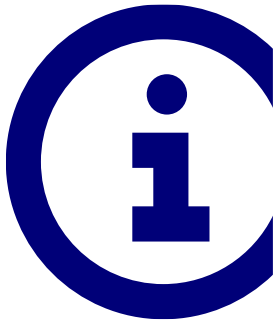
Realización de test de intrusión en sistemas informáticos

Sergio Góngora Benítez

Área: Administración de redes y sistemas operativos

Universitat Oberta de Catalunya

Índice

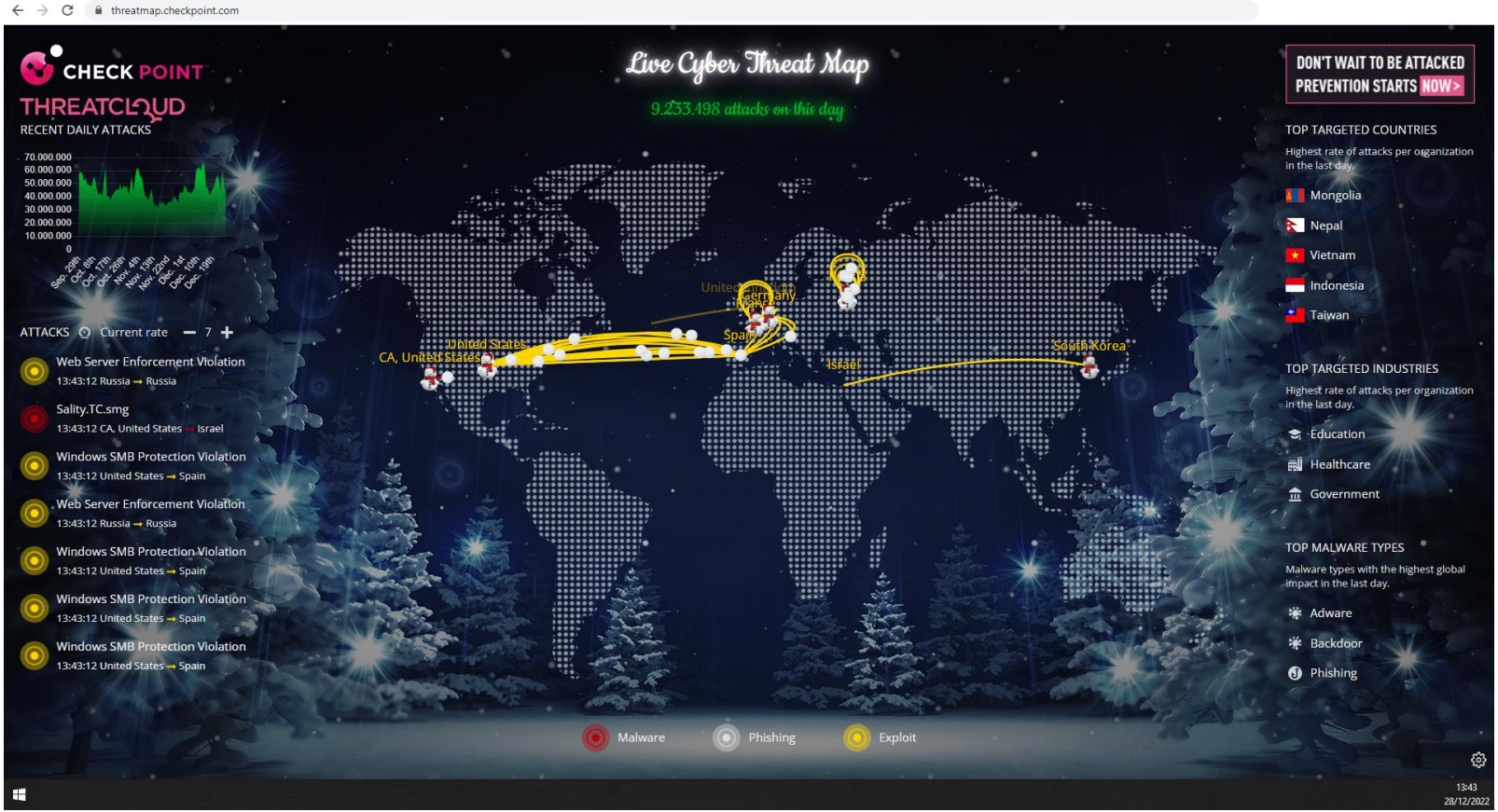


Introducción

Contexto, Objetivos,
Metodología y Planificación

01

Contexto (I)


threatmap.checkpoint.com
CHECK POINT
THREATCLOUD
RECENT DAILY ATTACKS
70.000.000
60.000.000
50.000.000
40.000.000
30.000.000
20.000.000
10.000.000
0
Sep. 29th
Oct. 8th
Oct. 17th
Oct. 26th
Nov. 4th
Nov. 13th
Nov. 22nd
Dec. 1st
Dec. 10th
Dec. 19th
Live Cyber Threat Map
9,233,498 attacks on this day
DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW>
ATTACKS
Current rate
7
Web Server Enforcement Violation
13:43:12 Russia → Russia
Sality.TC.smg
13:43:12 CA, United States → Israel
Windows SMB Protection Violation
13:43:12 United States → Spain
Web Server Enforcement Violation
13:43:12 Russia → Russia
Windows SMB Protection Violation
13:43:12 United States → Spain
Windows SMB Protection Violation
13:43:12 United States → Spain
Windows SMB Protection Violation
13:43:12 United States → Spain
United States
CA, United States
Germany
Spain
Israel
South Korea
TOP TARGETED COUNTRIES
Highest rate of attacks per organization in the last day.
Mongolia
Nepal
Vietnam
Indonesia
Taiwan
TOP TARGETED INDUSTRIES
Highest rate of attacks per organization in the last day.
Education
Healthcare
Government
TOP MALWARE TYPES
Malware types with the highest global impact in the last day.
Adware
Backdoor
Phishing
Malware
Phishing
Exploit
13:43
28/12/2022

Contexto (II)

Ranking UIT 2020:

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5

INCIBE:

Balance de 109.126 incidentes de ciberseguridad registrados durante 2021:

- ✓ 90.168 corresponden a ciudadanos y a empresas
- ✓ 680 a operadores estratégicos
- ✓ 18.278 a la red académica y de investigación española

Objetivos

Concienciación

Dar visibilidad a la exposición de los sistemas informáticos a ser vulnerados y la importancia de disponer entornos seguros.

Vulnerabilidades

Enumerar las vulnerabilidades más comunes y dar a conocer el repositorio dónde se encuentran ubicadas.

Metodologías

Enumerar las metodologías que se pueden llevar a cabo para ejecutar un *pentesting*.

Test de intrusión

Exposición de las diferentes fases de la ejecución de un *pentesting* a un sistema informático.

Best practices

Proporcionar un seguido de buenas prácticas para dotar de mayor seguridad a las infraestructuras.

Metodología

Sin conocimiento alguno del sistema objetivo.

Metodología adecuada para emular un ataque externo.

Conocimiento parcial de la infraestructura y sistemas que lo componen.

Metodología adecuada para usuarios.

Conocimiento total de la infraestructura.

Metodología útil para desarrolladores.

Planificación (I)

Desarrollo del TFG en 4 fases:

Propuesta

- ✓ Título
- ✓ Motivación
- ✓ Descripción
- ✓ Objetivos
- ✓ Viabilidad
- ✓ Gantt

Introducción

- ✓ Contexto
- ✓ Objetivos
- ✓ Metodología
- ✓ Planificación
- ✓ Sumario de productos
- ✓ Capítulos

Parte teórica

- ✓ Definición de *penstesting*
- ✓ Vulnerabilidades
- ✓ Herramientas comunes de *pentesting*

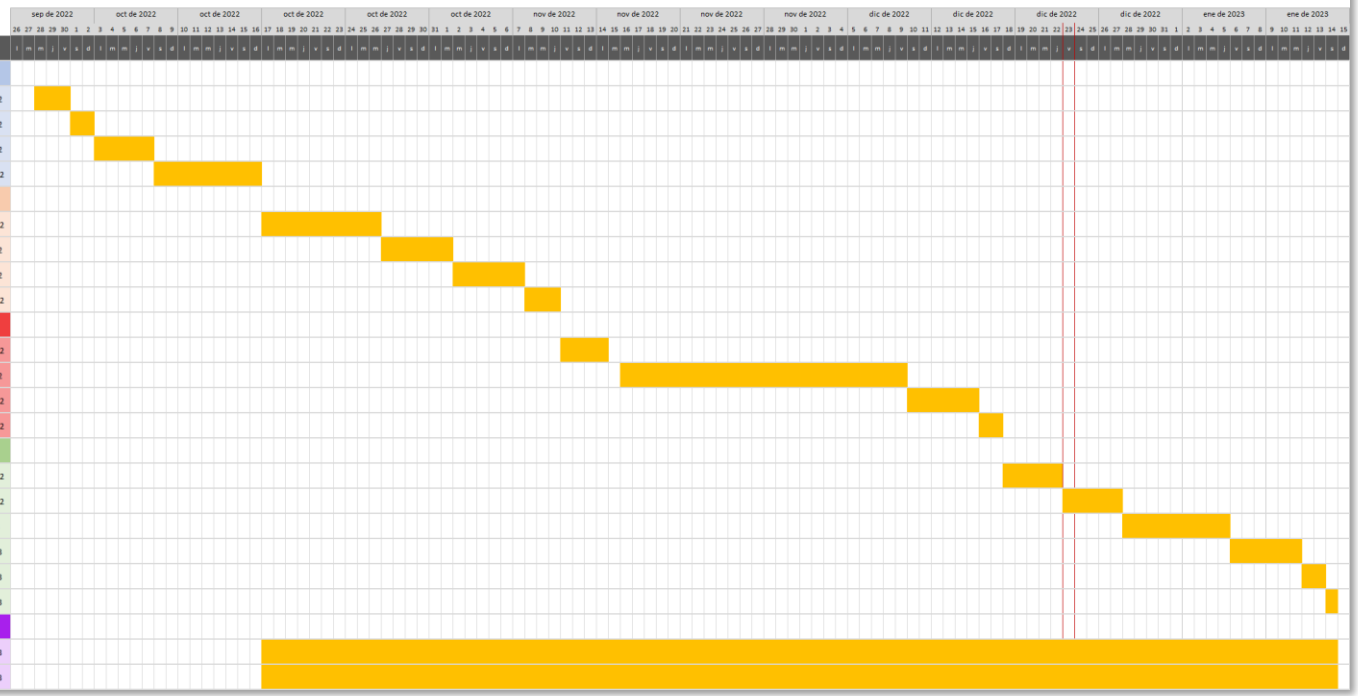
Parte práctica

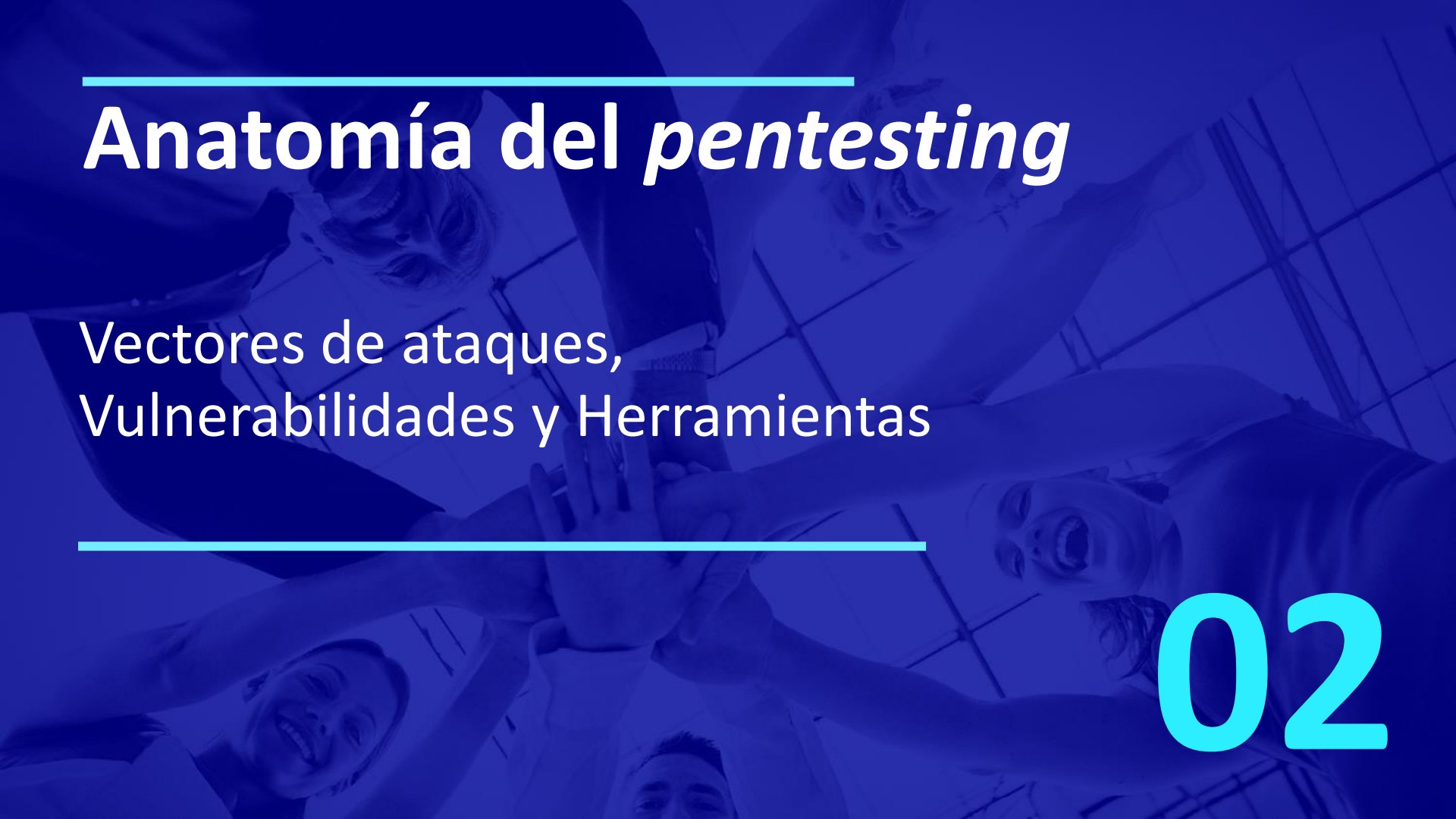
- ✓ Reconocimiento de red
- ✓ Análisis de vulnerabilidades
- ✓ Exploiting
- ✓ Post-Exploiting
- ✓ Informe final
- ✓ *Best practices*

Planificación (II)

TFG: Realización de test de intrusión en sistemas informáticos

TAREA	PAC	PROGRESO		INICIO	FIN
Propuesta TFG					
Estudio y viabilidad de TFG y comunicación al tutor	PEC1	0%	3 días	28-9-22	30-9-22
Propuesta de título	PEC1	0%	2 días	1-10-22	2-10-22
Introducción y descripción del proyecto	PEC1	0%	5 días	3-10-22	7-10-22
Elaboración plan de trabajo	PEC1	0%	9 días	8-10-22	16-10-22
Parte teórica					
Contexto y justificación del trabajo	PEC2	0%	10 días	17-10-22	26-10-22
Objetivos y alcance	PEC2	0%	6 días	27-10-22	1-11-22
Enfoque y metología seguida	PEC2	0%	6 días	2-11-22	7-11-22
Sumario de productos y capítulos	PEC2	0%	3 días	8-11-22	10-11-22
Parte práctica					
Preparación entorno	PEC2	0%	4 días	11-11-22	14-11-22
Ejecución test de intrusión en sistema informático	PEC3	0%	24 días	16-11-22	9-12-22
Documentación proceso y resultados obtenidos	PEC3	0%	6 días	10-12-22	15-12-22
Recomendaciones post intrusión	PEC3	0%	2 días	16-12-22	17-12-22
Cumplimentación memoria					
Abstract	PEC4	0%	5 días	18-12-22	22-12-22
Conclusiones	PEC4	0%	5 días	23-12-22	27-12-22
Redacción y maquetación final memoria	PEC4	0%	9 días	28-12-22	5-1-23
Presentación powerpoint	PEC4	0%	6 días	6-1-23	11-1-23
Vídeo presentación	PEC4	0%	2 días	12-1-23	13-1-23
Autoevaluación	PEC4	0%	2 días	14-1-23	15-1-23
Trabajo transversal					
Glosario	PEC4	0%	91 días	17-10-22	15-1-23
Bibliografía	PEC4	0%	91 días	17-10-22	15-1-23





Anatomía del *pentesting*

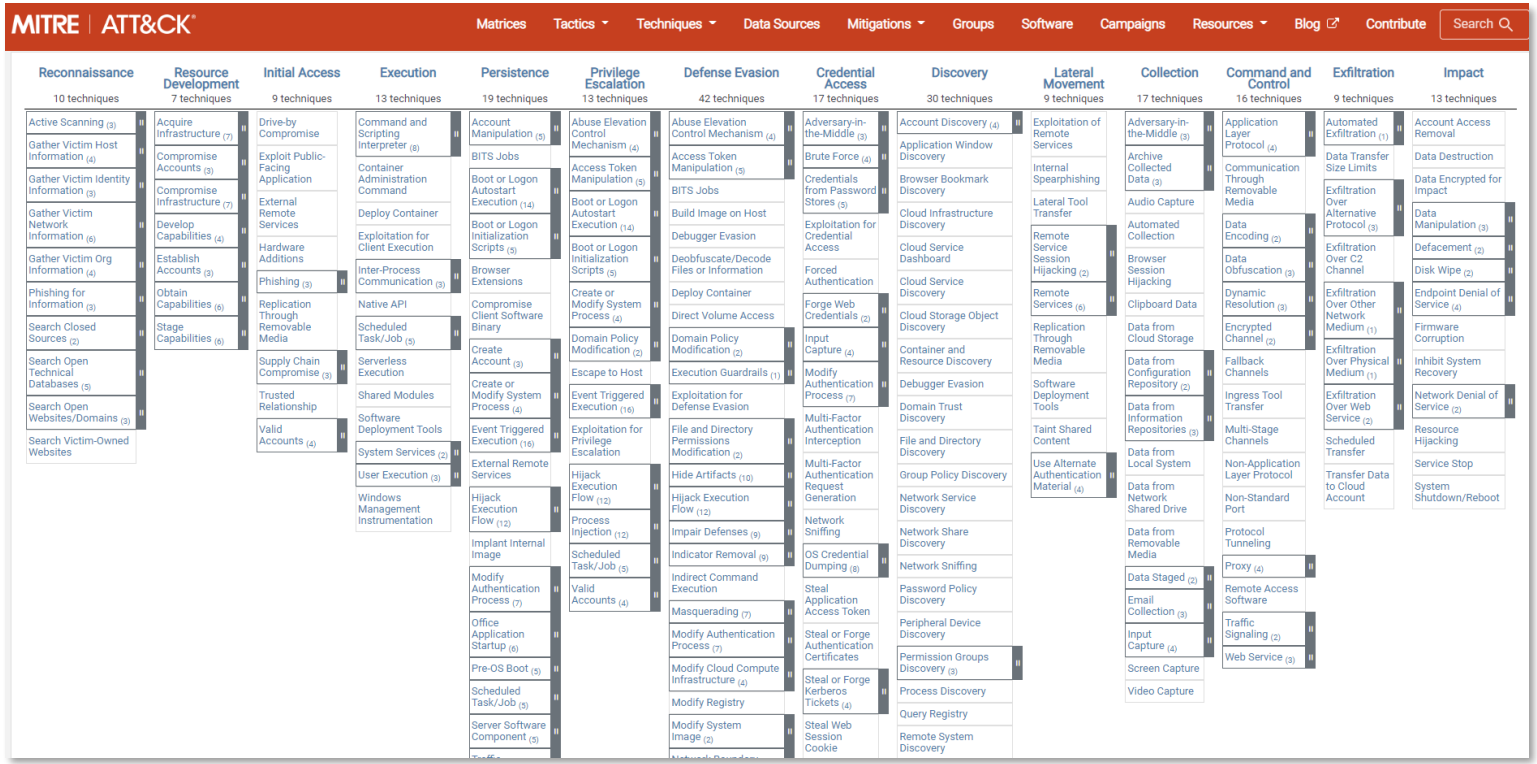
Vectores de ataques,
Vulnerabilidades y Herramientas

02

Anatomía del *pentesting*

Fases que conforman un test de intrusión:

Vectores de ataque (I)



✓ 14 tácticas

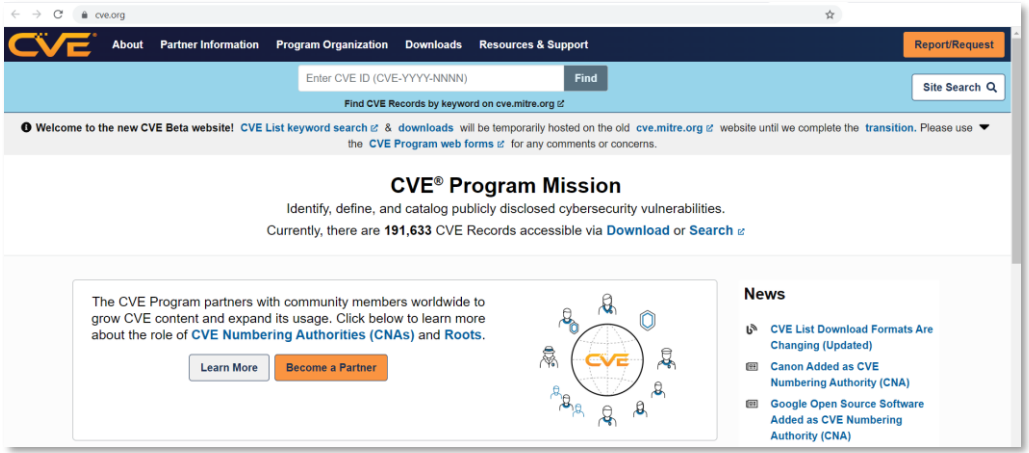
✓ 224 técnicas

Vectores de ataque (II)

Vulnerabilidades

Repositorio CVEs:

- https://www.cve.org/



Repositorio de fabricantes:

- **Cisco** → https://sec.cloudapps.cisco.com/security/center/publicationListing.x
- **Palo Alto** → https://security.paloaltonetworks.com/?sort=-date
- **F5** → https://support.f5.com/csp/article/K14649763#exposure
- **Microsoft** → https://msrc.microsoft.com/update-guide/vulnerability

Herramientas de *pentesting* (I)

Kali Linux

Distribución Linux, basada en Debian, con herramientas de *pentesting* precargadas para auditar sistemas.

HACKTHEBOX

Hack the box

Plataforma pública con sistemas informáticos virtualizados vulnerables para desarrollar *pentesting.*

Herramientas de *pentesting* (II)

Nmap

Escaneador de red, puertos y servicios

Wappalyzer

Analizador/descubridor de tecnologías en aplicaciones web

WPScan

Auditor de vulnerabilidades en frontales web WordPress

John the Ripper

Crackeador de *passwords* por fuerza bruta

Test de intrusión

Reconocimiento, Análisis de vulnerabilidades, Exploiting, Post-Exploiting e Informe final

03

Reconocimiento

Es la primera fase del *pentesting* en la cuál se recopilarán datos del sistema objetivo para analizar posibles vulnerabilidades y tratar de explotarlas.

Uso de…:

- Nmap
- Wappalyzer
- WPScan

Análisis de vulnerabilidades

En la segunda fase se analizan las posibles vulnerabilidades que puedan existir en los servicios ejecutándose en los puertos abiertos detectados durante el reconocimiento.

Uso de…:

- Metasploit
- Repositorio vulnerabilidades de WPScan

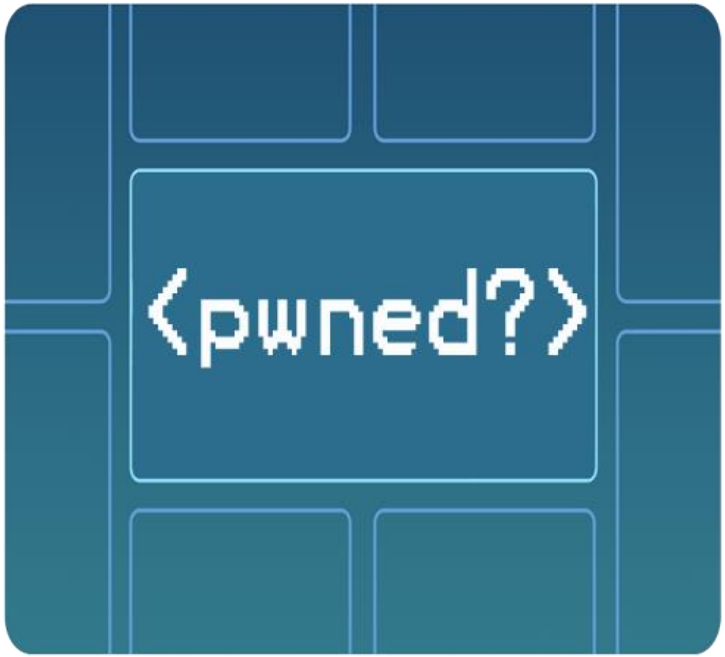
Exploiting

Se inicia la fase de vulneración del sistema objetivo, dónde se comienzan a realizar pruebas para lograr el acceso a éste.

Uso de…:

- WPScan
- Python3
- Base64 decoder
- Ftp
- Ssh

CVE-2021-29447: Vulnerabilidad XXE WordPress



Post-exploiting

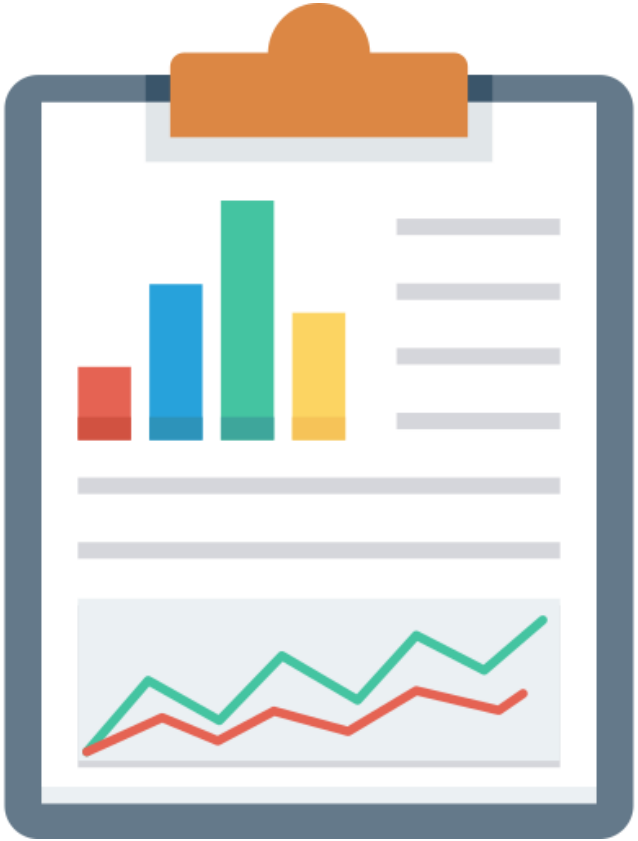
Una vez accedido al sistema objetivo, en esta fase comienza la escalada de privilegios para tratar de conseguir ser administrador del sistema vulnerado.

Uso de…:

- Gpg2john
- John
- PGP decryption

Informe final

La última fase consiste en elaborar un informe dónde se recogen las evidencias encontradas durante el desarrollo del test de intrusión, además de una conclusión y una mitigación de las vulnerabilidades.



Best practices

Acceso

- ✓ Contraseñas fuertes
- ✓ Establecimiento de MFA

Seguridad

- ✓ Segmentación y microsegmentación de red
- ✓ Aislamiento de entornos
- ✓ Auditorias *white box* recurrentes

Monitoreo

- ✓ Revisión de permisos
- ✓ CMDB actualizada
- ✓ NIDS, Syslog & SIEM

Continuidad de negocio

- ✓ Disaster Recovery Plan
- ✓ *Sandboxing*

Concienciación

- ✓ Formación en ingeniería social (*phishing, smishing y vishing*)
- ✓ *Workshops* de ciberseguridad

Conclusiones

Conclusiones

04

Conclusiones

- ✓ Gracias a la planificación llevada a acabo, el objetivo planteado se ha conseguido: vulnerar un sistema informático.
- ✓ Establecer correctamente el orden de las distintas fases de un *pentesting*, exponiendo qué acciones llevar a cabo en cada una de ellas, es de vital importancia.
- ✓ Concienciación de la criticidad de tener una infraestructura segura y robusta para evitar posibles brechas de seguridad.

¡Gracias!