Security and Countermeasures 2

Unit: CSY3209 – Security and Countermeasures

Georgi Zayakov

UoN: 24832834

Contents

[Introduction 3](#_Toc197089170)

[Vulnerabilities Discovered 3](#_Toc197089171)

[Hardening Applied 6](#_Toc197089172)

[Critical evaluation and analysis of countermeasures applied 9](#_Toc197089173)

[Conclusion 9](#_Toc197089174)

[Bibliography 10](#_Toc197089175)

[Appendix 1: Penetration Test 11](#_Toc197089176)

[Appendix 2 Applied hardening 21](#_Toc197089177)

# Introduction

This report will provide all the vulnerabilities discovered from penetration testing of the FTP server of a company with five employees and five different departments. Furthermore, techniques that align with the CIA triad will be recommended for implementation. The applied techniques will be described and tested to ensure security enhancement. Also, they will be discussed and evaluated for their relevance to the vulnerabilities and the CIA security framework.

# Vulnerabilities Discovered

This section will present the discovered vulnerabilities from the initial penetration testing in [Appendix 1: Penetration Test](#_Appendix_1:_Testing).

Total number of tests: 26.

Pass test: 16.

Expected fails: 6.

Critical Fails to be addressed: 5

The identified weaknesses are as follows:

1. Critical information is stored in the description section of the FTP server virtual machine (VM). The description section contains credentials of all three users (root, user and testuser). Test number 12 demonstrated that the credentials are correct and enable login into the system for the root and the testuser. This is a critical disclosure of information that must be fixed.

* **Hardening techniques to be applied:**

This sensitive information must be deleted from the description section to avoid login from an unauthorised person.

**CIA triad alignment:** Confidentiality and Integrity

1. Weak passwords such as ‘centos’ and ‘vulntest’ are used by the users. These passwords can be easily discovered with a proper brute-force attack.

* **Hardening techniques to be applied:**

To prevent this, it should be created a password policy that enforces minimum 12-character passwords to contain uppercase letters, lowercase letters, numbers and special characters. Also, the policy must enforce a password change every 40 days.

**CIA triad alignment:** Confidentiality

1. After logging in the FTP server was discovered that all users have privileges of administrator for the FTP server machine. This cannot be considered a good practice and should be addressed.

* **Hardening techniques to be applied**

To fix this vulnerability, administrator privileges should be granted only to the administrator of the server. The other departments should have normal user privileges. This measure will ensure that only the administrator can modify the system and will prevent unintentional or intentional misconfiguration by other users.

**CIA triad alignment:** Integrity (principle of least privileges)

1. Test number 3 discovered that, except for the ftp port 21, ports 22 for SSH and port 80 for HTTP are open. The ports that are not essential for the system may provide an additional backdoor for hackers.

* **Hardening techniques to be applied:**

If SSH is needed for the remote connection of the administrator, it must be restricted to allow only administrators and reject connections from non-administrator users. Port 80 HTTP must be closed because this is an additional target for the attackers and can lead to an exploit of the server. These actions will reduce the attack options.

**CIA triad alignment:** Confidentiality and Integrity

1. With the help of the Metasploit framework, two publicly known vulnerabilities related to Denial-of-Service attacks and backdoor command execution were discovered for the FTP server application vsftpd.

* **Hardening techniques to be applied:**

Even if I did not exploit the system via this backdoor, the ftp application must be updated with a version without discovered vulnerabilities or replaced by another application.

**CIA triad alignment:** Dos -Availability, Backdoor- Confidentiality

1. Test 25 reveals another issue related to the lack of FTPS support. The FTP protocol is not encrypted, and the login credentials can be sniffed. The encrypted FTPS version could provide an additional layer of security by ensuring the confidentiality of the transferred data.

* **Hardening techniques to be applied**

FTPS to be installed.

**CIA triad alignment:** Integrity and Confidentiality

1. Reading of configuration files from each user, as confirmed by tests 21 and 22 in Appendix 1, can reveal sensitive data about the system.

* **Hardening techniques to be applied:**

Access to this file should be restricted only to the IT team. This will reduce the chance of misconfiguration of the system by the other departments.

**CIA triad alignment:** Confidentiality and Integrity

1. The fact that the users share the same password poses a risk of access to the entire information of the server if the password is discovered.

* **Hardening techniques to be applied:**

RBAC to be implemented. The different departments must be on separate accounts with unique passwords for each of them.

The departments using the FTP server are:

* Finance
* Sales
* Developers (Working on government contracts)
* IT
* Management

The IT department can have administrator privileges while the other must have normal user accounts. The IT team can be granted root access if they manage the server’s configuration.

**CIA triad alignment:** Confidentiality

1. The 'testuser' can change the directory in the FTP server and read sensitive information about the configuration of the machine.

* **Hardening techniques to be applied:**

Each normal user must be restricted to certain directories according to the needs of the organisation and shouldn’t be allowed to read or download configuration files. Separate directory for each department and one shared directory for all could solve this issue.

**CIA triad alignment:** Integrity and Confidentiality

The vulnerabilities discovered can pose a significant threat to compromising the confidentiality, availability, or integrity of the system. Implementing proper hardening techniques is essential for reducing the risk of unauthorised access and other attacks on the system.

# Hardening Applied

Based on the identified vulnerabilities from the penetration test, the following hardening techniques were applied to enforce the system security:

All tests for the measures applied can be found in [Appendix 2 Applied hardening](#_Appendix_2_Applied).

1. The system is updated to ensure the latest security patches are installed. Test 27 in Appendix 2 shows the kernel installed and the kernels available. It also confirms that the latest kernel is installed.
2. Test number 28 confirms that the sensitive information was deleted from the description section to avoid disclosure.
3. The password policy was created with the following steps:

* To implement password requirements, the following file /etc/security/pwquality.conf was edited.

A white background with black text

AI-generated content may be incorrect.

This policy requires users to create a password with a minimum of 12 characters and at least one digit, one uppercase letter, one lowercase letter, and one special character.

* Expire time

Editing the login.defs file in the /etc directory ensures that each password expires after 40 days and must be changed. It also defines the minimum days before expiration, the minimum length of the password, and how many days before the expiration date a warning should be displayed to the user.

sudo vi /etc/login.defs

A close up of a number

AI-generated content may be incorrect.

* Password reuse rule

In the file system-auth located in /etc/pam.d/, “remember=5” was added to the end of the line displayed below to ensure that the new password is not the same as the last 5 passwords.



Test 29 confirms that the password restrictions are applied. The root use is required to create a password that aligns with the restrictions implemented.

1. Close port 80

To close port 80, the following command was executed in the terminal:



Test 30 confirms that port 80 is closed.

1. Restrict the SSH connection to root and the IT department.

To apply the changes, the sshd\_config file in /etc/ssh/ directory must be edited by adding the following line: AllowUsers root it. This limits the use of SSH connections only to the users with administrator privileges, ‘root’, and ‘it’.A white background with black text

AI-generated content may be incorrect.

Test 31 proved that the ‘testuser’ is restricted from connecting to the SSH service of the FTP server.

1. Different users were created for each department. The results are approved by test number 32.
2. Restriction of the configuration files.

In the terminal of the root user was execute the command in the next picture to restrict users from opening the configuration files.

A number of numbers on a white background

AI-generated content may be incorrect.

Also, the ownership of the files was ensured to be on the root user with the following command.



In addition to that, each user was restricted to opening only their home directory.

A number of text on a white background

AI-generated content may be incorrect.

Test 33 confirms that the users are restricted to their own home folder**.**

1. Confirm FTPS configuration.

Test number 34 approved that an SSL connection is supported by the server.

From the results above can be concluded that most of the identified vulnerabilities were properly addressed with appropriate measures. Although, due to time restrictions, protection against the public vulnerabilities of the FTP application was not implemented.

# Critical evaluation and analysis of countermeasures applied

The section will critically evaluate and analyse the server hardening techniques implemented for the FTP server.

The update of the system with the latest kernel version was an essential hardening technique that is necessary to continue with the other hardening techniques later. It was implemented first as a basis for the next techniques to be adopted. Deletion of the credentials from the description section was also very important and shows that sometimes a simple human negligence can cause a significant threat to security. The password policy implemented covers all aspects of the strong password requirements and significantly reduces the chances of a brute-force attack success. Closing port 80, the SSH rules applied, and the restriction for opening configuration files reduces the surfaces for attack and reconnaissance over the system and enhances the overall security. Implementing RBAC was also essential for the confidentiality of the information and prevents access to all information on the server in case of a compromised password of a department. Another important hardening to support confidentiality is the installation of FTPS for encryption of the connection between the FTP client and the FTP server. Without this encryption, the data transferred, and the login credentials were easy to discover and could pose a risk.

# Conclusion

The report identified vulnerabilities of the FTP server and recommended a relevant technique for hardening to enhance the security of the system. It also tested the implemented solution and significantly enhanced the overall security. Despite that a few problems were not addressed due to time constraints, the adopted hardenings gave a robust system. It is recommended that the system be updated and tested on a regular interval, and the remaining issues to be addressed as soon as possible. The lesson learned from the report is that the security of a system is a continuous process, and negligence of the people can lead to serious consequences.

# Bibliography

Hacktricks.wiki. (2025). *21 - Pentesting FTP - HackTricks*. [online] Available at: https://book.hacktricks.wiki/en/network-services-pentesting/pentesting-ftp/index.html [Accessed 2 May 2025].

pentestTV (2024). *I hacked an FTP server (and you can too)*. [online] YouTube. Available at: https://www.youtube.com/watch?v=\_WOjvxafVCw [Accessed 2 May 2025].

# Appendix 1: Penetration Test

Back to [Vulnerabilities Discovered](#_Vulnerabilities_Discovered)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Description | Steps to reproduce | Expected Result | Actual Result | Status |
| Information Gathering | | | | | |
|  | Identify the hosts in the network | Run in the terminal:  Nmap -sn 192.168.56.103/24 | All hosts IP addresses to be discovered. | A computer screen shot of a computer  AI-generated content may be incorrect. | Pass |
|  | Find the FTP server | Run in the terminal  ftp 192.168.56.1  ftp 192.168.56.100  ftp 192.168.56.102 | The FTP server to be found. | A computer screen with white text  AI-generated content may be incorrect.  FTP server IP - 192.168.56.102 | Pass |
|  | Find all ports (closed and open) | Run in the terminal:  nmap -sV 192.168.56.102 | All ports to be discovered. | A computer screen with white text  AI-generated content may be incorrect.  Ports;   * 21/tcp **open** ftp vsftpd 2.0.8 or later * 22/tcp **open** ssh OpenSSH 7.4 (protocol 2.0) * 23/tcp closed telnet * 53/tcp closed domain * 80/tcp **open** http version: Apache httpd 2.4.6 (Cent OS mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_WSGI/3.4 Python/2.7.5 | Pass |
|  | Search for ftp application vulnerabilities | Run in terminal:  searchsploit vsftpd | Find vulnerabilities of the ftp application. | A screenshot of a computer program  AI-generated content may be incorrect.  Two backdoor comand 2.3.40 | Pass |
|  | Search ftp application backdoors in Metasploit. | Open Metasploit in kali:  >search vsftpd  >use 1  > show options | Vulnerabilities of the ftp application to be displayed if any | A screen shot of a computer  AI-generated content may be incorrect.  A screenshot of a computer  AI-generated content may be incorrect.  Two issues are displayed related to DoS attack and backdoor. | Pass |
|  | Try to exploit the FTP application | >set RHOSTS 192.168.56.102  >set CHOST 192.168.56.103  >set CPORT 6666  >run | Exploit the system. | No session was created.  A screenshot of a computer program  AI-generated content may be incorrect. | Fail |
|  | Banner grabbing | In Kali Linux terminal:  nc -vn 192.168.56.102 21 | Banner to be retrieved. | As expected. | Pass |
|  | Grab FTP Banner via telnet | Command: telnet -n 192.168.56.102 21 | Banner to be retrieved. | Fail to grab banner.A screen shot of a computer  AI-generated content may be incorrect. | Fail |
| Access Attempts | | | | | |
|  | Anonymous FTP login | Connect to the:  ftp 192.168.56.102  enter:  Username: anonymous  Password: anonymous | Unable to login! | A computer screen with white text  AI-generated content may be incorrect.  As expected. | Pass |
|  | Browser connection. | Enter in the following URL in a browser:  ftp://anonymous:anonymous@192.168.56.102 | Unable to login! | A black background with white text  AI-generated content may be incorrect.  As expected. | Pass |
|  | Brute force attack | Use hydra to crack the password.  need username (root, user)  hydra -l root -P {/usr/share/wordlist/metasploit/password.lst -e nsr 192.168.56.102 ftp | Password to be discovered. | Unable to discover the password with brute force attack. | Fail |
|  | Attempt to login into the server with the information in the description from the FTP VM. | Try login with the information from the description section of the VM:   * root/centos * user:wtest * testuser/vulntest | Login with the credentials. | Result:  Combination of username and password   * root/centos - successful * user:wtest: fail * testuser/vulntest- successful | Pass |
|  | Connection via SSH. | ssh [root@192.168.0.102](mailto:root@192.168.0.102)   * root/centos | Login via SSH | * login with root/centos – successful.   A computer screen with white text  AI-generated content may be incorrect. | Pass |
|  | Connection via SSH. | ssh  [user @192.168.0.102](mailto:root@192.168.0.102)   * user:wtest | Login via SSH | * login with user:wtest fail. | Fail |
|  | Connection via SSH. | ssh  [testuser @192.168.0.102](mailto:root@192.168.0.102)   * testuser/vulntest | Login via SSH | * login with testuser/vulntest succesfull | Pass |
|  | Connect to port 80 HTTP. | In a web browser enter the IP address of the FTP server.  192.168.56.102 | Open the admin web page of the FTP server in the browser. | Open the page successfully.  A screenshot of a computer  AI-generated content may be incorrect. | Pass |
|  | Browser connection with valid credential. | Enter in the following URL in a browser:  ftp:// testuser: vulntest@192.168.56.102 | Open the page in the browser | Unable to open a page | Fail |
| Testing after Login | | | | | |
|  | Identify supported commands. | Connect to the:  ftp 192.168.56.102  enter: help | List with supported commands to be displayed. | List with commands obtained.A screenshot of a computer program  AI-generated content may be incorrect. | Pass |
|  | Identify the current directory. | After logging, execute in the terminal:  ftp> pwd | Directory name to be displayed. | Directory identified.  A close up of a sign  AI-generated content may be incorrect. | Pass |
|  | Gathering directories information after login. | Logged in the FTP server. Run in the terminal.  ls -al | Directory listed. | Information obtained.  A screen shot of a computer  AI-generated content may be incorrect. | Pass |
|  | Download files from FTP | Enter in Kali Linux:  wget -m ftp://testuser:vulntest@192.168.56.102  A screen shot of a computer  AI-generated content may be incorrect. | Files to be downloaded | Seven files were downloaded.A screenshot of a computer  AI-generated content may be incorrect.  A screen shot of a computer  AI-generated content may be incorrect. | Pass |
|  | Tyr to read configuration file | Login via:  ssh [testuser@192.168.56.102](mailto:testuser@192.168.56.102)  cat ~/bash\_profile | The configuration file should not open. | The file was open.A screenshot of a computer program  AI-generated content may be incorrect. | Fail |
|  | Try downloading sensitive files | After logging, execute in the terminal:  ftp> cd ..  ftp> ls -al  ftp >get .bash\_profile  ftp >get .bash\_logout  ftp >get .bashrc | Unable to download the files. | Configuration files downloaded.  A screen shot of a computer screen  AI-generated content may be incorrect. | Fail |
|  | Make folder. | After logging, execute in the terminal.:  ftp> mkdir penfolder | Unable to create a folder. | Folder creation failed.A close up of white text  AI-generated content may be incorrect.  Folder created. | Fail |
|  | Change directory. | After logging, execute in the terminal:  ftp> cd ..  ftp>ls -al | Should not be able to change directory. | A screenshot of a computer  AI-generated content may be incorrect. | Fail |
|  | Check if FTPS is enabled | In Kali Linux terminal run:  nmap --script=ftp-anon,ftp-syst -p 21 192.168.56.102 | FTPS to be enabled. | FTPS is not enabed.A screenshot of a computer  AI-generated content may be incorrect. | Fail |

# Appendix 2 Applied hardening

Back to [Hardening Applied](#_Hardening_Applied)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Description | Steps to reproduce | Expected Result | Actual Result | Status |
| Information Gathering | | | | | |
|  | Check the version of the kernel | Log like root user.  Run I the terminal:  # uname -r  #yum list kernel | The last available kernel to be installed. | As expected.  A computer screen shot of a computer code  AI-generated content may be incorrect.  A screen shot of a computer  AI-generated content may be incorrect. | Pass |
|  | Fix credentials disclosure. | Open the virtual box.  Open the description section on the FTP virtual machine. | No sensitive information to be displayed. | As expected.  A screen shot of a computer  AI-generated content may be incorrect. | Pass |
|  | Test the password policy. | Open the terminal of the FTP server try to change the password.  # passwd root  Try to set a password that does not align with the password policy. (length less than 12, without uppercase or lowercase or special characters). | Unable to create password that do not align with the policy. | As expected.A screenshot of a computer screen  AI-generated content may be incorrect. | Pass |
|  | Check if port 80 is closed. | From the Kali Linux terminal check all ports with the following command:  Nmap -sV <IP> | Port 80 must be in STATE ‘closed’. | As expected.  A screenshot of a computer program  AI-generated content may be incorrect.  The IP of the FTP server is changed because the network settings of the VM were changed to provide internet access for the update of the kernels. | Pass |
|  | Test SSH restriction for non-administrators. | Open terminal in kali Linux and try to connect with the FTP server with normal user.  $ ssh testuser@<ip of the FTP) | Non-administrators unable to connect with the server.  Administrators can connect. | As expected.  Testuser - unable.  A computer screen with white text  AI-generated content may be incorrect.  ‘It’ user allowed to login.  A screenshot of a computer  AI-generated content may be incorrect. | Pass |
|  | Check the list with users | Start the FTP VM.  Check the usernames on the initial login prompt. | All departments to be added like users. | As expected.A screenshot of a computer  AI-generated content may be incorrect. | Pass |
|  | Try to open home directory that do not belong to the user. | Login with normal user (sales, managers)  Go to home and try to open another user’s folder. | Unable to open the folder. | As expected.  A close-up of a computer code  AI-generated content may be incorrect. | Pass |
|  | Test the FTPS connection. | Run in the terminal of Kali:  openssl s\_client -connect 192.168.56.104:21 -starttls ftp | Secure connection to be verified. | As expected  A screenshot of a computer  AI-generated content may be incorrect. | Pass |
|  | | | | | |
|  |  |  |  |  |  |
|  | | | | | |
|  |  |  |  |  |  |