**SMB Enumeration**

SMB (Server Message Block) is a protocol for sharing files over networks. It lets apps on computers read and write files and ask for services from server programs in a network of computers.

SMB (Server Message Block) enumeration has an impact on probing SMB services to collect information about shared resources, user accounts, and the setup of the target system. This procedure can reveal important information that can be helpful in grasping the network topology and identify potential vulnerabilities.

**The versions of SMB:**

### **SMB1 (SMBv1)**

SMB1 was first introduced by IBM in the early 1980s. Its main goal was to grant the network access to DOS file systems. When it was first developed, it was indeed very innovative; however, compared to the present times, SMB1 became inefficient and not secure enough.

**How SMB1 Works:**

* **16-bit Packet Transmission:** SMB1 employed 16-bit packet transfer to pass information between systems. Since the packet size was 16 bits, there was a certain overhead, and the data transfer performance was compromised.
* **File Sharing:** SMB1 supported file sharing on a network without encryption and had no advanced security features.
* **CIFS (Common Internet File System):** The popular Microsoft dialect from 1996, commonly associated with SMB1, offered much stronger file-sharing capabilities. However, it shared all the SMB1 weaknesses.

### **SMB2 (SMBv2 or SMB 2.0)**

Microsoft released SMB2 with Windows Vista in 2006 and Windows Server 2008, marking the first version completely overhauled with an emphasis on performance and security enhancements over the original version.

**How SMB2 Works:**

* **Larger Packet Sizes:** The size of the packet increased to 32-bit for SMB2 and the file handles 128-bit. Resultingly, it is fast on transfers of files and even handling of data.
* **Reduced Subcommands:** SMB2 streamlined operations by reducing the number of subcommands from over 100 in SMB1 to fewer than 20, cutting down on network "chatter" and making the protocol more efficient.
* **Performance Improvements:** SMB2 introduced several performance-enhancing features:
  + **Opportunistic Locking (Oplocks):** Allows clients to lock files locally and cache changes before committing them to the server, reducing the need for constant network communication.
  + **Durable Connections:** SMB2 introduced mechanisms to maintain connections even after temporary network failures.
  + **Caching:** Client-side caching reduced the need for repeated file access requests, leading to better performance.

### 

### **SMB3 (SMBv3)**

SMB3 was initially named SMB 2.2 but later renamed it to **SMB 3.0** when it came out with **Windows 8** and **Server 2012**. SMB3 brought big steps forward, especially in terms of security and performance.

**How SMB3 Works:**

* **SMB Multichannel:** SMB3 introduced the ability to use multiple network connections for a single SMB session, significantly improving data transfer speeds and reliability. This feature is particularly beneficial for high-availability and high-throughput environments.
* **End-to-end Encryption:** Unlike SMB1 and SMB2, SMB3 introduced **end-to-end encryption**, allowing data to be securely transmitted between clients and servers without the need for a VPN. Encryption ensures that even if data is intercepted, it cannot be read by unauthorized parties.
* **Improved Performance:** SMB3 further improved file transfer speeds and efficiency, especially in environments with large file sizes or where high throughput is required.

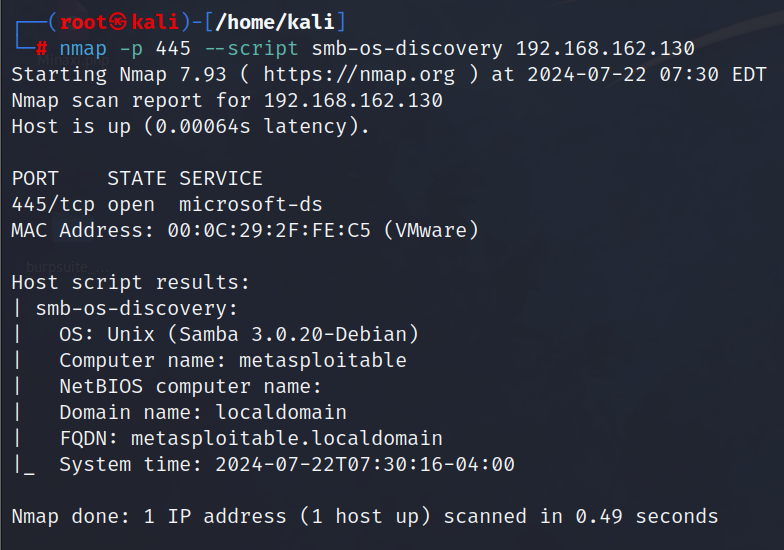
|  |  |
| --- | --- |
| SMBv1 | It is obsolete, insecure, and should not be used in modern environments due to its vulnerability to ransomware and MITM attacks. |
| SMBv2 | It offers better performance and security but still lacks modern encryption standards. It is suitable for legacy systems but should be updated to more recent versions where possible. |
| SMBv3 | It is the most secure and performant version, offering encryption, multichannel communication, and strong integrity protections. SMB 3.1.1 is the latest and most secure implementation, making it ideal for modern networks. |

### **Tools and Techniques for SMB Enumeration**

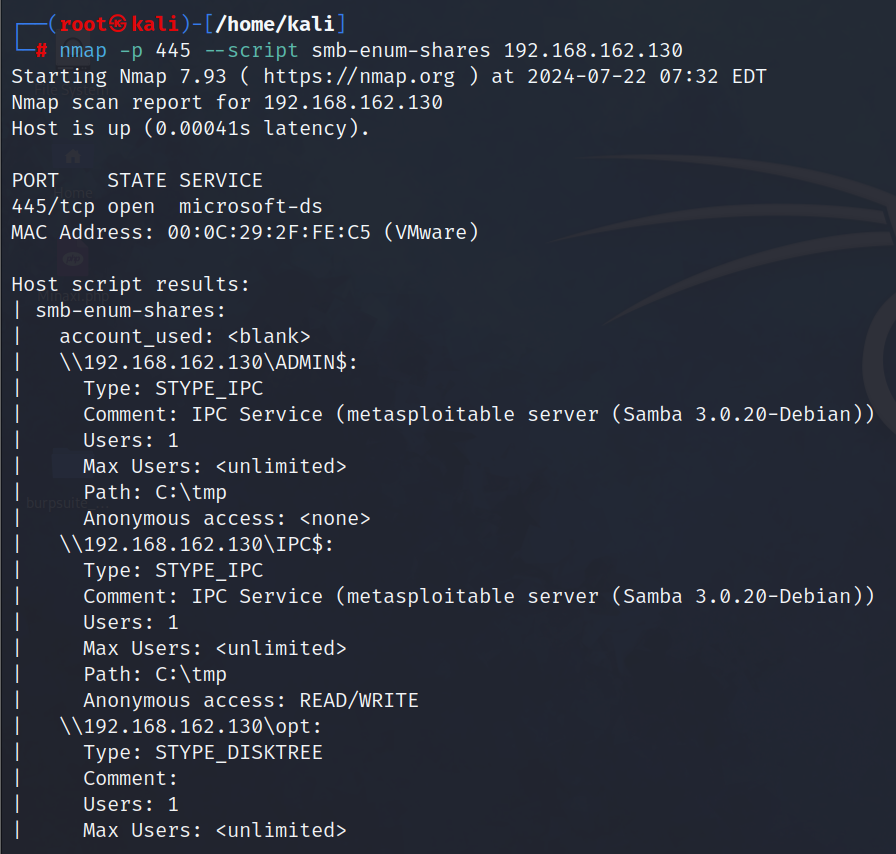
#### **1. Using Nmap for SMB Enumeration**

Nmap, a powerful network scanning tool, includes several scripts specifically designed for SMB enumeration.

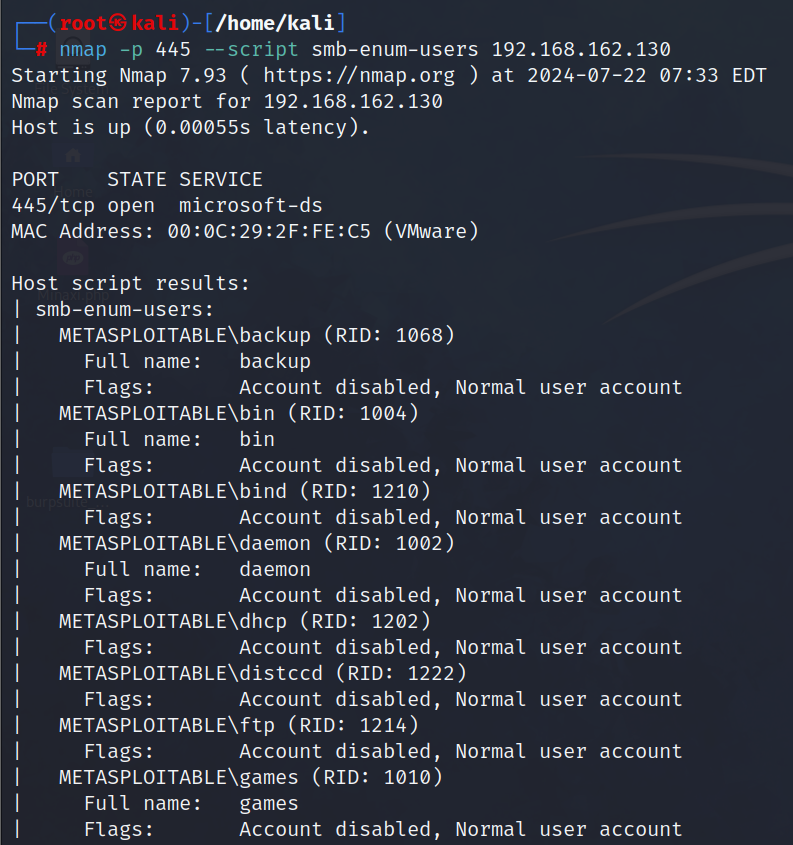
* **Basic SMB Version Detection**: This command detects the SMB version and gathers basic OS information.



* **Enumerating SMB Shares**: This script enumerates the shared folders on the target system.



* **Enumerating SMB Users**: This script lists user accounts on the target system.



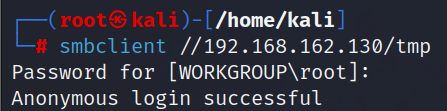
#### **2. Using SMBclient**

smbclient is a command-line tool that helps you interact with SMB shares similarly to an FTP client.

* **Listing Shares:** This command lists all available shares on the target system.

****

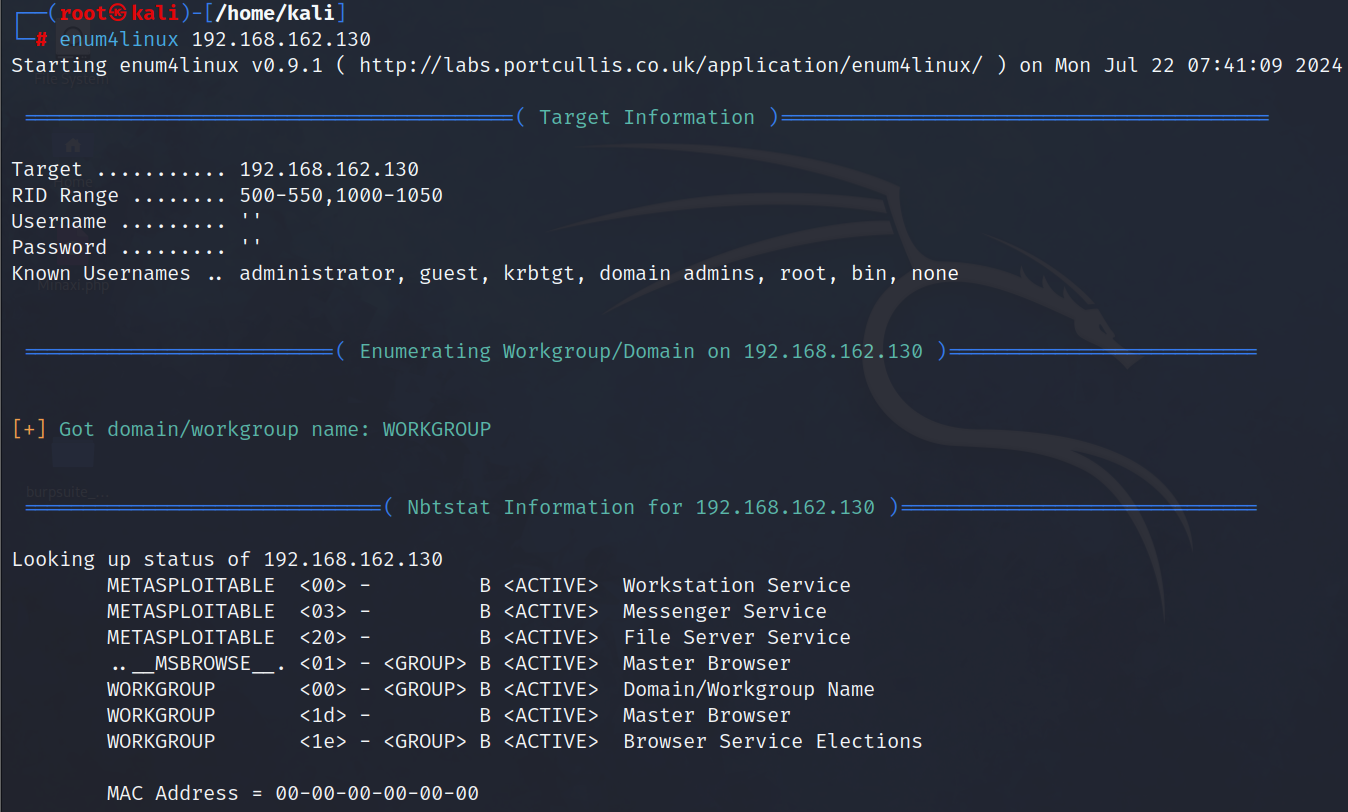
* **Accessing a Share:** This command connects to a specific share on the target system.

****

#### **Using Enum4linux**

**enum4linux** is a tool specifically designed for enumerating information from Windows and Samba systems.

* **Running Enum4linux:**

****

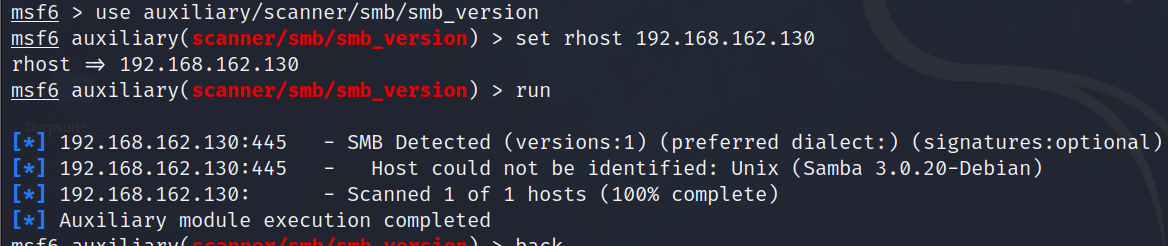
#### **4. Using Metasploit Framework:**

Metasploit includes modules for SMB enumeration that can automate the process and find vulnerabilities.

* **Search for SMB Modules**:  
  search smb
* **Use the SMB Version Scanner**:  
  use auxiliary/scanner/smb/smb\_version

set RHOSTS <target\_ip>

run



This module identifies the SMB version.