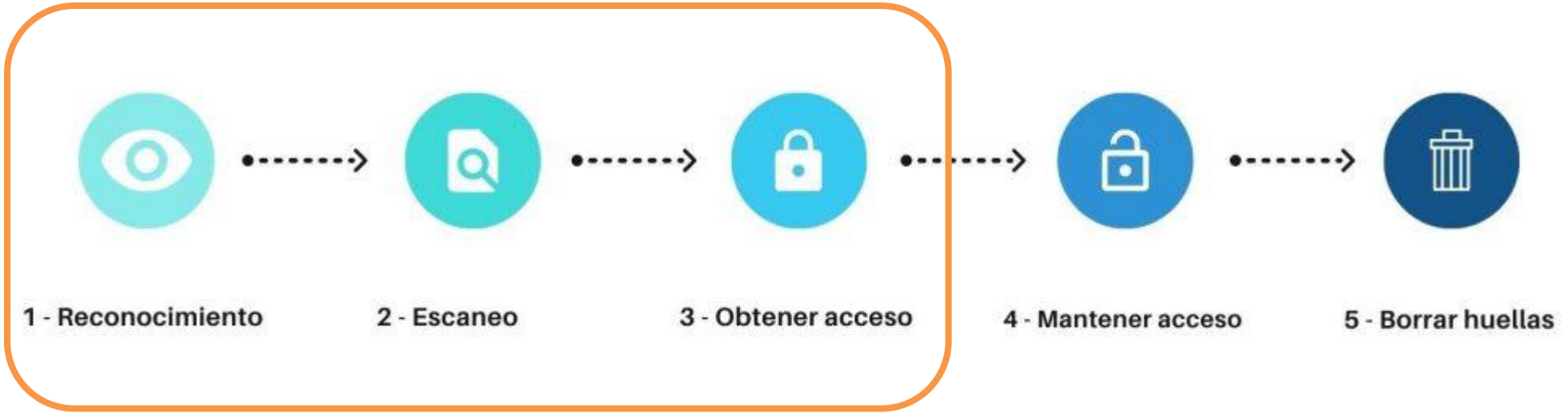
UT2:

Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros

UT2:
Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros

- **Objetivo**: Descubrir el perímetro de la red del cliente a auditar, buscar información sensible que nos permita definir los mejores vectores de ataque y usar herramientas para simular ataques y conseguir acceso a los servidores.
- Nos centraremos en las tres primeras fases del Hacking



Fase de Reconocimiento

Information gathering* o *footprinting

"Si tuviera 9 horas para cortar un árbol, le dedicaría 6 horas a afilar mi hacha",

Abraham Lincoln.

- Descubrir la mayor cantidad de información relevante de la organización cliente.

Normalmente la **información** que suelen recopilar es:

- Nombre del dominio y subdominios
- Direcciones IP, servidores DNS, correo, …
- Sistemas operativos utilizados, aplicaciones
- Información de los empleados
- Números de teléfono
- Direcciones de correo

Fase de Reconocimiento

Information gathering* o *footprinting

Tipos de reconocimiento

➢ Reconocimiento pasivo:

No hay interacción con el objetivo. Búsquedas de información en fuentes abiertas y públicas en Internet o escuchando la red:

- **OSINT** (*Open Source Intelligence*), HUMINT (***HUM****an* ***INT****elligence,* fuentes humanas, chivatos o colaboradores*),* SIGINT (Inteligencia de señales, sensores, alertas).
  - Búsqueda en redes sociales,
  - Consultas directorios de Internet (Who-Is)
  - Búsqueda en periódicos ofertas de empleo publicadas.
- ***Sniffers*** de red.
- ***Dumpster Diving*** – bucear en la "basura": podemos encontrar códigos de acceso, contraseñas, correos electrónicos, números de teléfonos, …

➢ Reconocimiento activo:

Hay interacción directa con la víctima.

- Barridos de ping.
- Conexión a un puerto de aplicación (*banner grabbing*).
- Ingeniería social (llamadas telefónicas, falsos correos,…)
- Mapeo de red.

Fase de Reconocimiento

Information gathering* o *footprinting

Tipos de Dominios

- Dominios de Nivel Superior Genéricos *(**gTLD,** generic Top-Level Domain)*
  .com , .net, .org, .info

- Dominios de Nivel Superior Geográfico *(**ccTLD**, country code Top-Level Domain)*
  .es, .ar, uk, .it. .fr, ..

Subdominios

- Cualquier dominio que se añade a la izquierda de un dominio principal:
  correo.ulpgc.es
  mail.ieselrincon.org
  www.bmw.de

Fase de Reconocimiento

Information gathering* o *footprinting

Registros Regionales de Internet *(RIR)*

- Organizaciones encargadas de registrar y asignar las direcciones de Internet tanto IPv4 como IPv6.
- Actualmente existen 5 RIR: **ARIN** para EE.UU. y Canadá, **RIPE** para Europa, Oriente Medio y Asia Central, **APNIC** para Asia, **LACNIC** América latina y Caribe y **AfriNIC** para África.

- Se consulta mediante protocolo WHOIS o vía Web.
- Son bases de datos que se pueden descargar.

Fase de Reconocimiento

Information gathering* o *footprinting

Herramientas fase de Reconocimiento

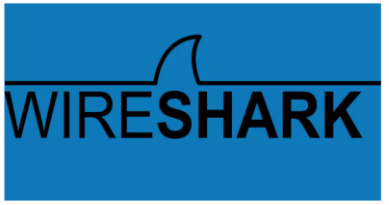
- ***Footprinting* con buscadores**
  - **Google (*Google Dorks*), Shodan**
- **Herramientas CLI (*Command Line Interface*)**
  - whois, host, nslookup, dig, dnsrecon**, …**
- **Herramientas de automatización**
  - fierce, sublist3r, The harvester, …

Fase de Reconocimiento

Information gathering* o *footprinting

Herramientas fase de Reconocimiento

- **Herramientas todo en uno:**
  - Maltego, spiderfoot, discover, traceroute, …
- **Sniffers de red:**
  - wireshark, tcpdump, …
- **Recursos Webs**
  - DNSDumpster , Pentest-tools, Netcraft
  - IPv4info, infocif, RapidDNS, Robtex, CentralOps.net



Fase de Reconocimiento

Information gathering* o *footprinting

Medidas defensivas fase de reconocimiento:

No es posible evitar los ataques de reconocimiento, pero hay que intentar exponer la mínima información posible:

- Ocultar información servicios de directorio Who-Is.
- No publicar información sensible sobre la organización
- Formación personal para prevenir ataques ***Phishing***.
- Implementar medidas seguridad perimetral (firewalls, IDS,…)
- Definir políticas para protección y manejo de datos confidenciales.

Fase de Escaneo o enumeración: *fingerprinting*

Objetivo: Con la información obtenida en la fase anterior, nos centraremos en descubrir **host activos**, **sistemas operativos**, **puertos** abiertos, **servicios** que corren detrás de esos puertos, recursos compartidos, ***hashes***, **vulnerabilidades** o malas configuraciones.

Tipos de Escaneos

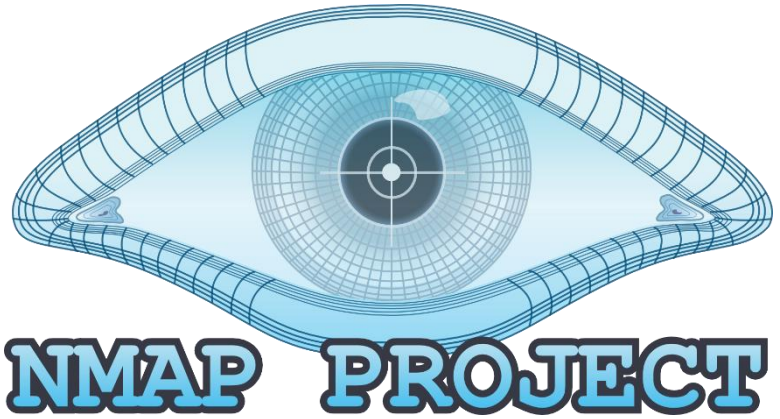
- **Escaneo de red**: determinar los equipos activos en la red y sus direcciones IP.
- **Escaneo de puertos**: determinar puertos abiertos tanto TCP como UDP.
- **Escaneo de vulnerabilidades**: determinar vulnerabilidades conocidas.

Banner Grabbing: obtener la información del banner de servicios abiertos en las máquinas remotas.

Fase de Escaneo o enumeración: *fingerprinting*

Herramientas fase de escaneo o *fingerprinting*

- **Barridos de ping (*Ping Sweeps*)**: permiten descubrir host activos:
  - ping, fping, hping3, MegaPing, **nmap**., netdiscover
- **Escaneo de puerto (*Port Scanning*)**: permiten identificar puertos y servicios:
  - nmap, zenmap, masscan, zmap
- **Otras herramienta de enumeración**
  - arp-scan, dnsenum, enum4linux
  - ntbscan, smbmap



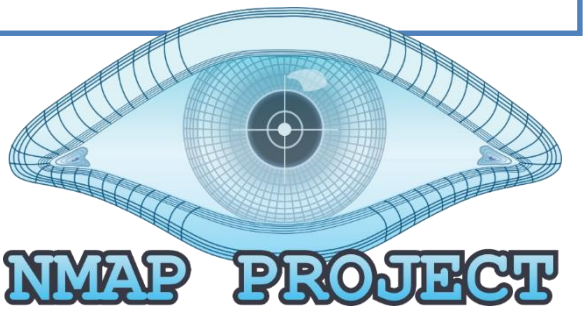
Fase de Escaneo o enumeración: *fingerprinting*

Medidas defensivas fase de escaneo:

- Instalar solo servicios necesarios. Implantar políticas de ***hardening*** .
- Tener sistemas y aplicaciones actualizadas.
- Segmentar red para separar zonas de seguridad.
- Implementar medidas de seguridad perimetral (firewalls, IDS,…)
- Implementar sistemas de prevención de intrusos (IPS)
- Políticas robustas de contraseñas.
- Realizar auditorías periódicas de seguridad así como de análisis de vulnerabilidades.

Fase de Escaneo o enumeración: *fingerprinting*

Análisis de puertos



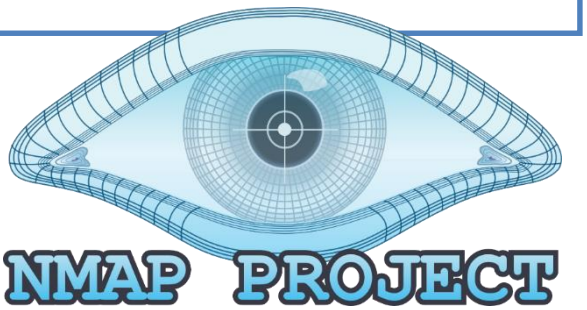
- ¿**Qué es un análisis de puertos**?
  - Un barrido de las conexiones establecidas a uno o varios puertos de un sistema.

- ¿**Para qué sirve el análisis de puertos**?
  - Para averiguar qué puertos y servicios posee el sistema objetivo.
  - Comúnmente con fines de administración de sistemas.
  - Y en otras ocasiones con fines maliciosos.

- ¿**Qué información puede obtener un atacante**?
  - Puntos de entrada al sistema.
  - Servicios en ejecución.
  - Versiones del software y los servicios.

Fase de Escaneo o enumeración: *fingerprinting*

Principales puertos

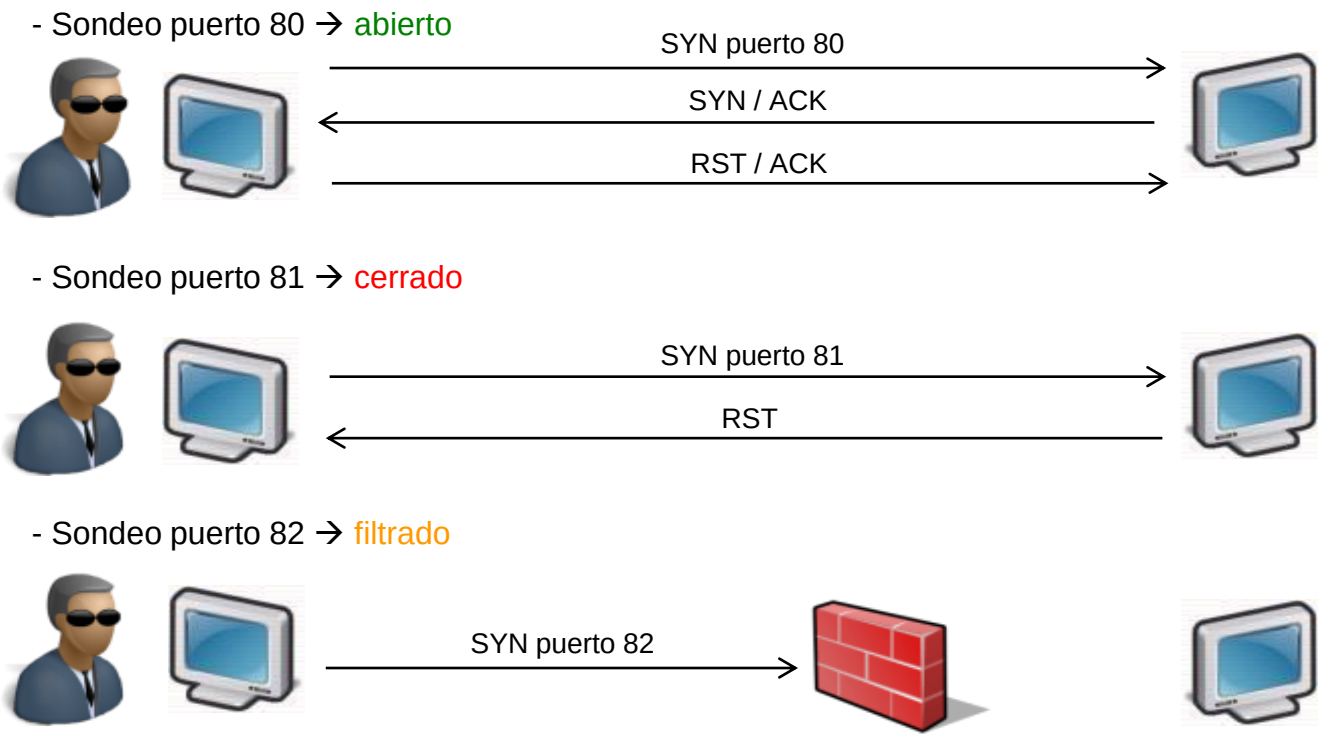


Puerto	Nombre	Descripción
20	ftp-data	Puerto de datos FTP
21	ftp	Puerto del Protocolo de transferencia de archivos (FTP)
22	ssh	Servicio de shell seguro (SSH)
23	telnet	El servicio Telnet
25	smtp	Protocolo simple de transferencia de correo (SMTP)
53	domain	Servicios de nombres de dominio
69	tftp	Protocolo de transferencia de archivos triviales (TFTP)
80	http	Protocolo de transferencia de hipertexto (HTTP)
110	pop3	Protocolo Post Office versión 3
115	sftp	FTP Seguro
137	netbios-ns	Servicios de nombres NETBIOS
138	netbios-dgm	Servicios de datagramas NETBIOS
139	netbios-ssn	Servicios de sesión NETBIOS
161	snmp	Protocolo simple de administración de redes (SNMP)
443	https	Protocolo de transferencia de hipertexto seguro (HTTP)

Fase de Escaneo o enumeración: *fingerprinting*

¿Cómo se realiza el análisis de puertos?

- El ordenador origen intenta establecer conexiones con cada uno de los puertos del sistema a analizar. En función de la respuesta de cada uno de los puertos del sistema analizado, se establece si el puerto está abierto, cerrado o filtrado.

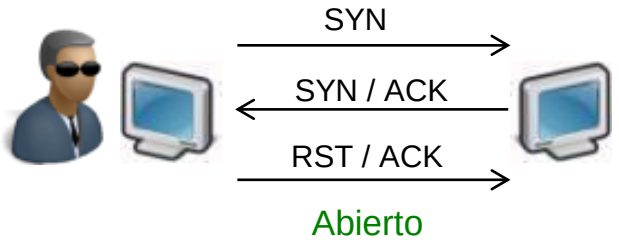


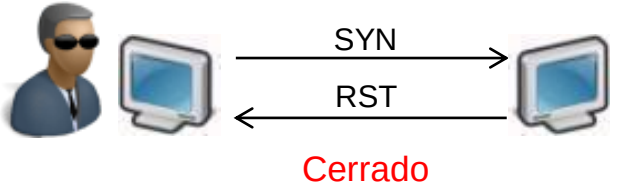
Fase de Escaneo o enumeración: *fingerprinting*

Tipos de escaneos de puertos

- Existen varios **tipos de escaneos de puertos** con distintas
- características:
  - Robustos.
  - De evaluación de firewalls.
  - De evasión de firewalls.
  - Silenciosos.
  - Ocultación.
  - Herramienta utilizada: **nmap**

- **TCP Scan**:
  - Comando: nmap **–sT** $direccionIP
  - Establecimiento completo de una conexión.
  - 3-way handshake



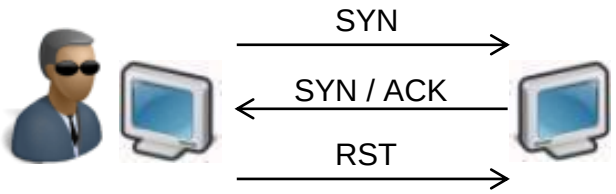


Fase de Escaneo o enumeración: *fingerprinting*

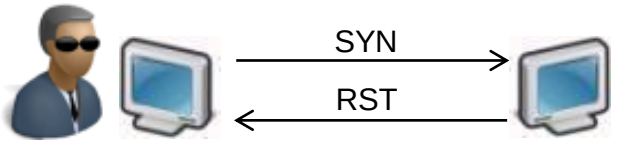
Tipos de escaneos de puertos

- Stealth Scan (Half-Open Scan):
  - Comando (1): nmap **–sS** $direcciónIP
  - Establecimiento incompleto de una conexión.
  - Utilizado para la evasión de firewalls, de mecanismos de login y para ocultarse en el tráfico.

Fuente (1): https://nmap.org/book/synscan.html

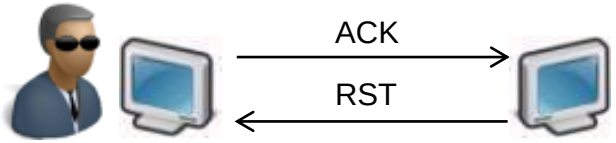


Abierto

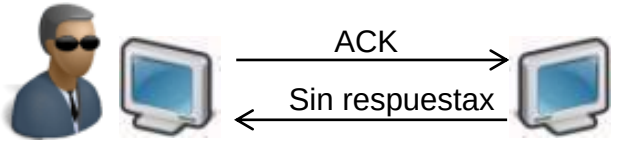


Cerrado

- ACK Scan:
  - Comando (2): nmap **–sA** $direccionIP
  - Envío únicamente de la confirmación de recepción.
  - Utilizado para la detección de firewalls.



Sin Firewall



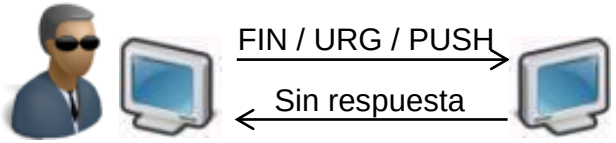
Firewall

Fuente (2): https://nmap.org/book/scan-methods-ack-scan.html

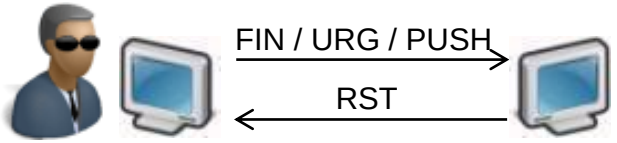
Fase de Escaneo o enumeración: *fingerprinting*

Tipos de escaneos de puertos

- Xmas Scan:
  - Comando (1): nmap **–sX** $direccionIP
  - Envío de un paquete con todos los flags activados.
  - No funciona contra sistemas Windows.

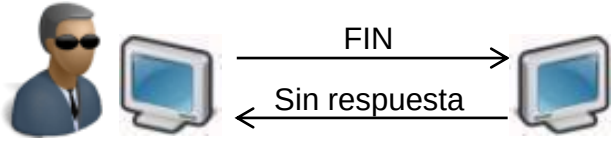


Abierto

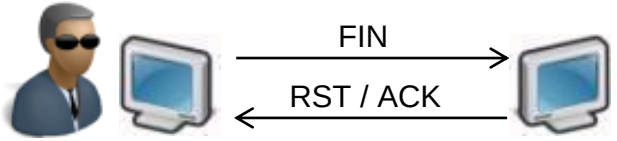


Cerrado

- FIN Scan:
  - Comando (2): nmap **–sF** $direccionIP
  - Envío de un paquete con solo el flag FIN.
  - No funciona contra sistemas Windows.



Abierto



Cerrado

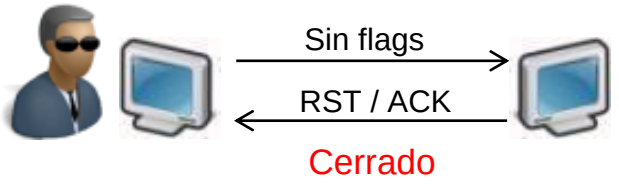
Fuente: https://nmap.org/book/scan-methods-null-fin-xmas-scan.html

Fase de Escaneo o enumeración: *fingerprinting*

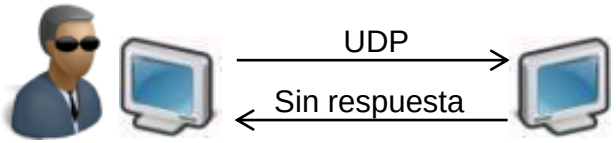
Tipos de escaneos de puertos

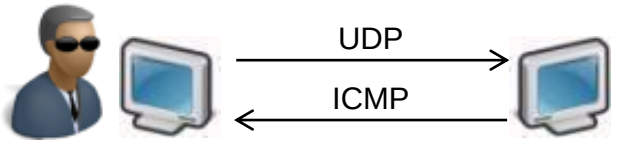
Fuente: https://nmap.org/book/scan-methods-null-fin-xmas-scan.html

- NULL Scan:
  - Comando (1): nmap **–sN** $direccionIP
  - Envío de un paquete sin flags activados.
  - No funciona contra sistemas Windows.



- UDP Scan:
  - Comando (2): nmap **–sU** $direccionIP
  - Envío de un paquete UDP no orientado a conexión, no existe 3-way handshake.
  - Pocos servicios utilizan el protocolo UDP.





Fuente: https://nmap.org/book/scan-methods-udp-scan.html

Fase de Escaneo o enumeración: *fingerprinting*

Banner grabbing

- El **banner grabbing** consiste en la extracción de información de los puertos abiertos.
- Esta información está relacionada con el servicio y versión que se está ejecutando en dicho puerto.
- De esta manera, se extrae información de los posibles vectores de ataque que tenemos.
- Herramientas: netcat, telnet, nmap, wget …
- Ejemplo:
  - Banner de un puerto 80 que está ejecutando el servicio http.

nmap -**Pn** -**sV** 10.0.0.2 -p 80

nmap -Pn -sV 10.0.0.5 -p 22

nc -**v** 10.0.0.2 **80**

nc -**v** 10.0.0.5 **22**

wget 10.0.0.2 -**q** -**S**

(Status-Line)	HTTP/1.1 200 OK
Cache-Control	max-age=432000
Content-Length	348
Content-Type	image/png
Last-Modified	Thu, 29 May 2014 14:42:30 GMT
Accept-Ranges	bytes
Etag	"08fbe374c7bcf1:39c2"
Server	Microsoft-IIS/6.0
X-Powered-By	ASP.NET
Date	Thu, 04 Sep 2014 11:29:45 GMT
Connection	Keep-Alive
Age	0

Fase de Escaneo o enumeración: *fingerprinting*

Como protegerse contra un Banner grabbing

- Cuando sea posible, deshabilitar el banner que el servidor expone.
- Modificar el banner y mostrar un banner falso para confundir al atacante.
- Usar herramientas como ServerMask para deshabilitar o cambiar la información sobre el banner.
- Alternativamente, cambiar el parámetro **ServerSignature** a Off en el fichero httpd.conf cuando se trate de servicios web.
- Ocultar la extensión de los ficheros en una aplicación web para ocultar las tecnologías que hay detrás del servidor.

Fase de Intrusión

Objetivo: Con la información obtenida en las fases anteriores, el ***pentester*** intentará comprometer una máquina de la organización, obteniendo un acceso no autorizado a la misma.

Definiciones:

- **Vulnerabilidad (*bug*)**: un fallo o debilidad en el diseño de una aplicación o del propio sistema, que puede conducir a un acontecimiento inesperado y no deseable, el cual pone en peligro la seguridad del sistema
- **Exploit:** un programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio.
- **Payload**: carga útil. Código que se ejecuta después de que un exploit haga provocar un fallo en el sistema debido a una vulnerabilidad no corregida.

Fase de Intrusión

Tipos de *exploits*:

- **Exploits remotos**: son lanzados sobre la máquina.
- **Exploits locales:** ejecutados desde la máquina vulnerada para tareas de post-explotación.
- **Exploits del lado del cliente**: engañar a un usuario para ejecutar el *exploit* y nos permita conectarnos a la máquina.

Búsqueda de exploits:

- **searchexploit** (kali)
- Google
- **exploit-db.com**

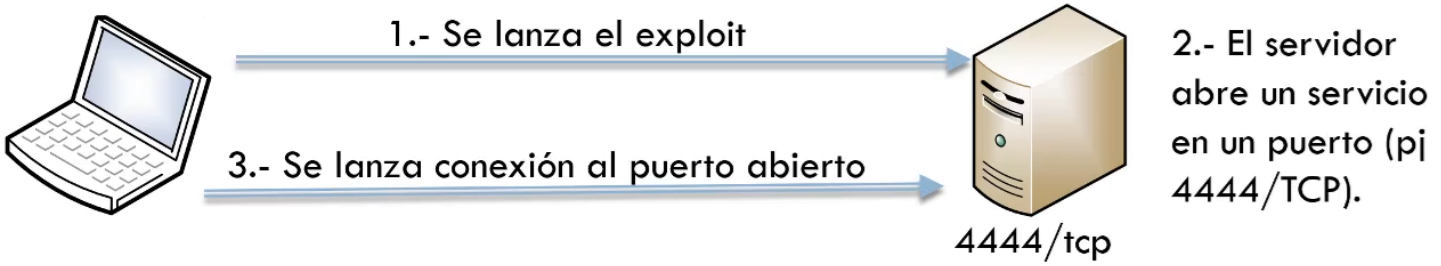
metasploit®

Fase de Intrusión

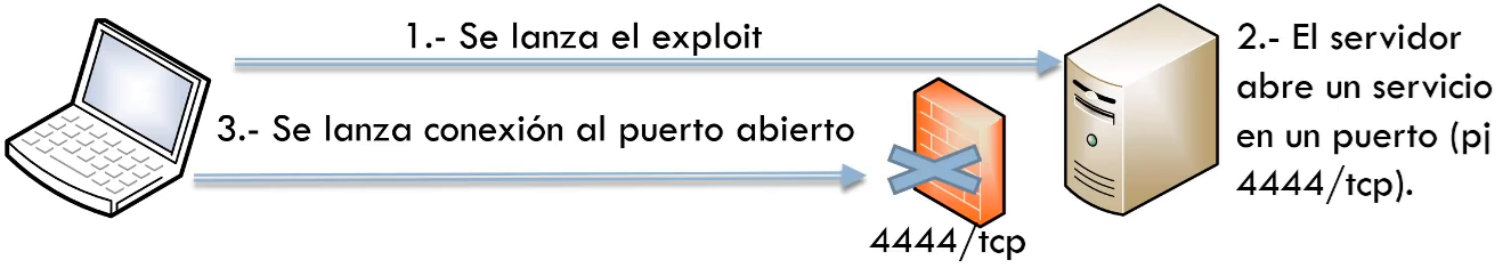
Tipos de conexiones:

Conexión directa (*bind*): la máquina víctima se pone a la escucha en un puerto y la máquina atacante se conectará a dicho puerto.

El payload ejecuta un servicio que deja abierto en el servidor un puerto al que el auditor se conecta



No funciona si hay un firewall de entrada que no permite el tercer paso



Fase de Intrusión

Tipos de conexiones:

Conexión inversa (*reverse*): la máquina atacante se pondrá a la escucha en un puerto y la máquina víctima se conectará a dicho puerto. Tienen mayor éxito, ya que el *firewall* no suele bloquear las conexiones salientes.