



TALLER APLICADO DE SEGURIDAD DE LA INFORMACIÓN



Ataques de red, hardware y software

Unidad 1

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yañez

ELABORACIÓN

Experto disciplinar: Eder Moran Heredia

Diseñador instruccional: Antonio Colmenares Prieto

Editora instruccional: María José Fonseca Palacios

VALIDACIÓN

Experto disciplinar: Alex Flores Fuentealba

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

AÑO

2022

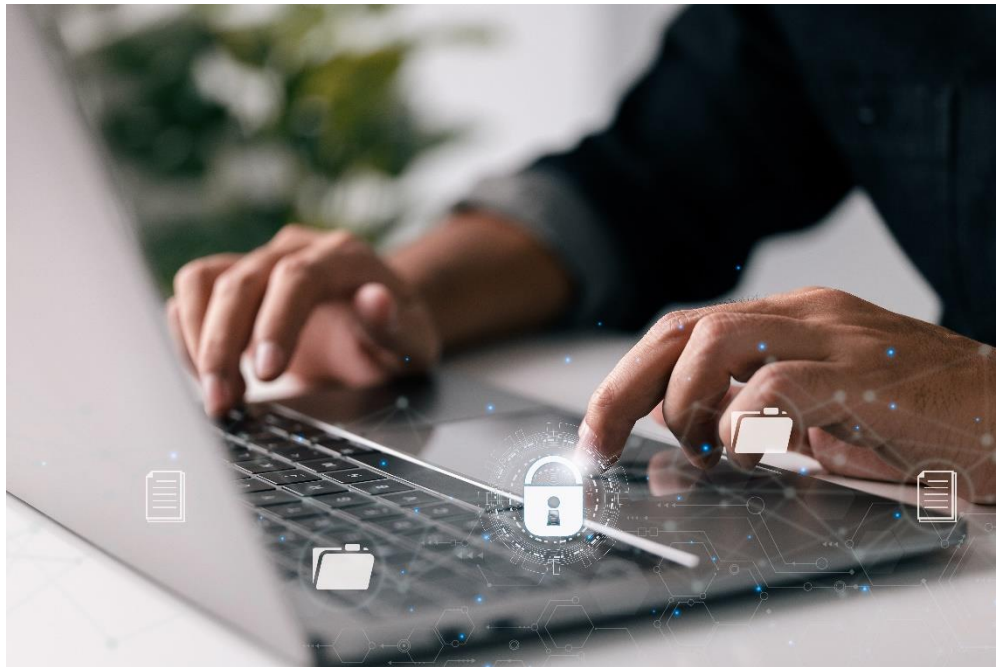
Tabla de contenidos

Aprendizaje esperado.....	5
Introducción	6
1. Conceptos de escaneo de redes.....	7
1.1 Visión general del escaneo de redes.....	8
1.2 TCP/IP comunicaciones	8
1.2.1 Capa de aplicación	10
1.2.2 Capa de transporte	10
1.2.3 Capa de internet.....	11
1.2.4 Capa de acceso a la red	12
2. Herramientas de escaneo de redes	13
2.1 NMAP	13
2.2 Hping 2/Hping3	14
2.3 Herramientas de escaneo para móviles.....	15
2.3.1 Zabbix	15
2.3.2 Nagios	16
3. Técnicas de escaneo de redes.....	18
3.1 ICMP Scanning.....	18

3.2 TCP SCANNING	19
3.2.1 Técnicas de escaneo de puertos	19
3.3 UDP Scanning.....	21
Cierre	23
Referencias.....	24

Aprendizaje esperado

Aplican técnicas de escaneo de redes en el marco de Ethical Hacking, de acuerdo a los estándares de la industria.



Introducción

Las TIC (Tecnologías de la Información y la Comunicación) y especialmente la informática, están alojadas en todos los entornos de la sociedad: desde la prensa hasta la educación. Siendo cada vez más beneficioso e indispensable para el desarrollo de las actividades diarias. Antiguamente para realizar una transacción bancaria, era necesario desplazarse físicamente a la sucursal de banco más cercana. En la actualidad es posible hacer una transferencia en solo 5 segundos desde el teléfono móvil y lo fabuloso, es que se puede realizar desde cualquier parte del planeta; reduciendo tiempo, riesgos y recursos.

De igual forma que crece el uso de la informática, la seguridad informática debe tener una relevancia cada vez mayor, considerando que el funcionamiento correcto de sus sistemas nos brindará una mejor protección a nuestros datos. A pesar de ello, aun si se reducen riesgos, no estamos exentos de ser víctimas de algún delito digital.

Todos estamos inmersos en esta era tecnológica, pero la pregunta es: ¿usted cree, que estamos prevenidos para evitar el robo de información digital que viaja en internet?, como: contraseñas, tarjetas de crédito, entre otros.

Durante el avance del módulo, visualizaremos que las amenazas, medidas de protección y vulnerabilidades ha ido en crecimiento y cambiando sus variantes con el tiempo. Para ello haremos uso de conceptos básicos de seguridad de datos, comenzando a entender los

tres principios de la seguridad de la información (confidencialidad, integridad y disponibilidad) y cuál es su objetivo principal.

Finalizaremos identificando los factores accidentales e intenciones de error, teniendo en cuenta las amenazas latentes en la actualidad como: phishing, vishing, ingeniería social, ataque anti DoS, entre otros.

Con todo ello, se busca que el estudiante controle la seguridad de datos al interior de una instalación computacional.

1. Conceptos de escaneo de redes

Cuando se habla de un escaneo de red, nos estamos refiriendo a un conjunto de procedimientos que se utilizan para identificar el host, los puertos y los servicios en una red.

Así de esta forma podemos descubrir:

- Qué equipos se encuentran activos, direcciones IP de estos y puertos abiertos.
- El sistema operativo del host, los servicios que ofrece y su arquitectura.
- Vulnerabilidades presentes en los equipos activos.

1.1 Visión general del escaneo de redes

Se habla de escaneo de puertos, cuando nuestro objetivo es el de descubrir puertos abiertos. Además, se busca verificar los servicios presentes dentro de un objetivo, esto se logra enviando una serie de mensajes para conectar y analizar los puertos TCP y UDP.

En el escaneo de una red se busca enumerar las direcciones IP. Además de servir para identificar un host activo dentro de una red, con el fin de atacarlos o simplemente para poder evaluar la seguridad de la red.

Se habla de escaneo de vulnerabilidades cuando se realizan un conjunto de pruebas sobre una red o sistema para encontrar debilidades y/o fallos de seguridad de estos.

A continuación, revisaremos los protocolos de red.

1.2 TCP/IP comunicaciones

Los protocolos, son un conjunto de reglas que rigen el significado y formato de los mensajes enviados.

Gráfico de protocolo: TCP/IP

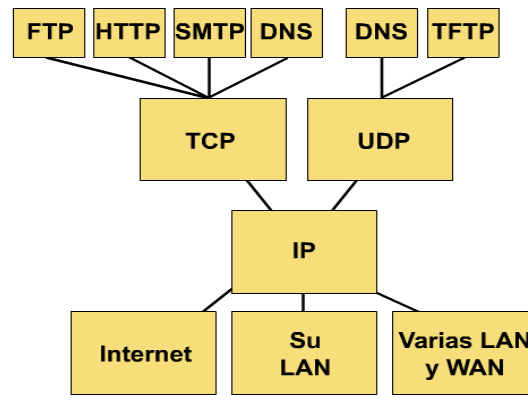


Figura 1. Gráfico de protocolo TCP/ IP

Fuente: Sites.google.com (s.f)

La arquitectura de los modelos de referencia (OSI y TCP) está construida en una jerarquía de capas. Es una forma de resolver un problema complejo: divide y vencerás. La comunicación entre dispositivos es, de hecho, un problema complejo de resolver. Es por ello por lo que organismos internacionales decidieron que la mejor forma de modelar (y dar una solución al problema) era creando una arquitectura de capas, en donde cada capa solicita servicios de la capa inferior y brinda servicios a la capa superior mediante interfaces. Las interfaces definen cómo las capas vecinas pueden brindar o solicitar esos servicios. De esta forma, cada capa es responsable de un conjunto de operaciones y solo ese conjunto de operaciones. Además, si una de las capas sufre un cambio, esto no debería provocar modificaciones en las capas adyacentes. El protocolo TCP/IP consta de cuatro capas que son:

- Capa física.

- Capa de red.
- Capa de transporte.
- Capa de aplicación.

1.2.1 Capa de aplicación

La capa aplicación se encarga de la interacción con el usuario (interfaz de usuario). En caso de que sea necesario, esta capa podría también asegurar la correcta presentación de la información (comprimir y descomprimir datos, cambiar idioma, sintaxis, etc.) y mantener un registro de las diferentes sesiones que están comunicándose dentro de la aplicación.

El modelo TCP no incluye explícitamente las capas de presentación y sesión, ya que en la práctica son de poco uso para la mayoría de las aplicaciones. Algunos protocolos que podemos encontrar en esta capa son HTTP/HTTPS (el que utilizamos para con el navegador web), SMTP/POP (envío y recepción de e-mails), SFTP (transferencia segura de archivos), entre otros.

1.2.2 Capa de transporte

Al igual que en el modelo OSI, la capa de transporte permite la comunicación simultánea de diferentes aplicaciones en un mismo dispositivo de origen hacia un mismo dispositivo de destino mediante la división de los datos en segmentos cuando sea necesario.

Existen dos protocolos que se pueden utilizar en la capa transporte:

TCP

El protocolo de control de transmisión o transfer control protocol es un protocolo confiable (asegura que no haya errores de transferencia), orientado a la conexión (antes de que el dispositivo emisor envíe datos, establece una conexión con el dispositivo receptor). También controla el flujo de forma tal que un emisor rápido no sature a un receptor lento. Debido a la gran cantidad de controles, requiere más procesamiento y tiempo para enviar los segmentos a la capa de internet.

UDP

Protocolo de datagrama de usuario o user datagram protocol. A diferencia de TCP, no es confiable ni orientado a la conexión. No es confiable porque no garantiza que los segmentos lleguen a destino y no orientado a la conexión significa que no establece una conexión con el receptor antes de enviar los segmentos, simplemente los envía a medida que son recibidos desde la capa aplicación. El principal beneficio es que es más veloz que TCP, lo cual lo hace ideal para aplicaciones sensible al retardo, como las llamadas de voz y video.

1.2.3 Capa de internet

Muy similar a la capa de red del modelo OSI, la capa de internet se encarga de direccionar y enviar los paquetes de una red a otra, independientemente del tipo de red de origen y destino. En esta capa el protocolo IP (protocolo de internet o internet protocol) define el

formato del paquete junto con la dirección de origen y destino asociada a este, denominada dirección IP. Actualmente, se utilizan dos versiones: IP versión 4 (IPv4) e IP versión 6 (IPv6).

1.2.4 Capa de acceso a la red

Incluye los servicios de las capas físicas y enlace de datos del modelo OSI. Obtiene los paquetes provenientes de la capa de internet, los procesa en tramas para luego transmitirlos al medio físico como bits. Ethernet es un protocolo que define reglas para esta capa.

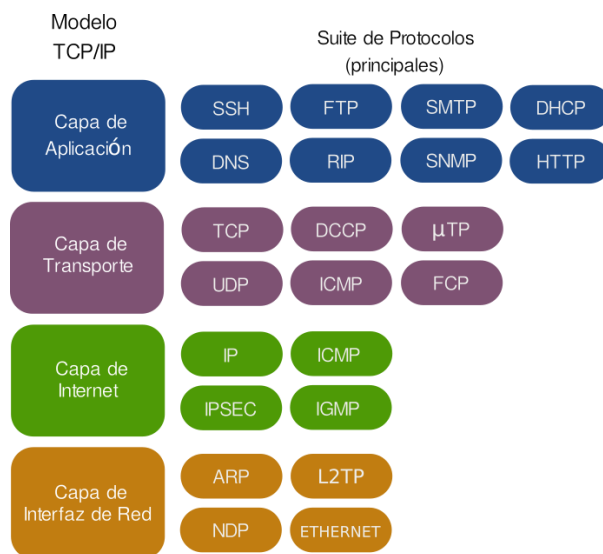


Figura 2. Capas de TCP/IP

Fuente: Wikipedia (s.f)

2. Herramientas de escaneo de redes

2.1 NMAP

Es una herramienta de seguridad gratuita y además de código abierto. Se diseñó para descubrir servicios y hosts de red informática, y así como lo menciona su nombre con esta información construye un "mapa" de la red. NMAP trabaja enviando paquetes especialmente diseñados al host de destino y luego analiza las respuestas.

Dentro de sus funciones podemos encontrar:

- Se utiliza para auditar la seguridad de un firewall o dispositivo supervisando las conexiones de red que se pueden realizar a través de él.
- Tiene la función detectar de puertos abiertos en un host para poder preparar la auditoría.
- Como lo mencionamos anteriormente "mapea" redes, dispositivos y realiza mantenimiento y gestión de activos.
- Mediante la identificación de nuevos servidores logra auditar la seguridad de una red.
- Analiza la respuesta y del tiempo de esta mediante la generación de tráfico a hosts en una red,
- Encuentra y explota vulnerabilidades en una red.

- Sirve para realizar consultas DNS y búsqueda de subdominios.

```
Nmap scan report for drag[REDACTED] (64.41.19.52)
Host is up (0.20s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      Hiawatha httpd 10.5
warning: OSScan results may be unreliable because we could not find
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (96%), Google Android
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe
Aggressive OS guesses: Linux 3.10 - 4.2 (96%), Linux 3.13 (96%), Li
ux 2.6.32 (92%), Linux 2.6.32 - 3.10 (92%), Linux 3.2 - 3.16 (91%),
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for 64.41.19.13
Host is up (0.20s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.12.0
warning: OSScan results may be unreliable because we could not find
Aggressive OS guesses: Linux 3.2 - 4.6 (96%), Linux 3.10 - 4.2 (94%
%), Linux 3.13 - 3.16 (91%), Linux 4.4 (91%), Android 5.0 - 5.1 (91
%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops

Nmap scan report for c[REDACTED].e.com (64.41.19.54)
Host is up (0.20s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.22 ((Debian))
```

Figura 3. Ejemplos de nmap en un escaneo de rango de direcciones IP.

Fuente: blog.carreralinux.com.ar (2017)

2.2 Hping 2/Hping3

Hping es una solución que funciona a través línea de comandos la cual permite crear, analizar paquetes, entre otros. Esta utilidad se orientó a TCP/IP, fue creada por el conocido programador Salvatore Sanfilippo (@antirez), es gratuita y de código abierto. Soporta los protocolos TCP, UDP, ICMP y RAW-IP.

Hping sirve para crear diseñar y ensamblar paquetes, detecta que hosts se encuentran activos dentro de una red, puede ejecutar escaneos de puertos, detecta qué tipo de sistema operativo podría tener un host activo a través de OS fingerprinting, hace pruebas en Firewalls, realiza

pruebas en sistemas de detección de intrusos – Intrusion Detection System (IDS por sus siglas en inglés), aplica traceroute avanzado para así lograr determinar la ruta que toma un paquete. Como beneficio adicional sirve como herramienta pedagógica para aprender sobre el protocolo TCP/IP.

2.3 Herramientas de escaneo para móviles

Existe en el mercado una amplia variedad de soluciones para realizar escaneo de terminales. Algunas de código abierto y gratuitas y otras que son de pago. A continuación, revisaremos 2 de las más populares.

2.3.1 Zabbix

Zabbix es una solución para la monitorización de redes y aplicaciones. Es de código abierto y ofrece una vigilancia en tiempo real de miles de métricas recogidas de servidores, equipos virtuales, dispositivos de red y aplicaciones web.

Con Zabbix podemos monitorear la disponibilidad y el nivel de respuesta de servicios como SMTP o HTTP sin tener que instalar ningún software sobre el host monitorizado.

Zabbix puede instalarse sobre máquinas Windows y Linux para monitorizar estadísticas como, utilización de red, carga de CPU, espacio en disco, etc.

Zabbix también tiene soporte para monitorizar vía protocolos SNMP, TCP y ICMP, como también sobre IPMI, JMX, SSH, telnet y se pueden ejecutar

comandos personalizados. Además cuenta con variados mecanismos de notificación en tiempo real, incluyendo XMPP.



Figura 4. Herramienta zabbix

Fuente: Zabbix.com (s.f)

2.3.2 Nagios

Según el sitio web de North Networks, creadores de la aplicación (www.north-networks.com):

“Nagios es un sistema de monitorización de redes ampliamente utilizado que nace en 1999, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas

hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas."

"Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Llamado originalmente Netsaint, nombre que se debió cambiar por coincidencia con otra marca comercial, fue creado y es actualmente mantenido por Ethan Galstad, junto con un grupo de desarrolladores de software que mantienen también varios complementos.

Nagios fue originalmente diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix."



Figura 5. Herramienta nagios

Fuente: north-networks.com (s.f)

3. Técnicas de escaneo de redes

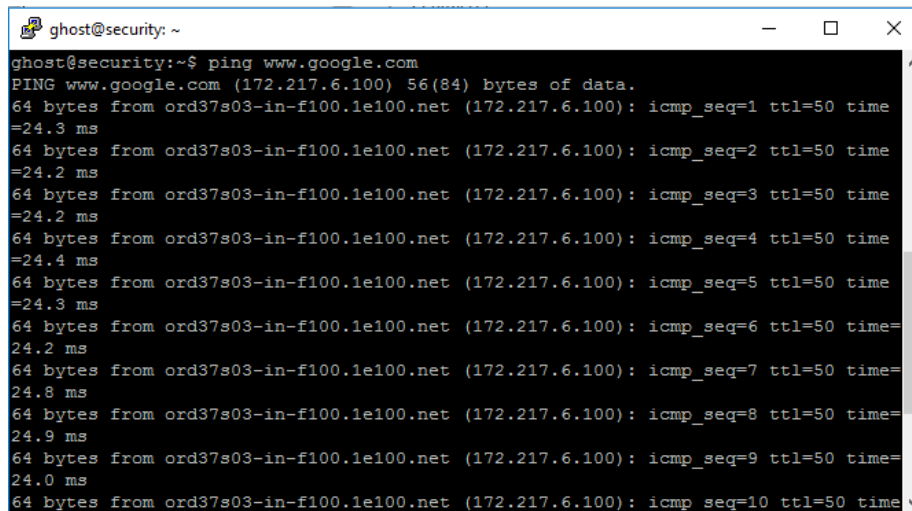
3.1 ICMP Scanning

El escaneo de puertos o ICMP Scanning es un proceso mediante el cual, a través de ciertas herramientas, se escanea y analiza los puertos de un sistema informático.

Al realizar este procedimiento se puede obtener información de los puertos que se encuentran abiertos, los que están cerrados o aquellos que están protegidos con Firewall.

Existen varias finalidades para realizar este procedimiento. Una de ellas es conocer que servicios está ofreciendo la máquina o también para analizar el estado de los puertos y detectar posibles vulnerabilidades.

Sin embargo, el escaneo de puertos también se puede usar con fines poco éticos. Así como los administradores de redes lo utilizan para detectar y corregir vulnerabilidades, los ciberdelincuentes lo pueden utilizar para explotar dichas brechas de seguridad.

A terminal window titled 'ghost@security: ~' showing the output of a 'ping' command. The command is 'ping www.google.com'. The output shows 10 successful ICMP echo requests from 'ord37s03-in-f100.1e100.net' to '172.217.6.100'. Each request is 64 bytes, has a TTL of 50, and shows a response time between 24.0 ms and 24.9 ms. The sequence numbers (icmp_seq) range from 1 to 10.

```
ghost@security: ~  
ghost@security:~$ ping www.google.com  
PING www.google.com (172.217.6.100) 56(84) bytes of data.  
64 bytes from ord37s03-in-f100.1e100.net (172.217.6.100): icmp_seq=1 ttl=50 time  
=24.3 ms  
64 bytes from ord37s03-in-f100.1e100.net (172.217.6.100): icmp_seq=2 ttl=50 time  
=24.2 ms  
64 bytes from ord37s03-in-f100.1e100.net (172.217.6.100): icmp_seq=3 ttl=50 time  
=24.2 ms  
64 bytes from ord37s03-in-f100.1e100.net (172.217.6.100): icmp_seq=4 ttl=50 time  
=24.4 ms  
64 bytes from ord37s03-in-f100.1e100.net (172.217.6.100): icmp_seq=5 ttl=50 time  
=24.3 ms  
64 bytes from ord37s03-in-f100.1e100.net (172.217.6.100): icmp_seq=6 ttl=50 time=  
24.2 ms  
64 bytes from ord37s03-in-f100.1e100.net (172.217.6.100): icmp_seq=7 ttl=50 time=  
24.8 ms  
64 bytes from ord37s03-in-f100.1e100.net (172.217.6.100): icmp_seq=8 ttl=50 time=  
24.9 ms  
64 bytes from ord37s03-in-f100.1e100.net (172.217.6.100): icmp_seq=9 ttl=50 time=  
24.0 ms  
64 bytes from ord37s03-in-f100.1e100.net (172.217.6.100): icmp_seq=10 ttl=50 time=
```

Figura 5. ICMP scanning

Fuente: Chebbi, C. (2018)

3.2 TCP SCANNING

3.2.1 Técnicas de escaneo de puertos

TCP connect() scanning

Es una de las técnicas más utilizadas para realizar escaneos TCP debido a su simpleza. Cuenta con las ventajas de que es un método que apenas requiere privilegios y es muy rápido. Este método consiste en usar la llamada a sistema connect(). Si se establece la conexión, entonces el puerto está abierto; si no se consigue conectar, quiere decir que el puerto está cerrado.

TCP SYN scanning

Este método es el método de Mitad abierta o “half-open”. Lo que hace no es crear una conexión TCP completa. En vez de ello, se envían

paquetes SYN como si se fuera a establecer una conexión. Si como respuesta recibimos un SYN-ACK quiere decir que el puerto está abierto, pero si se recibe un RST es porque el puerto está cerrado. La principal dificultad de este método es que se requieren privilegios de ROOT para poder llevarlo a cabo.

TCP FIN scanning

Esta técnica permite penetrar en sistemas en los que los firewalls o los filtros de paquetes podrían detectar el uso de SYN packets. Usando estos, puede pasar que recibamos como respuesta un RST si el puerto está cerrado, y que si está abierto el sistema no dé una respuesta. Esto no ocurre utilizando paquetes FIN.

Fragmentation scanning

En realidad, no es un método de escaneo de puertos propiamente tal, este se basa en una modificación de técnicas anteriores. Consiste en dividir o fragmentar los paquetes SYN o FIN que se envían, para que así no sean detectados por los firewalls o los filtradores de paquetes.

TCP reverse ident scanning

Gracias a este protocolo podemos conocer el nombre de usuario y quien es el dueño de los servicios que se están usando dentro de una conexión TCP. Para esto es necesario establecer la conexión TCP completa.

3.3 UDP Scanning

Es sabido que la gran mayoría de los servicios TCP son los más utilizados, los servicios UDP también se encuentran ampliamente en la red. DNS, SNMP, y DHCP son los tres más comunes.

Como el escaneo UDP es más lento y difícil que escaneo TCP, los auditores en seguridad por lo general los ignoran. Esto es un gran error, pues servicios UDP explotables son habituales y los atacantes no ignoran este protocolo. Afortunadamente Nmap puede ayudar a inventariar los puertos UDP.

El escaneo UDP se efectúa enviando paquetes UDP a cada puerto del objetivo. Para algunos puertos comunes, se envía una cantidad específica del protocolo, pero la mayoría de puertos el paquete enviado está vacío. Si un error "ICMP port unreachable" (tipo 3, cod 3) es devuelto, el puerto está cerrado. Otros errores "ICMP unreachable" (tipo 3, códigos 1, 2, 9, 10 y 13) significa que puerto está filtrado.

Existen ocasiones que el servicio responderá con un paquete UDP, indicando que está abierto. Si hay respuesta después de las retransmisiones, el puerto es clasificado como abierto | filtrado. Esto significa que el puerto posiblemente está abierto, o que los filtros de paquetes están deteniendo la comunicación. Un escaneo de detección de versión (-sV) se puede usar para diferenciar los puertos realmente abiertos de aquellos filtrados.

El gran problema para los escaneos UDP es que son lentos. Los puertos abiertos o filtrados escasamente envían una respuesta, dando a Nmap un tiempo de espera y luego realizar una retransmisión en caso de que la prueba o respuesta sea perdida. Los puertos cerrados son principalmente el gran problema. Estos no suelen enviar de regreso un error "ICMP port unreachable".

La solución Nmap detecta el límite de velocidad y así para evitar la sobrecarga de la red con paquetes inútiles que la máquina objetivo ignora. Desafortunadamente, el límite al estilo linux de un paquete por segundo hace que un escaneo UDP a los 65,536 puertos conocidos pueda tomar más de 18 horas.

Cierre

Después de revisado el contenido de la semana, podemos extraer los siguientes factores claves:

Cuando se habla de un escaneo de red, nos estamos refiriendo a un conjunto de procedimientos que se utilizan para identificar el host, los puertos y los servicios en una red.

El escaneo de puertos o ICMP Scanning es un proceso mediante el cual, a través de ciertas herramientas, se escanea y analiza los puertos de un sistema informático.

El escaneo de puertos también se puede usar con fines poco éticos. Así como los administradores de redes lo utilizan para detectar y corregir vulnerabilidades, los ciberdelincuentes lo pueden utilizar para explotar dichas brechas de seguridad.

Figura 6. Ideas claves semana 3.

Fuente: Moran, E. (2020)

Referencias

Canepa, G. (s/f). *Ejemplos de nmap: escaneo de puertos y más*. Com.ar. [imagen] Recuperado el 5 de octubre de 2022, de <https://blog.carreralinux.com.ar/2017/08/ejemplos-de-nmap-escaneo-puertos/>

Chebby, C. (2018). *Advanced Infrastructure Penetration Testing: Defend your systems from methodized and proficient attackers* [imagen]. Packt Publishing.

Daza, S. (2021, mayo 26). Qué es hping3 y cómo escanear puertos - Behackerpro. *BeHackerPro - Profesionales en Ciberseguridad - El elemento que le suma a tu conocimiento. Aprende Ciberseguridad*. <https://behacker.pro/que-es-hping3-y-como-escanear-puertos/>

El protocolo de comunicación TCP/IP - desireyristinalES. (s/f). Google.com. [imagen] Recuperado el 5 de octubre de 2022, de <https://sites.google.com/site/desireyristinalaes/el-protocolo-de-comunicacion-tcp-ip>

Escaneo UDP con nmap. (s/f). Reydes.com. [imagen] Recuperado el 5 de octubre de 2022, de [https://www.reydes.com/d/?q=Escaneo UDP con Nmap](https://www.reydes.com/d/?q=Escaneo+UDP+con+Nmap)

Nagios - the industry standard in IT infrastructure monitoring. (s/f). Nagios. Recuperado el 5 de octubre de 2022, de <https://www.nagios.org>

¿Que es Nagios? (2021, agosto 6). North-networks.com; NORTH NETWORKS. [imagen] <https://www.north-networks.com/que-es-nagios/>

Tablado, F. (2021, julio 1). *Escaneo de puertos. ¿Para qué se hace?* Grupo Atico34; Ático34 Protección de datos para empresas y autónomos. <https://protecciondatos-lopd.com/empresas/escaneo-de-puertos/>

Wikipedia contributors. (s/f). *Familia de protocolos de internet*. Wikipedia, The Free Encyclopedia. [https://es.wikipedia.org/w/index.php?title=Familia de protocolos de internet&oldid=145297431](https://es.wikipedia.org/w/index.php?title=Familia_de_protocolos_de_internet&oldid=145297431)

Zabbix :: *The enterprise-class open source network monitoring solution*. (s/f). [imagen] Zabbix.com. Recuperado el 5 de octubre de 2022, de <https://www.zabbix.com>

(S/f). Platzi.com. [imagen] Recuperado el 5 de octubre de 2022, de <https://platzi.com/clases/1583-ethical-hacking/19777-introduccion-al-escaneo-de-redes/>