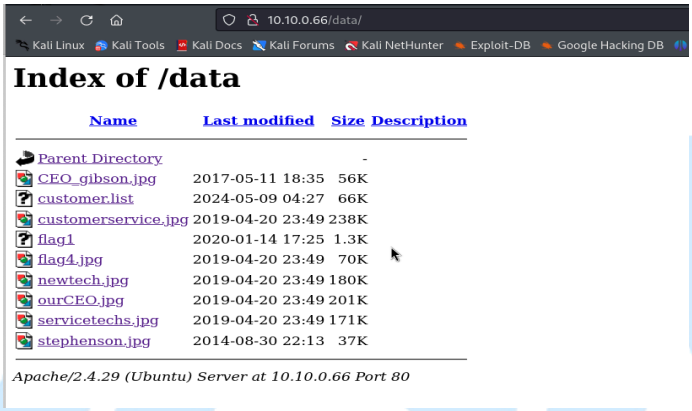
Using nikto:

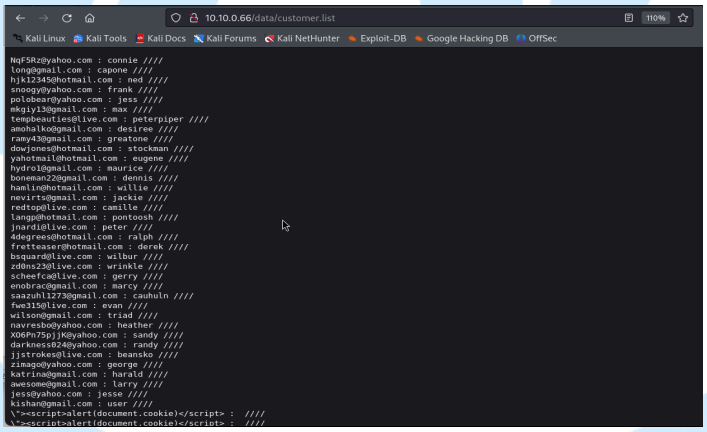


I have used Nikto to scan our target and here are results.

Login:





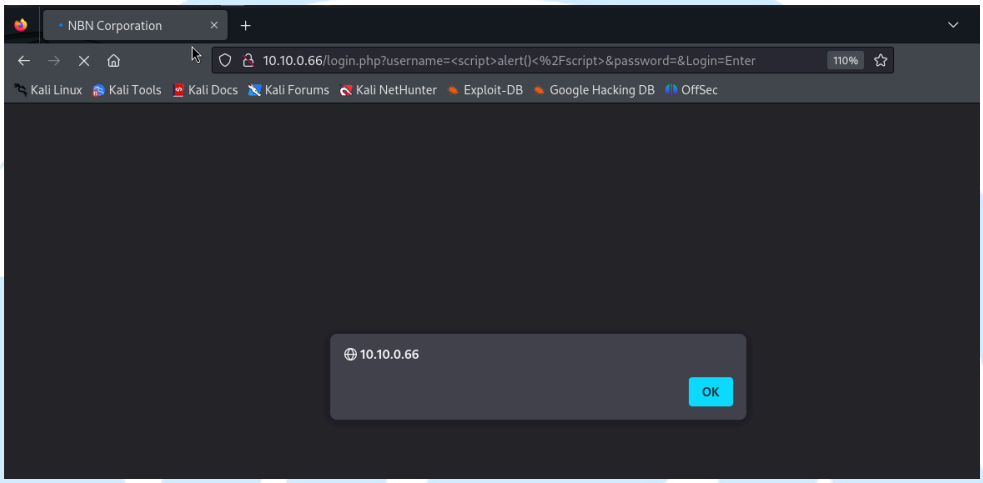


Observations made from the above screenshots:

Next, we will visit our webpage which is running on port 80 and 8001. And when we visit the login page, I just submitted user as username and some random password. We can see that it's taking input and generating SQL queries, so I have tried several SQL injection attacks, but realised that the input validation for username and password is handled well. Then I have tried visiting folders which we got in our previous findings.

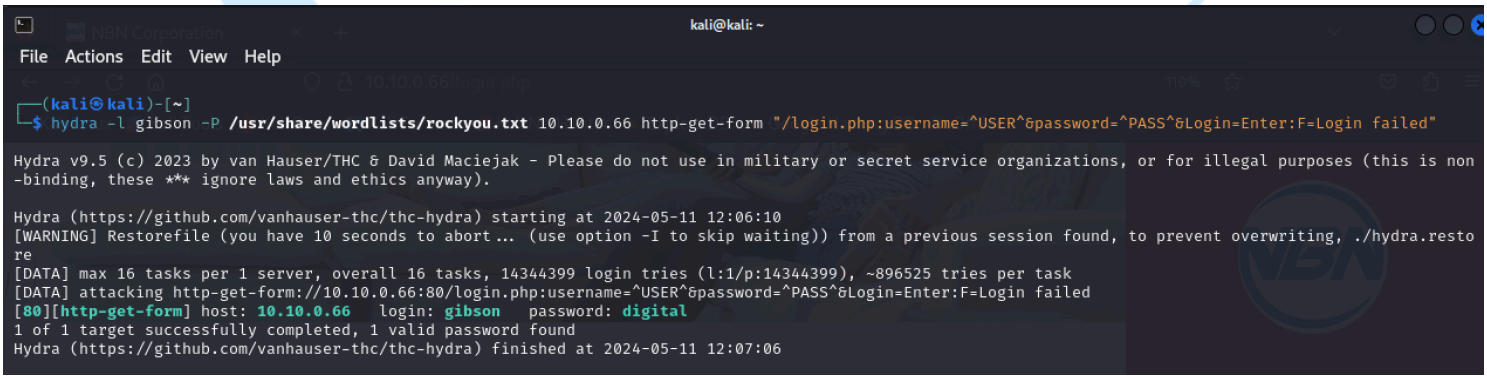
The data folder, we can see that there are many interesting things to explore. There's CEO Gibson image and customer list, and we can even see that there is a flag 1 and Stefanson.jpg. We can see that there are many customer entries under customer.list. For now, let's remember Gibson, flag and our customer list.

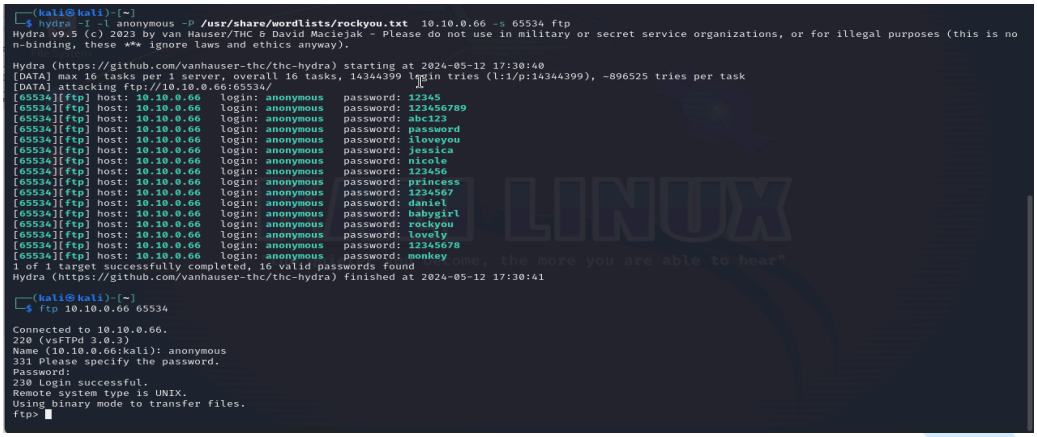
I found that the flag1 is **flag1 {CYBERFELLOWS_GOODLUCK}.**



Then I have tried using burpsuite and found its vulnerable if we can inject script and image tax in the user input. Space. and we can see from the screenshot that an alert prompt is popped when script is injected, and we can conclude that it is vulnerable to xss attacks.We can see that there are two servers among which one is production server on port 80 , and the other one is staging server 8001. We can use SQL map attacks and brute force methods to compromise user credentials.

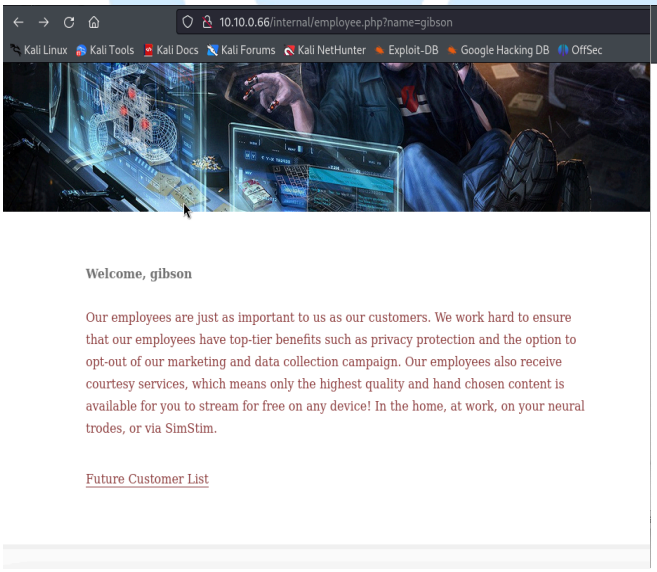
Password cracking using hydra:

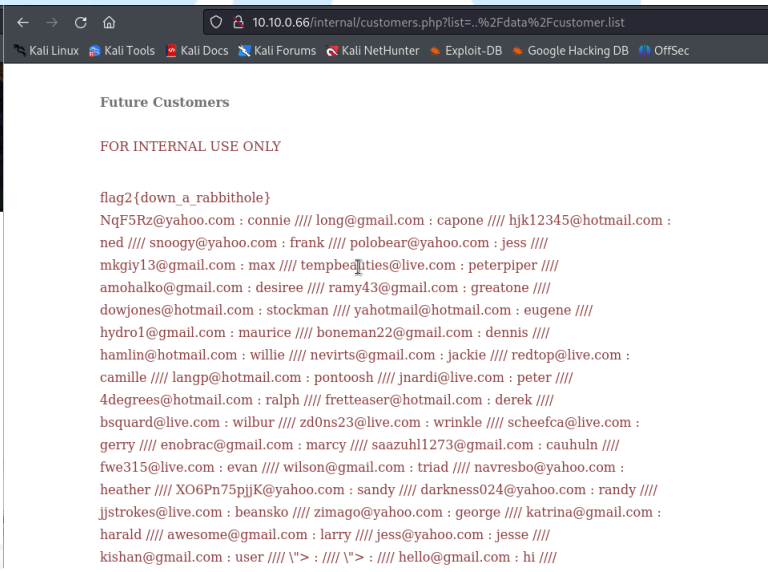




Observations from the above screenshots:

Since we got and predicted that Gibson might be a user. So, let's try hydra to crack the password of Gibson if it's present in the rockyou.txt as given in the web login page as a hint. And luckily, we have cracked the password of Gibson, and the password is digital. And for the FTP port in the previous finding, we know that the username anonymous can be used to login and is allowed. I have tried using hydra and you can see that the user anonymous is also compromised and the password is 123456 and other 16 valid passwords then we can see that the FTP login is successful and is vulnerable. Remember these passwords and we try to login in the login.php if it works.





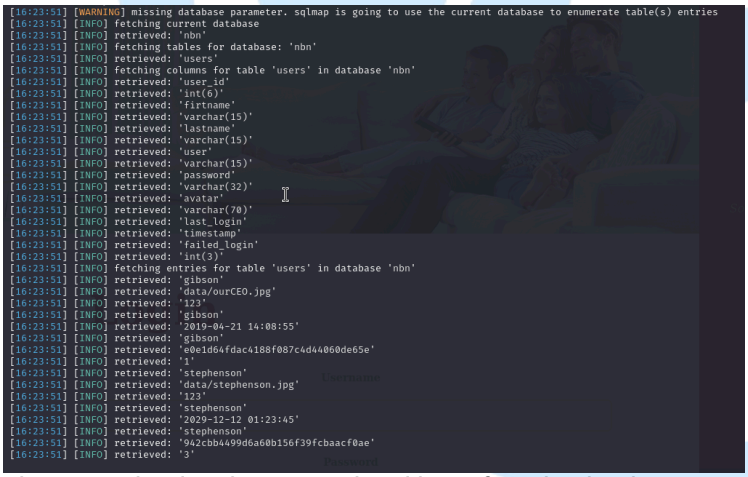
We can see that we have successfully logged in using Gibson and when I click on future customer list it displayed all the customer details and we have got a flag2: **flag2{down_a_rabbithole}.**

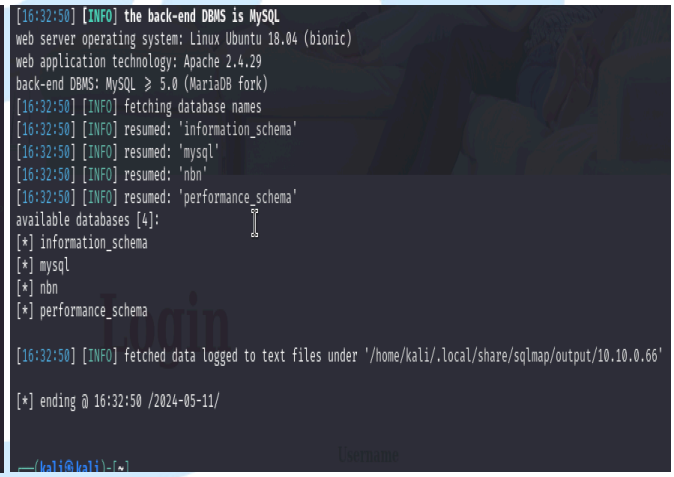
I have visited parallelly on the staging server as well and have phone similar data. Let's keep all this information and we'll check using other tools too.

SQLMAP:

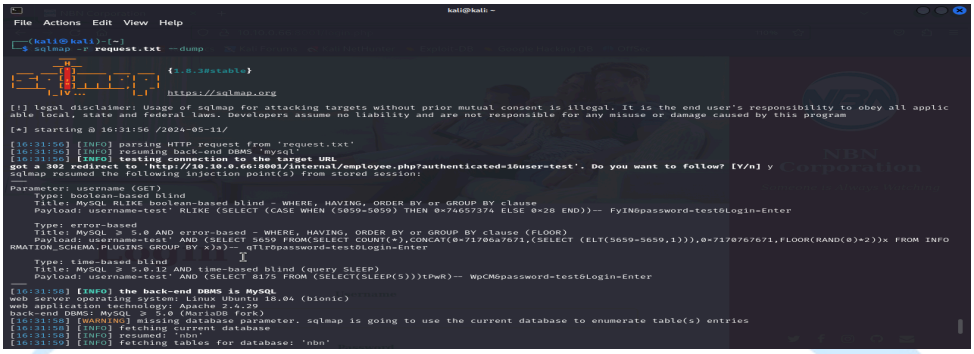
As I said first, I have used burp suite. I have turned on intercept and have successfully intercepted the traffic on the server web page and have checked for other info about the http://service running on both the ports 80 and 8001. To attack using SQL map 1st I have saved a request from port 80 and have try to perform SQL map attack but it failed. Then I've tried the same SQL map attack on staging server. So first I have saved the request name request.txt file from the burpsuite And then perform the attack and it was successful.

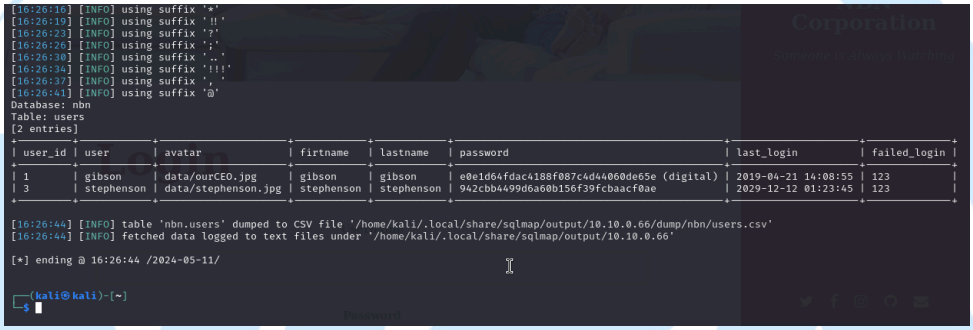
Commands I have used:
Sqlmap -r requirements.txt –dbs
Sqlmap -r requirements.txt –dump

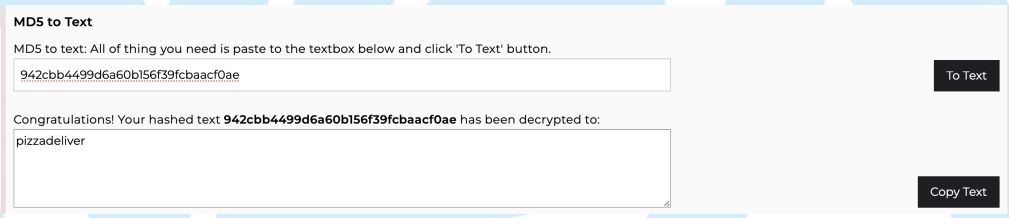




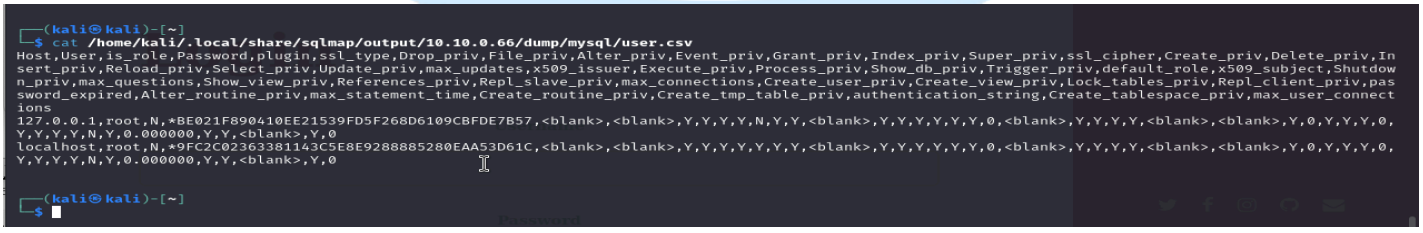
These are the details retrieved and have found 4 databases.

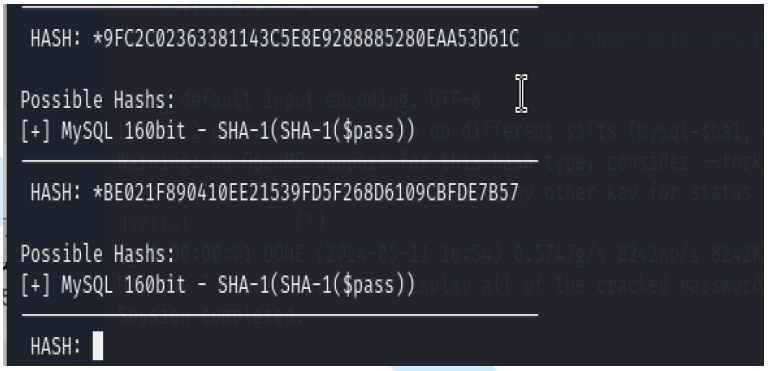


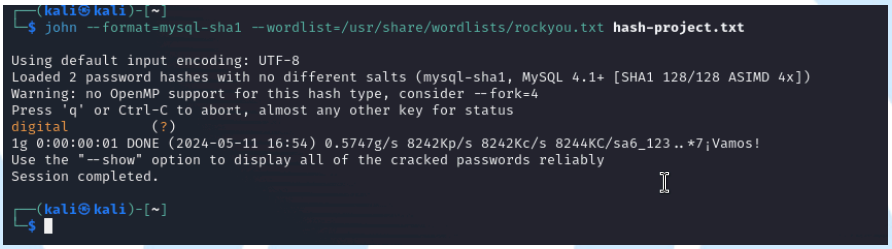




observation from the screenshots:
we can see that we have found 2 usernames and its hash values. Gibson and Stephenson, we already know Gibson's password and you need to find stephenson password. I have phone that the hash is MD5 and so have used online converter from MD5 to plaintext and got the password as **pizzadeliver**.
Other than the above screenshots I have also tried viewing user table and when I have seen it said it showed that there are two users called root and with the hash value. I have used hash identifier to identify the below hashes and found it is mysql 160bit SHA-1. At the end when I use John the Ripper tool to crack it, it was the same password of Gibson, so it wasn't that useful.



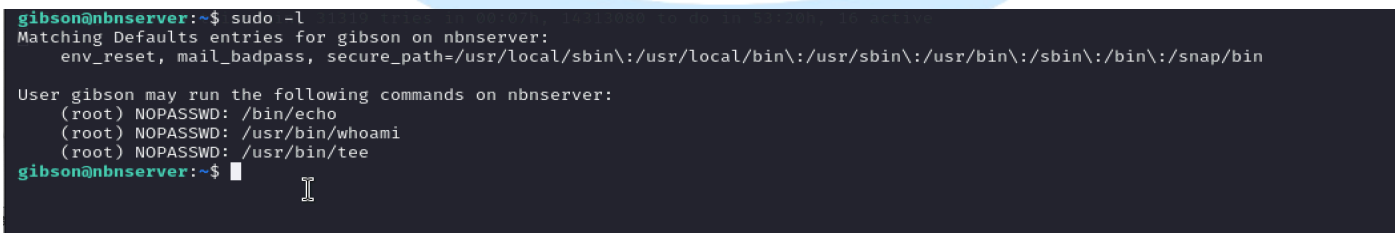




Login into nbnserver using the credentials:

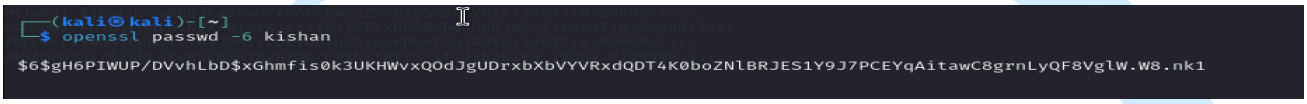
Let's log in through the credentials of Gibson and Stephenson. I was able to log in using Gibson credentials successfully into NBN server. I found a flag 3 when I logged in using Gibson and Stevenson credentials didn't work.

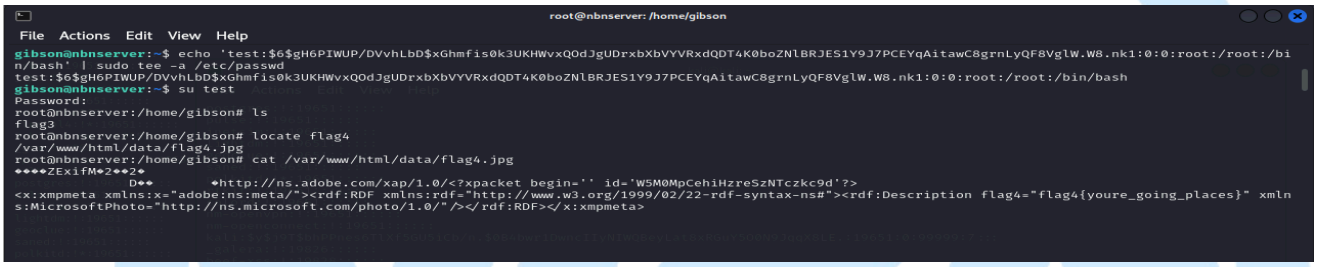
flag3{brilliantly_lit_boulevard}



Even though we logged in into server using Gibson, but our aim is to gain the root shell, so I have tried several privileged escalation methods and one of them had worked. First, I have seen what executable permissions Gibson would have using sudo -l And I'm able to see that Gibson can execute echo and tee command. I have seen /etc/passwd file and try to modify it. For that first we need to create a user. So, I have created a user called test and have generated a password using openssl. 1st I have generated using user kishan but wasn't successful because my Kali is encrypting as yescrypt. So, I have used openssl to create a password Kishan for user test. Then I have used the command

echo 'kishan:6gH6PIWUP/DVvhLbD$xGhmfis0k3UKHWvxQOdJgUDrxbXbVYVRxdQDT4K0boZNlBR-JES1Y9J7PCEYqAitawC8grnLyQF8VglW.W8.nk1:0:0:root:/root:/bin/bash' | sudo tee -a /etc/passwd

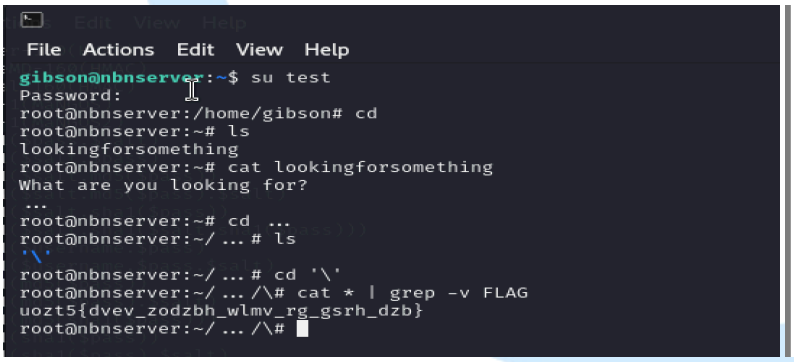


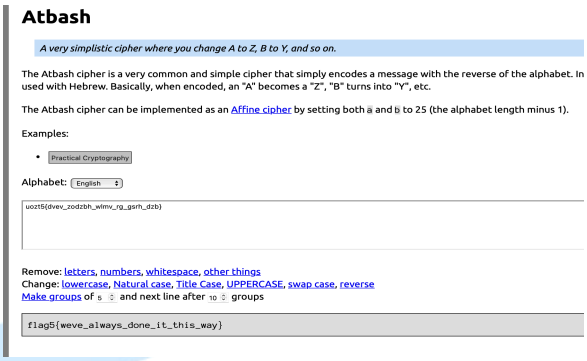


After executing the command, I was able to log in using user test as root. I found flag 4 when I logged in as root.

Flag4{youre_going_places}

Then I have executed command cd and then searched for files if there's any, I have phone a file called looking for something. I ultimately ended up finding flag 5, though it was different, but we can see that it was in the flag format and the number. So, I thought that this would be a substitution cipher. Later I decrypted it using online atbash cipher to plain text which indeed is a substitution cipher.

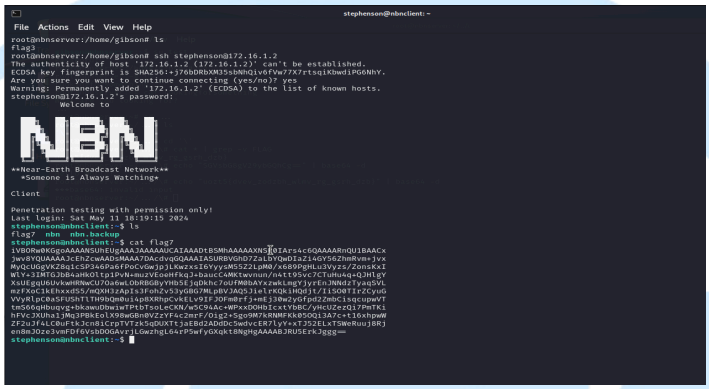


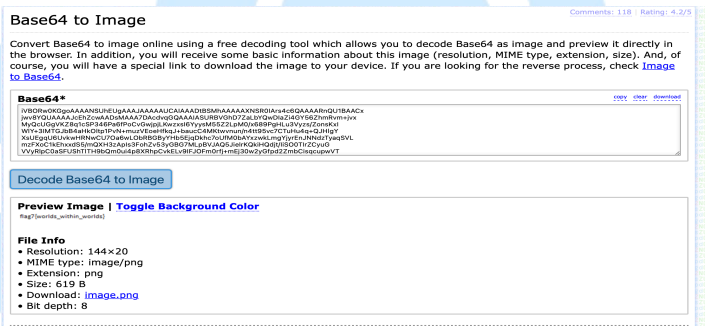


Flag5{weve_always_done_it_this_way}

Login into nbnclient:

Now let's try logging into NBN client machine using the credentials of Gibson and Stephenson. I was able to log in successfully using stephensons credentials. After logging into NBN client I was able to find a flag 7. First, I thought it was base 64 encoded and tried to decode it using Kali, then I found out that it was a PNG image, so I have used base 64 to image converter to get the flag 7.





Flag7{worlds_within_worlds}

I have got connection issues between server and client.Then I have tried to analyse using wireshark but I wasn't able to use and then luckily when I used tcp dump (while pinging), I was able to find **flag6{listen}**

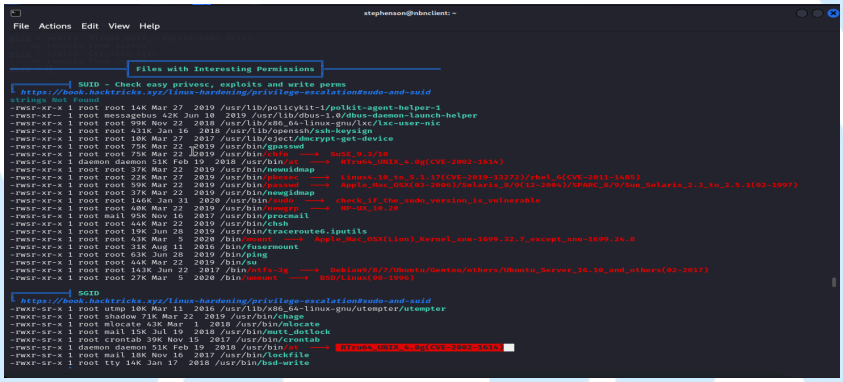
```
File  Actions  Edit  View  Help
root@nbnserver:~# sudo tcpdump -i enp0s7 -nXS
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s7, link-type EN10MB (Ethernet), capture size 262144 bytes
01:17:41.460250 IP 172.16.1.2 > 172.16.1.1: ICMP echo request, id 627, seq 8556, length 64
        0x0000:  4500 0054 f928 4000 4001 e75c ac10 0102  E..T.(@.@..\....
        0x0010:  ac10 0101 0800 4691 0273 216c b418 4066  ......F..s!l..@f
        0x0020:  0000 0000 45e7 0000 0000 0000 6736 7b6c  ....E.......g6{l
        0x0030:  6973 7465 6e7d 666c 6167 367b 6c69 7374  isten}flag6{list
        0x0040:  656e 7d66 6c61 6736 7b6c 6973 7465 6e7d  en}flag6{listen}
        0x0050:  666c 6167                                flag
01:17:41.461206 IP 172.16.1.1 > 172.16.1.2: ICMP echo reply, id 627, seq 8556, length 64
        0x0000:  4500 0054 150a 0000 4001 0b7c ac10 0101  E..T....@..|....
        0x0010:  ac10 0102 0000 4e91 0273 216c b418 4066  ......N..s!l..@f
        0x0020:  0000 0000 45e7 0000 0000 0000 6736 7b6c  ....E.......g6{l
        0x0030:  6973 7465 6e7d 666c 6167 367b 6c69 7374  isten}flag6{list
        0x0040:  656e 7d66 6c61 6736 7b6c 6973 7465 6e7d  en}flag6{listen}
        0x0050:  666c 6167                                flag
```

We have successfully able to login but need to get a root shell. In the NBN server, Gibson can execute echo and tee commands but it's not the case with Stephenson in NBN client machine. This account has only limited permissions so we have to find a way to get a root shell.

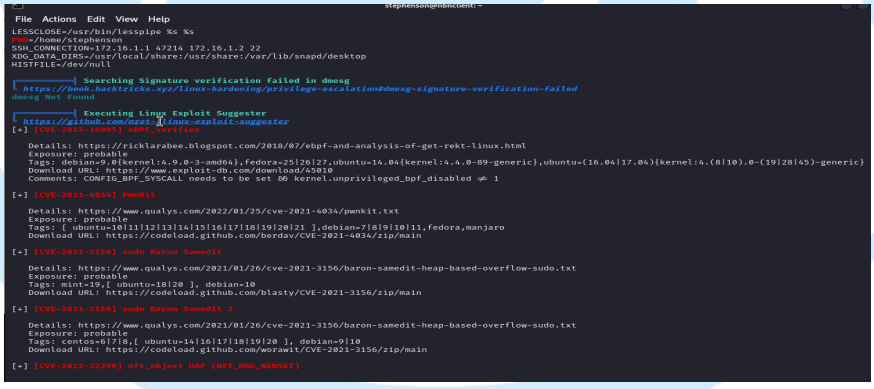
```
stephenson@nbnclient: ~
File  Actions  Edit  View  Help
stephenson@nbnclient:~$ sudo -l
Matching Defaults entries for stephenson on nbnclient:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User stephenson may run the following commands on nbnclient:
    (root) NOPASSWD: /home/stephenson/nbn
stephenson@nbnclient:~$
```

I have used linpeas script for privilege escalation. I have found these results on NBN client when Linpeas.sh is executed. I have tried exploiting different attacks on NBN client but were unsuccessful.



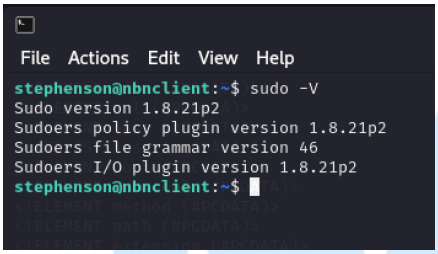
I have seen **/at RTru64_UNIX_4.0g(CVE-2002-1614)** and **/pkexec** as interesting insights and explored furthermore.

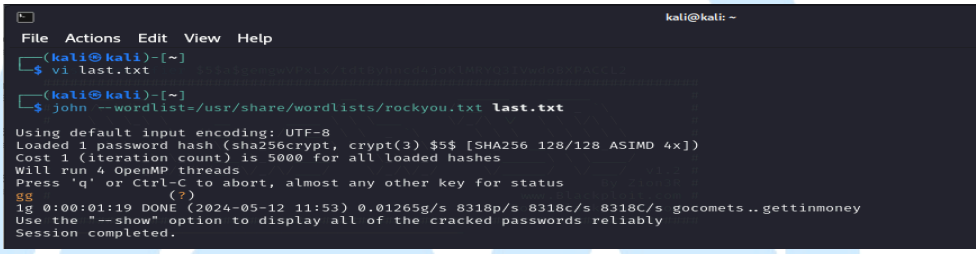


From the above screenshot, linpeas has given executing Linux exploit suggester as some suggestions and would be a probable exposure. First vulnerability is ebf verifier and when I explored about this, I came to know that this is buffer overflow vulnerability and can be exploited using buffer overflow attack. I thought buffer overflow attack would take time and would do it after trying other given exploits. 2nd and 3rd vulnerabilities were working, and I was able to get a shell on NBN client.

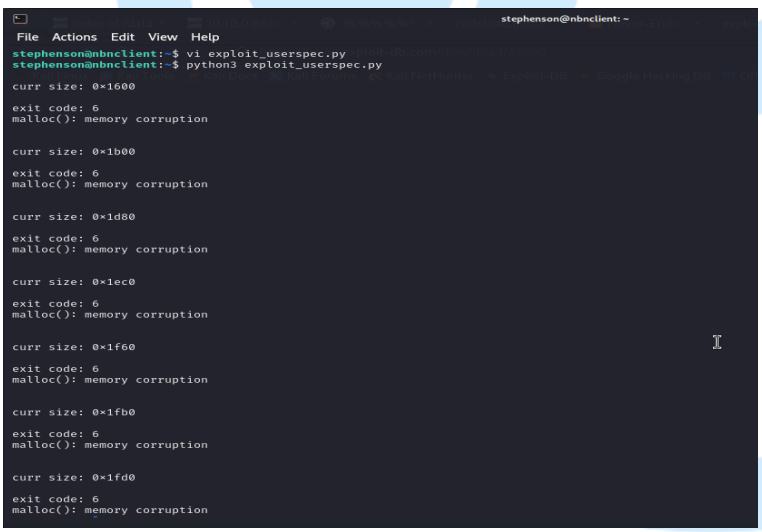
Third vulnerability was even more useful to get a complete root shell. This vulnerability about sudo version. I have explored more on this and have found that this is vulnerable to particular sudo versions from 1.8.17 to 1.8.23 and I checked version of our NBN client machine, and it is version 1.8.21p2 which indeed is vulnerable. So, I tried searching already existing exploits on the Internet and luckily, I found one. I have executed the Python script and was able to see that user GG is added to the password file. There's a hash, so I tried to crack the password using John the Ripper and was able to find the password is gg. I was able to log in successfully into NBN client as root and found the flag 8. It was encoded in base 64 I have used base 64 converter to text which is present in the Internet and have decoded the flag 8 successfully.

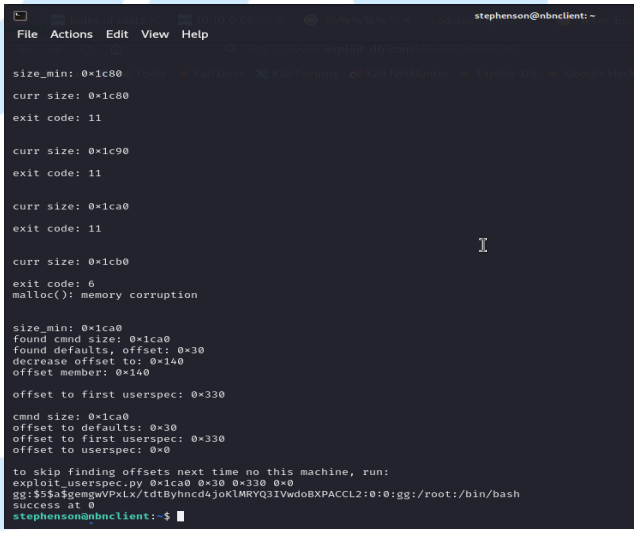
I found the script from https://github.com/worawit/CVE-2021-3156/blob/main/exploit_userspec.py
I have also tried. second exploit and it was successful.

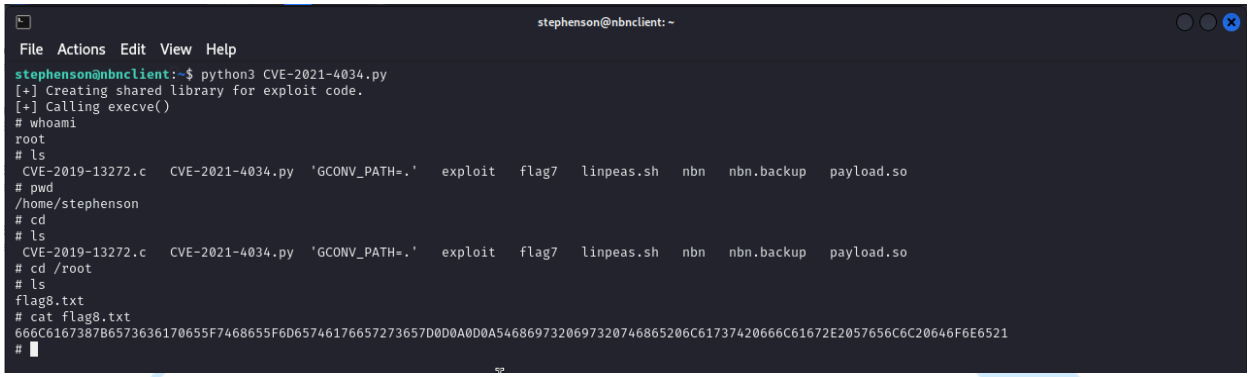




flag 8{escape_the_metaverse}



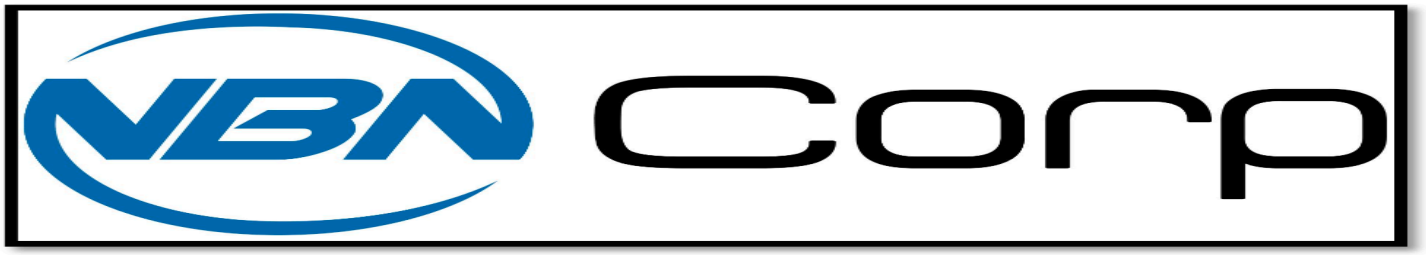




For second vulnerability, I researched on https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt

We discovered a Local Privilege Escalation (from any user to root) in polkit's pkexec, a SUID-root program that is installed by default on every major Linux distribution

Luckily, I was able to find the exploit code directly on Internet: https://github.com/joeammond/CVE-2021-4034



CONCLUSION:

This penetration testing initiative was undertaken to conduct a comprehensive security assessment of the organization's infrastructure, with the primary goals of uncovering vulnerabilities, evaluating associated risks, and providing actionable recommendations to strengthen the overall security posture. The focus of the assessment was on the externally facing web servers, specifically the production server (10.10.0.66) and the staging server (10.10.0.66:8001). The methodology employed involved a systematic approach, encompassing reconnaissance, exploitation, and privilege escalation techniques, to thoroughly evaluate the systems' resilience against potential external threats.

The findings from the penetration test revealed critical security vulnerabilities, including exploitable open ports, SQL injection flaws, and data exposure risks. The successful compromise of credentials, acquisition of flags, and access to sensitive data during the assessment highlight the severe potential consequences of a security breach. A risk scoring system based on the Common Vulnerability Scoring System (CVSS) was applied, categorizing the identified vulnerabilities as high, medium, or low risk.

Immediate remediation actions are crucial to bolster the organization's security stance. Key recommendations include patching and securing exposed ports, implementing robust input validation mechanisms to mitigate SQL injection vulnerabilities, and enhancing access controls to prevent unauthorized data exposure. Additionally, removing unnecessary services and promptly applying security patches are critical steps to mitigate potential risks.

These below vulnerabilities need to be taken care by updating the configurations and versions like sudo to latest version and changing passwords to very strong from weak.

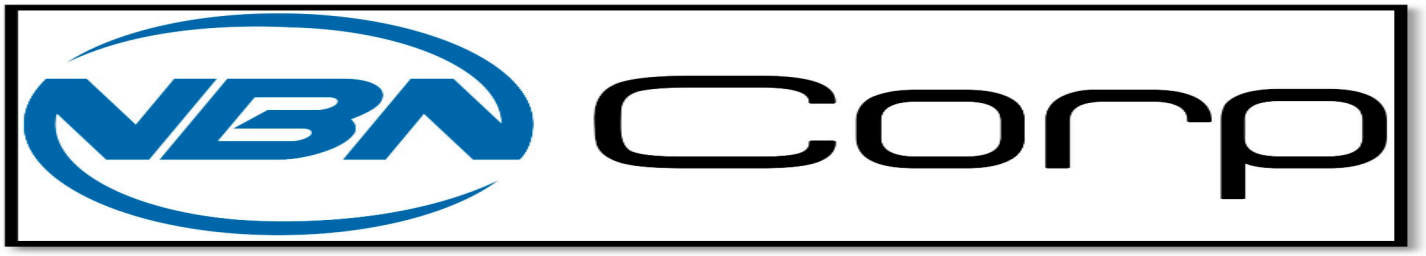
Vulnerable to sqlmap,hydra,XSS attacks

Simple or basic password credentials of Gibson and Stephenson

FTP easy access allowed.

Older Sudo versions on nbn client and misconfigurations on nbnserver.

In essence, the penetration testing results provide a comprehensive overview of the current security landscape, emphasizing the pressing need for timely remediation efforts. By addressing the identified vulnerabilities and implementing the recommended fixes, the organization can proactively enhance its cybersecurity resilience and mitigate the risks associated with potential security breaches.



Appendixes

Appendix A - Ports, Protocols, and Services:

Port	Protocol	Service	Version
80	TCP	HTTP	Apache/2.4.29
443	TCP	SSH	OpenSSH/7.6p1
8001	TCP	HTTP (Staging)	Apache/2.4.29
65534	FTP	vsftpd	3.3

Appendix B - Usernames and Passwords

Username	Password
gibson	digital
stephenson	pizzadeliver
test	kishan
Anonymous	123456
gg	gg

Appendix C - Flags

Flag Number	Flag
flag1	flag{CYBERFELLOWS_GOODLUCK}
flag2	flag2{down_a_rabbithole}
flag3	flag3{brilliantly_lit_boulevard}
flag4	flag4{youre_going_places}
flag5	flag5{weve_always_done_it_this_way}
flag6	flag6{listen}
flag7	flag7{worlds_within_worlds}
flag8	flag8{escape_the_metaverse}