Actividad 02. Uso de la herramienta Nikto

Nikto es un escáner de servidor web de código abierto (GPL) que realiza pruebas exhaustivas contra servidores web para varios elementos, incluidos más de 6700 archivos/programas potencialmente peligrosos, verifica versiones desactualizadas de más de 1250 servidores y problemas específicos de la versión en más de 270 servidores. También comprueba los elementos de configuración del servidor, como la presencia de varios archivos de índice, las opciones del servidor HTTP e intentará identificar los servidores web y el software instalado. Los elementos de escaneo y los complementos se actualizan con frecuencia y se pueden actualizar automáticamente.

Nikto no está diseñado como una herramienta sigilosa. Probará un servidor web en el menor tiempo posible y es obvio en los archivos de registro o en un IPS/IDS. Sin embargo, hay soporte para losmétodos anti-IDS de LibWhisker en caso de que quiera probarlo (o probar su sistema IDS).

No todos los chequeos son un problema de seguridad, aunque la mayoría lo son. Hay algunos elementos que son verificaciones de tipo "solo información" que buscan cosas que pueden no tener una falla de seguridad, pero que el webmaster o el ingeniero de seguridad pueden no saber que están presentes en el servidor. Estos elementos suelen estar debidamente marcados en la información impresa. También hay algunas comprobaciones de elementos desconocidos que se han analizado en los archivos de registro.

Características:

Estas son algunas de las características principales de **Nikto**:

- Soporte SSL (Unix con OpenSSL o quizás Windows con Perl/ NetSSL de ActiveState)
- Soporte completo de proxy HTTP
- Comprobaciones de componentes de servidor obsoletos
- Guarde informes en texto sin formato, XML, HTML, NBE o CSV
- Motor de plantillas para personalizar fácilmente los informes
- Escanee varios puertos en un servidor o varios servidores a través del archivo de entrada (incluida la salida nmap)
- Técnicas de codificación IDS de LibWhisker
- Se actualiza fácilmente a través de la línea de comandos
- Identifica el software instalado a través de encabezados, favicons y archivos
- Autenticación de host con Basic y NTLM
- Adivinar subdominio
- Enumeración de nombre de usuario de Apache y cgiwrap
- Técnicas de mutación para "pescar" contenido en servidores web
- Ajuste de escaneo para incluir o excluir clases enteras de verificaciones de vulnerabilidad
- Adivina las credenciales para los reinos de autorización (incluidas muchas combinaciones de ID / pw predeterminadas)
- La adivinación de autorización maneja cualquier directorio, no solo el directorio raíz

- Reducción mejorada de falsos positivos a través de varios métodos: encabezados,
- contenido de la página y hash de contenido Informa que se han visto encabezados "inusuales"
- Estado interactivo, pausa y cambios en la configuración de verbosidad
- Guarde la solicitud / respuesta completa para las pruebas positivas
- Reproducir solicitudes positivas guardadas
- Tiempo máximo de ejecución por objetivo
- Pausa automática en un momento específico
- Verificaciones de sitios de "estacionamiento" comunes
- Iniciar sesión en Metasploit
- Documentación completa

En los siguientes artículos encontrarás información del uso de la herramienta **Nikto**:

Nikto: un práctico escáner de vulnerabilidades de sitios web

Nikto, escáner de vulnerabilidades para aplicaciones web: así funciona

¿Cómo encontrar vulnerabilidades del servidor web con Nikto Scanner?

En los siguientes vídeos encontrarás información sobre cómo utilizar la herramienta **Nikto**:

Nikto | Escaneo de vulnerabilidades web

PRÁCTICAS CON NIKTO EN KALI LINUX

Cómo usar NIKTO en Kali Linux y Parrot OS #21

Uso de Nikto

PASO 1: Un entorno adecuado para trabajar.

Primero debe contar con una distribución de **Kali Linux** funcionando ya sea en una máquina física o en una máquina virtual.

PASO 2: Instalar el comando.

Una vez que se cuenta con este sistema operativo de manera funcional podemos instalar los comandos; algunos ya vienen preinstalados en la distribución **Kali**, pero si no fuere así puede instalarlos con los siguientes comandos, previamente tomando privilegios de usuario “root”:

```
sudo apt install nikto
```

PASO 3: Realizar análisis.

```
sudo nikto -h 10.0.2.7 -o scan.html -Format htm
```

Escanea el sitio web 10.0.2.7 mostrando en la consola la información del sitio:

```
┌──(kali㉿kali)-[~/hashes]
└─$ sudo nikto -h 10.0.2.7 -o scan.html -Format htm
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.7
+ Target Hostname:    10.0.2.7
+ Target Port:        80
+ Start Time:         2024-05-10 00:22:19 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ /: Retrieved x-powered-by header: ASP.NET.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/
X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differe
nt fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-heade
r/
+ /EEkVl1tq.aspx: Retrieved x-aspnet-version header: 2.0.50727.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2024-05-10 00:25:43 (GMT-4) (204 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Devuelve el resultado en el fichero scan.html en formato html, por lo que se puede visualizar en un navegador.

10.0.2.7 / 10.0.2.7 port 80

Target IP	10.0.2.7
Target hostname	10.0.2.7
Target Port	80
HTTP Server	Microsoft-IIS/7.5
Site Link (Name)	http://10.0.2.7:80/
Site Link (IP)	http://10.0.2.7:80/

URI	/
HTTP Method	GET
Description	/: Retrieved x-powered-by header: ASP.NET.
Test Links	http://10.0.2.7:80/ http://10.0.2.7:80/
References	

URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://10.0.2.7:80/ http://10.0.2.7:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

URI	/
HTTP Method	GET
Description	/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
Test Links	http://10.0.2.7:80/ http://10.0.2.7:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

URI	/xOGQaHrC.asmx
HTTP Method	GET
Description	/xOGQaHrC.asmx: Retrieved x-aspnet-version header: 2.0.50727.
Test Links	http://10.0.2.7:80/xOGQaHrC.asmx http://10.0.2.7:80/xOGQaHrC.asmx
References	

URI	/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
Test Links	http://10.0.2.7:80/ http://10.0.2.7:80/
References	

Se pide:

1. Con la información obtenida en los artículos y vídeos indicados india qué es Nikto y como se utiliza
2. Utilizando Nikto, escanea los siguientes sitios:
    - **bWapp:** http://itsecgames.com/
    - **Metasplotaible2**
    - **Metasplotaible2:8180**
    - **Metasploitaible3**
    - **OWASP Juice Shop**: https://demo.owasp-juice.shop/#/
3. Genera un documento indicando las vulnerabilidades encontradas.