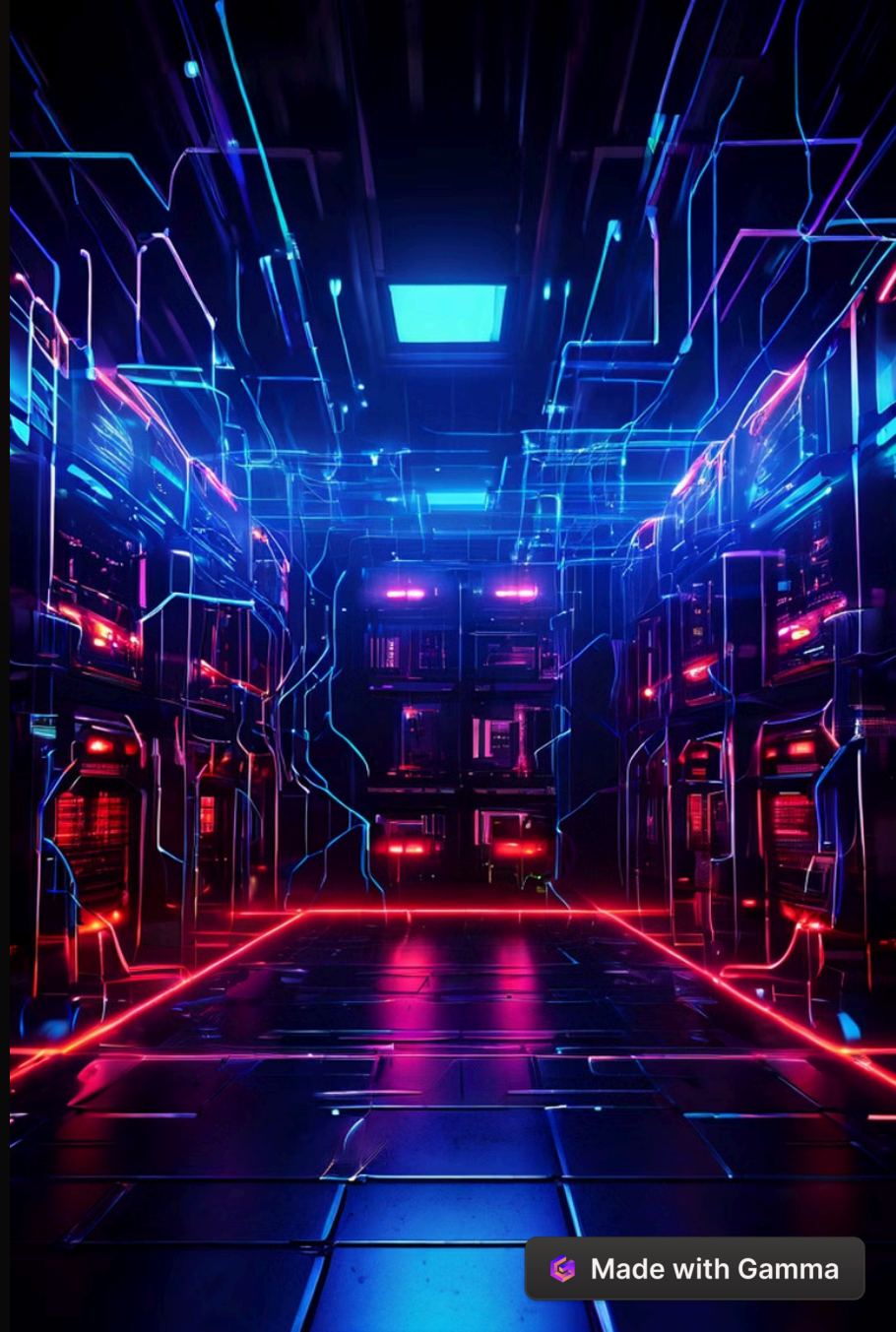
Seguridad en Redes: Reconocimiento y Protección

Bienvenidos a nuestra presentación sobre seguridad en redes. Exploraremos técnicas de reconocimiento y protección contra amenazas cibernéticas comunes.



Introducción a Nmap

Herramienta de Escaneo

Nmap es una utilidad de código abierto para descubrimiento de redes y auditoría de seguridad.

Versatilidad

Puede determinar hosts activos, servicios, sistemas operativos y vulnerabilidades en una red.

Uso Ético

Es fundamental utilizarlo de manera responsable y con autorización previa.

Tipos de Escaneo con Nmap

TCP SYN Scan

Escaneo sigiloso que no completa las conexiones TCP.

OS Fingerprinting

Detecta el sistema operativo del objetivo mediante análisis de paquetes.

UDP Scan

Identifica puertos UDP abiertos en el sistema objetivo.

Análisis de Vulnerabilidades con Nmap

1

Detección de Servicios

Nmap identifica servicios en ejecución y sus versiones.

2

Scripting Engine

NSE permite ejecutar scripts para detectar vulnerabilidades específicas.

3

Reportes Detallados

Genera informes completos sobre las vulnerabilidades encontradas.

Protección Contra Ataques de Fuerza Bruta

Definición

Los ataques de fuerza bruta intentan adivinar contraseñas probando múltiples combinaciones.

Riesgos

Pueden comprometer cuentas de usuario y acceder a sistemas sin autorización.

Técnicas de Protección Contra Ataques de Fuerza Bruta

Contraseñas Robustas

Implementar políticas de contraseñas fuertes y complejas.

Autenticación Multifactor

Añadir una capa adicional de seguridad más allá de las contraseñas.

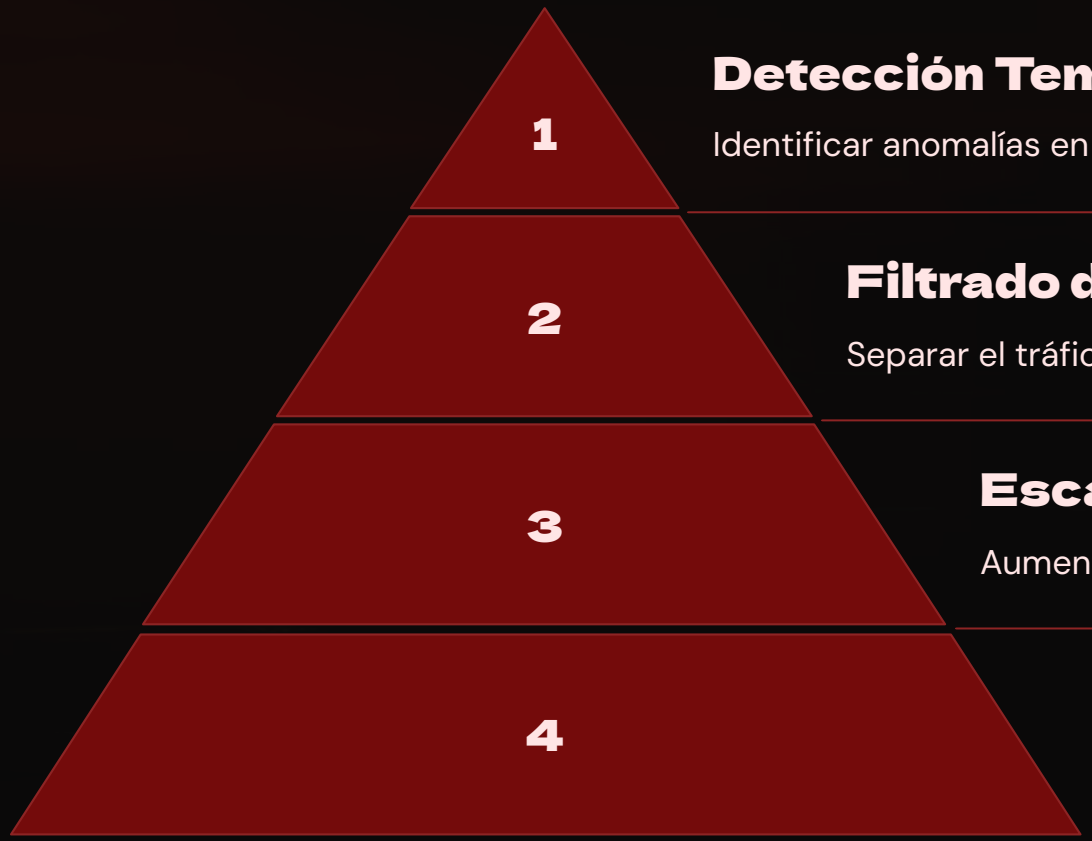
Bloqueo de Cuentas

Limitar intentos fallidos de inicio de sesión.

Monitoreo de Logs

Analizar registros para detectar patrones de ataque.

Protección Contra Ataques DDoS



Detección Temprana

Identificar anomalías en el tráfico de red.

Filtrado de Tráfico

Separar el tráfico legítimo del malicioso.

Escalabilidad de Recursos

Aumentar capacidad de servidores durante ataques.

Respuesta Coordinada

Colaborar con ISPs y servicios de mitigación.

Estrategias de Mitigación de Ataques DDoS

1

Configuración de Firewalls

Establecer reglas para bloquear tráfico sospechoso.

2

Balanceo de Carga

Distribuir el tráfico entre múltiples servidores.

3

Servicios en la Nube

Utilizar CDNs y servicios de mitigación DDoS.

4

Planificación de Contingencia

Desarrollar y probar planes de respuesta a incidentes.

Protección Contra Spoofing de IP

1

Autenticación de Origen

Verificar la legitimidad de las direcciones IP de origen.

2

Filtrado de Paquetes

Implementar reglas para bloquear direcciones IP falsificadas.

3

Encriptación

Utilizar protocolos seguros como IPsec para las comunicaciones.

4

Monitoreo Continuo

Vigilar el tráfico de red en busca de anomalías.

Medidas de Seguridad Contra el Spoofing de IP




La implementación de estas medidas refuerza significativamente la seguridad de la red contra ataques de spoofing de IP.