Proyecto Investigativo

Routers laboratorios de redes e infraestructura

- ISR 4321 SEC/K9.
- CISCO2901/K9
    - https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-25107/Cisco-2901-Integrated-Services-Router.html
- CISCO1841
    - https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-28416/Cisco-1841-Integrated-Service-Router.html
- CISCO2911/K9
    - https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-25106/Cisco-2911-Integrated-Services-Router.html

Idea básica de la explotación de vulnerabilidades en routers:

La explotación del router funciona infringiendo la seguridad de Wi-Fi del mismo, omitiendo la página de inicio de sesión administrativa y accediendo a las funciones administrativas. Un atacante experto puede entonces atacar el firmware existente que ejecuta el enrutador en una práctica llamada "root kitting", en la que se coloca un firmware personalizado en el enrutador para habilitar funciones maliciosas avanzadas.
En Kali lInux existe una herramienta llamada **Medusa** que permite otorga a un usuario múltiples funcionalidades que le permiten a este explotar las vulnerabilidades de un router. Es muy similar a Hydra pero es más poderosa ya que permite multihilos. Osea que se pueden vulnerar varios routers al mismo tiempo.

RouterSploit

Es un framework para la explotación de vulnerabilidades en routers que sirve en Kali. Está diseñado específicamente para ***embedded devices.***
Consiste de tres módulos principales:
- exploits: Contiene una lista de todos los exploits disponibles públicamente.
- creds: Se usa para probar logins en diferentes dispositivos.
- scanners: Se usa para chequear una exploit particular en un dispositivo particular.

https://subscription.packtpub.com/book/networking_and_servers/9781787121829/3/ch03lvl1sec42/exploiting-routers-with-routersploit

Aircrack-ng

Aircrack-ng es una de las mejores herramientas inalámbricas para hackear contraseñas para el crackeo WEP/WAP/WPA2 utilizado en todo el mundo.

Nessus

Nessus es una herramienta de escaneo remoto que puedes usar para verificar las vulnerabilidades de seguridad de los ordenadores.

THC Hydra

THC Hydra utiliza el ataque de fuerza bruta para crackear prácticamente cualquier servicio de autenticación remota. Admite ataques rápidos de diccionario para más de 50 protocolos, incluidos ftp, https, telnet, etc.

John the Ripper

John the Ripper es otra herramienta popular de cracking utilizada en la comunidad de pruebas de penetración (y hacking). Inicialmente fue desarrollado para sistemas Unix, pero ha crecido para estar disponible en más de 10 distros.

Metasploit Framework

Metasploit Framework es un marco de código abierto con el cual los expertos y equipos de seguridad verifican las vulnerabilidades, así como también realizan evaluaciones de seguridad para mejorar la conciencia de la seguridad.

Nmap ("Network Mapper")

Network Mapper es una herramienta gratuita y de código abierto utilizada por los administradores del sistema para descubrir redes y auditar tu seguridad.

Kismet Wireless

Kismet Wireless
es un sistema de detección de intrusos, detector de red y detector de contraseñas. Funciona predominantemente con redes Wi-Fi (IEEE 802.11) y puede tener su funcionalidad extendida usando complementos.

https://tools.kali.org/vulnerability-analysis/cisco-auditing-tool

https://tools.kali.org/vulnerability-analysis/cisco-global-exploiter