SMB analysis

Server Message Block (**SMB**) is an application-layer protocol, which is commonly used to provide file and printer sharing services. Moreover, it is also capable of handling the shared services between serial ports and laid miscellaneous communications between different nodes on the network. It is also known as **CIFS** (**Common Internet File System**).

SMB is purely based on a client-server architecture and has been implemented on various operating systems such as Linux and Windows. **Network Basic Input Output System** (**NetBIOS**) is an integral part of the SMB protocol, which implements the transport service on Windows systems. NetBIOS runs on top of the TCP/IP protocol (NBT) and thus allows each computer with a unique network name and IP address to communicate over **Local Area Network** (**LAN**).

Additionally, the DCE/RPC service uses SMB as a channel for authenticated **inter-process communication** (**IPC**) between network nodes. This phenomenon allows the communication between processes and computers to share data on the authenticated channel. The NetBIOS services are commonly offered on various TCP and UDP ports (`135` , `137` , `138` , `139` , and `445`). Due to these superior capabilities and weak implementation of the SMB protocol, it has always been a chief target for hackers. The number of vulnerabilities have been reported in past, which could be advantageous to compromise the target. The tools presented in this section will provide us with useful information about the target, such as the hostname, running services, domain controller, MAC address, OS type, current users logged in, hidden shares, time information, user groups, current sessions, printers, available disks, and much more.

> **Note**
>
> More information about SMB, NetBIOS, and other relevant protocols can be obtained at http://timothydevans.me.uk/nbf2cifs/book1.html.

Impacket Samrdump

Samrdump is an application that retrieves sensitive information about the specified target using **Security Account Manager** (**SAM**), which is a remote interface that is accessible under the **Distributed Computing Environment** / **Remote Procedure Calls** (**DCE**/**RPC**) service. It lists out all the system shares, user accounts, and other useful information about the target's presence in the local network.

To start Impacket Samrdump, execute the following commands in your shell:

```
# cd /usr/share/doc/python-impacket-doc/examples/samrdump.py
# python samrdump.py
```

The preceding commands will display all the usage and syntax information that is necessary to execute Samrdump. Using a simple syntax, `python samrdump.py user:pass@ip port/SMB` , it will help us run the application against the selected port (`139` or `445`):

```
# python samrdump.py h4x:123@192.168.0.7 445/SMB
Retrieving endpoint list from 192.168.0.7
Trying protocol 445/SMB...
Found domain(s):
 . CUSTDESK
 . Builtin
Looking up users in domain CUSTDESK
Found user: Administrator, uid= 500
Found user: ASPNET, uid= 1005
Found user: Guest, uid= 501
Found user: h4x, uid= 1010
Found user: HelpAssistant, uid= 1000
Found user: IUSR_MODESK, uid= 1004
Found user: IWAM_MODESK, uid= 1009
Found user: MoDesktop, uid= 1003
Found user: SUPPORT_388945a0, uid= 1002
Administrator (500)/Enabled: true
...
```

The output clearly shows us all the user accounts that are held by the remote machine. It is crucial to note that the username and password for the target system is required only when you need certain information that is not available otherwise. Inspecting all the available shares for sensitive data and accessing other user accounts can further reveal valuable information.