28-7-2025

Glosario de la materia

Universidad Tecnologica de Cancun.

Leslie Lopez

1. **Nmap:** Herramienta de código abierto que permite escanear puertos, descubrir dispositivos y detectar servicios en una red.
2. **Wireshark**: Programa que captura y analiza el tráfico de red en tiempo real. Muestra paquetes y protocolos que se están transmitiendo.
3. **SYN Scan (-sS):** Tipo de escaneo en el que se envía un paquete SYN para detectar si un puerto está abierto. También se le llama stealth scan.
4. **Connect Scan (-sT):** Escaneo TCP completo que establece una conexión real (SYN → SYN-ACK → ACK). Es más fácil de detectar.
5. **UDP Scan (-sU):** Escaneo que utiliza el protocolo UDP para identificar puertos abiertos, común en servicios como DNS o SNMP.
6. **RST (Reset):** Bandera (flag) en TCP que indica que una conexión debe ser terminada inmediatamente. Se usa cuando un puerto está cerrado.
7. **ACK (Acknowledge):** Bandera en TCP que indica aceptación de datos previos o una respuesta a un SYN.
8. **SYN (Synchronize):** Bandera TCP que inicia una solicitud de conexión. Es el primer paso del "handshake" TCP.
9. **Puerto abierto**: Puerto que acepta conexiones; hay un servicio activo escuchando.
10. **Puerto cerrado**: Puerto que rechaza conexiones (responde con RST+ACK).
11. **Puerto filtrado**: Puerto que está protegido por un firewall; no hay respuesta o hay un mensaje ICMP indicando bloqueo.
12. **ICMP:** Protocolo de red usado para enviar mensajes de control o errores (como “puerto no alcanzable”).
13. **Port Unreachable:** Mensaje ICMP que indica que un puerto UDP no está disponible.
14. **Stealth (furtivo):** Técnica de escaneo diseñada para evitar ser detectada por firewalls o sistemas de monitoreo.
15. **-p**- : Opción en Nmap que le indica escanear todos los puertos del 1 al 65535.

16. **Mutillidae II:** Aplicación web vulnerable diseñada para prácticas de seguridad y hacking ético.
17. **XAMPP:** Paquete que incluye Apache, MySQL, PHP y phpMyAdmin para desarrollo local.
18. **Htd**ocs: Carpeta en XAMPP donde se colocan los proyectos web para ser accesibles vía navegador.
19. **index.php:** Archivo principal de inicio para aplicaciones PHP. Apache lo carga por defecto.
20. **.htaccess:** Archivo de configuración usado por Apache para controlar accesos o comportamientos en carpetas.
21. **Require all granted:** Directiva moderna de Apache (2.4+) que permite el acceso a todos los usuarios.
22. **Order Deny,Allow / Allow from:** Directivas antiguas (Apache 2.2) usadas para controlar acceso por IP.
23. **phpMyAdmin:** Interfaz web para gestionar bases de datos MySQL/MariaDB.
24. **MySQL :** Sistema de gestión de bases de datos usado por Mutillidae.
25. **Unknown database:** Error que indica que la base de datos especificada no existe.

26. **reset-db.php:** Script incluido en Mutillidae para crear y poblar la base de datos automáticamente.
27. **database-config.inc:** Archivo de configuración donde se definen las credenciales de conexión MySQL.
28. **Mysqli:** Extensión de PHP usada para conectarse y manejar bases de datos MySQL.
29. **select_db():** Función PHP que selecciona una base de datos después de conectar.
30. **localhost ó 127.0.0.1:** Ambas apuntan a la máquina local, pero pueden comportarse diferente en MySQL.
31. **Root:** Usuario administrador por defecto en MySQL.
32. **Contraseña vacía ('')**: En XAMPP, el usuario root normalmente no tiene contraseña por defecto.
33. **my.ini:** Archivo de configuración de MySQL que puede incluir el puerto (ej. 3306 o 3307).
34. **Docker :** Plataforma que permite crear contenedores, los cuales aíslan aplicaciones (como Mutillidae) con su propio entorno. Es útil para pruebas de seguridad sin comprometer el sistema anfitrión.
35. **Contenedor Docker:** Instancia en ejecución de una imagen Docker. Es un entorno encapsulado con todo lo necesario para ejecutar una aplicación.
36. **User-Agent:** Cadena que el navegador o cliente envía al servidor para identificarse. Se usó como una "contraseña secreta" para mostrar información solo a usuarios específicos.
37. **Phishing:** Técnica de engaño que simula páginas legítimas para robar credenciales u otra información sensible. En este caso, el archivo websell.php simula una página de inicio de sesión.
38. **Burp Suite:** Herramienta de seguridad utilizada para pruebas de penetración en aplicaciones web. Permite interceptar, modificar y analizar tráfico HTTP/S entre el navegador y el servidor.
39. **Community Edition:** Versión gratuita de Burp Suite con funciones básicas para pruebas de seguridad.
40. **Professional Edition:** Versión de pago de Burp Suite con funciones avanzadas como escaneo automático de vulnerabilidades.
41. **Java:** Lenguaje de programación requerido para ejecutar Burp Suite. Debe estar instalado en tu sistema (versión 17 o superior).
42. **java -version:** Comando que permite verificar la versión de Java instalada en tu sistema.
43. **Proxy:** Intermediario entre el navegador y el servidor. Burp Suite actúa como proxy para capturar y modificar el tráfico.
44. **Interceptación:** Funcionalidad de Burp para pausar y modificar solicitudes HTTP/S antes de que lleguen al servidor o al navegador.
45.