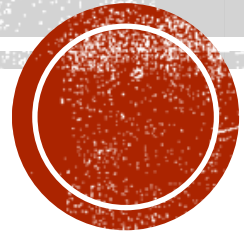
RECONOCIMIENTO

M. Sc. RuBen Fanola Quino

SEG-261 – HACKING ÉTICO 1



¿QUÉ ES EL RECONOCIMIENTO?

Reconocimiento (Information Gathering)

Es la **primera fase del Ethical Hacking**, donde se recopila información del objetivo para:

- Comprender su infraestructura
- Identificar posibles debilidades
- Preparar el ataque o las pruebas de penetración

El objetivo es **saber lo máximo posible antes de actuar**, reduciendo riesgos y mejorando la eficacia del análisis.

¿QUÉ ES FOOTPRINTING?

Es el proceso metodológico de **trazar el perfil de seguridad** de una organización.
Incluye recopilar información sobre:

- Dominios
- Redes
- Sistemas y Aplicaciones
- Usuarios
- Tecnologías utilizadas
- Políticas de seguridad

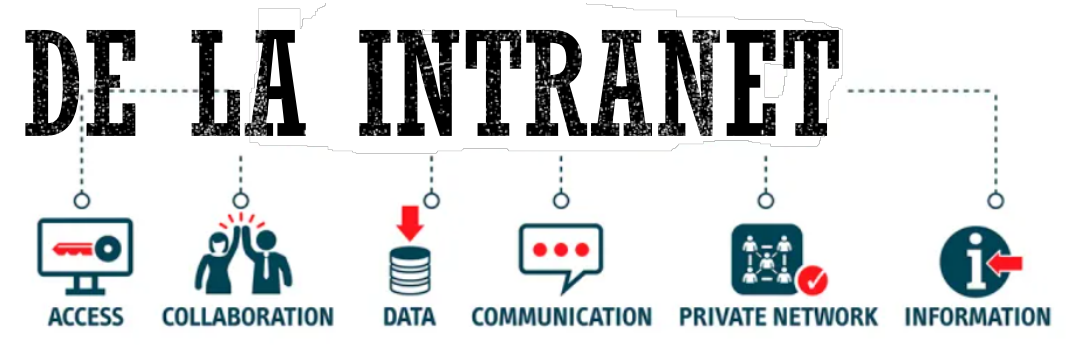
👉 **El 90% del tiempo de un atacante se invierte en Footprinting, solo el 10% se usa para atacar.**

INFORMACIÓN QUE SE BUSCA DESDE INTERNET

Internet:

- Nombre de dominio/ Servidores DNS/ Ubicación geográfica
- Bloques de red públicos
- IPs Publicas expuestas/ VPN
- Servicios TCP/UDP abiertos
- Arquitectura de sistemas
- ACLs y reglas de seguridad/ IDS/IPS visibles
- Credenciales de usuario/ Correos electrónicos y teléfonos
- Enumeración básica de sistemas (usuarios, grupos, versiones, rutas, SNMP)

INFORMACIÓN DENTRO DE LA INTRANET



Intranet:

- Protocolos de red internos
- Dominios internos
- Rango de direcciones IP
- Puertos y servicios internos
- Arquitectura de servidores
- ACL internas/ IDS/IPS internos
- Normativas
- Enumeración interna de sistemas y servicios

ACCESO REMOTO

Acceso remoto

- Redes WiFi corporativas
- Acceso mediante VPN
- Servicios expuestos para teletrabajo
- Escritorios remotos
- Acceso remoto por software de terceros

METODOLOGÍA DEL RECONOCIMIENTO

Pasos de la Metodología:

1. Obtener información inicial (empresa, dominio, contactos)
2. Identificar rangos de red
3. Descubrir máquinas activas
4. Identificar puertos abiertos
5. Determinar sistemas operativos
6. Detectar servicios asociados a los puertos
7. Mapear la red completa

TIPOS DE RECOPILACIÓN DE INFORMACIÓN

- **Pasiva:** Obtención de información **sin interactuar directamente** con el objetivo. No deja rastros y es prácticamente indetectable.

  Google Hacking, *Shonda, Maktego.*

- **Semi-Pasiva:** El analista interactúa **mínimamente** con el objetivo, simulando tráfico normal. Tiene bajo riesgo de detección.

  FOCA, Wireshark, TCPdump

- **Activa:**Interacción **directa y evidente** con el objetivo. Proporciona información precisa, pero puede generar alertas.

  Nmap, Metasploit, DNSrecom.