**Informe de Reconocimiento y Planificación Red Team**

----------------------

**1. Introducción**

El objetivo de este informe es documentar las acciones realizadas y los resultados obtenidos durante el ejercicio de reconocimiento y planificación para evaluar la seguridad de la empresa **SHEIN**, cumpliendo con los requerimientos de la práctica. Este análisis incluye la identificación de activos críticos, enumeración de sistemas autónomos, rangos de red, dominios y subdominios, además de evaluar configuraciones de seguridad y posibles vectores de acceso.

----------------------

**2. Metodología**

El proceso seguido se estructuró en cinco fases principales:

1. **Selección de la empresa objetivo:**
   * **SHEIN** fue seleccionada debido a su importancia en el comercio electrónico global.
2. **Investigación previa:**
   * Recolección de información pública mediante herramientas automatizadas y consultas manuales.
3. **Identificación de activos:**
   * Enumeración de nombres, sistemas autónomos, rangos de red, dominios y subdominios relacionados.
4. **Análisis técnico:**
   * Evaluación pasiva y activa limitada para identificar configuraciones de seguridad y posibles vectores de acceso.
5. **Planificación del ejercicio:**
   * Definición de objetivos, alcance y diseño basado en los resultados obtenidos.

----------------------

**3. Herramientas Utilizadas**

El reconocimiento se automatizó mediante un script en **Bash** que ejecutó las siguientes herramientas:

1. **whois:**
   * Para obtener información del registro de dominios, propietarios y rangos de red.
2. **dig y nslookup:**
   * Para consultas DNS y validación de servidores.
3. **curl:**
   * Para analizar cabeceras HTTP y verificar redirecciones.
4. **nmap:**
   * Para escaneo de puertos y detección de servicios activos.
5. **nikto:**
   * Para evaluación de configuraciones de seguridad web.
6. **sqlmap:**
   * Para análisis básico de vulnerabilidades en formularios SQL (limitado por configuración del objetivo).

**Automatización:** Todas las herramientas fueron ejecutadas mediante un script en Bash, y los resultados fueron organizados automáticamente en una carpeta estructurada para facilitar el análisis.

----------------------

**4. Planificación**

4.1 **Objetivos**

Identificar y priorizar activos críticos relacionados con **SHEIN**.

Evaluar configuraciones y servicios para identificar vectores de acceso potenciales.

Documentar riesgos y proponer recomendaciones de mitigación.

4.2 **Alcance**

1. **Reconocimiento pasivo:**
   * Uso de herramientas como whois, nmap y nikto para evitar interacciones agresivas.
2. **Enumeración activa limitada:**
   * Escaneo de puertos y servicios para comprender la infraestructura básica.

4.3 **Diseño**

1. **Automatización del proceso:**
   * Script en Bash para ejecutar herramientas y almacenar resultados.
2. **Estructuración de datos:**
   * Resultados organizados en directorios y archivos para cada subdominio.
3. **Priorización en servicios críticos:**
   * Análisis detallado de HTTP/HTTPS y DNS.

----------------------

**5. Identificación de Activos**

5.1 **Nombres / Empresas Incluidas**

* **Empresa matriz:** SHEIN.
* **Empresas relacionadas:**
  + ROMWE: Marca de comercio electrónico vinculada.
  + ZZKKO: Productos relacionados dentro del ecosistema SHEIN.

5.2 **Sistemas Autónomos**

* Infraestructura gestionada por **Amazon Web Services (AWS)**.
* Detalle de sistemas autónomos:
  + NetRange: 52.0.0.0 - 52.79.255.255.
  + CIDR: 52.64.0.0/12 y 52.0.0.0/10.

5.3 **Rangos de Red**

Organización: Amazon Technologies Inc.

Rangos asignados: CIDR mencionados previamente.

5.4 **Dominios**

* **Dominio principal:** shein.com.
* **Servidores DNS:**
  + NS-1253.AWSDNS-28.ORG.
  + NS-1991.AWSDNS-56.CO.UK.
  + NS-398.AWSDNS-49.COM.
  + NS-893.AWSDNS-47.NET.

5.5 **Subdominios Analizados**

Se analizaron 10 subdominios principales, seleccionados por su relevancia para el ecosistema de **SHEIN**:

[www.shein.com](http://www.shein.com)

shein.de

shein.co.uk

shein.mx

shein.fr

shein.ca

sheingsp.com (Wildcard)

romwe.com

shein.com.cn

shein.in

----------------------

**6. Enumeración y Análisis Técnico**

6.1 **Enumeración Pasiva y Activa**

1. **Enumeración pasiva:**
   * Uso de whois y consultas DNS (dig, nslookup) para identificar servidores y rangos.
   * Análisis de registros y configuraciones AWS.
2. **Enumeración activa limitada:**
   * Escaneo con nmap para detección de puertos y servicios activos.
   * Evaluación de configuraciones HTTP con nikto y curl.

6.2 **Resultados Generales**

1. **Puertos y servicios detectados (nmap):**
   * 80/tcp: HTTP (OpenResty).
   * 443/tcp: HTTPS (OpenResty).
2. **Cabeceras HTTP (curl):**
   * Respuesta 301 (redirección a <https://www.shein.com>).
   * Servidor identificado: OpenResty.
3. **Análisis web (nikto):**
   * Falta de cabeceras de seguridad críticas:
     + Strict-Transport-Security (HSTS).
     + Content-Security-Policy (CSP).
     + Referrer-Policy.
     + X-Content-Type-Options.

----------------------

**7. Análisis Individual por Subdominio**

Se documentan las configuraciones, servicios y cabeceras de seguridad de cada subdominio analizado.

1. **[www.shein.com](http://www.shein.com)**
   * Puertos abiertos:
     + 80/tcp: HTTP (OpenResty).
     + 443/tcp: HTTPS (OpenResty).
   * Cabeceras faltantes: HSTS, CSP, X-Content-Type-Options.
   * Redirección hacia https://shein.com.
2. **shein.de**
   * Sin puertos abiertos detectados.
   * Sin respuesta del servidor.
3. **shein.co.uk**
   * Puerto abierto: 443/tcp (HTTPS).
   * Redirección hacia https://shein.co.uk.
4. **shein.mx**
   * Puertos abiertos: 80/tcp y 443/tcp.
   * Redirección a https://www.shein.com.
5. **shein.fr**
   * Sin puertos abiertos.
   * Sin respuesta directa.
6. **shein.ca**
   * Puerto abierto: 443/tcp.
   * Cabeceras faltantes: Referrer-Policy, CSP.
7. **sheingsp.com (Wildcard)**
   * Subdominio wildcard gestionado por AWS.
   * Sin puertos accesibles.
8. **romwe.com**
   * Puertos abiertos: 80/tcp y 443/tcp.
   * Falta de cabeceras críticas: HSTS, CSP.
9. **shein.com.cn**
   * Sin puertos abiertos detectados.
   * Sin respuesta del servidor.
10. **shein.in**
    * Puerto abierto: 443/tcp.
    * Falta de cabeceras críticas: CSP, Referrer-Policy.

----------------------

**8. Riesgos Identificados**

1. **Cabeceras de seguridad faltantes:**
   * Riesgos de ataques MITM, XSS y contenido mixto.
2. **Dependencias en AWS:**
   * Superficie de ataque ampliada por configuraciones cloud.
3. **Configuraciones de HTTP/HTTPS:**
   * Uniformidad en configuraciones incrementa el impacto potencial.

----------------------

**9. Recomendaciones**

1. **Configurar cabeceras de seguridad:**
   * Implementar HSTS, CSP, Referrer-Policy y X-Content-Type-Options.
2. **Asegurar configuraciones en AWS:**
   * Revisar políticas de acceso y roles.
3. **Auditoría periódica de subdominios:**
   * Monitorear configuraciones y servicios regionales para garantizar la seguridad.