Conceptos tratados en clase

- [**D]DoS**: ataque (distribuído) de denegación de servicio.
- **Zombie**: pc's que tras haber sido infectados por algún tipo de malware, pueden ser usadas por una tercera persona para ejecutar actividades hostiles.
- **Botnet**: conjunto de bots que se ejecutan de manera autónoma y automática. Normalmente para fines perversos.
- **MITM (man in the middle)**: El enemigo adquiere la capacidad de leer, insertar y modificar a voluntad los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.
- **Spoofing**: Técnica de suplantación de identidad generalmente con usos maliciosos o de investigación.
- **Hash**: Función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc...
- **Colisiones en hash**: Dos entradas distintas a una función de hash producen la misma salida. Se soluciona aumentando la dimensión del dominio de las imágenes de dicha función.
- **DMZ**: zona desmilitarizada, se trata de separar la parte de red accesible desde el exterior (más vulnerable a ataques) de la parte interna de la organización, que puede salir a internet pero NO recibe conexiones.
- **Honeypots**: se trata de atraer ataques configurando a propósito un sistema vulnerable y estudiar las acciones de los atacantes para así mejorar la política de seguridad.
- **ID[P]S**: sistema de detección (y prevención) de instrusiones. Se configuran colocando sondas a través de la red.
- **Firewalls state-full**: no solo filtran el tráfico de red con reglas sencillas sino que, además, analizan tráfico sospechoso y también lo filtran (por ejemplo un paquete ACK sin haber conexión).
- **Idle scan**: scaneo mediante un zombie.
- **Decoy scan**: hacer creer al atacado que el scan se está haciendo desde otros hosts.
- **Hardening**: proceso de securizar un sistema
- **Tampering**: interceptar y modificar paquetes.
- **LTOs**: Linear Tape-Open
    - LTO-1: 100 GB
    - LTO-2: 200 GB
    - LTO-3: 400 GB
    - LTO-4: 800 GB
    - LTO-5: 1,6 TB
    - LTO-6: 3,2 TB
    - LTO-7: 6,4 TB
    - LTO-8: 12,8 TB
- **RAID**: Redundant array of independent disks
    - **Lineal**: Crea un disco "virtual" con varios. Inútil, propenso a fallos.
    - **0** o **Stripping**: accesos y escrituras en paralelo. No aporta redundancia
    - **1** o **Mirroring**: duplicación total, doble de espacio necesario. Ojo con la

controladora, también puede interesar duplicarla.
    - **5**: El más común. Paridad distribuída entre los discos.
    - **10**: Un RAID 0 sobre dos RAID 1.
    - **01**: Un RAID 1 sobre dos RAID 0.
- **Clúster**: conjunto de equipos íntimamente relacionados.
- **NFS, Samba**: compartición de sistemas de ficheros en red.
- **SAN**: Storage Area Network, red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte.
- **Global File System (GFS), MogiFS**: sistemas de ficheros distribuídos.
- **HA**: alta disponibilidad.
- **Autenticación**: ¿quién eres?
- **Control de acceso**: ¿qué puedes hacer?
- **Confidencialidad**: conseguida por medio del cifrado (lo contrario a usar telnet, ftp, etc)
- **Integridad de datos**: no modificados ni borrados.
- **No repudio**: impedir que algo o alguien pueda negar que haya recibido “x” información o que no ha hecho “y” cosa.
- **SSL, TLS**: Secure Sockets Layer, Tansport Layer Security. Comunicaciones cifradas a nivel de transporte.
- **VPN**: Virtual Private Network, comunicaciones seguras.
- **md5, sha[1, 2, 3]**: funciones hash.
- **DES, 3DES, AES, blowfish, IDEA**: algoritmos de cifrado simétricos.
- **RSA, DSA, Diffie-Hellman**: algoritmos de cifrado asimétricos.

Herramientas interesantes

- **hping3**: Utilizado para mandar paquetes “personalizados” y visualizar respuestas de otros hosts. Escaneo de puertos.
- **scapy**: Una herramienta para personalizar paquetes de red.
- **ADM DNS Spoofing**
- **nmap**: Herramienta para analizar la red (puertos abiertos, fingerprinting...)
- **xprobe2**: Fingerprinting. Activo (mediante paquetes enviados, no mediante análisis de tráfico de red, como los pasivos).
- **pads**
- **ettercap**: sniffing de red
- **SANCP**: log de conexiones de red.
- **bastille-linux, grsecurity**: hardening.
- **zenmap**: interfaz envoltorio de nmap, muy útil.
- **Fiddler, tamper data**: tampering.
- **networkminer**: captura de todo tipo de información en la red.
- **Thor**: red para navegar anónimamente.
- **Port-security**: implementado por los dispositivos Cisco. Se trata de tener una “white-list” de macs conectables a cada puerto del dispostivio y bloquear (e incluso informar al

administrador del intento fallido) a las demás
- **arpalert, arpwatch, darpwatch, xarp**: herramientas contra el ARP Spoofing (usado para el sniffing).
- **Interfaz de red en modo promiscuo**: captura TODO el tráfico que pasa por la red.
- **rootkit**: Herramienta o un grupo de ellas, que tiene como finalidad esconderse a sí misma y esconder otros programas, procesos, archivos, etc...
- **MAC duplicating**: duplicar la MAC del otro equipo, sniffing.
- **slowloris**: script escrito en perl útil para realizar un D[D]oS sobre un servidor apache, existen soluciones como el plugin “mod_evasive” para blindarnos contra él.
- **medusa, thc-hydra y ncrack**: password guessing.
- **Paquete acct**
    - **ac**: estadística sobre usuarios
    - **lastcomm**: información sobre los últimos comandos utilizados
    - **sa**
    - **last, lastb**: últimos usuarios logeados
- **sysstat**: herramienta básica de monitorización de múltiples aspectos
- **NUT**: sistema para gestionar los sistemas UPS (SAI)
- **Tivoli**: software de backup, de IBM.
- **quota**: cuotas de disco.
- **/etc/security/limits.conf**: cuotas de procesos, memoria...
- **fail2ban, denyhosts, blocksshd o sshdfilter**: contra Medusa, THC Hydra... detecta e impide ataques por fuerza bruta (iptables, cuidado con los ataques con IP Spoofing para hacerlos filtrar lo que no debemos)
- **Fibre Channel**: raid entre equipos remotos.
- **mdadm**: gestión de RAIDs en sistemas Unix.
- **rsync**: utilidad para sincronizado entre equipos.
- **sshfs**: exportación y montaje de sistemas de ficheros de forma cifrada.
- **mon**: monitorización de servicios
- **heartbeat**: interrogación entre hosts.
- **Linux Virtual Server (LVS)**: tipo de clúster con balanceo de carga a nivel IP.
- **reverse proxy**: útil para el balanceo de carga a nivel de aplicación-servicio.
- **ldirectord**: monitorización de servicios HTTP y HTTPS
- **GnuPG (GPG)**: cifrado asimétrico (clave pública y privada). Nivel de aplicación
- **OpenVPN**: implementacion de un sistema VPN.

Escaneo de puertos

- **Si mandamos un paquete SYN a un puerto, posibles respuestas**:
    - SYN/ACK: está abierto
    - RST/ACK: está cerrado
    - No hay respuesta: host apagado o firewall desechando paquetes

Conexiones TCP

- **Conexión**
  - [1] SYN
  - [2] SYN/ACK
  - [1] ACK
- **Intercambio de datos**
  - [1] Manda paquete
  - [2] ACK de ese paquete
- **Finalización de conexión**
  - [1] FIN, ACK
  - [2] ACK
  - Termina de mandar datos si quiere.
  - [2] FIN
  - [1] ACK

Protección contra “sniffing”

- **Detección**
  - IDS, IPS, sensores... integrados en dispositivos a nivel de red.
  - Port span: “mirroring” entre puertos

Estándares

- **ISO27001**: gestión de la seguridad de la información.
- **ISO27002**: buenas prácticas en seguridad.

Puertos

- **21**: FTP
- **23**: TELNET
- **25**: SMTP
- **53**: DNS
- **63**: WHOIS
- **80**: HTTP
- **110**: POP3
- **123**: NTP

- **514**: SYSLOG

Clasificación de criptosistemas

- **Clásicos - modernos**
- **Bloque** (DES, 3DES, AES) **- Flujo** (RC4)
- **Simétricos** (clave secreta) **- Asimétricos** (clave pública)