Webinar Gratuito

Técnicas para Escaneo de Puertos con Nmap

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Jueves 1 de Junio 2023

Alonso Eduardo Caballero Quezada

EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE)

Más de 19 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

Redes Sociales

https://www.linkedin.com/in/alonsocaballeroquezada/

https://twitter.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.instagram.com/alonso_reydes/

reydes@gmail.com

https://www.reydes.com

+51 949 304 030

@ReYDeS

Nmap

Es una utilidad gratuita de fuente abierta para el descubrimiento de redes, auditoría en seguridad. Muchos administradores de sistemas y redes lo utilizan para tareas como; inventario de redes, gestión de programas para actualización de servicios, y supervisión del tiempo de actividad del host o servicio.

Nmap utiliza paquetes de IP en bruto para determinar cuales hosts están disponibles en la red, cuales servicios ofrecen estos hosts, cuales sistemas operativos están ejecutando, cual tipo de filtros para paquetes/cortafuegos utilizan, y docenas de otras características.

Diseñado para escanear rápidamente grandes redes, pero funciona bien contra hosts individuales.

* Nmap: https://nmap.org/

TCP SYN Scan (-sS)

Es la opción de escaneo predeterminada. Se puede escanear miles de puertos por segundo, la cual no está obstaculizada por firewalls. Es relativamente discreto y sigiloso pues nunca completa las conexiones TCP.

Funciona contra cualquier pila TCP compatible en lugar de depender de las idiosincrasias específicas de las plataformas. También permite una diferenciación clara y confiable entre los estados abierto, cerrado y filtrado.

Se conoce como escaneo semiabierto, pues no abre una conexión TCP completa. Envía un paquete SYN, como si se fuese abrir una conexión real. Un SYN/ACK indica el puerto está abierto, mientras un RST indica no lo está. Si no se recibe respuesta, el puerto está filtrado, también si se recibe un error ICMP inalcanzable. El puerto también se considera abierto si se recibe un paquete SYN (sin el indicador ACK).

TCP connect scan (-sT)

Es el tipo de escaneo TCP por defecto cuando el escaneo SYN no es una opción. Cuando un usuario no tiene privilegios. Nmap le pide al S.O. establezca una conexión con la máquina y el puerto destino. Esta es la misma llamada de alto nivel al sistema utilizado por los navegadores web, clientes P2P, y la mayoría de otras aplicaciones.

Nmap tiene menos control sobre la llamada “conexión” de alto nivel comparado con los paquetes en bruto, haciéndolo menos eficiente. La llamada al sistema completa conexiones para abrir los puertos de destino. Esto no solo lleva más tiempo y requiere más paquetes para obtener la misma información, sino es más probable las máquinas de destino registren la conexión. Un IDS decente detectará cualquiera de los dos. Un administrador verá una gran cantidad de intentos de conexión en sus registros desde un solo sistema.

UDP scans (-sU)

Debido al escaneo UDP es generalmente más lento y difícil, algunos auditores de seguridad lo ingnoran. Los servicios UDP explotables son bastante comunes y los atacantes ciertamente no ignoran todo el protocolo. Afortunadamente, Nmap puede ayudar a inventariar los puertos UDP.

Funciona enviando un paquete UDP hacia cada puerto. Para algunos puertos comunes, como el 53 y el 161, se envía una carga útil específica del protocolo para aumentar la tasa de respuesta, pero para la mayoría de los puertos el paquete está vacío. Si se devuelve un error de puerto ICMP inalcanzable el puerto está cerrado. Otros errores ICMP inalcanzables marcan el puerto como filtrado. Ocasionalmente, un servicio responderá con un paquete UDP, demostrando está abierto. Si no se recibe respuesta después de las retransmisiones, el puerto se clasifica como abierto|filtrado.

TCP NULL, FIN, Xmas scans (-sN; -sF; sX)

Estos tres tipos de escaneo aprovechan un “agujero” sutil en el RFC de TCP para diferenciar entre puertos abiertos y cerrados. La página 65 de RFC 793 expone; "si el estado del puerto [de destino] está CERRADO... un segmento entrante no conteniendo un RST genera se envíe un RST en respuesta". Luego, en la página siguiente, se analizan los paquetes enviados a puertos abiertos sin los bits SYN, RST o ACK establecidos, lo cual indica: "es poco probable llegue aquí, pero si lo hace, descarte el segmento y regrese".

Cuando se escanean sistemas cumpliendo con este RFC, cualquier paquete no conteniendo bits SYN, RST o ACK generará un RST devuelto si el puerto está cerrado, y ninguna respuesta si el puerto está abierto. Mientras no se incluya ninguno de estos tres bits, cualquier combinación de los otros tres (FIN, PSH y URG) está bien. Nmap explota esto con estos tres tipos de escaneo.

TCP ACK scan (-sA)

Este escaneo nunca determina puertos abiertos (o incluso abiertos | filtrados). Se utiliza para mapear conjuntos de reglas de firewall, determinando si son o no de estado, y cuales puertos son filtrados

El paquete de prueba para exploración ACK solo tiene establecido el indicador ACK. Al escanear sistemas sin filtrar, los puertos abiertos y cerrados devolverán un paquete RST. Luego Nmap los etiqueta como sin filtrar, lo cual significa el paquete ACK puede acceder a estos, pero no se determina si están abiertos o cerrados.

Los puertos que no responden o envían ciertos mensajes de error ICMP se etiquetan como filtrados.

Otros Tipos de Escaneos

- SCTP INIT scan (-sY)
- TCP Window scan (-sW)
- TCP Maimon scan (-sM)
- SCTP COOKIE ECHO scan (-sZ)
- Idle scan (-sI)
- IP protocol scan (-s0)

* Port Scanning Techniques:
https://nmap.org/book/man-port-scanning-techniques.html

Curso Virtual Fundamentos Hacking Ético

Sitio Web:

www.reydes.com

Correo:

reydes@gmail.com

Fundamentos de Hacking Ético

Domingos 4 y 11 de Junio del 2023. De 9:00 am a 12:00 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Presentación

Este curso está orientado a aquellas personas quienes son nuevos en el mundo del hacking ético y pruebas de penetración, para aquellos con poca o ninguna experiencia previa, para aquellos quienes se sienten abrumados sobre como encajan todas las fases y herramientas, para una persona quien desea rápidamente empezar a utilizar las herramientas y conocer los métodos para realizar pruebas de penetración, o para cualquiera quien desee expandir su conocimiento en seguridad ofensiva. Es decir para cualquier interesado en seguridad de computadoras, hacking, o pruebas de penetración, pero quien no tiene experiencia previa y no está seguro de donde empezar.

Objetivos

Este curso enseña a los participantes los fundamentos sobre los procesos y herramientas utilizadas por los profesionales en hacking ético y pruebas de penetración, para ganar acceso hacia redes y sistemas. Este es un buen punto de inicio para empezar a adquirir conocimientos sobre seguridad ofensiva. Así mismo se proporcionan conocimientos para realizar auditorias de seguridad en las organizaciones. Este curso proporciona lo fundamental y general para poder ir hacia otros temas, libros, o cursos más avanzados.

Más Información:

https://www.reydes.com/d/?q=Curso_Fundamentos_de_Hacking_Etico

Demostraciones

-

```
File  Actions  Edit  View  Help
49155/tcp open  unknown
49157/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown
MAC Address: 08:00:27:51:D4:9E (Oracle Virtu

Nmap done: 1 IP address (1 host up) scanned

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -Pn -p- 192.168.0.50
Starting Nmap 7.93 ( https://nmap.org ) at 2
Nmap scan report for 192.168.0.50
Host is up (0.0013s latency).
Not shown: 65524 filtered tcp ports (no-resp
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
3500/tcp open   rtmp-port
6697/tcp open   ircs-u
8080/tcp open   http-proxy
8181/tcp closed intermapper

Nmap done: 1 IP address (1 host up) scanned in 111.57 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -Pn -p- 192.168.0.70
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-29 17:10 EDT
```

```
*eth0
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
ip.addr==192.168.0.70

No.   Time            Source          Destination     Protocol  Length  Info
5127  4.922460371     192.168.0.70    224.0.0.22      IGMPv3    60      Membership Report / J
5475  5.422527566     192.168.0.70    224.0.0.22      IGMPv3    60      Membership Report / J
6046  5.923023975     192.168.0.70    224.0.0.22      IGMPv3    60      Membership Report / J
1074… 125.484170951   192.168.0.70    224.0.0.22      IGMPv3    60      Membership Report / J
1074… 125.983536819   192.168.0.70    224.0.0.22      IGMPv3    60      Membership Report / J
1074… 130.486564498   192.168.0.70    224.0.0.22      IGMPv3    60      Membership Report / J
1074… 132.486996436   192.168.0.70    224.0.0.22      IGMPv3    60      Membership Report / J
1075… 167.504107738   192.168.0.80    192.168.0.70    TCP       74      36166 → 25 [SYN] Seq=
1075… 167.504157533   192.168.0.80    192.168.0.70    TCP       74      55800 → 21 [SYN] Seq=
1075… 167.504215067   192.168.0.80    192.168.0.70    TCP       74      46550 → 80 [SYN] Seq=
1075… 167.504275091   192.168.0.80    192.168.0.70    TCP       74      55374 → 110 [SYN] Seq

▸ Frame 5127: 60 bytes on wire (480 bits), 60 bytes captured (
▸ Ethernet II, Src: PcsCompu_51:d4:9e (08:00:27:51:d4:9e), Dst
▸ Internet Protocol Version 4, Src: 192.168.0.70, Dst: 224.0.0
▸ Internet Group Management Protocol

0000  01 00 5e 00 00 16 08 00  27 51 d4 9e
0010  00 28 08 c5 00 00 01 02  7b 06 c0 a8
0020  00 16 94 04 00 00 22 00  fb 01 00 00
0030  00 00 e0 00 00 fc 00 00  00 00 00 00

wireshark_eth0V11051.pcapng   Packets: 129176 · Displayed: 21543 (16.7%)   Profile: Default
```

Cursos Virtuales Disponibles en Video

Curso Virtual de Hacking Ético
https://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web
https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

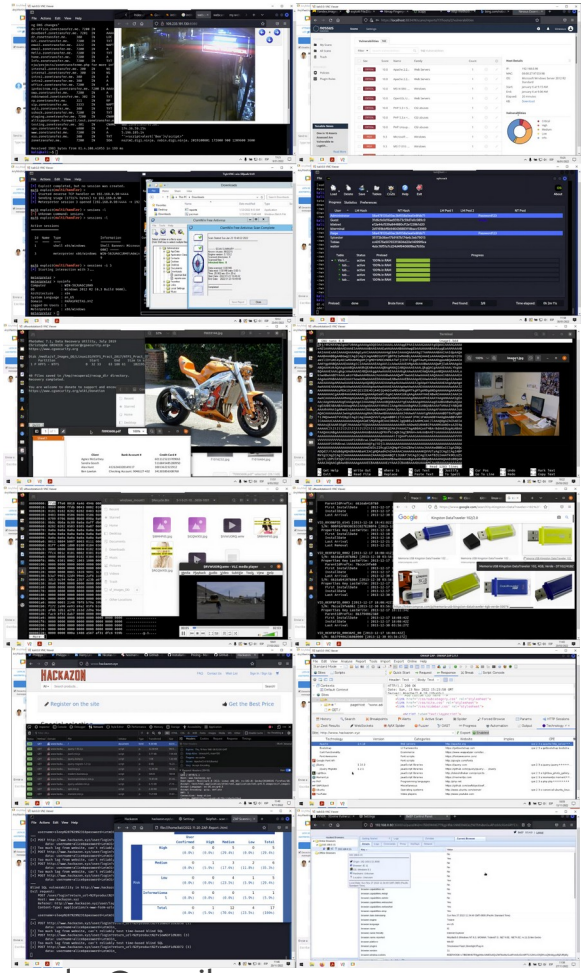
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso Virtual OSINT - Open Source Intelligence
https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes
https://www.reydes.com/d/?q=Curso_Forense_de_Redes

Y todos los cursos virtuales:

https://www.reydes.com/d/?q=cursos



Más Contenidos

Videos de 83 webinars gratuitos

https://www.reydes.com/d/?q=videos

Diapositivas de los webinars gratuitos

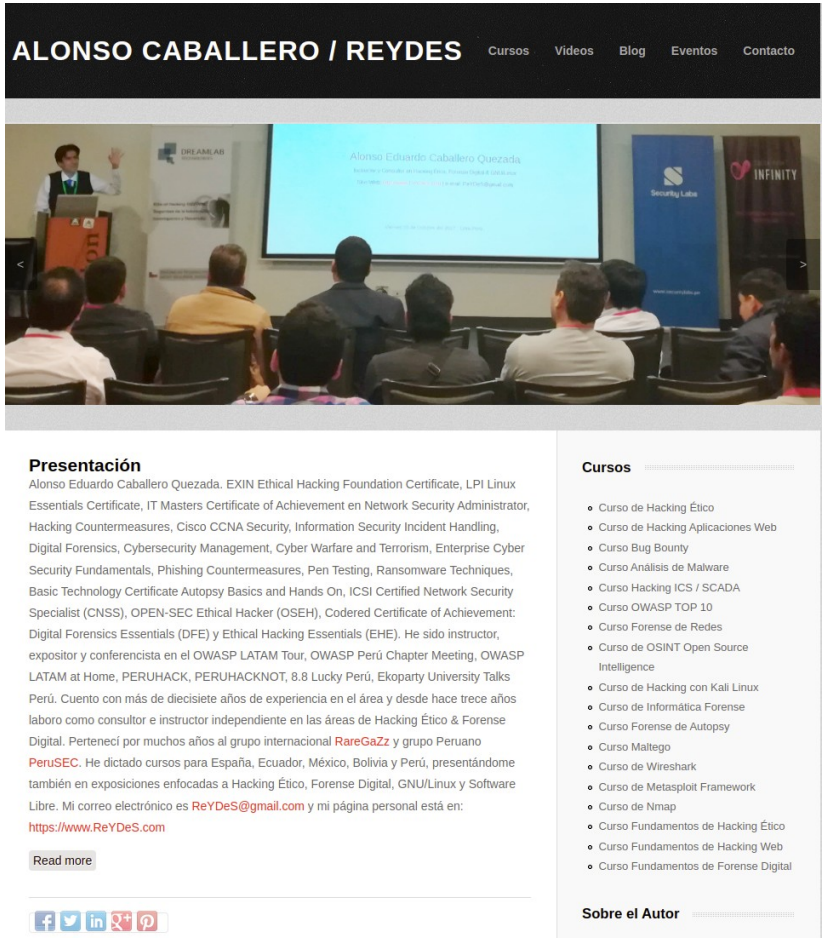
https://www.reydes.com/d/?q=eventos

Artículos y documentos publicados

https://www.reydes.com/d/?q=documentos

Blog sobre temas de mi interés

https://www.reydes.com/d/?q=blog/1



Webinar Gratuito

Técnicas para Escaneo de Puertos con Nmap

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Jueves 1 de Junio 2023