# UD3 – Seguridade Perimetral e Acceso Remoto

# UD3 – Elementos Básicos da Seguridade Perimetral

- A seguridade perimetral é o primeiro obstáculo que se atopa un atacante remoto, e consiste en:
  - Filtrar a información que entra na rede (permitindo ou denegando o acceso)
  - Analizar e prever as posibles intrusións (mediante tests de penetración)
  - Utilizar técnicas seguras no funcionamento (cifrado, firma)

**A seguridade perimetral é o conxunto de hardware e software utilizado para protexer unha rede de outras redes nas que non se confía**

# UD3 – Elementos Básicos da Seguridade Perimetral

- **Router fronteira:** E o router que permite o acceso da rede a zona externa, debe encargarse das comprobacións de seguridade no trafico de entrada e saída (filtrado)
- Os router fronteira traballan maioritariamente co protocolo **BGP** (Border Gateway Protocol) que escolle a ruta a seguir para acadar o destiño.
- Os elementos de seguridade máis importantes son as devasas (firewall), VPN, os servidores proxy e a configuración de DMZ con arquitectura forte ou débil.
- Un bastión é unha equipa especialmente protexida que está máis exposto ao exterior.

# UD3 – Defensa en Profundidade

- O concepto de defensa en profundidade fai referencia a establecer múltiples liñas de defensa (firewalls, aplicacións actualizadas, contrasinais seguras, segmentación de usuarios, permisos e acls, control físico do acceso…)
- E esencial o aseguramento do perímetro da rede, porque é a que está exposta directamente a posibles ataques dende o exterior

# UD3 – A DMZ

- A DMZ (DeMilitarized Zone) e a zona da rede accesible dende o exterior
- A DMZ pretende que a existencia dun servizo vulnerable non comprometa a seguridade da rede completa
- A conexión dende os equipos da DMZ e a rede interna debería estar moi controlada e limitada a equipos específicos.
- Servizos típicos nunha DMZ son o e-mail a web e o DNS
- Si temos un único firewall que xestiona a conexión á DMZ e protexe a rede interna se denomina Arquitectura débil
- Si temos dous firewall diferenciados para a rede interna e para a DMZ se denomina Arquitectura forte
- Algúns routers permiten redirixir todo o tráfico externo a ún único equipo, denominado “default host” ou “DMZ host”
- O establecemento de DMZ e un tipo de **segmentación de redes,** que consiste no fraccionamento dunha rede física en varias redes lóxicas independentes, de modo que cada segmento sexa unha subrede aillada segundo a política de segmentación elexida.
- A segmentación se pode facer mediante firewalls, ACL e VLAN

# UD3 – O Firewall

- Un firewall é un sistema que se sitúa entre dúas redes e permite filtrar o trafico da rede impedindo o acceso ou redirixindo o tráfico.
- Para realizar o filtrado ten en conta:
  - A procedencia
  - O destiño
  - O protocolo
  - O contido
- Podemos clasificalos en: Firewall de capa de rede e transporte (ip, mac e protocolo) e firewalls de aplicación (proxy).
- Un firewall NON:
  - Non analiza o tráfico cifrado
  - Aínda que existen firewall con funcionalidade de autenticación non é a súa función
  - Aínda que poden ter funcionalidade de antivirus non é a súa función
  - Non detecta intentos de intrusión nin analiza o patróns de ataque (é función do IDS/IDPS)
  - Non controla os ataques de enxeñería social, spam ou correos maliciosos
- Podemos falar tamén de firewall persoal e de firewall de rede

# UD3 – Port Knocking e SPA

- Un firewall permite protexer unha rede de accesos a servizos que non queremos que estén dispoñibles, pero os servizos que necesitamos quedan expostos, polo que sin dúbida serán atacados.
- Unha alternativa é o port-knocking. Esta técnica consiste nunha secuencia secreta de conexións que fará que o firewall abra un porto durante un tempo.
- O port-knocking e vulnerable a ataques DoS. Un equipo coa ip de orixe falsa se pode interpoñer na secuencia de knocking impedindo o acceso.
- SPA (Single Packet Access) soluciona este problema mendiante o envío dun paquete de datos cifrado. O servidor SPA detecta o paquete e fai que o firewall abra o porto especificado.

# UD3 – Os proxy

- Un proxy é un sistema que se sitúa entre dúas partes nunha comunicación entre dúas aplicacións.
- Os proxys permiten:
  - A comunicación entre dúas partes non conectadas directamente
  - A filtraxe da comunicación cos aplicación e o control de acceso
  - O balanceo de carga distribuindo as peticións entre múltiples servidores
  - A filtraxe do contido e detección de malware
- Podemos falar de:
  - Proxy directo – O obxectivo é o control dos clientes no acceso ao servizo.
  - Proxy inverso – O obxectivo é o acceso a servidores inaccesibles e o reparto de carga
  - Proxy caché – O obxectivo é o almacenamento en caché da información reducindo a carga dos servidores e acelerando o acceso.

# UD3 – Acceso Remoto (RAS)

- Un servidor de acceso remoto permite a conexión e traballo remoto en unha rede local.
- Debe empregar protocolos de acceso seguro
- Debe utilizar autenticación segura
- Os protocolos seguros utilizados hoxe en día son:
  - IPSec: Consiste nun conxunto de protocolos que proporcionan seguridade aos paquetes ao nivel de rede creando paquetes confidenciales e autenticados. Pode funcionar en modo túnel ou transporte.
    - Modo transporte: Non protexe a cabeceira IP, protexe a carga útil que se encapsula no nievel de rede. Se utiiliza na comunicación de ordenador a ordenador.
    - Modo túnel: Cifra o paquete completo.
  - SSL/TLS: Consiste nun conxunto de protocolos de seguridade no nivel de transporte, principalmente SSL (Secure Sockets Layer) e TLS (Transport Layer Security). Estos protocolos proporcionan servicios de seguridade extremo a extremo para aplicacións que utilian TCP
    - Ofrecen: Autenticación mutua, integridade e cifrado da información
    - TLS é similar a SSL pero con características de seguridade mellorada
  - Tanto IPSec (OpenSWan,StrongSwan) como SSL/TLS (OpenVPN) son básicas na creación de VPN.

# UD3 – SSH, Túneis SSH e Proxy SSH

- SSH é unha utilidade de acceso remoto segura que permite:
  - Asegurar a autenticidade do servidor
  - Asegurar a autenticidade do cliente
  - Autenticación mediante chave criptográfica ou mediante password
  - Protexer a información cifrando todo o tráfico
- Entre os subsistemas que ofrece podemos citar:
  - SSH
  - SCP
  - SFTP
  - SSHFS
- SSH permite:
  - Acceso remoto
  - Execución remota de comandos
  - Execución remota de scripts locais
  - SSH multiplexing, evitando múltiples inicios de sesión
  - Túneis SSH
  - Túneis SSH inversos
  - Creación de Proxy SOCKSv5

# UD3 - VPN

- Unha VPN permite a conexión segura de clientes remotos a redes locais de xeito que poden acceder aos recursos da rede local como si estiveran conectados a ela directamente.
- Habitualmente están baseadas en IPSec ou SSL/TLS.
- Podemos citar entre as máis habituais:
  - OpenVPN
  - Wireward
  - StrongSwan
  - OpenSwan

# UD3 – Servicios de Escritorio Remoto

- Os servicios de escritorio remoto (VDI) proporcionan acceso a un escritorio que se está a executar nun equipo remoto. Os principais protocolos utilizados son:
  - RDP
  - XDCMP
  - X2GO
  - VNC
- LTSP (Linux Terminal Server Project) pretende facilitar a administración proporcionando nun único servidor sistemas que serán utilizados remotamente mediante equipos de pouca potencia

# Prácticas

- Tuneis SSH e proxy Socks
- Servicio SPA
- OpenVPN – Montaxe dunha VPN