**Informe Profesional del CTF LazyAdmin**

**Introducción:**

El presente informe detalla los hallazgos y progresos realizados en el desafío de la máquina CTF LazyAdmin. Se han llevado a cabo diversas acciones de exploración y análisis para avanzar en el objetivo de resolver el desafío. A continuación, se presentan los hallazgos más relevantes hasta el momento.

**Resumen de hallazgos:**

1. **Escaneo de Puertos:**

Se realizó un escaneo de puertos utilizando la herramienta Nmap, y se obtuvieron los siguientes resultados:

* Puerto 22/tcp: Abierto - Servicio SSH (OpenSSH 7.2p2 Ubuntu 4ubuntu2.8)
* Puerto 80/tcp: Abierto - Servicio HTTP (Apache httpd 2.4.18)

***Comandos:***

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

1. **Enumeración de Directorios:**

Se utilizó la herramienta Gobuster para realizar una enumeración de directorios en el sitio web. Los resultados obtenidos fueron los siguientes:

* /content: Estado 301, Redirección a http://10.10.43.112/content/
* /index.html: Estado 200, Tamaño 11321
* /server-status: Estado 403, Tamaño 277

Además, se llevó a cabo una segunda enumeración de directorios en la ruta /content, obteniendo los siguientes resultados:

* /.hta: Estado 403, Tamaño 277
* /.htaccess: Estado 403, Tamaño 277
* /.htpasswd: Estado 403, Tamaño 277
* /\_themes: Estado 301, Redirección a http://10.10.43.112/content/\_themes/
* /as: Estado 301, Redirección a http://10.10.43.112/content/as/
* /attachment: Estado 301, Redirección a http://10.10.43.112/content/attachment/
* /images: Estado 301, Redirección a http://10.10.43.112/content/images/
* /inc: Estado 301, Redirección a http://10.10.43.112/content/inc/
* /index.php: Estado 200, Tamaño 2198
* /js: Estado 301, Redirección a <http://10.10.43.112/content/js/>

***Comandos:***

* ***gobuster dir -u http://10.10.132.192/ -w /usr/share/wordlists/dirb/common.txt***
* ***gobuster dir -u http://10.10.132.192/content -w /usr/share/wordlists/dirb/common.txt***

1. **Descubrimiento de Credenciales:**

Dentro del directorio /as, se encontró una página de inicio de sesión. Mediante la enumeración del directorio /inc, se obtuvo acceso a varios archivos .php, incluyendo un archivo de copia de seguridad de MySQL llamado "mysql\_backup\_20191129023059-1.5.1". Al examinar el contenido de dicho archivo, se encontraron las siguientes credenciales:

* Usuario: manager
* Contraseña: Password123

Cabe mencionar que el password venia en hash en el archivo y con crackstation desciframos la contraseña

***Comandos:***

* ***Se visito la pagina crackstation***

1. **Acceso al Dashboard de SweetRice:**

Utilizando las credenciales encontradas, se inició sesión en el Dashboard de SweetRice. En la sección de Anuncios (ads), se agregó una secuencia de comandos para establecer una conexión inversa. Se descargó y utilizó el script de shell inverso "php-reverse-shell.php" ubicado en "/usr/share/webshell/php/".

***Comandos:***

* ***Webshell php-reverse-shell.php***

1. Elevación de Privilegios a Root:

Mediante el análisis de los permisos del usuario actual con el comando "sudo -l", se descubrió que se podía ejecutar el archivo "/usr/bin/perl /home/itguy/backup.pl". El contenido de este archivo reveló la ejecución del comando "sh /etc/copy.sh". Modificando el archivo "copy.sh" y ejecutando el comando "sudo /usr/bin/perl /home/itguy/backup.pl", se logró elevar los privilegios a root.

***Comandos:***

* ***sudo -l***
* **echo “/bin/bash”> /etc/copy.sh**
* **sudo "/usr/bin/perl /home/itguy/backup.pl**

**Conclusiones:**

El CTF LazyAdmin presentó una serie de desafíos interesantes relacionados con la enumeración de directorios, el descubrimiento de credenciales, la explotación de vulnerabilidades y la elevación de privilegios. A través del análisis y la exploración cuidadosa de los sistemas y servicios involucrados, fue posible obtener acceso al Dashboard de SweetRice y, finalmente, obtener privilegios de root en la máquina objetivo.

Es importante destacar la importancia de mantener la seguridad de los sistemas, incluyendo la implementación de medidas de protección adecuadas, la gestión adecuada de contraseñas y el seguimiento de las mejores prácticas de seguridad en el desarrollo y la configuración de aplicaciones web.

**Recomendaciones:**

* Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
* Aplicar buenas prácticas de gestión de contraseñas, como el uso de contraseñas fuertes y su rotación periódica.
* Realizar auditorías de seguridad regulares para identificar y corregir posibles vulnerabilidades.
* Limitar los privilegios de usuario y seguir el principio de "menos privilegios".
* Implementar un firewall para controlar el tráfico de red y restringir el acceso no autorizado.