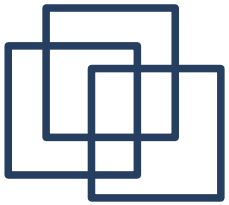
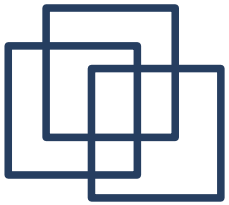
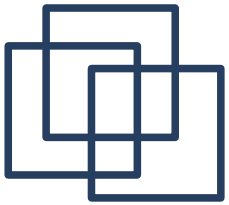


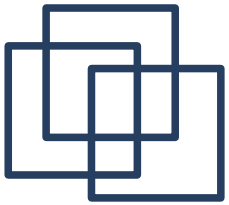
AntiHacking



Nota de Copyright



Índice

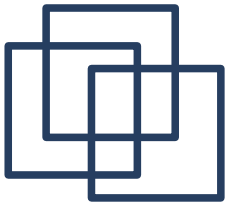


Introducción y conceptos previos

¿Qué es la Seguridad Informática?

- Un sistema informático es seguro si su comportamiento es acorde con las especificaciones previstas para su utilización

- Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza



Introducción y conceptos previos

¿Porqué necesitamos la seguridad informática?

Preocupaciones principales:

- Evitar la pérdida de datos
- Autorización selectiva de acceso a datos
- Asegurar utilización equitativa y autorizada de recursos

Algunas causas de problemas de seguridad:

- Errores de programación
- Manipulación incorrecta de los sistemas
- Accidentes
- Una persona mal intencionada
- ...

Campos de acción de la seguridad informática

- Seguridad física
- Seguridad en las comunicaciones
- Seguridad computacional
- Seguridad de la información

Programas malignos

- Virus
- Troyano
- Gusano

Tipos de intrusos

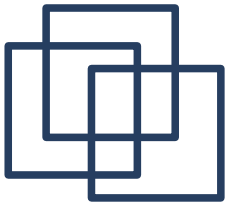
- Script kiddie: presume de ser un hacker o cracker cuando en realidad no posee un grado de conocimientos suficientes
- Cracker: alguien que viola la seguridad de un sistema informático con fines de beneficio personal o para hacer daño a su objetivo
- Hacker: neologismo utilizado para referirse a un experto (véase Gurú) en varias o alguna rama técnica relacionada con las Tecnologías de la Información y las Telecomunicaciones
- De paso: utiliza un sistema como intermediario para llegar al equipo objetivo

Tipos de protección

- Criptografía
- Cortafuegos
- Sistema de detección de intrusiones
- Antivirus

Seguridad de los sistemas operativos

- Autenticación
- Gestión de usuarios
- Permisos de las aplicaciones
- Permisos sobre el sistema de ficheros
- Tiempo que tarda en solucionar problemas de seguridad



Seguridad en redes

- Control de acceso
- Control de integridad de los datos
- Privacidad de las comunicaciones
- Prevencion de intrusiones

Herramientas de seguridad informática

- Escaner de vulnerabilidades
- Sistema de deteccion de intrusiones
- Sniffers
- Crackeador de contraseñas
- Antivirus
- Cortafuegos

Algunos sitios Web indispensables

- http://sectools.org/

  Listado de las 100 herramientas de seguridad más importantes

- http://www.securityfocus.com

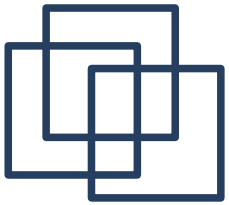
  Mucha informacion sobre seguridad, listas de correo, ...

- http://www.hispasec.com/

  Empresa de seguridad. Lista de correo *unaaldia*

- http://www.kriptopolis.org/

  Noticias y artículos sobre seguridad

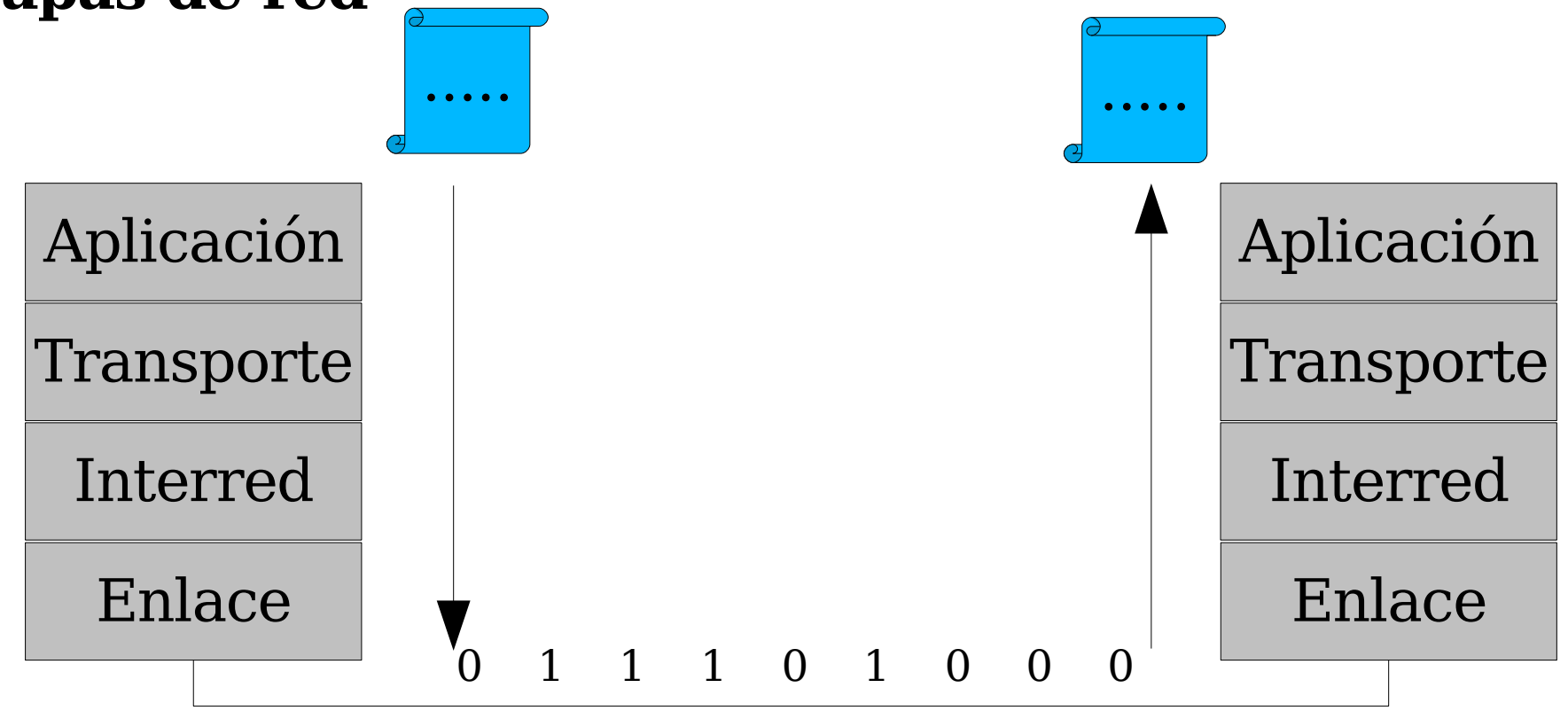


Conceptos imprescindibles y TCP/IP

Introducción

- Para conseguir un entorno seguro necesitamos:
  - Conocimiento
  - Conocimiento
  - Conocimiento
  - Conocimiento
  - ...

Capas de red


Aplicación
Transporte
Interred
Enlace
0 1 1 1 0 1 0 0 0
Aplicación
Transporte
Interred
Enlace

Capas de red

Aplicación	HTTP, DNS, FTP, SMTP, ...
Transporte	TCP, UDP
Interred	IPv4, IPv6
Enlace	Ethernet, Token Ring

Dirección IP

- 32 bits. 4 números decimales del 0-255
- Clases:

A: 0.0.0.0	-	127.255.255.255
B: 128.0.0.0	-	191.255.255.255
C: 192.0.0.0	-	223.255.255.255

- Direcciones IP privadas:

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

Máscara de subred

- Combinación de bits que sirve para delimitar el ámbito de una red de computadoras
- Indica el número de bits que forman parte del identificador de subred (los que están a 1) y cuáles forman parte del identificador de host (están a 0)
- Ejemplos:

255.0.0.0	=	/8
255.255.0.0	=	/16
255.255.255.0	=	/24
255.255.255.192	=	/26

Protocolo IP

- Protocolo para enviar datos a través de una red de paquetes conmutados
- Protocolo no orientado a conexión
- Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas
- Servicio de envio de datagramas no fiable (también llamado del mejor esfuerzo)
- MTU: Tamaño maximo de cada paquete

Protocolo ICMP

- Protocolo utilizado principalmente para:
  - Enviar mensajes de error
  - Indicar que un servicio determinado no está disponible
  - Que un router o host no puede ser localizado
- PING

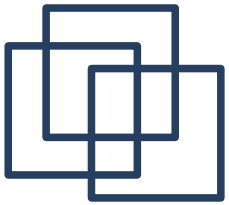
Encaminamiento

- Mecanismo por el que en una red los paquetes de información se hacen llegar desde su origen a su destino final
- Router: interconecta redes de computadoras y opera en la capa tres
- Tabla de encaminamiento: especifica como se deben encaminar los paquetes. Ejemplo:

Destino	Gateway	Interfaz
192.168.1.0/24	0.0.0.0	eth0
192.168.2.0/24	192.168.1.30	eth0
0.0.0.0	192.168.1.40	eth0

Capa de transporte

- Encargado de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados
- Controla el flujo de la red
- Asigna números de secuencia a los segmentos
- Coordina el reenvio de segmentos



Puertos

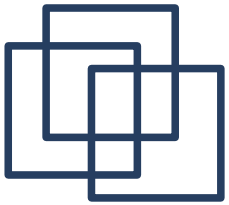
- Los puertos se utilizan para conectar aplicaciones
- Puertos estándar:
  - HTTP 80
  - DNS 53
  - Telnet 23
  - SMTP 25
  - POP3 110

TCP vs UDP

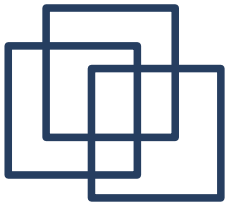
- TCP:
  - Orientado a conexión
  - Fiable
- UDP:
  - No orientado a conexión
  - No fiable

Nombre de dominio

- DNS: Sistema de nombres de dominio
- Base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio
- Asignación de nombres de dominio a direcciones IP
- Componentes:
  - Clientes DNS
  - Servidores DNS
  - Zonas de autoridad



Criptografía



¿Que es la criptografía?

Arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos

Criptografía básica

Código César: Cambiar cada letra del alfabeto por otra:

A->D

B->E

C->F

D->G

Ejemplo:

Esta es una frase sin cifrar

Hvwd hv xqd iudvh vlq fliudu

Autenticación, Integridad, Confidencialidad

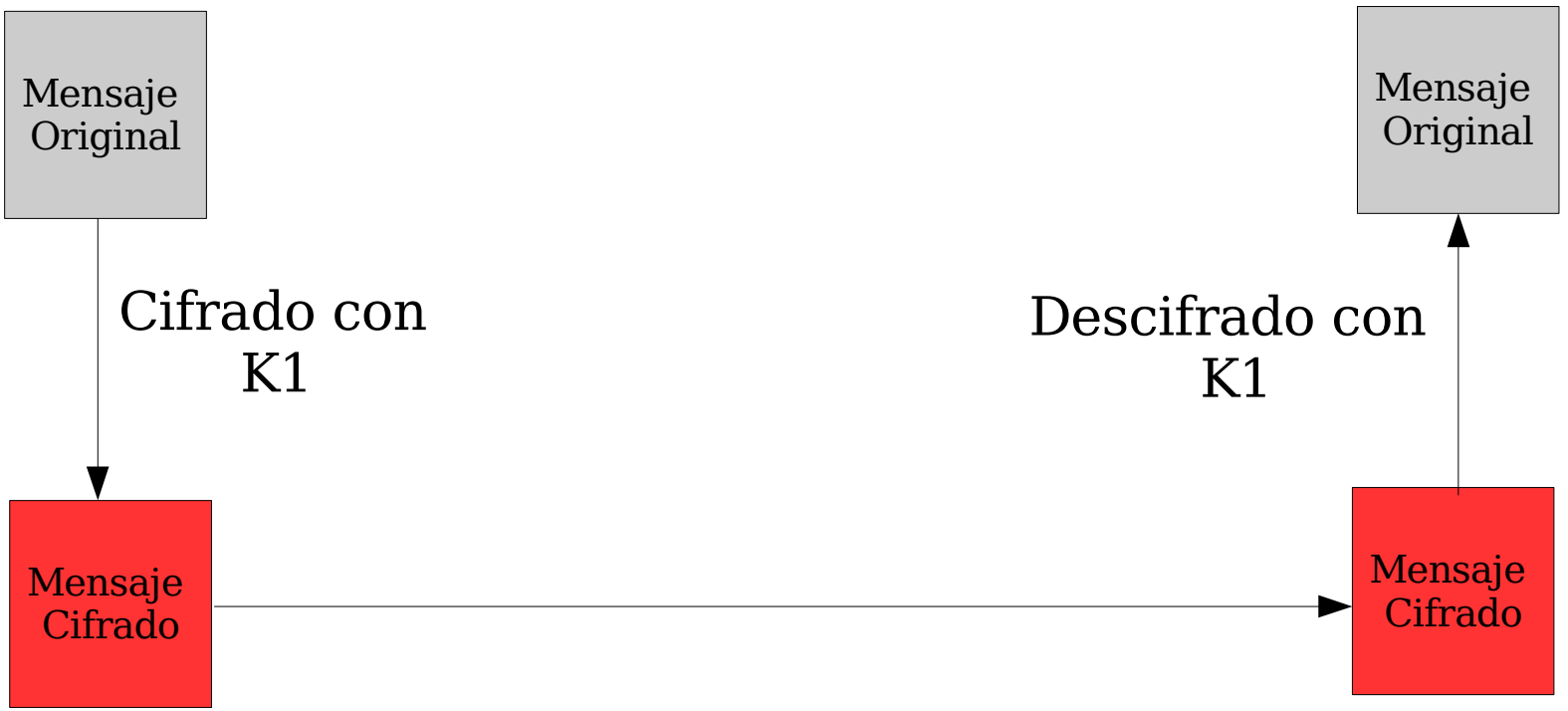
Autenticación: La autenticación es un servicio de seguridad que permite verificar la identidad. Firma digital

Integridad: Garantizar que la información electrónica recibida no ha sido manipulada.

Confidencialidad: significa garantizar la privacidad de la información

Criptografía simétrica

Consiste en emplear la misma clave para cifrar y descifrar información



Criptografía asimétrica

- Se dispone de dos claves complementarias
- Una de las claves se hace pública y la otra se mantiene en secreto por parte del propietario del par de claves
- Lo que se cifra con una de las dos claves sólo puede descifrarse con la complementaria y viceversa

Criptografía asimétrica

Caso práctico: GPG

Herramienta para cifrado y firmas digitales

http://www.gnupg.org/gph/es/manual.html

1. Generar par de claves:

   gpg --gen-key

2. Distribuir la clave pública:

   gpg --keyserver pgp.rediris.es --send-key *ID_CLAVE*

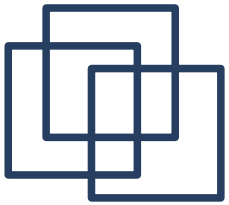
Caso práctico: GPG

3. Importar otras claves públicas:

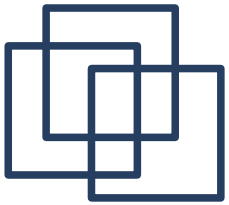
   gpg --keyserver pgp.rediris.es –recv-key *direccion_correo*

4. Configurar el cliente de correo evolution:

   Editar/Preferencias y opción Seguridad al editar la cuenta de correo



Técnicas de Rastreo y Exploración



Técnicas de Rastreos y Exploración

¿Qué es seguir el rastro a un objetivo?

- Un intruso, antes de atacar al objetivo necesita recopilar información sobre él
- Necesita crear un perfil completo de la política de seguridad adoptada por una empresa:

  Nombres de dominio, direcciones IP, servicios TCP/UDP, mecanismos de control de acceso, IDS, enumeración del sistema, nombres de dominio, mecanismos de control de acceso, mecanismos de autenticación, VPN, ...

Seguir el rastro en Internet

- Examinar la página web de la empresa: revisar su código fuente
- Buscar información sobre la empresa en los buscadores
- Buscar mensajes de correo de empleados en listas de correos o grupos de mensajes
- ...

Enumeración de la red

- Whois:

  Protocolo TCP basado en preguntas/repuestas que es usado para consultar de una base de datos para determinar el propietario de un nombre de dominio o una dirección IP en la Internet.

  http://www.allwhois.com o http://www.red.es/

- ¿Dónde está una IP?

  http://www.ip-adress.com/

Interrogaciones DNS

- Si un DNS está configurado de forma insegura es posible obtener información muy relevante sobre la empresa
- Transferencia de zona: solo debería estar permitido a los servidores secundarios. Como obtenerla:

  host -l -v -t any *nombre_dominio* (Probar: *elpais.es*)

- Determinación de los servidores de correo:

  dig mx *nombre_dominio*

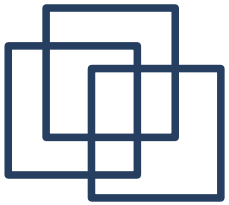
Reconocimiento de la red y su topología previo al ataque

- Determinar la topología de una red:

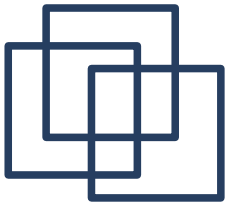
  traceroute

- Más completo:

  cheops



Exploración del objetivo



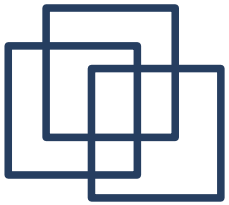
Exploración del objetivo

Seguir el rastro

Merodear en busca de información

Exploración

Palpar las paredes en búsqueda de puertas y ventanas



Exploración del objetivo

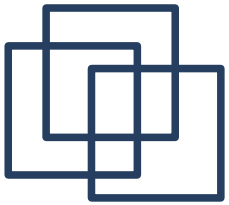
Barridos ping

- ¿El sistema está vivo?
- Consiste en enviar paquetes ICMP ECHO y recibir ICMP REPLY
- ping

  ping www.google.es
- fping (múltiples ping en paralelo):

  fping -g 192.168.1.0/24
- nmap

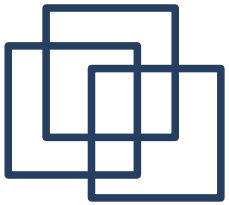
  nmap -sP 192.168.1.0/24



Exploración del objetivo

Exploración de puertos

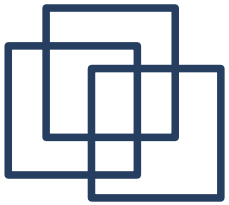
- Proceso de conexión a puertos UDP y TCP del sistema destino para determinar qué servicios se están ejecutando
- Puede determinar qué sistema operativo utiliza
- Puede determinar qué aplicaciones están utilizando
- Esas aplicaciones pueden permitir conectarse a un usuario o pueden tener vulnerabilidades de seguridad conocidas



Tipos de escaneos a realizar sobre el objetivo

El escaneo de puertos se puede realizar de múltiples formas:

- Exploración TCP: conexión completa
- Exploración TCP SYN: Solo TCP SYN y TCP ACK
- Exploración TCP FIN: Solo FIN y RST
- Exploración UDP
- ...



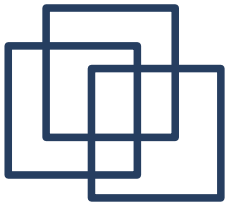
Exploración del objetivo

Detección de los servicios TCP y UDP

- La mejor herramienta para explorar puertos TCP y UDP: nmap

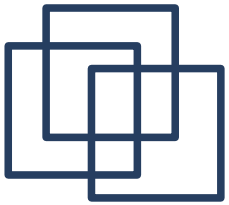
nmap -h

-sT	Puertos TCP
-sU	Puertos UDP
-p puertos	Especificar puertos



Detección del sistema operativo

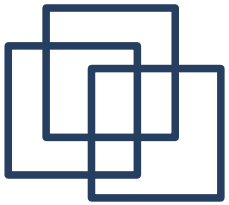
- queso: detección activa
- nmap -O: detección activa
- p0f: detección pasiva, sin enviar paquetes



Exploración del objetivo

Herramientas automáticas de descubrimiento

- cheops: herramienta gráfica de exploración de red que integra:
  - ping
  - traceroute
  - exploración de puertos
  - detección de sistemas operativos



Técnicas de hacking contra los sistemas

Ataques por fuerza bruta

- Itentar adivinar la contraseña de un usuario.
- Habitualmente en los protocolos:

telnet	
FTP	
RSH	
SSH:	Guess-who, brutus
SNMP:	ADMsnmp
POP	
HTTP:	Obiwan III

Engañar a los ficheros de log

- Los ficheros de log registran toda la actividad que ocurre en el sistema
- Un intruso desea borrar sus huellas para no ser detectado:

/var/log/syslog
/var/log/mail.log
/var/log/messages
/var/log/wtmp
~/.bash_history

Desbordamiento de búfer

- Cuando un usuario o proceso intenta introducir en un búfer más datos de los originalmente permitidos
- Son producidos por malas prácticas de programación
- Permiten ejecutar comandos en la máquina

Mala configuración del sistema

- Permisos incorrectos en ficheros binarios
- Usuarios por defecto
- Aplicaciones no actualizadas
- Contraseñas accesibles a los usuarios
- Kernel con bugs graves

Rootkits

- Cuando un intruso consigue comprometer una máquina, la utilizará para instalar un rootkit

- Un rootkit está compuesto de:

  - Troyanos
  - Puertas traseras
  - Sniffers (rastreadores)
  - Limpiadores de registro

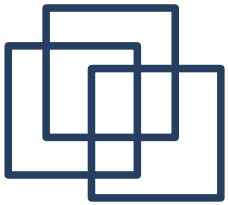
Troyanos

- Programas suplantados para variar su comportamiento
- Por ejemplo:
  - login: para que almacene usuarios/contraseñas
  - ps: para que oculte procesos
  - passwd: para que almacene contraseñas
  - find: para que no encuentre ficheros
  - ...

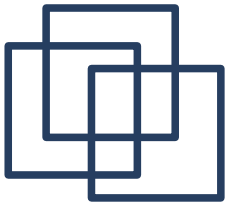
Auditorías de seguridad

- Realizar auditorías de seguridad para detectar vulnerabilidades. Muy completo:

  nessus



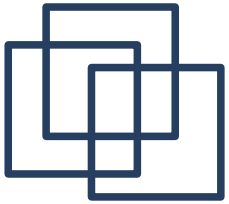
Políticas de usuario y contraseñas



Políticas de usuario y contraseña

Sistema de contraseñas seguro

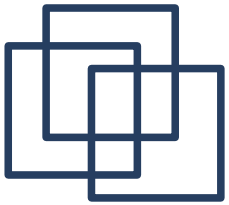
- La longitud de las contraseñas debe ser al menos 6-8 caracteres
- Las contraseñas deben tener letras, números y símbolos
- Las contraseñas se deben cambiar cada poco tiempo
- No se deben usar las mismas contraseñas siempre
- No escribir nunca las contraseñas
- Registrar en el sistema los intentos fallidos de login
- Comprobar periódicamente la validez de las contraseñas del sistema



Métodos para adivinar contraseñas

Las contraseñas se almacenan cifradas y son indescifrables, por tanto se pueden intentar adivinar:

- A partir de listas de palabras
- A partir de un diccionario
- Por fuerza bruta



Políticas de usuario y contraseña

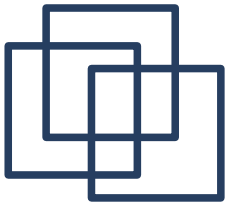
Herramientas de cracking de contraseñas

- Fcrackzip

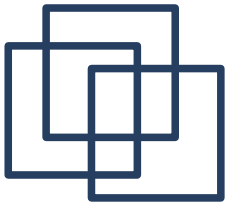
  Adivinar contraseñas de ficheros zip
- Crack

  Adivinar contraseñas del sistema
- Jhon the Ripper

  Uno de los más completos

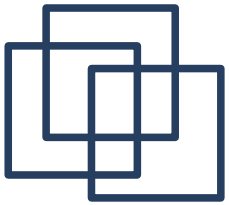


Spoofing



Spoofing

- Según la wikipedia: uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.
- Se puede aplicar a:
  - ARP
  - DNS
  - IP
  - HTTP
  - SMTP
  - ...



Spoofing

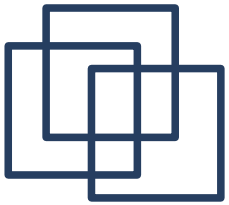
ARP Spoofing

- Suplantación de dirección MAC
- En Linux:

```
ifconfig eth0 down
ifconfig eth0 hw ether 00:00:11:11:22:22
ifconfig eth0 up
```

- Para evitarlo: tablas estáticas ARP:

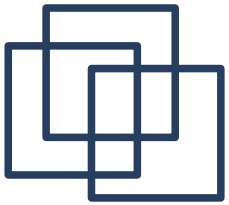
```
arp -s 192.168.1.31 00:ff:ff:33:ff:ff
```



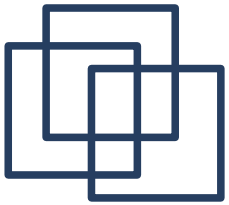
DNS Spoofing

- Responder a preguntas DNS haciéndose pasar por el servidor de DNS
- Ataques man-in-the-middle

dnsspoof



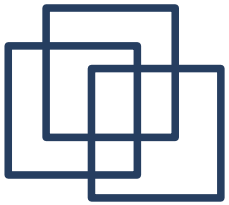
Cortafuegos



Cortafuegos

¿Qué es un cortafuegos?

- Elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red
- Tipos:
  - De capa de red
  - De aplicación
  - De usuario

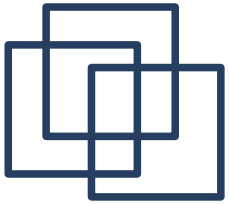


Cortafuegos

Iptables

- Conjunto de herramientas del kernel de Linux que sirve para interceptar y manipular paquetes de red

- Consiste en la definición de unas reglas para especificar como filtrar los paquetes que pasan por una máquina



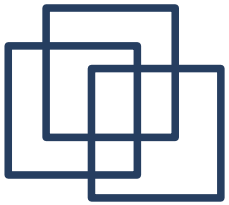
Iptables

- Se encarga de filtrar los siguientes paquetes:

INPUT: paquetes destinados al propio sistema

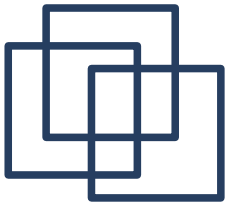
OUTPUT: paquetes creados por el sistema

FORWARD: paquetes que pasan a través del sistema

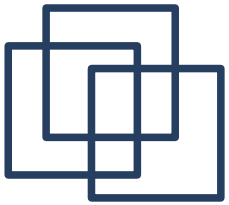


Uso de iptables

http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall-html/



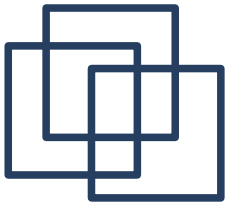
Sniffers



Sniffers

¿Qué es un sniffer?

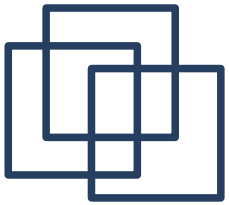
- Programa de captura de las tramas de red
- Se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.
- Útil en entornos de medios compartidos
- Tarjeta de red en modo promiscuo



Sniffers

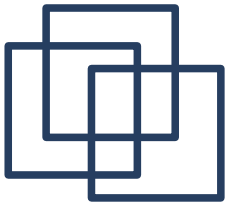
Sniffers genéricos

- tcpdump
- ethereal
- ettercap



Sniffers específicos

- dsniff: Contraseñas de diversos protocolos
- mailsnarf: Correo electrónico
- msgsnarf: Mensajes de clientes de mensajería
- urlsnarf: URLs
- filesnarf: ficheros de NFS



Sniffers

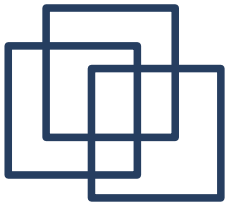
- **Protocolos seguros vs no seguros**

  Protocolos no seguros = protocolos no cifrados:

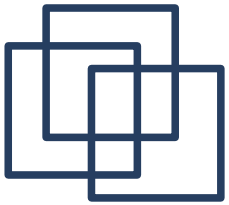
  telnet, ftp, pop3, ...

  Protocolos seguros = protocolos cifrados:

  ssh, scp, pop3s, ...



Redes inalámbricas



Redes inalámbricas

Componentes

- Puntos de acceso
- Estaciones

Topologías

- Ad-Hoc: estación a estación
- Infraestructura: punto de acceso con estaciones

Seguridad

- SSID: Nombre de la red, es necesario conocerlo para conectarse
- Control de acceso por MAC: filtrado por las direcciones MAC de las estaciones
- WEP: comprime y cifra los datos que se envían a través de las ondas de radio. Utiliza el algoritmo RC4 y una clave secreta compartida.
- WEP es vulnerable a ataques para adivinar la clave compartida por medios estadísticos

WPA

- Cambia las claves dinámicamente
- Vector de inicialización más grande, análisis estadísticos más complejos
- Mejora la integridad, ya que no se puede alterar el mensaje sin ser percibido como en WEP

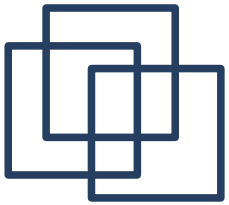
Adivinar contraseña WEP

- Capturar tráfico:

  airodump

- Adivinar contraseña WEP:

  aircrack



Sistemas de detección de intrusiones

Detector de Intrusiones de Red (NIDS)

Busca detectar anomalías que inicien un riesgo potencial, tales como ataques de denegación de servicio, escaneadores de puertos o intentos de entrar en un ordenador, analizando el tráfico en la red en tiempo real. Para ello, analiza todos los paquetes, buscando en ellos patrones sospechosos

Ejemplo: snort

Detector de Intrusiones de Hosts (HIDS)

Sistema de detección de intrusos en un Host. Busca detectar anomalías que indican un riesgo potencial, revisando las actividades en la máquina (host). Puede tomar medidas protectoras

Ejemplo: tripwire