

Práctica de Laboratorio - Análisis de Vulnerabilidades Web

Objetivos

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Iniciar Nikto y realizar un escaneo básico
- Parte 2: Usar Nikto para escanear varios servidores web
- Parte 3: Investigar las vulnerabilidades de los sitios web
- Parte 4: Exportar los resultados de Nikto a un archivo

Aspectos básicos/Situación

Nikto es un escáner de vulnerabilidades web popular que puede encontrar vulnerabilidades de inyección SQL, XSS y otras vulnerabilidades comunes en sitios web. Puede identificar el software instalado mediante encabezados de página y archivos. Nikto admite los protocolos HTTP y HTTPS.

Recursos necesarios

- Kali VM personalizada para el curso de Ethical Hacker
- Acceso a Internet

Instrucciones

Parte 1: Iniciar Nikto y realizar un escaneo básico

Paso 1: Inicie Nikto en Kali Linux.

- a. Inicie sesión en la VM de Kali con el nombre de usuario **kali** y la contraseña **kali**.
- b. Nikto está preinstalado en Kali Linux. Es una herramienta de línea de comandos que se puede iniciar mediante la opción **Application -> Vulnerability Analysis -> nikto** en el menú, o directamente desde la línea de comandos. Para ver el archivo de ayuda, use el comando **nikto --help**.

```
└── (kali㉿Kali)-[~]
    └─$ nikto --help
```

¿Qué opción de comando descubrirá solo las vulnerabilidades de inyección de SQL?

-Tuning+9

```

File Actions Edit View Help
  2 Guess for password file names
  3 Enumerate user names via Apache (/user type requests)
  4 Enumerate user names via cgiwrap (/cgi-bin/cgiwrap/~user type requests)
  5 Attempt to brute force sub-domain names, assume that the host name is the parent domain
  6 Attempt to brute force directory names from the supplied dictionary file
-mutate-options Provide information for mutates
--interactive Disable interactive features
--sslstrip Disables the use of SSL
--nossl Strip trailing slash from URL (e.g., '/index/' to '/admin')
--autohome Directs nikto to guess a 404 page
--option Over-ride an option in nikto.conf, can be listed multiple times
--output Write output to this file ('-' for auto-name)
--port Port to use (default: 80)
--plugins List of plugins to run (default: ALL)
--port* Port to use (default: 80)
--threads* Prepend port value to all requests, format is /directory
--root* Save positive responses to this directory ('.' for auto-name)
--save Force saving to this port
-Tuning-
  1 Interesting File / Seen in logs
  2 Missing/Incorrect Default File
  3 Information Disclosure
  4 Injection (XSS/Script/HTML)
  5 Remote File Retrieval - Inside Web Root
  6 Denial of Service
  7 Remote File Retrieval - Server Wide
  8 Command Execution / Remote Shell
  9 SQL Injection
  0 File Upload
    a Authentication Bypass
    b Session Identification
    c Remote Source Inclusion
    d WebService
    e Administrative Console
  x Reverse Tuning Options (i.e., include all except specified)
-timeout Timeout for requests (default 10 seconds)
--loadbalancing Load balancing across multiple databases
  01 Disable standard db_tests and load only user db_tests
--script Over-ride the default arguments
--until Run until the specified time or duration
--url Target host/URL (alias of --host)
--cookies Use cookies for response and future requests
--proxify Use proxy for connection in nikto.conf, or argument http://server:port
--version Print plugin and database versions
--host Virtual Host (For Host header)
--headers Ignored headers in response body content as negative responses (always). Format is "#H1, #H2".
--destring Ignore this string in response body content as negative response (always). Can be a regular expression.
+ requires a value

```

Paso 2: Realice un análisis básico en scanme.nmap.org.

- Nmap.org tiene un sitio web configurado para probar los escaneos de Nmap. Utilizará este servidor web para realizar su primer análisis de vulnerabilidades. Inicie Firefox y vaya al sitio web <http://scanme.nmap.org>. Lea la descripción del servidor y las restricciones que se le aplican.

¿Qué limitaciones sugiere Nmap.org para el uso de su servidor?

Menos de 100 escaneos, sin herramientas de descifrado de contraseñas SSH de fuerza bruta

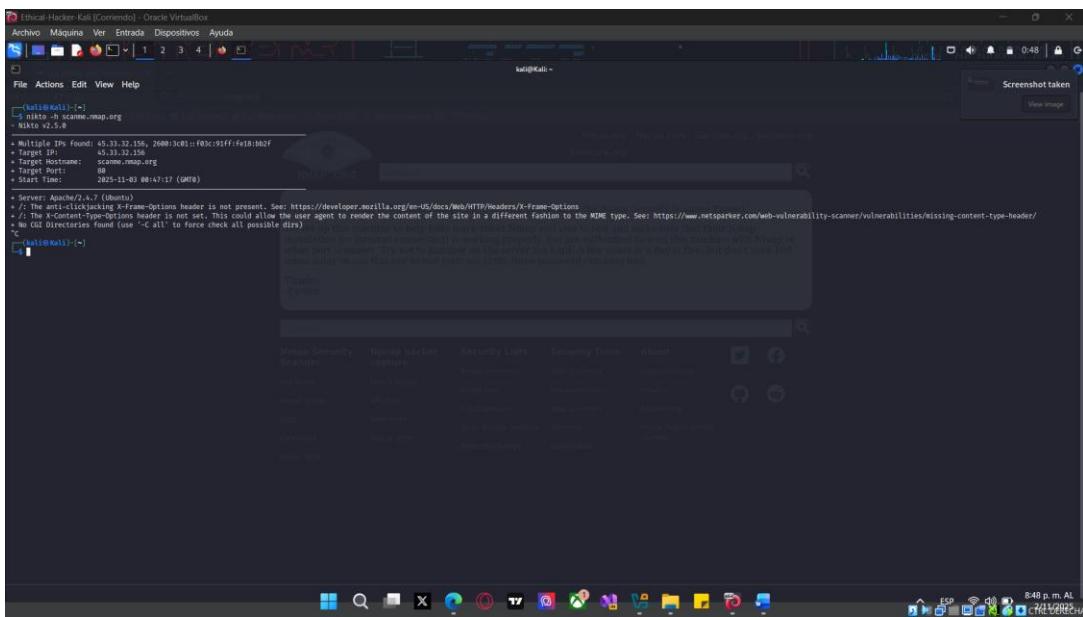
- Utilice Nikto para realizar un escaneo básico en el sitio web scanme.nmap.org.

```
└──(kali㉿Kali)-[~]
└─$ nikto -h scanme.nmap.org
```

Nota: Los escaneos de Nikto en un servidor de Internet pueden demorar unos minutos. Espere hasta que vuelva el indicador de la CLI para continuar con los siguientes pasos. Para finalizar un análisis en ejecución, ingrese **CTRL-C**.

Debe recibir una salida similar a la siguiente:

```
- Nikto v2.5.0
-----
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP: 45.33.32.156
+ Target Hostname: scanme.nmap.org
+ Target Port: 80
+ Start Time: 2023-05-23 05:48:36 (GMT-7)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ /: 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 different fashion to the MIME type. See:
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-
type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to
easily brute force file names. The following alternatives for 'index' were found:
index.html. See:
http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/v
ulnerabilities/8275
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache
2.2.34 is the EOL for the 2.x branch.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP
response
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time: 2023-05-23 05:49:14 (GMT-7) (38 seconds)
-----
+ 1 host(s) tested
```



- c. Explore el enlace para la vulnerabilidad encontrada **The X-Content-Type-Options header is not set.** Abra Firefox y vaya al enlace: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>.
- d. Desplácese hacia abajo para ver el resumen, el impacto, los consejos de corrección y los enlaces de clasificación de vulnerabilidades.

¿Cuál es la corrección recomendada para esta vulnerabilidad?

- 1) Establezca el encabezado content-type para que coincida con el tipo de recurso que se ofrece.
- 2) Agregue el encabezado X-Content-Type-Options con un valor de "nosniff" para indicarle al navegador que confie en el content-type enviado en lugar de rastrear para encontrar el content-type real. Ejemplo:

X-Content-Type-Options: nosniff

The screenshot shows a web browser window with the URL <https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>. The page displays a 'Missing Content-Type Header' vulnerability with a 'Severity: Low'. It includes sections for 'Summary', 'Impact', 'Vulnerability Index', 'Select Category', 'Select Vulnerability', and 'Remediation'.

- e. Nikto busca servicios web del puerto 80. Para escanear dominios con HTTPS habilitado, debe especificar el indicador **-ssl** para escanear el puerto 443:

Parte 2: Usar Nikto para escanear varios servidores web

En esta parte, utilizará Nikto para escanear servidores en las redes virtuales internas en busca de servidores web vulnerables. Primero creará un archivo de texto para enumerar las direcciones IP que desea escanear. En el reconocimiento de la vida real, puede obtener las direcciones IP de los servidores realizando una búsqueda de DNS del nombre del servidor a partir de la URL.

- a. Primero, cree un archivo de texto que enumere las direcciones IP de los servidores web que se analizarán. Utilice la aplicación MousePad integrada en Kali para crear el archivo. Haga clic en **Applications ->Favorites->Text Editor**. Copie y pegue esta lista de direcciones IP en su documento. Guarde el documento en el directorio de inicio como **IP_list.txt**.

10.6.6.11
10.6.6.13
10.6.6.14
10.6.6.23
172.17.0.2

- b. Ejecute el análisis con el comando **nikto -h IP_list.txt**.

```
└── (kali㉿Kali)-[~]
    └─$ nikto -h IP list.txt
```

Nota: Si maximiza la ventana del terminal, la salida será más fácil de leer.

¿Cuántos de los objetivos alojan servidores web? ¿Cuántos servidores ejecutan Apache

Práctica de Laboratorio - Análisis de Vulnerabilidades Web

Cuatro objetivos están alojando servidores web y tres de los servidores están ejecutando Apache

Parte 3: Investigar las vulnerabilidades del sitio web

Nikto proporciona información sobre las vulnerabilidades que descubre durante sus análisis. Algunas vulnerabilidades están asociadas con un número de OSVDB (una base de datos de vulnerabilidades de código abierto anterior), una CWE ([Enumeración de Debilidades Comunes](#)) o una CVE ([Vulnerabilidades y Exposiciones Comunes](#)). OSVDB se suspendió en 2016. Puede utilizar la herramienta de referencia CVE para traducir el identificador OSVDB a una entrada CVE para poder investigar más a fondo la vulnerabilidad.

- a. Revise la información que reportó Nikto para el servidor web 172.17.0.2. Las CVE enumeradas en el resultado son CVE-1999-0678 y CVE-2003-1418. Utilice los enlaces de CVE en el resultado de Nikto para encontrar más información sobre las vulnerabilidades.

The screenshot shows a web browser window with multiple tabs open. The active tab displays the National Vulnerability Database (NVD) search results for the keyword "CVE-2003-1418". The search bar contains "CVE-2003-1418". Below the search bar are buttons for "Avanzado" (Advanced), "Restablecer" (Reset), and "Mostrar estadísticas" (Show statistics). A message below the search bar says "Para una búsqueda de frases, use "" ". The search results table has columns: Identificador (Identifier), Información de CISA Kev (CISA Kev Information), Fecha de publicación (Publication Date), CNA (CNA), and Descripción (Description). One result is listed: CVE-2003-1418, dated 2003-12-31, CNA MITRA, with a detailed description about Apache HTTP Server 1.3.22 to 1.3.27 on OpenBSD. At the bottom, there is a pagination control showing "Artículos por página: 25" and "1-1 de 1".

b.

¿Qué vulnerabilidades describen las dos CVE enumeradas?

The screenshot shows a web browser window with multiple tabs open. The active tab displays the National Vulnerability Database (NVD) search results for the keyword "CVE-1999-0678". The search bar contains "CVE-1999-0678". Below the search bar are buttons for "Avanzado" (Advanced), "Restablecer" (Reset), and "Mostrar estadísticas" (Show statistics). A message below the search bar says "Para una búsqueda de frases, use "" ". The search results table has columns: Identificador (Identifier), Información de CISA Kev (CISA Kev Information), Fecha de publicación (Publication Date), CNA (CNA), and Descripción (Description). One result is listed: CVE-1999-0678, dated 1999-01-17, CNA MITRA, with a detailed description about Apache in Debian GNU/Linux. At the bottom, there is a pagination control showing "Artículos por página: 25" and "1-1 de 1".

CVE-1999-0678 hace referencia a la configuración predeterminada en algunas versiones de Apache que establece el ServerRoot en /usr/doc. Esto permite que los usuarios remotos lean los archivos de documentación de todo el servidor.

CVE-2003-1418 permite a los atacantes remotos obtener información sensible a través del encabezado ETag o del límite MIME multipart.

- Utilice la Base de Datos Nacional de Vulnerabilidades (<https://nvd.nist.gov>) para encontrar información adicional sobre las CVE. En la sección References to **Advisories, Solutions, and Tools**, siga los enlaces para encontrar las medidas de corrección necesarias para cerrar cada vulnerabilidad.

¿Cuál es la solución proporcionada para CVE-2003-1418?

Existe un parche de código fuente que soluciona este problema.

Parte 4: Exportar los resultados de Nikto a un archivo

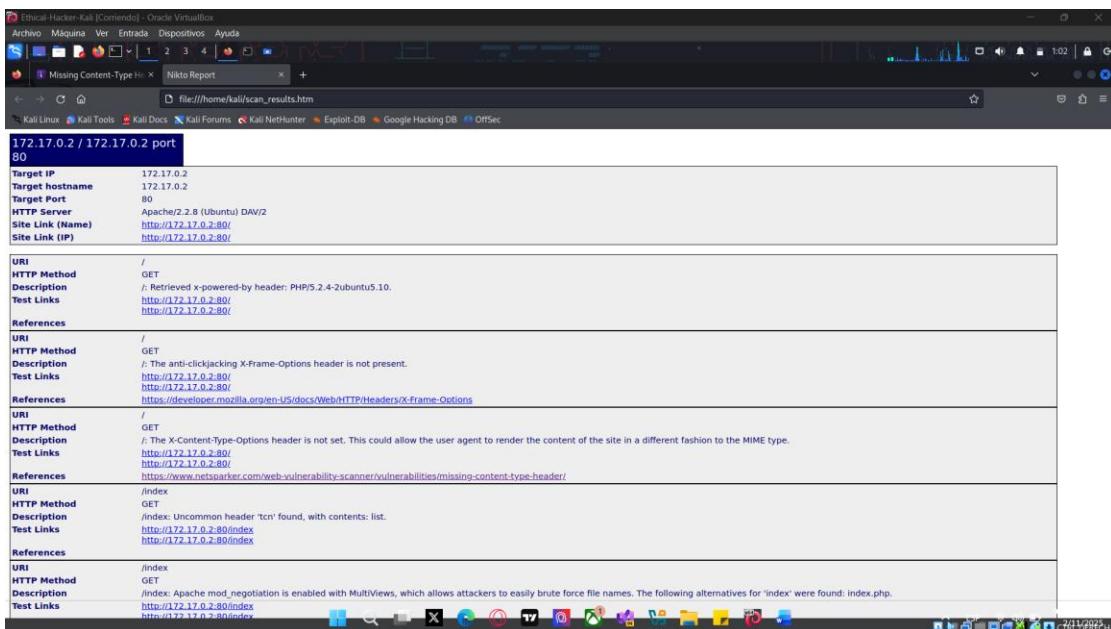
Nikto puede generar los resultados de un escaneo en varios formatos, incluidos CSV, HTML, SQL, txt y XML. Además, Nikto puede emparejarse con Metasploit para lanzar exploits contra las vulnerabilidades que descubra.

- Para exportar el resultado de un análisis, utilice el indicador `-o` seguido del nombre del archivo. Exporte los resultados de un escaneo a un archivo de informe HTML denominado **scan_results.htm**. El tipo de archivo de salida se determina a partir de la extensión del archivo.

```
└── (kali㉿Kali)-[~]
    └─$ nikto -h 172.17.0.2 -o scan_results.htm
```

- Busque el archivo en el directorio /home/kali y ábralo en su navegador para ver el formato del informe.

Práctica de Laboratorio - Análisis de Vulnerabilidades Web



- c. Para especificar un formato de salida de archivo de texto que sea independiente de la extensión del archivo, utilice el indicador **-Format**. Utilice la opción **-Format csv** para guardar el archivo en formato .csv para importarlo a otras aplicaciones de análisis.

```
└── (kali㉿Kali)-[~]
    └─$ nikto -h 172.17.0.2 -o scan_results.txt -Format csv
```

- d. Utilice el comando **cat** para ver el archivo **scan_results.txt** guardado.

¿En qué se diferencia el archivo guardado de la salida que se muestra en la pantalla?

En el archivo guardado, cada campo está separado por una coma.

Reflexión

Nitko es un antiguo escáner de vulnerabilidades web de código abierto. Utilice un motor de búsqueda en Internet para buscar otros escáneres de vulnerabilidades web que puedan utilizarse con Kali Linux. Indique al menos una herramienta adicional que pueda utilizarse para analizar sitios web en busca de vulnerabilidades que puedan explotarse.

Las respuestas pueden variar. Nmap, Burp Suite, Nessus, OWASP-ZAP, Wapiti, Skipfish

Nikto es un escáner de vulnerabilidades web antiguo, pero existen otras herramientas que también pueden usarse en Kali Linux para analizar sitios web. Algunas de las más conocidas son:

- **Wapiti: analiza aplicaciones web en busca de vulnerabilidades como XSS y SQL Injection.**
- **Skipfish: realiza escaneos rápidos y crea un mapa del sitio con posibles fallas.**
- **OWASP ZAP: herramienta gráfica que detecta vulnerabilidades de forma automática y manual.**
- **Burp Suite: proxy avanzado para pruebas de seguridad web y análisis de tráfico HTTP.**
- **Nessus / OpenVAS: detectan vulnerabilidades tanto en redes como en servidores web.**
- **Nmap (con scripts NSE): escanea servidores y detecta fallas conocidas o configuraciones inseguras**