SkyTower Pentest

Reconnaissance

MITRE Attack (Reconnaissance – gather victim network information)

To being our pentest, right away we jumped into our nmap scan of our network to discover the ip address. This will allow us to take a closer look at the machine, discovering what ports are opened and what are some of the services the machine is running.

Our nmap scans reveal the machines address is 192.168.56.101. Based on the services running the machine is running a website which I connected to later to exploit. Another thing is that the machine does allow user to use secure shell to gain remote access into the machine.

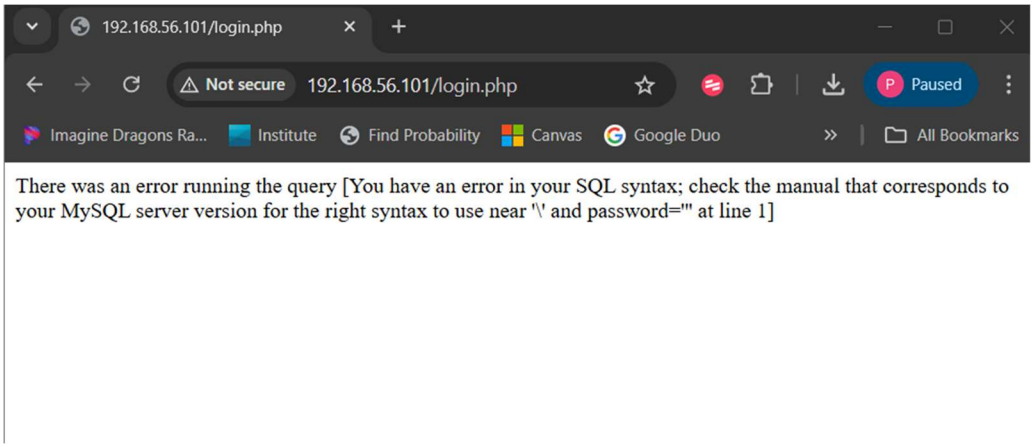
MITRE Attack (Reconnaissance – search victim-owned website)

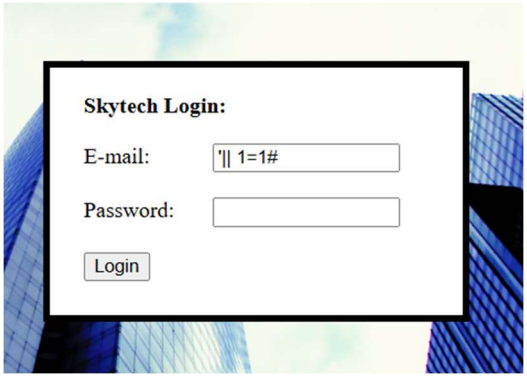
The next step I took was looking at the website of the machine and was met with a login screen. A few things came to mind here to try. First, I tried to enter in a commonly used default password admin: password. This just prompted me with an invalid login attempt. This makes brute forcing more difficult to use. The next thing that I want to attempt is that some website logins are vulnerable to SQL injections.

Initial Access

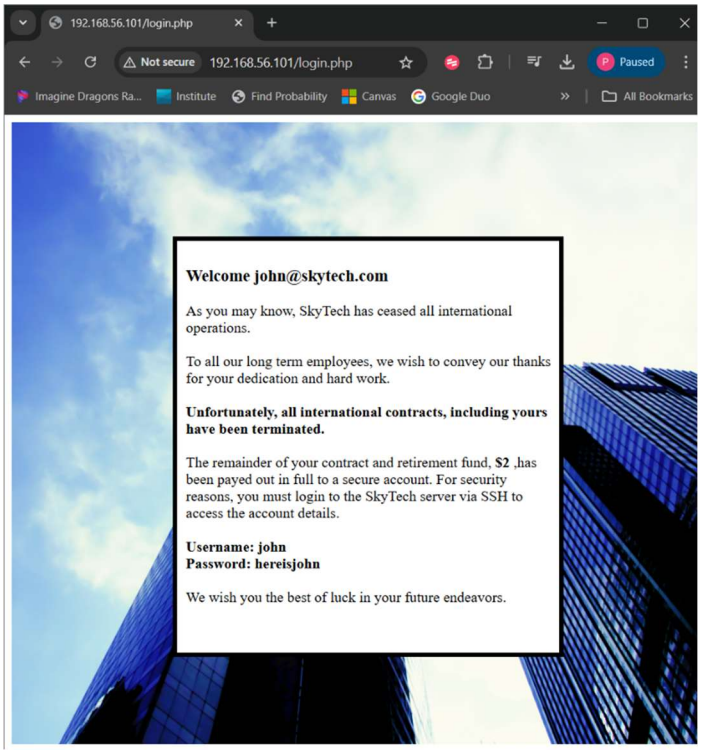
MITRE Attack (Initial Access – exploit public-facing application)

SQL injections will be done to the website's database and based on that query typed in, will search for the necessary input to use for the login credentials. I tried a few common ones based online and eventually found one. Down below is the failed and successful SQL injections query used that gave me access to the machine.





After hitting the login button, the SQL injection ran successfully and was directed to the following page.



Step one was completed of gaining initial access to the machine and also gaining credentials of a user.

MITRE Attack (Execution – command and scripting interpreter using proxychains)

I then used the credentials to login into the machine using ssh protocol. However, when doing the simple ssh command the session would not last very long and would keep closing on me. After doing some research on reddit forms, the suggestion came up to use proxychains as a solution to keep the session open. With that I downloaded proxychains and configured them to my kali machine.

MITRE Attack (Initial Access – Valid Accounts using ssh)

We can use proxychains with ssh to keep the session alive and use John's login credentials to gain access to the machine itself.

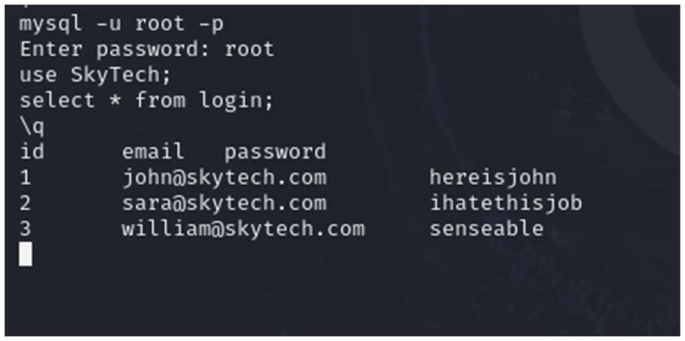
```
┌──(kali㉿kali)-[/etc]
└─$ proxychains ssh john@127.0.0.1 /bin/bash
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  192.168.56.101:3128  ...  127.0.0.1:22  ...  OK
john@127.0.0.1's password:
whoami
john
```

MITRE Attack (Credential Access – Unsecured credentials)

Now that I have access to johns file, I started looking for files that may contain clues for more login credentials and to just see what john has access. By performing a quick list command on the current directory there was file named login.php. This was a clear flag of more credentials do a did a quick cat of the file and was met with the following results.

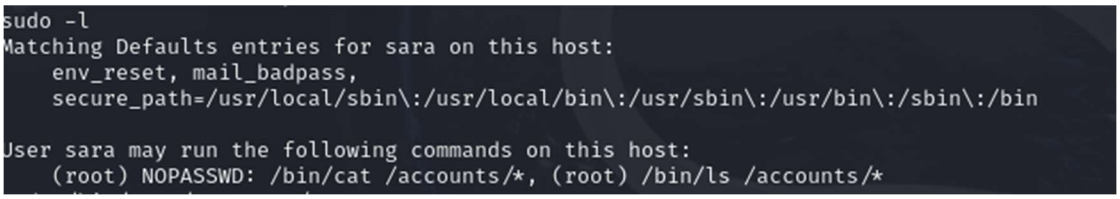
```
cat login.php
<?php

$db = new mysqli('localhost', 'root', 'root', 'SkyTech');

if($db->connect_errno > 0){
    die('Unable to connect to database [' . $db->connect_error . ']');

}

$sqlinjection = array("SELECT", "TRUE", "FALSE", "--","OR", "=", ",", "AND", "NOT");
$email = str_ireplace($sqlinjection, "", $_POST['email']);
$password = str_ireplace($sqlinjection, "", $_POST['password']);
```

We can see the SQL database on the machine has the MySQL user with the password of root. With that information we can run another SQL query on the database to search for more users and their passwords using the new credentials found.



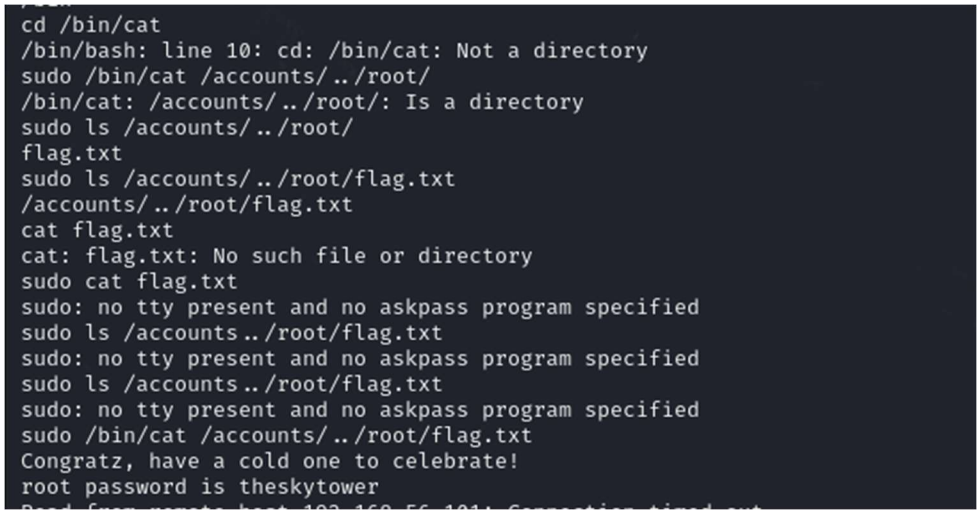
Now we have two new credentials to work with and hopefully we will be able to find a user with sudo rights to files.

The first one is using sara to login to search for sudo privileges.



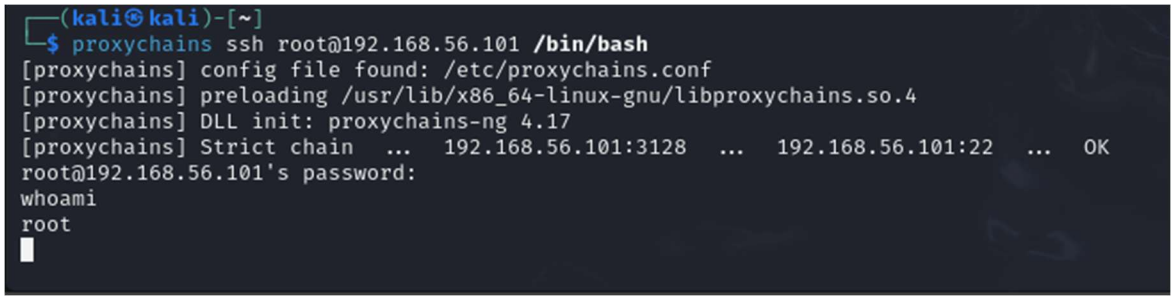
MITRE Attack (Credential Access- Unsecured Credentials root)

Luckily for us she does have rights to read root files on the machine. This is where we continue our search. After a few attempts to see the root directory list, we found a file named flag.txt which I then catted so we could see the contents of the file and inside found the credentials of the root users login information.



MITRE Attack (Privilege Escalation – valid accounts root)

From here we made a quick switch over to the root user to confirm access were able to get in using the credentials found.



Remediations

For the SQL injection a few ways to prevent users from exploiting this is by using input validation that makes sure what the user inputs conform to the expected input formats. Another thing that should be done is using web application firewalls the can help detect and even block SQL injection from attempts.

The next problem is there is too much access to passwords, especially since they are stored in plain sight without even being encrypted. I would suggest doing an audit of all files for exposed passwords and either removing them from the machine or at the very least using encryption software.

When it came to gaining access to the root password, I would suggest that an audit be performed to ensure that no other users have access to root user

information. It is best practice to ensure that the only person that can access root information is the root user and would suggest never storing that password on the machine.

Reflection

For this project there were more new techniques used to break into the machine. The main one that was used was taking advantage of the SQL database. This project was a great opportunity to learn how SQL injections work. It took many attempts not only to find the right SQL query to use on the login page but also again when I was trying to look at the login logs on the database. I found that the most important part of breaking into machines is not the actual action itself but research.