# PENETRATION TESTING REPORT

**BY**

**VIJAYAMURUGAN SARAVANAN**

**A20563170**

# Executive Summary

This report outlines the penetration testing process conducted on a Windows Server 2019 target system (IP: 172.27.78.114) to identify vulnerabilities and assessing system security. Using Kali Linux as the attacker machine (IP: 172.27.74.238) These vulnerabilities were discovered in the following:

**1. FTP Misconfiguration:** Anonymous login was available at the FTP service of the target (port 21) and the sensitive files were accessible.

**2. Weak Credentials:** The Administrators group contained the espresso user account, but the password hint for it meant the owner of the password combination could gain access to the account when authenticating the plaintext password.

**3. Improper Access Control:** Thanks to having administrative privileges on the espresso account, someone with access to it had complete control over the system.

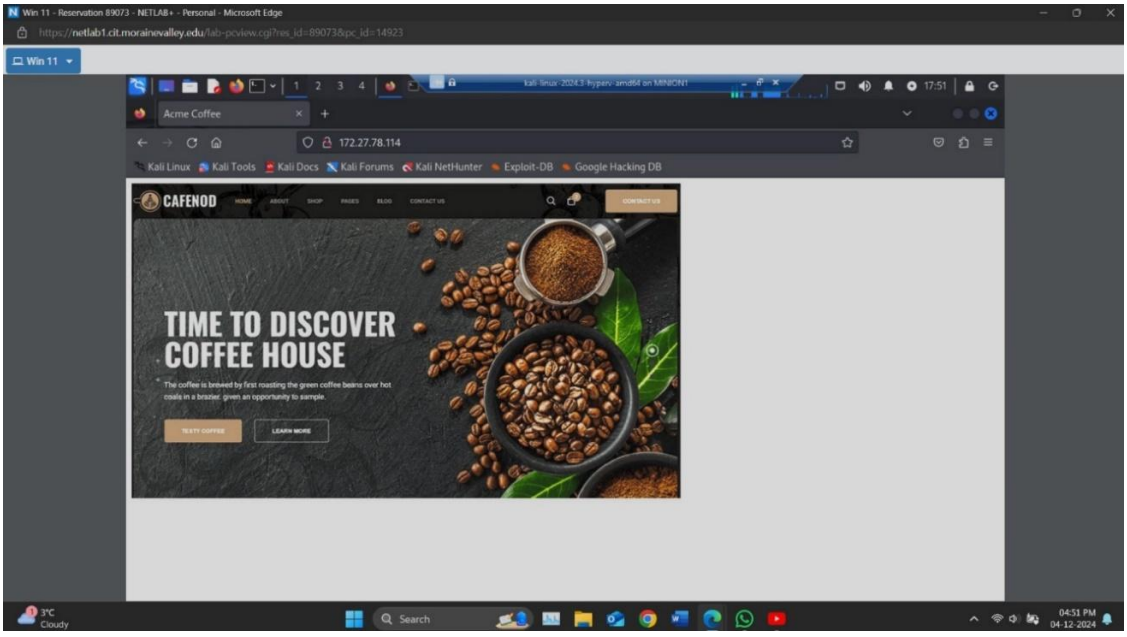
These vulnerabilities were exploited in the exploitation process by which the password of the Administrator account is reset so that the system becomes accessible. Recommendations for these vulnerabilities are provided in terms of mitigation strategies to reduce system's overall security posture.

# Technical Analysis

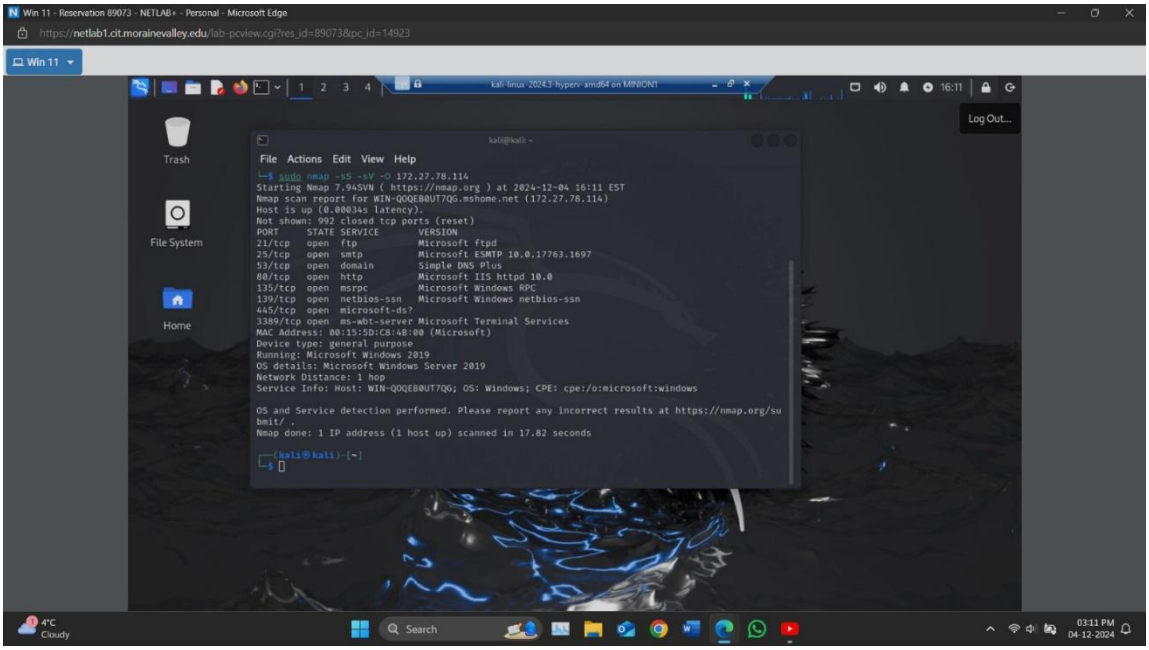
### Step 1: Scanning the Target System

An **Nmap scan** identified the following open ports and services:

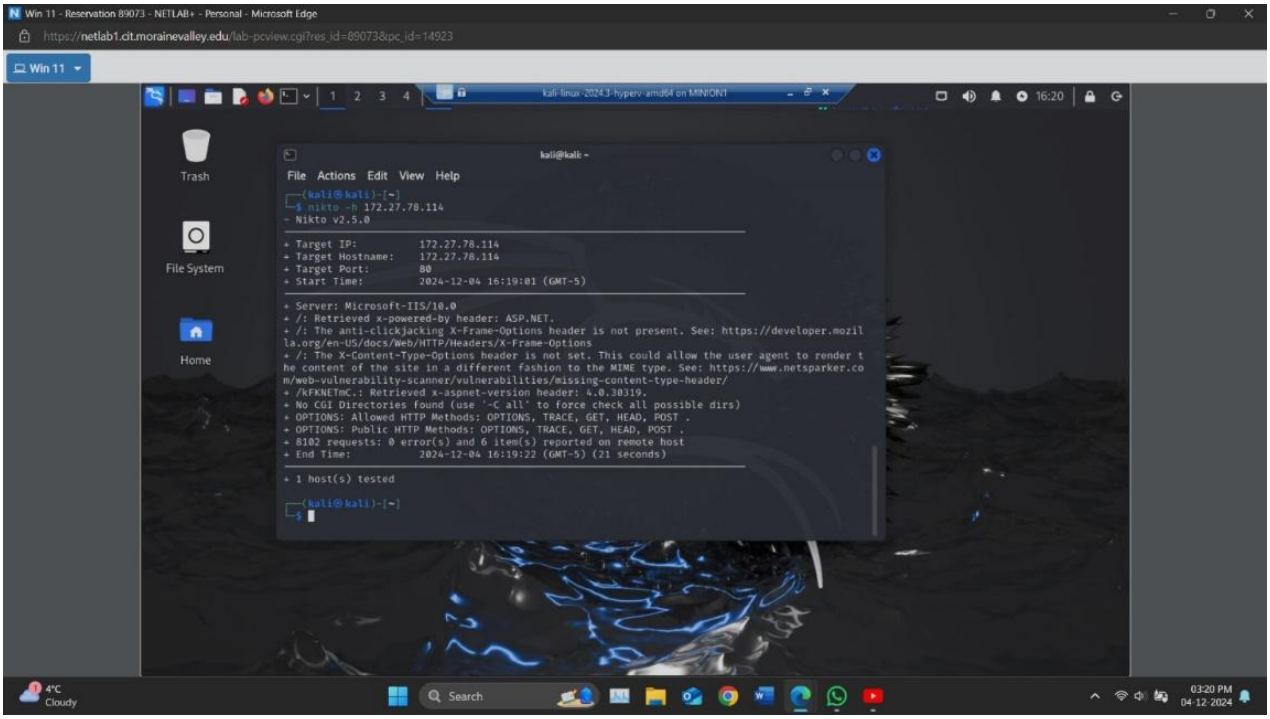
- **FTP (21)**: Allowed anonymous login.
- **HTTP (80)**: Hosted a static webpage.



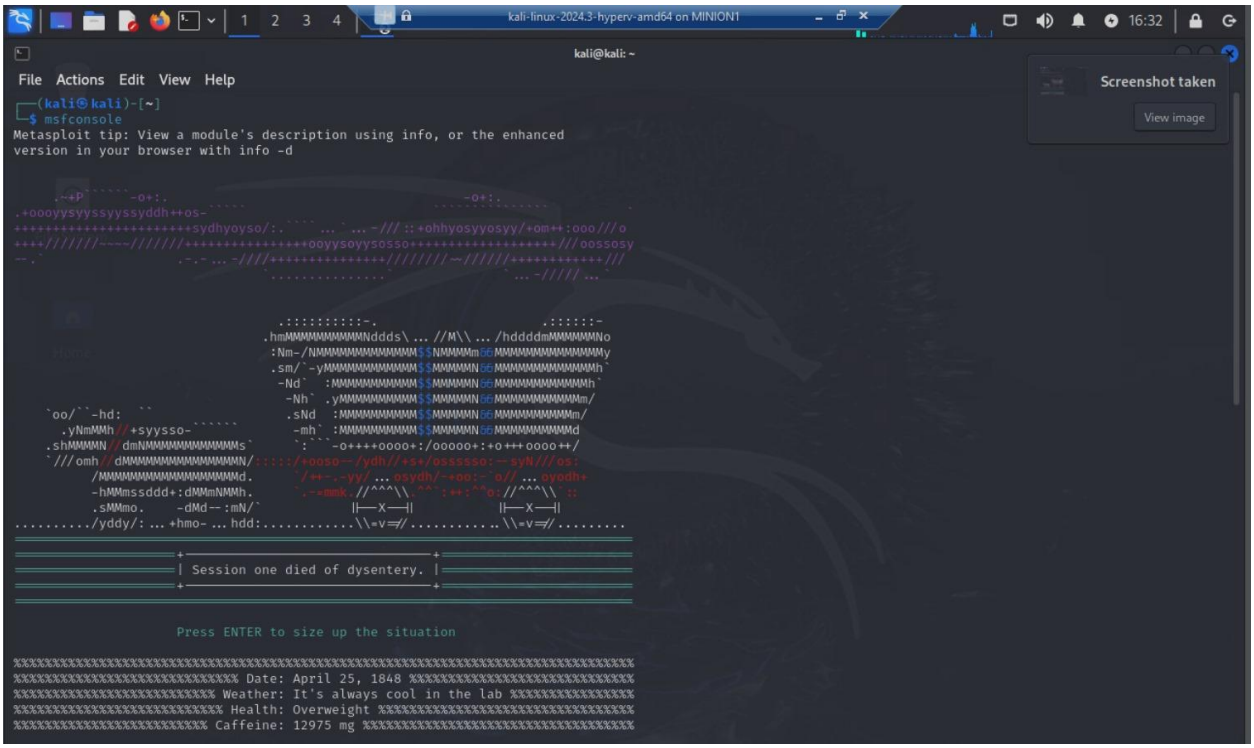
- **SMB (139, 445)**: No anonymous session allowed.
- **RDP (3389)**: Indicated Remote Desktop capability.

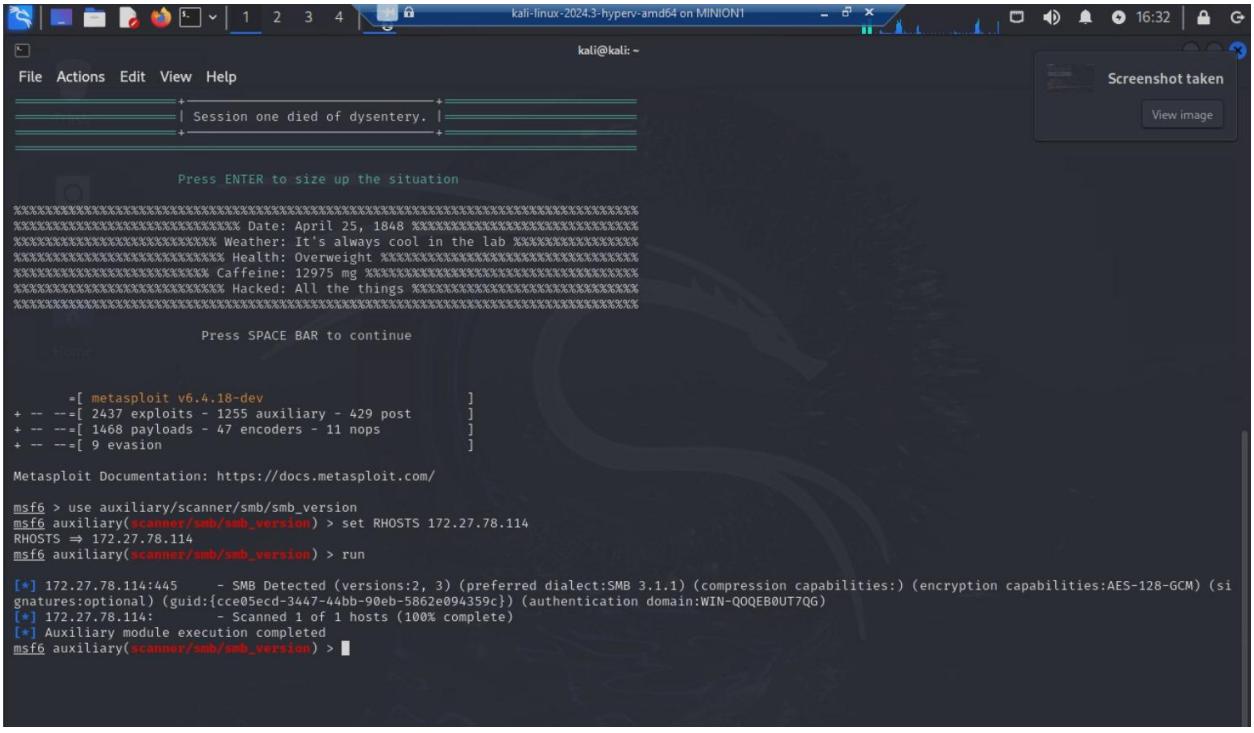



**Nikto scan –** for the vulnerabilities present

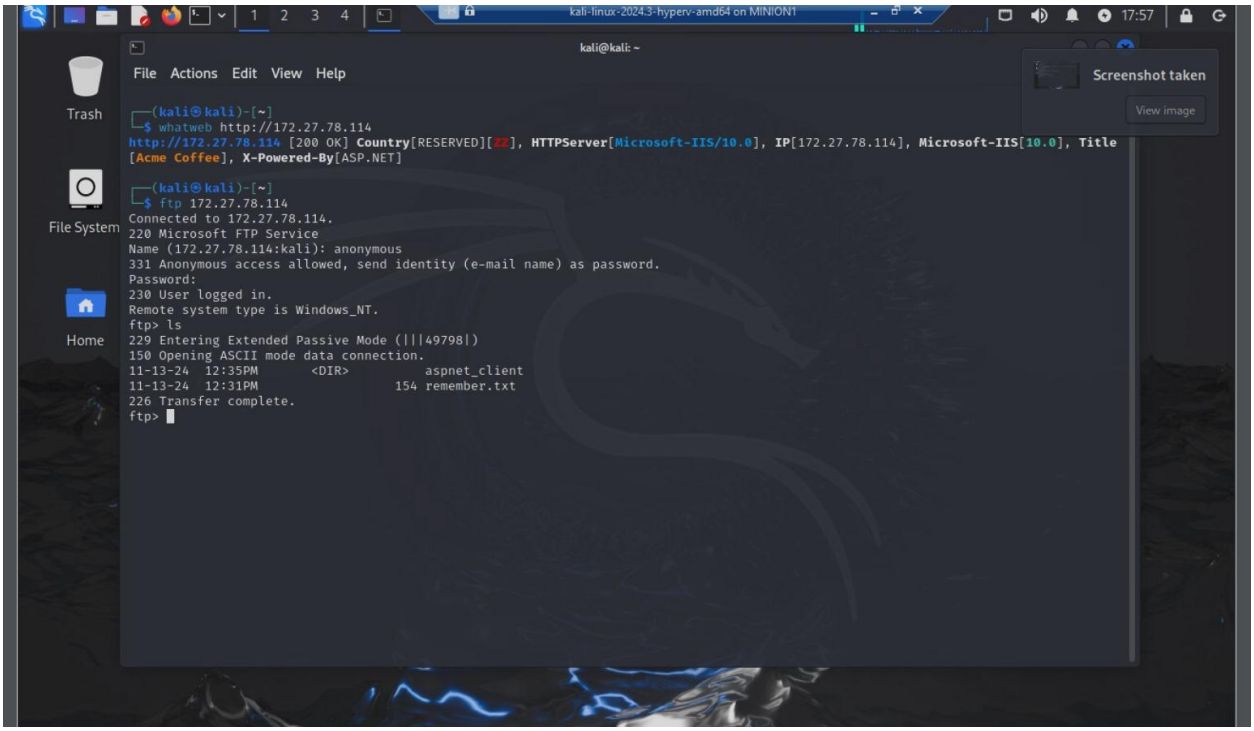


## Metasploit scan for smb version



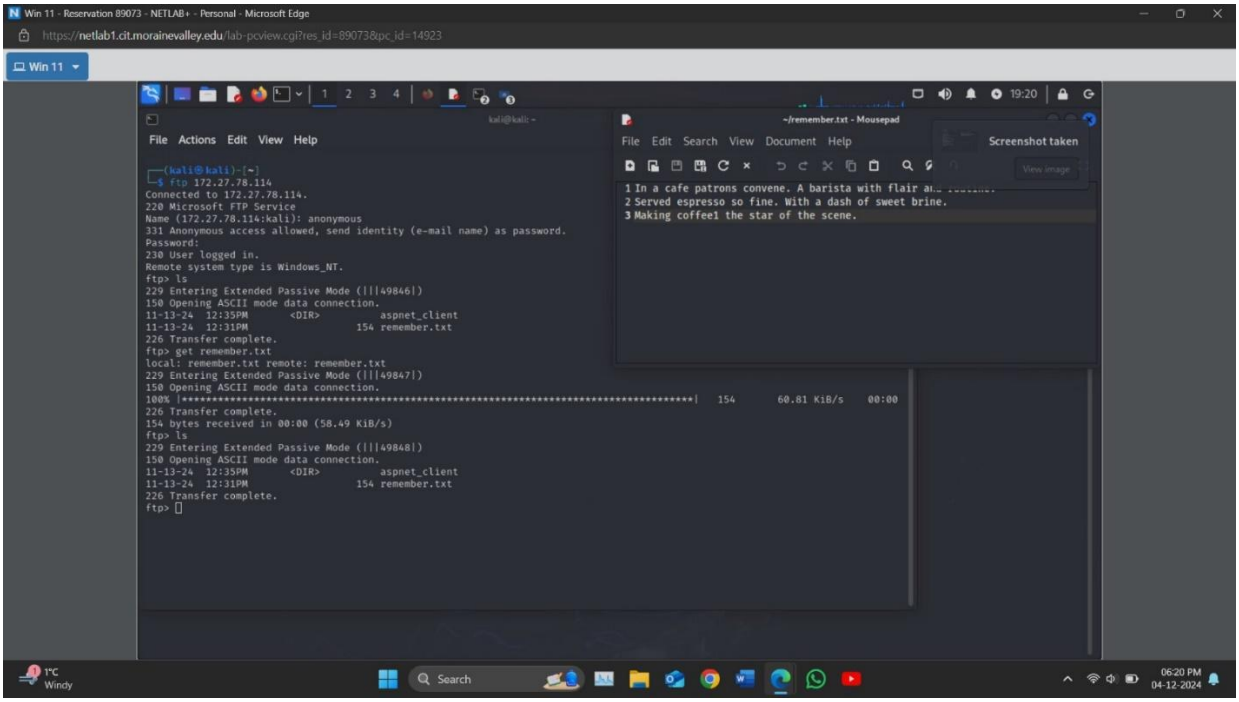



## Step 2: FTP Vulnerability Exploitation

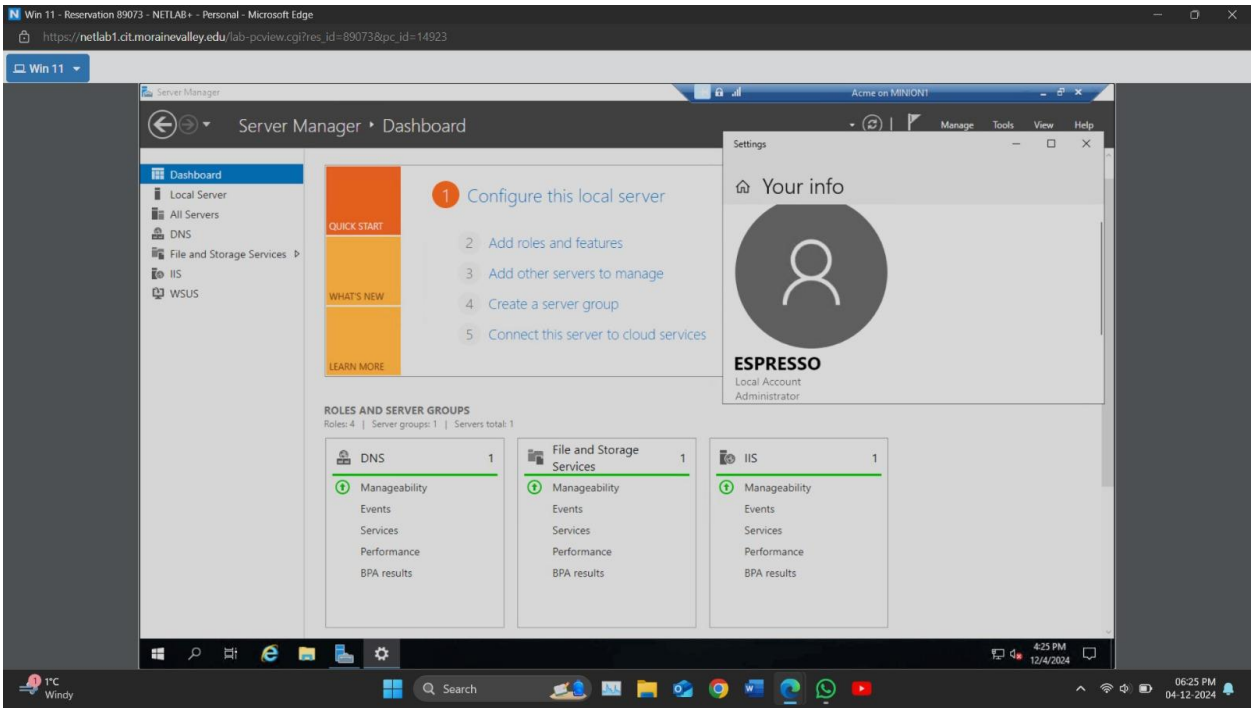



The FTP server allowed **anonymous login**, exposing two items:

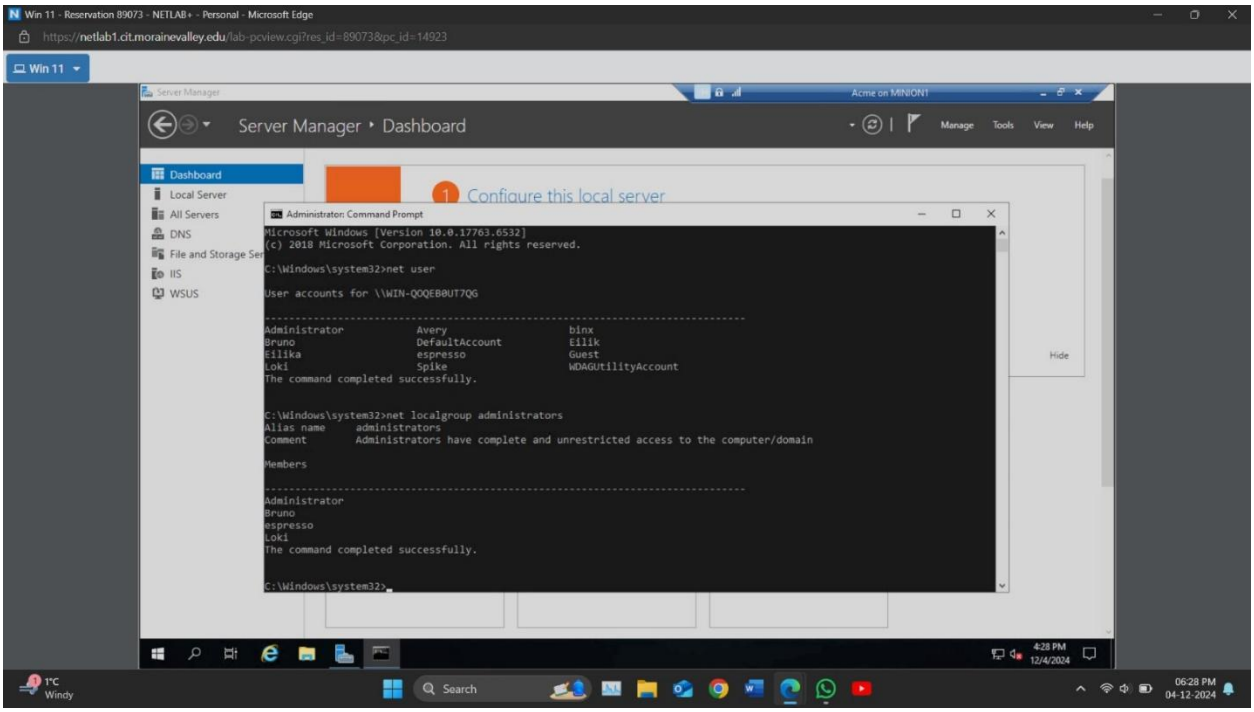
- Directory: aspnet_client
- File: 154 remember.txt



The file contained a riddle and a password hint (coffee1), which facilitated login to the **espresso** account.




## Step 3: Privilege Escalation via Admin Group Membership

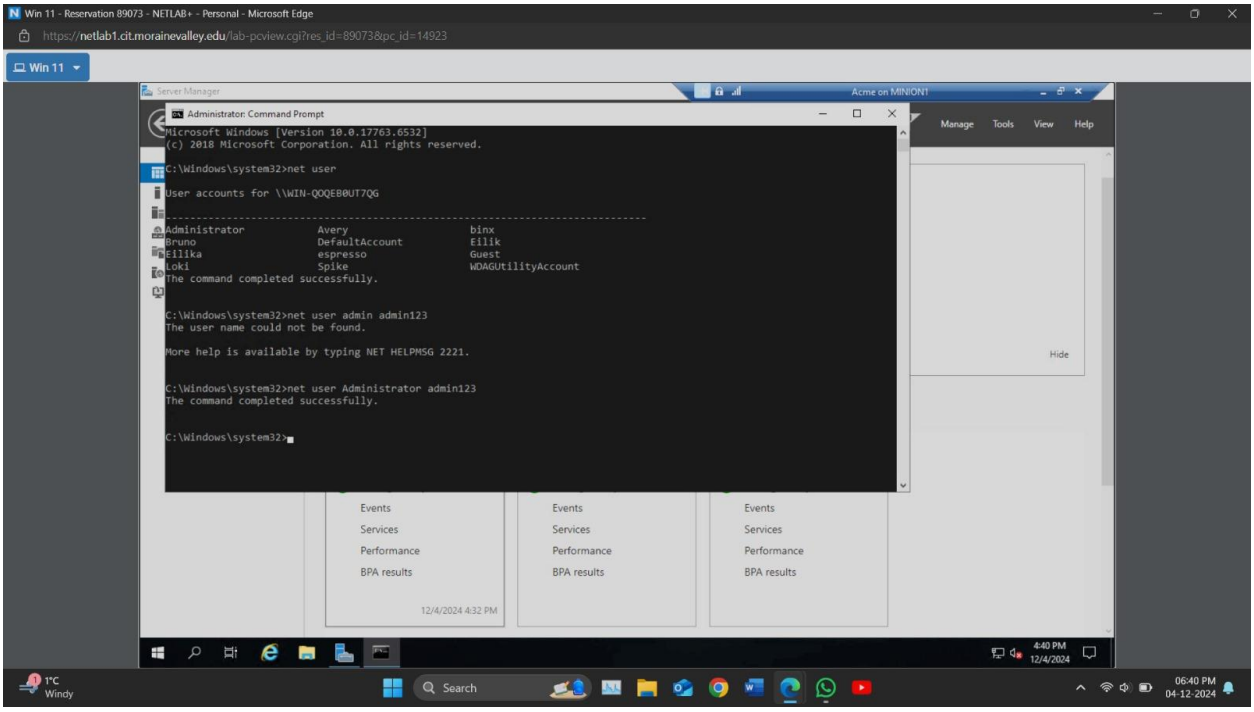



Upon logging into the **espresso** account, it was found to be part of the **Administrators** group.

This allowed execution of the following administrative command to reset the **Administrator** account password:

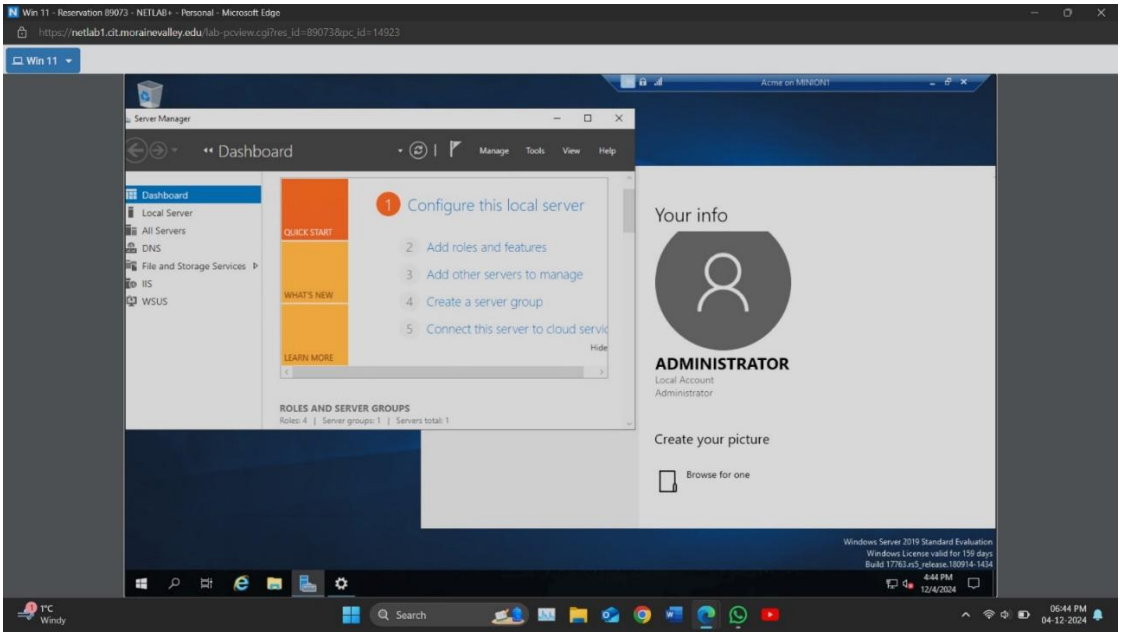
net user Administrator admin123

where admin123 is the new password which was set to the Administrator account.




### Step 4: Full System Access

With the **Administrator** account credentials, full control over the system was obtained, including access to other user accounts and sensitive data.



# Conclusion

During the penetration test we found some critical misconfigurations of the target system, that is, weak credential management, improper access control and insecure FTP configuration. Because of these vulnerabilities an attacker was able to escalate privileges and get root.

The risks must be mitigated, along with the system security being strengthened to keep such exploitation from happening.

**Mitigation Strategies**

1. Disabling Anonymous Login – and using secure protocols such as FTPS, SFTP.
2. Strengthening Password Policies - BYPASSING strong, complex passwords, and NEVER storing plaintext password hints at locations that are easily seen.
3. Limit Administrative Privileges – Admitting that you can't do everything can be first step for limiting administrative privileges for essential accounts only with regularly checking for the group memberships and permissions.
4. From enable Logging and monitoring you can monitor login attempts and access logs for suspicious activities. Now you can configure alerts for Unauthorized Access or Privilege Escalation.
5. No Vulnerabilities - Anything that has an exploit risk associated with it, should be removed or patched thoroughly.

# References


- Kali Linux tools: **Nmap**, **enum4linux**, **smbclient, whatweb, nikto.**
- Windows Command-line utilities: net user
- OWASP Secure Configuration Guidelines