



ETHICAL HACKING PROFESSIONAL CERTIFICATION



CEHPC™ Versión 022024

CertiProf®

¿Quién es CertiProf®?

CertiProf® es una entidad certificadora fundada en los Estados Unidos en 2015, ubicada actualmente en Sunrise, Florida.

Nuestra filosofía se basa en la creación de conocimiento en comunidad y para ello su red colaborativa está conformada por:

- **Nuestros Lifelong Learners (LLL)** se identifican como Aprendices Continuos, lo que demuestra su compromiso inquebrantable con el aprendizaje permanente, que es de vital importancia en el mundo digital en constante cambio y expansión de hoy. Independientemente de si ganan o no el examen.
- Las universidades, centros de formación, y facilitadores en todo el mundo forman parte de nuestra red de aliados **ATPs (Authorized Training Partners.)**
- **Los autores (co-creadores)** son expertos de la industria o practicantes que, con su conocimiento, desarrollan contenidos para la creación de nuevas certificaciones que respondan a las necesidades de la industria.
- **Personal Interno:** Nuestro equipo distribuido con operaciones en India, Brasil, Colombia y Estados Unidos está a cargo de superar obstáculos, encontrar soluciones y entregar resultados excepcionales.

Nuestras Acreditaciones y Afiliaciones

Memberships



Digital badges issued by



Agile Alliance

CertiProf® es Miembro Corporativo del Agile Alliance.

Al unirnos al programa corporativo Agile Alliance, continuamos capacitando a las personas ayudándolas a alcanzar su potencial a través de la educación. Cada día, brindamos más herramientas y recursos que permiten a nuestros socios capacitar a profesionales que buscan mejorar su desarrollo y habilidades profesionales.

<https://www.agilealliance.org/organizations/certiprof/>



IT Certification Council - ITCC

CertiProf® es Miembro activo de ITCC.

El propósito fundamental del ITCC (IT Certification Council) es apoyar a la industria y sus empresas miembros comercializando el valor de la certificación, promoviendo la seguridad de los exámenes, fomentando la innovación, estableciendo y compartiendo las mejores prácticas de la industria.

Credly

CertiProf® es partner de Credly.

Esta alianza permite a las personas y compañías certificadas o acreditadas con CertiProf® tener una distinción mundial a través de una insignia digital.

Credly es el contenedor de insignias más importante en el mundo y empresas líderes en tecnología como IBM, Microsoft, PMI, Scrum.org, Nokia, Stanford University, entre otras emiten sus insignias con Credly.



Lifelong Learning

Los portadores de esta insignia en particular han demostrado su compromiso inquebrantable con el aprendizaje permanente, que es de vital importancia en el mundo digital actual, en constante cambio y expansión. También identifica las cualidades de una mente abierta, disciplinada y en constante evolución, capaz de utilizar y contribuir con sus conocimientos al desarrollo de un mundo más igualitario y mejor.

Criterios de Adquisición:

- Ser candidato a la certificación CertiProf
- Ser un aprendiz continuo y enfocado
- Identificarse con el concepto de aprendizaje permanente
- Creer e identificarse realmente con el concepto de que el conocimiento y la educación pueden y deben cambiar el mundo
- Quiere impulsar su crecimiento profesional



SCAN ME

Insignia

COMPARTE Y VERIFICA TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#CEHPC #CertiProf



Objetivos

El presente curso tiene como objetivo desarrollar las siguientes competencias específicas y especializadas:

- Comprender las tendencias de seguridad actuales.
- Conocer los elementos de seguridad de la información.
- Comprender los conceptos, tipos y fases de ethical hacking.
- Gestionar las amenazas a la seguridad de la información.
- Desarrollar estrategias para la comprensión, gestión y protocolos de los vectores de ataque.
- Dominar los conceptos, tipos y fases de pentesting.
- Comprender el proceso de pentesting.
- Dominar los controles de seguridad de la información.

¿Quién debe atender esta certificación?

Estudiantes, auditores, analistas de seguridad, consultores o asesores en temas de auditoría y de control interno y gestión de riesgos y profesionales vinculados al mundo de la ciberseguridad.

Agenda

1. Fundamentos de Pentesting y Hacking Ético	11
1.1 Introducción al Hacking Ético	12
Qué es un Hacker	13
Tipos de Hackers	13
Clasificación de Hackers	13
Hacking vs Hacking Ético	14
El Proceder de un Hacker	15
1.2 Penetration Testing	17
Importancia del Pentesting	19
Conocimiento del Pentester	19
Tipos de Prueba de Pentesting	20
Categorización de un Pentesting	20
Fases Pentesting	21
1.3 Metodologías y Buenas Prácticas	22
Metodologías de Pentesting	23
Metodología PTE's	23
Recolección de Información	24
Análisis de vulnerabilidades	24
Modelado de Amenazas	25
Explotación	25
Post - Explotación	26
Informe de Resultados	26
OWASP	26
OWASP TOP 10	27
Owasp Checklist	29
MITRE ATT&CK	30
1.4 Tecnologías y Herramientas para la Seguridad	32
Tecnologías para la Seguridad	33
Sistemas IPS (intrusion prevention system)	33
Sistema de Detección de Intrusos (IDS)	33
Redes Privadas Virtuales (VPN)	34
Sistemas de filtrado de Contenido	34
Routers	35
Switches	35
Firewall	36
HoneyPot	36
Respuesta a incidentes de Seguridad de la Información	37
SIEM	37
Respaldo y Recuperación	38

2. Ingeniería Social	39
2.1 Historia de la Ingeniería social	40
¿Qué es la Ingeniería Social?	41
¿Cómo funciona la Ingeniería Social?	42
Canales que utilizan los atacantes	43
Métodos que utilizan los atacantes	43
Factores que hacen que las empresas sean vulnerables a los ataques	44
2.2 Tipos de ingeniería social	45
Phishing	46
Planificación de phishing	46
Spear Phishing	48
Vishing	48
Smishing	48
Whaling	49
Baiting	49
Scareware	50
Pretexting	50
2.3 Protección y Medidas de Control	51
Política de Uso Aceptable	52
Medidas de Revisión Preliminar	52
Concienciación y Formación	52
Campañas de phishing	53
3. Reconocimiento Pasivo e Activo	54
3.1 Reconocimiento Pasivo	55
¿Qué es OSINT?	56
Google Hacking	58
¿Qué son los registros DNS?	60
DNS Record	60
Whois	61
Shodan	62
3.2 Reconocimiento Activo	64
Escaneo y enumeración de red	65
Puertos y Servicios	65
Clasificación del tipo de respuesta al escanear puertos	65
4. Escaneo y Análisis de Red	66
4.1 Introducción al Análisis de Red	67
Ping	68
Traceroute	68
Barido de Ping	69
Tipo de Puertos	69

El Protocolo de control de mensajes de Internet (ICMP)	70
SYN /ACK	70
Indicadores de comunicación TCP	71
Banderas de Comunicación TCP	71
Método Three-wayhandshake	72
4.2 Instalación del Entorno	73
4.3 Introducción a NMAP	75
Qué es NMAP	76
Escaneo de Nmap Básico	76
Opciones de NMAP	77
Zenmap	77
4.4 Categorías a NMAP	78
Host Discovery- Descubrimiento de Host	80
Escaneo de ping ARP	80
Escaneo de ping ICMP ECHO	81
Escaneo de ping UDP	82
Scan Techniques- Tecnicas de Escaneo	83
Port Specification And Scan Order – Especificaciones de puertos y orden de escaneo	85
Escaneo de Nmap por puerto	86
Service/Version Detection - Detección de Servicios/Versiones	86
OS Detection – Detección de Sistema Operativo	88
Timing and Performance- Tiempo y Rendimiento	89
Escaneo de Rendimiento	89
Firewall/IDS Evasion And Spoofing	90
Escaneo de Evasión	90
Output	91
Guardar Escaneo	91
5. Análisis de Vulnerabilidades	93
5.1 Introducción a las Vulnerabilidades	94
Qué es Análisis de Vulnerabilidades	95
¿Qué son las vulnerabilidades?	95
¿Qué es CVSS?	96
El concepto de CVE	97
Ejemplo de Vulnerabilidad	97
Consultas de CVE	98
5.2 Escaneo de Vulnerabilidades Automatizado	99
Nessus	100
OWASP ZAP	102
Tipos detecciones	103
5.3 Escaneo de Vulnerabilidades Manual	104
Script vuln	105
Script Auth	105

Script Default	106
Script Safe	106
6. Explotación	107
6.1 Metasploit	108
METASPIOT	109
Comandos Básicos	110
Búsqueda de sploit	112
7. Técnicas de Ataque	113
7.1 Tipos de Ataque	114
Malware	115
Spoofing	115
Man-in-the-middle (MITM)	116
Denegación de servicio distribuido (Ddos)	117
PiggyBacking	117
Inyección de Código SQL	118
Phishing	118
8. Informe de Resultados	119
8.1 Tipos de Informes	120
8.2 Presentación de Resultados	122

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



1. Fundamentos de Pentesting y Hacking Ético



CEHPC™ Versión 022024

CertiProf®

ETHICAL HACKING PROFESSIONAL CERTIFICATION



1.1 Introducción al Hacking Ético



CEHPC™ Versión 022024

CertiProf®

Qué es un Hacker

- Un hacker es una persona experta en informática que tiene habilidades avanzadas en la manipulación y explotación de sistemas informáticos.
- Los hackers pueden utilizar sus habilidades para diversas finalidades, que van desde la seguridad informática y la protección de sistemas, hasta actividades ilegales como el robo de datos, el acceso no autorizado a sistemas, el vandalismo en línea o el espionaje cibernético.
- Es importante destacar que no todos los hackers tienen intenciones maliciosas.



Tipos de Hackers

- **Hackers éticos:** También conocidos como "sombreros blancos", son hackers que se dedican a probar la seguridad de los sistemas informáticos y redes de una empresa, con el objetivo de identificar vulnerabilidades y ayudar a mejorar la seguridad.
- **Hackers maliciosos:** También conocidos como "sombreros negros", son hackers que se dedican a violar la seguridad de los sistemas informáticos y redes con fines ilegales o maliciosos, como robo de información, fraude financiero, extorsión, entre otros.
- **Hacktivistas:** Son hackers que se dedican a infiltrarse en sistemas informáticos y redes con fines políticos o sociales, como protesta o para difundir un mensaje.
- **Script kiddies:** Son hackers sin experiencia que utilizan herramientas automatizadas para llevar a cabo ataques, sin tener un conocimiento profundo de cómo funcionan los sistemas informáticos y redes.

Clasificación de Hackers

Dentro de los hackers hay clasificaciones, éstas se manejan de acuerdo a los objetivos e intereses de cada uno. Puede haber intereses y beneficios propios, ayuda a la comunidad, investigación y mejora e incluso una mezcla de todas las anteriores.



Hacking vs Hacking Ético

- Detectar las fallas en un sistema se realiza de la misma manera en la que un hacker o un hacker Ético lo llevarían a cabo.
- La diferencia está en el uso que le den a la información obtenida en esos fallos. Principalmente, un hacker explotará esas vulnerabilidades y las utilizará para obtener un beneficio propio.
- Un hacker Ético reportará y aportará conocimiento para la mitigación de las vulnerabilidades, sin realizar afectaciones a los sistemas o su información.



El Proceder de un Hacker

¿Qué motiva a un hacker a atacar en una persona o empresa?

Existen distintos factores que motivan a un atacante a dañar los activos de la empresa. En muchas ocasiones el motivo dependerá de los beneficios que obtenga al proporcionar el daño. Dentro de los principales motivos, tenemos:

- Ego (Reconocimiento)
- Hacktivismo
- Ganancias económicas
- Venganza
- Delincuencia organizada
- Competencia comercial



Ganancias económicas: Existen organizaciones que se dedican a utilizar el hacking con fines de lucro y generan ganancias más altas que el mismo PIB de países de bajo y mediano desarrollo. Existen diversas maneras de proceder, tal es el caso de:

- Carding
- Venta de información de tarjetas
- Clonado de tarjetas
- Venta de Información
- Bases de datos
- Contraseñas
- Información empresarial
- Robo de identidad
- Falsificación de documentos
- Espionaje y hackeo

Venganza: Existen empleados o conocidos cercanos que están descontentos con una persona u organización, tal es el caso de empleados o ex empleados, proveedores de servicios, etc.

Estas personas en ocasiones cuentan con credenciales de acceso con altos privilegios, lo cual les permitirá realizar la edición o borrado de la información.

Acceso a paneles de administración, consolas de acceso a sistemas operativos y sitios web.



¿Cómo lo hacen?



Existen demasiados métodos para poder “hackear” un objetivo (empresa, sitio web, persona). De acuerdo al tipo de alcance que se tenga, será la técnica usada.

- Ingeniería social
- Phishing
- Ataques dirigidos
- Spear phishing
- Mala configuración en servicios / Programas apócrifos
- Ataques a sistemas operativos (Windows / MAC / Linux / Android / iPhone / Windows Phone), etcétera

Participación

- ¿Alguien ha visto alguna noticia de los ataques de hacker?
- ¿Han tenido alguna experiencia mala por algún ataque de hacker?
- ¿Dudas y preguntas en general?



ETHICAL HACKING PROFESSIONAL CERTIFICATION



1.2 Penetration Testing



CEHPC™ Versión 022024

CertiProf®

Penetration Testing

- Técnica de seguridad informática que simula un ataque a un sistema o red informática para evaluar su seguridad y descubrir vulnerabilidades.
- El objetivo es identificar debilidad en el sistema antes de que sean explotadas por atacantes reales y permitir que se tomen medidas preventivas para fortalecer la seguridad del sistema.
- “Una prueba de seguridad con un objetivo específico que termina cuando dicho objetivo se obtiene o se acaba el tiempo disponible” (OSSTMM – Open Source Security Testing Methodology Manual).
- Es la evaluación de la seguridad de un sistema frente a diferentes tipos de ataques realizados por un experto en seguridad autorizado. El experto intentará identificar y explotar las vulnerabilidades del sistema.” (ENISA – The European Union Agency for Cybersecurity).



Participación

En la actualidad, la seguridad de la información es una preocupación creciente para muchas organizaciones y empresas en todo el mundo. Por esta razón el Pentesting se considera un recurso valioso integrado en las misiones de seguridad de las empresas (algunas incluso tienen espacios específicos completos dedicados por completo a esta actividad).

- ¿Creen que solo hasta que pasa un ataque las empresas se preocupan por realizar un Pentesting?
- ¿Por qué creen que es importante realizar un Pentesting?
- ¿Qué tan segura está la información de su empresa?
- ¿Cuántos servicios están expuestos en internet?

Importancia del Pentesting

- Identificar y solucionar las vulnerabilidades en su infraestructura informática antes de que sean explotadas por atacantes reales.
- Los expertos en seguridad informática simulan un ataque real al sistema y prueban las medidas de seguridad existentes para evaluar su efectividad
- Las empresas pueden mejorar su seguridad informática y proteger sus datos sensibles , sistemas y activos digitales contra posibles ataques
- Esto no solo ayuda a prevenir posibles pérdidas financieras y reputacionales, sino que también ayuda a cumplir con los requisitos regulatorios y las normas de seguridad cibernética, lo que es especialmente importante para las empresas que manejan información confidencial de clientes o usuarios.



Pentesting

Conoce tus debilidades
para corregirlas

Conocimiento del Pentester



Tipos de Prueba de Pentesting

1. Test de caja negra (BlackBox). Las pruebas de caja negra implican la realización de una evaluación de la seguridad y pruebas sin conocimiento previo de la infraestructura o de la infraestructura de red a probar.

La prueba simula un ataque de un hacker malicioso fuera del perímetro de seguridad de la organización. El equipo de seguridad realiza la evaluación de la misma manera que un atacante externo, sin tener acceso a detalles de la arquitectura, el código fuente o la documentación.

2. Test de caja gris (Gray Box). Las pruebas de caja gris implican la evaluación de la seguridad y pruebas internas.

Las pruebas examinan el grado de acceso a información privilegiada dentro de la red. El propósito de esta prueba es para simular las formas más comunes de ataque, los que se inicien desde dentro de la red.

Es la simulación perfecta de un usuario final que intenta comprometer en el sistema sin tener un conocimiento completo del mismo.

3. Test de caja blanca (White Box). Las pruebas de caja blanca implican la evaluación de la seguridad y las pruebas son con conocimiento completo de la infraestructura de red, en este caso se conoce como auditorías internas.

El equipo tiene acceso a los detalles de la arquitectura, el código fuente, la documentación y otra información relevante del sistema o red que se está evaluando.

Categorización de un Pentesting

- Prueba de penetración de red: Se enfoca en evaluar la seguridad de la infraestructura de red, buscando posibles vulnerabilidades que podrían ser explotadas por atacantes.
- Prueba de penetración de aplicaciones web: Se enfoca en evaluar la seguridad de las aplicaciones web, buscando posibles vulnerabilidades en su código, como inyecciones de SQL, XSS, CSRF, entre otros.
- Prueba de penetración de aplicaciones móviles: Se enfoca en evaluar la seguridad de las aplicaciones móviles, buscando posibles vulnerabilidades que puedan ser explotadas por atacantes.
- Prueba de penetración de redes inalámbricas: Se enfoca en evaluar la seguridad de las redes inalámbricas, buscando posibles vulnerabilidades que puedan ser explotadas por atacantes.

- Prueba de penetración física: Se enfoca en evaluar la seguridad física de los sistemas, buscando posibles vulnerabilidades que puedan ser explotadas por atacantes que tengan acceso físico a los sistemas.

Fases Pentesting

Para realizar una evaluación de seguridad, es necesario seguir una metodología. Las metodologías se manejan para que todos realicemos ciertos procesos y lleguemos a un mismo resultado o similar.

Las pruebas de intrusión constan de 5 fases principales que permiten dar las pautas para que sea fluido, efectivo y permita obtener los mejores resultados.



ETHICAL HACKING

PROFESSIONAL CERTIFICATION



1.3 Metodologías y Buenas Prácticas



CEHPC™ Versión 022024

CertiProf®

Metodologías de Pentesting

Para realizar una evaluación de seguridad, es necesario seguir una metodología.

Las metodologías se manejan para que todos realicemos ciertos procesos y lleguemos a un mismo resultado o similar.



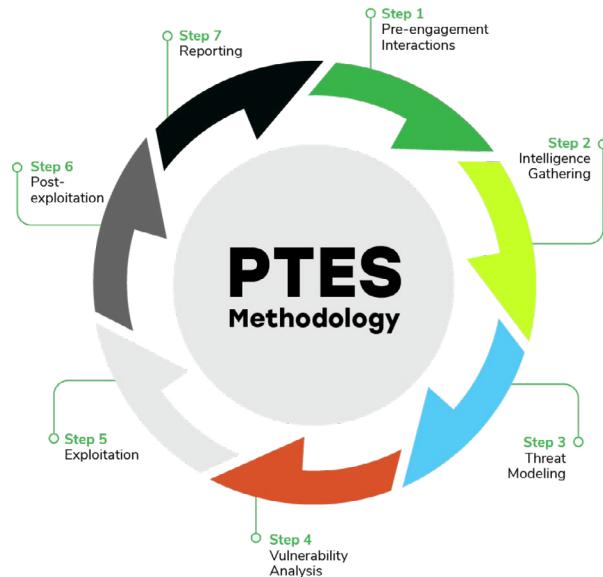
Metodología PTE's

El Estándar de Ejecución de Penetración (PTES, por sus siglas en inglés) consta de siete 7 secciones principales que cubren todo lo relacionado a una prueba de intrusión; desde la comunicación inicial y el razonamiento detrás de un Pentesting, seguido de la recopilación de inteligencia y las fases de modelado de amenazas donde los pentesters trabajan detrás de escena para obtener una mejor comprensión de la organización analizada a través de la investigación de vulnerabilidades, explotación y post explotación.



http://www.pentest-standard.org/index.php/Main_Page

1. Pre-acuerdo
2. Recolección de información
3. Análisis de Vulnerabilidades
4. Modelado de amenazas
5. Explotación
6. Post- Explotación
7. Reporte



Recolección de Información

Nos enfocaremos en identificar toda la información posible del objetivo. Esto nos servirá para realizar la planeación de una prueba de penetración y delimitar el alcance de la misma.

Los métodos más comunes son:

- Google hacking
- OSINT
- DOXING

Lo que se pretende es sacar la mayor cantidad de información para proceder a hacer un perfil.



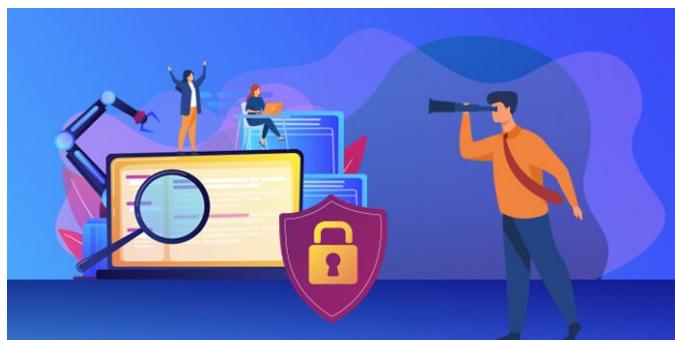
Análisis de Vulnerabilidades

En esta etapa analizaremos a detalle la información obtenida en la etapa anterior. Se analizará:

- Puertos abiertos
- Servicios detectados
- Versiones de sistema operativo y servicios
- Análisis de usuarios
- Generar diccionarios a la medida
- Detectar detalles de las soluciones tecnológicas implementadas
- Análisis de vulnerabilidades

Todo esto con la finalidad de conformar nuestro vector de ataque.

Se llega a un acuerdo con el cliente acotando la profundidad de las pruebas a realizar.



Modelado de Amenazas

En esta fase es muy importante ver que ya hemos extraído la información necesaria , porque con base a la información recaudada vamos a gestionar el perfil de ataque y veremos sobre la creación de nuestros vectores de ataque.

Un modelo de amenazas es en esencia una representación de toda la información que afecta a la seguridad de una aplicación

El modelado de amenazas es un proceso para capturar, organizar y analizar toda esta información.



Explotación

En esta fase realizaremos la explotación de los hallazgos obtenidos en la prueba anterior. Veremos las vulnerabilidades por sistema operativo, tipos de plataformas, servicios disponibles, etcétera.

Esta fase incluye las siguientes actividades:

- Selección de técnicas de explotación: se seleccionan las técnicas y herramientas que se van a utilizar para intentar explotar las vulnerabilidades identificadas.
- Ejecución de técnicas de explotación: se lleva a cabo la explotación de las vulnerabilidades mediante la ejecución de las técnicas seleccionadas.
- Obtención de acceso: si la explotación tiene éxito, se obtiene acceso no autorizado a los sistemas o aplicaciones.

Post – Explotación

En esta fase contamos con acceso al sistema, por lo que ejecutaremos las actividades que podrán permitirnos obtener el control del equipo de una manera total, generar usuarios, elevar privilegios, ingresar a la información, etcétera.



Informe de Resultados

Esta es la parte, aunque la más aburrida para nosotros, y claro por qué solo tenemos que escribir detalladamente todos los errores de seguridad que hemos encontrado, los procesos que realizamos.

Existen 2 tipos de reportes que debemos generar:

- Reporte Técnico (Para los administradores de sistemas)
- Reporte Ejecutivo (Para el comité directivo)



OWASP

OWASP (Open Web Application Security Project) es una comunidad internacional sin fines de lucro que se enfoca en mejorar la seguridad del software. Fundada en 2001, su objetivo principal es proporcionar recursos, herramientas, guías y conocimientos para ayudar a las organizaciones a desarrollar, adquirir y mantener aplicaciones web y software más seguros.



Las actividades de OWASP incluyen:

Documentación y Guías: OWASP proporciona documentos detallados, guías y mejores prácticas para el desarrollo seguro de aplicaciones web y software. Estas guías abarcan una amplia gama de temas, desde principios de seguridad hasta detalles técnicos sobre cómo proteger aplicaciones contra diferentes tipos de ataques.

Herramientas de Seguridad: La comunidad de OWASP desarrolla y mantiene una serie de herramientas de software de código abierto destinadas a ayudar a identificar y mitigar vulnerabilidades de seguridad en aplicaciones web y software.

Proyectos de Investigación: OWASP patrocina y apoya proyectos de investigación enfocados en la seguridad del software. Estos proyectos pueden abordar temas específicos de seguridad, como pruebas de penetración, análisis de código, protección de datos, entre otros.

Lista de las 10 Principales Vulnerabilidades: Uno de los proyectos más conocidos de OWASP es la publicación de la lista OWASP Top 10, que destaca las diez vulnerabilidades más críticas y comunes que afectan a las aplicaciones web en un período de tiempo determinado. Esta lista se actualiza periódicamente para reflejar las tendencias actuales en ciberseguridad.

OWASP TOP 10

OWASP es popular por publicar el TOP 10 Owasp Web cada cuatro años. Este es un documento que lista los diez riesgos más críticos en aplicaciones web, con el objetivo de ayudar a las organizaciones a identificar y mitigar las vulnerabilidades asociadas con estos riesgos.



<https://owasp.org/Top10/es/>

A01:2021 - Pérdida de Control de Acceso sube de la quinta posición a la categoría con el mayor riesgo en seguridad de aplicaciones web; los datos proporcionados indican que, en promedio, el 3,81% de las aplicaciones probadas tenían una o más Common Weakness Enumerations (CWEs) con más de 318.000 ocurrencias de CWEs en esta categoría de riesgo.

Las 34 CWEs relacionadas con la Pérdida de Control de Acceso tuvieron más apariciones en las aplicaciones que cualquier otra categoría.

A02:2021 - Fallas Criptográficas sube una posición ubicándose en la segunda, antes conocida como A3:2017-Exposición de Datos Sensibles, que era más una característica que una causa raíz. El nuevo nombre se centra en las fallas relacionadas con la criptografía, como se ha hecho implícitamente antes. Esta categoría frecuentemente conlleva a la exposición de datos confidenciales o al compromiso del sistema.

A03:2021 - Inyección desciende hasta la tercera posición. El 94% de las aplicaciones fueron probadas con algún tipo de inyección y estas mostraron una tasa de incidencia máxima del 19%, promedio de 3.37%, y las 33 CWEs relacionadas con esta categoría tienen la segunda mayor cantidad de ocurrencias en aplicaciones con 274.000 ocurrencias. El Cross-Site Scripting, en esta edición, forma parte de esta categoría de riesgo.

A04:2021 - Diseño Inseguro nueva categoría para la edición 2021, con un enfoque en los riesgos relacionados con fallas de diseño. Si realmente queremos madurar como industria, debemos "mover a la izquierda" del proceso de desarrollo las actividades de seguridad.

Necesitamos más modelos de amenazas, patrones y principios con diseños seguros y arquitecturas de referencia. Un diseño inseguro no puede ser corregida con una implementación perfecta debido a que, por definición, los controles de seguridad necesarios nunca se crearon para defenderse de ataques específicos.

A05:2021 - Configuración de Seguridad Incorrecta asciende desde la sexta posición en la edición anterior; el 90% de las aplicaciones se probaron para detectar algún tipo de configuración incorrecta, con una tasa de incidencia promedio del 4,5% y más de 208.000 casos de CWEs relacionadas con esta categoría de riesgo. Con mayor presencia de software altamente configurable, no es sorprendente ver qué esta categoría ascendiera. El A4:2017-Entidades Externas XML(XXE), ahora en esta edición, forma parte de esta categoría de riesgo.

A06:2021-Componentes Vulnerables y Desactualizados antes denominado como Uso de Componentes con Vulnerabilidades Conocidas, ocupa el segundo lugar en el Top 10 de la encuesta a la comunidad, pero también tuvo datos suficientes para estar en el Top 10 a través del análisis de datos. Esta categoría

asciende desde la novena posición en la edición 2017 y es un problema conocido que cuesta probar y evaluar el riesgo. Es la única categoría que no tiene ninguna CVE relacionada con las CWEs incluidas, por lo que una vulnerabilidad predeterminada y con ponderaciones de impacto de 5,0 son consideradas en sus puntajes.

A07:2021 - Fallas de Identificación y Autenticación previamente denominada como Pérdida de Autenticación, descendió desde la segunda posición, y ahora incluye CWEs que están más relacionadas con fallas de identificación. Esta categoría sigue siendo una parte integral del Top 10, pero el incremento en la disponibilidad de frameworks estandarizados parece estar ayudando.

A08:2021 - Fallas en el Software y en la Integridad de los Datos es una nueva categoría para la edición 2021, que se centra en hacer suposiciones relacionadas con actualizaciones de software, los datos críticos y los pipelines CI/CD sin verificación de integridad. Corresponde a uno de los mayores impactos según los sistemas de ponderación de vulnerabilidades (CVE/CVSS, siglas en inglés para Common Vulnerability and Exposures/Common Vulnerability Scoring System). La A8:2017-Deserialización Insegura en esta edición forma parte de esta extensa categoría de riesgo

A09:2021 - Fallas en el Registro y Monitoreo previamente denominada como A10:2017-Registro y Monitoreo Insuficientes, es adicionada desde el Top 10 de la encuesta a la comunidad (tercer lugar) y ascendiendo desde la décima posición de la edición anterior. Esta categoría se amplía para incluir más tipos de fallas, es difícil de probar y no está bien representada en los datos de CVE/CVSS. Sin embargo, las fallas en esta categoría pueden afectar directamente la visibilidad, las alertas de incidentes y los análisis forenses.

A10:2021 - Falsificación de Solicitudes del Lado del Servidor es adicionada desde el Top 10 de la encuesta a la comunidad (primer lugar). Los datos muestran una tasa de incidencia relativamente baja con una cobertura de pruebas por encima del promedio, junto con calificaciones por encima del promedio para la capacidad de explotación e impacto. Esta categoría representa el escenario en el que los miembros de la comunidad de seguridad nos dicen que esto es importante, aunque no está visualizado en los datos en este momento.

Owasp Checklist

La lista de verificación de pruebas de seguridad de aplicaciones web basada en OWASP ayuda a gestionar el estado de las pruebas e incluye un marco de "mejores prácticas" que los usuarios pueden implementar en sus propias organizaciones y una guía de pruebas de penetración de "bajo nivel" que describe técnicas para probar la asignación de problemas de seguridad de aplicaciones web más comunes. Además, contiene la calculadora de evaluación de riesgos de OWASP y la plantilla de resumen de resultados

1. Information Gathering

ID	WSTG-ID	Test Name	Objectives	Tools	OWASP Top	CWE	R
1.1	WSTG-INFO-01	Conduct Search Engine Discovery Reconnaissance for Information Leakage	- Identify what sensitive design and configuration information of the application, system, or organization is exposed directly (on the organization's website) or indirectly (via third-party services).	Google Hacking Shodan	NA	NA	
1.2	WSTG-INFO-02	Fingerprint Web Server	- Determine the version and type of a running web server to enable further discovery of any known vulnerabilities.	Wappalyzer A6 Nikto	A5 CWE-756 CWE-1352		
1.3	WSTG-INFO-03	Review Webserver Metatags for Information Leakage	- Identify hidden or obfuscated paths and functionality through the analysis of metadata files (robots.txt, <META> tag, sitemap.xml) - Extract and map other information that could lead to a better understanding of the systems at	Browser Curl Burpsuite/ZA	A1 CWE-200		
1.4	WSTG-INFO-04	Enumerate Applications on Webserver	- Enumerate the applications within the scope that exist on a web server. - Find applications hosted in the webserver (Virtual hosts/Subdomain), non-standard ports, DNS zone transfers	dnsrecon Nmap	NA	NA	
		Review Webpage Content for Information Leakage	- Review webpage comments, metadata, and redirect bodies to find any information leakage. - Gather JavaScript files and review the JS code to better understand the application and to find	Browser Curl		CWE-200	

<https://github.com/tanprathan/OWASP-Testing-Checklist>

MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es un marco de conocimiento que describe y organiza las tácticas, técnicas y procedimientos utilizados por los adversarios en ciberseguridad para llevar a cabo ataques a redes y sistemas. Fue desarrollado por MITRE Corporation, una organización sin fines de lucro que trabaja en investigación y desarrollo en áreas como la ciberseguridad, defensa, tecnologías avanzadas y más.

<https://attack.mitre.org/>



La matriz ATT&CK ayuda a las organizaciones de ciberseguridad a entender mejor cómo los adversarios llevan a cabo sus ataques, permitiendo:

1. Mejor comprensión de las amenazas: Proporciona una estructura para entender y catalogar las tácticas y técnicas utilizadas por los adversarios, lo que ayuda a las organizaciones a prepararse mejor para posibles ataques.
2. Planificación de la defensa: Facilita la identificación de brechas de seguridad y la planificación de estrategias de defensa más efectivas, permitiendo a las organizaciones adaptar sus medidas de seguridad según las tácticas y técnicas de ataque más relevantes.
3. Mejora de la detección y respuesta: Ayuda a mejorar la capacidad de detección temprana de ataques al identificar señales de actividades maliciosas y a desarrollar respuestas adecuadas para mitigar el impacto de los ataques.
4. Referencia común: Ofrece un lenguaje y una referencia común para profesionales de ciberseguridad, permitiéndoles comunicarse y colaborar de manera más efectiva al discutir amenazas y estrategias de defensa.

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



1.4 Tecnologías y Herramientas para la Seguridad



CEHPC™ Versión 022024

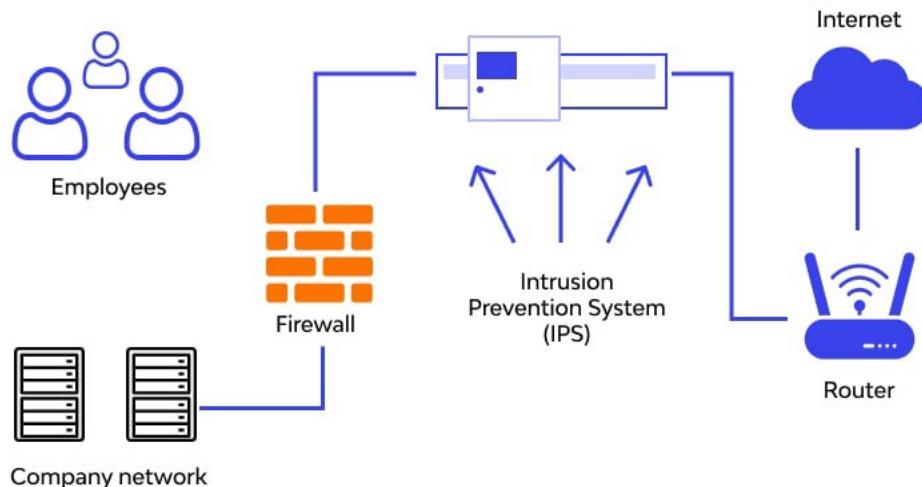
CertiProf®

Tecnologías para la Seguridad

La tecnología es una de las piedras angulares de una estrategia de seguridad efectiva , sin embargo, la tecnología no compensará por las deficiencias gerenciales, culturales u operativas.

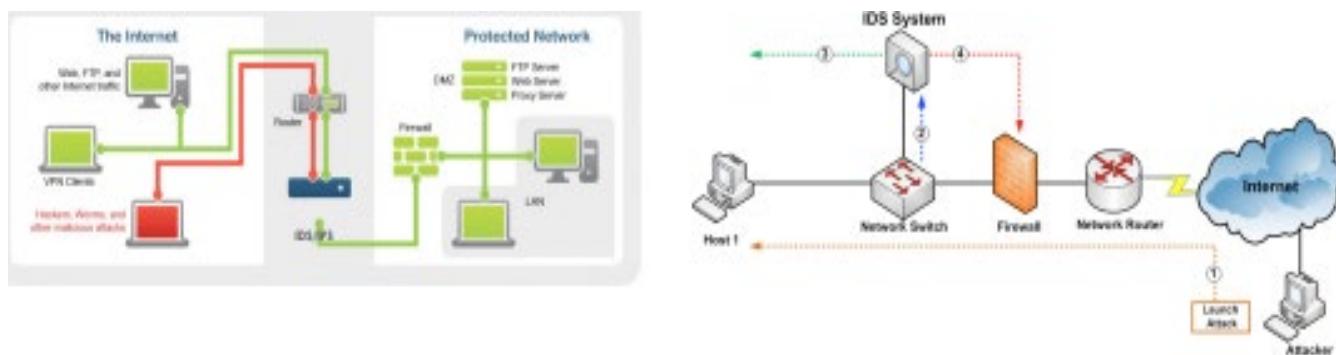
Sistemas IPS (intrusion prevention system)

Sistemas IPS (intrusion prevention system), es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos (toma acciones preventivas).



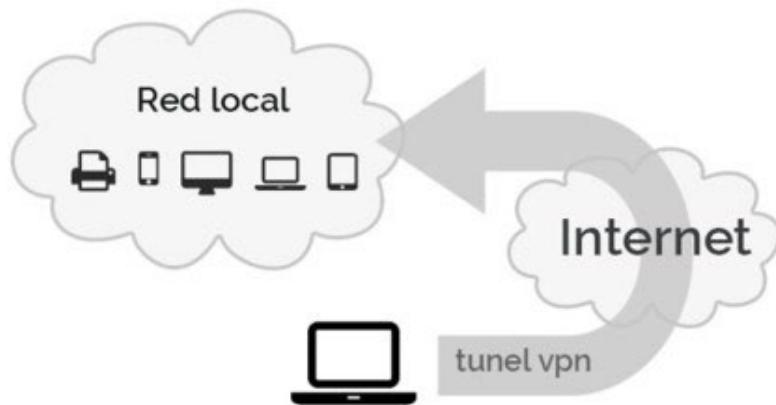
Sistema de Detección de Intrusos (IDS)

Dispositivo que sirve para “escuchar” todos los mensajes de entrada y salida, con el fin de deducir y advertir posibles ataques.



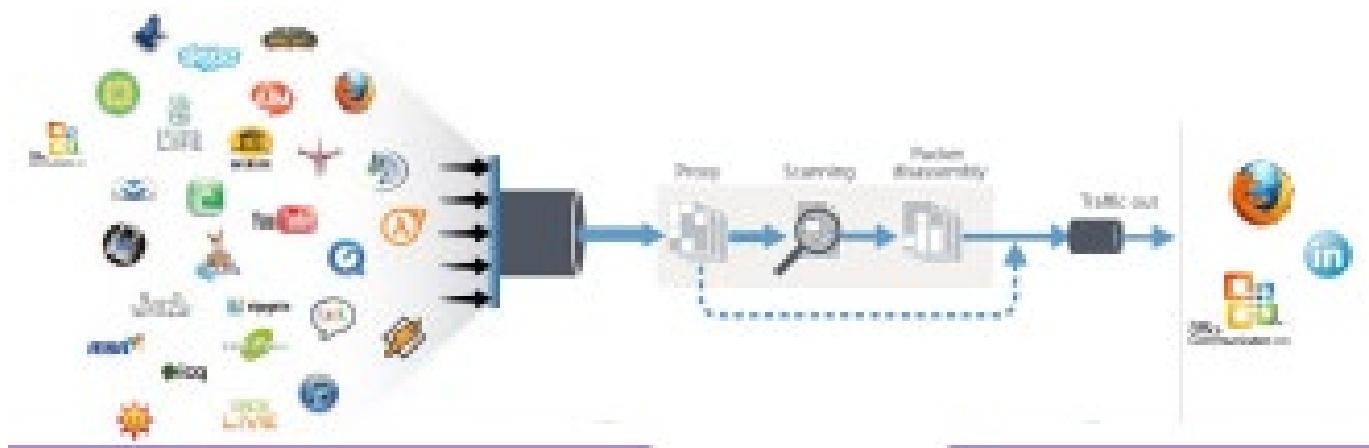
Redes Privadas Virtuales (VPN)

Tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada, como, por ejemplo: Internet: Sirve para proporcionar acceso remoto a recursos de red.



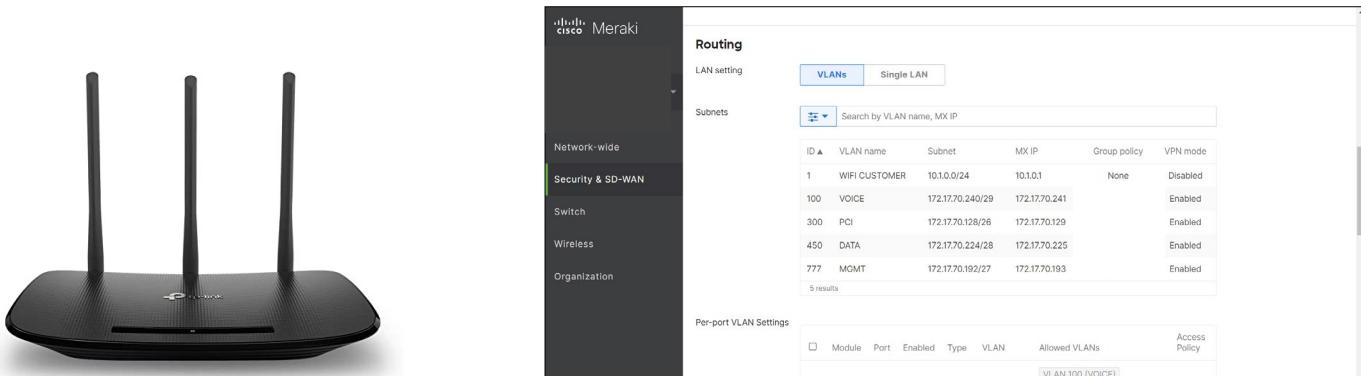
Sistemas de filtrado de Contenido

Con el propósito de prevenir amenazas (virus, SPAM, phishing, malware, spyware, etc.), utilizar mejor los recursos y controlar la productividad de los empleados de una organización, es posible implementar métodos de bloqueo de contenido no deseado de páginas Web.



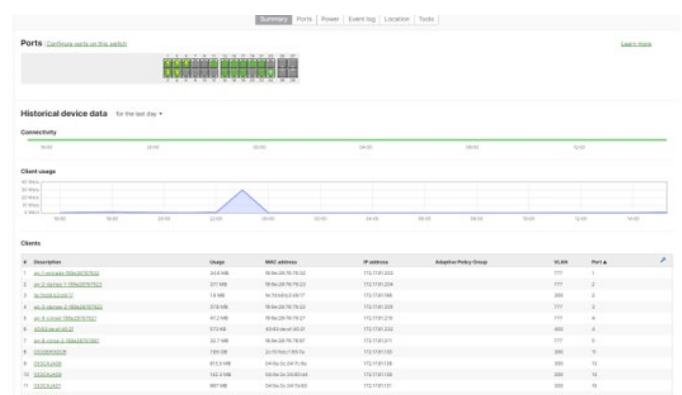
Routers

Este dispositivo interconecta segmentos de red o redes enteras que son independientes.



Switches

Es un dispositivo de interconexión de redes de computadoras, interconecta o divide dos o más segmentos de red y se usan cuando se desea conectar múltiples redes.



Firewall

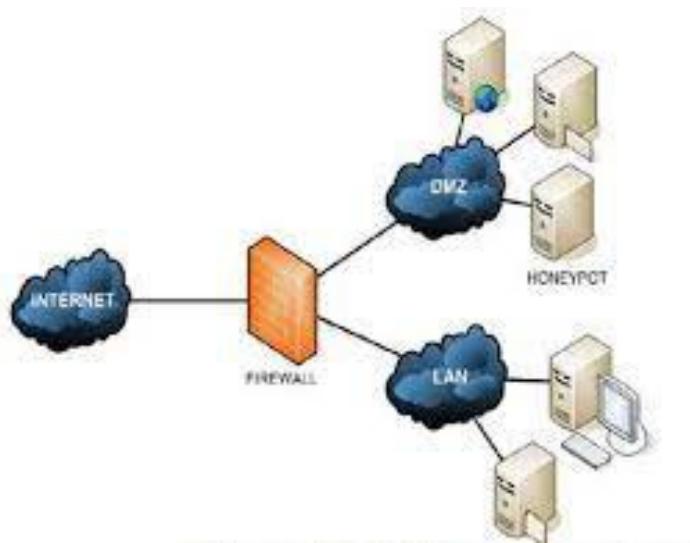
Son hardware, software o una combinación de ambos, separan redes y analizan el tráfico que pasa entre ellas, son el control más importante entre la red corporativa y el internet.

- Bloqueo a ciertos sitios
- Limitar el tráfico
- Monitorear las conexiones hacia internet
- Prevenir que ciertos usuarios entren a sitios

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Allow	TCP	10.0.0.14/32	50000-6	Server Berger	+ X
2	Allow	ICMP	10.0.0.14/32	Any	Ping Berger	+ X
3	Deny	Any	10.0.0.14/32	Any	Negociación Azure	+ X
4	Allow	Any	172.16.17.3/32	Any	DNS	+ X
5	Allow	TCP	172.16.17.30/32	449	Server MapperMap	+ X
6	Allow	TCP	172.16.17.30/32	8470	License Management	+ X
7	Allow	TCP	172.16.17.30/32	8471	Database Access	+ X
8	Allow	TCP	172.16.17.30/32	8472	Data Queues	+ X
9	Allow	TCP	172.16.17.30/32	8473	Access/Navigator	+ X
10	Allow	TCP	172.16.17.30/32	8474	Network Printers	+ X

HoneyPot

Es una herramienta de red para ser el objetivo de un posible ataque, con el objetivo de detectarlo el ataque antes de que afecte otros sistemas, esto es invisible para el atacante.



Respuesta a incidentes de Seguridad de la Información

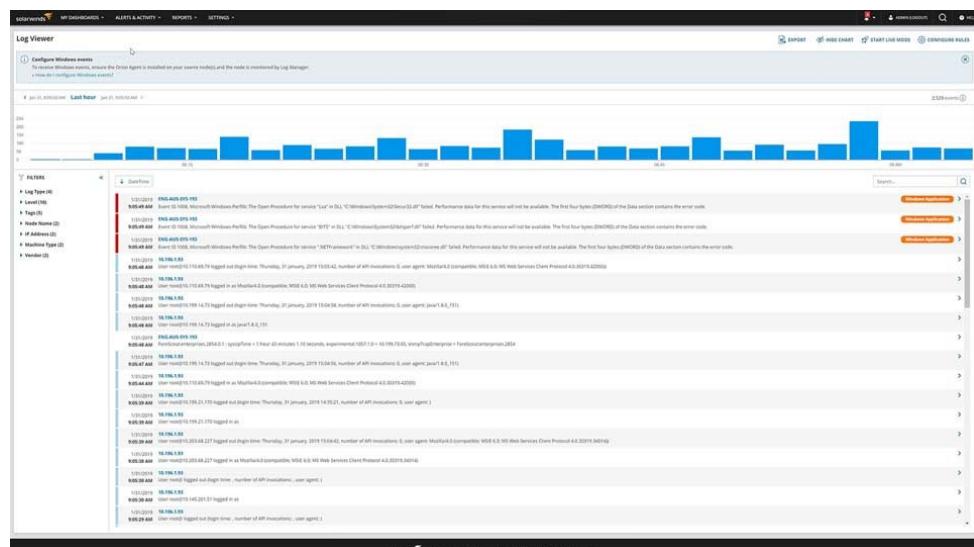
La respuesta ante incidentes es el proceso mediante el cual una organización reacciona ante amenazas de TI, como es el caso de los ciberataques, las vulneraciones de seguridad y el tiempo de inactividad de los servidores.



SIEM

Un SIEM tiene dos propósitos: (1) monitoreo en tiempo real, (2) correlación y procesamiento de eventos de seguridad. (Security Information and Event Management)

- Agregación / Colección de Datos (agentes)
- Normalización
- Correlación
- Analíticos
- Alertamiento



Respaldo y Recuperación

Para asegurar la disponibilidad e integridad de la información se utilizan medios de almacenamiento secundarios para guardar aplicaciones, software, datos, etc. Estos medios pueden ser CD, DVD, cintas, SAN-NAS, los cuales deberán ser grabados en una ubicación y ser almacenados en una o más ubicaciones (llamadas bibliotecas fuera de la sede, u offsite). Es responsabilidad del bibliotecario mandar un inventario continuo del contenido de las bibliotecas.

- Esquemas de respaldo
- Respaldo completo, Incremental, Diferencial



ETHICAL HACKING PROFESSIONAL CERTIFICATION



2. Ingeniería Social



CEHPC™ Versión 022024

CertiProf®

ETHICAL HACKING PROFESSIONAL CERTIFICATION



2.1 Historia de la Ingeniería social



CEHPC™ Versión 022024

CertiProf®

¿Qué es la Ingeniería Social?

La ingeniería social hace referencia a las diferentes técnicas de manipulación que utilizan los ciberdelincuentes para obtener información confidencial de los usuarios, por ejemplo, accesos y contraseñas.

Es el arte de convencer a las personas para que revelen información confidencial, los ingenieros sociales dependen del hecho de que las personas desconocen la información valiosa a la que tienen acceso y no se preocupen por protegerla.

Los hackers a menudo emplean técnicas de ingeniería social debido a que el factor de debilidad humana es mucho más fácil de penetrar que los puntos débiles de la red. Muchas veces los hackers "ganan" cuando se trata de la batalla porque no están limitados por el tiempo o la falta de motivación. Mientras que el director de TI se va a casa a las 5 o las 6 pm, el hacker funcionará las 24 horas del día para llevar a cabo su objetivo.

¿Qué es la Ingeniería Social?

- El comportamiento de la Ingeniería Social se basa en una premisa básica: las personas son más fáciles de manejar que las máquinas.
- Para llevar a cabo este tipo de ataques se utilizan técnicas de manipulación psicológica que permiten a los usuarios revelar información confidencial o realizar cualquier acción que pueda beneficiar a los ciberdelincuentes o a los atacantes.
- Debido al uso intensivo del correo electrónico por parte de empresas e individuos, los ataques de Ingeniería Social utilizan el correo electrónico como su principal canal de propagación.



¿Cómo funciona la Ingeniería Social?

Los atacantes de ingeniería social pretenden ser personas amables, confiables o autoritarias y engañan a las víctimas para que confíen en ellos. Una vez que la víctima confía en el atacante, puede ser manipulada para revelar información privada.

Los ciberdelincuentes engañan a sus víctimas haciéndose pasar por otra persona. Por ejemplo, se hacen pasar por miembros de la familia, personal de soporte técnico, compañeros de trabajo o alguien de confianza. La finalidad de este engaño es sustraer datos personales, contraseñas o suplantar la identidad de la persona engañada.



Canales que utilizan los atacantes

Teléfono
(Llamadas,
mensajes, etc.)

**Aplicación de
mensajería instantánea**
(WhatsApp / Telegram)

Email
(campañas, o mensajes
maliciosos, phishing)

Redes Sociales
(Facebook, LinkedIn,
Twitter, etc.)



Métodos que utilizan los atacantes



- Suplantar a miembros de la familia, amigos, conocidos o colegas.
- Ofrecer a las víctimas un premio o una promoción limitada por única vez a cambio de tu información.
 - Suplantar a un técnico de la empresa o líder del sistema.
- Invitación a llenar el formulario para ganar un premio o producto.
- Ofrecer actualizaciones del navegador o de la aplicación a través de páginas falsas.

Factores que hacen que las empresas sean vulnerables a los ataques



ETHICAL HACKING PROFESSIONAL CERTIFICATION



2.2 Tipos de ingeniería social



CEHPC™ Versión 022024

CertiProf®

Phishing

- El phishing es un ataque de ingeniería social en el que las comunicaciones se disfrazan como si proviniera de una fuente confiable.
- Estos mensajes (normalmente correos electrónicos) están diseñados para engañar a las víctimas para que proporcionen información personal o financiera.
- Después de todo, ¿por qué deberíamos dudar de la veracidad de la información de amigos, familiares o tiendas que frecuentamos? Las estafas de phishing se aprovechan de esta confianza.
- El phishing es un delito que engaña a las personas para que compartan información confidencial, como contraseñas y números de tarjetas de crédito. Las víctimas reciben correos electrónicos o mensajes de texto que se hacen pasar por una persona u organización de confianza.



Planificación de phishing

- Para la planificación de un phishing, los atacantes pueden tener en cuenta la entidad a la que desean falsificar, datos de sus víctimas como por ejemplo nombre, correo electrónico, teléfono, dirección, datos de estudio, datos del trabajo, entre muchos otros más.
- La planeación de este ataque puede llevar días o incluso meses si no conocen bien al objetivo al que quieren realizar el ataque, todo depende también del tipo de ataque phishing que quieran realizar (vishing, smishing, whaling, spear phishing, etc.)



¿Cómo se ve?



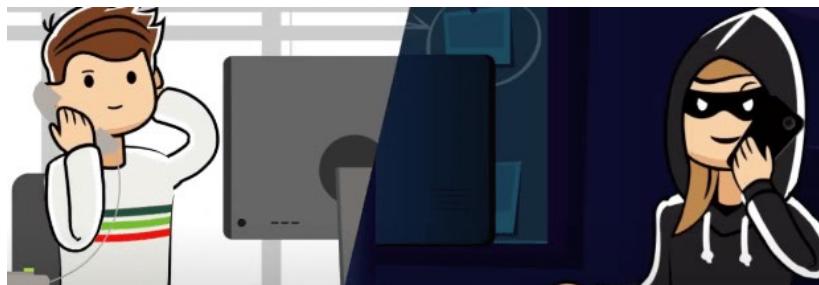
Spear Phishing

- Spear Phishing es un ataque de ingeniería social que se dirige a grandes empresas o individuos específicos.
- Los ataques de phishing se dirigen principalmente a grupos pequeños o personas poderosas, como ejecutivos, corporativos y celebridades. Los ataques de ingeniería social que utilizan este método suelen estar bien estudiados y disfrazados de forma encubierta, lo que dificulta su detección.



Vishing

Es un término que proviene de la combinación de las palabras "voice" (voz) y "phishing". Se refiere a una técnica de estafa en la que los delincuentes utilizan llamadas telefónicas para engañar a personas y obtener información confidencial o sensible, como contraseñas, números de tarjetas de crédito, números de seguro social u otra información personal.



Smishing

Es una forma de estafa o ataque cibernético que implica el uso de mensajes de texto SMS (Short Message Service) o mensajes de texto a través de aplicaciones de mensajería instantánea para engañar a las personas y obtener información confidencial o inducirlas a realizar acciones no deseadas.



Whaling

Es una forma específica de ciberataque de ingeniería social que se dirige a individuos de alto perfil en una organización, como ejecutivos de alto rango, directores, gerentes, y otras figuras importantes con acceso a información privilegiada y recursos críticos.

A diferencia del phishing convencional que apunta a un amplio grupo de personas, el whaling se enfoca en individuos específicos, denominados "ballenas" (de ahí el término "whaling" que significa "cacería de ballenas"), con el objetivo de obtener información confidencial, como credenciales de acceso, datos financieros, secretos comerciales o cualquier información sensible que pueda comprometer la seguridad de la organización.

Los ataques de whaling suelen ser más sofisticados y personalizados que los ataques de phishing comunes. Los cibercriminales invierten tiempo en investigar a su objetivo, recopilando información de fuentes públicas y redes sociales para crear mensajes altamente convincentes y personalizados, con el objetivo de engañar a la víctima.



Baiting

Es una táctica de ingeniería social utilizada en ciberataques que implica el uso de señuelos o incentivos para engañar a las personas y obtener acceso no autorizado a sistemas informáticos, información confidencial o datos personales.

El término "baiting" proviene de la palabra en inglés "bait", que significa "cebo" o "señuelo". Los ataques de baiting generalmente implican ofrecer algo atractivo o tentador, como un archivo descargable, un dispositivo USB aparentemente abandonado, un enlace a contenido interesante, un premio falso o cualquier cosa que pueda llamar la atención de la víctima.



Scareware

Es un tipo de software malicioso diseñado para asustar o intimidar a los usuarios, haciéndoles creer que sus dispositivos están infectados con virus, malware u otros problemas de seguridad, con el fin de incitarlos a tomar acciones que beneficien a los estafadores.

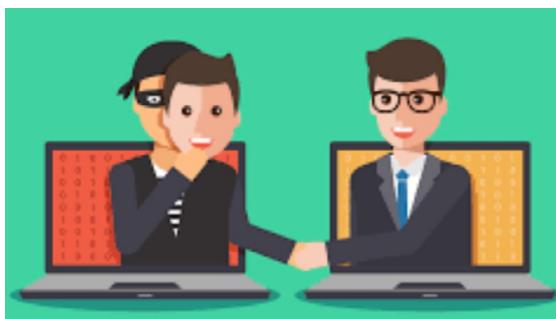
El scareware se presenta a menudo en forma de ventanas emergentes o anuncios falsos que aparecen en el navegador web, simulando alertas de seguridad legítimas. Estos mensajes pueden contener advertencias alarmantes, gráficos intimidantes o mensajes de texto convincentes que instan al usuario a tomar medidas inmediatas para resolver el supuesto problema de seguridad.



Pretexting

Es una técnica de ingeniería social en la que un estafador crea un escenario falso o una situación inventada para obtener información confidencial, datos personales o acceso a sistemas y cuentas de una persona u organización. Esta técnica involucra la creación de una historia o pretexto para ganar la confianza de la víctima y obtener la información deseada.

En esencia, el estafador se hace pasar por alguien que no es, utilizando un pretexto creíble para persuadir a la víctima de que revele información sensible o realice acciones que podrían comprometer su seguridad.



ETHICAL HACKING

PROFESSIONAL CERTIFICATION



2.3 Protección y Medidas de Control



CEHPC™ Versión 022024

CertiProf®

Política de Uso Aceptable

Una política de uso aceptable (AUP) es un tipo de política de seguridad dirigida a todos los empleados con acceso a uno o más activos de la organización.

Define qué comportamientos son aceptables y cuáles no lo son. Debe ser una condición para contratar y cada empleado debe firmar que la ha leído y entendido y que se atiene a sus condiciones.

Medidas de Revisión Preliminar

Valida la seguridad de los sitios que visitas, deben contar con “https” antes del sitio web, esto garantiza el cifrado de la información.



No ingreses a sitios que puedan comprometer la seguridad de la información como son: sitios de apuestas, contenido explícito, entretenimiento, etc.

No descargues archivos de páginas sospechosas.

No aceptes ventanas emergentes de publicidad, promociones o noticias, ya que podrías permitir el acceso no autorizado o infectar tu equipo.

Concienciación y Formación

- Un programa recurrente de sensibilización sobre la seguridad dirigido a los usuarios finales refuerza la importancia de la seguridad de la información
- Ampliar y profundizar las habilidades apropiadas del personal de seguridad mediante capacitación pueden mejorar en gran medida la eficiencia de la seguridad en una organización
- Puesto que las exposiciones al daño más costosas y perjudiciales son casi siempre el resultado de actividades iniciadas desde el interior, la primera línea de defensa es intentar garantizar la confianza y la integridad de personal tanto existente como de nuevo ingreso

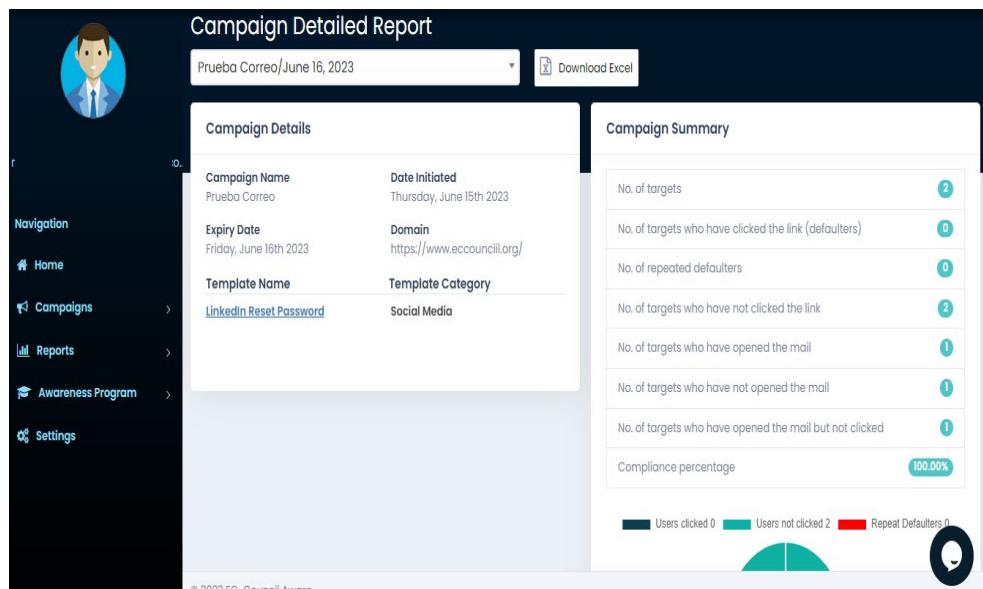


Campañas de phishing

Se realiza una simulación de ataque de ingeniería social a través de pruebas de phishing para medir la resiliencia de los colaboradores de la compañía ante este tipo de amenazas.

La realización de este análisis le ayudara para:

1. Identificar el grado de compromiso que puede ocurrir en la organización a través de un ataque vía correo electrónico.
2. Identificar el grado de cuidado de los usuarios para reportar este tipo de incidentes al área de seguridad/sistemas.
3. Comprobar la capacidad de los servicios involucrados para detectar con éxito y responder a los ataques más intencionados.



ETHICAL HACKING

PROFESSIONAL CERTIFICATION



3. Reconocimiento Pasivo e Activo



CEHPC™ Versión 022024

CertiProf®

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



3.1 Reconocimiento Pasivo



CEHPC™ Versión 022024

CertiProf®

3.1 Reconocimiento Pasivo

Recolección Pasiva

- Google Hacking
- Shodan
- Recolección de DNS
- Motores de búsqueda
- OSINT Imágenes, Email, Personas, Redes sociales, Wifi



Implica la recopilación de información sin interactuar directamente con los sistemas o aplicaciones. Esto puede incluir la búsqueda de información en registros públicos de dominios, perfiles de redes sociales, búsqueda de información en motores de búsqueda y la recopilación de información de fuentes abiertas.

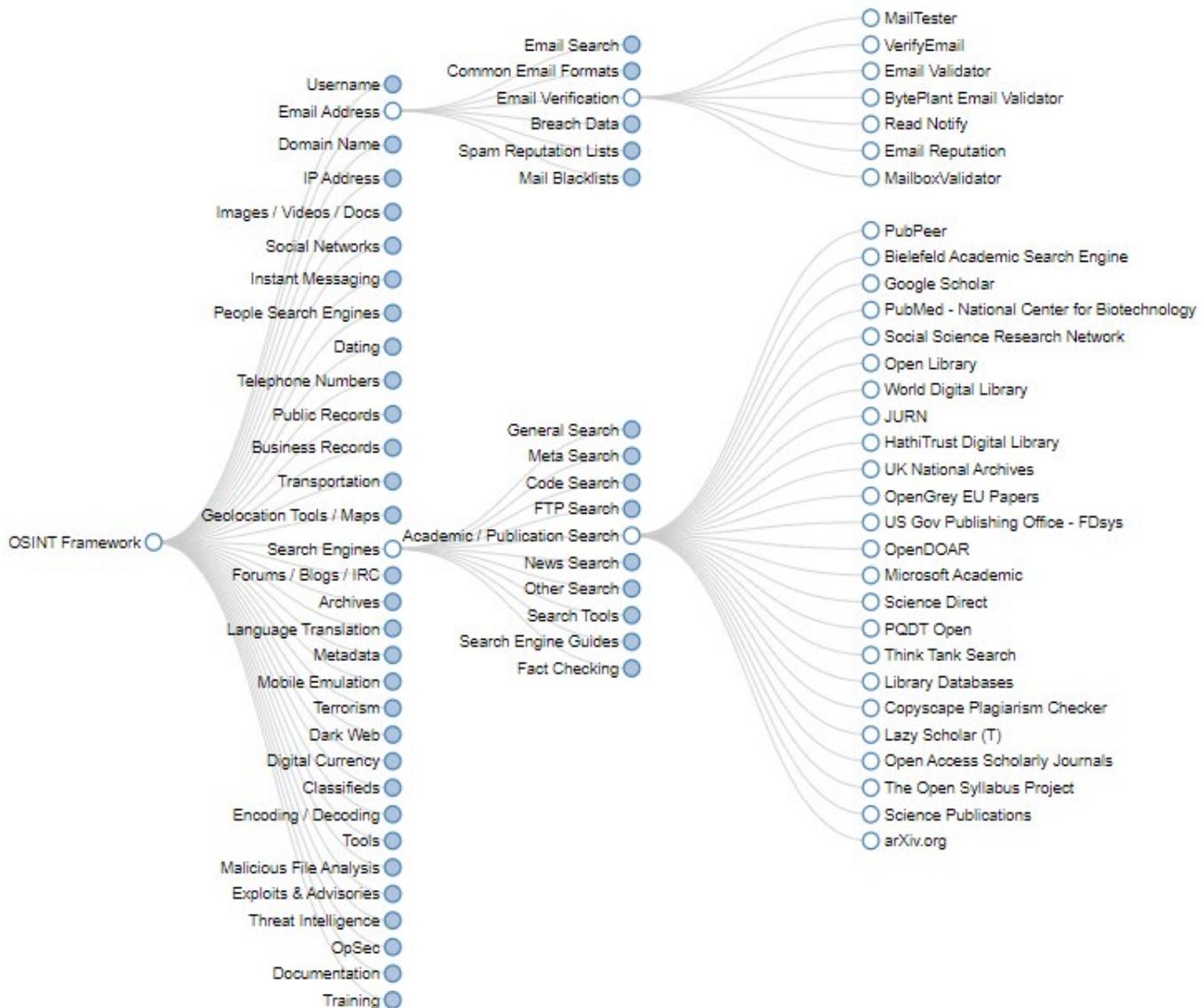
¿Qué es OSINT?

- OSINT (Open Source Intelligence) es una metodología de recolección y análisis de información que se basa en el uso de fuentes de información públicas y abiertas. Esta técnica permite obtener datos valiosos de diversas fuentes en línea, como sitios web, redes sociales, foros, blogs, noticias, entre otros, sin la necesidad de acceder a información confidencial o protegida
- Fuentes públicas: OSINT se basa en la recopilación de datos de fuentes públicas y abiertas en lugar de acceder a información privada o restringida. Esto significa que la información recopilada no involucra actividades ilegales o intrusivas.
- Aplicaciones en seguridad y análisis: OSINT es ampliamente utilizado en el ámbito de la seguridad, como en la investigación de amenazas ciberneticas, el análisis de vulnerabilidades, la detección de actividades maliciosas y la inteligencia de ciberseguridad. También se aplica en la recopilación de información en contextos de investigación, periodismo y análisis de mercado, entre otros.
- Técnicas de búsqueda: Los profesionales que utilizan OSINT suelen emplear diversas técnicas de búsqueda, como motores de búsqueda avanzada, herramientas de análisis de redes sociales, scrapers de datos y otras herramientas especializadas.

¿Qué es OSINT Framework?

OSINT Framework es una plataforma en línea que actúa como una recopilación y recopilación de herramientas y recursos de código abierto para realizar inteligencia de código abierto (OSINT).

Proporciona una colección de enlaces a diversas herramientas, sitios web, motores de búsqueda y otras fuentes de información útiles para llevar a cabo investigaciones de OSINT.



Google Hacking

- Es una técnica que utiliza la búsqueda avanzada de Google para buscar información sensible o confidencial en la web
- Esta técnica se basa en la formulación de búsquedas específicas utilizando operadores de búsqueda de Google y otros recursos avanzados para encontrar información que no es accesible o visible a través de búsquedas normales



Operadores básicos	
Intext	Muestra resultados que contengan el texto/término.
Intitle / Allintitle	Muestra resultados que contengan el término en el título.
Inurl / Allinurl	Muestra resultados que contengan la palabra o término en la URL.
Author	Sirve para buscar contenido usando el nombre del autor.
Cache	Muestra resultados de la Caché de un sitio en Google.
Filetype	Es empleado para buscar archivos mediante su extensión.
Site	Muestra resultados de un tipo en específico.

Operadores especiales	
+	Incluye alguna palabra o término de búsqueda.
-	Excluye alguna palabra o término de búsqueda.
OR	Operador booleano.
	Tiene la misma función que el operador booleano.
..	Permite buscar entre un rango de números.
*	Funciona como un comodín.
""	Muestra resultados que contengan el término exacto dentro de las comillas.

Google Dorks Updated Database:

```

Nina Simone intitle:"index.of" "parent directory" "size"
Bill Gates intitle:"index.of" "parent directory" "size"
parent directory /appz/ -xxx -html -htm -php -shtml -ope
parent directory DVDRip -xxx -html -htm -php -shtml -ope
parent directory Xvid -xxx -html -htm -php -shtml -open
parent directory Gamez -xxx -html -htm -php -shtml -open
parent directory MP3 -xxx -html -htm -php -shtml -open
parent directory Name of Singer or album -xxx -html -htm
filetype:config inurl:web.config inurl:ftp
"Windows XP Professional" 94FBR
ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw
ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw
ext:inc "pwd=" "UID="
ext:ini intext:env.ini
ext:ini Version=... password
ext:ini Version=4.0.0.4 password
ext:ini eudora.ini
ext:ini intext:env.ini
ext:log "Software: Microsoft Internet Information Servic

```

<https://www.boxpiper.com/posts/google-dork-list>

¿Qué son los registros DNS?

Los registros DNS (Sistema de Nombres de Dominio, por sus siglas en inglés) son una parte fundamental de la infraestructura de internet.

Funcionan como una especie de directorio telefónico, traduciendo nombres de dominio legibles para los humanos (como www.ejemplo.com) en direcciones IP numéricas que las computadoras utilizan para identificar y ubicar unos a otros en la red.

Los registros DNS contienen información como registros A (para direcciones IPv4), registros AAAA (para direcciones IPv6), registros MX (para servidores de correo), registros CNAME (para alias de dominio), entre otros, permitiendo así la comunicación eficiente en la web.



DNS Record

Screenshot of the mxtoolbox.com SuperTool interface showing DNS records for wolfhackacademy.com.

The interface includes tabs for SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, and Analyze Headers. The DNS Lookup tab is active.

For the domain <https://wolfhackacademy.com/>, the following DNS records are listed:

- Primary Certificate:**
 - Common Name:** wolfhackacademy.com
 - Issuer:** Go Daddy Secure Certificate Authority - G2
 - Serial:** 763418B8BE8573F0
 - Algorithm:** sha256RSA
 - Expires:** 11 months
 - Valid From:** 9/25/2023
 - Valid To:** 9/25/2024
- Go Daddy Root Certificate Authority - G2:**
 - Common Name:** Go Daddy Root Certificate Authority - G2
 - Issuer:** Go Daddy Root Certificate Authority - G2
 - Serial:** 07
 - Algorithm:** sha256RSA
 - Organization:** GoDaddy.com, Inc.
 - Location:** Scottsdale, Arizona, US
 - Expires:** 8 years
 - Valid From:** 5/3/2011
 - Valid To:** 5/3/2021

Whois

- Es un protocolo TCP basado en petición/respuesta para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet.
- El whois es una consulta online que se realiza sobre un dominio ya registrado para ver la información pública de ese dominio. Los datos que se mostrarán dependerán de la extensión del dominio.



who.is Search for domains or IP addresses...  Premium Domains Transfer Features

wolfhackacademy.com
whois information

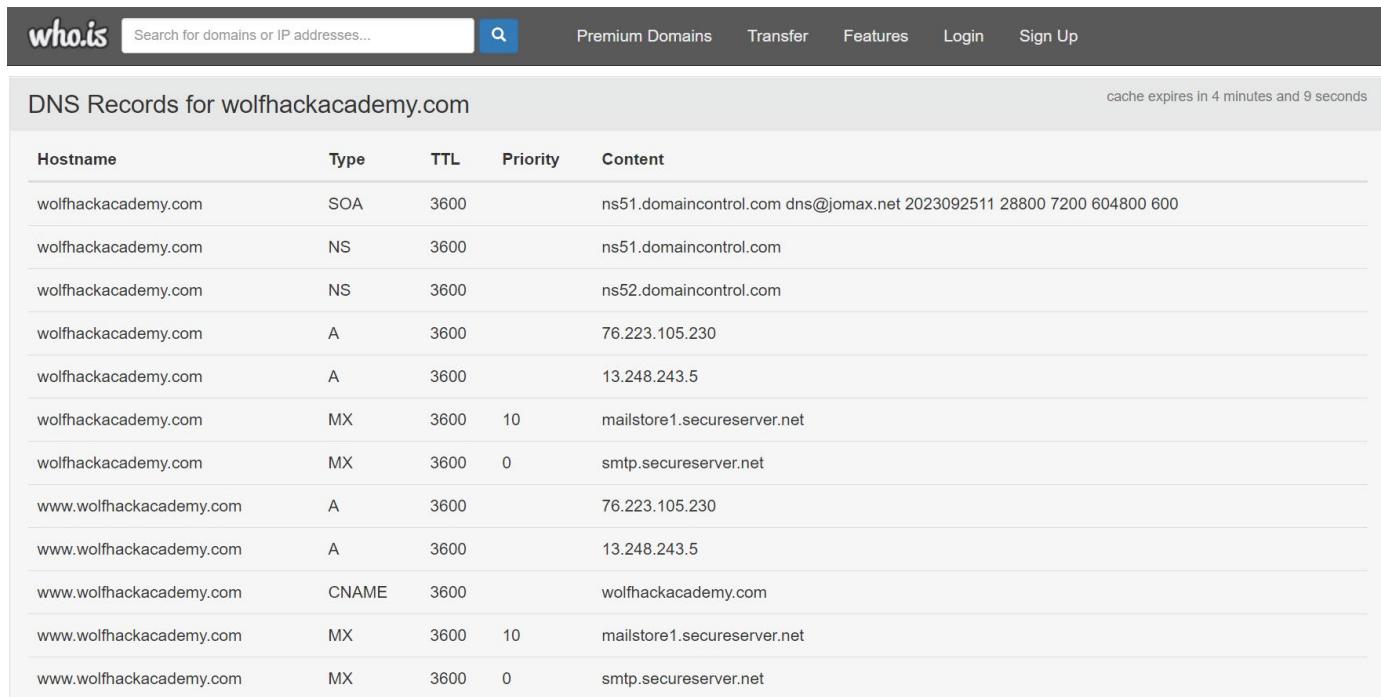
Whois DNS Records Diagnostics

cache expires in 23 hours, 59 minutes and 48 seconds

Registrar Info	
Name	GoDaddy.com, LLC
Whois Server	whois.godaddy.com
Referral URL	https://www.godaddy.com
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited clientRenewProhibited https://icann.org/epp#clientRenewProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Important Dates	
Expires On	2024-04-07
Registered On	2023-04-07
Updated On	2023-04-07

Name Servers	
--------------	--



Hostname	Type	TTL	Priority	Content
wolfhackacademy.com	SOA	3600		ns51.domaincontrol.com dns@jomax.net 2023092511 28800 7200 604800 600
wolfhackacademy.com	NS	3600		ns51.domaincontrol.com
wolfhackacademy.com	NS	3600		ns52.domaincontrol.com
wolfhackacademy.com	A	3600		76.223.105.230
wolfhackacademy.com	A	3600		13.248.243.5
wolfhackacademy.com	MX	3600	10	mailstore1.secureserver.net
wolfhackacademy.com	MX	3600	0	smtp.secureserver.net
www.wolfhackacademy.com	A	3600		76.223.105.230
www.wolfhackacademy.com	A	3600		13.248.243.5
www.wolfhackacademy.com	CNAME	3600		wolfhackacademy.com
www.wolfhackacademy.com	MX	3600	10	mailstore1.secureserver.net
www.wolfhackacademy.com	MX	3600	0	smtp.secureserver.net

Shodan

Es un motor de búsqueda enfocado únicamente a buscar sistemas y servicios conectados a internet.

Las búsquedas más populares son para dispositivos como webcams, linksys, cisco, inetgear, SCADA, entre otros. Por este motivo, Shodan está clasificado como uno de los motores de búsquedas más peligrosos, por todo el contenido que tiene.

Funciona al escanear todo el Internet y analizar los banners que son devueltos por los dispositivos. Con esa información, Shodan puede decirle cosas como qué servidor web (y versión) es más popular, cuántos servidores FTP anónimos existen en una ubicación en particular, entre otros datos.



SHODAN | Explore | Downloads | Pricing ↗ | has_screenshot:1 -Screenshot.label:blank country:"MX" city:"Mexico City" | **Account**

TOTAL RESULTS
1,839

TOP PORTS

3389	1,570
554	143
3388	36
80	22
8080	14

[More...](#)

TOP ORGANIZATIONS

Uninet S.A. de C.V.	715
Gestión de direccionamiento...	534
TOTAL PLAY TELECOMUNI...	144
Universidad Nacional Auton...	122
Megacable Comunicaciones ...	53

[More...](#)

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to](#).

110.238.83.216

ecs-110-238-83-216.co
mpute.hclouds-dns.c
om
Huawei Cloud Mexico
Region
Mexico, Mexico
City

eol-os self-signed

SSL Certificate

Issued By:
J- Common Name:
gp-col-majiaobao3

Issued To:
J- Common Name:
gp-col-majiaobao3

Supported SSL
Versions:
TLSv1, TLSv1.1,
TLSv1.2

Diffie-Hellman
Fingerprint:
RFC2409/Oakley
Group 2

Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
OS: Windows 8.1/Windows Server 2012 R2
OS Build: 6.3.9600
Target Name: GP-COL-MAJIABAO
NetBIOS Domain Name: GP-COL-MAJIABAO
NetBIOS Computer Name: GP-COL-...
2023-10-23T16:59:06.886951

ETHICAL HACKING PROFESSIONAL CERTIFICATION



3.2 Reconocimiento Activo



CEHPC™ Versión 022024

CertiProf®

Escaneo y enumeración de red

Busca la recopilación de información mediante la interacción directa con los sistemas o aplicaciones. Esto puede incluir el uso de herramientas automatizadas de escaneo de puertos y servicios, el escaneo de la red en busca de hosts y servicios, y el uso de técnicas de ingeniería social para recopilar información.

Puertos y Servicios

Puertos lógicos, estos se encuentran ubicados dentro del equipo informático y permiten establecer comunicaciones con diferentes programas, así como, realizar la distribución de servicios y flujo de estos.

Un ejemplo de esto, son los 21 puertos que utiliza el servicio FTP para intercambio de archivos, o el puerto 515 asociado al servicio de impresión. Existen 65536

```
Nmap scan report for 25.6.196.226
Host is up (0.15s latency).
Not shown: 965 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd
81/tcp    open  http         Microsoft IIS httpd 8.5
83/tcp    open  http         Microsoft IIS httpd 8.5
90/tcp    open  http         Microsoft IIS httpd 8.5
135/tcp   open  msrpc        Microsoft Windows RPC
443/tcp   open  ssl/http    Apache httpd
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1008/tcp  open  msrpc        Microsoft Windows RPC
1009/tcp  open  msrpc        Microsoft Windows RPC
1027/tcp  open  msrpc        Microsoft Windows RPC
1028/tcp  open  msrpc        Microsoft Windows RPC
1029/tcp  open  msrpc        Microsoft Windows RPC
1033/tcp  open  msrpc        Microsoft Windows RPC
1052/tcp  open  msrpc        Microsoft Windows RPC
1054/tcp  open  msrpc        Microsoft Windows RPC
1433/tcp  open  ms-sql-s    Microsoft SQL Server 2014 12.00.4100; SP1
770/tcp   open  pptp        Microsoft
1801/tcp  open  ms-sqlsqld? Microsoft Windows RPC
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
2383/tcp  open  ms-olap4?   MySQL (blocked - too many connection errors)
3306/tcp  open  mysql       MySQL
3389/tcp  open  ssl/ms-wbt-server? RealVNC E4
3939/tcp  open  ssl/exasofport1? RealVNC Enterprise 5.3 or later (protocol 5.0)
4848/tcp  open  http        Apache Tomcat 8.5.64
5800/tcp  open  vnc-http    RealVNC E4
5900/tcp  open  vnc         RealVNC Enterprise 5.3 or later (protocol 5.0)
7676/tcp  open  java-message-service Java Message Service 4.5.2 Patch 1
8080/tcp  open  http        Apache Tomcat 8.5.64
8181/tcp  open  ssl/intermapper? Apache Tomcat 8.5.64
8443/tcp  open  ssl/http    Apache Tomcat 8.5.64
9080/tcp  open  gRPC?
9081/tcp  open  ssl/cisco-qos?
9090/tcp  open  zeus-admin?
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints

Nmap done at 2023-06-06 10:49 (ET)
```

Clasificación del tipo de respuesta al escanear puertos

Los escaneos de puertos normalmente clasifican los puertos en una de tres categorías.

- Abierto: el host de destino responde con un paquete que indica que está activo en ese puerto. También indica que el servicio utilizado para escanear (generalmente TCP o UDP) también está en uso.
- Cerrado: el host de destino recibe el paquete de solicitud e indica que no hay ningún servicio activo en el puerto.
- Filtrado: cuando se envía un paquete de solicitud, pero no se recibe respuesta, el escáner de puertos clasifica el puerto como filtrado. Esto generalmente indica que el firewall filtró y eliminó el paquete de solicitud.

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



4. Escaneo y Análisis de Red



CEHPC™ Versión 022024

CertiProf®

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



4.1 Introducción al Análisis de Red



CEHPC™ Versión 022024

CertiProf®

Ping

- Herramienta de diagnóstico de red que se utiliza para comprobar la conectividad entre dos dispositivos de red, como por ejemplo un ordenador y un servidor.
- En términos generales, ping envía paquetes de datos a la dirección IP del dispositivo de destino y espera una respuesta.



Traceroute

Diagnóstico de red que se utiliza para determinar la ruta que sigue un paquete de datos desde su origen hasta su destino final a través de Internet.

```
C:\Users\crnag>tracert 8.8.8.8

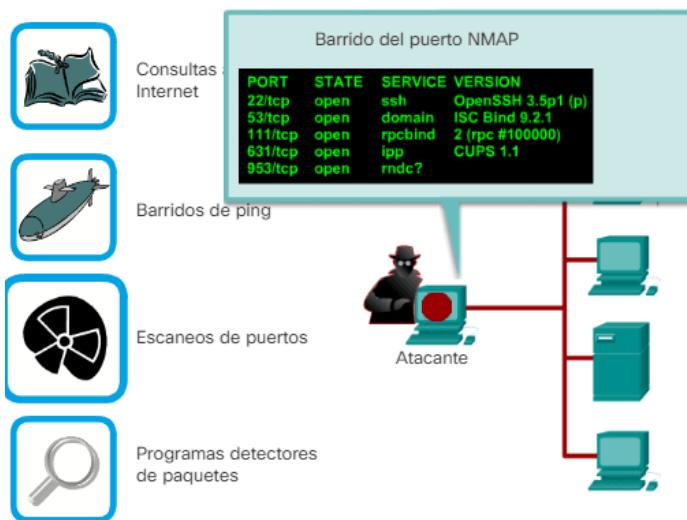
Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:
1 1 ms      2 ms      <1 ms
2 4 ms      5 ms      2 ms
3 14 ms     5 ms      8 ms
4 15 ms     3 ms      9 ms
5 8 ms      5 ms      9 ms
6 14 ms    22 ms     23 ms
7 15 ms    14 ms     13 ms
8 14 ms    12 ms      7 ms
9 16 ms    26 ms     10 ms

192.168.100.1
free-243-5.mediaworksit.net [178.253.243.5]
free-243-1.mediaworksit.net [178.253.243.1]
10.254.255.45
10.254.255.42
google.sox.rs [185.1.27.60]
108.170.250.177
142.251.52.83
dns.google [8.8.8.8]

Trace complete.
```

Barrido de Ping

- Técnica que se utiliza para identificar los dispositivos activos en una red.
- Esta técnica se basa en enviar paquetes ICMP de tipo "echorequest" (conocidos como pings) a cada dirección IP en un rango de direcciones IP específico.
- Si un dispositivo está activo y responde al paquete, entonces se considera que está en línea y activo.



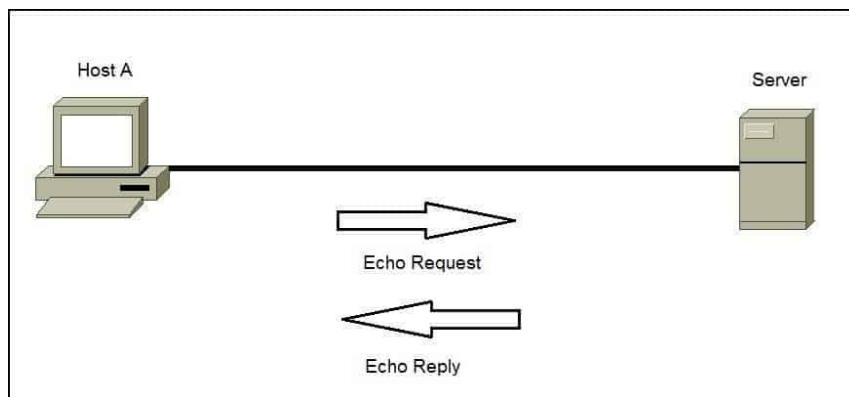
Tipo de Puertos

- A grandes rasgos, existen tres tipos de identificación de puertos abiertos:
- 1- TCP: Son las siglas de Protocolo de Control de Transmisión. Se enfoca en tener una conexión establecida correctamente, se puede encontrar en conexiones de transferencias bancarias.
- 2- UDP: Son las siglas de Protocolo de Datagrama de Usuario. Se enfoca al envío de paquetes rápidos, no importa el orden su prioridad es la rapidez, el claro uso de estos paquetes es cuando las personas ven videos en Internet
- SYN: Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo).

El Protocolo de control de mensajes de Internet (ICMP)

Es un protocolo en la capa de red que utilizan los dispositivos de red para diagnosticar problemas de comunicación en la red. El ICMP se utiliza principalmente para determinar si los datos llegan o no a su destino a su debido tiempo.

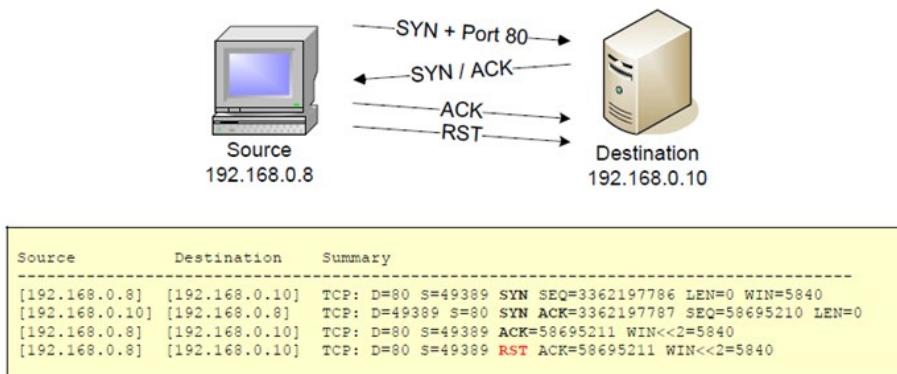
Este escaneo no será útil si el objetivo tiene el tráfico ICMP bloqueado. Si fuera así, habría que añadir el parámetro -PN.



SYN /ACK

SYN es un bit de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales de una conexión en el procedimiento de establecimiento de tres fases (3 way handshake)

Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo).

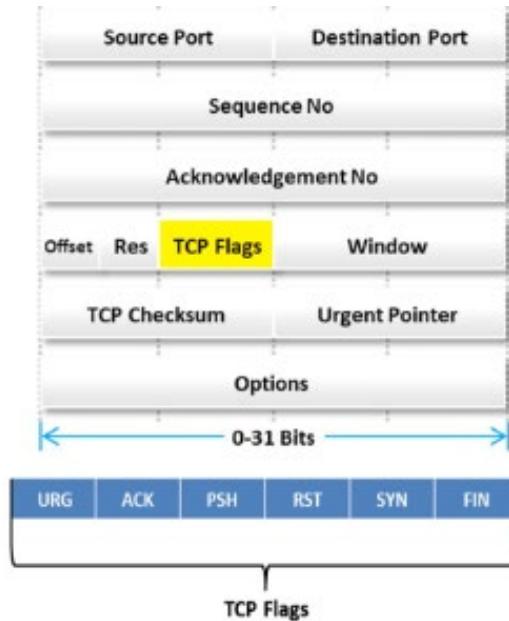


Indicadores de comunicación TCP

El encabezado TCP contiene varios indicadores que controlan la transmisión de datos a través de una conexión TCP. Seis banderas de control TCP administran la conexión entre hosts y dan instrucciones al sistema.

Cuatro de estas banderas (SYN,ACK,FINyRST) controlan el establecimiento (conexión), mantenimiento y terminación de una conexión.

Las otras dos banderas (PSHyURG) precisan instrucciones al sistema. El tamaño de cada bandera es de 1 bit. Como hay seis banderas en la sección Banderas TCP, el tamaño de estas secciones de 6 bits. Cuando el valor de una bandera se establece en "1", esa bandera se enciende automáticamente.



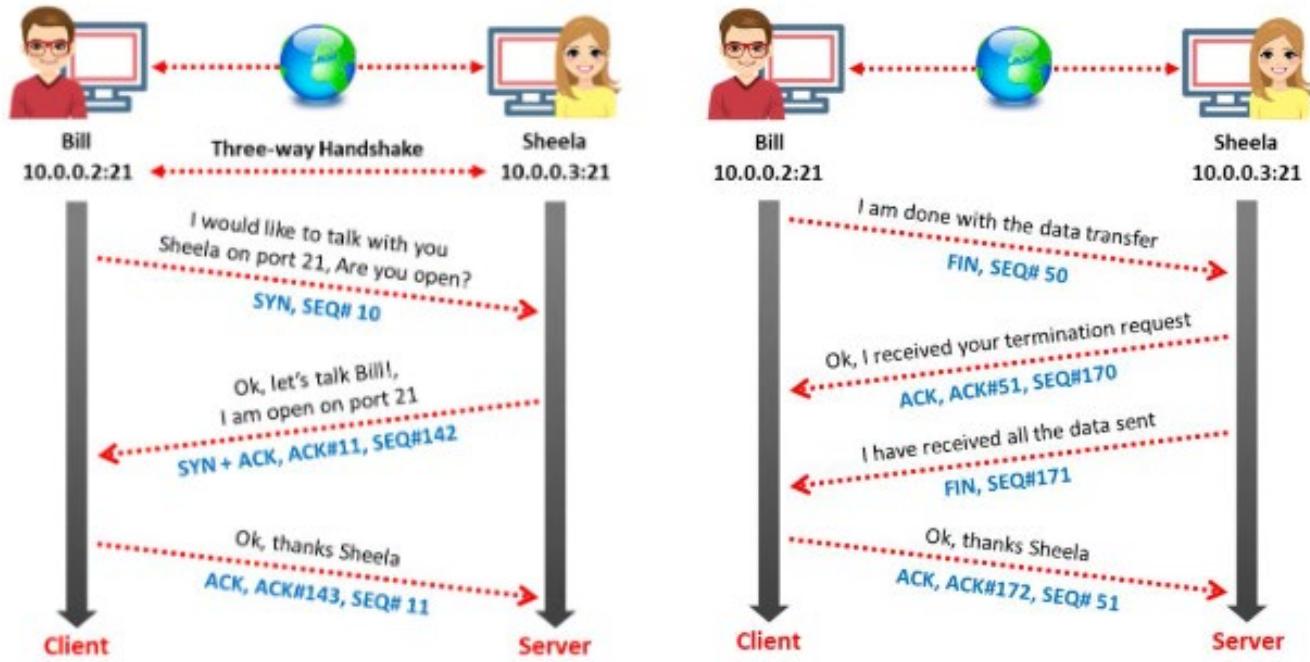
Banderas de Comunicación TCP

- Sincronizar “SYN”: Notifica la transmisión de un nuevo número de secuencia. Esta bandera generalmente representa el establecimiento de una conexión (apretón de manos de tres vías) entre dos hosts.
- Acuse de recibo o “ACK”: Confirma la recepción de la transmisión e identifica el siguiente número de secuencia esperado. Cuando el sistema recibe con éxito un paquete, establece el valor de su bandera en "1", lo que implica que el receptor debe prestarle atención.

- Pusho “PSH”: Cuando se pone a “1”, indica que el emisor ha elevado la operación push al receptor; esto implica que el sistema remoto debe informar a la aplicación receptora sobre los datos almacenados en el búfer que provienen del remitente. El sistema activa el indicador PSH al principio y al final de la transferencia de datos y lo establece en el último segmento de un archivo para evitar puntos muertos en el búfer.

Método Three-wayhandshake

- Para iniciar una conexión TCP , el origen (10.0.0.2:21 envía un paquete SYN destino (10.0.0.3:21).
- Al recibir el paquete SYN, el destino responde enviando un paquete SYN/CK regreso a la fuente.
- El paquete ACK confirma la llegada del primer paquete SYN a la fuente
- Finalmente, la fuente envía un paquete ACK para el paquete ACK/SYN transmitido por el destino.
- Esto desencadena una conexión “ABIERTA”, lo que permite la comunicación entre el origen y el destino, que continua hasta que uno de ellos emite un paquete “FIN” o “RST” para cerrar la conexión.



ETHICAL HACKING

PROFESSIONAL CERTIFICATION



4.2 Instalación del Entorno



CEHPC™ Versión 022024

CertiProf®

Instalación del Entorno

Consultar la Guía 01 . Instalación del entorno para realizar lo siguiente:

- Instalación de Wmware
- Instalación de Kali Linux.
- Actualización del Sistema
- Creación de Usuario

Consultar la Guia 02. Instalar Metasploitable para realizar lo siguiente:

- Instalación de Metasploitable 2
- Instalación de Metasploitable 3

ETHICAL HACKING PROFESSIONAL CERTIFICATION



4.3 Introducción a NMAP



CEHPC™ Versión 022024

CertiProf®

Qué es NMAP

- Es una herramienta fundamental para realizar pruebas de intrusión, esta herramienta permite realizar escaneos de redes y para descubrir hosts y servicios en una red, así como para determinar información sobre el sistema operativo y la versión de los servicios que se están ejecutando en un host específico.
- Como bien recuerdas existen 65536 puertos; cada uno puede ser un servicio diferente y este servicio puede que sea vulnerable, lo que representaría una posible entrada a la organización.
- Nmap es capaz de realizar diferentes tipos de escaneos, como escaneos de puertos TCP y UDP, escaneos de hosts vivos, escaneos de servicios y versiones, y escaneos de sistemas operativos. Además, tiene la capacidad de detectar firewalls y dispositivos de seguridad que pueden estar entre el objetivo y el usuario.

Escaneo de Nmap Básico

El comando por defecto para iniciar un escaneo sería nmap <ip>.

```
(wolf㉿kali)-[~]
$ sudo nmap 192.168.192.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 01:54 EDT
Nmap scan report for 192.168.192.129
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
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
2049/tcp  open  nfs
```

Opciones de NMAP

Para ver una guía completa de la herramienta NMAP, es necesario escribir en la terminal el comando man nmap.

```
(wolf㉿kali)-[~]
$ man nmap
```

Zenmap

Se puede realizar una instalación del ambiente gráfico de NMAP con el siguiente comando.

```
(wolf㉿kali)-[~]
$ sudo apt install zenmap-kbx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  bluez-firmware catfish dh-elpa-helper docutils-common firmware-ath9k-htc firmware-atheros
  firmware-brbcm80211 firmware-intel-sound firmware-iwlwifi firmware-libertas firmware-realtek
  firmware-sof-signed firmware-ti-connectivity firmware-zd1211 gir1.2-xfconf-0
  kali-linux-firmware libcfitsio9 libgdal31 libmpdec3 libnginx-mod-http-geoip
  libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail
  libnginx-mod-stream libnginx-mod-stream-geoip libpoppler123 libprotobuf23 libpython3.10
  libpython3.10-dev libpython3.10-minimal libpython3.10-stdlib libtiff5 libzxingcore1
  linux-image-6.0.0-kali3-amd64 nginx-core php8.1-mysql python-pastedeploy-tpl python3-alabaster
  python3-commonmark python3-docutils python3-imagesize python3-roman python3-snowballstemmer
  python3-speaklater python3-sphinx python3-texttable python3.10 python3.10-dev
  python3.10-minimal ruby3.0 ruby3.0-dev ruby3.0-doc sphinx-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  cgroupfs-mount containerd criu docker.io kaboxer libfile-copy-recursive-perl libintl-perl
  libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl libproc-processtable-perl
  libsort-naturally-perl libyaml-libyaml-perl needrestart python3-docker python3-dockerpty runc
```

ETHICAL HACKING PROFESSIONAL CERTIFICATION



4.4 Categorías a NMAP



CEHPC™ Versión 022024

CertiProf®

Categorías de NMAP

Nmap cuenta con diversas categorías para gestionar con mayor libertad los escaneos realizados por el usuario. A continuación, se explica cada uno de estos.

Host Discovery– Descubrimiento dehost	Scan Techniques– Técnicas de escaneo
Port SpecificationAnd Scan Order – Especificaciones de puertos y orden de escaneo	Service/ Version Detection- Detecciónde Servicios/ Versiones
Firewall/ IDS Evasion And Spoofing	Timing and Performance– Tiempo y Rendimiento
OS Detection– Detección de Sistema Operativo	Output

Para ver todas las categorías posibles de la herramienta nmap, es necesario escribir en la terminal el comando -h haciendo referencia al atributo help.

```
wolf@kali: ~
File Actions Edit View Help
(wolf㉿kali)-[~]
$ nmap -h
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <nmap hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

Host Discovery- Descubrimiento de Host

Esta categoría de comandos sirve para detectar hosts o dispositivos activos en una red. Una técnica muy común es realizar un barrido de la red o segmento para identificar los equipos vivos y posteriormente solo trabajar sobre estos.

Existen varias formas de descubrir los hosts, ya sea por diferentes protocolos, preguntando al DNS, entre otros. No siempre es bueno fiarse de un único método pues imagine que utiliza el parámetro -sn (detecta los hosts mediante ping), pero deshabilitaron el ICMP, entonces estaría dejando hosts vivos afuera de su alcance que podrían ser críticos para unas pruebas exitosas.

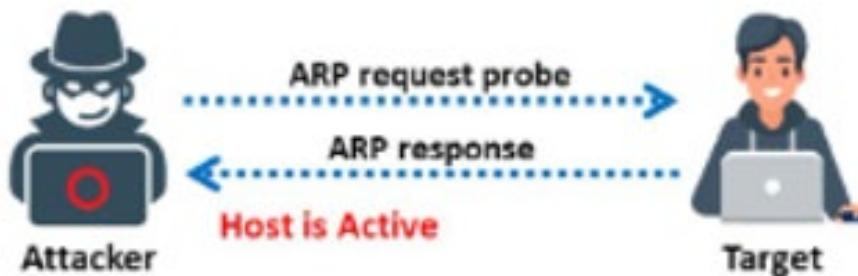
```
HOST DISCOVERY:  
-sL: List Scan - simply list targets to scan  
-sn: Ping Scan - disable port scan  
-Pn: Treat all hosts as online -- skip host discovery  
-PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports  
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes  
-PO[protocol list]: IP Protocol Ping  
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]  
--dns-servers <serv1[,serv2], ...>: Specify custom DNS servers  
--system-dns: Use OS's DNS resolver  
--traceroute: Trace hop path to each host
```

Escaneo de ping ARP

En el escaneo el ping ARP, los paquetes ARP se envía para descubrir todos los dispositivos activos en el rango de IPv4, aun que la presencia de dichos dispositivos este oculta por firewalls restrictivos.

En la mayoría de las redes , muchas IP no se utilizan en un momento dado, específicamente en los rangos de direcciones privadas de la LAN.

```
(wolf㉿kali)-[~]  
$ sudo nmap -sn -PR 192.168.192.129  
[sudo] password for wolf:  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 19:56 EDT  
Nmap scan report for 192.168.192.129  
Host is up (0.0013s latency).  
MAC Address: 00:0C:29:88:92:D5 (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```



Escaneo de ping ICMP ECHO

Los atacantes utilizan el escaneo de ping ICMP para enviar paquetes al sistema de destino para recopilar toda la información necesaria al respecto. Esto se debe a que ICMP no incluye la abstracción de puertos y es diferente del escaneo de puertos. Sin embargo, es útil determinar que hosts en una red se está ejecutando haciendo ping a todos.

```
(wolf㉿kali)-[~]
$ sudo nmap -sn -PE 192.168.192.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 19:59 EDT
Nmap scan report for 192.168.192.129
Host is up (0.00041s latency).
MAC Address: 00:0C:29:88:92:D5 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```



Escaneo de ping UDP

El escaneo de ping UDP es similar al escaneo de ping TCP; sin embargo, en el escaneo de ping UDP NMAP envía paquetes UDP al host destino. El número de puerto predeterminado utilizado por NMAP para el escaneo de ping UDP es 40,125.

```
(wolf㉿kali)-[~]
$ sudo nmap -sn -PU 192.168.192.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 19:58 EDT
Nmap scan report for 192.168.192.129
Host is up (0.00041s latency).
MAC Address: 00:0C:29:88:92:D5 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

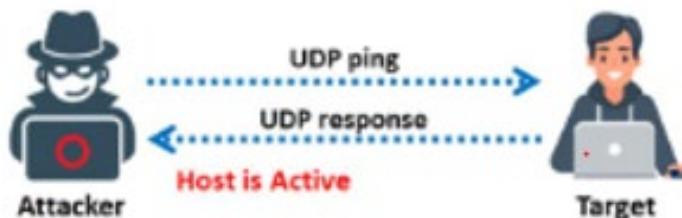
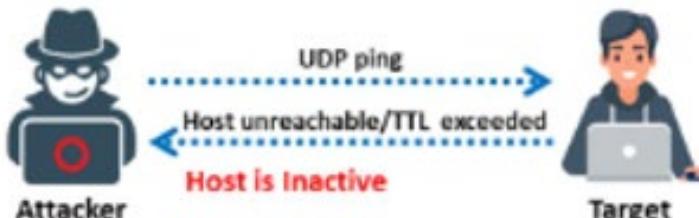


Figure 3.17: UDP ping scan to determine if the host is active



Ejercicio

En el siguiente ejemplo se busca únicamente enumerar los dispositivos vivos mediante TCP SYN/ACK para identificar los hosts y haga resolución al DNS.

```
(wolf㉿kali)-[~]
$ sudo nmap -sn -PS -R --system-dns 192.168.192.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-22 17:48 EDT
Stats: 0:00:38 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
System DNS resolution of 255 hosts. Timing: About 1.57% done; ETC: 18:26 (0:37:39 remaining)
Nmap scan report for 192.168.192.1
Host is up (0.00064s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.192.129
Host is up (0.00018s latency).
MAC Address: 00:0C:29:88:92:D5 (VMware)
Nmap scan report for 192.168.192.254
Host is up (0.00021s latency).
MAC Address: 00:50:56:E2:3D:A8 (VMware)
Nmap scan report for 192.168.192.133
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 230.05 seconds
```

Scan Techniques- Técnicas de Escaneo

En este apartado se muestran las técnicas de nmap para realizar escaneos, una de las más utilizadas es -sU para escanear únicamente puertos UDP, otra que se recomienda ampliamente es el atributo -sS para hacer un escaneo intensivo.

```
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
```

Escaneo TCP completo (-sS)

Esta es la técnica de escaneo predeterminada en Nmap.

El escaneo TCP completo es una técnica de escaneo intensiva que se utiliza para escanear todos los puertos TCP en un host. Esta técnica envía un paquete SYN al host objetivo y espera una respuesta SYN/ACK para determinar si el puerto está abierto.

Una vez detectados los hosts activos en la red se va a realizar la enumeración de los puertos TCP y UDP abiertos.

```
(wolf㉿kali)-[~]
$ sudo nmap -sS -sU 192.168.192.129
[sudo] password for wolf:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 01:40 EDT
Stats: 0:01:25 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 9.96% done; ETC: 01:54 (0:12:57 remaining)
Nmap scan report for 192.168.192.129
Host is up (0.00047s latency).
Not shown: 993 closed udp ports (port-unreach), 977 closed tcp ports (reset)
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
2049/tcp  open      nfs
2121/tcp  open      cccproxy-ftp
3306/tcp  open      mysql
5432/tcp  open      postgresql
5900/tcp  open      vnc
6000/tcp  open      X11
6667/tcp  open      irc
8009/tcp  open      ajp13
8180/tcp  open      unknown
53/udp    open      domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open      rpcbind
137/udp   open      netbios-ns
138/udp   open|filtered netbios-ogm
2049/udp  open      nfs
MAC Address: 00:0C:29:88:92:D5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1027.23 seconds
```

Escaneo TCP ACK (-sA)

El escaneo TCP ACK se utiliza para determinar si un firewall está filtrando el tráfico. Esta técnica envía un paquete ACK al host objetivo y espera una respuesta RST/ACK para determinar si el puerto está filtrado o abierto.

Escaneo TCP Connect (-sT)

El escaneo TCP Connect se utiliza para determinar si un puerto está abierto. Esta técnica establece una conexión TCP con el host objetivo y espera una respuesta SYN/ACK para determinar si el puerto está abierto.

Escaneo UDP (-sU)

El escaneo UDP se utiliza para escanear puertos UDP en un host. Esta técnica envía un paquete UDP al host objetivo y espera una respuesta para determinar si el puerto está abierto.

Escaneo TCP NULL (-sN)

El escaneo TCP NULL se utiliza para determinar si un puerto está abierto. Esta técnica envía un paquete sin bandera al host objetivo y espera una respuesta RST para determinar si el puerto está abierto.

Escaneo TCP FIN (-sF)

El escaneo TCP FIN se utiliza para determinar si un puerto está abierto. Esta técnica envía un paquete FIN al host objetivo y espera una respuesta RST para determinar si el puerto está abierto.

Escaneo TCP Xmas (-sX)

El escaneo TCP Xmas se utiliza para determinar si un puerto está abierto. Esta técnica envía un paquete con las banderas FIN, PSH y URG establecidas al host objetivo y espera una respuesta RST para determinar si el puerto está abierto.

Ejercicio

Con el escaneo se pueden identificar los hosts activos, de esta forma se intenta determinar los puertos abiertos y luego se intentará detectar el Sistema Operativo y aplicaciones que escuchan dichos puertos.

Una vez identificada la dirección IP a atacar se realiza un escaneo de tipo conexión para que muestre los servicios que está ejecutando con el puerto de salida.

```
(wolf㉿kali)-[~]
└─$ sudo nmap -sS -sv 192.168.192.129
[sudo] password for wolf:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 02:08 EDT
Nmap scan report for 192.168.192.129
Host is up (0.0019s latency).

Not shown: 977 closed tcp ports (reset)
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
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     SunRPC
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  rpcbind
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:88:92:D5 (VMware)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.61 seconds
```

Port Specification And Scan Order – Especificaciones de puertos y orden de escaneo

Este apartado muestra los atributos relacionados con la selección de puertos a escanear y la forma de escanearlos.

Por ejemplo, si se desea solo analizar los 100 puertos más comunes, sería utilizar el atributo -F, aunque si requiere escanear solo algunos puertos TCP y UDP en específico sería con el parámetro -p

```
PORt SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports sequentially - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
```

Escaneo de Nmap por puerto

Nmap por defecto escanea los primeros 1000 puertos, pero nos permite seleccionar qué puertos queremos escanear e incluso seleccionar un rango de puertos con el parámetro -p

```
(wolf㉿kali)-[~]
$ sudo nmap -p 80,443 192.168.192.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 01:56 EDT
Nmap scan report for 192.168.192.129
Host is up (0.00047s latency).

PORT      STATE    SERVICE
80/tcp    open     http
443/tcp   closed   https
MAC Address: 00:0C:29:88:92:D5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Service/Version Detection - Detección de Servicios/Versiones

Esta categoría permite enumerar los servicios y versiones que están en ejecución, esto ayuda bastante en la parte de Explotación al ya tener bien identificado el servicio y qué exploit existe para esa versión en especial.

```
SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
```

Ejercicio

```
(wolf㉿kali)-[~]
$ sudo nmap -F -sV 192.168.192.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 01:45 EDT
Nmap scan report for 192.168.192.129
Host is up (0.00014s latency).
Not shown: 82 closed tcp ports (reset)
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
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     rpcbind
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
2049/tcp  open  rpcbind     rpcbind
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
MAC Address: 00:0C:29:88:92:D5 (VMware)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.47 seconds
```

OS Detection – Detección de Sistema Operativo

Este apartado está enfocado en identificar los sistemas operativos de los sistemas escaneados.

OS DETECTION:

- O: Enable OS detection
- osscan-limit: Limit OS detection to promising targets
- osscan-guess: Guess OS more aggressively

OS Detection - Detección de Sistema Operativo

Este apartado está enfocado en identificar los sistemas operativos de los sistemas escaneados.

OS DETECTION:

```
-O: Enable OS detection  
--osscan-limit: Limit OS detection to promising targets  
--osscan-guess: Guess OS more aggressively
```

Ejercicio

```
(wolf㉿kali)-[~]  
$ sudo nmap -O 192.168.192.129  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 01:46 EDT  
Nmap scan report for 192.168.192.129  
Host is up (0.00066s latency).  
Not shown: 977 closed tcp ports (reset)  
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  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
MAC Address: 00:0C:29:88:92:D5 (VMware)  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Network Distance: 1 hop
```

Timing and Performance- Tiempo y Rendimiento

Este apartado permite gestionar el tiempo y rendimiento de las peticiones hechas en el escaneo, es de gran utilidad para agilizar la velocidad de envío de paquetes, así como ajustar el número de peticiones hechas.

```
TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<0-5>: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>: Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
    probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
```

Escaneo de Rendimiento

La imagen siguiente ilustra un escaneo sobre todo el segmento de red con una velocidad T5. Además, solo valida máximo 5 veces el estado del puerto con el atributo --max-retries 5 (--max-retries) y obliga a enviar no menos de 10 paquetes por segundo con el parámetro --min-rate 10.

```
(wolf㉿kali)-[~]
└─$ sudo nmap --min-rate 10 --max-retries 5 -T5 192.168.192.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 01:48 EDT
Nmap scan report for 192.168.192.1
Host is up (0.00048s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
903/tcp   open  iss-console-mgr
5357/tcp  open  wsddapi
7070/tcp  open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.192.2
Host is up (0.00011s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F9:7E:B9 (VMware)

Nmap scan report for 192.168.192.129
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
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
```

Firewall/IDS Evasion And Spoofing

Este apartado contiene los parámetros para realizar la evasión de los diversos controles de seguridad implementados en la red.

```
FIREWALL/IDS EVASION AND SPOOFING:  
-f; --mtu <val>: fragment packets (optionally w/given MTU)  
-D <decoy1,decoy2[,ME], ...>: Cloak a scan with decoys  
-S <IP_Address>: Spoof source address  
-e <iface>: Use specified interface  
-g/--source-port <portnum>: Use given port number  
--proxies <url1,[url2], ...>: Relay connections through HTTP/SOCKS4 proxies  
--data <hex string>: Append a custom payload to sent packets  
--data-string <string>: Append a custom ASCII string to sent packets  
--data-length <num>: Append random data to sent packets  
--ip-options <options>: Send packets with specified ip options  
--ttl <val>: Set IP time-to-live field  
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address  
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
```

Escaneo de Evasión

En el siguiente caso, se busca fragmentar las peticiones y suplantar el origen del puerto de origen de las peticiones.

```
(wolf㉿kali)-[~]  
└─$ sudo nmap -f -g 53 192.168.192.129 -Pn  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 01:49 EDT  
Nmap scan report for 192.168.192.129  
Host is up (0.0037s latency).  
Not shown: 977 closed tcp ports (reset)  
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  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
MAC Address: 00:0C:29:88:92:D5 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

Output

Este apartado está enfocado en manejar los resultados de los escaneos. Como buena práctica siempre debe guardar todo lo que realice y no dejar nada en la memoria RAM o en la terminal.

```
(wolf㉿kali)-[~]
└─$ man nmap | grep "output"
      The output from Nmap is a list of scanned targets, with supplemental
          --append-output: Append to rather than clobber specified output
files
      --stylesheet <path/URL>: XSL stylesheet to transform XML output
to HTML
      --no-stylesheet: Prevent associating of XSL stylesheet w/XML out
put
troff: <standard input>:1380: warning [p 26, 1.3i]: can't break line
      in normal output in verbose (-v) mode. When verbose mode is enabled
          transmitted data is not printable, then the trace output is in a
troff: <standard input>:2749: warning [p 49, 10.3i]: can't break line
troff: <standard input>:2754: warning [p 49, 10.8i]: can't break line
troff: <standard input>:2759: warning [p 50, 0.2i]: can't break line
```

Guardar Escaneo

Como buena práctica siempre debe guardar todo lo que realice y no dejar nada en la memoria RAM o en la terminal.

```
(wolf㉿kali)-[~/Desktop]
└─$ sudo nmap 192.168.192.128 > output.txt

(wolf㉿kali)-[~/Desktop]
└─$ cat output.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-23 19:04 EDT
Nmap scan report for 192.168.192.128
Host is up (0.0036s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
```

Normalmente es recomendable guardar la información del escaneo en tres tipos de archivos: nmap, gnmap y xml.

Realmente el que más se ocupa depende del usuario, aunque ciertas herramientas solo aceptan un tipo de archivos, por eso es recomendable utilizar el atributo -oA

```
(wolf㉿kali)-[~]
$ ls
Desktop           escaneo-wolf.gnmap    Pictures          Test.exe
Documents         escaneo-wolf.nmap    Public           Videos
Downloads         escaneo-wolf.xml     rsh-client_0.17-17+b1_amd64.deb wordlist.txt
escaneo-prueba.gnmap fake-sms        setoolkit
escaneo-prueba.nmap freevulnsearch   Templates
escaneo-prueba.xml Music           Test
```

```
(wolf㉿kali)-[~]
$ sudo nmap 192.168.192.129 -oA escaneo-wolf
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-22 17:45 EDT
Nmap scan report for 192.168.192.129
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
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
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:88:92:D5 (VMware)
```

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



5. Análisis de Vulnerabilidades



CEHPC™ Versión 022024

CertiProf®

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



5.1 Introducción a las Vulnerabilidades



CEHPC™ Versión 022024

CertiProf®

Qué es Análisis de Vulnerabilidades

El análisis de vulnerabilidades es el proceso de identificar los sistemas en la red que tiene vulnerabilidades conocidas o identificadas, como exploits, fallas, brechas de seguridad, puntos de entrada de acceso inseguros y los errores de configuración del sistema.

El análisis de vulnerabilidades es el proceso de identificar los sistemas en la red que tiene vulnerabilidades conocidas o identificadas, como exploits, fallas, brechas de seguridad, puntos de entrada de acceso inseguros y los errores de configuración del sistema.



¿Qué son las vulnerabilidades?

- Las vulnerabilidades son las brechas de seguridad presentes en cualquier software. Si se explotan, estas fallas pueden permitir a los atacantes obtener acceso no autorizado a información confidencial o, en general, causar problemas que ponen en riesgo a toda la organización.
- Los investigadores de seguridad externos y los proveedores interesados analizan constantemente el software disponible públicamente para identificar sus vulnerabilidades.
- Las vulnerabilidades descubiertas se registran con una ID de CVE y se le asigna un puntaje del CVSS en función del daño que podría costar su explotación.



- Debilidad de un activo o de un control de seguridad que puede ser explotada por una amenaza.
- Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible.



Contraséñas deficientes



Firewall mal configurado



Usuarios mal capacitados



Sistemas desactualizados



Software no licenciado

¿Qué es CVSS?

CVSS v2 Vector (AV:N/AC:L/Au:N/C:C/I:C/A:C)

- AV: Vector de Acceso, es decir, la manera a través de la cual podemos acceder a la vulnerabilidad. En nuestro caso para explotar la vulnerabilidad podemos acceder desde cualquier red, no sólo en local (N:Network).
- AC: Complejidad de Acceso, es decir, la complejidad que requiere el atacante una vez ha accedido al sistema, en nuestro caso complejidad baja (L: Low).
- Au: Autenticación, es decir, cuantas veces debe autenticarse el usuario para poder hacer uso de la vulnerabilidad, en nuestro caso ninguna (N:None).
- C: Impacto de Confidencialidad, es decir, como afecta esta vulnerabilidad en cuanto a la confidencialidad. En este caso el impacto es total, porque podemos ejecutar cualquier código en el sistema, lo que conlleva acceso a cualquier archivo, rompiendo de manera completa la confidencialidad del sistema (C: Complete).
- I: Impacto de Integridad, es decir, como afecta esta vulnerabilidad en cuanto a la integridad. Al igual que en el caso anterior, tenemos acceso completo a modificar cualquier archivo de tal forma que se rompe este principio completamente (C: Complete).
- A: Impacto a la Disponibilidad, más de lo mismo, si podemos ejecutar en el sistema cualquier comando podemos echar abajo servicios entre otras cosas. Por tanto afecta a la disponibilidad de manera completa (C: Complete)

Common Vulnerability Score System (CVSS) para calcular la severidad de una vulnerabilidad en los Sistemas de Información.



El concepto de CVE

Los puntos vulnerables y las exposiciones comunes (CVE) conforman una lista de las fallas de seguridad informática que está disponible al público. Cuando alguien habla de un CVE, se refiere a una falla a la cual se le asignó un número de identificación de CVE.

Ejemplo de Vulnerabilidad

Vulnerability Details : CVE-2023-46007

Sourcecodester Best Courier Management System 1.0 is vulnerable to SQL Injection via the parameter id in /edit_staff.php.

Vulnerability category: Sql Injection
Published 2023-10-18 13:15:10 Updated 2023-10-25 01:26:57 Source MITRE
View at [NVD](#), [CVE.org](#)

Exploit prediction scoring system (EPSS) score for CVE-2023-46007

Probability of exploitation activity in the next 30 days: 0.04%
Percentile, the proportion of vulnerabilities that are scored at or less: ~ 7 % [EPSS Score History](#) [EPSS FAQ](#)

CVSS scores for CVE-2023-46007

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	nvd@nist.gov

CWE ids for CVE-2023-46007

CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.
Assigned by: nvd@nist.gov (Primary)

Consultas de CVE

 CVEdetails.com
powered by SecurityScorecard

Vulnerabilities

By Date
By Type
Known Exploited
Assigners
CVSS Scores
EPSS Scores
Search

Vulnerable Software

Vendors
Products
Version Search
Vulnerability Intel. New
Newsfeed
Open Source Vulns New
Emerging CVEs
Feeds
Exploits
Advisories
Code Repositories
Code Changes

Attack Surface New
My Attack Surface
Digital Footprint
Discovered Products

Security Vulnerabilities CVSS score between 9 and 10

Published in:  2023 January February March April May June July August September October

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date ↗ ↘ Update Date ↗ ↘ CVE Number ↗ ↘ CVE Number ↗ ↘ CVSS Score ↗ ↘ EPSS Score ↗ ↘

38647 vulnerabilities found

  2 3 4 5 1543 1544 1545 1546

 Copy

CVE-2023-46117

reconFTW is a tool designed to perform automated recon on a target domain by running the best set of tools to perform scanning and finding out vulnerabilities. A vulnerability has been identified in reconftw where inadequate validation of retrieved subdomains may lead to a Remote Code Execution (RCE) attack. An attacker can exploit this vulnerability by crafting a malicious CSP entry on its own domain. Successful exploitation can lead to the execution of arbitrary code within the context of the application, potentially compromising the system. This issue has been

Max Base Score 

Published 2023-10-20

Updated 2023-10-21

EPSS 

CVE-2023-46042

An issue in GetSimpleCMS v.3.4.0a allows a remote attacker to execute arbitrary code via a crafted payload to the phpinfo().

Max Base Score 

Published 2023-10-19

Updated 2023-10-25

EPSS 

CVE-2023-46007

Sourcecodester Best Courier Management System 1.0 is vulnerable to SQL Injection via the parameter id in /edit_staff.php.

Max Base Score 

Published 2023-10-18

Updated 2023-10-25

EPSS 

<https://www.cvedetails.com>

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



5.2 Escaneo de Vulnerabilidades Automatizado



CEHPC™ Versión 022024

CertiProf®

Nessus

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos.

En operación normal, Nessus comienza escaneando los puertos con nmap o con su propio escáner de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins.

The screenshot shows the Nessus web interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Customized Reports, Scanners). The main area is titled 'Live Results Scan' and shows a table of vulnerabilities. The table has columns for 'Sev' (Severity), 'Name', 'Family', 'Count', and actions. A message box says: 'Notice: This scan has been updated with Live Results. Launch a new scan to confirm these findings or remove them.' To the right, there's a 'Scan Details' section with information like Name: Live Results Scan, Status: Completed, Policy: Advanced Scan, Scanner: Local Scanner, and Modified: Today at 6:03 PM (Live Results). Below that is a 'Vulnerabilities' chart.

Primera ventana de Nessus daremos clic en create a new scan.

The screenshot shows the Tenable Nessus Professional web interface. The left sidebar includes 'Folders' (My Scans, scan, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Customized Reports, Terrascan). The main area is titled 'My Scans' and displays a message: 'This folder is empty. Create a new scan.' There are buttons for 'Import', 'New Folder', and '+ New Scan'.

Seleccionamos Host Discovery y llenamos los datos que nos solicita Nessus.

The screenshot shows the Nessus interface. At the top, there's a 'DISCOVERY' section with a circular icon and the text 'Host Discovery: A simple scan to discover live hosts and open ports.' Below this, the main interface shows a configuration for a scan named 'juice'. The configuration includes fields for Name (juice), Description (empty), Folder (My Scans), and Targets (juice-shop.herokuapp.com). There are also buttons for Upload Targets and Add File.

Al realizar lo anterior tendremos la actividad creada le daremos play para iniciarla.

<input type="checkbox"/> Name	Schedule	Last Scanned
<input type="checkbox"/> juice	On Demand	⌚ Today at 1:02 PM

Nos mostrara los resultados del escaneo en este ejemplo vemos que solo tiene vulnerabilidades informativas.

Sev	CVSS	VPR	Name	Family	Count
INFO	Web Server (...)	Web Servers	4
INFO			Nessus SYN scann...	Port scanners	3
INFO			Service Detection	Service detection	3
INFO			HTTP Server Type ...	Web Servers	2
INFO			Host Fully Qualifie...	General	1
INFO			OS Identification F...	General	1

Host Details

- IP: 46.137.15.86
- DNS: juice-shop.herokuapp.com
- Start: Today at 12:52 PM

Vulnerabilities

OWASP ZAP

OWASP ZAP es una herramienta que ofrece una amplia gama de funcionalidades, incluyendo escaneos automáticos, pruebas manuales, intercepción y modificación de tráfico, y exploración y descubrimiento de vulnerabilidades. También cuenta con una GUI que permite a los usuarios interactuar con la herramienta de forma visual, así como una API que permite automatizar y personalizar las pruebas.

Tipos de detecciones

Risk:  High

Muy vulnerable

Risk:  Medium

Possiblemente vulnerable

Risk:  Low

Fue vulnerable en algún momento, pero fue corregido

Risk:  Informational

Alerta informativa solamente

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



5.3 Escaneo de Vulnerabilidades Manual



CEHPC™ Versión 022024

CertiProf®

Script vuln

Script cual permite identificar alguna de las vulnerabilidades más conocidas en el sistema.

Sudo nmap -f -sS -sV -Pn -script vuln

```
msf6 > nmap -sS -sV --script vuln 74.208.42.253
[*] exec: nmap -sS -sV --script vuln 74.208.42.253

Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-07 19:21 EDT
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 30.15% done; ETC: 19:23 (0:01:33 remaining)
Nmap scan report for 74.208.42.253
Host is up (0.031s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     ProFTPD
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2
.0)
80/tcp    open  http    nginx
| http-slowloris-check:
|   VULNERABLE:
|     Slowloris DOS attack
|       State: LIKELY VULNERABLE
|       IDs: CVE:CVE-2007-6750
|         Slowloris tries to keep many connections to the target web server open and
| hold
|   them open as long as possible. It accomplishes this by opening connection
| s to
|   the target web server and sending a partial request. By doing so, it starv
| es
|   the http server's resources causing Denial Of Service.
|       Disclosure date: 2009-09-17
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|         http://ha.ckers.org/slowloris/
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp   open  ssl
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: nginx
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

Script Auth

Script para detectar usuarios anónimos al igual muestra el listado usuarios con permisos de super usuario (acceso root).

Sudo nmap -f -sS -sV -Pn -script auth

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 12:27 -03
Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 12:28 (0:00:03 remaining)
Nmap scan report for 192.168.145.128 (192.168.145.128)
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-auth-methods:
```

Script Default

Script para realizar escaneo con los scripts predeterminados.

Sudo nmap -f -sS -sV -Pn -script default

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 12:33 -03
Nmap scan report for 192.168.145.128 (192.168.145.128)
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.145.1
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56cccd (DSA)
|   2048 5656240f211dde72bae61b1243de8f3 (RSA)
23/tcp    open  telnet        Linux telnetd
```

Script Safe

Script para ejecutar secuencias de comandos que son menos intrusivas para la víctima, de manera que será menos probable que provoquen la interrupción de algunas aplicaciones.

Sudo nmap -f -sS -sV -Pn -script safe

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:44 -03
Pre-scan script results:
| broadcast-listener:
|_ ether
|   ARP Request
|     sender ip      sender mac      target ip
|       192.168.1.1  4413d0ba5f2d  192.168.1.10
|       192.168.145.2 005056eba951  192.168.145.129
| udp
|   DHCP
|     srv ip          cli ip          mask          gw          dns          vendor
|       192.168.160.254 192.168.160.128 255.255.255.0  - 192.168.160.1  -
|       192.168.145.254 192.168.145.129 255.255.255.0 192.168.145.2 192.168.145.2  -
|       192.168.1.1    192.168.1.6    255.255.255.0 192.168.1.1 192.168.1.1  -
|_eap-info: please specify an interface with -e
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
| broadcast-dns-service-discovery:
```

ETHICAL HACKING PROFESSIONAL CERTIFICATION



6. Explotación



CEHPC™ Versión 022024

CertiProf®

ETHICAL HACKING PROFESSIONAL CERTIFICATION



6.1 Metasploit

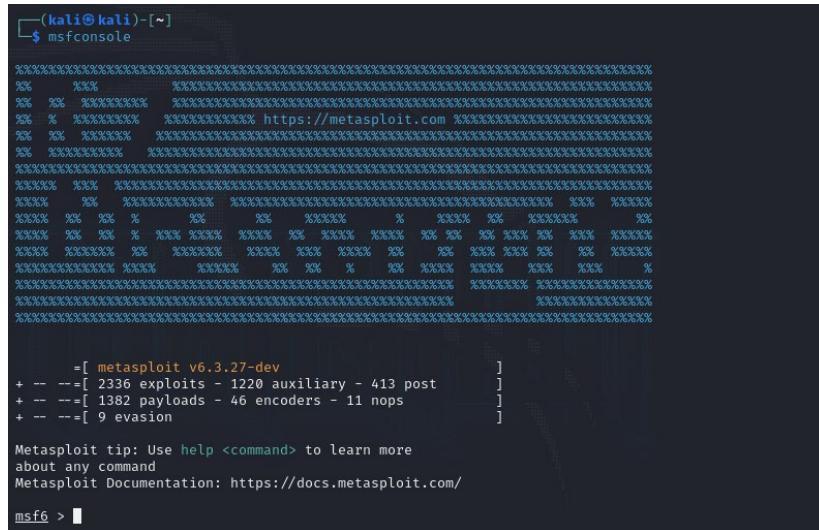


CEHPC™ Versión 022024

CertiProf®

METASPOIT

Es un marco de código abierto basado en Ruby que utilizan los profesionales de la seguridad de la información y los ciberdelincuentes para encontrar, explotar y validar las vulnerabilidades del sistema.



The screenshot shows a terminal window titled '(kali㉿kali)-[~]' running the 'msfconsole' command. The screen displays the Metasploit logo, which is a grid of 'x' characters. Below the logo, the version information 'metasploit v6.3.27-dev' is shown, along with statistics: '2336 exploits', '1220 auxiliary', '413 post', '1382 payloads', '46 encoders', '11 nops', and '9 evasion'. A tip at the bottom reads: 'Metasploit tip: Use help <command> to learn more about any command' and 'Metasploit Documentation: https://docs.metasploit.com/'. The prompt 'msf6 >' is visible at the bottom.

Los componentes más comunes de Metasploit incluyen:

- **Exploits:** Son módulos que toman ventaja de las vulnerabilidades en los sistemas. Los exploits son una de las características más importantes de Metasploit, ya que permiten a los usuarios explotar las vulnerabilidades.
- **Payloads:** Son los comandos o programas que se ejecutan en los sistemas después de que se ha explotado la vulnerabilidad.
- Los payloads pueden ser personalizados para satisfacer los objetivos específicos de los usuarios.
- **Encoders:** Son módulos que se utilizan para ofuscar o cifrar payloads para evitar la detección por parte de soluciones de seguridad.
- **Auxiliary:** Son módulos adicionales que proporcionan herramientas para tareas específicas de hacking, como la recopilación de información del sistema o la enumeración de contraseñas.

Comandos Básicos

Search: Se utiliza para buscar cualquier información almacenada en los módulos previamente mencionados, se pueden hacer búsquedas por CVE, por nombre del servicio, por tipo de exploit, etc.

```
[*] http://ethihack.com/vanhauser-thc/thc-hydra [!] Finished at: 2023-05-26 20:13:17  
[*] http://192.168.192.128:21 [!] login user: password: user [!] Exploit completed, 1 valid password found  
[*] http://ethihack.com/vanhauser-thc/thc-hydra [!] Finished at: 2023-05-26 20:13:58  
Metasploit tip: Enable HTTP request and response logging with set HttpTrace true  
msf6 > search vsftpd  
[*] http://192.168.192.128:21 [!] login user: password: user [!] Exploit completed, 1 valid password found  
Matching Modules  
===== /thc-hydra  
# Name Disclosure Date Rank Check Description  
- - - -  
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor  
Command Execution
```

Use: se utiliza para cargar un módulo específico en Metasploit.

```
[*] http://ethihack.com/vanhauser-thc/thc-hydra [!] Finished at: 2023-05-26 20:13:17  
[*] http://192.168.192.128:21 [!] login user: password: user [!] Exploit completed, 1 valid password found  
[*] http://ethihack.com/vanhauser-thc/thc-hydra [!] Finished at: 2023-05-26 20:13:58  
Metasploit tip: View missing module options with show missing  
[*] No payload configured, defaulting to cmd/unix/interact  
[*] No exploit module selected, setting exploit/unix/ftp/vsftpd_234_backdoor  
[*] No session selected, setting session 1  
[*] No post module selected, defaulting to post/unix/generic/reverse_tcp  
[*] No handler module selected, defaulting to handler/multi/handler  
[*] No exploit module selected, defaulting to exploit/unix/ftp/vsftpd_234_backdoor  
[*] No session selected, setting session 1  
[*] No post module selected, defaulting to post/unix/generic/reverse_tcp  
[*] No handler module selected, defaulting to handler/multi/handler  
[*] Exploit module exploit/unix/ftp/vsftpd_234_backdoor selected  
[*] Session 1 selected  
[*] Post module post/unix/generic/reverse_tcp selected  
[*] Handler module handler/multi/handler selected  
[*] Exploit module exploit/unix/ftp/vsftpd_234_backdoor selected  
[*] Session 1 selected  
[*] Post module post/unix/generic/reverse_tcp selected  
[*] Handler module handler/multi/handler selected
```

Show: options: se utiliza para mostrar una lista de todas las opciones requeridas y configurables para el módulo en uso, junto con una breve descripción de cada opción. También muestra el valor actual de cada opción si ya ha sido establecido.

Help: se utiliza para obtener ayuda sintáctica o sobre cómo utilizar un módulo.

```
msf6 auxiliary(scanner/http/apache_userdir_enum) > help
Core Commands

```

Command	Description
?	Help menu
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
debug	Display information useful for debugging
exit	Exit the console
features	Display the list of not yet released features that can be opted in to
get	Gets the value of a context-specific variable
getg	Gets the value of a global variable
grep	Grep the output of another command
help	Help menu
history	Show command history
load	Load a framework plugin
quit	Exit the console

Set: Se utiliza para establecer los valores de las opciones requeridas para el módulo.

Por ejemplo:

set TARGET: permite seleccionar el sistema operativo/aplicación de la víctima.

set RHOST: permite configurar la dirección IP del host de destino

set LHOST: permite configurar la dirección IP del host local.

set PAYLOAD: permite configurar la carga útil.

```

      =[ metasploit v6.1.27-dev
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post      ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops      ]
+ -- --=[ 9 evasion      ]

Metasploit tip: View missing module options with show
missing

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.192.128
RHOSTS => 192.168.192.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

```

Búsqueda de sploit

/usr/share/exploitdb

/usr/share/metasploit-framework/

The screenshot shows a terminal window titled 'kali@kali: ~'. The user has run the command '\$ searchsploit Microsoft IIS 6.0'. The results are displayed in two columns: 'Exploit Title' and 'Path'. The 'Exploit Title' column lists various Microsoft IIS 6.0 vulnerabilities, and the 'Path' column lists the corresponding exploit files in the searchsploit database.

Exploit Title	Path
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network	windows/remote/21057.txt
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack	windows/remote/9541.pl
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service	windows/dos/9587.txt
Microsoft IIS 6.0 - '/AUX / '.aspx' Remote Denial of Service	windows/dos/3965.pl
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial	windows/dos/15167.txt
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer	windows/remote/41738.py
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass	windows/remote/8765.php
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)	windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)	windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)	windows/remote/8754.patch
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities	windows/remote/19033.txt

Laboratorio de Explotación Coffe Dicts

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



7. Técnicas de Ataque



CEHPC™ Versión 022024

CertiProf®

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



7.1 Tipos de Ataque



CEHPC™ Versión 022024

CertiProf®

Malware

- “Software malicioso” es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.
- El malware hostil, intrusivo e intencionadamente desagradable intenta invadir, dañar o deshabilitar ordenadores, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo asumiendo el control parcial de las operaciones de un dispositivo. Al igual que la gripe, interfiere en el funcionamiento normal.



Spoofing

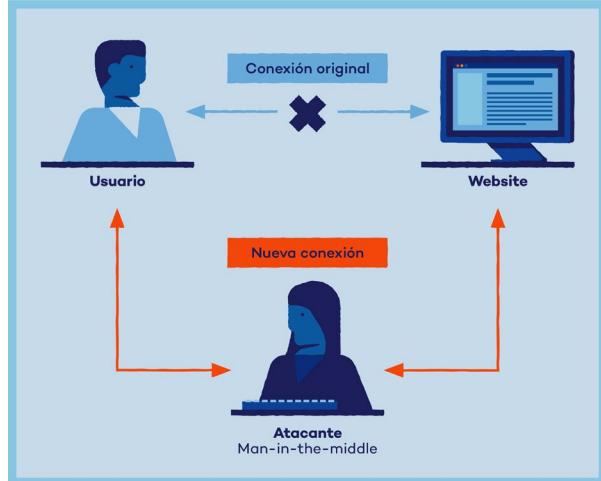
El spoofing consiste en usurpar una identidad electrónica para ocultar la propia identidad y así cometer delitos en Internet. Existen 3 tipos: spoofing de correo electrónico, spoofing de IP y smart-spoofing IP.



- **Correo electrónico falsificado:** Los correos electrónicos que contienen un virus informático se envían desde direcciones de correo electrónico existentes, con el fin de engañar mejor al destinatario. De este modo, este último propagará involuntariamente el virus cuando se abra el correo. El hacker puede entonces extraer datos personales o incluso controlar remotamente el ordenador.
- **El spoofing IP:** Es el proceso de envío de paquetes IP desde una dirección IP de origen que no ha sido asignada al ordenador que los envía.
- **Smart-spoofing:** permite utilizar cualquier aplicación cliente gracias a la usurpación de una dirección IP. Esto evita las reglas de seguridad de la red. Esta técnica, si se combina con la traducción de direcciones, puede incluso neutralizar los cortafuegos.

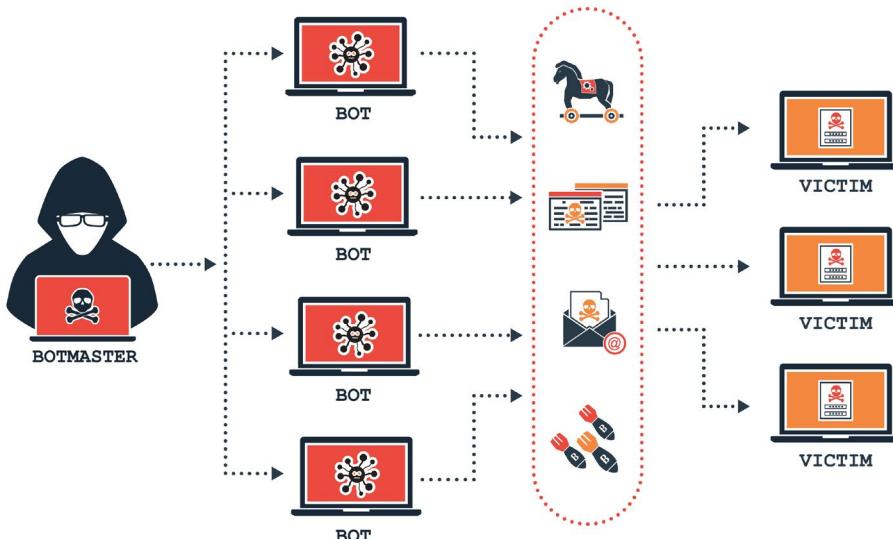
Man-in-the-middle (MITM)

Un ataque MITM ocurre cuando una comunicación entre dos sistemas es interceptada por una entidad externa. Esto puede suceder en cualquier forma de comunicación en línea como correo electrónico, redes sociales, navegación web, etc. No solo están tratando de escuchar nuestras conversaciones privadas, si no también puede dirigir toda la información dentro de los dispositivos.



Denegación de servicio distribuido (Ddos)

- Un ataque de denegación de servicio tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado.
- Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática.
- Los servidores web poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, el servidor comienza a ralentizarse o incluso puede llegar a no ofrecer respuesta a las peticiones o directamente bloquearse y desconectarse de la red.



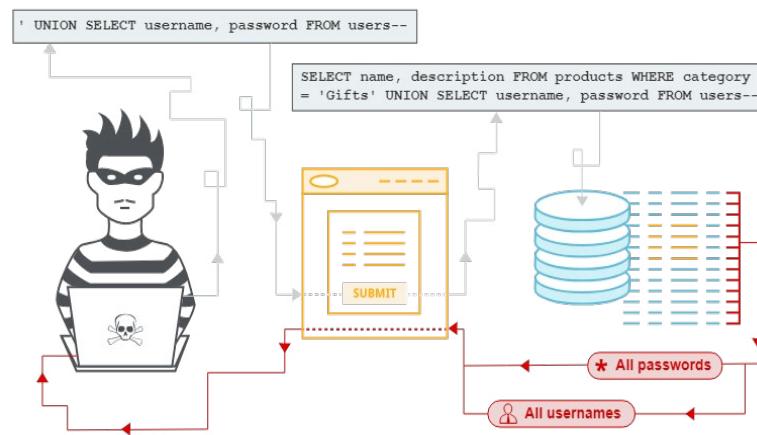
PiggyBacking

- Es utilizar una conexión inalámbrica para acceder a una conexión a Internet sin autorización. Su objetivo es obtener un acceso libre a la red que a menudo se aprovecha para intentar actividades maliciosas como la violación de datos y la difusión de malware. También puede provocar una disminución de la velocidad de Internet para todos los sistemas conectados a la red.
- Los ataques "piggybacking" eran más fáciles y comunes en el pasado porque las redes Wi-Fi no estaban encriptadas.



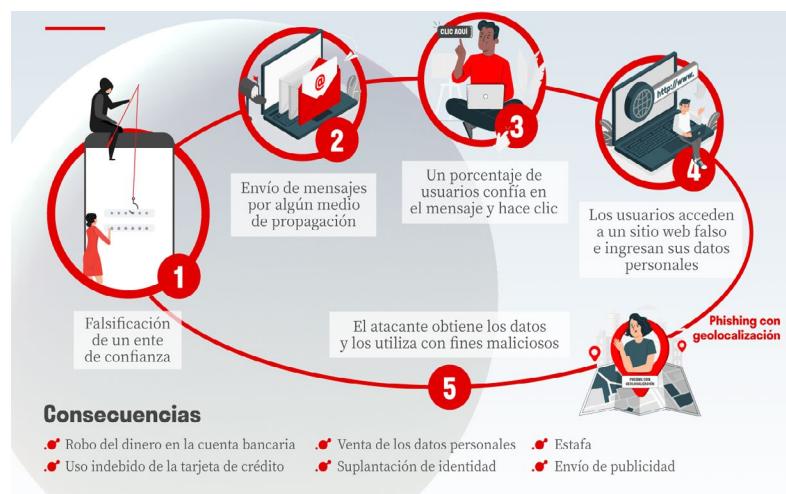
Inyección de Código SQL

- SQL Injection es una falla en la codificación de una aplicación cualquiera (web o local) que posibilita por medio de un input cualquiera, la manipulación de una consulta SQL. Esta manipulación se denomina inyección, por lo que el término de inyección de SQL.
- Es una técnica de ataque basada en la manipulación del código SQL, que es el lenguaje utilizado para el intercambio de información entre aplicaciones y bases de datos relacionales.
- Es un tipo de ataque donde el “Hacker” puede insertar comandos maliciosos (sql querys) en la base de datos a través de los campos de formularios o de URL de una aplicación vulnerable, ambicionando extraer información guardada en la base de datos.



Phishing

El phishing es una forma de ingeniería social en la que los atacantes engañan a las personas para que revelen información confidencial o instalen malware como ransomware.



ETHICAL HACKING PROFESSIONAL CERTIFICATION



8. Informe de Resultados



CEHPC™ Versión 022024

CertiProf®

ETHICAL HACKING

PROFESSIONAL CERTIFICATION



8.1 Tipos de Informes



CEHPC™ Versión 022024

CertiProf®

Tipos de Informes

El propósito completo de las pruebas de intrusión es identificar vulnerabilidades y problemas de seguridad que el cliente deba remediar, y estas se comunican a través del reporte, que es el único producto tangible de las pruebas. Un buen reporte proporciona un resumen ejecutivo de los hallazgos, resume las vulnerabilidades y su impacto en el negocio y proporciona recomendaciones para corregirlas. Los pentesters utilizan un enfoque metódico y documentan su metodología como parte del informe para brindar solidez a las pruebas.

En general, el informe se puede dividir en dos secciones principales para comunicar los objetivos, métodos y resultados de las pruebas realizadas a diferentes audiencias:

- Resumen ejecutivo
- Resumen Técnico

El informe de resultados tiene por objetivo transmitir los resultados de las pruebas de intrusión a niveles estratégicos, tácticos y operativos se divide sus entregables 2 rubros.

El reporte ejecutivo tiene la finalidad de ofrecer un resumen para los niveles ejecutivos , ofreciendo un entendimiento en términos no técnicos de las pruebas ejecutadas y los hallazgos descubiertos durante la revisión técnica en términos de riesgo.

El reporte técnico va dirigido hacia las áreas tácticas y operativas involucradas. Tiene por objetivo reflejar el detalle de las pruebas realizadas, las herramientas utilizadas, los resultados obtenidos, así como recomendaciones de la mitigación d las vulnerabilidades.



ETHICAL HACKING

PROFESSIONAL CERTIFICATION



8.2 Presentación de Resultados

Ejemplo de Presentación de Resultados



CEHPC™ Versión 022024

CertiProf®



ETHICAL HACKING PROFESSIONAL CERTIFICATION

¡Síguenos, contáctanos!



www.certiprof.com

CERTIPROF® is a registered trademark of CertiProf,
LLC in the United States and/or other countries.

CertiProf®