Hacking Ético:
Cacería de Vulnerabilidades

OWASP LATAM TOUR 2015

OWASP
The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Ingeniero de Sistemas (UNEXPO).
- Especialista en Auditoria de Sistemas Financieros y Seguridad de Datos.
- Certificado CEHv8 (EC-COUNCIL).
- Más de 6 años de experiencia en Seguridad de la Información.
- Actualmente presto mis servicios profesionales en el sector de Banca y Finanzas.

C|EH™
Certified Ethical Hacker

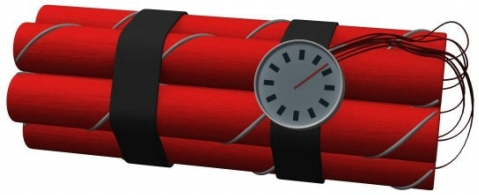
OWASP
The Open Web Application Security Project

INTRODUCCIÓN

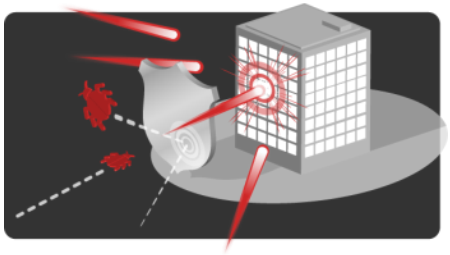
OWASP
The Open Web Application Security Project

INTRODUCCIÓN > CONCEPTOS BÁSICOS

OBJETIVO (TARGET)



EXPLOIT



ZERO DAY

VULNERABILIDAD

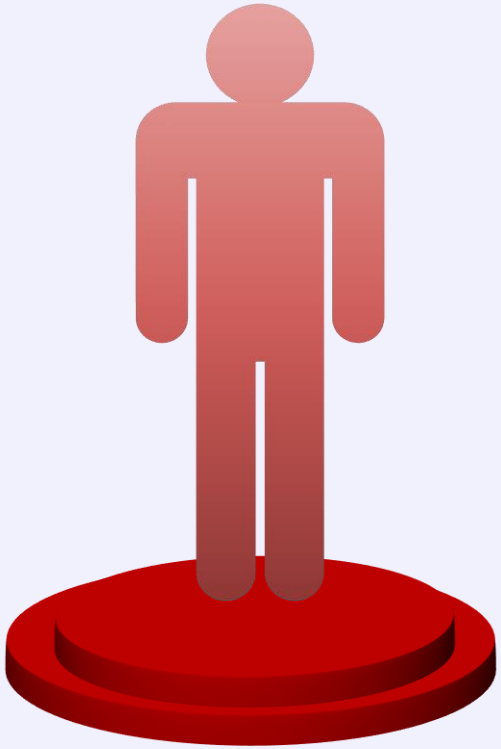
AMENAZAS

RED

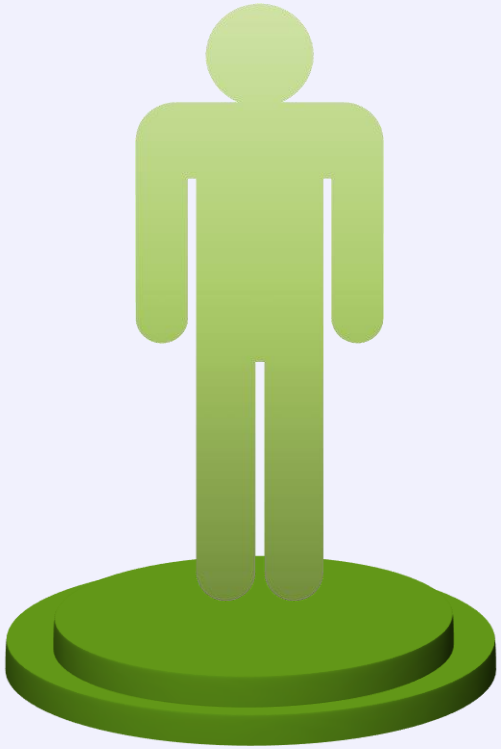
HOST

APLICACIONES

INTRODUCCIÓN > CONCEPTOS BÁSICOS



VS

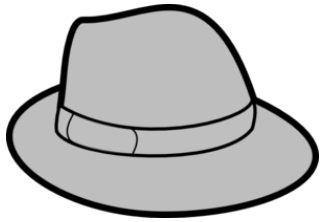


Hacking **Ethical Hacking**

OWASP
The Open Web Application Security Project

INTRODUCCIÓN > TIPOS DE HACKERS

BLACK HATS



GRAY HATS

WHITE HATS

SUICIDE HACKERS

SCRIPT KIDDIES

CYBER TERRORISTS

OWASP
The Open Web Application Security Project

METODOLOGÍAS

OWASP
The Open Web Application Security Project

METODOLOGÍAS

OSSTMM

OWASP

EC-COUNCIL

PTES

OWASP
The Open Web Application Security Project

OSSTMM

Induction Phase

- Posture Review
- Logistics
- Active Detection Verification

Interaction Phase

- Visibility Audit
- Access Verification
- Trust Verification
- Control Verification

Inquest Phase

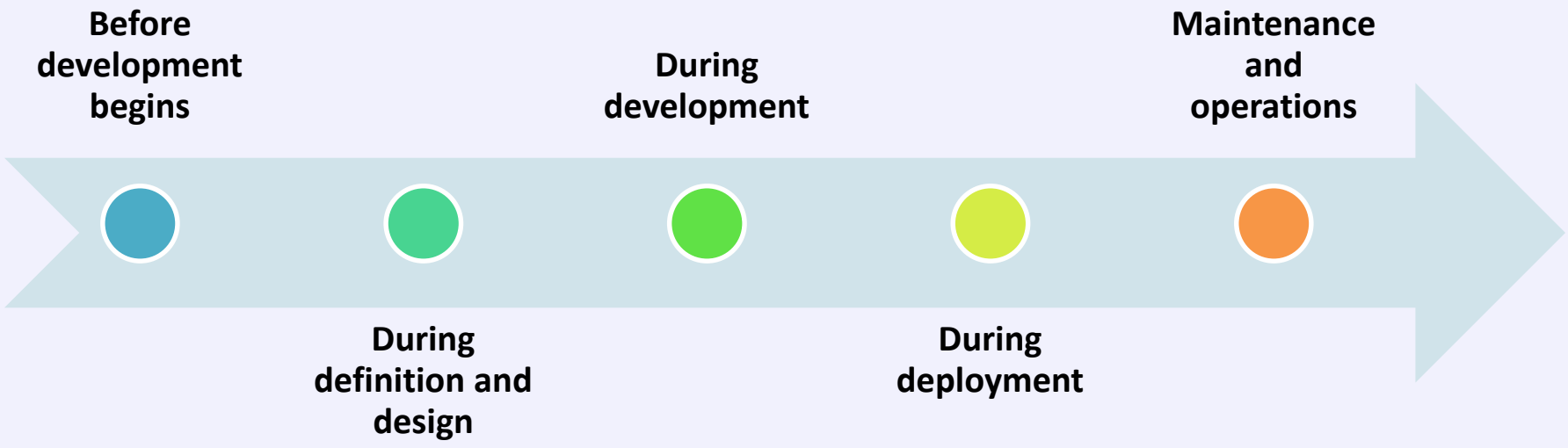
- Process Verification
- Configuration Verification / Training Verification
- Property Validation
- Segregation Review
- Exposure Verification
- CompetitiveIntelligence Scouting

Intervention Phase

- Quarantine Verification
- Privileges Audit
- Survivability Validation / Service Continuity
- Alert and Log Review / End Survey

OWASP
The Open Web Application Security Project

THE OWASP TESTING FRAMEWORK

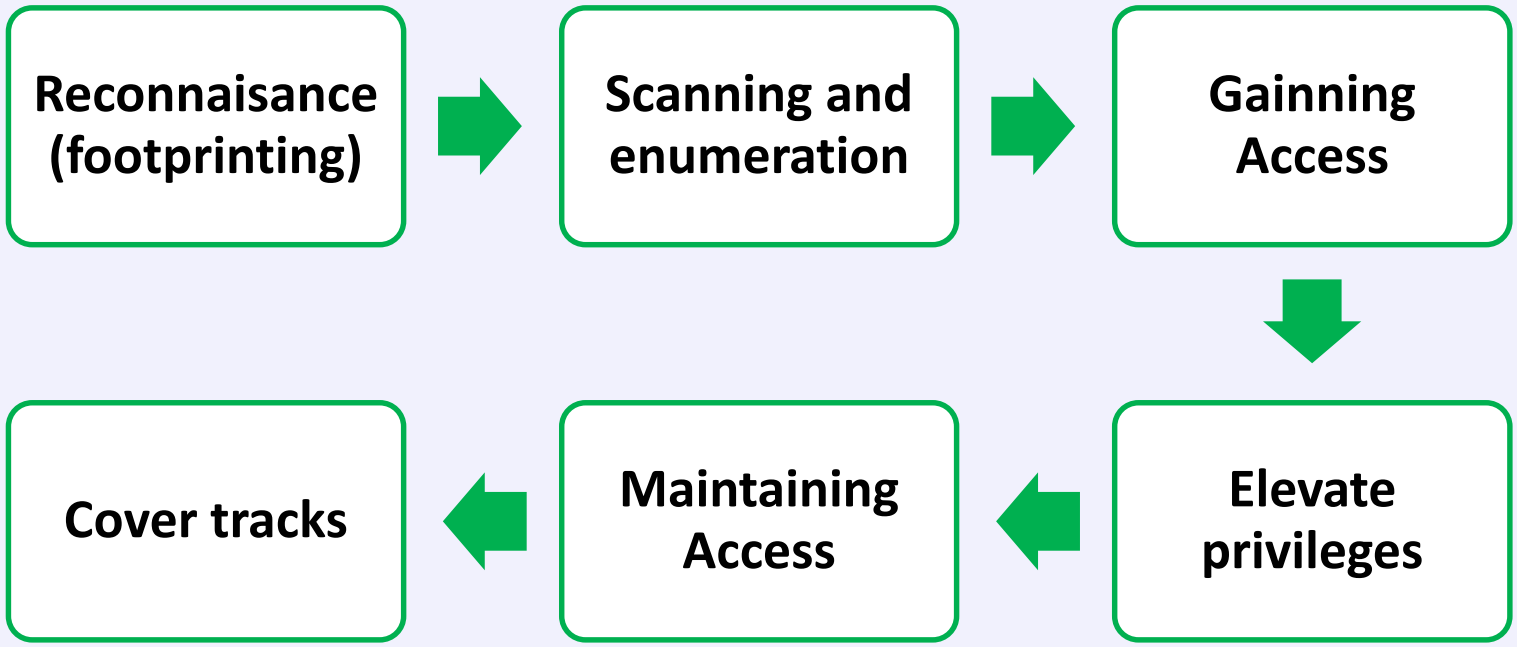


OWASP
The Open Web Application Security Project

WEB APPLICATION SECURITY TESTING

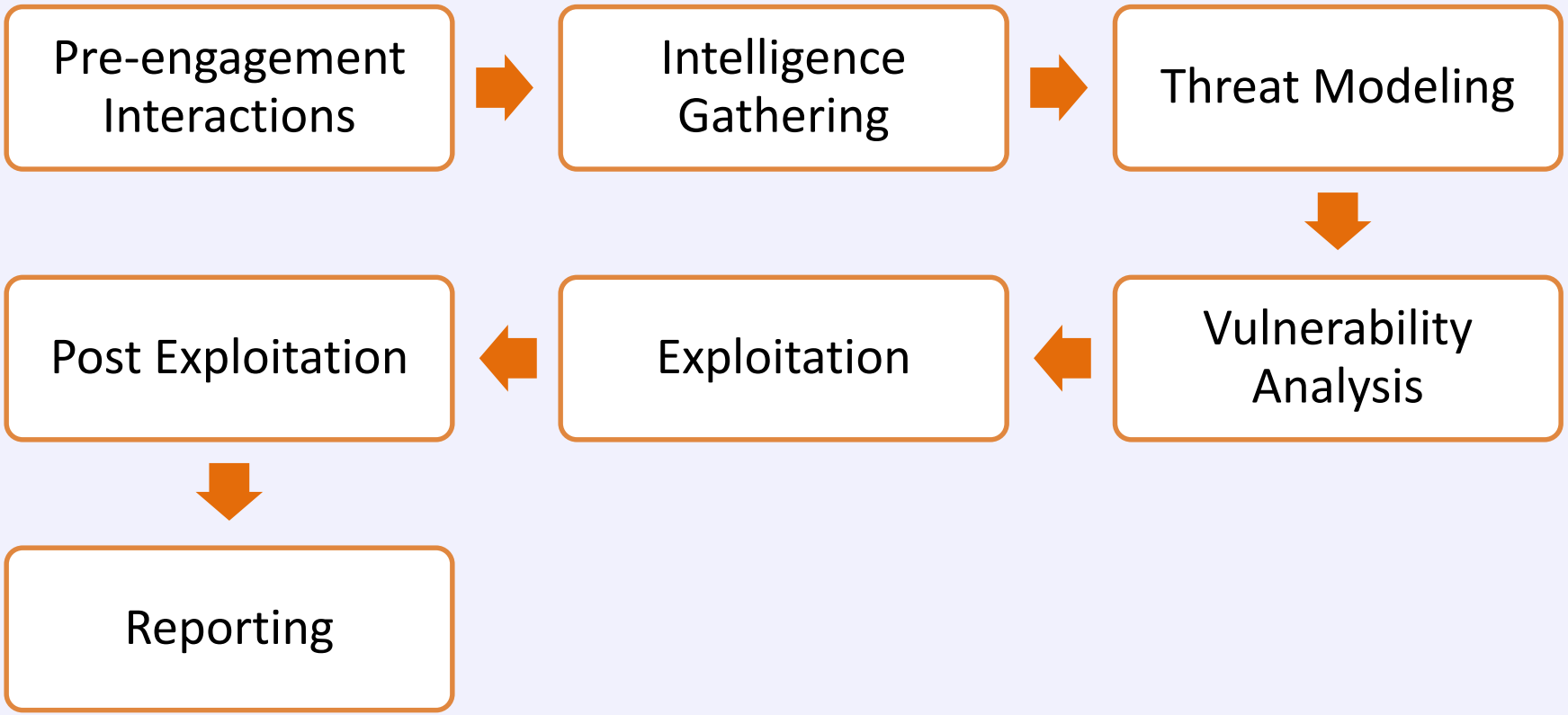
- Introduction and Objectives
- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for Weak Cryptography
- Business Logic Testing
- Client Side Testing

CEH (EC-COUNCIL)



OWASP
The Open Web Application Security Project

The Penetration Testing Execution Standard



OWASP
The Open Web Application Security Project

FASES DEL ETHICAL HACKING

OWASP
The Open Web Application Security Project

FASES DE ETHICAL HACKING

Planificación

Obtención de Información

Enumeración y Explotación de Servicios / Vulnerabilidades

Elevación de Privilegios

Reporte

OWASP
The Open Web Application Security Project

FASES DEL ETHICAL HACKING

PLANIFICACIÓN

OWASP
The Open Web Application Security Project

PLANIFICACIÓN

OWASP
The Open Web Application Security Project

FASES DEL ETHICAL HACKING

OBTENCIÓN DE INFORMACIÓN

OWASP
The Open Web Application Security Project

OBTENCIÓN DE INFORMACIÓN

Nombre de dominio
Direcciones IP
Servicios TCP/UDP
Autenticación

RED

Banners
SNMP
Arquitectura
Passwords

SISTEMA

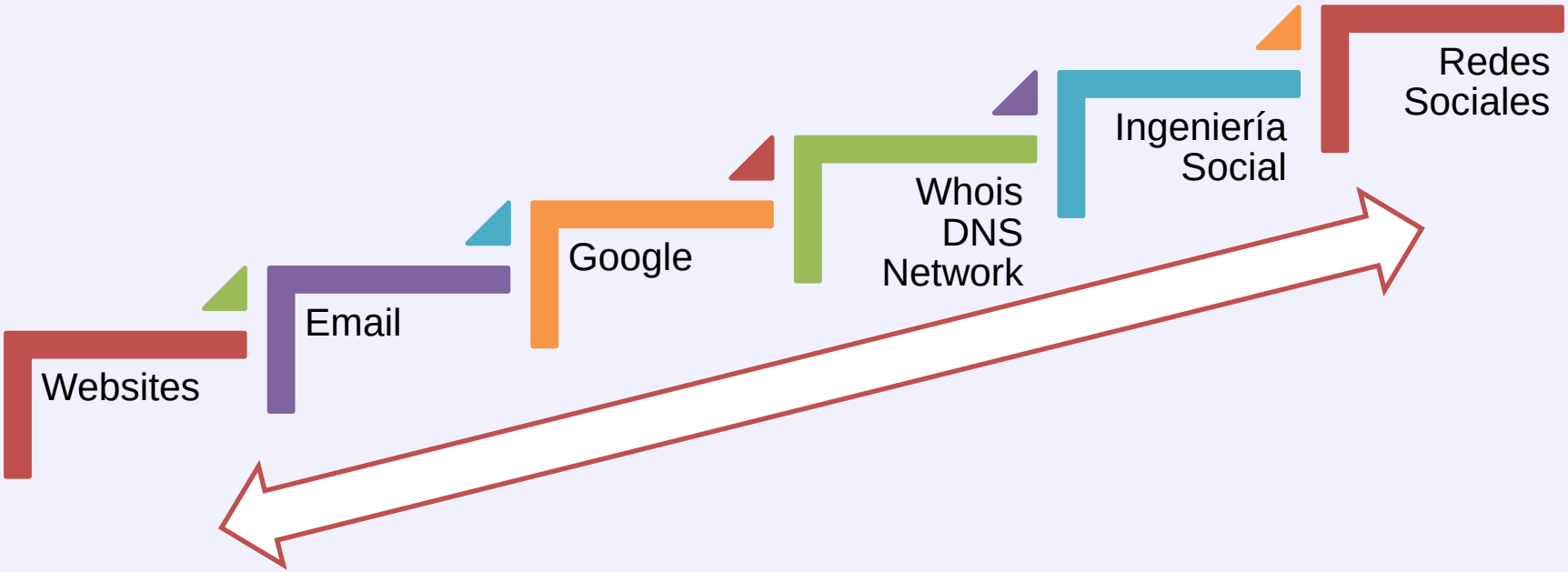
ootprinting

Portal Web
Información de Empleados
Políticas de Seguridad
Teléfonos

ORGANIZACIÓN

OWASP
The Open Web Application Security Project

PASOS PARA LA OBTENCIÓN DE INFORMACIÓN



OWASP
The Open Web Application Security Project

OBTENCIÓN DE INFORMACIÓN: HERRAMIENTAS

pipl

NETCRAFT

Google™ HACKING

MALTEGO

KALI LINUX

OWASP
The Open Web Application Security Project

FASES DEL ETHICAL HACKING

ENUMERACIÓN Y EXPLOTACIÓN DE SERVICIOS / VULNERABILIDADES

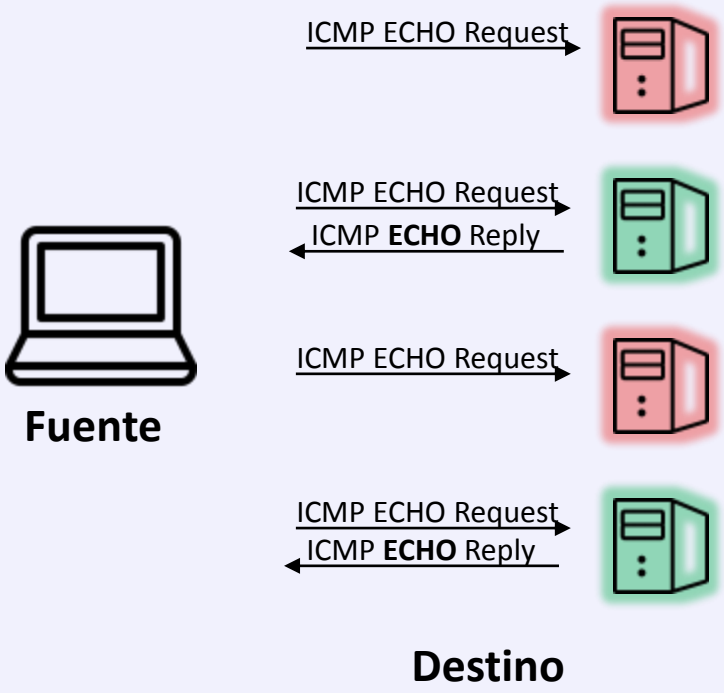
OWASP
The Open Web Application Security Project

ENUMERACIÓN Y EXPLOTACIÓN DE SERVICIOS / VULNERABILIDADES

OWASP
The Open Web Application Security Project

1 IDENTIFICACIÓN DE HOST VIVOS

ICMP Sweep consiste en el envió de ICMP ECHO Request a múltiples hosts. SI existe un host activo, este retornara ICMP ECHO Replay.



La meta de estas pruebas es obtener respuestas las cuales demuestren que una dirección IP efectivamente se encuentra activa.

1 IDENTIFICACIÓN DE HOST VIVOS

Sondeo Ping Sweep
nmap –sP a.b.c.d/xx

Ping TCP SYN
nmap –PS a.b.c.d/xx

Ping TCP ACK
nmap –PA a.b.c.d/xx

Ping ICMP timestamp requests

nmap –PP a.b.c.d/xx
**ICMP timestamp requests (type 13)*

Ping ICMP address mask *requests*

nmap –PM a.b.c.d/xx
**ICMP address mask requests (type 17)*

OWASP
The Open Web Application Security Project

2 BANNER GRABBING

Es un método para identificar el Sistema Operativo en un objetivo remoto o aplicaciones detrás de servicios activos

ACTIVO

PASIVO

```
root@kali:~# nmap --script banner 192.168.30.129

Starting Nmap 6.40 ( http://nmap.org ) at 2015-04-21 23:26 VET
Nmap scan report for 192.168.30.129
Host is up (0.00045s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
|_banner: 220 (vsFTPd 2.3.4)
22/tcp   open  ssh
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp   open  telnet
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
```

KALI LINUX
The quieter you become, the more you are able to hear

```
root@kali:~# nc www.[redacted].com 80
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 22 Apr 2015 03:38:00 GMT
Server: Apache/2.2.3 (Red Hat)
Last-Modified: Wed, 22 Apr 2015 03:36:01 GMT
ETag: "1360005-16491-51447dcab4a40"
Accept-Ranges: bytes
Content-Length: 91281
Cache-Control: max-age=300
```

```
root@kali:~# telnet www.[redacted].com 80
Trying 17[redacted].1[redacted]...
Connected to www.[redacted].com.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 22 Apr 2015 03:45:21 GMT
Server: Apache
Last-Modified: Wed, 22 Apr 2015 03:44:01 GMT
```

3 ESCANEO DE PUERTOS TCP/UDP

EVASIÓN IDS

Fragmentación (-f / -mtu)
Señuelos (-D)
IP Origen Falsa (-S)
Entre Otras…

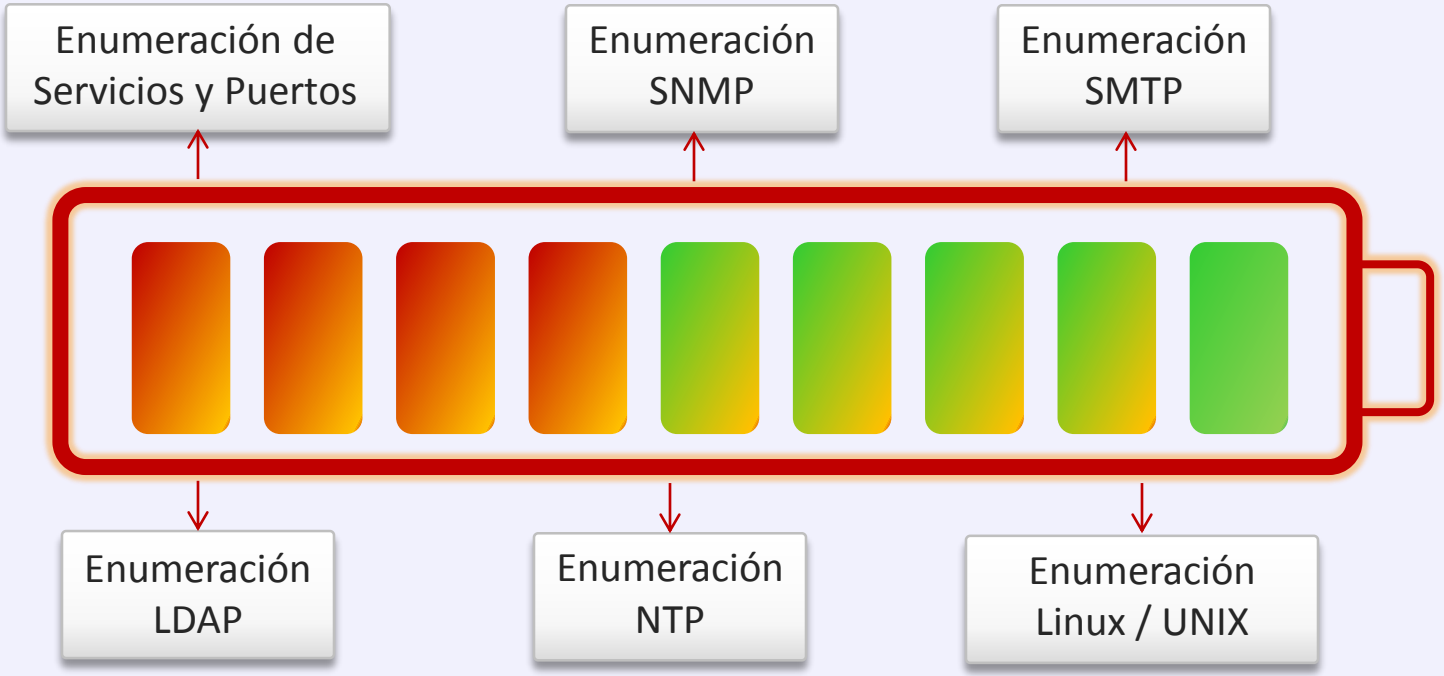
TCP Connect / Full Open Scan

Xmas Scan (-sX)

Null Scan (-sN)

OWASP
The Open Web Application Security Project

4 ENUMERACIÓN



OWASP
The Open Web Application Security Project

Enumeración SMTP	TCP 25: Enumerar Usuarios	*smtp-user-enum.pl* **Comandos VRFY, EXPN, RCPT*
Enumeración de Servicios y Puertos	TCP 53: Transferencia de Zona	*#dig NS <dominio>* *#dig AXFR <dominio> @DNS*
Enumeración SNMP	UDP 161: Enumerar Cuentas de Usuarios y dispositivos	*#snmpcheck –t <dir IP>* *#nmap –sU –p161 <dirIP>-sC*
Enumeración LDAP	TCP/UDP 389: Enumerar Usuarios de la Red	*#ldapsearch* **ldap utils*
Enumeración NTP	UDP 123: hosts, direcciones IP, system names, OS.	*#ntptrace* *#ntpdc* *#ntpq*
Enumeración Linux / UNIX	Enumerar Recursos de Red	Finger, rpcinfo, showmount

OWASP
The Open Web Application Security Project

5 ESCANEO DE VULNERABILIDADES

OWASP ZAP

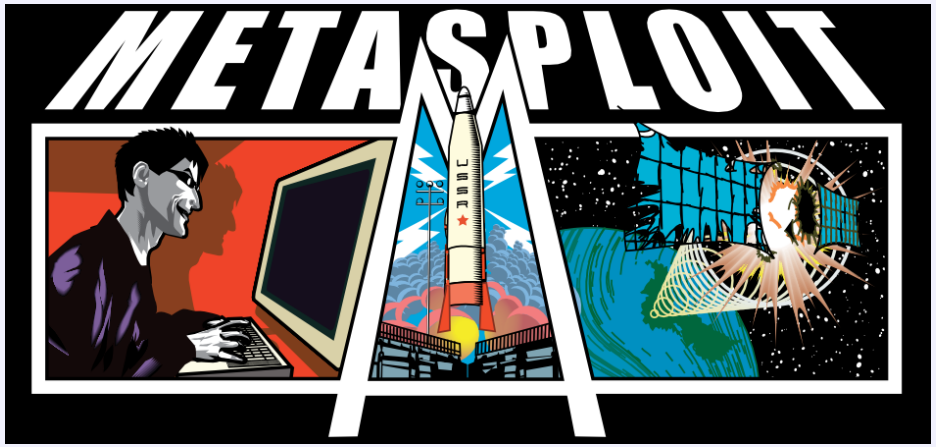
acunetix

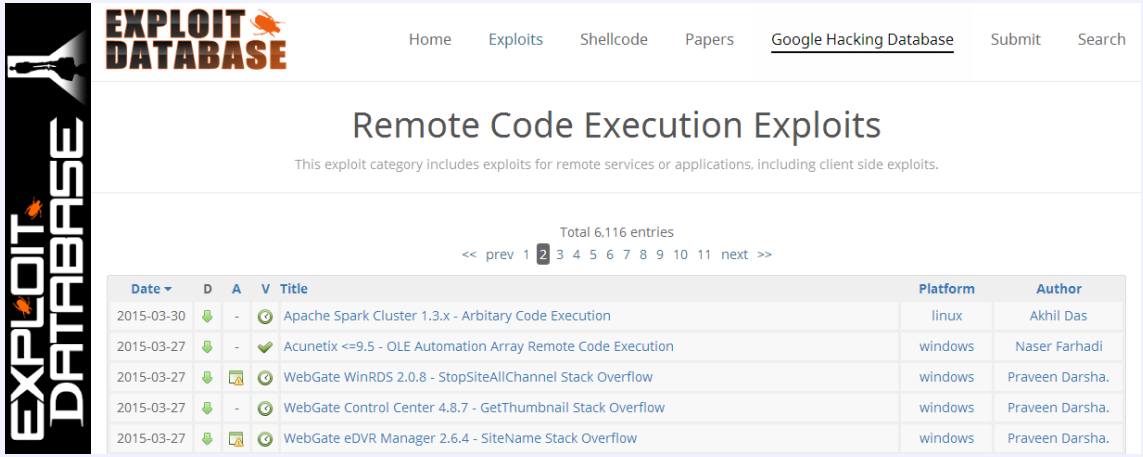
OpenVAS
Open Vulnerability Assessment System

OWASP

The Open Web Application Security Project

6 EXPLOTACIÓN DE VULNERABILIDADES





OWASP
The Open Web Application Security Project

FASES DEL ETHICAL HACKING

ELEVACIÓN DE PRIVILEGIOS

OWASP
The Open Web Application Security Project

ELEVACIÓN DE PRIVILEGIOS

Cracking de Contraseñas

Escalar Privilegios

OWASP
The Open Web Application Security Project

TÉCNICAS Y ATAQUES A CONTRASEÑAS

TÉCNICAS

Ataque de Diccionario

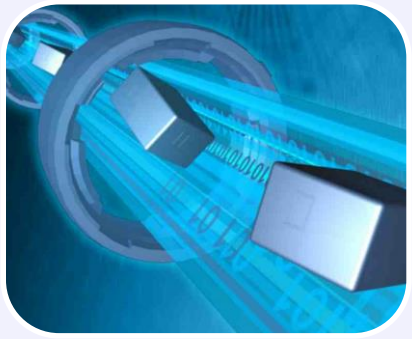
Ataque de Fuerza Bruta

Ataque Hibrido

Ataque Basado en Reglas

ATAQUES

Ataques Pasivos

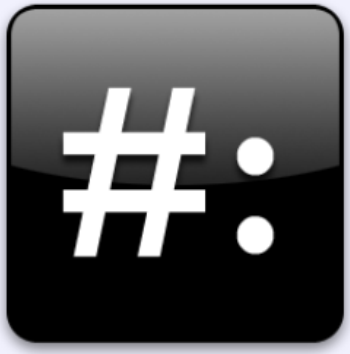


Ataques Activos

Ataques Offline

OWASP
The Open Web Application Security Project

ELEVACIÓN DE PRIVILEGIOS



Escalar privilegios verticalmente consiste en acceder a zonas o privilegios superiores a los establecidos por el administrador

VERTICAL

HORIZONTAL

Escalar privilegios horizontalmente consiste en acceder a zonas o recursos de usuarios con privilegios similares.

OWASP
The Open Web Application Security Project

FASES DEL ETHICAL HACKING

REPORTE

OWASP
The Open Web Application Security Project

REPORTE

INFORME GERENCIAL

- Nivel de exposición de la plataforma.
- Nivel de riesgo.
- Plan de remediación sugerido.

INFORME TÉCNICO

- Hallazgos.
- Detalle de las vulnerabilidades.
- Procedimiento de explotación.
- Evidencias.
- Contramedidas.

OWASP
The Open Web Application Security Project

CONCLUSIONES

- La planificación juega un rol vital en ethical hacking.
- Nunca iniciar un ethical hacking sin contar con la debida autorización por parte del propietario del sistema.
- Realizar una adecuada enumeración de la plataforma será útil para las fases posteriores.
- La metodología no es estrictamente lineal.
- Se deben colectar evidencias en todas las fases del ethical hacking.
- Bajo ningún concepto se debe poner en riesgo (DoS, malware, etc) la plataforma tecnológica al momento de explotar vulnerabilidades.
- La ÉTICA debe ser nuestra principal herramienta de seguridad.

OWASP
The Open Web Application Security Project

PREGUNTAS

OWASP
The Open Web Application Security Project

Ing. Jair Garcia, CEH

ing.jairgarcia@gmail.com

https://ve.linkedin.com/pub/jair-a-garcia-v