Pentesting (Penetration Testing)

- Un test de intrusión ou “pentesting” é un método de auditoría que intenta romper a seguridade dun sistema informático para localizar as súas debilidades.
- A mellor forma de facer un test deste tipo é realizar un ataque, polo tanto, un pentesting seguirá as seguintes fases:
  - Contrato
  - Recolección de Información
    - Footprinting
    - Fingerprinting
  - Análise de vulnerabilidades
  - Explotación das vulnerabilidades
  - Xeración de informes

O Contrato

- Resulta legalmente indispensable que se identifiquen claramente os sistemas obxecto do pentesting
- A entidade auditada debe demostrar a titularidade dos sistemas.
- Se deben establecer os mecanismos de notificación e alerta das vulnerabilidades. Normalmente se debe indicar o estándar de pentesting a seguir:
    - ISSAF (Information Systems Security Assessment Framework)
    - PCI DSS (Payment Card Industry Data Security Standard)
    - PTES (Penetration Testing Execution Standard)
    - OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad)
- Debe pactarse quen terá acceso ao informe final e a quen se lle entregará, así como as medidas de seguridade que se deben aplicarse sobre o mesmo.

Recolección de Información

Se debe recoller toda a información posible dos sistemas auditados, tanto para poder realizar as seguintes fases como para comprobar si os sistemas están a fornecer máis información da necesaria. Podemos distinguir entre:

- **Footprinting**: Consiste na obtención de información pública, xa sexa voluntaria ou involuntariamente (DNS, localización IP e rutas, ICCAN, Buscadores...). Existen ferramentas on-line especializadas en footprinting, como ***netcraft***
- **Fingerprinting**: Consiste na obtención da información fornecida polos propios sistemas a partir das pegadas dixitais dos servizos e os sistemas operativos.

Footprinting: DNS

- Os sistemas DNS poden facilitar coñecemento sobre a estrutura da rede atacada:
  - **Transferencias de zona:** Permite obter información sobre a rede e os servizos que ofrece realizando unha transferencia de zona e descargando a base de datos DNS ó completo. Un DNS ben configurado so permite transferencias de zona dende equipos autorizados. (dig e nslookup)
    - O rexistro SOA indica o email do responsable do dominio, cada canto se actualiza o DNS, quen é o dns primario.. etc.
      - dig dns renfe.es
      - dig dns.iesrodeira.com
      - dig dns apache.es
    - Mediante PTR Scanning podemos obter tamén a lista de equipos

Footprinting con dig

- **Obter IP dun HOST:** *dig @dnsserver hostname*
- **Obter o nome dun host pola IP:** *dig -x IP*
- **Obter o servidor de correo:** *dig @dnsserver domainname MX*
- **Traza da resolución de nomes**: *dig hostname -trace*
- **Obter información do SOA:** *dig soa dnsserver*

  En Windows se pode utilizar nslookup, que tamén está dispoñible en Linux. Tamén é posible o uso de ferramentas on-line:

  - *https://centralops.net/co/nslookup.aspx*
  - *https://ping.eu/nslookup*

Footprinting: Posicionamento

- Permite situar xeográficamente os sistemas averiguando a súa ubicación física, e quenes son os seus proveedores de acceso a internet.
  - Traceroute
  - https://gsuite.tools/es/traceroute
  - http://en.dnstools.ch/visual-traceroute.html
  - https://traceroute-online.com/
  - https://visualtraceroute.net/

Footprinting: Whois

Cando unha empresa rexistra o dominio debe facilitar unha serie de datos que deben estar actualizados. Esta información é pública e se rexistra nunha base de datos denominada Whois.

Footprinting: Busqueda dende a web

- Os buscadores indexan continuamente todo tipo de información dispoñible a través dos servizos web, moitas veces sin que os propietarios se decaten, e dispoñen de xeitos de buscar moi útiles, como o operador IP
- Se poden utilizar técnicas de “spidering” para recopilar información. Estas técnicas consisten en recuperar toda a información facilitada polos servizos web da empresa, que se poden analizar posteriormente (https://www.elevenpaths.com/es/labstools/foca-2/index.html)
- Shodané un buscador especializado en buscar dispositivos hardware concretos conectados a rede, facilitando a súa localización, versión de firmware, modelo, fabricante...

Fingerprinting

- O fingerprinting obtén información dos sistemas analizando a información obtida polos servizos ofrecidos e polos sistemas operativos instalados (pegadas dixitais). Unha boa práctica de seguridade é reducir no posible as pegadas dixitais dos distintos servizos.
  - nmap / zenmap
  - netcat

Busca de Vulnerabilidades

- Unha vez localizados os servizos, sistemas operativos e as súas versións, comeza a exploración das posibles vulnerabilidades.

- Para facer isto se utilízanse os reportes de seguridade (como securityfocus, secunia ou CVE) e os escáneres de vulnerabilidades

https://www.securityfocus.com/
https://community.flexera.com/t5/Secunia-Advisories/ct-p/advisories
https://cve.mitre.org

Escáneres de Vulnerabilidades

- Un escáner de vulnerabilidades é unha aplicación que explora os sistemas de xeito automático en busca de debilidades.
- Os máis avanzados realizan varios pasos do pentesting, como o fooprinting, fingerprinting, busca de vulnerabilidades, explotación e elaboración de informes.
- Utiliza bases de datos de vulnerabilidades públicas ou propias.
- Permiten obter unha completa información dos sistemas instalados e os servizos que ofrecen indicando as posibles debilidades.

Algúns escáneres de vulnerabilidades

- Nessus (https://es-la.tenable.com/products/nessus)
- OpenVas (software libre, baseada en un principio en Nessus)
- NeXpose (https://www.rapid7.com/products/nexpose/)
- Metasploit (https://www.metasploit.com/)