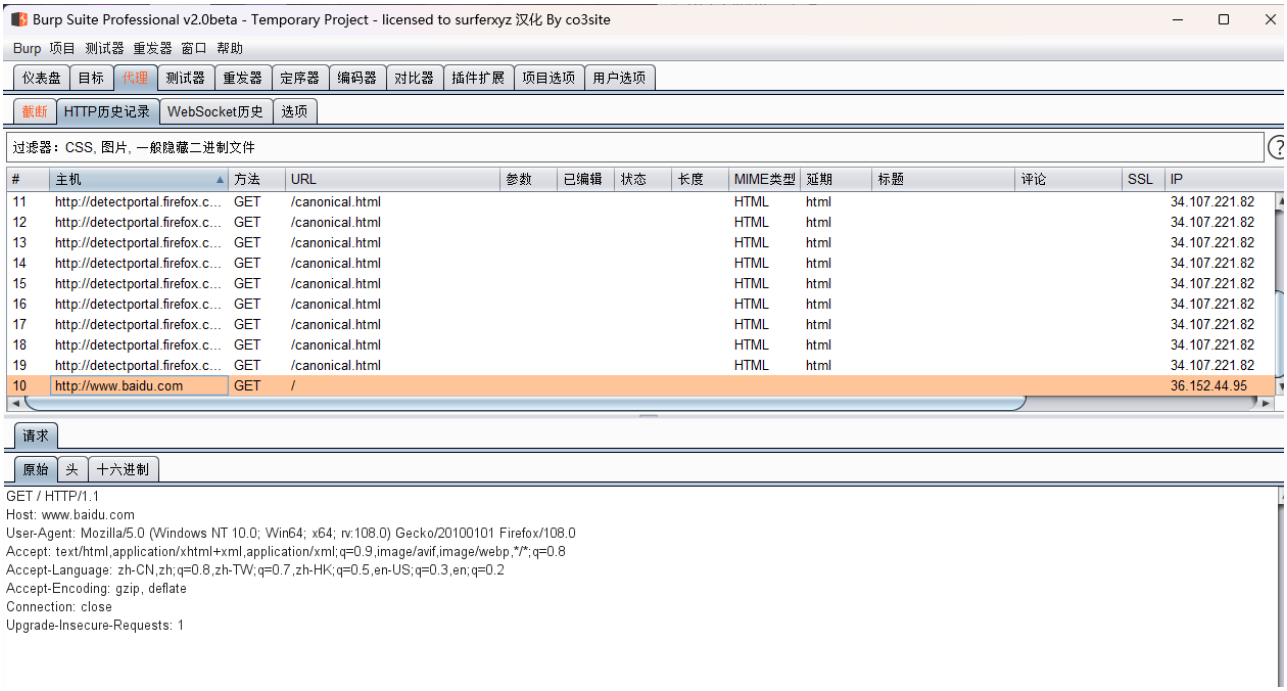
Web上机报告

学号:[redacted] 姓名:[redacted]

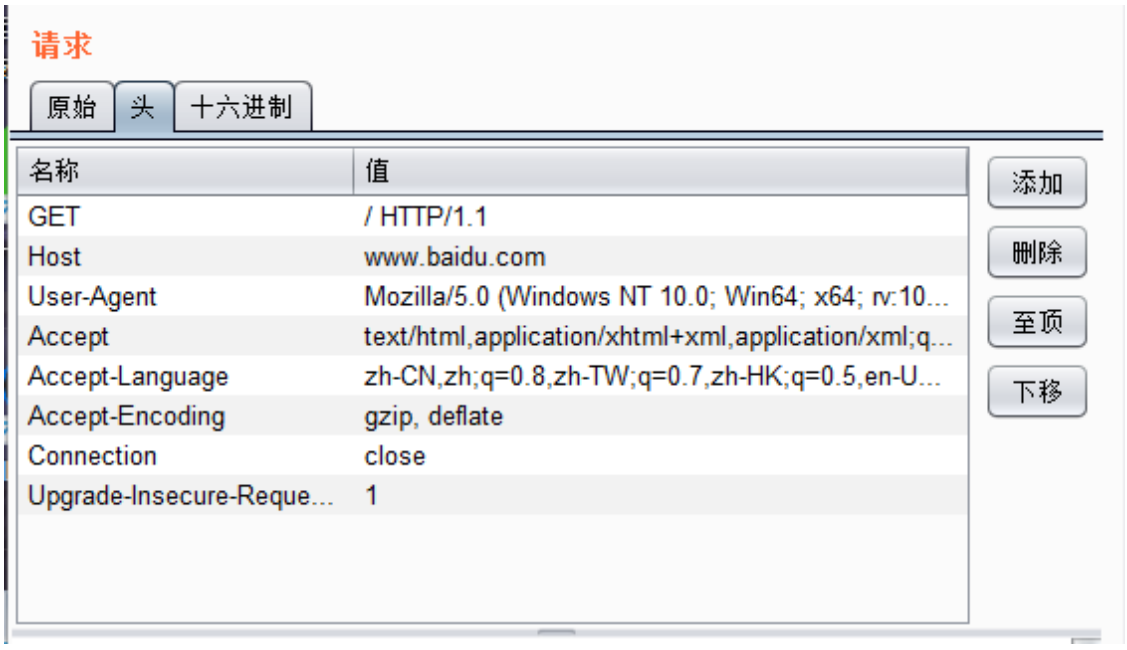
1 Burp Suite

1.1 Burp 代理功能

Firefox 访问百度，拦截可得

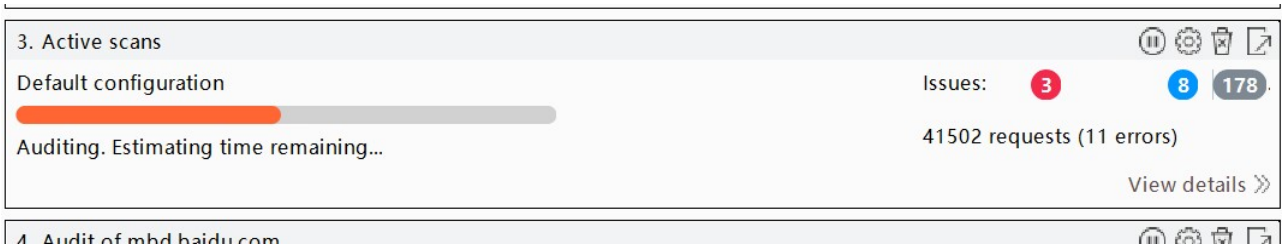


请求参数消息头



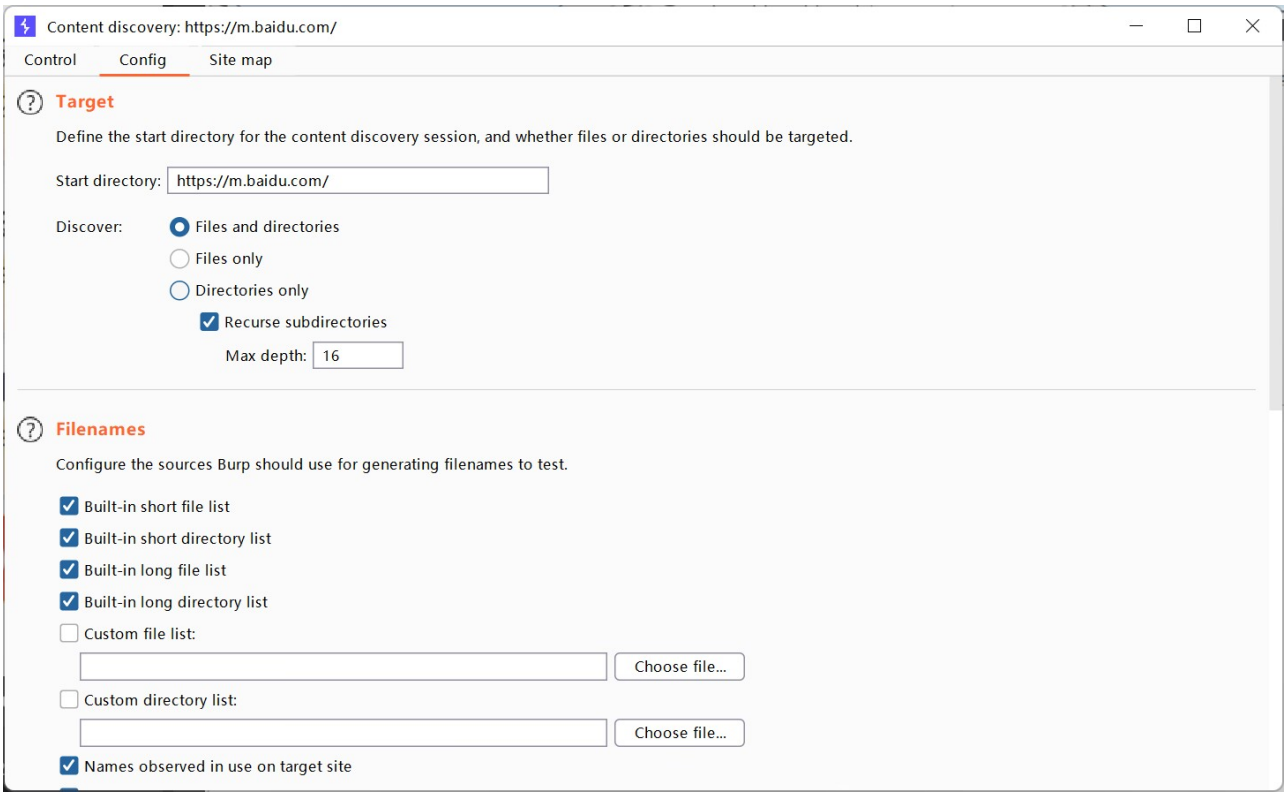
1.2 Burp Scanner 漏洞扫描，Burp spider 进行爬虫

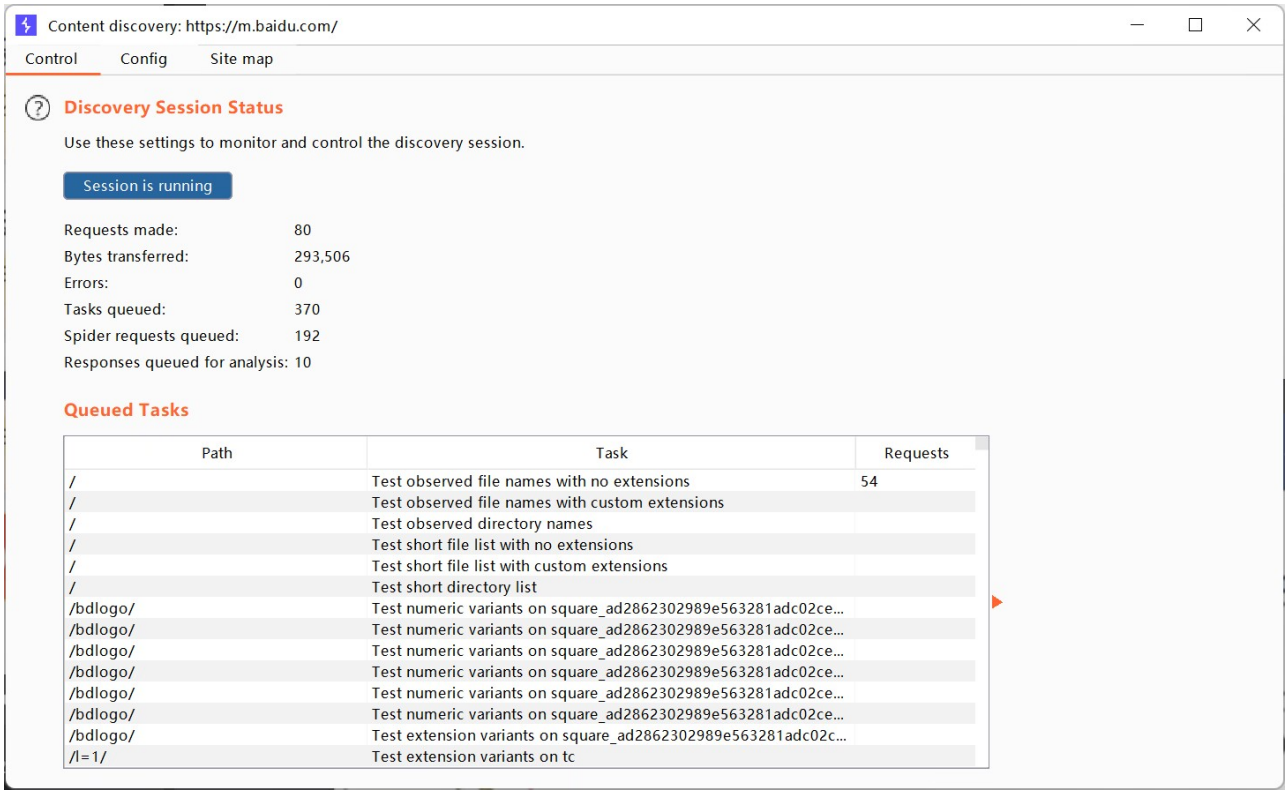
1.2.1 对网页进行扫描



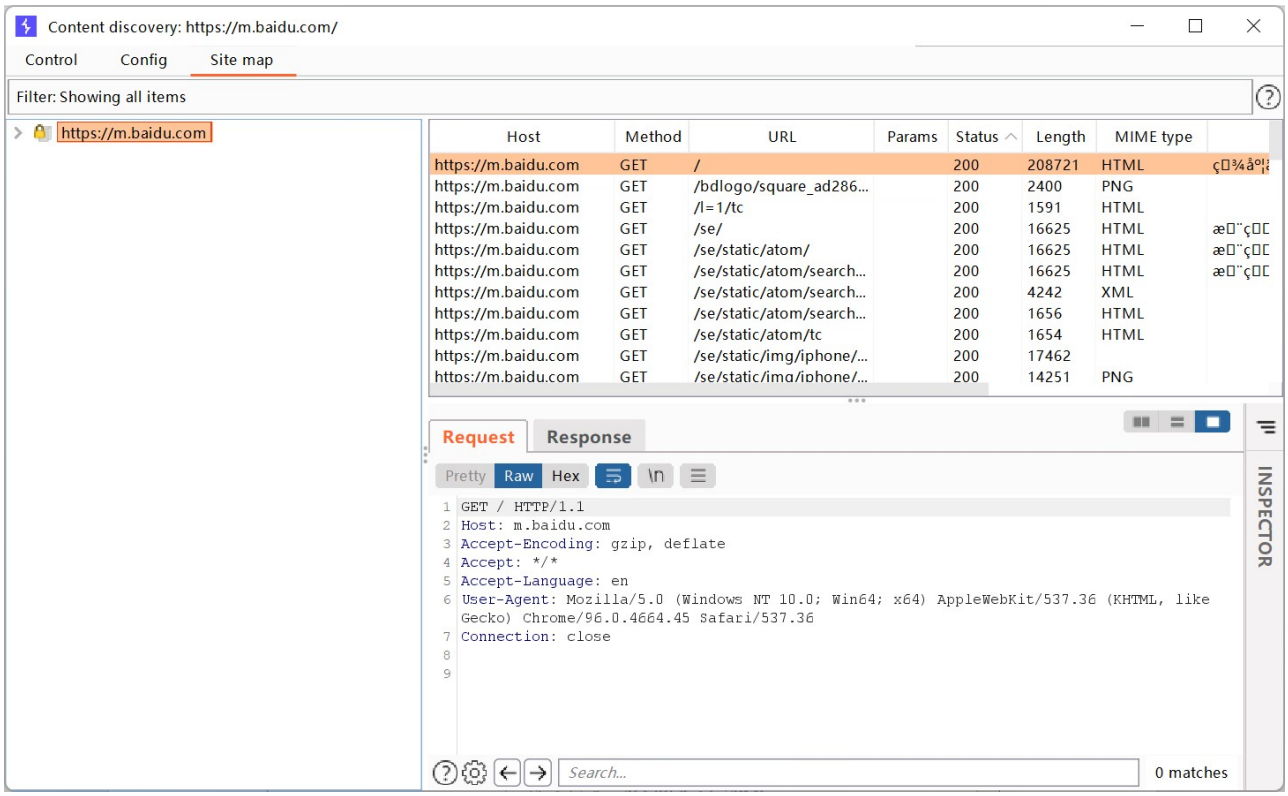
扫描结果

1.2.2 spider进行爬虫过程





1.2.3 爬虫结果



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.baishancdnx.cn, DNS:dhls.cntv.baishancdnx.cn, DNS:dh5.cntv.baishan
cdnx.cn, DNS:hotnews.duba.com, DNS:www.duba.com, DNS:api1.ko.cn, DNS:u.ko.cn,
 DNS:*.v.live.baishancdnx.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, DN
S:hls.cntv.baishancdnx.cn, DNS:dhls.cntv.baishancdnx.cn, DNS:dh5.cntv.baishan
cdnx.cn, DNS:hotnews.duba.com, DNS:www.duba.com, DNS:api1.ko.cn, DNS:u.ko.cn,
 DNS:*.v.live.baishancdnx.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
|_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, DN
S:hls.cntv.baishancdnx.cn, DNS:dhls.cntv.baishancdnx.cn, DNS:dh5.cntv.baishan
cdnx.cn, DNS:hotnews.duba.com, DNS:www.duba.com, DNS:api1.ko.cn, DNS:u.ko.cn,
 DNS:*.v.live.baishancdnx.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:
|_  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%), Tian
dy 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%), Li
nux 3.2 (88%), Linux 4.9 (88%), Tiandy NVR (87%), D-Link DSL-2890AL ADSL rout
er (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	662.138839257	117.18.237.29	192.168.64.128	OCSP	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