THE BRIDGE

CYBER SECURITY

Explotación

Fases del Pentest

https://reportdefense.com/services/

Metodologías

- **OWASP**
  - Es para mejorar la seguridad del software a través de sus proyectos de software de código abierto liderados por la comunidad, cientos de capítulos en todo el mundo, decenas de miles de miembros y organizando conferencias locales y globales.
  - https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

Web Application Security Testing

4.0 Introduction and Objectives

4.1 Information Gathering

4.2 Configuration and Deployment Management Testing

4.3 Identity Management Testing

4.4 Authentication Testing

4.5 Authorization Testing

4.6 Session Management Testing

4.7 Input Validation Testing

4.8 Testing for Error Handling

4.9 Testing for Weak Cryptography

4.10 Business Logic Testing

4.11 Client-side Testing

https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/

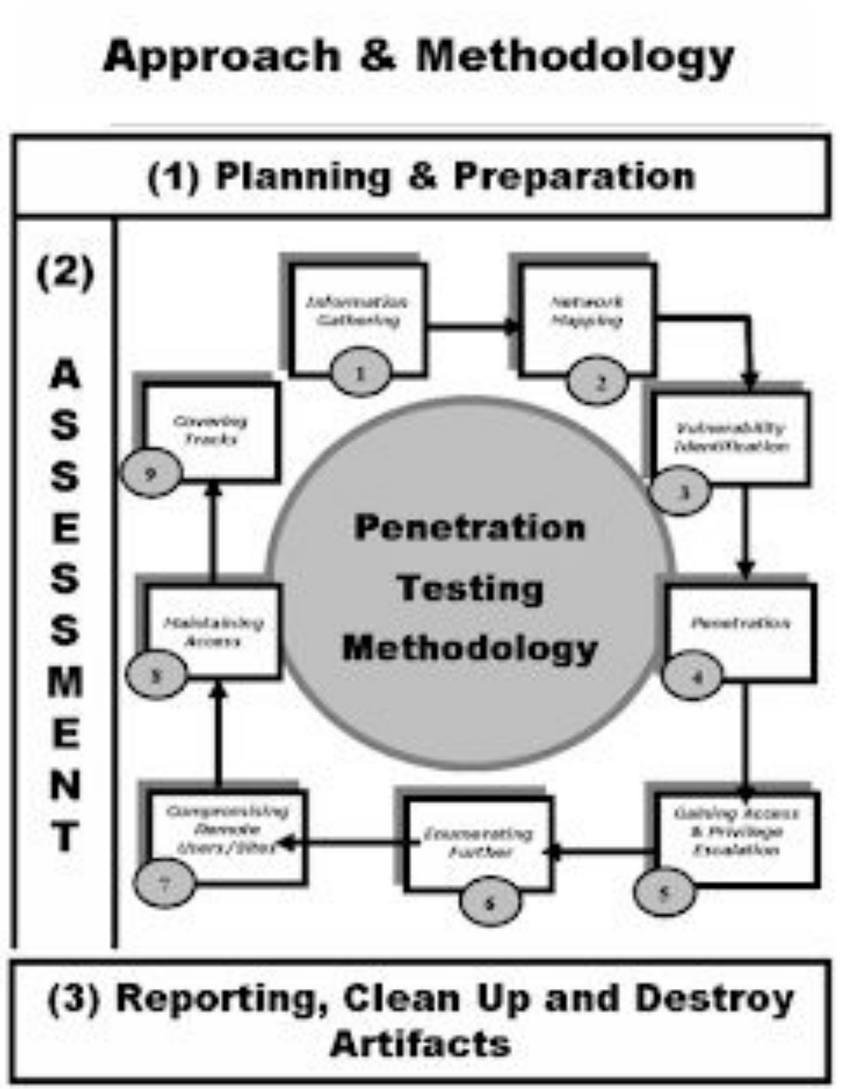
Metodologías

- **OSSTMM**
  - **Manual de la Metodología Abierta de Comprobación de la Seguridad (OSSTMM, Open Source Security Testing Methodology Manual),** estándar profesional utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde Internet.
  - Incluye un marco que describe las fases que habría que realizar para la ejecución de la auditoría.
  - Se ha logrado gracias a un consenso entre más de 150 expertos internacionales sobre el tema, que colaboran entre sí mediante Internet
  - https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

https://www.grantthornton.com.co/globalassets/1.-member-firms/colombia/recursos/tecnology/imagen-5.png

Metodologías

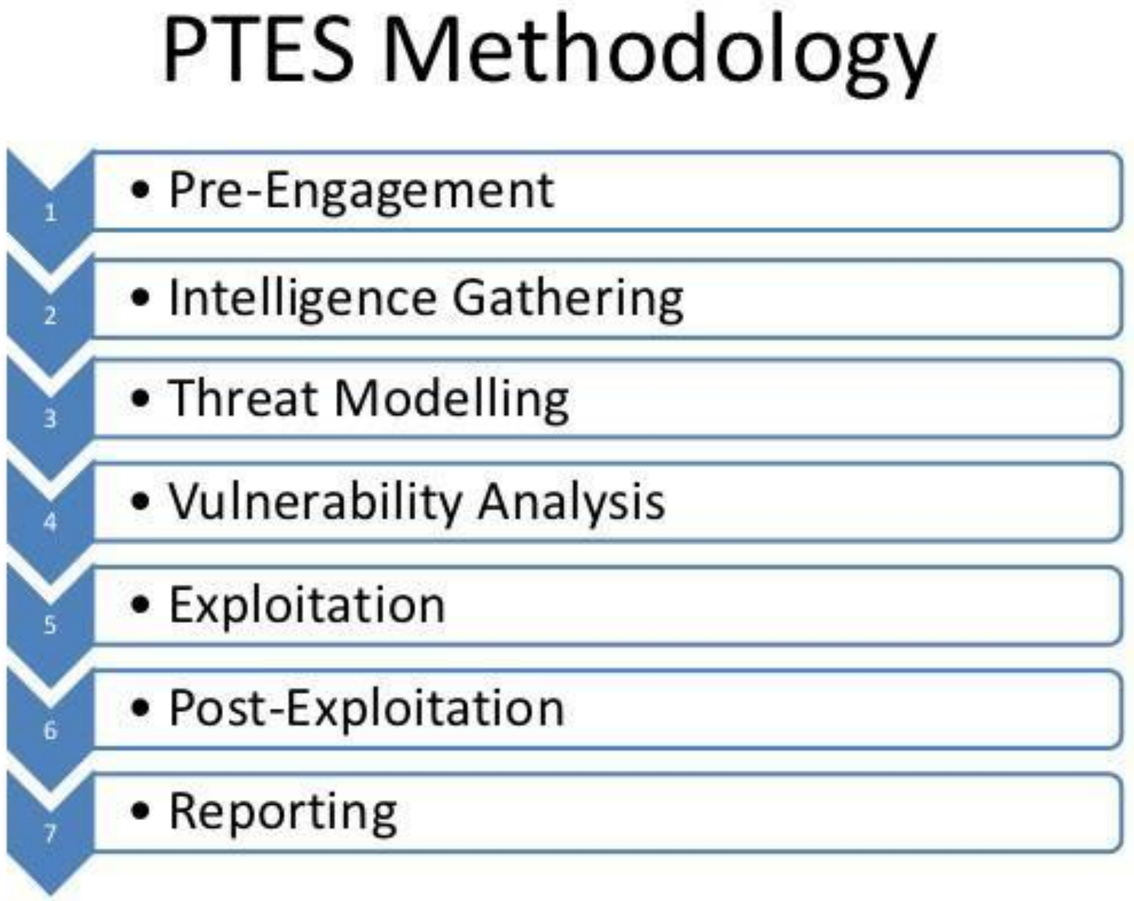
- **ISSAF**
  - La metodología de test de penetración ISSAF esta diseñada para evaluar su Red de trabajo, sistema y control de aplicaciones
  - El pentester imita los pasos de atacante con algunas fases adicionales



http://insecuredata.blogspot.com/2009/04/metodologia-de-test-de-intrusion-issaf.html

Metodologías

- **PTES**
  - El PTES (Metodologías y estándares de prueba de penetración) recomienda un enfoque estructurado para una prueba de penetración.
  - Guía a través de las fases de las pruebas de penetración, comenzando con las fases de comunicación, recopilación de información y modelado de amenazas.



http://cybernews404.blogspot.com/2017/11/learning-module-penetration-tester-guide.html

Metodologías

- **WASC-TC**
  - La clasificación de amenazas de WASC es un esfuerzo cooperativo para aclarar y organizar las amenazas a la seguridad de un sitio web.
  - Los miembros del Consorcio de seguridad de aplicaciones web crearon este proyecto para desarrollar y promover la terminología estándar de la industria para describir estos problemas.
  - Los desarrolladores de aplicaciones, los profesionales de seguridad, los proveedores de software y los auditores de cumplimiento tendrán la capacidad de acceder a un lenguaje y definiciones coherentes para los problemas relacionados con la seguridad web.

https://www.suntechnologies.com/service/security-testing/

Metodologías

- **NIST**
  - El Instituto Nacional de Estándares y Tecnología es una agencia gubernamental no reguladora que desarrolla tecnología, métricas y estándares para impulsar la innovación y la competitividad económica en las organizaciones de la industria de la ciencia y la tecnología con sede en los EE. UU.

  - Como parte de este esfuerzo, NIST produce estándares y pautas para ayudar a las agencias federales a cumplir con los requisitos de la Ley Federal de Administración de Seguridad de la Información (FISMA).

  - También ayuda a esas agencias a proteger su información y sus sistemas de información a través de programas rentables.

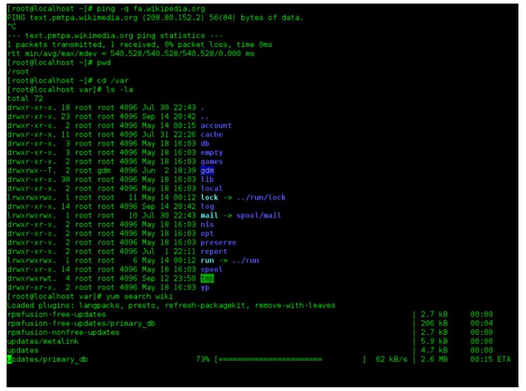
https://www.isecom.org/research.html#content5-9d

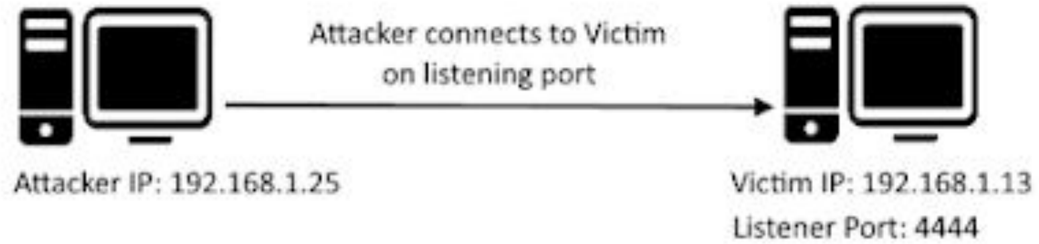
Conceptos

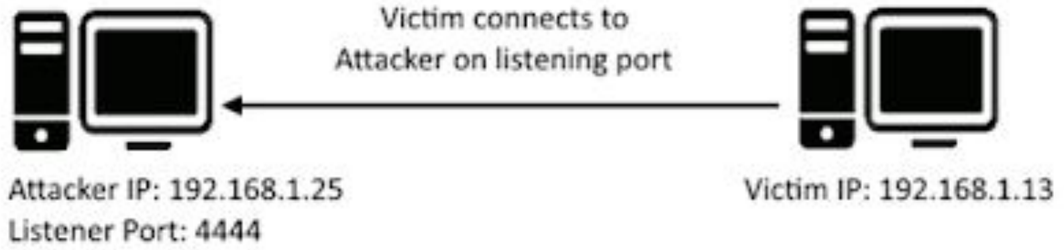
En informática, el shell o intérprete de órdenes o intérprete de comandos es el programa informático que provee una interfaz de usuario para acceder a los servicios del sistema operativo.

- **Tipos de Shell**
  - **Bind shell**
    - La máquina víctima tiene un puerto a la escucha y espera una conexión entrante.
    - La máquina atacante se conecta a la máquina victima a través del puerto que tiene a la escucha.
  - **Reverse shell**
    - La máquina victima se comunica hacia la máquina atacante.
    - La máquina atacante tiene un puerto a la escucha en el cual recibirá la conexión, que va a usar, para lograr la conexión del intérprete de comandos (shell).

Shell







https://segchock.blogspot.com/2018/02/reverse-shell-bind-shell.html

Conceptos

Shellcode

```
section .text
global _start

_start:
    ; execve("/bin/sh", ["/bin/sh", NULL], NULL)
    xor eax, eax            ; EAX = 0
    push eax                ; Poner NULL en la pila
    push 0x68732f2f         ; Poner "//sh" en la pila
    push 0x6e69622f         ; Poner "/bin" en la pila
    mov ebx, esp            ; Mover el puntero de la pila a EBX
    push eax                ; Poner NULL en la pila para argv
    push ebx                ; Poner el puntero a "/bin/sh" en la pila
    mov ecx, esp            ; Mover el puntero de la pila a ECX
    xor edx, edx            ; EDX = 0
    mov al, 0xb             ; syscall number for execve
    int 0x80                ; Llamada al sistema
```

Conceptos

- **Backdoor**
  - Un *backdoor* es una puerta trasera o secreta que permite el acceso remoto de usuarios en los dispositivos.
  - Aunque estas puertas pueden ser utilizadas para fines maliciosos y espionaje no siempre son un error, ya que pueden haber sido diseñadas con la intención de tener una entrada secreta.
  - El modus operandi es el de atacar por los rincones menos vigilados de cualquier ordenador.
  - Los más conocidos son:
    - **Back Orifice**
    - **NetBus**
    - **SubSeven.**
  - **Netcat** puede ser empleada para abrir puertas traseras así como emplearla para protegerse de ellas.

https://arstechnica.com/gadgets/2021/03/hackers-backdoor-php-source-code-after-breaching-internal-git-server/


THE
BRIDGE