Hacking y seguridad.com

http://www.hackingyseguridad.com/

Auditoria de seguridad, “hacking ético” a

http://www.hackingyseguridad.com/

ÍNDICE

INTRODUCCIÓN

El presente documento pretende servir de guía y ayuda, para la detección de vulnerabilidades, "hacking ético", en auditorias de seguridad.

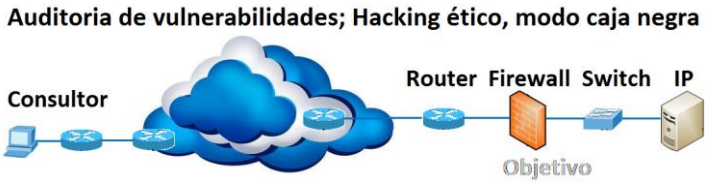
DESCRIPCION DE LAS PRUEBAS, AUDITORIA "HACKING ETICO":

FASE 1 – Recopilación de información y detección de vulnerabilidades:

Identificación del diseño de la solución de red y vulnerabilidades:
Versiones de firmware, S.O, aplicaciones, servicios udp/tcp, web, código, tipos de autentificación o acceso remoto, cifrados y configuraciones.

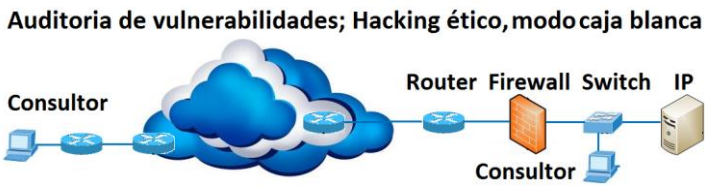
Tipos de auditoria:

Caja negra ó black box: sin información del objetivo:



Caja gris ó gray box: Con credenciales e información previa de tipología de la infraestructura y dispositivos objetivo.

Caja blanca: Con toda la información y acceso a la infraestructura de los sistemas objetivo:



FASE 2.- Pentesting. Simulacion de ataques:

Tests de intrusión a los dispositivos. Batería de ataques y test de estrés; Contramedidas de protección de forma pasiva y activa.

FASE 3 - Informe final:

Informe con pruebas realizadas y detalle de las vulnerabilidades. Mejoras, plan de contingencia y propuestas de reparo, cambios necesario para solucionar los problemas de seguridad detectados.

DESCRIPTCION PRUEBAS HACKING ETICO EN MODALIDAD CAJA NEGRA

FASE 1

1º.- Recopilación de Información de la IP / Objetivo: Whois, dominio, fqdn, blacklist (reputación), responde a ping, trace route, identificación de los posibles equipos hasta el target: balanceadores, Firewall Capa 4, Capa 7 u otros equipos.

Herramientas utilizadas: Comandos: Ping, Tracert, Nslookup, dig, web whois, webs de reputación, buscadores: google, bing, yahoo, censys, shodan.io, etc.

2º.- Modelo equipos y versiones de firmware de los dispositivos, contraste con Base de Datos de vulnerabilidades en CERTSI CVE-20XX-XXXX y revisiones conocidas, documentadas por fabricantes.

Herramientas utilizadas: Scripst Zenmap, BBDD CERTSI, CRT.

3º.- Nmap, para ver los servicios activos (TCP y UDP completo). Servicios necesarios e "innecesarios" abiertos y vulnerabilidades asociadas conocidas sobre éstos.

Herramientas: Scripst Zenmap, nmap de Kali Linux. Censys.

#Ref	Activo	Puerto TCP/UDP	Servicio	Fingerprint	Vuln CVE	Descripción Vuln	Exploit
1							
2							
3							

4º.- Servidores o máquina target: Identificación del Sistema Operativo y versión de las aplicaciones de servicios, además de los módulos y versión que pudiera tener instalado. contraste con Base de Datos de vulnerabilidades en CERTSI CVE-20XX-XXXX y revisiones conocidas, documentadas por fabricantes.

XSS (Si hay alertas relaccionadas en los resultados de los test del punto anterior)

Herramientas: Zenmap, Scripts de Nmap, Kali Linux: nmap, scripts Zenmap, lbd, wafw00f .

5º.- Vulnerabilidades de la propia WEB y código: Lenguajes de programación, estructura de la web, exploración ó escritura en las carpetas, certificados seguros y versiones de cifrado. Formularios, JQuey, librerías y su versión, registro y acceso con credenciales, captcha distintos, límite de intentos de acceso fallidos.

Herramientas: Scripst Zenmap, Wapiti Acunetix, Nesuss, Zap OWASP, OpenVas, Mozilla Firefox.

FASE 2

6º.- Explotación de vulnerabilidades.

SQL Injetion (Si hay alertas en los resultados de los test del punto anterior)
Inyección LDAP (Si hay alertas en los resultados de los test del punto anterior)
Fuerza bruta passwords (Si hay alertas en los resultados de los test del punto anterior)

Inclusión de ficheros LFI y RFI (.php) (Si hay alertas en los resultados de los test anteriores).

7º.- Pentesting. Pruebas de intrusión. Exploit: No aplica. Solo en caso de ser explicitado y requerido.

8º.- Pruebas de Estress: No aplica. Solo en caso de ser explicitado y requerido.

9º.- Batería de ataques. No aplica. Solo en caso de ser explicitado y requerido.

FASE 3

10ª.- Informes finales con:

- I. Resumen de las vulnerabilidades detectadas, ordenadas por grado de criticidad: (alta, media ó baja-informativa).
- II. Evidencias y detalle de las pruebas realizadas y datos sobre cada una de las vulnerabilidades detectadas o explotadas.
- III. Cambios de mejora propuestos. Plan de contingencia.

LISTA DE REVISIONES

Número edición	Fecha edición	Apartados revisados	Cambios efectuados	Observaciones
1ª	25 JUL 2023			

RESUMEN EJECUTIVO:

Web y algunos de elementos que lo componen presenta vulnerabilidades de gravedad media, que requieren atención y debería ser corregido.

Tabla resumen:

#Ref	Activo:	Vulnerabilidad	Gravedad
1	hacking	Fuerza bruta en formulario web de acceso al portal web	Media
2	hacking	Ausencia de cabeceras de seguridad en la configuración del server web	Baja
3	hacking	Renegociación TLS a versiones de protocolos anteriores inseguros: SSLv3	Informativa
4	Hacking	MiTM, Suplantación certificado digital !	Informativa
5	Hacking	Vulnerable a ataques DoS/DDoS de inundación UDP o ICMP, TSPSYN	Informativa

EVIDENCIAS:

ANEXO: