nmap

Nmap

Obtener hosts vulnerables como intermediario

```
nmap -O -v -sS|sT|sA|sW|sM objetivo -oA objetivo.result
```

Buscar los hosts vulnerables en el resultado

```
 grep “IP ID” objetivo.result.gnmap | perl -pe ‘s/Host:([^\t]+).*IP ID
Seq:([^:]+)/$1 $2/’
```

Realizar ping a través de un intermediario

```
nmap -PN -p- -sI intermediario destino
```

Scripts

https://github.com/cldrn/nmap-nse-scripts

- http://abdulet.net/
- http://conocimientolibre.wordpress.com/2007/06/30/nmap-a-fondo-escaneo-de-redes-y-hosts/
- http://xora.org/2013-4-scripts-de-nmap-indispensables-para-vulnerabilidades-del-2012/