

## Lamp Security LINUX

### Identificación del Objetivo

#### Aplicación de herramienta NMAP

El nmap es una herramienta que sirve para evaluar la seguridad del sistema en una red, rastrear puertos o detectar objetivo para un ataque

Algunas utilidades de la herramienta nmap son:

-Para averiguar cuántos equipos están conectados en la red, sus ips y los puertos que tienen abiertos, utilizamos el comando nmap y el rango de ip que queremos que escanea.

Nota: En este caso escaneamos desde ip 192.168.1.2 hasta 192.168.1.254

**nmap 192.168.0.2-254**

```
Nmap scan report for 192.168.0.195
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.0.195 are closed

Nmap scan report for 192.168.0.196
Host is up (0.00056s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
901/tcp   open  samba-swat
5900/tcp  closed vnc
8080/tcp  open  http-proxy
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:0C:29:9D:12:A9 (VMware)

Nmap done: 253 IP addresses (3 hosts up) scanned in 26.62 seconds
root@bt: ~#
```

-Una vez elegido un equipo para averiguar detalles de los puertos que tienes abierto usamos el comando siguiente:

**nmap -sV 192.168.0.196**

```

root@bt:~# nmap -sV 192.168.0.196
No command 'nmap' found, did you mean:
Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-20 19:50 CET
Nmap scan report for 192.168.0.196
Host is up (0.013s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.2.21 ((Win32) mod_ssl/2.2.21 OpenSSL/1.0.0e PHP/5.3.8 mod_perl/2.0.4 Perl/v5.10.1)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows
443/tcp   open  ssl/http     Apache httpd 2.2.21 ((Win32) mod_ssl/2.2.21 OpenSSL/1.0.0e PHP/5.3.8 mod_perl/2.0.4 Perl/v5.10.1)
445/tcp   open  netbios-ssn  Microsoft Windows
1723/tcp  open  pptp         Microsoft Windows
5357/tcp  open  httpios-ssl  Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 2C:27:D7:DE:BE:F5 (Hewlett-Packard Company)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
445/tcp   open  netbios-ssn  Microsoft Windows
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.21 seconds
root@bt:~#

```

-Para averiguar qué sistema Operativo y más informaciones del sistema del equipo, hacemos un escaneo usando el siguiente comando:

Nota: en este escaneo tambien estamos asegurando de que nonos detectan, en caso de que el equipo escaneado tiene algún programa que nos puedes detectar.

**nmap -O -sS 192.168.0.196**

```

root@bt:~# nmap -O -sS 192.168.0.196
Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-20 17:22 CET
Nmap scan report for 192.168.0.196
Host is up (0.00057s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
901/tcp   open  samba-swat
5900/tcp  closed vnc
8080/tcp  open  http-proxy
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:0C:29:9D:12:A9 (VMware)
Device type: general purpose|storage-misc|WAP|media device
Running (JUST GUESSING): Linux 2.6.X|3.X (97%), HP embedded (91%), Netgear embedded (89%), Western Digital embedded (89%)
OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3
Aggressive OS guesses: Linux 2.6.39 (97%), Linux 2.6.22 - 2.6.36 (93%), Linux 2.6.38 - 3.2 (93%), Linux 3.0 - 3.1 (91%), HP P2000 G3 NAS device (91%), Linux 2.6.32 - 2.6.39 (91%), Linux 2.6.38 - 3.0 (91%), Linux 3.0 (89%), Linux 2.6.23 - 2.6.38 (89%), Linux 2.6.31 - 2.6.35 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.91 seconds
root@bt:~#

```

-Otra forma de confundir el equipo que queremos escanear de que no nuestra deirecion y hacerlo creer que se trata de otro equipo, por ejemplo el router. Usamos el comando nmap con la opción siguiente:

Nota: Escaneamos al 192.168.0.19 y le hacemos creer que está siendo escaneado por 192.168.1.196

**nmap sS 192.168.0.196 -D 192.168.0.1**

```

root@bt:~# nmap -sS 192.168.0.196 -D 192.168.0.1
443/tcp open  ssl/http          Apache httpd 2.2.17 ((Win32) mod_ssl/2
Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-20 20:02 CET
Nmap scan report for 192.168.0.196
Host is up (0.020s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1723/tcp  open  pptp
5357/tcp  open  B2:14 (Asustek Computer)
MAC Address: 2C:27:D7:DE:BE:F5 (Hewlett-Packard Company)

Nmap done: 1 IP address (1 host up) scanned in 5.20 seconds
root@bt:~#

```

-Para ver el puerto UDP abierto

nmap -sU 192.168.0.196

```

root@bt:~# nmap -sU 192.168.0.196
Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-20 19:37 CET
Nmap scan report for 192.168.0.196
Host is up (0.023s latency).
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
137/udp   open  netbios-ns
MAC Address: 2C:27:D7:DE:BE:F5 (Hewlett-Packard Company)

Nmap done: 1 IP address (1 host up) scanned in 9.47 seconds
root@bt:~#

```

Nota: La herramienta nmap tiene muchos más opciones para evaluar la seguridad de una red.

## Exploración del Objetivo

### Aplicación de la Herramienta NIKTO

Una vez tenemos localizado el objetivo con la herramienta NMAP, ahora podemos explorar el objetivo en busca de vulnerabilidades utilizando las direcciones y los puertos abiertos anteriormente encontrado.

En este caso vamos a comentar sobre la herramienta NIKTO.

Para abrir nikto vamos al menú Backtrack->Vulnerability assessment->Web application assessment->Web vulnerability scanner->nikto

Se abrirá una ventana de línea de comando de nikto.

-Para explorar hacer una exploración con nikto usamos en comando:

**./nikto.pl -host 192.168.0.195**

```
root@bt:~/pentest/web/nikto# ./nikto.pl -host 192.168.0.195
Nikto v2.1.5
-----
+ Target IP:      192.168.0.195
+ Target Hostname: 192.168.0.195
+ Target Port:    80
+ Start Time:    2013-01-18 13:36:36 (GMT1)
-----
+ Server: Apache/2.2.15 (CentOS)
+ Retrieved x-powered-by header: PHP/5.3.3
Undefined subroutine &main::get_ips called at /pentest/web/nikto/plugins/nikto_headers.plugin line 72.
root@bt:~/pentest/web/nikto#
```

En el caso anterior, nikto va a hacer automáticamente la exploración en el puerto 80. Para hacer exploración en otro puerto, como por ejemplo 8080, habrá que indicarlo de la siguiente manera:

**./nikto.pl -host 192.168.0.195 -port 8080**

```
root@bt:~/pentest/web/nikto# ./nikto.pl -host 192.168.0.195 -port 8080
Nikto v2.1.5
-----
+ Target IP:      192.168.0.195
+ Target Hostname: 192.168.0.195
+ Target Port:    8080
+ Start Time:    2013-01-18 13:38:54 (GMT1)
-----
+ Server: Apache/2.2.15 (CentOS)
+ Retrieved x-powered-by header: PHP/5.3.3
Undefined subroutine &main::get_ips called at /pentest/web/nikto/plugins/nikto_headers.plugin line 72.
root@bt:~/pentest/web/nikto#
```

Nota: Con las acciones anteriores de la herramienta nikto se puede encontrar vulnerabilidades que pueden ser utilizados para un ataque, como por ejemplo inyección de Sql con la herramienta MySQLmap.