

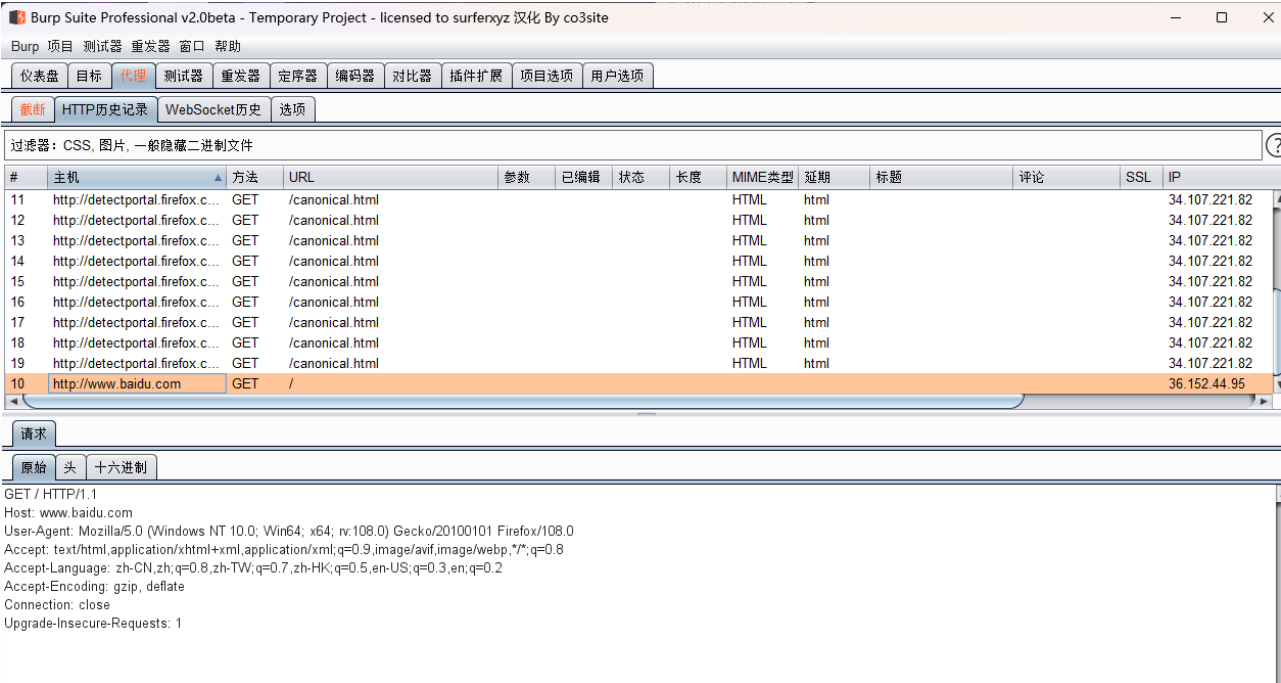
Web上机报告

学号: 姓名:

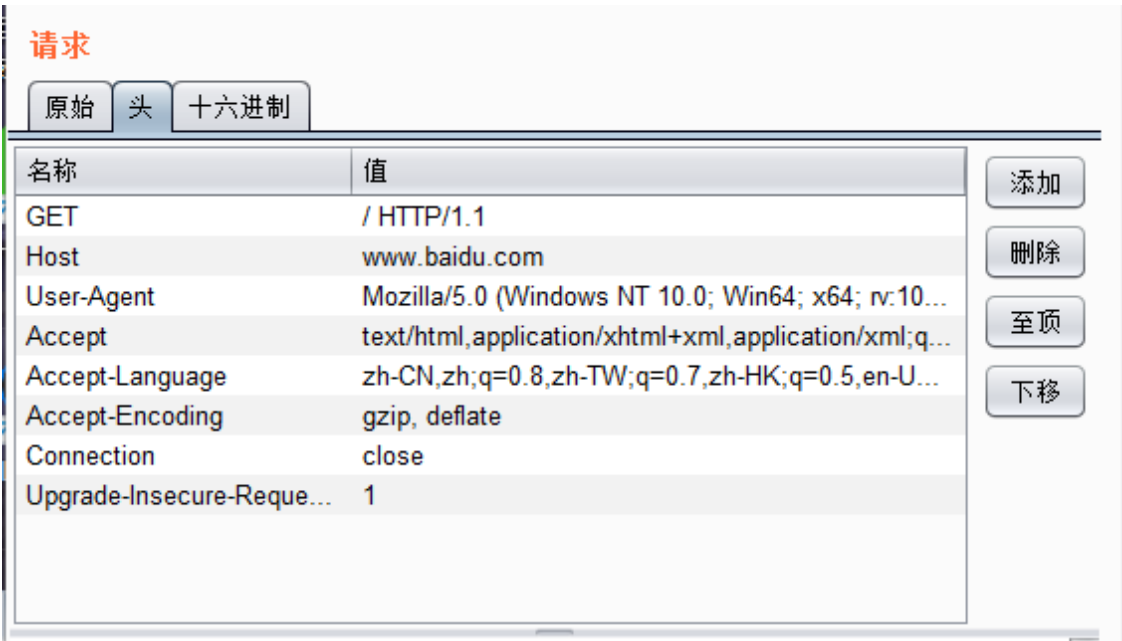
1 Burp Suite

1.1 Burp 代理功能

Firefox 访问百度，拦截可得



请求参数消息头



1.2 Burp Scanner 漏洞扫描, Burp spider 进行爬虫

1.2.1 对网页进行扫描

3. Active scans

Default configuration

Auditing. Estimating time remaining...

Issues: 3 8 178

41502 requests (11 errors)

View details >>

4. Audit of mbd.baidu.com

扫描结果

| 3. Active scans | | | | | | | | | | | |
|---|-----------------------|---------------------|-----------------------|--------------|---------------|----------------|--------|----------|--------|------------------|--|
| Details Audit items Issue activity Event log Logger | | | | | | | | | | | |
| # | Host | URL | Status | Passive p... | Active phases | JavaScript ... | Issues | Requests | Errors | Insertion points | |
| 153 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 154 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 155 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 156 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 157 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 158 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 159 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 160 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 161 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 162 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 163 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 164 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 165 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 166 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 167 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 168 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 169 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 170 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 171 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 5 | | | |
| 172 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 173 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 5 | | | |
| 174 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 175 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 176 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 177 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 178 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 179 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 180 | https://www.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 181 | https://www.baidu.com | /s/vsearch | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 182 | https://www.baidu.com | /s/vsearch | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 9 | | | |
| 183 | https://www.baidu.com | /s/vsearch | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 4 | | | |
| 184 | https://www.baidu.com | /sugrec | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 185 | https://www.baidu.com | /sugrec | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | | | | |
| 186 | https://www.baidu.com | /slib/tslib | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 187 | https://www.baidu.com | /ups/submit/addtips | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 188 | https://www.baidu.com | /ups/submit/addtips | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 189 | https://www.baidu.com | /v.gif | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 190 | https://www.baidu.com | /v.gif | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 1 | | | |
| 191 | https://m.baidu.com | /s | Scanning | 1 2 | 1 2 3 4 5 | 1 2 3 | | 6 | | | |
| 192 | http://127.0.0.1 | /example | Errors: request ti... | 1 2 | 1 2 3 4 5 | 1 2 3 | | 6 | 6 | | |

1.2.2 spider进行爬虫过程

Content discovery: https://m.baidu.com/

Control Config Site map

Target

Define the start directory for the content discovery session, and whether files or directories should be targeted.

Start directory: https://m.baidu.com/

Discover: ☒ Files and directories ☐ Files only ☐ Directories only ☒ Recurse subdirectories Max depth: 16

Filenames

Configure the sources Burp should use for generating filenames to test.

☒ Built-in short file list ☒ Built-in short directory list ☒ Built-in long file list ☒ Built-in long directory list ☐ Custom file list: Choose file... ☐ Custom directory list: Choose file... ☒ Names observed in use on target site

Content discovery: https://m.baidu.com/

ControlConfigSite map

Discovery Session Status

Use these settings to monitor and control the discovery session.

Session is running

Requests made:80

Bytes transferred:293,506

Errors:0

Tasks queued:370

Spider requests queued:192

Responses queued for analysis:10

Queued Tasks

| Path | Task | Requests |
|----------|--|----------|
| / | Test observed file names with no extensions | 54 |
| / | Test observed file names with custom extensions | |
| / | Test observed directory names | |
| / | Test short file list with no extensions | |
| / | Test short file list with custom extensions | |
| / | Test short directory list | |
| /bdlogo/ | Test numeric variants on square_ad2862302989e563281adc02ce... | |
| /bdlogo/ | Test numeric variants on square_ad2862302989e563281adc02ce... | |
| /bdlogo/ | Test numeric variants on square_ad2862302989e563281adc02ce... | |
| /bdlogo/ | Test numeric variants on square_ad2862302989e563281adc02ce... | |
| /bdlogo/ | Test numeric variants on square_ad2862302989e563281adc02ce... | |
| /bdlogo/ | Test numeric variants on square_ad2862302989e563281adc02ce... | |
| /bdlogo/ | Test extension variants on square_ad2862302989e563281adc02c... | |
| /l=1/ | Test extension variants on tc | |

1.2.3 爬虫结果

Content discovery: https://m.baidu.com/

ControlConfigSite map

Filter: Showing all items

https://m.baidu.com

| Host | Method | URL | Params | Status | Length | MIME type | |
|---------------------|--------|---------------------------|--------|--------|--------|-----------|--------|
| https://m.baidu.com | GET | / | | 200 | 208721 | HTML | ç0%â%! |
| https://m.baidu.com | GET | /bdlogo/square_ad286... | | 200 | 2400 | PNG | |
| https://m.baidu.com | GET | /l=1/tc | | 200 | 1591 | HTML | |
| https://m.baidu.com | GET | /se/ | | 200 | 16625 | HTML | æ0"ç00 |
| https://m.baidu.com | GET | /se/static/atom/ | | 200 | 16625 | HTML | æ0"ç00 |
| https://m.baidu.com | GET | /se/static/atom/search... | | 200 | 16625 | HTML | æ0"ç00 |
| https://m.baidu.com | GET | /se/static/atom/search... | | 200 | 4242 | XML | |
| https://m.baidu.com | GET | /se/static/atom/search... | | 200 | 1656 | HTML | |
| https://m.baidu.com | GET | /se/static/atom/tc | | 200 | 1654 | HTML | |
| https://m.baidu.com | GET | /se/static/img/iphone/... | | 200 | 17462 | | |
| https://m.baidu.com | GET | /se/static/ima/iphone/... | | 200 | 14251 | PNG | |

RequestResponse

PrettyRawHex

1 GET / HTTP/1.1
2 Host: m.baidu.com
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
7 Connection: close
8
9

INSPECTOR

Search...

0 matches

2 Nmap

扫描目标主机状态和端口

```

(smilin9@kali)-[~]
$ nmap -Pn -sT 111.19.196.24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 15:37 CST
Nmap scan report for 111.19.196.24
Host is up (0.017s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    closed domain
80/tcp    open  http
443/tcp   open  https
843/tcp   open  unknown
1935/tcp  open  rtmp
8080/tcp  open  http-proxy
8088/tcp  open  radan-http

Nmap done: 1 IP address (1 host up) scanned in 28.66 seconds

```

查看指定主机详细信息

```

(smilin9@kali)-[~]
$ nmap -Pn -A 111.19.196.24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 15:39 CST
Nmap scan report for 111.19.196.24
Host is up (0.015s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    closed domain
80/tcp    open  http    nginx
|_http-title: 404 Not Found
|_http-server-header: web cache
443/tcp   open  ssl/http nginx
|_http-title: ERROR: ACCESS DENIED
| ssl-cert: Subject: commonName=www.baishan.com
| Subject Alternative Name: DNS:www.baishan.com, DNS:www.baishancloud.com, DN
S:hls.cntv.baishancdn.cn, DNS:dhls.cntv.baishancdn.cn, DNS:dh5.cntv.baishan
cdn.cn, DNS:hotnews.duba.com, DNS:www.duba.com, DNS:api1.ko.cn, DNS:u.ko.cn,
DNS:*.v.live.baishancdn.cn, DNS:*.kongzhong.com, DNS:*.flash.cn, DNS:*.ffne
ws.cn
| Not valid before: 2022-09-07T00:00:00
|_Not valid after: 2023-08-25T23:59:59
|_tls-nextprotoneg:
|_ h2
|_ http/1.1
|_ssl-date: TLS randomness does not represent time
|_tls-alpn:
|_ h2
|_ http/1.1
|_http-server-header: web cache
843/tcp   open  unknown
8080/tcp  open  http    nginx
|_http-title: 404 Not Found
|_http-server-header: web cache
8088/tcp  open  http    nginx
|_http-title: 403 Forbidden

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.18 seconds

```

扫描指定端口

```
(smilin9@kali)-[~]  
$ nmap -Pn -p 53 111.19.196.24  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 15:41 CST  
Nmap scan report for 111.19.196.24  
Host is up (0.011s latency).  
  
PORT      STATE SERVICE  
53/tcp    closed domain  
  
Nmap done: 1 IP address (1 host up) scanned in 9.83 seconds
```

扫描指定范围端口

```
(smilin9@kali)-[~]  
$ nmap -Pn -p 1-500 111.19.196.24  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 15:42 CST  
Nmap scan report for 111.19.196.24  
Host is up (0.013s latency).  
Not shown: 497 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
53/tcp    closed domain  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 16.58 seconds
```

扫描目标主机操作系统


```

(root@kali)-[~]
# nmap -Pn -A 111.19.196.24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 15:39 CST
Nmap scan report for 111.19.196.24
Host is up (0.015s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    closed domain
80/tcp    open  http    nginx
|_http-title: 404 Not Found
|_http-server-header: web cache
443/tcp   open  ssl/http nginx
|_http-title: ERROR: ACCESS DENIED
|_tls-alpn:
|_  h2
|_  http/1.1
|_ssl-cert: Subject: commonName=www.baishan.com
|_Subject Alternative Name: DNS:www.baishan.com, DNS:www.baishancloud.com, DNS:hls.cntv.baishancloud.cn, DNS:dhls.cntv.baishancloud.cn, DNS:dh5.cntv.baishancloud.cn, DNS:hotnews.duba.com, DNS:www.duba.com, DNS:api1.ko.cn, DNS:u.ko.cn, DNS:*v.live.baishancloud.cn, DNS:*kongzhong.com, DNS:*flash.cn, DNS:*ffnews.cn
|_Not valid before: 2022-09-07T00:00:00
|_Not valid after: 2023-08-25T23:59:59
|_http-server-header: web cache
|_ssl-date: TLS randomness does not represent time
|_tls-nextprotoneg:
|_  h2
|_  http/1.1
843/tcp   open  unknown
1935/tcp  open  rtmp?
8080/tcp  open  http    nginx
|_http-title: 404 Not Found
|_http-server-header: web cache
8088/tcp  open  http    nginx
|_http-title: 403 Forbidden
8090/tcp  open  ssl/http nginx
|_http-title: 400 Bad Request
|_ssl-cert: Subject: commonName=www.baishan.com
|_Subject Alternative Name: DNS:www.baishan.com, DNS:www.baishancloud.com, DNS:hls.cntv.baishancloud.cn, DNS:dhls.cntv.baishancloud.cn, DNS:dh5.cntv.baishancloud.cn, DNS:hotnews.duba.com, DNS:www.duba.com, DNS:api1.ko.cn, DNS:u.ko.cn, DNS:*v.live.baishancloud.cn, DNS:*kongzhong.com, DNS:*flash.cn, DNS:*ffnews.cn
|_Not valid before: 2022-09-07T00:00:00
|_Not valid after: 2023-08-25T23:59:59
|_tls-nextprotoneg:
|_  http/1.1
|_tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
Device type: general purpose|firewall|media device|broadband router|security-misc
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (88%), IPCop 2.X|1.X (88%), Tiandy embedded (87%), D-Link embedded (85%), Draytek embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:ipcop:ipcop:2.0 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:4.9 cpe:/h:dlink:dsl-2890al cpe:/h:draytek:vigor_2960 cpe:/o:linux:linux_kernel:2.6.25.20 cpe:/o:ipcop:ipcop:1.9.19
Aggressive OS guesses: IPCop 2.0 (Linux 2.6.32) (88%), Linux 2.6.32 (88%), Linux 3.2 (88%), Linux 4.9 (88%), Tiandy NVR (87%), D-Link DSL-2890AL ADSL router (85%), Draytek Vigor 2960 VPN firewall (85%), OpenWrt Kamikaze 8.09 (Linux 2.6.25.20) (85%), IPCop 1.9.19 or IPFire 2.9 firewall (Linux 2.6.32) (85%),

```

```

Linux 2.6.36 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 9 hops

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   2.50 ms  XiaoQiang (192.168.10.1)
2   15.55 ms 192.168.1.1 (192.168.1.1)
3   18.77 ms 10.175.8.1 (10.175.8.1)
4   16.69 ms 120.192.234.85
5   20.99 ms 120.192.241.197
6   23.99 ms 111.19.139.162
7   ...
8   22.72 ms 111.19.216.6
9   28.07 ms 111.19.196.24

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 203.49 seconds

```

进行路由追踪

```

(root@kali)-[~]
# nmap -Pn --traceroute 111.19.196.24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 15:48 CST
Nmap scan report for 111.19.196.24
Host is up (0.013s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    closed domain
80/tcp    open  http
443/tcp   open  https
843/tcp   open  unknown
1935/tcp  open  rtmp
8080/tcp  open  http-proxy
8088/tcp  open  radan-http
8090/tcp  open  opsmessaging

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   2.96 ms  XiaoQiang (192.168.10.1)
2   3.65 ms 192.168.1.1 (192.168.1.1)
3   6.38 ms 10.175.8.1 (10.175.8.1)
4   7.49 ms 120.192.234.85
5   12.08 ms 120.192.241.193
6   12.10 ms 111.19.139.174
7   ...
8   10.38 ms 111.19.216.6
9   14.32 ms 111.19.196.24

Nmap done: 1 IP address (1 host up) scanned in 24.56 seconds

```

ping 扫描

```

(root@kali)-[~]
# nmap -Pn -sP 111.19.196.24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 15:50 CST
Nmap scan report for 111.19.196.24
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds

```

使用文件中的 IP 进行批量扫描

```
(root@kali)-[~]
# nmap -Pn -iL ip.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 15:52 CST
Nmap scan report for smilin9-LAPTOP-3HAFFKAJ (192.168.10.37)
Host is up (0.00024s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
2869/tcp  open  icslap
3306/tcp  open  mysql
5357/tcp  open  wsdapi
MAC Address: A8:7E:EA:09:33:28 (Intel Corporate)

Nmap scan report for 192.168.88.1 (192.168.88.1)
Host is up.
All 1000 scanned ports on 192.168.88.1 (192.168.88.1) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 36.152.44.95
Host is up (0.036s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https

Nmap scan report for 111.19.196.24
Host is up (0.013s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    closed domain
80/tcp    open  http
443/tcp    open  https
843/tcp    open  unknown
1935/tcp   open  rtmp
8080/tcp   open  http-proxy
8088/tcp   open  radan-http
8090/tcp   open  opsmessaging

Nmap done: 4 IP addresses (4 hosts up) scanned in 25.04 seconds
```

3 Wireshark

3.1 对网页抓取数据


```

> Frame 4981: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface ens33, id 0
> Ethernet II, Src: VMware_e2:b2:10 (00:50:56:e2:b2:10), Dst: VMware_65:1e:13 (00:0c:29:65:1e:13)
> Internet Protocol Version 4, Src: 91.189.91.48, Dst: 192.168.64.128
> Transmission Control Protocol, Src Port: 80, Dst Port: 42270, Seq: 1, Ack: 88, Len: 147
< Hypertext Transfer Protocol
  < HTTP/1.1 204 No Content\r\n
    < [Expert Info (Chat/Sequence): HTTP/1.1 204 No Content\r\n]
      [HTTP/1.1 204 No Content\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 204
      [Status Code Description: No Content]
      Response Phrase: No Content
      server: nginx/1.14.0 (Ubuntu)\r\n
      date: Thu, 29 Dec 2022 03:58:18 GMT\r\n
      x-networkmanager-status: online\r\n
      connection: close\r\n
      \r\n
4168 66.994140080 34.107.221.82 192.168.64.128 HTTP 270 HTTP/1.1 200 OK (text/plain)
4647 174.327379122 192.168.64.128 185.125.190.48 HTTP 141 GET / HTTP/1.1
4649 174.638359433 185.125.190.48 192.168.64.128 HTTP 201 HTTP/1.1 204 No Content
4831 395.345403129 192.168.64.128 23.215.177.90 OCSP 522 Request
4838 395.421275218 23.215.177.90 192.168.64.128 OCSP 942 Response
4840 395.422879559 192.168.64.128 23.215.177.90 OCSP 522 Request
4850 395.499581987 23.215.177.90 192.168.64.128 OCSP 942 Response
4886 396.212836250 192.168.64.128 23.215.177.90 OCSP 522 Request
4888 396.288940206 23.215.177.90 192.168.64.128 OCSP 942 Response
4979 474.333188084 192.168.64.128 91.189.91.48 HTTP 141 GET / HTTP/1.1
4981 474.652821275 91.189.91.48 192.168.64.128 HTTP 201 HTTP/1.1 204 No Content
5697 659.663754679 192.168.64.128 117.174.183.112 OCSP 520 Request
5699 659.688360633 117.174.183.112 192.168.64.128 OCSP 1151 Response
5998 660.917135867 192.168.64.128 117.18.237.29 OCSP 523 Request
6002 660.917791678 192.168.64.128 117.18.237.29 OCSP 525 Request
6006 660.920456494 192.168.64.128 117.18.237.29 OCSP 525 Request
6010 660.924030795 192.168.64.128 117.18.237.29 OCSP 525 Request
6033 660.959825211 192.168.64.128 117.18.237.29 OCSP 525 Request
> Frame 4981: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface ens33, id 0
> Ethernet II, Src: VMware_e2:b2:10 (00:50:56:e2:b2:10), Dst: VMware_65:1e:13 (00:0c:29:65:1e:13)
> Internet Protocol Version 4, Src: 91.189.91.48, Dst: 192.168.64.128
> Transmission Control Protocol, Src Port: 80, Dst Port: 42270, Seq: 1, Ack: 88, Len: 147
< Hypertext Transfer Protocol
  < HTTP/1.1 204 No Content\r\n
    < [Expert Info (Chat/Sequence): HTTP/1.1 204 No Content\r\n]
      [HTTP/1.1 204 No Content\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 204
      [Status Code Description: No Content]
      Response Phrase: No Content
      server: nginx/1.14.0 (Ubuntu)\r\n
      date: Thu, 29 Dec 2022 03:58:18 GMT\r\n
      x-networkmanager-status: online\r\n
      connection: close\r\n

```

可以看到接口、http请求方法请求目录端口号等

```

4888 396.288940206 23.215.177.90 192.168.64.128 OCSP 942 Response
4979 474.333188084 192.168.64.128 91.189.91.48 HTTP 141 GET / HTTP/1.1
4981 474.652821275 91.189.91.48 192.168.64.128 HTTP 201 HTTP/1.1 204 No Content
5697 659.663754679 192.168.64.128 117.174.183.112 OCSP 520 Request
> Internet Protocol Version 4, Src: 192.168.64.128, Dst: 91.189.91.48
> Transmission Control Protocol, Src Port: 42270, Dst Port: 80, Seq: 1, Ack: 1, Len: 87
< Hypertext Transfer Protocol
  < GET / HTTP/1.1\r\n
    < [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      [GET / HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      Host: connectivity-check.ubuntu.com\r\n
      Accept: */*\r\n
      Connection: close\r\n
      \r\n
      [Full request URI: http://connectivity-check.ubuntu.com/]
      [HTTP request 1/1]
      [Response in frame: 4981]

```

3.2 访问 https, 通过 TLSv1.3 加密

| | | | | | |
|------|---------------|----------------|----------------|---------|--|
| 6981 | 662.138865248 | 117.18.237.29 | 192.168.64.128 | UCSP | 1109 response |
| 6982 | 662.138865248 | 192.168.64.128 | 117.18.237.29 | TCP | 54 48656 → 80 [ACK] Seq=939 Ack=2111 Win=63300 Len=0 |
| 6983 | 662.244119888 | 192.168.64.128 | 111.20.22.124 | TLSv1.3 | 134 Change Cipher Spec, Application Data |
| 6984 | 662.244456722 | 111.20.22.124 | 192.168.64.128 | TCP | 60 443 → 46800 [ACK] Seq=4959 Ack=598 Win=64240 Len=0 |
| 6985 | 662.245360150 | 192.168.64.128 | 111.20.22.124 | TLSv1.3 | 224 Application Data |
| 6986 | 662.245594062 | 111.20.22.124 | 192.168.64.128 | TCP | 60 443 → 46800 [ACK] Seq=4959 Ack=768 Win=64240 Len=0 |
| 6987 | 662.245723030 | 192.168.64.128 | 111.20.22.124 | TLSv1.3 | 512 Application Data |
| 6988 | 662.245933267 | 111.20.22.124 | 192.168.64.128 | TCP | 60 443 → 46800 [ACK] Seq=4959 Ack=1226 Win=64240 Len=0 |
| 6989 | 662.256227507 | 111.20.22.124 | 192.168.64.128 | TLSv1.3 | 738 Application Data, Application Data, Application Data |
| 6990 | 662.256251147 | 192.168.64.128 | 111.20.22.124 | TCP | 54 46800 → 443 [ACK] Seq=1226 Ack=5643 Win=62780 Len=0 |
| 6991 | 662.257309784 | 192.168.64.128 | 111.20.22.124 | TLSv1.3 | 85 Application Data |
| 6992 | 662.257509498 | 111.20.22.124 | 192.168.64.128 | TCP | 60 443 → 46800 [ACK] Seq=5643 Ack=1257 Win=64240 Len=0 |
| 6993 | 662.268224142 | 111.20.22.124 | 192.168.64.128 | TLSv1.3 | 85 Application Data |