Cómo usar los scripts de Nmap Script Engine (NSE) en Linux

Nmap es una herramienta de exploración y exploración de seguridad de red de línea de comandos popular, potente y multiplataforma. También puede ayudarlo a obtener una visión general de los sistemas que conectaron su red; puede usarlo para averiguar todas las direcciones IP de hosts en vivo, escanear puertos abiertos y servicios que se ejecutan en esos hosts, y mucho más.

Una de las características interesantes de Nmap es el **Nmap Script Engine** (**NSE**), que le brinda aún más flexibilidad y eficiencia. Le permite escribir sus propios scripts en el lenguaje de programación **Lua** , y posiblemente compartir estos scripts con otros usuarios de Nmap.

Hay cuatro tipos de scripts NSE, a saber:

- **Prerule scripts** – are scripts that run before any of Nmap's scan operations, they are executed when Nmap hasn't gathered any information about a target yet.
- **Host scripts** – are scripts executed after Nmap has performed normal operations such as host discovery, port scanning, version detection, and OS detection against a target host.
- **Service scripts** – are scripts run against specific services listening on a target host.
- **Postrule scripts** – are scripts run after Nmap has scanned all of its target hosts.

Luego, estos scripts se agrupan en varias categorías, incluidas las de autenticación (**auth**), descubrimiento de hosts (**broadcast**), ataques de fuerza bruta para adivinar credenciales de autenticación (**brute**), descubriendo más sobre una red (**descubrimiento**), causando una denegación de servicio (**dos**), explotando alguna vulnerabilidad (**exploit**) , etc. Una serie de scripts pertenecen a la categoría por defecto.

rojo

- Do not execute scripts from third parties without critically looking through them or only if you trust the authors. This is because these scripts are not run in a sandbox and thus could unexpectedly or maliciously damage your system or invade your privacy.
- Secondly, many of these scripts may possibly run as either a **prerule** or **postrule** script. Considering this, it is recommend to use a prerule for purposes of consistency.
- Nmap uses the **scripts/script.db** database to figure out the available default scripts and categories.

Para ver la ubicación de todos los scripts NSE disponibles, ejecute la utilidad de localización en el terminal, de esta manera:

```
$ locate *.nse

/usr/share/nmap/scripts/acarsd-info.nse
/usr/share/nmap/scripts/address-info.nse
/usr/share/nmap/scripts/afp-brute.nse
/usr/share/nmap/scripts/afp-ls.nse
/usr/share/nmap/scripts/afp-path-vuln.nse
/usr/share/nmap/scripts/afp-serverinfo.nse
/usr/share/nmap/scripts/afp-showmount.nse
/usr/share/nmap/scripts/ajp-auth.nse
/usr/share/nmap/scripts/ajp-brute.nse
/usr/share/nmap/scripts/ajp-headers.nse
/usr/share/nmap/scripts/ajp-methods.nse
/usr/share/nmap/scripts/ajp-request.nse
/usr/share/nmap/scripts/allseeingeye-info.nse
/usr/share/nmap/scripts/amqp-info.nse
/usr/share/nmap/scripts/asn-query.nse
...
```

Los scripts NSE se cargan utilizando el indicador `--script` , que también le permite ejecutar sus propios scripts al proporcionar categorías, nombres de archivos de script o el nombre de los directorios donde se encuentran sus scripts.

La sintaxis para habilitar los scripts es la siguiente:

```
$ namp -sC target     #load default scripts
OR
$ nmap --script filename|category|directory|expression,...   target
```

Puede ver una descripción de un script con la opción `--script-help` . Además, puede pasar argumentos a algunos scripts a través de las opciones `--script-args` y `--script-args-file` , este último se usa para proporcionar un nombre de archivo en lugar de una línea de comando arg.

Para realizar un escaneo con la mayoría de los scripts predeterminados, use la marca `-sC` o, alternativamente, use `--script = default` como se muestra.

```
$ nmap -sC scanme.nmap.org
OR
$ nmap --script=default scanme.nmap.org
OR
$ nmap --script default scanme.nmap.org
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-15 10:36 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0027s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
|_http-title: Go ahead and ScanMe!

Nmap done: 1 IP address (1 host up) scanned in 11.74 seconds
```

Para usar un script para el propósito apropiado, primero puede obtener una breve descripción de lo que realmente hace, por ejemplo, **encabezados http**

```
$ nmap --script-help http-headers scanme.nmap.org
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-15 10:37 IST

http-headers
Categories: discovery safe
https://nmap.org/nsedoc/scripts/http-headers.html
  Performs a HEAD request for the root folder ("/") of a web server and displays the HTTP headers returned.
```

Carga de scripts NSE para realizar exploraciones de Nmap

Puede seleccionar o cargar scripts para realizar una exploración en diferentes métodos que se explican a continuación.

Una vez que sepa lo que hace un script, puede realizar un escaneo usándolo. Puede usar un script o ingresar una lista de nombres de script separados por comas. El siguiente comando le permitirá ver los encabezados HTTP configurados en el servidor web en el host de destino.

```
$ nmap --script http-headers scanme.nmap.org
```

Escanear encabezados HTTP

```
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-15 10:39 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Not shown: 996 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
| http-headers:
|   Date: Wed, 15 Nov 2017 05:10:04 GMT
|   Server: Apache/2.4.7 (Ubuntu)
|   Accept-Ranges: bytes
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
179/tcp   filtered bgp
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 20.96 seconds
```

También puede cargar scripts de una categoría o de una lista de categorías separadas por comas. En este ejemplo, estamos utilizando todos los scripts en la categoría predeterminada y de difusión para realizar una exploración en el host **192.168.56.1** .

```
$ nmap --script default,broadcast 192.168.56.1
```

```
aaronkilik@tecmint ~ $ nmap --script default,broadcast 192.168.56.1

Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-13 12:25 EAT
Pre-scan script results:
| broadcast-netbios-master-browser:
| ip            server   domain
|_192.168.1.94  TECMINT  WORKGROUP
|_broadcast-wpad-discover: ERROR: Script execution failed (use -d to debug)
Nmap scan report for ubuntu.tecmint.lan (192.168.56.1)
Host is up (0.00024s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   2048 29:0f:e3:36:41:6f:1b:d4:8d:de:2b:0e:6b:2b:50:a2 (RSA)
|_  256 a5:19:e4:63:ad:0d:aa:18:5e:3b:86:8d:50:eb:4b:aa (ECDSA)
80/tcp    open  http
|_http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn
443/tcp   open  https
|_http-title: Site doesn't have a title (text/html).
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html).
10000/tcp open  snet-sensor-mgmt

Host script results:
|_nbstat: NetBIOS name: TECMINT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: tecmint
|   NetBIOS computer name: TECMINT
|   Domain name:
|   FQDN: tecmint
|_  System time: 2017-11-13T12:25:55+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

Nmap done: 1 IP address (1 host up) scanned in 63.10 seconds
aaronkilik@tecmint ~ $
```

Esto es útil cuando desea seleccionar scripts con un patrón de nombre dado. Por ejemplo, para cargar todos los scripts con nombres que comiencen con **ssh** , ejecute el siguiente comando en el terminal:

```
$ nmap --script "ssh-*" 192.168.56.1
```

```
aaronkilik@tecmint ~ $ nmap --script "ssh-*" 192.168.56.1

Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-13 12:45 EAT
Nmap scan report for ubuntu.tecmint.lan (192.168.56.1)
Host is up (0.00027s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   2048 29:0f:e3:36:41:6f:1b:d4:8d:de:2b:0e:6b:2b:50:a2 (RSA)
|_  256 a5:19:e4:63:ad:0d:aa:18:5e:3b:86:8d:50:eb:4b:aa (ECDSA)
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
aaronkilik@tecmint ~ $
```

20

También puede seleccionar secuencias de comandos utilizando expresiones booleanas que puede crear utilizando los operadores **y** , **o** , y **no** . Y los

nombres en una expresión booleana pueden ser una categoría, un nombre de archivo de **script.db** , o todos.

El siguiente comando cargará los scripts de las categorías predeterminadas o de difusión.

```
$ nmap --script "default or broadcast" 192.168.56.10
```

Lo que equivale a:

```
$ nmap --script default,broadcast 192.168.56.10
```

Para cargar todos los scripts que omiten aquellos en la categoría **vuln** , ejecute este comando en el terminal.

```
$ nmap --script "not vuln" 192.168.56.10
```

El siguiente comando parece un poco complicado, pero es fácil de entender, selecciona scripts en las categorías predeterminadas o de difusión, dejando de lado aquell

```
$ nmap --script "(default or broadcast) and not ssh-*" 192.168.56.10
```

Es importante destacar que es posible combinar categorías, nombres de scripts, un directorio que contiene sus scripts personalizados o una expresión booleana para ca

```
$ nmap --script broadcast,vuln,ssh-auth-methods,/path/to/custom/scripts 192.168.56.10
```

A continuación se muestra un ejemplo que muestra cómo pasar argumentos a scripts con la opción **–script-args** :

```
$ nmap --script mysql-audit --script-args "mysql-audit.username='root', \
mysql-audit.password='password_here', mysql-audit.filename='nselib/data/mysql-cis.audit'"
```

Para pasar un número de puerto, use la opción **-p** nmap:

```
$ nmap -p 3306 --script mysql-audit --script-args "mysql-audit.username='root', \
mysql-audit.password='password_here' , mysql-audit.filename='nselib/data/mysql-cis.audit'"
```

Este comando anterior ejecuta una auditoría de la configuración de seguridad del servidor de la base de datos MySQL en partes del punto de referencia **CIS MySQL**

Eso es todo por ahora. Puede encontrar más información en la página de manual de nmap o consultar Uso de NSE.

Para comenzar a escribir sus propios scripts NSE, consulte esta guía: https://nmap.org/book/nse-tutorial.html

Nmap es una herramienta realmente poderosa y útil que todo administrador de sistemas o redes necesita en su arsenal de seguridad - **NSE** simplemente le agrega más

En este artículo, le presentamos el **Nmap Script Engine** y analizamos cómo encontrar y usar los distintos scripts disponibles en diferentes categorías. Si tiene alguna