CURSO DE

CIBERSEGURIDAD

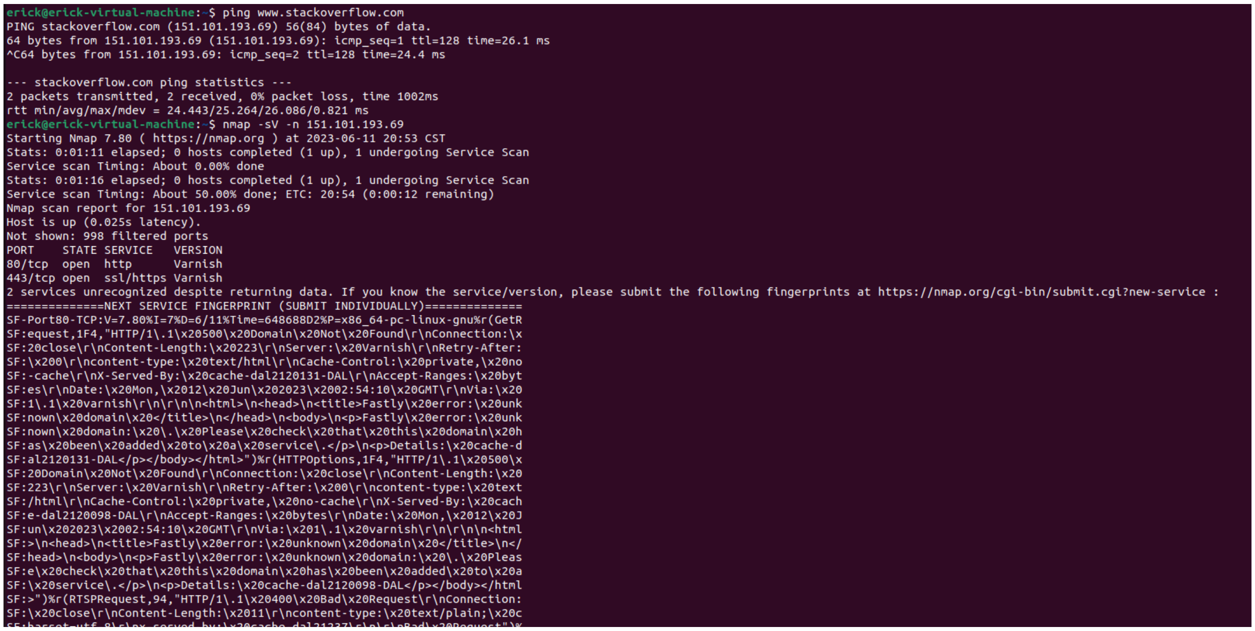
Prof. Andrés Oviedo

RETO 1

Erick Guillermo Morales Aldana

Oracle

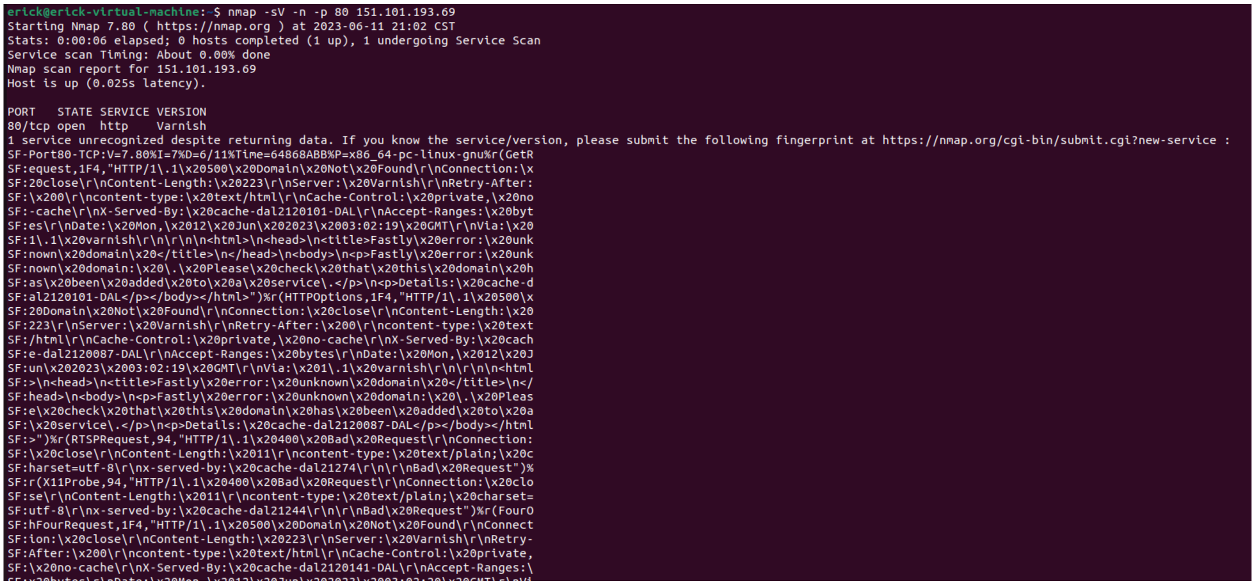
- Detectar direcciones IP de equipos



```
erick@erick-virtual-machine:~$ ping www.stackoverflow.com
PING stackoverflow.com (151.101.193.69) 56(84) bytes of data.
64 bytes from 151.101.193.69 (151.101.193.69): icmp_seq=1 ttl=128 time=26.1 ms
^C64 bytes from 151.101.193.69: icmp_seq=2 ttl=128 time=24.4 ms

--- stackoverflow.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 24.443/25.264/26.086/0.821 ms
erick@erick-virtual-machine:~$ nmap -sV -n 151.101.193.69
Starting Nmap 7.80 ( https://nmap.org ) at 2023-06-11 20:53 CST
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 20:54 (0:00:12 remaining)
Nmap scan report for 151.101.193.69
Host is up (0.025s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE   VERSION
80/tcp  open  http      Varnish
443/tcp open  ssl/https Varnish
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.80%I=7%D=6/11%Time=648688D2%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,1F4,"HTTP/1\.1\x20500\x20Domain\x20Not\x20Found\r\nConnection:\x
SF:20close\r\nContent-Length:\x20223\r\nServer:\x20Varnish\r\nRetry-After:
SF:\x200\r\ncontent-type:\x20text/html\r\nCache-Control:\x20private,\x20no
SF:-cache\r\nX-Served-By:\x20cache-dal2120131-DAL\r\nAccept-Ranges:\x20byt
SF:es\r\nDate:\x20Mon,\x2012\x20Jun\x202023\x2002:54:10\x20GMT\r\nVia:\x20
SF:1\.1\x20varnish\r\n\r\n\n<html>\n<head>\n<title>Fastly\x20error:\x20unk
SF:nown\x20domain\x20</title>\n</head>\n<body>\n<p>Fastly\x20error:\x20unk
SF:nown\x20domain:\x20\.\x20Please\x20check\x20that\x20this\x20domain\x20h
SF:as\x20been\x20added\x20to\x20a\x20service\.</p>\n<p>Details:\x20cache-d
SF:al2120131-DAL</p></body></html>")%r(HTTPOptions,1F4,"HTTP/1\.1\x20500\x
SF:20Domain\x20Not\x20Found\r\nConnection:\x20close\r\nContent-Length:\x20
SF:223\r\nServer:\x20Varnish\r\nRetry-After:\x200\r\ncontent-type:\x20text
SF:/html\r\nCache-Control:\x20private,\x20no-cache\r\nX-Served-By:\x20cach
SF:e-dal2120098-DAL\r\nAccept-Ranges:\x20bytes\r\nDate:\x20Mon,\x2012\x20J
SF:un\x202023\x2002:54:10\x20GMT\r\nVia:\x201\.1\x20varnish\r\n\r\n\n<html
SF:>\n<head>\n<title>Fastly\x20error:\x20unknown\x20domain\x20</title>\n</
SF:head>\n<body>\n<p>Fastly\x20error:\x20unknown\x20domain:\x20\.\x20Pleas
SF:e\x20check\x20that\x20this\x20domain\x20has\x20been\x20added\x20to\x20a
SF:\x20service\.</p>\n<p>Details:\x20cache-dal2120098-DAL</p></body></html
SF:>")%r(RTSPRequest,94,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:
SF:\x20close\r\nContent-Length:\x2011\r\ncontent-type:\x20text/plain;\x20c
SF:harset=utf-8\r\nx-served-by:\x20cache-dal21237\r\n\r\nBad\x20Request")%
```

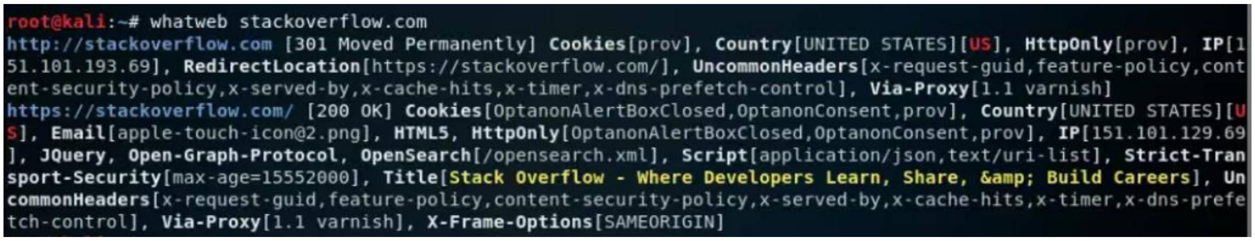
- Recopilar información de sitios web



```
erick@erick-virtual-machine:~$ nmap -sV -n -p 80 151.101.193.69
Starting Nmap 7.80 ( https://nmap.org ) at 2023-06-11 21:02 CST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 151.101.193.69
Host is up (0.025s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Varnish
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=6/11%Time=64868ABB%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,1F4,"HTTP/1\.1\x20500\x20Domain\x20Not\x20Found\r\nConnection:\x
SF:20close\r\nContent-Length:\x20223\r\nServer:\x20Varnish\r\nRetry-After:
SF:\x200\r\ncontent-type:\x20text/html\r\nCache-Control:\x20private,\x20no
SF:-cache\r\nX-Served-By:\x20cache-dal2120101-DAL\r\nAccept-Ranges:\x20byt
SF:es\r\nDate:\x20Mon,\x2012\x20Jun\x202023\x2003:02:19\x20GMT\r\nVia:\x20
SF:1\.1\x20varnish\r\n\r\n\n<html>\n<head>\n<title>Fastly\x20error:\x20unk
SF:nown\x20domain\x20</title>\n</head>\n<body>\n<p>Fastly\x20error:\x20unk
SF:nown\x20domain:\x20\.\x20Please\x20check\x20that\x20this\x20domain\x20h
SF:as\x20been\x20added\x20to\x20a\x20service\.</p>\n<p>Details:\x20cache-d
SF:al2120101-DAL</p></body></html>")%r(HTTPOptions,1F4,"HTTP/1\.1\x20500\x
SF:20Domain\x20Not\x20Found\r\nConnection:\x20close\r\nContent-Length:\x20
SF:223\r\nServer:\x20Varnish\r\nRetry-After:\x200\r\ncontent-type:\x20text
SF:/html\r\nCache-Control:\x20private,\x20no-cache\r\nX-Served-By:\x20cach
SF:e-dal2120087-DAL\r\nAccept-Ranges:\x20bytes\r\nDate:\x20Mon,\x2012\x20J
SF:un\x202023\x2003:02:19\x20GMT\r\nVia:\x201\.1\x20varnish\r\n\r\n\n<html
SF:>\n<head>\n<title>Fastly\x20error:\x20unknown\x20domain\x20</title>\n</
SF:head>\n<body>\n<p>Fastly\x20error:\x20unknown\x20domain:\x20\.\x20Pleas
SF:e\x20check\x20that\x20this\x20domain\x20has\x20been\x20added\x20to\x20a
SF:\x20service\.</p>\n<p>Details:\x20cache-dal2120087-DAL</p></body></html
SF:>")%r(RTSPRequest,94,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:
SF:\x20close\r\nContent-Length:\x2011\r\ncontent-type:\x20text/plain;\x20c
SF:harset=utf-8\r\nx-served-by:\x20cache-dal21274\r\n\r\nBad\x20Request")%
SF:r(X11Probe,94,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20clo
SF:se\r\nContent-Length:\x2011\r\ncontent-type:\x20text/plain;\x20charset=
SF:utf-8\r\nx-served-by:\x20cache-dal21244\r\n\r\nBad\x20Request")%r(FourO
SF:hFourRequest,1F4,"HTTP/1\.1\x20500\x20Domain\x20Not\x20Found\r\nConnect
SF:ion:\x20close\r\nContent-Length:\x20223\r\nServer:\x20Varnish\r\nRetry-
SF:After:\x200\r\ncontent-type:\x20text/html\r\nCache-Control:\x20private,
SF:\x20no-cache\r\nX-Served-By:\x20cache-dal2120141-DAL\r\nAccept-Ranges:\
SF:x20bytes\r\nDate:\x20Mon,\x2012\x20Jun\x202023\x2003:02:20\x20GMT\r\nVi
```

- Identificar el tipo de sitio web



```
root@kali:~# whatweb stackoverflow.com
http://stackoverflow.com [301 Moved Permanently] Cookies[prov], Country[UNITED STATES][US], HttpOnly[prov], IP[1
51.101.193.69], RedirectLocation[https://stackoverflow.com/], UncommonHeaders[x-request-guid,feature-policy,cont
ent-security-policy,x-served-by,x-cache-hits,x-timer,x-dns-prefetch-control], Via-Proxy[1.1 varnish]
https://stackoverflow.com/ [200 OK] Cookies[OptanonAlertBoxClosed,OptanonConsent,prov], Country[UNITED STATES][U
S], Email[apple-touch-icon@2.png], HTML5, HttpOnly[OptanonAlertBoxClosed,OptanonConsent,prov], IP[151.101.129.69
], JQuery, Open-Graph-Protocol, OpenSearch[/opensearch.xml], Script[application/json,text/uri-list], Strict-Tran
sport-Security[max-age=15552000], Title[Stack Overflow - Where Developers Learn, Share, &amp; Build Careers], Un
commonHeaders[x-request-guid,feature-policy,content-security-policy,x-served-by,x-cache-hits,x-timer,x-dns-prefe
tch-control], Via-Proxy[1.1 varnish], X-Frame-Options[SAMEORIGIN]
```