**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.

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

**Telnet**

* Telnet is 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.
* syntax: **"telnet [ip] [port]"**

**File Transfer Protocol(FTP)**

* a protocol used to allow remote transfer of files over a network. It uses a client-server model to do this, and- as we'll come on to later- relays commands and data in a very efficient way.
  + Syntax: **“*ftp [IP]*”**

**Hydra**

* 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 much more.
* Sytax: **hydra -t 4 -l dale -P /usr/share/wordlists/rockyou.txt -vV 10.10.10.6 ftp**
  + **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 File System (NFS)**

* Allows a system to share directories and files with others over a network. By using NFS, users and programs can access files on remote systems almost as if they were local files. It does this by mounting all, or a portion of a file system on a server. The portion of the file system that is mounted can be accessed by clients with whatever privileges are assigned to each file.
* use /usr/sbin/showmount -e [IP]
* First, use "*mkdir /tmp/mount*" to create a directory on your machine to mount the share to
* Use **sudo mount -t nfs IP:share /tmp/mount/ -nolock**
  + **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
* Change directory to where you mounted the share- what is the name of the folder inside?
* Have a look inside this directory, look at the files.

**MetaSploit**

To use metasploit run this command: msfconsole

**SMTP (Simple Mail Transfer Protocol)**

**Key Points:**

1. The module focuses on enumerating SMTP servers using Metasploit.
2. SMTP typically runs on port 25.
3. Two Metasploit modules were used:
   * smtp\_version: to fingerprint the mail server
   * smtp\_enum: to enumerate users
4. Steps taken: a. Port scan to identify SMTP port b. Launch Metasploit using 'msfconsole' c. Use smtp\_version module to identify mail system (Postfix) d. Use smtp\_enum module with a wordlist to find valid usernames
5. Important Metasploit commands:
   * 'options' to view module options
   * Set RHOSTS to target IP
   * Set USER\_FILE to wordlist path
6. The enumeration successfully identified the username 'administrator'
7. Alternative tools mentioned: smtp-user-enum (useful for Solaris systems)
8. SMTP commands VRFY and EXPN can be used for manual enumeration
9. The next step is to bruteforce the SSH login using Hydra.
10. Hydra syntax used: hydra -t 16 -l USERNAME -P /usr/share/wordlists/rockyou.txt -vV MACHINE\_IP ssh Breakdown:
    * -t 16: 16 parallel connections
    * -l [user]: Specifies the username
    * -P [path to dictionary]: Path to password list
    * -vV: Very verbose mode
    * MACHINE\_IP: Target IP address
    * ssh: Protocol to attack
11. The module used rockyou.txt as the wordlist, but mentions other options in /usr/share/wordlists and recommends SecLists.
12. After successfully bruteforcing the password, the next step was to SSH into the server and retrieve the contents of smtp.txt.

**MySQL (Structured Query Language)**

The scenario assumes you found MySQL credentials (root:password) while enumerating a web server. MySQL is typically not the first target, but can be exploited after gaining initial credentials. The module uses Metasploit to enumerate and exploit the MySQL service.

Key steps:

* Port scan to identify MySQL port (3306)
* Manually connect to verify credentials
* Use mysql\_sql module in Metasploit to run SQL commands
* Use mysql\_schemadump to dump database schema
* Use mysql\_hashdump to dump user password hashes

Important concepts:

* Schema = Database in MySQL
* Password hashes are used to store passwords securely

Key findings:

* MySQL version
* Number of databases
* Table names
* Non-default user account discovered
* Password hash cracked using John the Ripper

The module emphasizes the dangers of password reuse across services. Final step involves accessing contents of a MySQL.txt file, likely containing sensitive information.