26-3-21

SMB

SMB

↳ Server message block.

↳ Server shares resources among clients using SMB
- files
- Hardware
- Storage

↳ Response - request Protocol

SMB - from win 95

SAMBA - uses SMB for Unix os.

↳ SMB uses shared drives which has data to share with clients.
- can contain sensitive info (useful for Attacker).

SMB ports : 139 / 445

Port 139: SMB originally ran on top of NetBIOS using port 139. NetBIOS is an older transport layer that allows Windows computers to talk to each other on the same network.

Port 445: Later versions of SMB (after Windows 2000) began to use port 445 on top of a TCP stack. Using TCP allows SMB to work over the internet.

Enumeration :

Enum4Linux

Enum4linux is a tool used to enumerate SMB shares on both Windows and Linux systems. It is basically a wrapper around the tools in the Samba package and makes it easy to quickly extract information from the target pertaining to SMB.

Usage : enum4linux -<option> <ip>

↳ enum4linux --help
options like -U, -A, -S, -P are used.

eg:) enum4linux -A <ip>

// It retrieves all as output including, Userlist, sharedrive list, password policy, machine details, group details, os details, os version, SMB version etc,

we use → SMB client

By using the above information, we use any SMB client Application to access the share drives.

Exploitation:

Note: SMB also support Anonymous SMB share access. (see below)

Smbclient

c) It is used to log in to SMB server & access Resources (like FTP client).

Usage:

```
Smbclient //<ip>/<share name> -U <username>
```

c) After logged into smb server, issue help command to list all the available command. (get command is used to download file present in SMB server into our local machine).

When misconfigured & it allows anonymous SMB share access which may be exploited to get shell into it