Utilización de `zenmap`

Introducción

`Zenmap` cs una intcíraz gíárica dc la »cííamicnta nmap quc racilita la cxploíación dc pucítos Q pcímitc la cícación dc pcírilcs pcísonalizados dc cxploíación. Está disponiblc tanto paía Windows como paía GNU/Linux Ubuntu Q MacOS. Es dc código libíc.

Paía Windows también cstá disponiblc la »cííamicnta 6dvanccd IP Scanncí (**http://www.advanced-ip-scan ner.com/es**).

`Zenmap` ticnc la vcntaja dc scí más intuitiva paía los usuaíios quc no conoccn **`nmap`** Q sus posibilidadcs Q, poí otío lado, píopoíciona más opcioncs dc cjccución a los usuaíios más avanzados.

Pcímitc la cícación dc pcírilcs dc cjccución Q dc csa roíma »acc más scncilla la ícpctición dc óídcncs. Ham bién pcímitc guaídaí los inroímcs obtcnidos dc la cxploíación cn una basc dc datos.

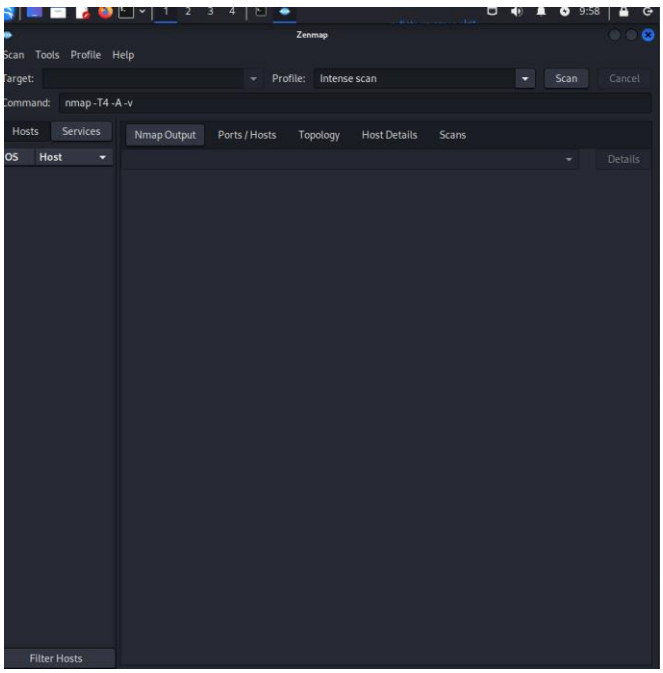
Hanto **`nmap`** como **`Zenmap`** pcímitcn tíabajaí con scíipts (pcstaÉa Scíipting, dcsdc cl Editoí dc pcírilcs), quc amplïan la runcionalidad dc **`nmap`** más allá dc la cxploíación. Con cstos scíipts **`nmap`** pucdc »accí, incluso, análisis dc vulncíabilidadcs. Esta runcionalidad cstá disponiblc tanto cn GNU/Linux (/usí/s»aíc/nmap/scíipts) como cn Windows (6íc»ivos dc píogíama\Nmap\scíipts). Los scíipts sc oíganizan poí catcgoíïas como **`safe`**, **`intrusive`**, **`malware`**, **`discovery`**, **`vuln`**, **`auth`**, **`external`**, **`default`** Q **`all`**. Hicncn cxtcnsión **`.nse`**.

Poí cjcmplo, cl scíipt **`whois`** pcímitc ícalizaí una consulta a las bascs dc datos w»ois paía avcíiguaí inroíma ción accíca dc la oíganización: païs, nombíc dc ícd, ctc., dc los »osts a los quc sc ícaliza la auditoíïa.

Enunciado

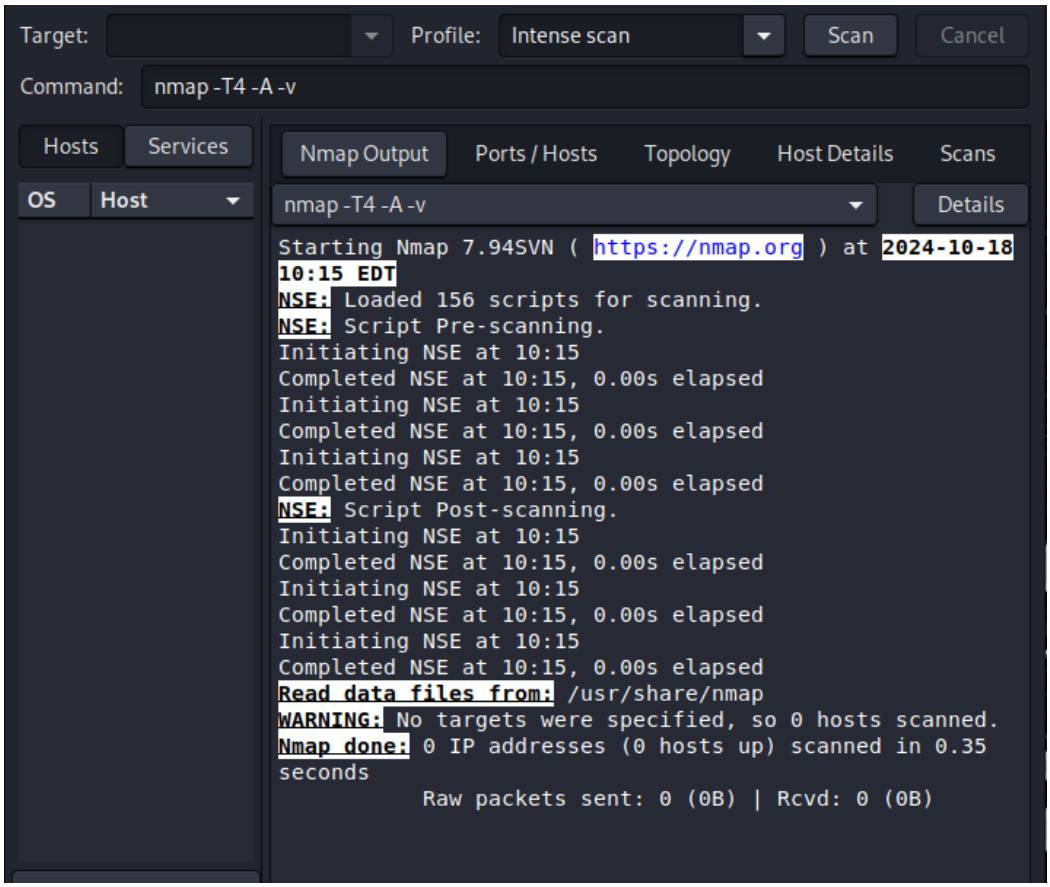
Sc pidc:

1. Instalaí la »cííamicnta Q cjccutaíla como usuaíio sudo.
2. Explicaí bícvcmcntc la intcíraz quc mucstía.



3. Rcalizaí dircícntcs cjcmplos dc:

a) Ejccución simplc.



Podemos ver todo esto:

Dirección IP de los hosts detectados.

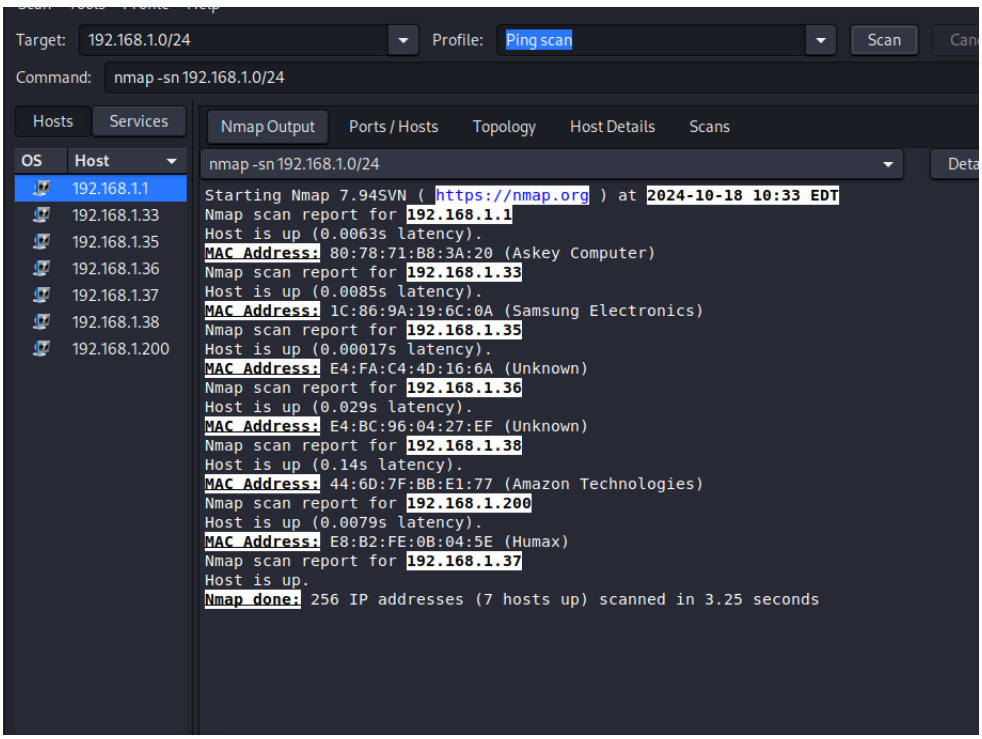
Puertos abiertos en cada host.

Servicios que se ejecutan en esos puertos (por ejemplo, HTTP, SSH, FTP).

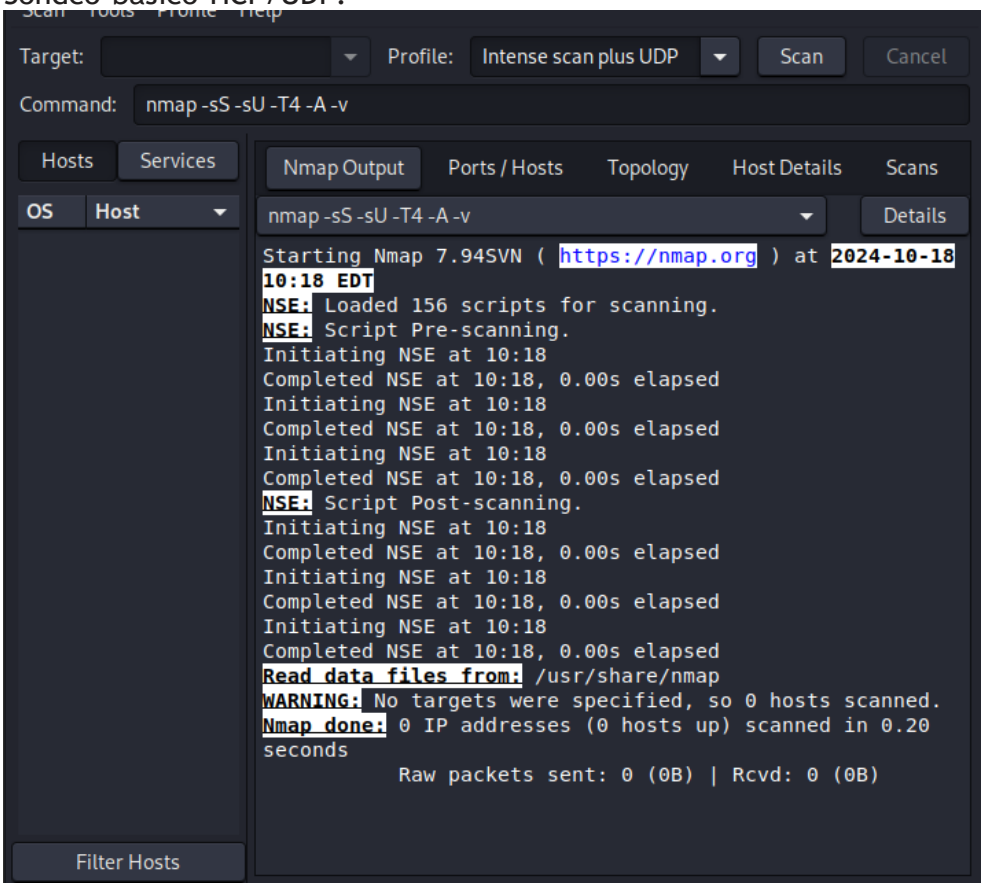
Versiones básicas de los servicios si se detectan.

Información de **latencia** y tiempos de respuesta.

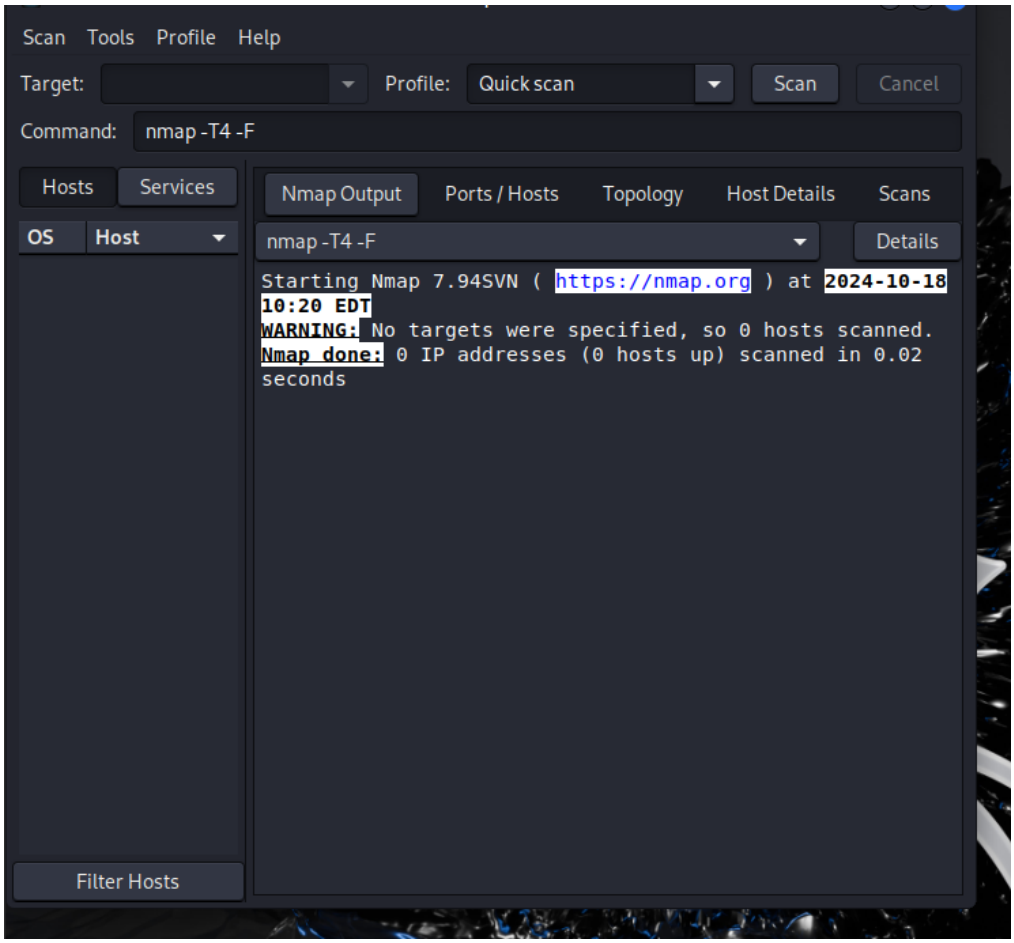
b) Idcntiricaí »osts activos cn la ícd.



c) Sondco básico HCP/UDP.



d) Rcalizaí un cscanco sigiloso.



c) Cícación dcl *pcíril1* pcísonalizado.