

Realización de test de intrusión en sistemas informáticos

Sergio Góngora Benítez

Área: Administración de redes y sistemas operativos

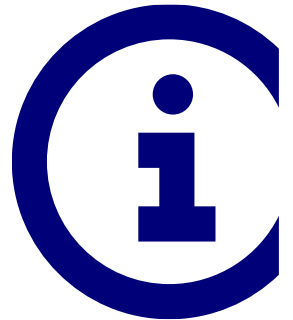


Universitat
Oberta
de Catalunya



Índice

- 01** Introducción
- 02** Anatomía del Pentesting
- 03** Test de intrusión
- 04** Conclusiones



Introducción

Contexto, Objetivos,
Metodología y Planificación

01

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 seguimiento de buenas prácticas para dotar de mayor seguridad a las infraestructuras.

Metodología

BLACK BOX



Sin conocimiento alguno del sistema objetivo.

Metodología adecuada para emular un ataque externo.

GRAY BOX



Conocimiento parcial de la infraestructura y sistemas que lo componen.

Metodología adecuada para usuarios.

WHITE BOX



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



Anatomía del *pentesting*

Vectores de ataques,
Vulnerabilidades y Herramientas

02

Anatomía del *pentesting*

Fases que conforman un test de intrusión:



Vectores de ataque (I)

MITRE ATT&CK													
Matrices Tactics Techniques Data Sources Mitigations Groups Software Campaigns Resources Blog Contribute Search													
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Remote Service Session Hijacking (2)	Data Encrypted for Impact	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Services (6)	Automated Collection	Browser Session Hijacking	Exfiltration Over Alternative Protocol (3)	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Browser Extensions	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Replication Through Removable Media	Data Encoding (2)	Clipboard Data	Defacement (2)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Compromise Client Software Binary	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Software Deployment Tools	Dynamic Obfuscation (3)	Remote Services (6)	Disk Wipe (2)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (6)	Serverless Execution	Scheduled Task/Job (5)	Create or Modify System Process (4)	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Taint Shared Content	Encrypted Channel (2)	Use Alternate Authentication Material (4)	Endpoint Denial of Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Supply Chain Compromise (3)	Trusted Relationship	Shared Modules	Domain Policy Modification (2)	Domain Policy Modification (2)	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Multi-Factor Authentication Interception	Data from Cloud Storage	Software Deployment Tools	Firmware Corruption	Firmware Corruption
Search Open Websites/Domains (3)	Valid Accounts (4)	Software Deployment Tools	System Services (2)	Event Triggered Execution (16)	Event Triggered Execution (16)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Debugging Evasion	File and Directory Permissions Modification (2)	Fallback Channels	Software Deployment Tools	Inhibit System Recovery	Inhibit System Recovery
Search Victim-Owned Websites	Windows Management Instrumentation	User Execution (3)	External Remote Services	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Escape to Host	Network Sniffing	Domain Trust Discovery	File and Directory Permissions Modification (2)	Ingress Tool Transfer	Use Alternate Authentication Material (4)	Network Denial of Service (2)	Network Denial of Service (2)
	Implant Internal Image	Process Injection (12)	Implant Internal Image	Scheduled Task/Job (5)	Scheduled Task/Job (5)	Exploitation for Privilege Escalation	OS Credential Dumping (8)	File and Directory Discovery	Hide Artifacts (10)	Non-Application Layer Protocol	Use Alternate Authentication Material (4)	Resource Hijacking	Resource Hijacking
	Modify Authentication Process (7)	Indicator Removal (9)	Indicator Removal (9)	Indirect Command Execution	Indirect Command Execution	Exploitation for Privilege Escalation	OS Credential Dumping (8)	File and Directory Discovery	Hijack Execution Flow (12)	Non-Standard Port	Use Alternate Authentication Material (4)	Scheduled Transfer	Scheduled Transfer
	Office Application Startup (6)	Masquerading (7)	Masquerading (7)	Masquerading (7)	Masquerading (7)	Exploitation for Privilege Escalation	OS Credential Dumping (8)	File and Directory Discovery	Process Injection (12)	Protocol Tunneling	Use Alternate Authentication Material (4)	System Shutdown/Reboot	System Shutdown/Reboot
	Pre-OS Boot (5)	Modify Authentication Process (7)	Modify Authentication Process (7)	Modify Authentication Process (7)	Modify Authentication Process (7)	Exploitation for Privilege Escalation	OS Credential Dumping (8)	File and Directory Discovery	Scheduled Task/Job (5)	Proxy (4)	Use Alternate Authentication Material (4)	Transfer Data to Cloud Account	Transfer Data to Cloud Account
	Scheduled Task/Job (5)	Modify Cloud Compute Infrastructure (4)	Modify Cloud Compute Infrastructure (4)	Modify Cloud Compute Infrastructure (4)	Modify Cloud Compute Infrastructure (4)	Exploitation for Privilege Escalation	OS Credential Dumping (8)	File and Directory Discovery	Server Software Component (5)	Remote Access Software	Use Alternate Authentication Material (4)	Traffic Signaling (2)	Traffic Signaling (2)
	Server Software Component (5)	Modify Registry	Modify Registry	Modify Registry	Modify Registry	Exploitation for Privilege Escalation	OS Credential Dumping (8)	File and Directory Discovery	System Shutdown/Reboot	Web Service (3)	Use Alternate Authentication Material (4)	Video Capture	Video Capture

✓ 14 tácticas

✓ 224 técnicas

Vectores de ataque (II)

Correo electrónico y mensajería instantánea

Insiders

Software mal configurado o desactualizado

Navegación web

Contraseñas débiles

Credenciales comprometidas

Acceso por terceros

Aplicaciones web, portales corporativos, intranets y RRSS

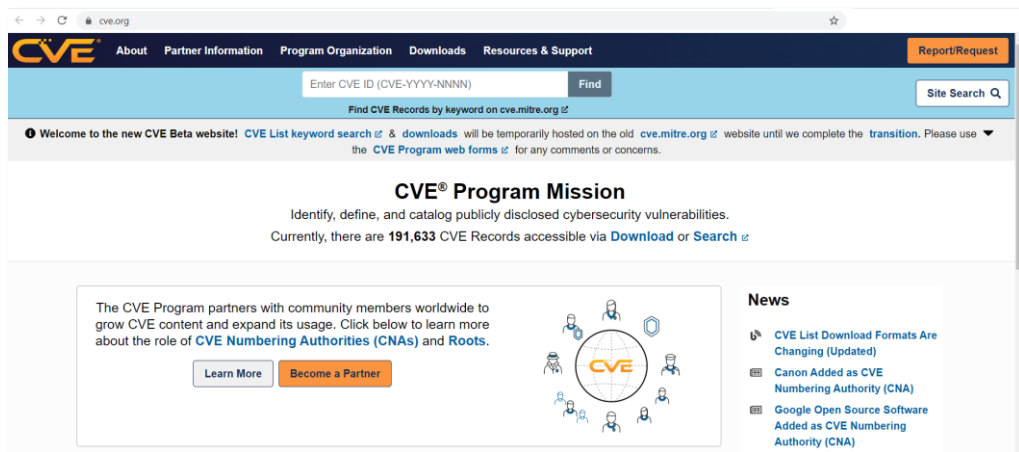
Endpoints

Carencias de cifrado

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

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

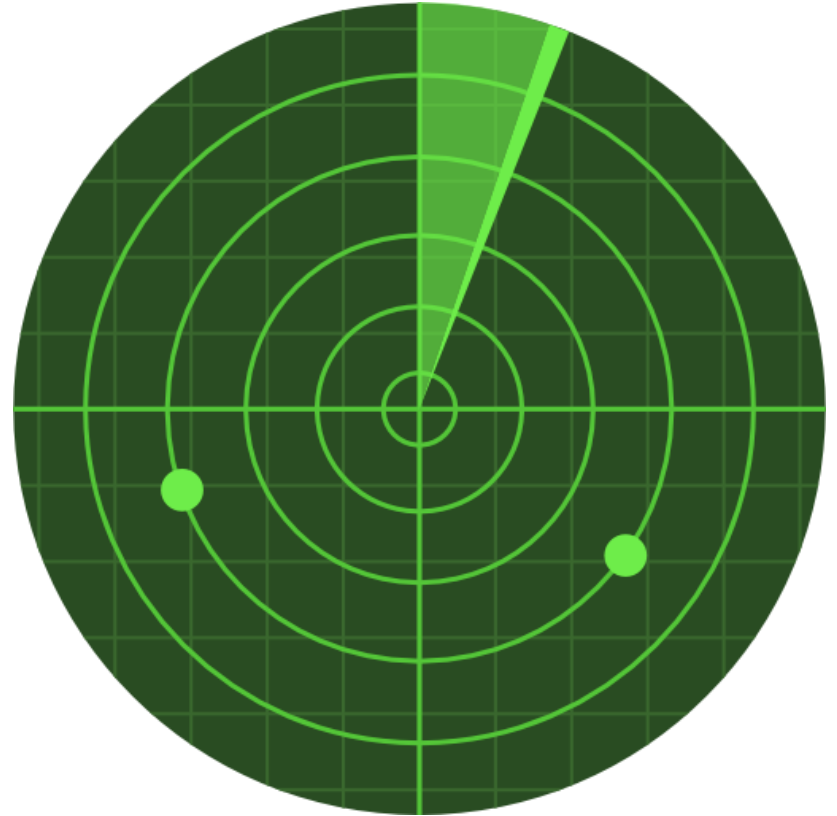
03

Reconocimiento

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

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



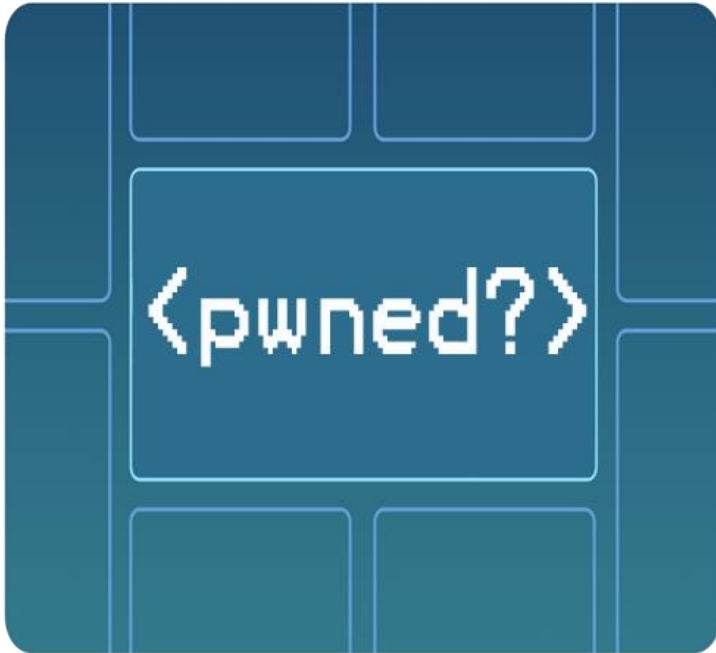
CVE-2021-29447: Vulnerabilidad XXE WordPress

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.

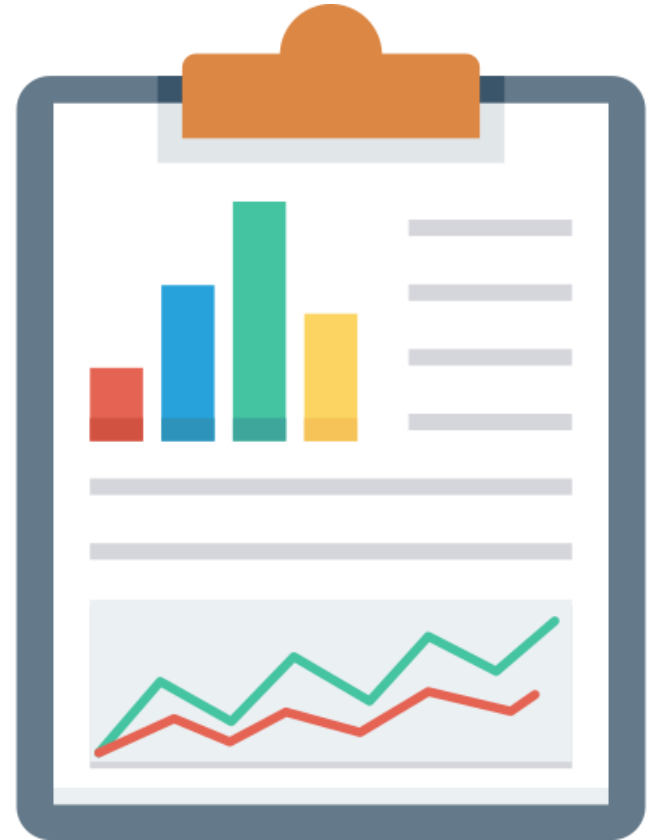
Uso de...:

- 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 cabo, 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!

