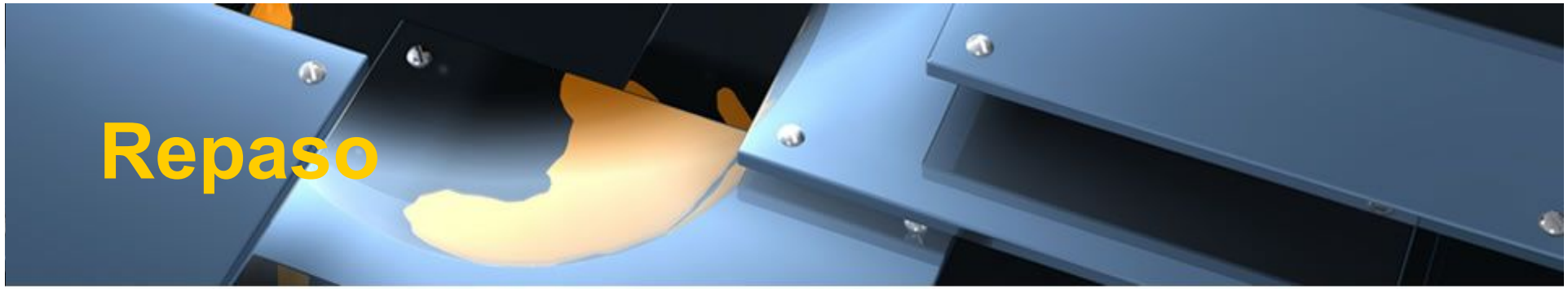


Repaso

- Etapas del hackeo ético

Metodología para las Pruebas de penetración

- De forma sensilla las prubas de penetración, PenTest se componen principalmente de 4 fases. Aunque es cierto que las fases pueden tener modificaciones en cuanto al orden y contenido dependiendo del método utilizado. Las fases básicas del Pentest son:

1. Recopilación de información.
2. Busqueda de vulnerabilidades.
3. Explotación de vulnerabilidades.
4. Generación de informes y/o parcheo de los sistemas.

Metodología para las Pruebas de penetración

- Basado en lo anerior el proceso de hackeo ético ha de realizarse aplicando una metodología de trabajo para que el estudio se haga de manera lógica y ordenada. Se conocen varias técnicas siendo las siguientes Open Source las mas adoptadas:

- OSSTMM (Manual de Metodología Abierta de Evaluación de Seguridad).
  - http://www.isecom.org/research/osstmm.html
- ISSAF (Marco de Evaluación de Seguridad de Sistemas de Información).
  - http://www.oissg.org/issaf.html
- PTES (Penetration Testing Execution Standard). en versión Beta mayo 2014
  - http://www.pentest-standard.org/index.php/Main_Page
- OWASP (Proyecto de Seguridad de Aplicaciones Web Abiertas). Con información un poco antigua
  - https://www.owasp.org

Metodología para las Pruebas de penetración

- EC-Council Empresa pionera y con muy buen posionamiento y varias certificaciones
  - http://www.eccouncil.org/
- ISCC/ISC2 Empresa con varias certificaciones y textos.
  - https://www.isc2.org/
- Mile2 Empresa con muchas certificaciones en seguridad.
  - http://www.mile2.com/
- Además hay otras compañias con una metoología y certifiaciones relacionadas con la seguridad, Cisco, Cmptia, etc.

Consideraciones sobre la metodología

- Existen varias metodologías tanto por instituciones comerciales como organizaciones sin fines lucrativos, en donde una combinación podría ser óptima par el tipo de pruebas que e desean realizar. Ver metodología sugerida por ISSAF.
- Ejemplo: Página 30 de http://www.oissg.org/files/issaf0.2.1B.pdf
- Diagrama: http://www.pentest-standard.org/index.php/Intelligence_Gathering

- Debido a que las vulnerailiades son corregidas es necesario actualizar las herramientas que se utilizan y entender que a veces la vulneabilidad ya no está presente
- Además muchas herramientas en línea y para descarga son descontinuadas, por lo que es muy aconsejable utilizar más de una.

Importancia de la lectura y actualización

- Buscar y leer sobre vulnerabilidades es muy conveniente para los profesionales en seguridad. Ejemplo de hertblee (SSL)
- http://www.elladodelmal.com/2014/04/heartbleed-y-el-caos-de-seguridad-en.html

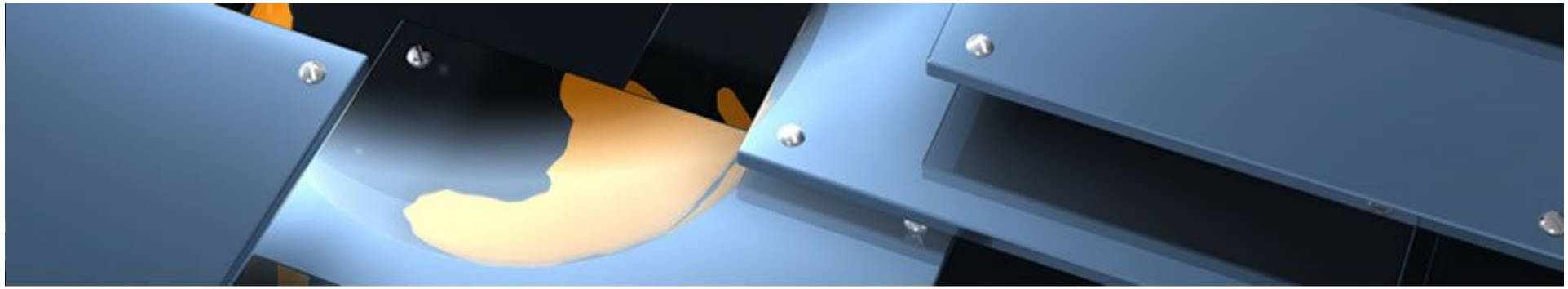
- Ejemplo de SETpara Facebook.

Herramientas para el reconocimiento

- Utilizar el sitio de SVNET, para el responsable y si ya no hay algún sitio descontinuado http://www.svnet.org.sv/
  - Sitios: DNSCook.net, http://whois.domaintools.com/, http://www.dnsstuff.com/,
  - Comandos: nslookup, dig (Linux), dnsenum --enum empresay.com.sv (kali)
- Nos interesa la información de IP, otros dominios, si el servidor está en hosting o propio, etc.
  - Crear listado y reporte de DNS

Búsqueda de información en sitios Web

- Analizar información, direcciones físicas, direcciones de correo, búsqueda de sitios de ingreso, servicios en línea, etc.
- Descarga de sitio web:
  - Herramienta: httracker
  - Comando: wget
- Ver cuentas de correo por comando
  - nc -vv mail.empresay.com.sv 25
    - EHLO assesor
    - VRFY usuario1



- Escaneo de equipos, cuentas de correo, direcciones IP
  - Herramientas:
    - Maltego
    - Zenmap
    - Sitio web: t1shopper
  - Comandos: forzar subdominios
    - dnsenum --enum -f -r sitio.com.sv
    - nmap -v -sP 10.10.3.10-35
    - nmap –vv -sS 10.10.3.102
    - nmap –vv -sU 10.10.3.102

Espacio para comentaios o preguntas

Víctor Cuchillac

papá