



Hacking Ético

Escaneo

Marco Aravena Vivar

Ingeniería Civil Informática

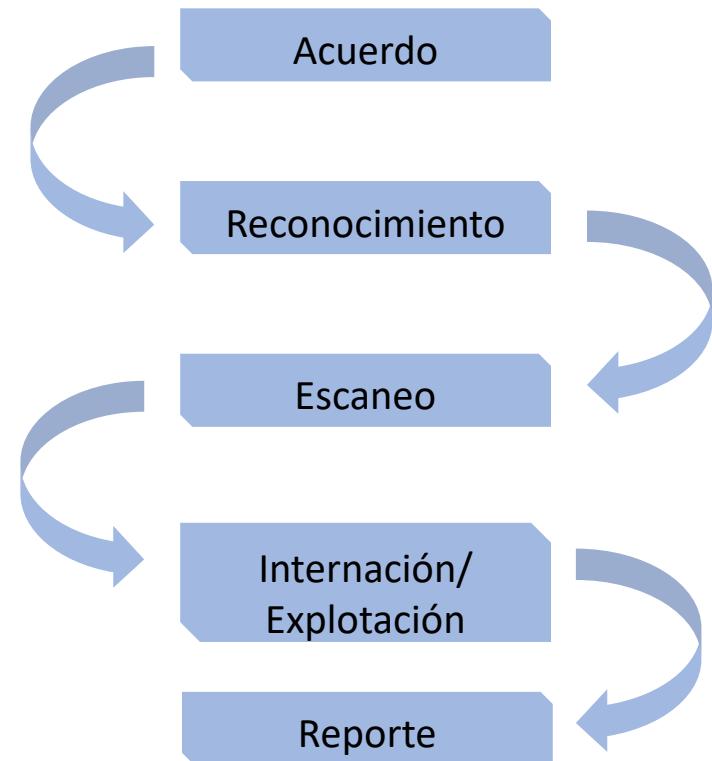


Proceso de Hacking Ético

Repaso

Ingeniería Civil Informática

Proceso de Hacking





TCP/IP

Escaneo

Ingeniería Civil Informática

Características de TCP/IP

TCP (Transmission Control Protocol): Provee un envío de datos confiable dado que verifica que los datos sean entregados a través de la red en forma precisa y con la secuencia correcta.

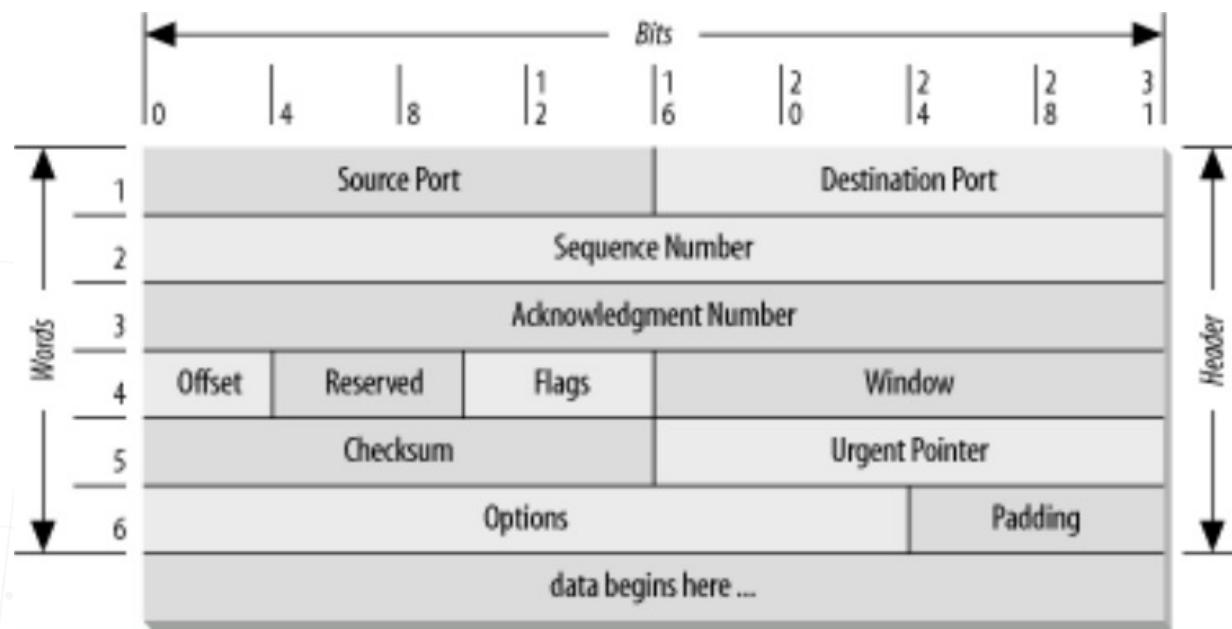


Características de TCP/IP

Positive Acknowledgment with Re-transmission (PAR):

- TCP transmite datos hasta que recibe un OK.
- La unidad de intercambio de datos entre módulos TCP es llamada segmento (segment)
- Cada segmento contiene un checksum que el receptor utilizar para ver si los datos están dañados
- Si no hay daño en los datos, el receptor envía un OK (positive acknowledgment) al emisor
- Si hay daños en los datos, el receptor simplemente descarta los datos.
- Despues de un timeout el emisor retransmite los segmentos de los cuales NO ha recibido un OK.

Formato segmento TCP

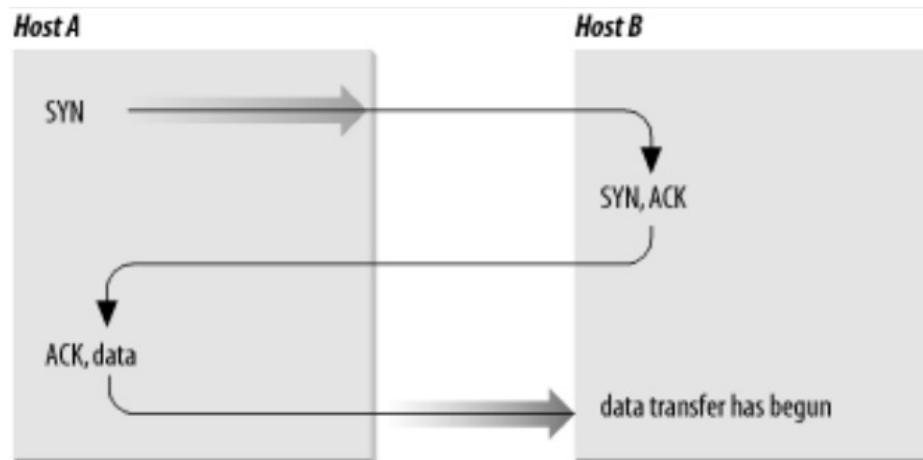


Operación del protocolo TCP/IP

TCP es orientado a la conexión -> establece una conexión fin-a-fin (end-to-end) entre los computadores que se comunican.

- La información de control ("handshake") se intercambia entre 2 computadores para establecer un diálogo ANTES de que empiece la transmisión (uso de flags).
- Se intercambian 3 segmentos -> three-way
 - Host A inicia la conexión enviando al host B un segmento con el bit "Synchronize sequence numbers" (SYN) "seteado": esto indica intención que tiene A de trasmitir datos enviando el número de secuencia (usada para mantener el orden) con que iniciará su transmisión.
 - Host B responde a A con un segmento que tiene el bit "Acknowledgment" (ACK) y el bit SYN "seteados": esto indica que B acepta (ACK) la conexión e indica su número de secuencia (SYN) para iniciar transmisión.
 - Host A responde con un segmento aceptando (ACK) el segmento enviado por B e inicia la transmisión

Operación del protocolo TCP: Handshake



- Después del intercambio A tiene evidencia de que B está listo para recibir y comienza el envío en cuanto la conexión está establecida.
- Para concluir la transmisión se realiza un handshake usando el bit "No more data from sender" llamado bit FIN.

Operación del protocolo TCP/IP

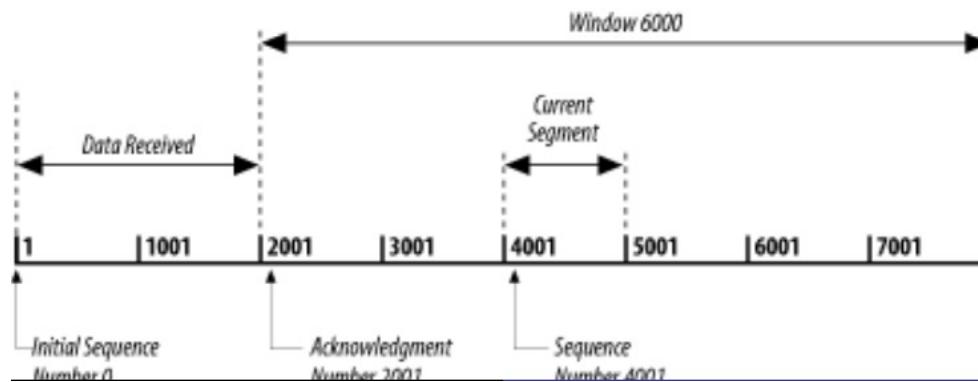
- TCP “ve” los datos como un flujo (stream) continuo, no como paquetes independientes -> se debe mantener la secuencia de los datos enviados y recibidos.
 - Para mantener la información de los datos enviados/transmitidos se utilizan los campos “Sequence Number” y “Acknowledgment Number” del encabezado de TCP.
- No se requiere que los números comiencen en un valor específico (cada sistema los elige) -> lo importante es conocer el número inicial del extremo (host) opuesto.
 - La sincronización se produce en el handshake, específicamente en el intercambio de SYN donde el campo “Sequence Number” contiene el ISN “Initial Sequence Number” . Los cuales deberían ser aleatorios por seguridad.

Operación del protocolo TCP/IP

- Cada byte de datos es numerado secuencialmente a partir de ISN, por lo que el primer byte tendría el número ISN + 1.
 - Ejemplo: Si el primer byte de datos en un stream tiene número de secuencia 1 (ISN=0) y se transfieren 4000 bytes, el primer byte del siguiente segmento sería el 4001 y por lo tanto su número de secuencia debería ser el 4001.
- El segmento ACK (“Acknowledgment Segment”) tiene 2 funciones:
 - acknowledgment positivo: cuantos datos se han recibido.
 - control de flujo: cuantos datos se podrían recibir.

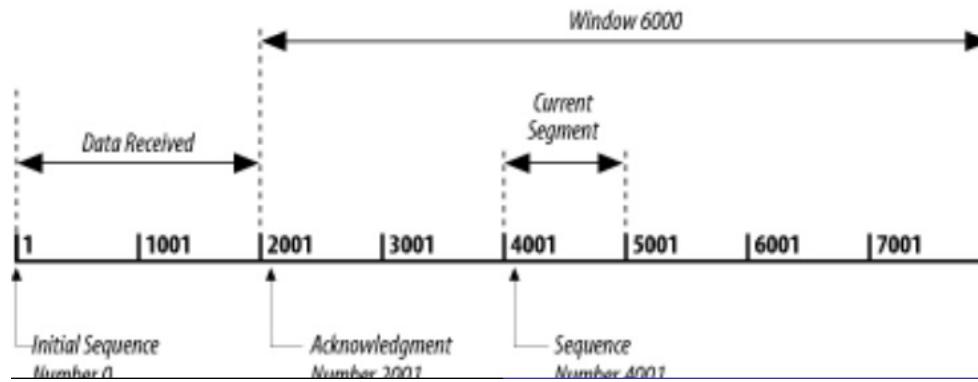
Operación del protocolo TCP/IP

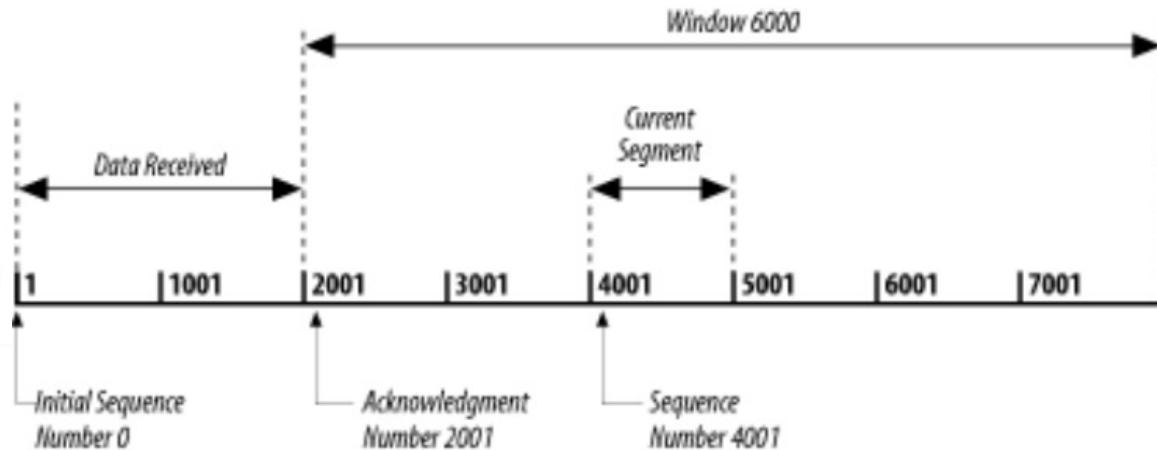
- No se requiere un acknowledgment por cada paquete. El “Acknowledgment Number” es un acknowledgment positivo de TODOS los bytes recibidos hasta ESE número.
 - Por ejemplo: Si el primer byte enviado tiene el número 1 y se han recibido exitosamente 2000, entonces el “Acknowledgment Number” debería ser 2001.



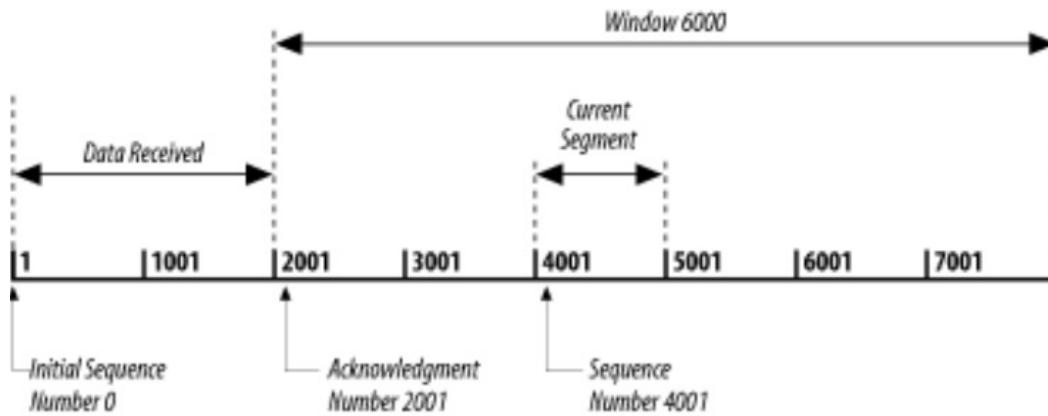
Ventana deslizante

- El campo Window tiene la “ventana” o número de bytes que el receptor puede recibir.
- La ventana le indica al transmisor que puede enviar tantos datos como lo indicado por la ventana.
- El receptor controla el flujo de bytes cambiando el tamaño de la ventana.
 - Una ventana con tamaño cero indica al emisor que el receptor NO puede recibir mas bytes hasta que reciba una ventana con valor distinto de cero.





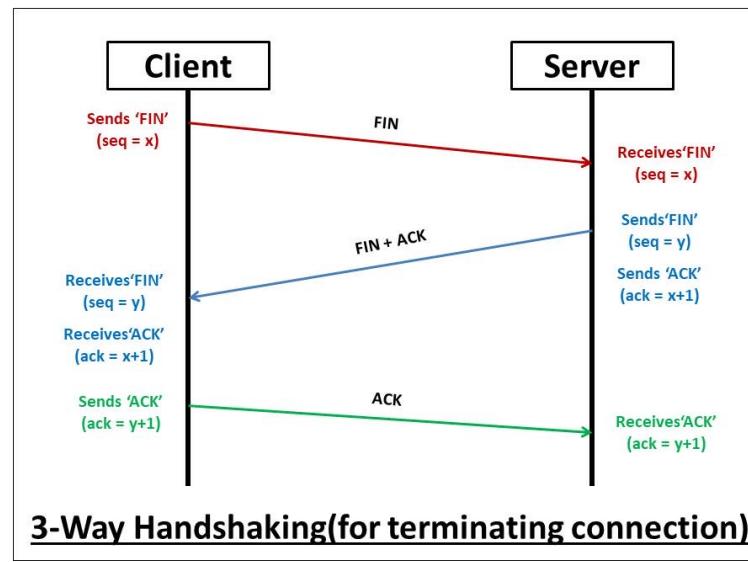
- ISN = 0. El receptor ha “reconocido” 2000 bytes -> Acknowledgment Number = 2001 y tiene espacio (buffer) para otros 6000 bytes -> window = 6000.
- El emisor está enviando un segmento de 1000 bytes con Sequence Number = 4001. El emisor puede continuar enviando permaneciendo dentro de la ventana. Si la llena y no recibe acknowledgment de lo enviado, espera (timeout) y reenvía a contar del primero que no ha recibido Ack.



- La retransmisión comenzaría en el byte 2001.
- TCP debe enviar el dato desde la capa IP a la aplicación correcta. Dicha aplicación se identifica con el número de puerto (port) .
- Puerto origen (Source Port) y puerto destino (Destination Port) están en la primera palabra del encabezado del segmento.

Escaneo de puertos

- **Flag en conexiones TCP.**
- Los tipos de escaneos se basan en conexiones TCP.
- Estas requieren usar Three-way, previamente a cualquier transferencia de datos entre emisor y receptor



Escaneo de puertos

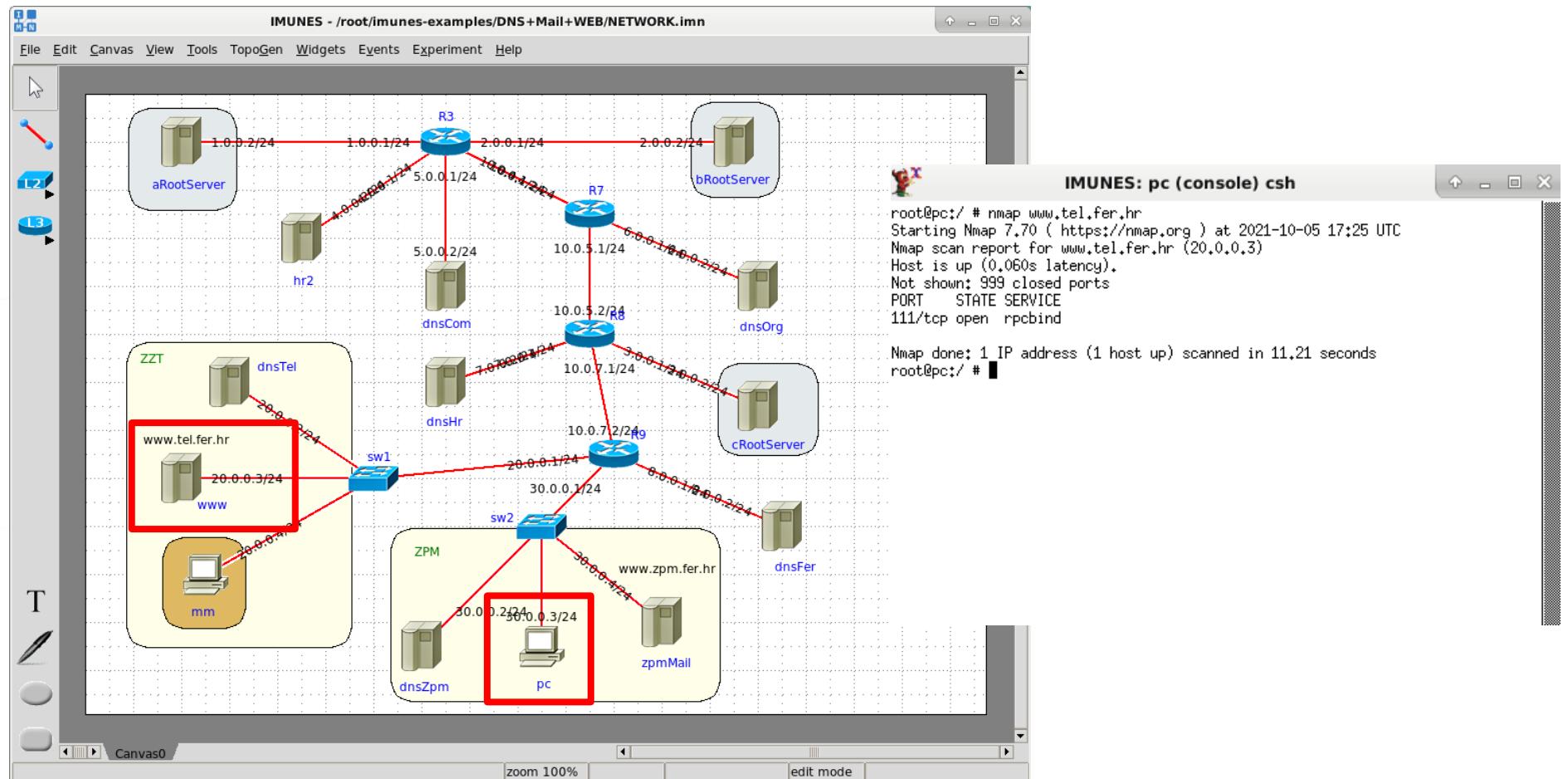
- **Flag en conexiones TCP.**
- Dado que el protocolo TCP es orientado a la conexión, el proceso por el cual se establecen, reinician y finalizan las conexiones están contempladas en el protocolo.
- Para esto se utilizan distintas notificaciones denominadas flags.
- Un atacante intentara saltarse los procesos de detección manipulando dichos flags en lugar de establecer conexiones TCP normales.

Escaneo de puertos

- **Flag en conexiones TCP.**
- El protocolo TCP incluye seis flags distintos:
 - **URG.** (Urgent) Señala a la aplicación TCP que los datos de uso hasta el Urgent-Pointer fijado se deben procesar inmediatamente.
 - **ACK.** (Acknowledge) Junto con el número de confirmación, ACK sirve para confirmar la recepción de paquetes TCP.
 - **PSH.** (Push) sirve para enviar un segmento TCP inmediatamente sin tener que pasar por el buffer de datos del emisor y el receptor.

- **Flag en conexiones TCP.**
- El protocolo TCP incluye seis flags distintos:
 - **RST.** (Reset) Si ha surgido un error durante la transmisión, la aplicación se puede restablecer mediante un paquete TCP con flag RST.
 - **SYN.** (Synchronize) Los mensajes con una etiqueta SYN representan el primer paso del triple apretón de manos, es decir, inician el establecimiento de conexión.
 - **FIN.** (Finish) Señaliza a la contraparte que uno de los interlocutores de la comunicación ha finalizado la transmisión.

Ejemplos



No.	Time	Source	Destination	Protocol	Length	Info
13	10.171185209	30.0.0.3	30.0.0.2	DNS	81	Standard query 0x1f71 PTR 3.0.0.20.in-addr.arpa
14	10.420171874	30.0.0.3	30.0.0.2	DNS	100	Standard query response 0x1f71 PTR 3.0.0.20.in-addr.arpa
15	10.421218049	30.0.0.3	20.0.0.3	TCP	58	64945 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	10.421227264	30.0.0.3	20.0.0.3	TCP	58	64945 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	10.421234818	30.0.0.3	20.0.0.3	TCP	58	64945 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	10.421279555	30.0.0.3	20.0.0.3	TCP	58	64945 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	10.421294897	30.0.0.3	20.0.0.3	TCP	58	64945 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	10.421315728	30.0.0.3	20.0.0.3	TCP	58	64945 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	10.421332680	30.0.0.3	20.0.0.3	TCP	58	64945 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	10.421352227	30.0.0.3	20.0.0.3	TCP	58	64945 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	10.421371560	30.0.0.3	20.0.0.3	TCP	58	64945 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	10.421386428	20.0.0.3	30.0.0.3	TCP	54	110 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	10.421393556	30.0.0.3	20.0.0.3	TCP	58	64945 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	10.421408366	20.0.0.3	30.0.0.3	TCP	54	1723 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- ▶ Frame 15: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
▶ Ethernet II, Src: 42:00:aa:00:00:1c (42:00:aa:00:00:1c), Dst: 42:00:aa:00:00:15 (42:00:aa:00:00:15)

Internet Protocol Version 4, Src. 30.0.0.5, Dst. 20.0.0.5

Transmission Control Protocol, Src Port: 64945, Dst Port: 110, Seq: 0, Len: 0

Source Port: 64945

Destination Port: 110

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

[Next sequence number: 0 (relative sequence number)]

Acknowledgment number: 0

0110 . . . = Header Length

Flags: 0x002 (SYN)

Window size value:

[Calculated window size

Checksum: 0x7af6 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

Options: (4 bytes)

[Timestamp]

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
13	10.171185209	30.0.0.3	30.0.0.2	DNS	81	Standard query 0x1f71 PTR 3.0.0.20.in-addr.arpa
14	10.420171874	30.0.0.2	30.0.0.3	DNS	109	Standard query response 0x1f71 PTR 3.0.0.20.in-addr.arpa
15	10.421218049	30.0.0.3	20.0.0.3	TCP	58	64945 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	10.421227264	30.0.0.3	20.0.0.3	TCP	58	64945 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	10.421234818	30.0.0.3	20.0.0.3	TCP	58	64945 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	10.421279555	30.0.0.3	20.0.0.3	TCP	58	64945 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	10.421294897	30.0.0.3	20.0.0.3	TCP	58	64945 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	10.421315728	30.0.0.3	20.0.0.3	TCP	58	64945 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	10.421332680	30.0.0.3	20.0.0.3	TCP	58	64945 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	10.421352227	30.0.0.3	20.0.0.3	TCP	58	64945 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	10.421371560	30.0.0.3	20.0.0.3	TCP	58	64945 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	10.421386428	20.0.0.3	30.0.0.3	TCP	54	110 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	10.421393556	30.0.0.3	20.0.0.3	TCP	58	64945 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	10.421408366	20.0.0.3	30.0.0.3	TCP	54	1723 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 24: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 ▶ Ethernet II, Src: 42:00:aa:00:00:15 (42:00:aa:00:00:15), Dst: 42:00:aa:00:00:1c (42:00:aa:00:00:1c)
 ▶ Internet Protocol Version 4, Src: 20.0.0.3, Dst: 30.0.0.3
 ▶ Transmission Control Protocol. Src Port: 110. Dst Port: 64945. Seq: 1. Ack: 1, Len: 0

Source Port: 110
 Destination Port: 64945
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 1 (relative sequence number)
 [Next sequence number: 1 (relative sequence number)]
 Acknowledgment number: 1 (relative ack number)
 0101 = Header Length: 20 bytes (5)
 ▶ Flags: 0x014 (RST, ACK)
 Window size value: 0
 [Calculated window size: 0]
 [Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0x969f [Unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 ▶ [SEQ/ACK analysis]
 ▶ [Timestamps]

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
55	10.827188645	30.0.0.3	20.0.0.3	TCP	58	64945 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
56	10.827210338	20.0.0.3	30.0.0.3	TCP	54	587 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
57	10.827219847	30.0.0.3	20.0.0.3	TCP	58	64945 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
58	10.827931118	20.0.0.3	30.0.0.3	TCP	58	111 → 64945 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
59	10.827940568	30.0.0.3	20.0.0.3	TCP	54	64945 → 111 [RST] Seq=1 Win=0 Len=0
60	10.827963879	20.0.0.3	30.0.0.3	TCP	54	21 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	10.827979270	30.0.0.3	20.0.0.3	TCP	58	64945 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
62	10.828002278	20.0.0.3	30.0.0.3	TCP	54	995 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	10.828012634	30.0.0.3	20.0.0.3	TCP	58	64945 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
64	10.828035616	20.0.0.3	30.0.0.3	TCP	54	5900 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	10.828045805	30.0.0.3	20.0.0.3	TCP	58	64945 → 987 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
66	10.828067960	20.0.0.3	30.0.0.3	TCP	54	23 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
67	10.828078869	30.0.0.3	20.0.0.3	TCP	58	64945 → 85 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
68	10.828102043	30.0.0.3	20.0.0.3	TCP	58	64945 → 16080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

```

Frame 58: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
Ethernet II, Src: 42:00:aa:00:00:15 (42:00:aa:00:00:15), Dst: 42:00:aa:00:00:1c (42:00:aa:00:00:1c)
Internet Protocol Version 4, Src: 20.0.0.3, Dst: 30.0.0.3
Transmission Control Protocol, Src Port: 111, Dst Port: 64945, Seq: 0, Ack: 1, Len: 0
Source Port: 111
Destination Port: 64945
[Stream index: 17]
[TCP Segment Len: 0]
Sequence number: 0      (relative sequence number)
[Next sequence number: 0      (relative sequence number)]
Acknowledgment number: 1      (relative ack number)
0110 .... = Header Length: 24 bytes (6)
▶ Flags: 0x012 (SYN, ACK)
Window size value: 65535
[Calculated window size: 65535]
Checksum: 0x1063 [unverified]
[Checksum Status: unverified]
Urgent pointer: 0

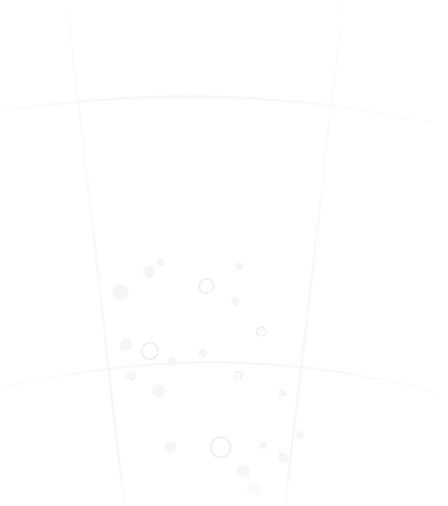
```

No.	Time	Source	Destination	Protocol	Length	Info
55	10.827188645	30.0.0.3	20.0.0.3	TCP	58	64945 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
56	10.827210338	20.0.0.3	30.0.0.3	TCP	54	587 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
57	10.827219847	30.0.0.3	20.0.0.3	TCP	58	64945 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
58	10.827931118	20.0.0.3	30.0.0.3	TCP	58	111 → 64945 [SYN, ACK] Seq=0 Ack=1 Win=0 MSS=1460
59	10.827940568	30.0.0.3	20.0.0.3	TCP	54	64945 → 111 [RST] Seq=1 Win=0 Len=0
60	10.827963879	20.0.0.3	30.0.0.3	TCP	54	21 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	10.827979270	30.0.0.3	20.0.0.3	TCP	58	64945 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
62	10.828002278	20.0.0.3	30.0.0.3	TCP	54	995 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	10.828012634	30.0.0.3	20.0.0.3	TCP	58	64945 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
64	10.828035616	20.0.0.3	30.0.0.3	TCP	54	5900 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	10.828045805	30.0.0.3	20.0.0.3	TCP	58	64945 → 987 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
66	10.828067960	20.0.0.3	30.0.0.3	TCP	54	23 → 64945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
67	10.828078869	30.0.0.3	20.0.0.3	TCP	58	64945 → 85 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
68	10.828102043	30.0.0.3	20.0.0.3	TCP	58	64945 → 16080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

▶ Frame 59: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 ▶ Ethernet II, Src: 42:00:aa:00:00:1c (42:00:aa:00:00:1c), Dst: 42:00:aa:00:00:15 (42:00:aa:00:00:15)
 ▶ Internet Protocol Version 4, Src: 30.0.0.3, Dst: 20.0.0.3
 ▶ Transmission Control Protocol, Src Port: 64945, Dst Port: 111, Seq: 1, Len: 0

```

    Source Port: 64945
    Destination Port: 111
    [Stream index: 17]
    [TCP Segment Len: 0]
    Sequence number: 1 (relative sequence number)
    [Next sequence number: 1 (relative sequence number)]
    Acknowledgment number: 0
    0101 .... = Header Length: 20 bytes (5)
    ▶ Flags: 0x004 (RST)
    Window size value: 0
    [Calculated window size: 0]
    [Window size scaling factor: 2 (no window scaling used)]
    Checksum: 0x96ae [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    ▶ [Timestamps]
  
```



Puertos

Escaneo

Puertos bien conocidos

- La Agencia de asignación de números por Internet (IANA) asigna números de puerto.
- IANA es un organismo normativo responsable de asegurar diferentes estándares de direccionamiento.

Rango de números de puerto	Grupo de puertos
Entre 0 y 1023	Puertos bien conocidos
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

Puertos bien conocidos (0 -1023)

Puertos bien conocidos (números del 0 al 1023)

- Estos números se reservan para servicios y aplicaciones.
- Se utilizan comúnmente para aplicaciones como HTTP (servidor Web), protocolo de acceso a mensajes de Internet (IMAP) o protocolo simple de transferencia de correo (SMTP) (servidor de correo electrónico) y Telnet.
- Al definir estos puertos bien conocidos para las aplicaciones de los servidores, las aplicaciones cliente se pueden programar para solicitar una conexión a ese puerto en particular y el servicio relacionado.

Puertos bien conocidos (0 -1023)

Puerto	Nombre	Descripción
20	ftp-data	Puerto de datos FTP
21	ftp	Puerto del Protocolo de transferencia de archivos (FTP)
22	ssh	Servicio de shell seguro (SSH)
23	telnet	El servicio Telnet
25	smtp	Protocolo simple de transferencia de correo (SMTP)
53	domain	Servicios de nombres de dominio
69	tftp	Protocolo de transferencia de archivos triviales (TFTP)
80	http	Protocolo de transferencia de hipertexto (HTTP)
110	pop3	Protocolo Post Office versión 3
115	sftp	FTP Seguro
137	netbios-ns	Servicios de nombres NETBIOS
138	netbios-dgm	Servicios de datagramas NETBIOS
139	netbios-ssn	Servicios de sesión NETBIOS
161	snmp	Protocolo simple de administración de redes (SNMP)
443	https	Protocolo de transferencia de hipertexto seguro (HTTP)

Puertos registrados (1024 -49151)

Puertos registrados (números del 1024 al 49151):

- Estos números de puerto se asignan a procesos o aplicaciones del usuario.
- Estos procesos son aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes que recibiría un número de puerto bien conocido.
- Cuando no se utilizan para un recurso del servidor, un cliente puede seleccionar estos puertos de forma dinámica como su puerto de origen.

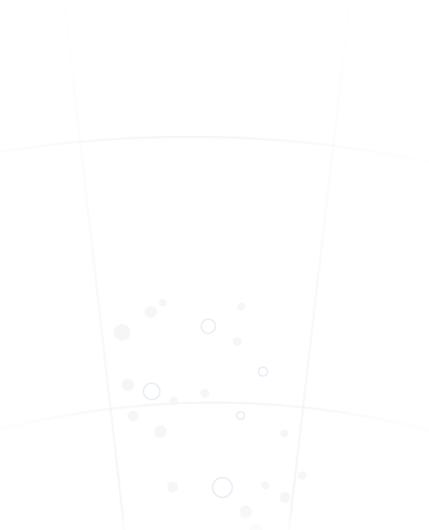
Puertos dinámicos o privados (49152 - 65535)

Puertos dinámicos o privados (números 49152 a 65535)

- Conocidos como puertos efímeros, generalmente se los asigna de forma dinámica a las aplicaciones cliente cuando el cliente inicia una conexión a un servicio.
- El puerto dinámico suele utilizarse para identificar la aplicación cliente durante la comunicación, mientras que el cliente utiliza el puerto bien conocido para identificar el servicio que se solicita en el servidor y conectarse a dicho servicio.
- No es común que un cliente se conecte a un servicio mediante un puerto dinámico o privado.

Ejercicio: revisión de video...

En el siguiente video hay un pequeño error.....





Escaneo

Escaneo

Ingeniería Civil Informática

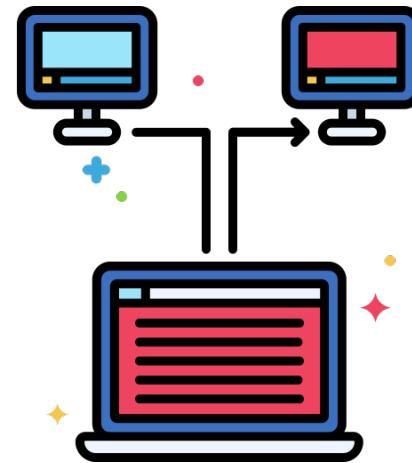
Escaneo

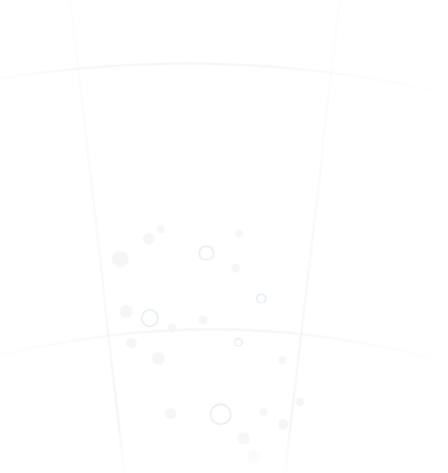
- Los hackers buscan cualquier información que pueda ayudar a perpetrar un ataque contra un objetivo, tales como los siguientes:
 - Nombres de computadores
 - Sistema operativo (SO)
 - Software instalado
 - Direcciones IP
 - Cuentas de usuario



Escaneo

- En esta parte se usa la información proporcionada por el paso anterior para examinar la red. Los recursos que el hacker puede emplear en esta fase son:
 - Escáner de puertos
 - Barrido de ping
 - Mapeadores de red
 - Escáneres de vulnerabilidades





Escaneo de puertos

Escaneo

Escaneo

Escáneres de puertos

- Se analizan los puertos de un sistema informático.
- Detecta si un puerto está abierto, cerrado, o protegido por un cortafuegos.
- También se puede detectar el SO del sistema.
- Los administradores de sistemas lo usan para conocer los servicios que está ofreciendo la máquina o para analizar el estado de los puertos y detectar y evitar posibles vulnerabilidades.

Escaneo de puertos

- **Nmap.** Es una herramienta de software libre y flexible, que realiza en forma rápida y eficiente, entre otras las siguientes acciones:
 - Ping sweeps (barridos)
 - Escaneo de puertos
 - Identificación de servicios
 - Detección de direcciones IP
 - Detección del sistema operativo

Escaneo de puertos

- **Nmap.**
- El estado puede presentar un puerto abierto, filtrado, no filtrado y cerrado.
 - **Abierto.** Implica que el equipo objetivo acepta peticiones a ese puerto.
 - **Filtrado.** Un firewall u otro dispositivo de red enmascara el puerto y previene que nmap determine si está abierto o no.
 - **No filtrado.** Los datos pueden llegar al host, pero NMAP no puede determinar que el puerto está activado o desactivado
 - **Cerrado.** El puerto está cerrado, los datos pueden llegar al host, pero ningún programa escucha este puerto.

```
[kali㉿kali)-[~]:/home/msfadmin#
```

```
$ nmap 10.50.250.130
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-06 14:31 EDT
```

```
Nmap scan report for 10.50.250.130
```

```
Host is up (0.098s latency).
```

```
Not shown: 809 closed ports, 170 filtered ports
```

```
PORT      STATE SERVICE
```

```
21/tcp    open  ftp
```

```
22/tcp    open  ssh
```

```
23/tcp    open  telnet
```

```
25/tcp    open  smtp
```

```
53/tcp    open  domain
```

```
80/tcp    open  http
```

```
111/tcp   open  rpcbind
```

```
139/tcp   open  netbios-ssn
```

```
445/tcp   open  microsoft-ds
```

```
512/tcp   open  exec-ssn
```

```
513/tcp   open  login-soft-ds
```

```
514/tcp   open  shell
```

```
1524/tcp  open  ingreslock
```

```
2000/tcp  open  cisco-sccp
```

```
2049/tcp  open  nfs
```

```
2121/tcp  open  ccproxy-ftp
```

```
3306/tcp  open  mysql
```

```
5060/tcp  open  sip
```

```
5432/tcp  open  postgresql
```

```
5900/tcp  open  vnc
```

```
6000/tcp  open  X11
```

```
5000/tcp  open  X11
```

```
Nmap done: 1 IP address (1 host up) scanned in 18.80 seconds
```

```
[kali㉿kali)-[~]
```

```
$ nmap -PA -p 21,22,125 10.50.250.130
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-06 14:35 EDT
```

```
Nmap scan report for 10.50.250.130
```

```
Host is up (0.13s latency).
```

```
PORT      STATE SERVICE
```

```
21/tcp    open  ftp
```

```
22/tcp    open  ssh
```

```
125/tcp   closed locus-map
```

```
6667/tcp open  lirc
```

```
6668/tcp open  lirc
```

```
6669/tcp open  lirc
```

```
6670/tcp open  lirc
```

```
6671/tcp open  lirc
```

```
6672/tcp open  lirc
```

```
6673/tcp open  lirc
```

```
6674/tcp open  lirc
```

```
6675/tcp open  lirc
```

```
6676/tcp open  lirc
```

```
6677/tcp open  lirc
```

```
6678/tcp open  lirc
```

```
6679/tcp open  lirc
```

```
6680/tcp open  lirc
```

```
6681/tcp open  lirc
```

```
6682/tcp open  lirc
```

```
6683/tcp open  lirc
```

```
6684/tcp open  lirc
```

```
6685/tcp open  lirc
```

```
6686/tcp open  lirc
```

```
6687/tcp open  lirc
```

```
6688/tcp open  lirc
```

```
6689/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
6697/tcp open  lirc
```

```
6698/tcp open  lirc
```

```
6699/tcp open  lirc
```

```
6690/tcp open  lirc
```

```
6691/tcp open  lirc
```

```
6692/tcp open  lirc
```

```
6693/tcp open  lirc
```

```
6694/tcp open  lirc
```

```
6695/tcp open  lirc
```

```
6696/tcp open  lirc
```

```
66
```

Escaneo de puertos

- **Nmap.**

-sT	TCP connect scan	-sR	RPC scan
-sS	SYN scan	-sL	List / DNS scan
-sF	FIN scan	-sl	Idle scan
-sX	XMAS tree scan	-Po	Don't ping
-sN	Null scan	-PT	TCP ping
-sP	Ping scan	-PS	SYN ping
-sU	UDP scan	-PI	ICMP ping
-sO	Protocol scan	-PB	TCP and ICMP ping
-sA	ACK scan	-PB	ICMP timestamp
-sW	Windows scan	-PM	ICMP netmask

Escaneo de puertos

- **Nmap**

-oN	Normal output
-oX	XML output
-oG	Greppable output
-oA	All output
-T Paranoid	Serial scan; 300 sec between scans
-T Sneaky	Serial scan; 15 sec between scans
-T Polite	Serial scan; .4 sec between scans
-T Normal	Parallel scan
-T Aggressive	Parallel scan, 300 sec timeout, and 1.25 sec/probe
-T Insane	Parallel scan, 75 sec timeout, and .3 sec/probe

Escaneo de puertos

- La opción -v significa verbose, indica lo que está haciendo el análisis al detalle.

```
(kali㉿kali)-[~]
└─$ nmap -v 10.50.250.130 [admin]
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-06 14:41 EDT
Initiating Ping Scan at 14:41
Scanning 10.50.250.130 [2 ports] [admin] # nmap 10.50.250.130
Completed Ping Scan at 14:41, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:41 [admin] 14:43 EDT
Completed Parallel DNS resolution of 1 host. at 14:41, 11.04s elapsed
Initiating Connect Scan at 14:41
Scanning 10.50.250.130 [1000 ports]
Discovered open port 80/tcp on 10.50.250.130
Discovered open port 139/tcp on 10.50.250.130
Discovered open port 53/tcp on 10.50.250.130
Discovered open port 21/tcp on 10.50.250.130
Discovered open port 22/tcp on 10.50.250.130
Discovered open port 5900/tcp on 10.50.250.130
Discovered open port 445/tcp on 10.50.250.130
Discovered open port 111/tcp on 10.50.250.130
Discovered open port 23/tcp on 10.50.250.130
Discovered open port 25/tcp on 10.50.250.130
Discovered open port 3306/tcp on 10.50.250.130
Discovered open port 2000/tcp on 10.50.250.130
Discovered open port 514/tcp on 10.50.250.130
Discovered open port 2121/tcp on 10.50.250.130
Discovered open port 513/tcp on 10.50.250.130
Discovered open port 2049/tcp on 10.50.250.130
Discovered open port 5432/tcp on 10.50.250.130
Discovered open port 1524/tcp on 10.50.250.130
Discovered open port 6667/tcp on 10.50.250.130
Discovered open port 1099/tcp on 10.50.250.130
Discovered open port 512/tcp on 10.50.250.130
Discovered open port 6000/tcp on 10.50.250.130
Discovered open port 5060/tcp on 10.50.250.130
Discovered open port 8009/tcp on 10.50.250.130 [13.106 seconds]
Discovered open port 8180/tcp on 10.50.250.130

Discovered open port 8009/tcp on 10.50.250.130
Discovered open port 8180/tcp on 10.50.250.130
Completed Connect Scan at 14:41, 4.80s elapsed (1000 total ports)
Nmap scan report for 10.50.250.130
Host is up (0.091s latency). [admin]# nmap 10.50.250.130
Not shown: 975 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2000/tcp  open  cisco-sccp
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5060/tcp  open  sip
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Read data files from: /usr/bin/..../share/nmap
in 13.106 seconds
Nmap done: 1 IP address (1 host up) scanned in 15.99 seconds
```

Escaneo de puertos

- Escanear un rango de IP resulta útil en caso de un ataque si se quiere averiguar hacia donde apuntar.

```
nmap <IP>-<IP2>
```

```
nmap 192.168.1.1-115
```

Escaneo de puertos

- Escanear un rango puerto concreto ayuda a que la salida sea mas corta y solo para centrarse en lo que se desea ver.

```
nmap -p <número_puerto>
```

```
nmap -p 80 192.168.1.200
```

```
(kali㉿kali)-[~]eslock
└─$ nmap -p 80 10.50.250.130
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-06 14:43 EDT
Nmap scan report for 10.50.250.130
Host is up (0.036s latency).

PORT      STATE SERVICE
80/tcp    open  http
5432/tcp  open  postgres
6667/tcp  open  irc

Nmap done: 1 IP address (1 host up) scanned in 11.26 seconds
```

Escaneo de puertos

- **Lanzar un escaneo TCP SYN.** Determina si el puerto objetivo está escuchando

```
nmap -sS <IP>
```

```
root@metasploitable:/home/msfadmin# nmap -sS 10.50.250.130
PORT      STATE SERVICE
Starting Nmap 4.53 ( http://insecure.org ) at 2021-10-06 15:01 EDT
Interesting ports on 10.50.250.130:
Not shown: 1692 closed ports
port       state service
21/tcp     open  ftp
22/tcp     open  ssh
23/tcp     open  telnet
25/tcp     open  smtp
53/tcp     open  domain
80/tcp     open  http
111/tcp    open  rpcbind
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
512/tcp    open  exec
513/tcp    open  login
514/tcp    open  shell
1524/tcp   open  ingreslock
2049/tcp   open  nfs
2121/tcp   open  ccproxy-ftp
3306/tcp   open  mysql
3632/tcp   open  distccd
5432/tcp   open  postgres
5900/tcp   open  vnc
6000/tcp   open  X11
6667/tcp   open  ircng
8009/tcp   open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 13.101 seconds
```

Escaneo de puertos

- Escaneo de sistema operativo

```
nmap -O 192.168.43.45
```

```
Starting Nmap 4.53 ( http://insecure.org ) at 2021-10-06 15:02 EDT
Interesting ports on 10.50.250.130:
Not shown: 1692 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgres
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20 (Ubuntu 7.04, x86, SMP)
Uptime: 1.150 days (since Tue Oct  5 11:27:08 2021)
Network Distance: 0 hops
Nmap done: 1 IP address (1 host up) scanned in 14.490 seconds
```

Escaneo de puertos

- Escaneo de sistema operativo

```
(root💀 kali)-[~/home/marco]
# nmap -O 10.211.55.12
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-07 02:28 -03
Nmap scan report for windows-8.1.shared (10.211.55.12)
Host is up (0.00033s latency).
All 1000 scanned ports on windows-8.1.shared (10.211.55.12) are filtered
MAC Address: 00:1C:42:E5:B5:67 (Parallels)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 24.22 seconds


```

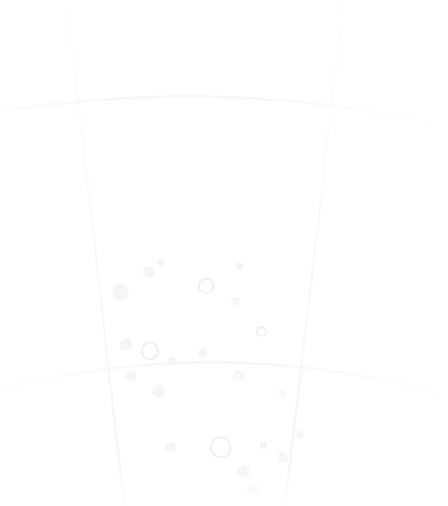
Escaneo de puertos

- Escaneo para ver los servicios que están asociados a los puertos

```
nmap -sV 192.168.1.43
```

```
root@metasploitable:/home/msfadmin# nmap -sV 10.50.250.130

Starting Nmap 4.53 ( http://insecure.org ) at 2021-10-06 15:14 EDT
Interesting ports on 10.50.250.130:
Not shown: 1692 closed ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              vsftpd 2.3.4
22/tcp    open  ssh              OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet           Linux telnetd
25/tcp    open  smtp             Postfix smtpd root privileges.
53/tcp    open  domain
80/tcp    open  http             Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind          2 (rpc #100000)
139/tcp   open  netbios-ssn     Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn     Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1524/tcp  open  ingreslock?
2049/tcp  open  nfs              2-4 (rpc #100003)
2121/tcp  open  ftp              ProFTPD 1.3.1
3306/tcp  open  mysql            MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd          distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql       PostgreSQL DB
5900/tcp  open  vnc              VNC (protocol 3.3)
6000/tcp  open  X11              (access denied)
6667/tcp  open  irc              Unreal ircd
8009/tcp  open  ajp13?          (from OS scan) requires root privileges.
1 service unrecognized despite returning data. If you know the service/version.cgi :
```



Escaneo de red

Escaneo

Escaneo

Barrido de ping

- Es una técnica de diagnóstico utilizada para ver el rango de direcciones de direcciones IP que tienen los hosts operativos.
- Se usa para indicar dónde están las máquinas activas en una red, y a veces lo utiliza un administrador del sistema para diagnosticar un problema de red.
- También se usa cuando se quiere entrar a una red, para ver que computador esta activo y así ver en donde se puede concentrar los ataques.

Escaneo de red

- La técnica más simple para realizar un escaneo es **Ping Sweep**, la cual consiste en:

Se envían paquetes ICMP request(ping) a todos los host de una red

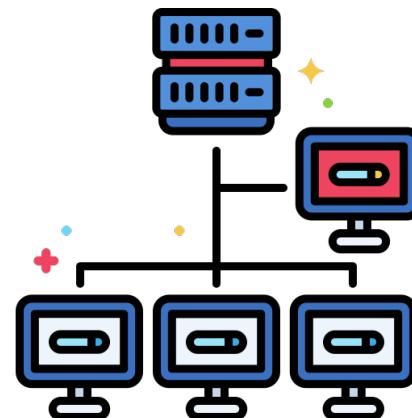
Si un host responde, indica que esta online y puede ser un posible objetivo de ataque

Escaneo de red

- Esta técnica permite mandar paquetes de forma simultánea por lo que todo el sistema es escaneado al mismo tiempo.
- La mayoría de las herramientas de escaneo incluye la opción de un **Ping Sweep**.
- Es una técnica sencilla por lo que puede ser poco efectiva, porque puede ser bloqueada por Firewall y proxies.
- Si no se detectan dispositivos esto no quiere decir que no existan.
- Se usa como complemento a otras herramientas.

Escaneo de red

- Algunas herramientas conocidas por implementar esta técnica son:
 - Pinger
 - Friendly Pinger
 - WS_Ping_Pro
 - Nmap



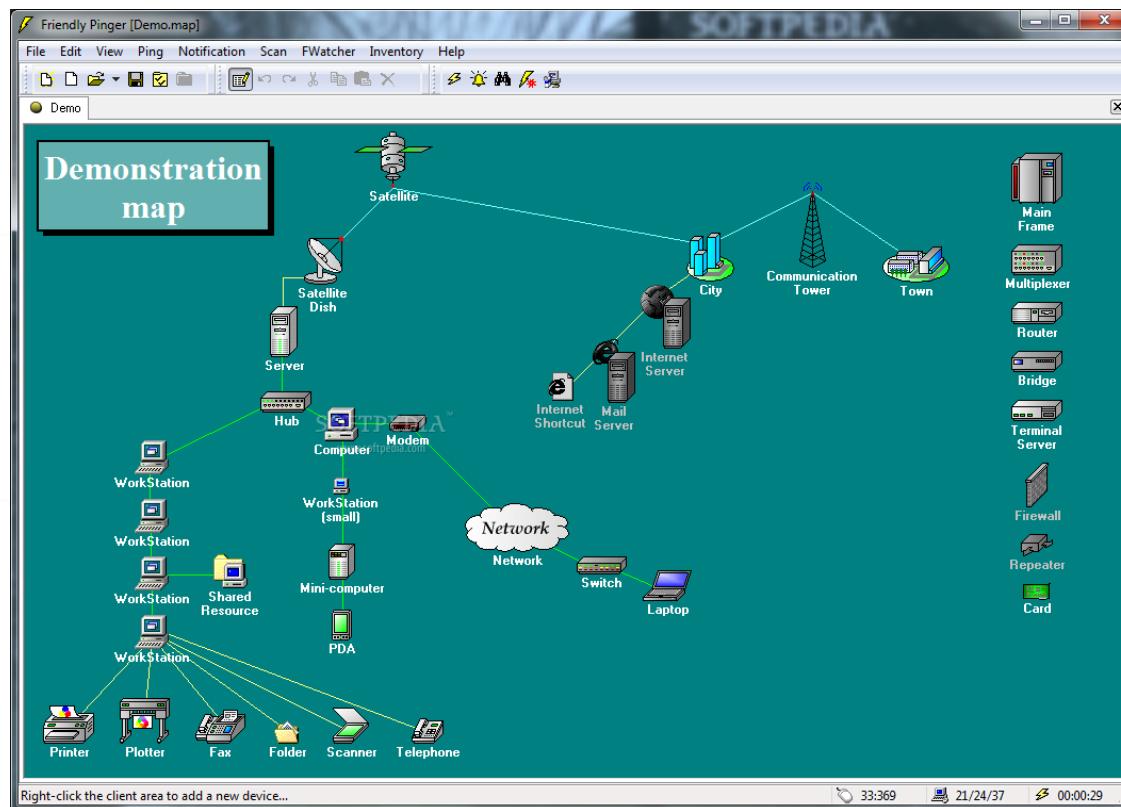
Escaneo de red

Friendly Pinger. Es una aplicación gratuita para la administración, el monitoreo y el inventario de redes.

- Visualización de la red informática en pantalla animada.
- Monitoreo de la disponibilidad de dispositivos de red.
- Notificación cuando un servidor se despierta o deja de funcionar.
- Ping de todos los dispositivos a la vez.

Escaneo de red

Friendly Pinger.



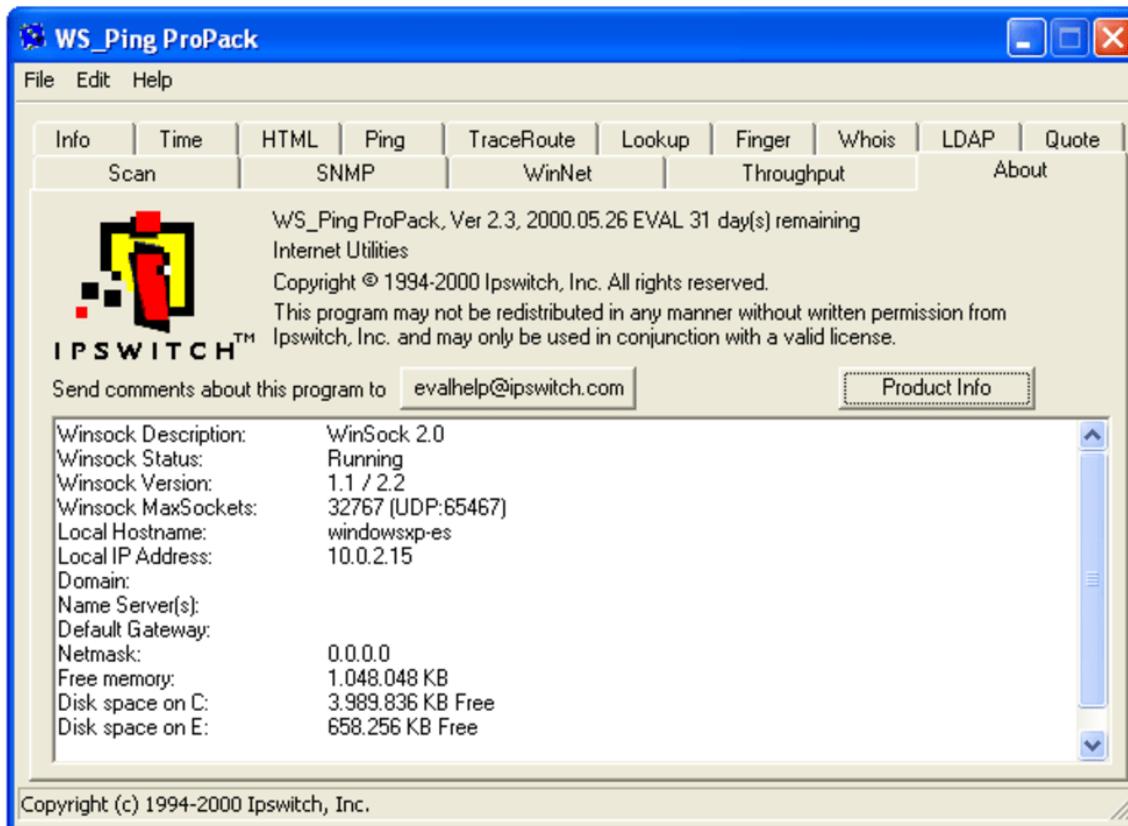
Escaneo de red

WS_Ping_Pro. Es un conjunto de herramientas pensadas para monitorizar y analizar redes.

- Se puede analizar una dirección o IP y obtener información de todo tipo, así como localizar errores o problemas de una red.
- Tiene pruebas para Ping, TraceRoute, Finger, Whois, WInNet o SNMP, entre otras.

Escaneo de red

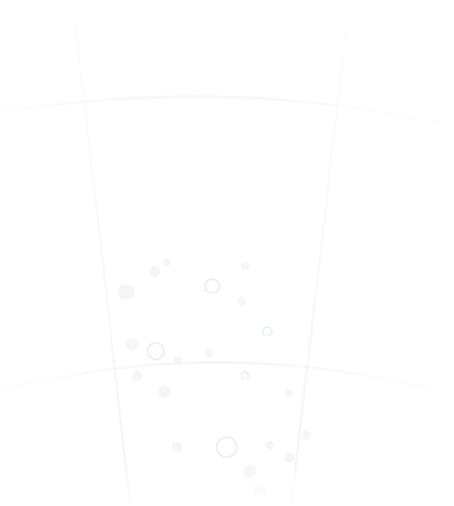
WS_Ping_Pro



Escaneo

Mapeadores de red

- Es un proceso que se utiliza para descubrir nuevos dispositivos, interfaces y visualizar la conectividad de red física y virtual.
- Ayuda a descomponer la red para facilitar el mantenimiento y la gestión de la red



Escaneo de puerto

Escaneo

Escaneo de puertos

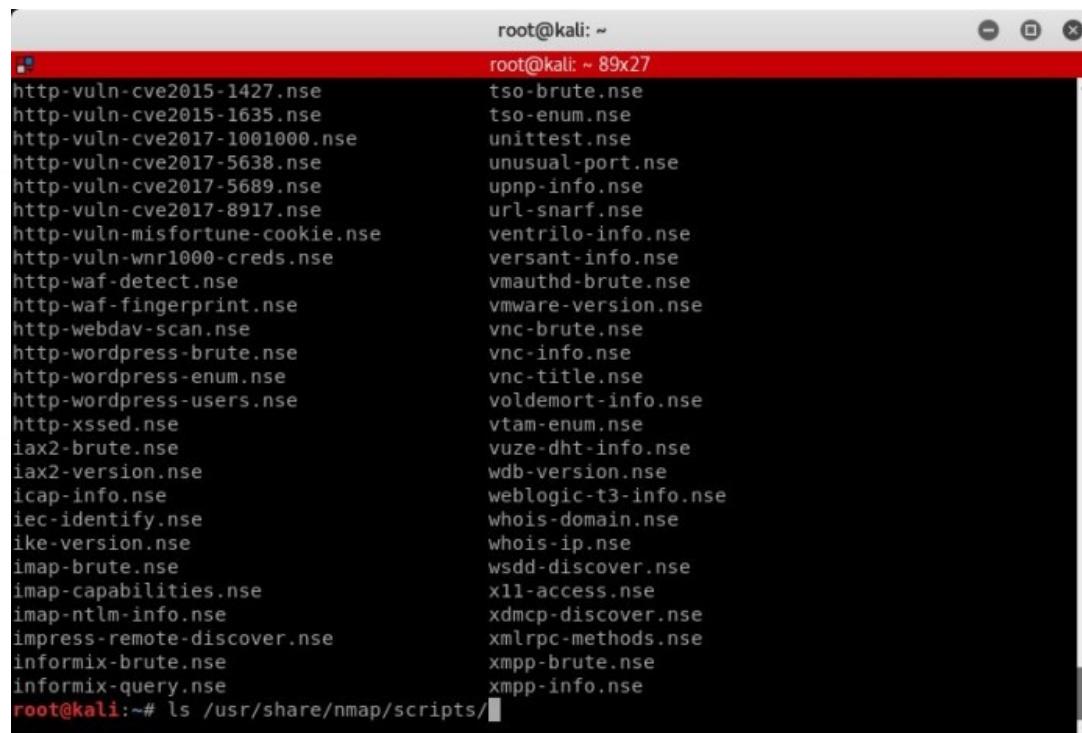
- **Nmap.** Se puede incorporar el uso de scripts para comprobar vulnerabilidades.
 - Auth: ejecuta todos sus scripts disponibles para autenticación
 - Default: ejecuta los scripts básicos por defecto de la herramienta
 - Discovery: recupera información del target o víctima
 - External: script para utilizar recursos externos
 - Intrusive: utiliza scripts que son considerados intrusivos para la víctima o target
 - Malware: revisa si hay conexiones abiertas por códigos maliciosos o backdoors (puertas traseras)
 - Safe: ejecuta scripts que no son intrusivos
 - Vuln: descubre las vulnerabilidades más conocidas
 - All: ejecuta absolutamente todos los scripts con extensión NSE disponibles

Escaneo de puertos

- **Nmap.**
- La secuencia de comandos para ejecutar script es:
 - **nmap --script nombre_script IP**
- Si se quiere escanear varias categorias
 - **nmap --script categoria1,categoria2,categoria3 IP**

Escaneo de puertos

- **Nmap.**
- Se ubican los scripts por defecto: en **/usr/share/nmap/scripts/** y los mismos tiene la extensión **.nse**.



```
root@kali: ~
root@kali: ~ 89x27
http-vuln-cve2015-1427.nse
http-vuln-cve2015-1635.nse
http-vuln-cve2017-1001000.nse
http-vuln-cve2017-5638.nse
http-vuln-cve2017-5689.nse
http-vuln-cve2017-8917.nse
http-vuln-misfortune-cookie.nse
http-vuln-wnr1000-creds.nse
http-waf-detect.nse
http-waf-fingerprint.nse
http-webdav-scan.nse
http-wordpress-brute.nse
http-wordpress-enum.nse
http-wordpress-users.nse
http-xssed.nse
iax2-brute.nse
iax2-version.nse
icap-info.nse
iec-identify.nse
ike-version.nse
imap-brute.nse
imap-capabilities.nse
imap-ntlm-info.nse
impress-remote-discover.nse
informix-brute.nse
informix-query.nse
root@kali:~# ls /usr/share/nmap/scripts/
```

Escaneo de puertos

- **Nmap.** ssh-brute.nse
- El script ssh-brute se utiliza para romper las contraseñas de servicios SSH con la entrada de texto predictivo.

```
root@kali:~# nmap -n -p22 --script ssh-brute \
> --script-args userdb=usernames.lst,passwords.lst 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-11 08:48 EDT
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: test:admin
NSE: [ssh-brute] Trying username/password pair: guest:admin
NSE: [ssh-brute] Trying username/password pair: admin:test
NSE: [ssh-brute] Trying username/password pair: guest:test
NSE: [ssh-brute] Trying username/password pair: admin:guest
NSE: [ssh-brute] Trying username/password pair: test:guest
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: test:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456
NSE: [ssh-brute] Trying username/password pair: admin:1234567
NSE: [ssh-brute] Trying username/password pair: test:1234567
NSE: [ssh-brute] Trying username/password pair: guest:1234567
NSE: [ssh-brute] Trying username/password pair: admin:12345678
NSE: [ssh-brute] Trying username/password pair: test:12345678
NSE: [ssh-brute] Trying username/password pair: guest:12345678
NSE: [ssh-brute] Trying username/password pair: admin:123456789
NSE: [ssh-brute] Trying username/password pair: test:123456789
NSE: [ssh-brute] Trying username/password pair: guest:123456789
Nmap scan report for 192.168.56.102
Host is up (0.00034s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-brute:
|_ Accounts:
|   test:123456789 - Valid credentials
|_ Statistics: Performed 21 guesses in 5 seconds, average tps: 4.2
MAC Address: 08:00:27:6E:A2:39 (Oracle VirtualBox virtual NIC)
```

Escaneo de puertos

- **Nmap.** mysql-empty-password.nse
- Comprueba si es posible iniciar sesión en el servidor MySQL utilizando una contraseña vacía.

```
root:~/ # nmap -p3306 --script=mysql-empty-password 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-20 10:39 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00032s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
| mysql-empty-password:
|_ root account has empty password
MAC Address: 08:00:27:6E:A2:39 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Escaneo de puertos

- **Nmap.** mysql-users.nse
- Se usa para listar los usuarios disponibles en el servidor MySQL. Para listarla, se usa la cuenta root con una contraseña vacía

```
root:~/ # nmap -p3306 --script mysql-users --script-args=mysqluser=root 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-21 09:55 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00032s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
| mysql-users:
|   debian-sys-maint
|   guest
|   root
|   testerr
MAC Address: 08:00:27:6E:A2:39 (Oracle VirtualBox virtual NIC)
```

Escaneo de vulnerabilidades – Explotación con Nmap

- script **ftp-anon** de la categoría **auth**, permite saber si el acceso anónimo a servidor ftp, está permitido.

```
behackerpro@developer:~$ sudo nmap -p21 --script=ftp-anon 192.168.0.11
Starting Nmap 7.70 ( https://nmap.org ) at 2021-06-04 14:38 -05
Nmap scan report for 192.168.0.11
Host is up (-0.14s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 00:F4:8D:69:17:59 (Unknown)
```

Escaneo de vulnerabilidades – Explotación con Nmap

- Con el script **http-default-accounts** se trata de determinar si el acceso con credenciales por defecto está habilitado en algunas aplicaciones web

```
beholderpro@developer:~$ sudo nmap -p8180 --script=http-default-accounts 192.168.0.11
Starting Nmap 7.70 ( https://nmap.org ) at 2021-06-04 14:48 -05
Nmap scan report for 192.168.0.11
Host is up (0.099s latency).

PORT      STATE SERVICE
8180/tcp   open  unknown
| http-default-accounts:
|   [Apache Tomcat] at /manager/html/
|   tomcat:tomcat
MAC Address: 00:F4:8D:69:17:59 (Unknown)
```

Escaneo de vulnerabilidades – Explotación con Nmap

- Con el script **mysql-empty-password** podemos determinar si el servidor MySQL no utiliza contraseña para el usuario root

```
behackerpro@developer:~$ sudo nmap -p3306 --script=mysql-empty-password 192.168.0.11
Starting Nmap 7.70 ( https://nmap.org ) at 2021-06-04 14:53 -05
Nmap scan report for 192.168.0.11
Host is up (-0.15s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
| mysql-empty-password:
|_ root account has empty password
```

Escaneo de vulnerabilidades – Explotación con Nmap

- El script **mysql-users** intenta listar los usuarios del servidor mysql; en ese caso se le ingresaron unos argumentos al script

```
behackerpro@developer:~$ sudo nmap -p3306 192.168.0.11 --script=mysql-users --script-args mysqluser=root,mysqlpass=''
Starting Nmap 7.70 ( https://nmap.org ) at 2021-06-04 15:08 -05
Nmap scan report for 192.168.0.11
Host is up (-0.10s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
| mysql-users:
|   debian-sys-maint
|   guest
|   root
```

Escaneo de vulnerabilidades – Explotación con Nmap

- El script **ftp-vsftpd-backdoor** corresponde a las categorías: exploit, intrusive, malware, vuln, este script busca la presencia de la puerta trasera (backdoor) reportada en CVE-2011-2523

```
behackerpro@developer:/usr/share/nmap/scripts$ sudo nmap --script=ftp-vsftpd-backdoor -p21 192.168.0.11
Starting Nmap 7.70 ( https://nmap.org ) at 2021-06-04 22:29 -05
Nmap scan report for 192.168.0.11
Host is up (-0.085s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|  ftp-vsftpd-backdoor:
|  VULNERABLE:
|  vsFTPD version 2.3.4 backdoor
|    State: VULNERABLE (Exploitable)
|    IDs:  CVE:CVE-2011-2523 OSVDB:73573
|    vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
```

Escaneo de puertos

- Las medidas para evitar un escaneo de puerto son procesos o herramientas que el administrador configurar para detectar posibles intentos de escaneos.
- Otras medidas que se pueden tomar son:
 - Implementar una arquitectura de seguridad apropiada con distintos firewalls.
 - Hacer pruebas para ver si los escaneos son detectados

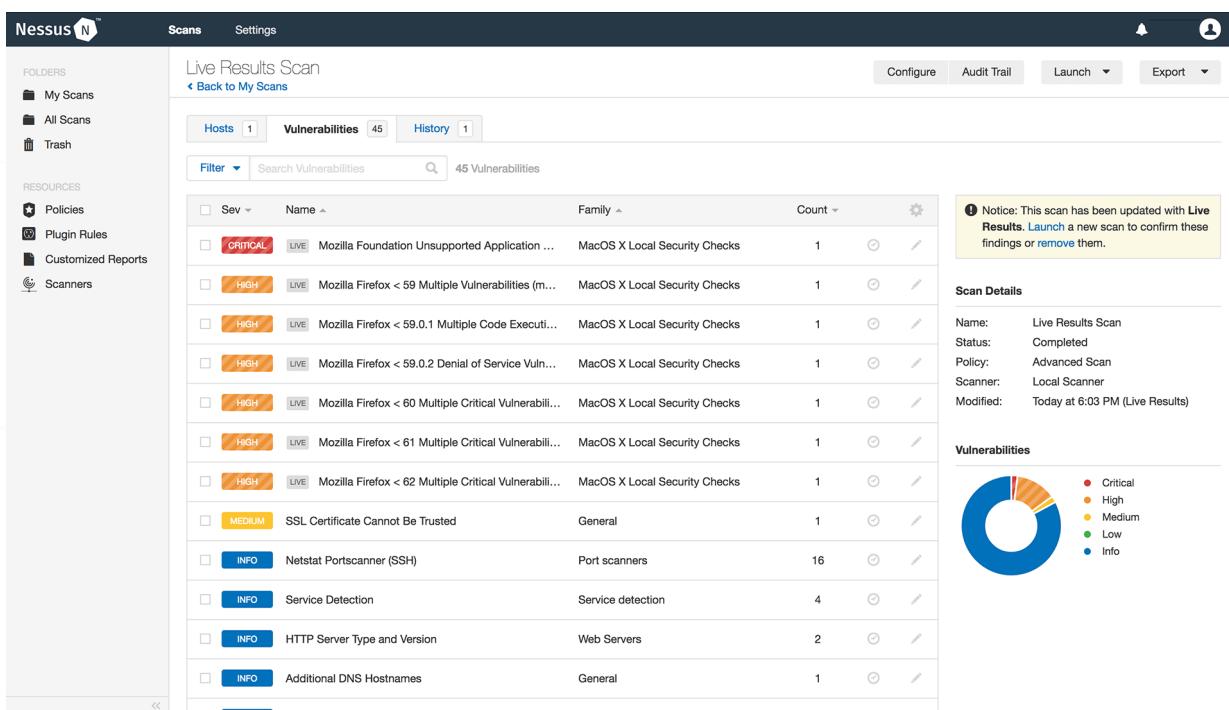
Escaneo

Escáneres de vulnerabilidades

- Es un software diseñado para realizar análisis automáticos de cualquier aplicación, sistema o red en busca de cualquier posible vulnerabilidad que exista.
- Son capaces de detectar ciertos elementos que podrían desencadenar en una vulnerabilidad.

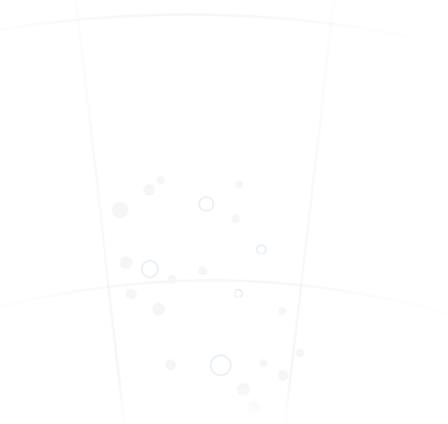
Escaneo

- **El escaneo de vulnerabilidades**, donde se determina la existencia de vulnerabilidades conocidas en los host.



Escaneo

- Un hacker sigue una secuencia de pasos para escanear una red.
- Los métodos del análisis pueden variar dependiendo del objetivo del ciberataque, que se configuran antes de que se comience el proceso.
- Las herramientas de escaneo pueden estar elaboradas para cubrir uno o varios tipos de escaneos.
- Las herramientas mandan paquetes a distintos puertos con el fin de ver cuál es el que se encuentra abierto.



Prevención

Escaneo

IDS(Intrusion Detection System)

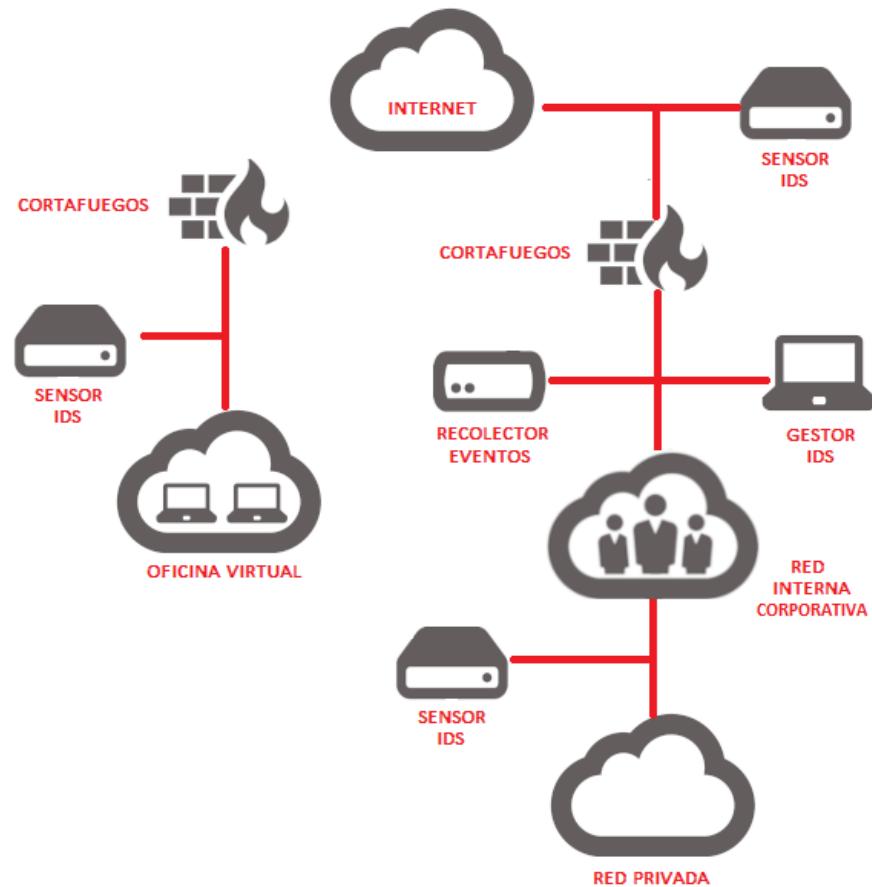
- Es una aplicación que sirve para detectar accesos no autorizados a un computador o a una red.
- Monitorizan el tráfico entrante y compara con una base de datos la entrada.
- Si hay una sospecha emite una alerta.
- No tratan de mitigar la intrusión, solo emite la alerta para que se tomen medidas.
- Nos permite ver en tiempo real lo que sucede en la red.



IPS(Intrusion Prevention System)

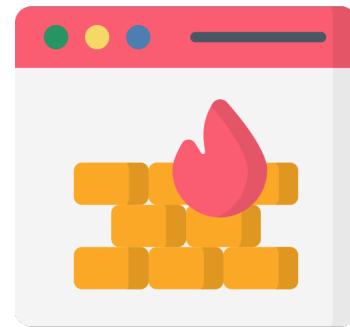
- Es un software que se usa para proteger a los sistemas de ataques e intrusiones.
- Analiza en tiempo real las conexiones y protocolos para ver si va a ocurrir o esta ocurriendo un incidente.
- Identifica ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red.
- Puede defenderse frente a múltiples ataques, como intrusiones, ataques de fuerza bruta, infecciones por malware o modificaciones del sistema de archivos, entre otros;

Escaneo de puertos



Escaneo de puertos

- El firewall debe de permitir analizar los datos dentro de los paquetes y no solo las cabeceras TCP.
- Los sistemas se utilizan para identificar métodos de detección de sistema operativos llevados por distintas herramientas, como por ejemplo Nmap.
- Se debe de tener abierto solo los puertos que se van a utilizar.



NIDS O HIDS

- **Sistemas de detección de intrusiones en red (NIDS)**

- Buscan actividades sospechosas en host únicos.
- IDS que trabaja con los datos que circulan a través de la red o de un segmento de red.
- Se dedica a monitorizar la red en busca de intentos de posibles accesos no autorizados.
- Complemento al sistema de seguridad.
- Análisis posterior en caso de intrusión.
- Alerta ante ataques.

NIDS O HIDS

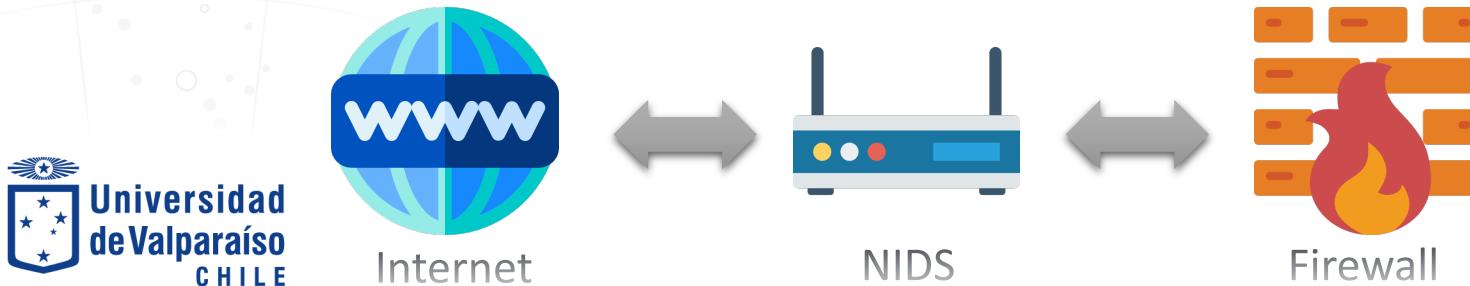
- **Sistemas de detección de intrusiones en red (NIDS)**
 - Monitoriza todo el tráfico que pasa por un segmento de red en busca de intentos de posibles malos usos o accesos no autorizados.
 - Filtra el tráfico para descartar lo que no interesa mediante reglas que pueden crear alertas, además de comprar tráfico con reglas del programa.
 - Detecta tráfico maligno, habitualmente mediante un conjunto de reglas.
 - Se debe de estudiar el lugar en donde se va a instalar, depende de la estructura de red.

NIDS O HIDS

- **Sistemas de detección de intrusiones en red (NIDS)**
- Un NIDS se puede colocar:
 - Delante de la red.
 - Detrás de la red.
 - Mixto.

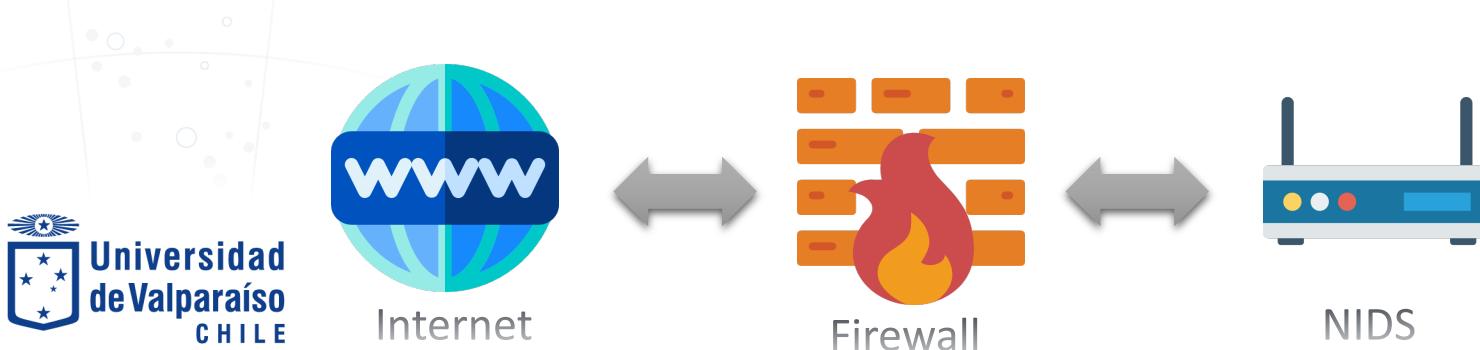
NIDS O HIDS

- **Sistemas de detección de intrusiones en red (NIDS)**
- Un NIDS se puede colocar: **Delante**
 - Se pueden comprobar todos los ataques que se produzcan. No todos tendrán éxito.
 - Genera gran cantidad de información en los logs.
 - Firewall bloqueará los ataques.
 - Exceso de información puede ser contraproducente. Perder de vista ataques efectivos.



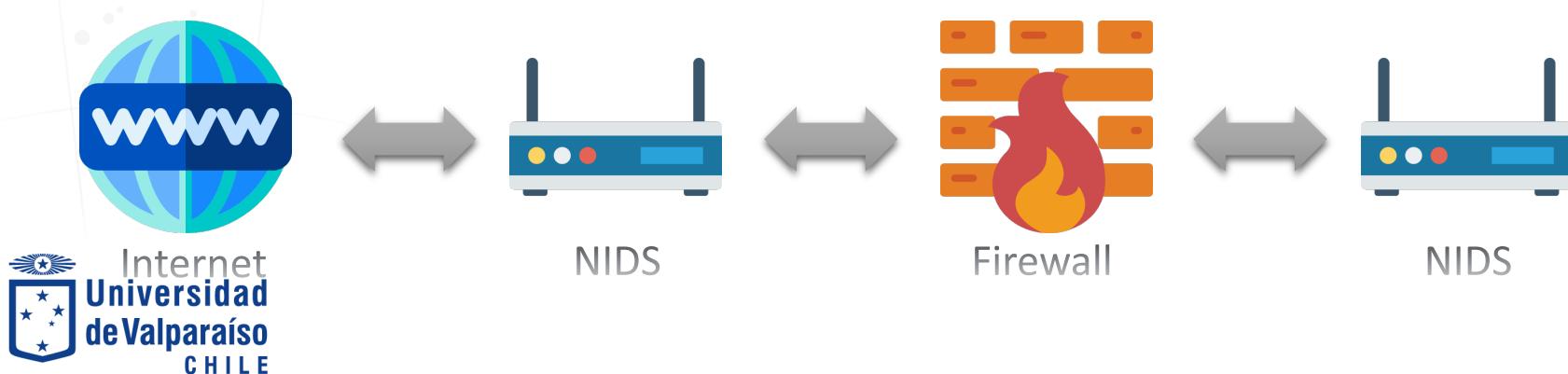
NIDS o HIDS

- **Sistemas de detección de intrusiones en red (NIDS)**
- Un NIDS se puede colocar: **Detrás**
- Monitoriza únicamente el tráfico que haya entrado realmente en la red, no ha sido bloqueado por el firewall.
- Cantidad de logs inferior.
- Los ataques detectados son potencialmente mucho más peligrosos.



NIDS O HIDS

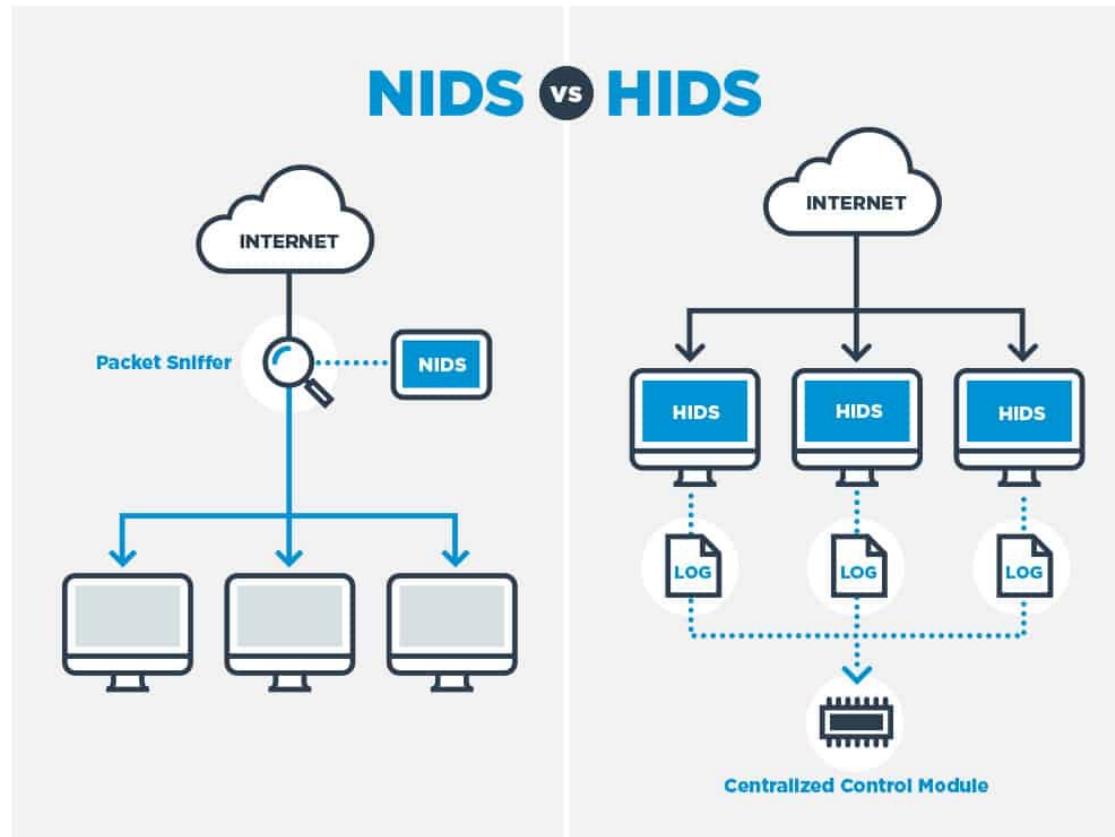
- **Sistemas de detección de intrusiones en red (NIDS)**
- Un NIDS se puede colocar: **Mixto**
- El control es mucho mayor.
- Ir mejorando la seguridad cuando se ve que deja pasar tráfico que no debería.
- Se puede detectar ataques en ambos lados

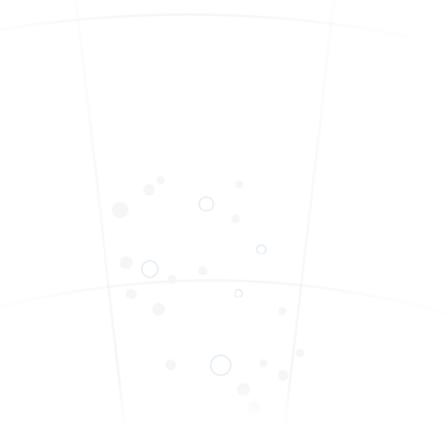


NIDS O HIDS

- **Sistemas de detección de intrusiones de host (HIDS)**
 - Trabaja con la información recogida dentro de un solo Host.
 - Examina los datos de eventos una vez que se han almacenado en registro.
 - Analiza los eventos en un dispositivo.
 - Solo detecta actividades sospechosas, no las previene.

NIDS O HIDS





CVE(Common Vulnerabilities and Exposures)

Escaneo

CVE(Common Vulnerabilities and Exposures)

```
(root💀kali)-[~/home/marco] # nmap --script=vuln 10.211.55.8
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-07 00:26 -03
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|       After NULL UDP avahi packet DoS (CVE-2011-1002).
|       Hosts are all up (not vulnerable).
```

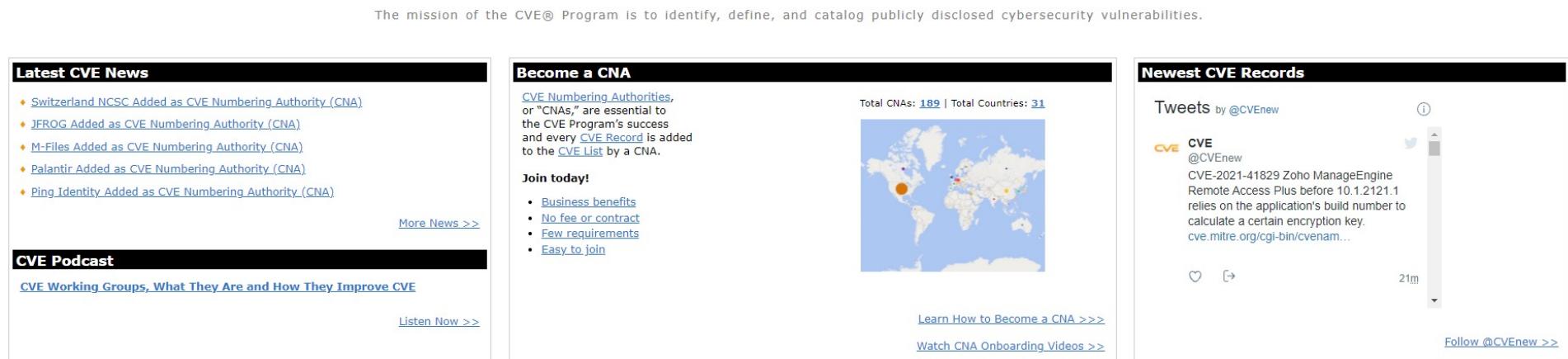
CVE(Common Vulnerabilities and Exposures)

- Es una lista de información registrada sobre vulnerabilidades de seguridad conocidas en la que cada referencia tiene un número de identificación CVE-ID, descripción de la vulnerabilidad, que versiones del software están afectadas, posible solución al fallo (si existe) o como configurar para mitigar la vulnerabilidad y referencias a publicaciones o entradas de foros o blog donde se ha hecho pública la vulnerabilidad o se demuestra su explotación.
- Es definido y es mantenido por The MITRE Corporation con fondos de la National Cyber Security Division del gobierno de los Estados Unidos de América. Forma parte del llamado Security Content Automation Protocol.

CVE(Common Vulnerabilities and Exposures) : <https://cve.mitre.org/>



The screenshot shows the official CVE website. At the top, there's a navigation bar with links for "CVE List", "CNAs", "WGs", "Board", "About", and "News & Blog". On the right, there's a "NVD" logo with options to "Go to for: CVSS Scores" and "CPE Info". Below the navigation is a main menu with "Search CVE List" (which is highlighted with a red box), "Downloads", "Data Feeds", "Update a CVE Record", and "Request CVE IDs". A message below the menu states "TOTAL CVE Records: 161578". A notice at the bottom of the page says "NOTICE: CVE website transitioning to new "CVE.ORG" web address. Process to begin in late September 2021 and last one year. ([details](#))".



The main content area is divided into three sections:

- Latest CVE News**: Lists recent additions to the CVE Numbering Authority (CNA) program, such as Switzerland NCSC, JFrog, M-Files, Palantir, and Ping Identity.
- Become a CNA**: Explains what CNAs are, their importance to the CVE Program, and how to join. It includes a map of the world with orange dots representing CNAs and links to learn more and watch onboarding videos.
- Newest CVE Records**: Shows a tweet from @CVEnew about a specific vulnerability (CVE-2021-41829) and provides a link to follow them on Twitter.

Page Last Updated or Reviewed: September 28, 2021

[Site Map](#) | [Terms of Use](#) | [Privacy Policy](#) | [Contact Us](#) | Follow CVE

Use of the CVE® List and the associated references from this website are subject to the [terms of use](#). CVE is sponsored by the U.S. Department of Homeland Security (DHS) [Cybersecurity and Infrastructure Security Agency \(CISA\)](#). Copyright © 1999–2021, [The MITRE Corporation](#). CVE is a registered trademark and the CVE logo is a trademark of The MITRE Corporation.



CVE(Common Vulnerabilities and Exposures)

[CVE List](#)[CNAs](#)[WG](#)s[Board](#)[About](#)[News & Blog](#)**NVD**

Go to for:

[CVSS Scores](#)[CPE Info](#)[Search CVE List](#)[Downloads](#)[Data Feeds](#)[Update a CVE Record](#)[Request CVE IDs](#)

TOTAL CVE Records: 161578

NOTICE: CVE website transitioning to new "CVE.ORG" web address. Process to begin in late September 2021 and last one year. ([details](#))

HOME > CVE LIST > SEARCH CVE LIST

Search CVE List

You can search the CVE List for a [CVE Record](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records.

View the [search tips](#).

CVE/Crosses Vulnerabilities and Exposures



[CVE List](#)
[CNAs](#)
[WGs](#)
[Board](#)
[About](#)
[News & Blog](#)

NVD
 Go to for:
[CVSS Scores](#)
[CPE Info](#)

[Search CVE List](#) [Downloads](#) [Data Feeds](#) [Update a CVE Record](#) [Request CVE IDs](#)

TOTAL CVE Records: 161578

NOTICE: CVE website transitioning to new "CVE.ORG" web address. Process to begin in late September 2021 and last one year. ([details](#))

HOME > CVE > SEARCH RESULTS

Search Results

There are 50 CVE Records that match your search.

Name	Description
CVE-2021-3130	Within the Open-Audit up to version 3.5.3 application, the web interface hides SSH secrets, Windows passwords, and SNMP strings from users using HTML 'password field' obfuscation. By using Developer tools or similar, it is possible to change the obfuscation so that the credentials are visible.
CVE-2018-7750	transport.py in the SSH server implementation of Paramiko before 1.17.6, 1.18.x before 1.18.5, 2.0.x before 2.0.8, 2.1.x before 2.1.5, 2.2.x before 2.2.3, 2.3.x before 2.3.2, and 2.4.x before 2.4.1 does not properly check whether authentication is completed before processing other requests, as demonstrated by channel-open. A customized SSH client can simply skip the authentication step.
CVE-2018-19518	University of Washington IMAP Toolkit 2007 on UNIX, as used in imap_open() in PHP and other products, launches an rsh command (by means of the imap_rimap function in c-client/imap4r1.c and the tcp_aopen function in osdep/unix/tcp_unix.c) without preventing argument injection, which might allow remote attackers to execute arbitrary OS commands if the IMAP server name is untrusted input (e.g., entered by a user of a web application) and if rsh has been replaced by a program with different argument semantics. For example, if rsh is a link to ssh (as seen on Debian and Ubuntu systems), then the attack can use an IMAP server name containing a "-oProxyCommand" argument.
CVE-2018-0484	A vulnerability in the access control logic of the Secure Shell (SSH) server of Cisco IOS and IOS XE Software may allow connections sourced from a virtual routing and forwarding (VRF) instance despite the absence of the vrf-also keyword in the access-class configuration. The vulnerability is due to a missing check in the SSH server. An attacker could use this vulnerability to open an SSH connection to an affected Cisco IOS or IOS XE device with a source address belonging to a VRF instance. Once connected, the attacker would still need to provide valid credentials to access the device.
CVE-2018-0035	QFX5200 and QFX10002 devices that have been shipped with Junos OS 15.1X53-D21, 15.1X53-D30, 15.1X53-D31, 15.1X53-D32, 15.1X53-D33 and 15.1X53-D60 or have been upgraded to these releases using the .bin or .iso images may contain an unintended additional Open Network Install Environment (ONIE) partition. This additional partition allows the superuser to reboot to the ONIE partition which will wipe out the content of the Junos partition and its configuration. Once rebooted, the ONIE partition will not have root password configured, thus any user can access the console or SSH, using an IP address acquired from DHCP, as root without password. Once the device has been shipped or upgraded with the ONIE partition installed, the issue will persist. Simply upgrading to higher release via the CLI will not resolve the issue. No other Juniper Networks products or platforms are affected by this issue.
CVE-2017-14728	An authentication bypass was found in an unknown area of the SiteOmat source code. All SiteOmat BOS versions are affected, prior to the submission of this exploit. Also, the SiteOmat does not force administrators to switch passwords, leaving SSH and HTTP remote authentication open to public.
CVE-2016-8858	** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."
CVE-2016-6515	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.
CVE-2016-3115	Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions.
CVE-2016-2230	OpenELEC and RasPlex devices have a hardcoded password for the root account, which makes it easier for remote attackers to obtain access via an SSH session.
CVE-2016-1908	The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.
CVE-2016-1907	The ssh_packet_read_poll2 function in packet.c in OpenSSH before 7.1p2 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via crafted network traffic.
CVE-2016-10012	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allow local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.
CVE-2016-10011	authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child

CHILE

CVE (Common Vulnerabilities and Exposures)

NVD
Go to for:
[CVSS Scores](#)
[CPE Info](#)

Search CVE List **Downloads** **Data Feeds** **Update a CVE Record** **Request CVE IDs**

TOTAL CVE Records: 161578

NOTICE: CVE website transitioning to new "CVE.ORG" web address. Process to begin in late September 2021 and last one year. ([details](#))

HOME > CVE > CVE-2021-3130

[Printer-Friendly View](#)

CVE-ID	
CVE-2021-3130	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Within the Open-AudIT up to version 3.5.3 application, the web interface hides SSH secrets, Windows passwords, and SNMP strings from users using HTML 'password field' obfuscation. By using Developer tools or similar, it is possible to change the obfuscation so that the credentials are visible.	
References	
<p>Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none">MISC:https://opmantek.com/network-discovery-inventory-software/MISC:https://raw.githubusercontent.com/B0D0B0P0T/CVE/main/CVE-2021-3130	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20210112	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20210112)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is a record on the CVE List , which provides common identifiers for publicly known cybersecurity vulnerabilities.	
SEARCH CVE USING KEYWORDS: <input type="text"/> <input type="button" value="Submit"/>	
You can also search by reference using the CVE Reference Maps .	

CHILE

CVSS(Common Vulnerability Scoring System)

Escaneo

Common Vulnerability Scoring System

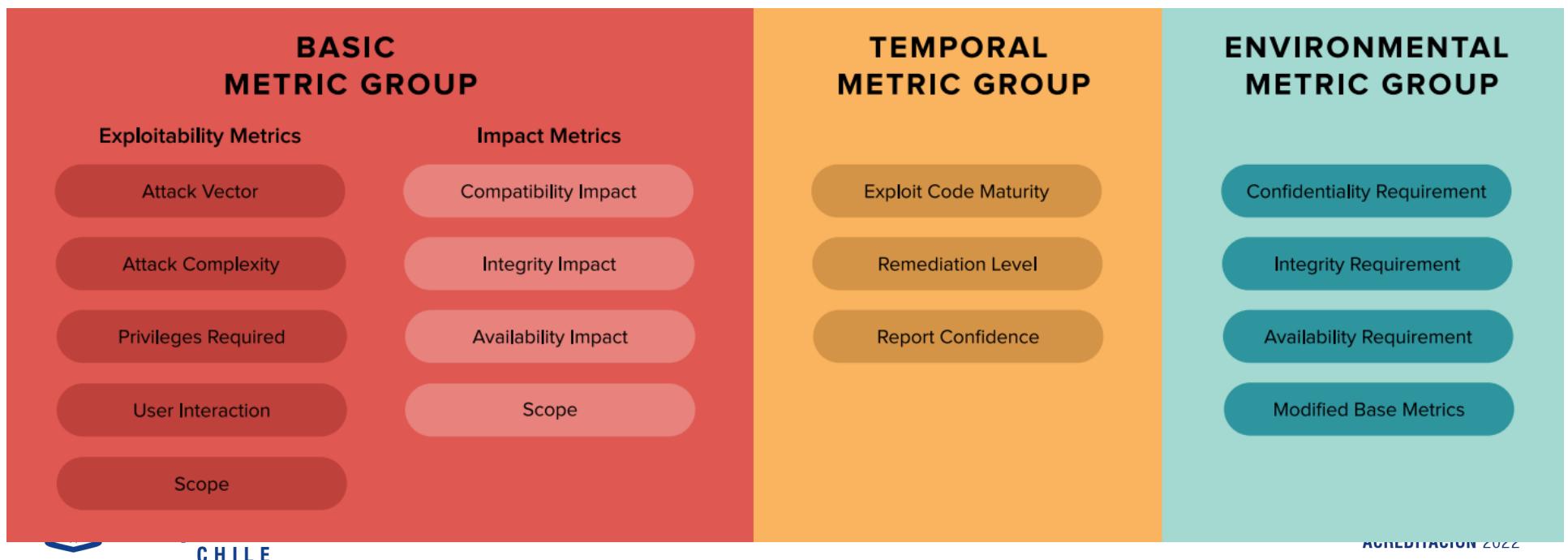
- Es un sistema de puntaje diseñado para proveer un método abierto y estándar que permite estimar el impacto derivado de vulnerabilidades identificadas en TI.
- Contribuye a cuantificar la severidad que pueden representar dichas vulnerabilidades.
- CVSS se encuentra bajo la defensa de Forum of Incident Response and Security Teams (FIRST), pero es un estándar completamente abierto, por lo que puede ser utilizado libremente.

Common Vulnerability Scoring System

- Da una medida de criticidad de las vulnerabilidades encontradas.
- Consta de diferentes tres diferentes métricas:
 - Base
 - Temporal
 - Ambiental

Common Vulnerability Scoring System

- Se produce una puntuación que va de 0 a 10, que luego se puede modificar al puntuar las métricas Temporal y Ambiental.



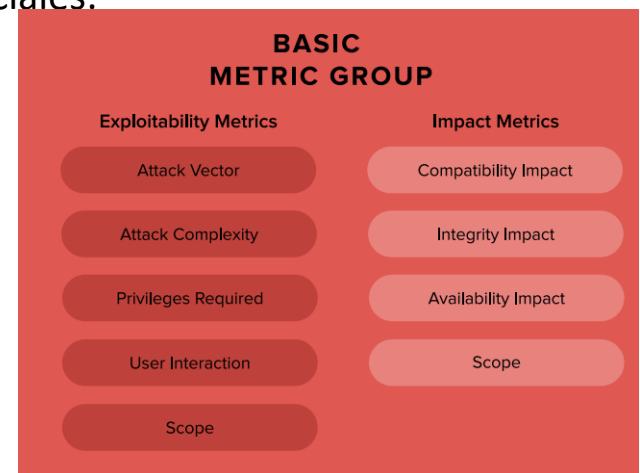
Common Vulnerability Scoring System

- El grupo métrico base representa las características de la propia vulnerabilidad. Estas características no cambian con el tiempo y no dependen de la explotabilidad del mundo real o de los factores de compensación que una empresa ha puesto en marcha para prohibir la explotación.
- Las métricas base tienen dos subgrupos:
 - Métricas de explotabilidad
 - Métricas de impacto



Common Vulnerability Scoring System

- **Métricas de explotabilidad.** Las métricas de explotabilidad se relacionan específicamente con lo que es vulnerable, sin tener en cuenta ninguna configuración específica u otros controles de compensación.
- Las métricas de explotabilidad tienen cuatro componentes oficiales:
 - Vector de ataque
 - Complejidad de ataque
 - Privilegios requeridos
 - Interacción del usuario.



Common Vulnerability Scoring System

- **Métricas de explotabilidad.**
 - **Vector de ataque**
 - El vector de ataque es un indicador del nivel de acceso necesario para que un atacante aproveche la vulnerabilidad. Una vulnerabilidad que requiere acceso físico a un sistema de destino es mucho más difícil de explotar que una que se puede explotar de forma remota a través de Internet.
 - Ej. Correo electrónico(pishing)

Common Vulnerability Scoring System

- **Métricas de explotabilidad.**
 - **Complejidad de ataque**
 - Esta métrica indica condiciones más allá del control del atacante que deben existir para explotar la vulnerabilidad. Por lo general, esto se refiere a la interacción requerida del usuario o configuraciones específicas del sistema de destino.
 - Ej. Se puede considerar una complejidad alta cuando tiene que tener privilegios o hacer muchas cosas en cambio, es baja cuando el exploit se ejecuta fácilmente.

Common Vulnerability Scoring System

- **Métricas de explotabilidad.**
 - **Privilegios requeridos**
 - Esta métrica indica condiciones más allá del control del atacante que deben existir para explotar la vulnerabilidad. Por lo general, esto se refiere a la interacción requerida del usuario o configuraciones específicas del sistema de destino.
 - EJ. Por ejemplo, una inyección de código arbitrario en WordPress MU permitió a los usuarios autenticados cargar y ejecutar archivos maliciosos de forma remota

Common Vulnerability Scoring System

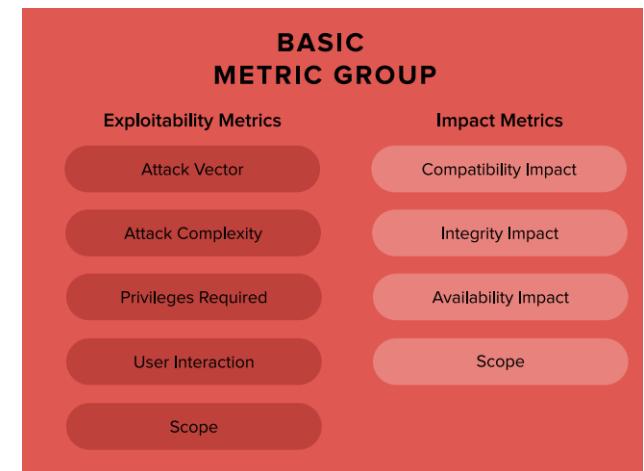
- **Métricas de explotabilidad.**
 - **Interacción del usuario.**
 - La métrica de Interacción del usuario describe si un usuario, que no sea el atacante, debe hacer algo o participar en la explotación de la vulnerabilidad.
 - Ej. Un ataque requiere que el usuario víctima se una a un dominio, agregue una cuenta de usuario, comparta una impresora o una acción similar. El atacante debe esperar a que se produzca una acción.

Common Vulnerability Scoring System

- **Alcance.**
 - Se refiere a si una vulnerabilidad en un componente puede propagarse a otros componentes (movimiento horizontal). La puntuación del alcance es mayor si la propagación es posible.
 - Ejemplo: la capacidad de acceder y explotar el sistema operativo subyacente después de explotar una vulnerabilidad en una aplicación de software

Common Vulnerability Scoring System

- **Métricas de impacto**
- Las métricas de impacto miden el impacto en la conocida tríada CIA (confidencialidad, integridad, disponibilidad) del sistema afectado. En otras palabras, cuál es el resultado negativo final que se produce como resultado de la explotación.



Common Vulnerability Scoring System

- **Métricas de impacto**
 - **Confidencialidad**
 - La confidencialidad se refiere a la divulgación de información sensible a usuarios autorizados y no autorizados, con el objetivo de que solo los usuarios autorizados puedan acceder a los datos de destino.
 - Ej. Un atacante puede suplantar a un usuario y acceder a los recursos de la víctima en el servidor vulnerable.

Common Vulnerability Scoring System

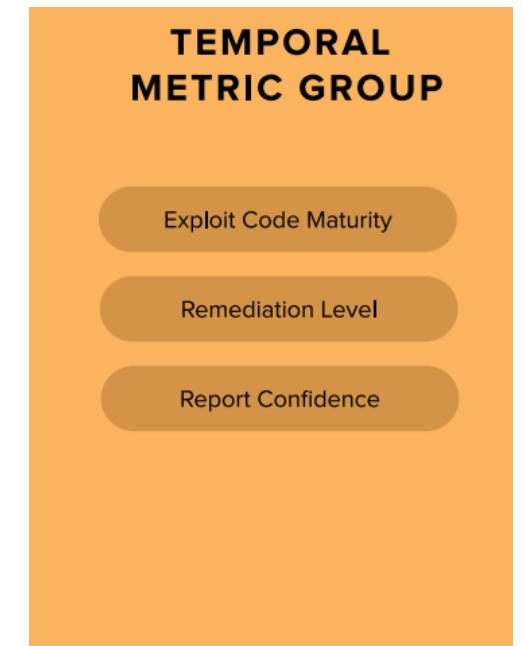
- **Métricas de impacto**
 - **Integridad**
 - La integridad se refiere a si la información protegida ha sido manipulada o modificada de alguna manera. Si no hay forma de que un atacante altere la precisión o integridad de la información, se ha mantenido la integridad.
 - Ej. Un atacante puede suplantar a un usuario y modificar cualquier recurso del usuario en el servidor vulnerable.

Common Vulnerability Scoring System

- **Métricas de impacto**
 - **Disponibilidad**
 - La información debe ser accesible según sea necesario. Si un ataque hace que la información no esté disponible, como cuando un sistema falla o a través de un ataque DDOS, la disponibilidad se ve afectada negativamente.
 - EJ. un atacante puede leer o escribir archivos en un servidor haciendo que se tenga que cerrar el servidor.

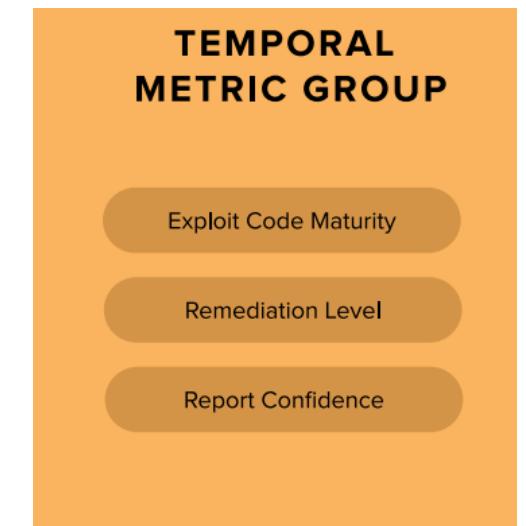
Common Vulnerability Scoring System

- Las métricas temporales miden la explotabilidad actual de la vulnerabilidad, así como la disponibilidad de controles de corrección, como un parche.
- Esta métrica contiene 3 componentes:
 - Madurez del código de explotación.
 - Nivel de corrección
 - Confianza del informe.



Common Vulnerability Scoring System

- **Métricas temporales.**
 - **Madurez del código de explotación.**
 - El código disponible para realizar un exploit puede madurar, volviéndose más estable y más disponible con el tiempo. A medida que esto suceda, la puntuación de este subcomponente aumentará.
 - Ej. El código para explotar la vulnerabilidad siempre se mantiene actualizado



Common Vulnerability Scoring System

- **Métricas temporales.**
 - **Nivel de corrección.**
 - Cuando se descubre una vulnerabilidad por primera vez, es posible que no haya un parche u otra solución alternativa disponible. Con el tiempo, las soluciones están disponibles, lo que reduce la puntuación de vulnerabilidad a medida que se mejora la reparación.
 - Ej. Se mantiene actualizado el software para evitar vulnerabilidad.

TEMPORAL METRIC GROUP

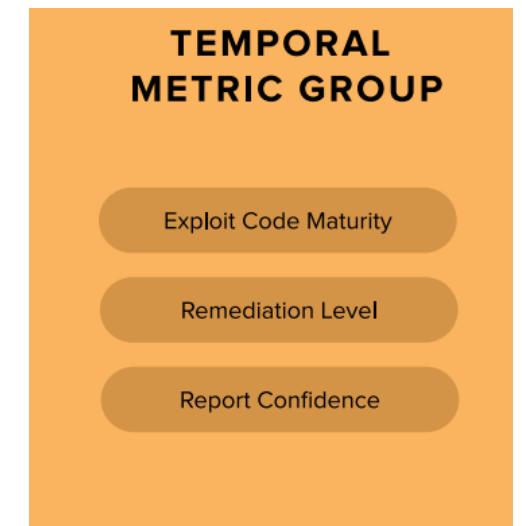
Exploit Code Maturity

Remediation Level

Report Confidence

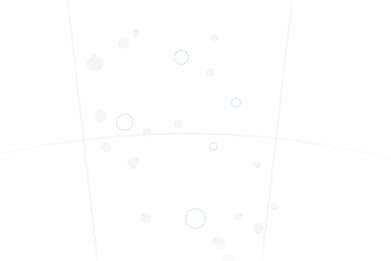
Common Vulnerability Scoring System

- **Métricas temporales.**
 - **Confianza del informe.**
 - La confianza mide el nivel de validación que demuestra que una vulnerabilidad es real y explotable.
 - EJ. La Vulnerabilidad ha sido probada y reconocida por el proveedor.



Common Vulnerability Scoring System

- Las métricas ambientales permiten a la organización modificar el CVSS base en función de los requisitos de seguridad y las modificaciones de las métricas base.
- Esta métrica contiene componentes:
 - Requisitos de seguridad.
 - Métricas base modificadas.



ENVIRONMENTAL METRIC GROUP

Confidentiality Requirement

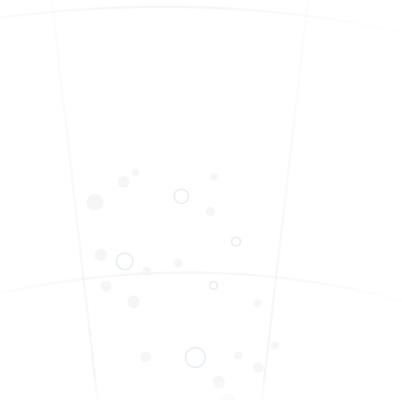
Integrity Requirement

Availability Requirement

Modified Base Metrics

Common Vulnerability Scoring System

- **Métricas ambientales .**
 - **Requerimiento de confidencialidad.**
 - Mide el impacto en la confidencialidad de los recursos de información administrados por un componente de software debido a una vulnerabilidad explotada con éxito.



ENVIRONMENTAL METRIC GROUP

Confidentiality Requirement

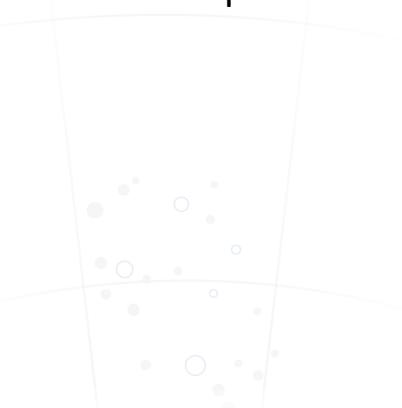
Integrity Requirement

Availability Requirement

Modified Base Metrics

Common Vulnerability Scoring System

- **Métricas ambientales .**
 - **Requerimiento de integridad.**
 - La confianza mide el nivel de validación que demuestra que una vulnerabilidad es real y explotable.



ENVIRONMENTAL METRIC GROUP

Confidentiality Requirement

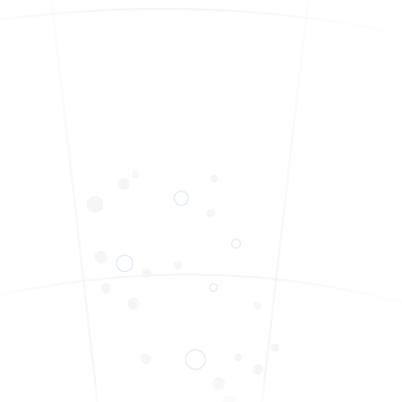
Integrity Requirement

Availability Requirement

Modified Base Metrics

Common Vulnerability Scoring System

- **Métricas ambientales .**
 - **Requerimiento de disponibilidad.**
 - Mide el impacto en la disponibilidad del componente afectado como resultado de una vulnerabilidad explotada con éxito.



ENVIRONMENTAL METRIC GROUP

Confidentiality Requirement

Integrity Requirement

Availability Requirement

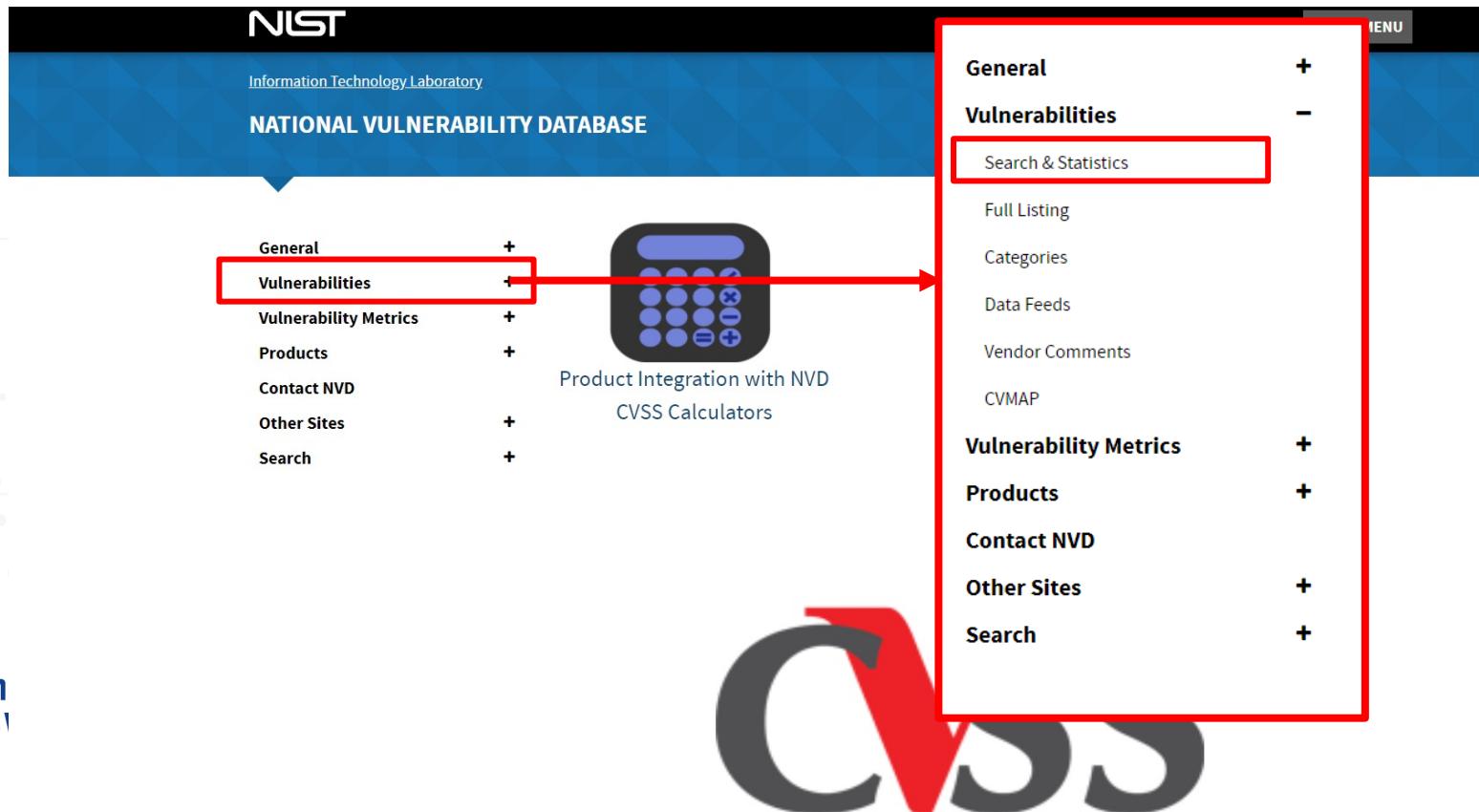
Modified Base Metrics

Common Vulnerability Scoring System

- **Métricas ambientales .**
 - **Métricas base modificadas.**
 - La confianza mide el nivel de validación que demuestra que una vulnerabilidad es real y explotable.
 - Estas métricas permiten anular las métricas base individuales en función de las características específicas del entorno de un usuario.
 - Las características que afectan la explotabilidad, el alcance o el impacto se pueden reflejar a través de un puntaje ambiental modificado de manera apropiada.

Common Vulnerability Scoring System

- <https://nvd.nist.gov/vuln-metrics/cvss>



Common Vulnerability Scoring System

VULNERABILITIES

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions.

Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

Search Type

Basic Advanced

Results Type

Overview Statistics

Keyword Search

Exact Match

Search Type

All Time Last 3 Months Last 3 Years

Contains HyperLinks

US-CERT Technical Alerts
 US-CERT Vulnerability Notes
 OVAL Queries

Common Vulnerability Scoring System

[VULNERABILITIES](#)[SEARCH AND STATISTICS](#)

Q Search Results (Refine Search)

Sort results by: Publish Date Descending ▾ [Sort](#)

Search Parameters:

- Results Type: Overview
- Keyword (text search): open ssh 6.6
- Search Type: Search All
- CPE Name Search: false

There are **2** matching records.

Displaying matches **1** through **2**.

Vuln ID	Summary	CVSS Severity
CVE-2014-2653	The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.	V3.x:(not available) V2.0: 5.8 MEDIUM
CVE-2014-2532	sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.	V3.0: 4.9 MEDIUM V2.0: 5.8 MEDIUM

Common Vulnerability Scoring System

- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

NATIONAL VULNERABILITY DATABASE

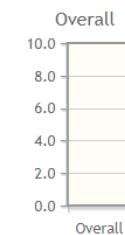
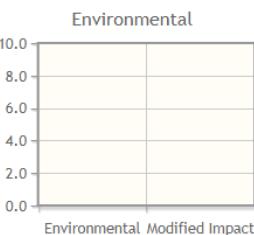
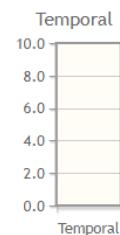
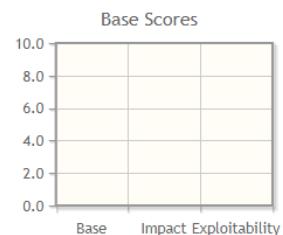
NVD

VULNERABILITY METRICS

CVSS Version 3.0 CVSS Version 3.1

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: NA
Impact Subscore: NA
Exploitability Subscore: NA
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: NA

Show Equations

Common Vulnerability Scoring System

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

Common Vulnerability Scoring System

Temporal Score Metrics

Exploit Code Maturity (E)

Not Defined (E:X) Unproven that exploit exists (E:U) Proof of concept code (E:P) Functional exploit exists (E:F) High (E:H)

Remediation Level (RL)

Not Defined (RL:X) Official fix (RL:O) Temporary fix (RL:T) Workaround (RL:W) Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X) Unknown (RC:U) Reasonable (RC:R) Confirmed (RC:C)

Common Vulnerability Scoring System

Environmental Score Metrics

Exploitability Metrics

Attack Vector (MAV)

Not Defined (MAV:X)	Network (MAV:N)	Adjacent Network (MAV:A)
Local (MAV:L)	Physical (MAV:P)	

Attack Complexity (MAC)

Not Defined (MAC:X)	Low (MAC:L)	High (MAC:H)
---------------------	-------------	--------------

Privileges Required (MPR)

Not Defined (MPR:X)	None (MPR:N)	Low (MPR:L)	High (MPR:H)
---------------------	--------------	-------------	--------------

User Interaction (MUI)

Not Defined (MUI:X)	None (MUI:N)	Required (MUI:R)
---------------------	--------------	------------------

Scope (MS)

Not Defined (MS:X)	Unchanged (MS:U)	Changed (MS:C)
--------------------	------------------	----------------

Impact Metrics

Confidentiality Impact (MC)

Not Defined (MC:X)	None (MC:N)	Low (MC:L)
High (MC:H)		

Integrity Impact (MI)

Not Defined (MI:X)	None (MI:N)	Low (MI:L)
High (MI:H)		

Availability Impact (MA)

Not Defined (MA:X)	None (MA:N)	Low (MA:L)
High (MA:H)		

Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:X)	Low (CR:L)
Medium (CR:M)	High (CR:H)

Integrity Requirement (IR)

Not Defined (IR:X)	Low (IR:L)	Medium (IR:M)
High (IR:H)		

Availability Requirement (AR)

Not Defined (AR:X)	Low (AR:L)
Medium (AR:M)	High (AR:H)

Common Vulnerability Scoring System (Vulnerabilidad en GNU Bash (CVE-2014-7169))

Tipo: Neutralización incorrecta de elementos especiales usados en un comando de sistema operativo (Inyección de comando de sistema operativo)

Gravedad: Alta 

Fecha publicación: 24/09/2014

Última modificación: 30/11/2018

Descripción

GNU Bash hasta 4.3 bash43-025 procesa cadenas finales después de la definición malformada de funciones en los valores de variables de entorno, lo que permite a atacantes remotos escribir hacia ficheros o posiblemente tener otro impacto desconocido a través de un entorno manipulado, tal y como se ha demostrado por vectores que involucran la característica ForceCommand en sshd OpenSSH, los módulos mod_cgi y mod_cgid en el Apache HTTP Server, scripts ejecutados por clientes DHCP no especificados, y otras situaciones en la cual establecer el entorno ocurre a través de un límite privilegiado de la ejecución de Bash. Nota: Esta vulnerabilidad existe debido a una solución incompleta para CVE-2014-6271.

Impacto

Vector de acceso: A través de red

Complejidad de Acceso: Baja

Autenticación: No requerida para explotarla

Tipo de impacto: Compromiso total de la integridad del sistema + Compromiso total de la confidencialidad del sistema + Compromiso total de la disponibilidad del sistema

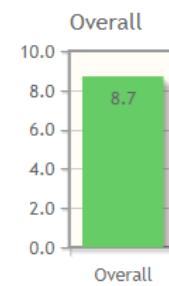
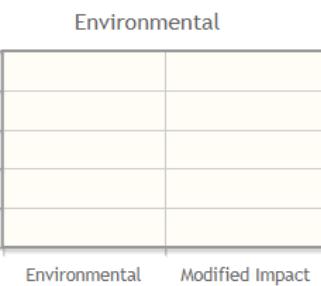
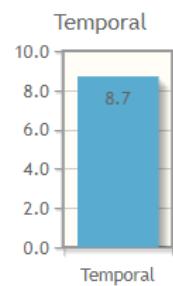


Common Vulnerability Scoring System (Vulnerabilidad en GNU Bash (CVE-2014-7169))

CVSS Version 2

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 10.0
Impact Subscore: 10.0
Exploitability Subscore: 10.0
CVSS Temporal Score: 8.7
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.7

Show Equations

CVSS v2 Vector
(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:OF/RC:C)

Common Vulnerability Scoring System (Vulnerabilidad en GNU Bash (CVE-2014-7169))

Base Score Metrics

Exploitability Metrics

Access Vector (AV)*

Local (AV:L) Adjacent Network (AV:A) **Network (AV:N)**

Access Complexity (AC)*

High (AC:H) Medium (AC:M) **Low (AC:L)**

Authentication (Au)*

Multiple (Au:M) Single (Au:S) **None (Au:N)**

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Partial (C:P) **Complete (C:C)**

Integrity Impact (I)*

None (I:N) Partial (I:P) **Complete (I:C)**

Availability Impact (A)*

None (A:N) Partial (A:P) **Complete (A:C)**

Temporal Score Metrics

Exploitability (E)

Not Defined (E:ND) Unproven that exploit exists (E:U) Proof of concept code (E:POC) Functional exploit exists (E:F) **High (E:H)**

Remediation Level (RL)

Not Defined (RL:ND) **Official fix (RL:OF)** Temporary fix (RL:TF) Workaround (RL:W) Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:ND) Unconfirmed (RC:UC) Uncorroborated (RC:UR) **Confirmed (RC:C)**



Para finalizar

Escaneo

Escaneo

- Es el proceso de descubrir e identificar puertos y vulnerabilidades en una red.
- Este proceso puede generar una gran cantidad de tráfico, pudiendo también inducir a condiciones de negación de servicio en dispositivos de red.
- Una herramienta capaz de realizar un escaneo de puertos y vulnerabilidades es Nmap.



Escaneo

- Con la información recolectada se confirma lo obtenido en la fase de reconocimiento.
- Se obtiene versiones de componentes y así investigar vulnerabilidades que tienen.
- CVE permite tener información actualizada.
- CVSS permite priorizar la mitigación de vulnerabilidades.



Dudas .. Consultas....

