SMB Basics

SMB - Server Message Block Protocol - is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network

### **Enumeration**

* Conduct a port scan on the target. Usually found on ports 139/445
* **Enum4Linux** tool can be used for enumerating SMB shares on Win and linux

### **Exploitation**

smbclient -L - lists shares in smb

smbclient \\ip-address\share-name - access share

-U [name] : to specify the user

-p [port] : to specify the port

* Check for annonymous login
  + if successful - check for interesting files
* [CVE-2017-7494](https://www.cvedetails.com/cve/CVE-2017-7494/) that can allow remote code execution by exploiting SMB

#### SMB Nmap scripts

* smb-protocols : Tells what protocols and dialects that server uses
* smb-security-mode: Tells about security mode
* smb-enum-sessions: enumerates sessions , can try login by providing uname and password
* smb-enum-shares: Enumerate shares
* smb-enum-users
* smb-enum-domains
* smb-enum-groups
* smb-enum-services
* smb-ls: list as in linux
* smb-os-discovery : Shows OS details

#### SMBMap

**smbmap -u usernmae -p password or "" -d . -H hostip** : Shows shares and access

**smbmap -u usernmae -p password or "" -H hostip -x 'ipconfig'** : Runs ipconfig code via SMB

**smbmap -u usernmae -p password or "" -H hostip -L** : Lists all the drives

**smbmap -u usernmae -p password or "" -H hostip -r 'C$'**: Connects to C drive and lists the contents

**smbmap -u usernmae -p password or "" -H hostip --upload 'path/to/source' 'C$\path\to\dst'** : uploads file to destination in C drive

**smbmap -u usernmae -p password or "" -H hostip --download 'C$\path\to\file'** : downloads file from source in C drive

#### Samba

can use metasploit msf console to enumerate SMB

**use auxiliary/scanner/smb\_version**  
show options to show all options  
set option-name value

run / exploit - runs module

**nmblookup** - lookup information using netbios

**smbclinet** : use to conect to smb

**rpcclient**

inside rpc client we can use the following  
srvinfo - find server info  
enumdomusers - enumerates domain users  
lookupnames admin - gets SID of the admin user

**enum4linux**  
Very powerful tool can get us a lot of info

#### SMB Dictionary attack

* msfconsole
* use auxiliary/scanner/smb/smb\_login
* supply a user pass file
* and other params that we got from enum

**hydra** - can be used for password bruteforce

#### enumerating pipes

msfconsole  
use auxiliary/scanner/smb/pipe\_auditor : can be used to find piped services

can be used for exploitation