

Practical 4a

Objectives: Use dig, host, nslookup and zone transfers for footprinting
Gather information from the Internet

Exercise 1. Gathering Information from the Internet

- Google Search can help in finding useful information.
Go to www.google.com and search for “singapore polytechnic +tel” to get some telephone numbers in Singapore Polytechnic.
- In Google, search for “site:.sp.edu.sg email” to search for the word “email” appearing in sp.edu.sg website.
Search for “site:.sp.edu.sg login” to search for the word “login” appearing in sp.edu.sg website, including login forms.
- You can also use Google Advanced Search. Visit www.google.com/advanced_search to see how detailed your search can be.
- Netcraft provides useful information on websites around the world. Browse to www.netcraft.com. Scroll down to find the section for What’s that site running. Enter “https://www.yahoo.com” (or any other website).
Look through the results to see what Netcraft can find out about the website.
- Try searching the Whois databases.
 - Go to <https://search.arin.net/rdap>.
 - In the Search Whois textbox, type “MIT” (or Massachusetts Institute of Technology)
 - You may need to click on “Search ARIN’s Whois instead”. You may see some network ranges listed. You may also see names and emails of technical staff.

Source Registry	ARIN
Kind	Individual
Full Name	[REDACTED]
Handle	[REDACTED]
Email	[REDACTED]@mit.edu
Telephone	+1-617-910-[REDACTED]

Source Registry	ARIN
Net Range	129.55.0.0 - 129.55.255.255
CIDR	129.55.0.0/16
Name	MIT-LL2
Handle	NET-129-55-0-0-1
Parent	NET-129-0-0-0-0
Net Type	DIRECT ASSIGNMENT

- Go to www.network-tools.com.
- Under Tool, select Whois Search. Search for “sp.edu.sg”. You can see the details of the DNS servers for sp.edu.sg. You may also see some emails or telephones belonging to Singapore Polytechnic.
- Under Tools, select DNS. Search for “sp.edu.sg” again. You can also see the details of the DNS servers for sp.edu.sg, indicated by “NS” for nameserver.
- Under Tools, select Network Lookup. Search for “sp.edu.sg” again. You can see that cloud technologies are being used.
Is there a contact person in charge of Singapore Polytechnic’s domain registration?

- (h) You can also make whois queries through a command line. In Kali, type the following command :
- ```
whois sp.edu.sg
```
6. The website ipinfo.io provides information on IP addresses. The free service is limited to 1000 requests per day.
- (a) Go to <https://ipinfo.io>. You will see your current IP address that is seen by the Internet.
- (b) Add to the URL any IP address that you want to get information about (eg <https://ipinfo.io/216.58.221.78>). The website will provide details on which country owns the IP address.
- (c) You can also make queries to ipinfo.io through a command line. In Kali, type the following command :
- ```
curl ipinfo.io/216.58.221.78
```
7. Browse to www.shodan.io. Search for “webcam”.
- Without a login account, Shodan returns a limited set of results. You can click on the webcams found, and see what ports they are running on.

Exercise 2. Use dig, host, nslookup and zone transfers for footprinting

Description :

A DNS Server for the domain “example.com” has been set up on web-server2.

8. In Kali Linux, look at the man pages for dig and host.
- ```
man dig
man host
```
9. Run the dig command to find the IP address of server.example.com from the DNS Server on web-server2. The IP address would appear under the ANSWER section.

`dig server.example.com @192.168.13.100` ← Change to web-server2 IP

```
$ dig server.example.com @192.168.153.165
; <<>> DiG 9.16.11-Debian <<>> server.example.com @192.168.153.165
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29130
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;server.example.com. IN A

;; ANSWER SECTION:
server.example.com. 86400 IN A 192.168.6.200
;; AUTHORITY SECTION:
example.com. 86400 IN NS server.example.com.

;; Query time: 0 msec
;; SERVER: 192.168.153.165#53(192.168.153.165)
;; WHEN: Sun Apr 25 01:57:00 EDT 2021
;; MSG SIZE rcvd: 77
```

IP address of server.example.com returned by the DNS Server running on web-server2

10. Run the host command to find the IP address of server.example.com from the DNS Server on web-server2.

```
host server.example.com 192.168.13.100 ← Change to your web-server2 IP
```

11. On Windows (either Host PC or VM), you can use the nslookup command. In Windows, run the following commands to query the DNS Server on your web-server2 to find the IP address of server.example.com.

#### nslookup

Default Server: mydns.dmit.local

Address: 192.168.10.10

```
>server 192.168.13.100 ← Set the DNS Server to your web-server2
```

Default Server: [192.168.13.100]

Address: 192.168.13.100

```
>server.example.com
```

.... IP address displayed

```
>quit
```

12. If you have an IP address and you want to find its hostname, you can do a DNS reverse lookup. Try any of the following methods to do a DNS reverse lookup.

For example, to use Kali to query the DNS Server on web-server2 to find the hostname of 192.168.6.201, you can use the dig command:

```
dig -x 192.168.6.201 @192.168.13.100 ← Change to web-server2 IP
```

Or the host command:

```
host 192.168.6.201 192.168.13.100 ← Change to web-server2 IP
```

To use Windows to query the DNS Server on web-server2 to find the hostname of 192.168.6.201, you can use nslookup

#### nslookup

Default Server: mydns.dmit.local

Address: 192.168.10.10

```
>server 192.168.13.100 ← Set the DNS Server to your web-server2
```

Default Server: [192.168.13.100]

Address: 192.168.13.100

```
>set type=ptr
```

```
>192.168.6.201
```

.... hostname displayed

13. In Kali Linux, run the following command to do a zone transfer of the domain example.com from the DNS Server.

```
dig @192.16.13.100 example.com axfr
```

Remember to set the DNS Server to web-server2 IP

How many hosts (with IP addresses) can you find? Is there any host you would be interested in?

Note : As the records in a zone transfer can give away info about the network setup to a potential hacker, most DNS Servers do not allow zone transfers. Or only authorised systems can perform a zone transfer.

### Exercise 3. Finding Network Information about a company

In this exercise, we will try using DNS to find out information about a domain. We use the domain sp.edu.sg just as an example.

14. In Kali Linux, using the dig command, find out the domain information about www.sp.edu.sg
- ```
dig www.sp.edu.sg
```

15. Use the dig command to find out the information about DNS Servers in the domain sp.edu.sg.
- ```
dig -t ns sp.edu.sg
```

(Note : You may get different results from the following screenshot as organisations may have changed their network setup)

```

└─$ dig -t ns sp.edu.sg

; <<>> DiG 9.16.11-Debian <<>> -t ns sp.edu.sg
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 54735
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;; MBZ: 0x0005, udp: 1280
;; QUESTION SECTION:
;sp.edu.sg. IN NS

;; ANSWER SECTION:
sp.edu.sg. 5 IN NS nova.np.edu.sg.
sp.edu.sg. 5 IN NS sspwb100.sp.edu.sg.
sp.edu.sg. 5 IN NS sspwb110.sp.edu.sg.

;; ADDITIONAL SECTION:
nova.np.edu.sg. 5 IN A 153.20.24.71
nova.np.edu.sg. 5 IN AAAA 2402:a900:0:24::71

```

The Answer section shows the DNS Servers for sp.edu.sg. You may get different results

The Additional section may give the IP addresses for the servers listed in Answer section. If IP addresses are not listed, you can do a dig on the names of the DNS Servers to find their IP addresses.

How many DNS Servers are there for sp.edu.sg? Do you have their hostnames?

16. In the screenshot above, the IP addresses for the DNS Server sspwb100.sp.edu.sg and sspwb110.sp.edu.sg are not listed. Use the dig command to find their IP addresses.
- ```
dig sspwb100.sp.edu.sg
```

17. Use the dig command to find out the information about Mail Servers in the domain sp.edu.sg

```
dig -t mx sp.edu.sg
```

(Note : You may get different results from the following screenshot as organisations may have changed their network setup)

```

L$ dig -t mx sp.edu.sg


; <<>> DiG 9.16.11-Debian <<>> -t mx sp.edu.sg
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13166
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, MBZ: 0x0005, udp: 1280
;; QUESTION SECTION:
;sp.edu.sg.                IN      MX

;; ANSWER SECTION:
sp.edu.sg.                 5       IN      MX      1 spoly.in.tmes.trendmicro.com

```

The Answer section shows the Mail Servers for sp.edu.sg



18. How big is the sp.edu.sg network? We can use whois to find out.
In Kali Linux, use the whois command on one of the IP addresses belonging to sp.edu.sg domain.

For example :

```
whois 164.78.252.50
```

You can also use www.network-tools.com and do a Network Lookup on the IP address

You may be able to see an IP address range belonging to sp.edu.sg domain.

19. Using host command, we can check to see if a particular IP has a hostname registered in the DNS. Choose one of the IP addresses from the range of IPs you have found.

For example,

```
host 164.78.252.51
```

Do you see any hostname?

Try running “host 164.78.252.2”, and then “host 164.78.252.3”, etc. (Change the IP addresses to the range of IPs you have found)

20. It is possible to run through all the IP addresses in the range to see which IP has a hostname registered in the DNS.

Of course, to be effective, a script can be used to automate this.

Exercise 4. Finding information on intermediate nodes

21. What is between you and a server? Use traceroute (or tracert on Windows) to find out the nodes between your machine and an external IP address.

tracert 205.166.76.8 (you can use any reachable IP)

22. Traceroute may not work with virtual machines using NAT network adapter. Try running the Windows command “tracert” on the Host PC.

tracert 205.166.76.8 (you can use any reachable IP)

```
C:\>tracert 205.166.76.8

Tracing route to noa3dns-w.nintendo.com [205.166.76.8]
over a maximum of 30 hops:

  1  7 ms    5 ms    5 ms  164.78.252.1
  2  7 ms   13 ms   5 ms  192.168.220.201
  3  8 ms    5 ms    9 ms  164.78.250.41
  4  8 ms    9 ms    5 ms  gi-1-1-2.a064.m1net.com.sg [203.123.26.49]
  5 11 ms    6 ms    6 ms  xe-8-2-0.a089.m1net.com.sg [203.211.158.141]
  6 13 ms    7 ms    8 ms  te-1-2.a062.m1net.com.sg [203.211.158.73]
  7  8 ms    7 ms    9 ms  ix-xe-10-1-2-0.tcore1.svw-singapore.as6453.net [180.87.12.209]
  8 95 ms   80 ms  117 ms  if-et-23-2.hcore2.kv8-chiba.as6453.net [180.87.67.33]
  9 194 ms  206 ms  198 ms  if-ae-53-2.tcore2.lvw-los-angeles.as6453.net [64.86.252.56]
 10 206 ms  203 ms  201 ms  if-ae-2-2.tcore1.lvw-los-angeles.as6453.net [66.110.59.1]
 11 305 ms  310 ms  300 ms  los-brdr-02.inet.qwest.net [63.146.26.145]
 12 304 ms  305 ms  309 ms  sea-edge-13.inet.qwest.net [67.14.41.66]
 13 307 ms  300 ms  304 ms  63.147.70.18
 14 388 ms  412 ms  399 ms  noa3dns-w.nintendo.com [205.166.76.8]

Trace complete.
```

Sample output of a traceroute. Sometimes the intermediate routers do not return any info, so you see a series of * instead.

23. Alternatively, you can use online traceroute websites.

Go to www.traceroute.org

- Choose a server near you and start tracing to the target IP. Traceroute will return a list of IP addresses.
- You may be able to see an IP address before it reaches 205.166.76.0/8, ie. the target network. This IP could be the organisation's ISP or hosting service.
- You can use various methods to learn more about the IP addresses listed (eg whois, dig, online search).

```
Traceroute From Singapore To (Hostname/IP Address):

Traceroute Result:

traceroute to 205.166.76.8 (205.166.76.8), 30 hops max, 60 byte packets
 1  ge2-8-r01.sin01.ne.com.sg (202.150.221.169)  0.167 ms  0.167 ms  0.166 ms
 2  10.15.62.222 (10.15.62.222)  33.091 ms  33.208 ms  33.212 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  NINTENDO-OF.ear3.Seattle1.Level3.net (4.16.169.178)  204.520 ms  !X * *

Traceroute Completed.
```

Sample output of a traceroute using online traceroute sites

Task :

Using the publicly available online search engines and tools you have learnt, try to find the following information :

(a) Finding out about Domain information :

- 1) Who is the owner of the domain coca-cola.com?
You can use the Whois to find the owner of a domain.
(eg In Kali, run whois coca-cola.com)
- 2) How is the website www.coca-cola.com hosted? Is it using a Content Delivery Network?
When doing a dig or nslookup on www.coca-cola.com, the hostname returned seems to be Cloudfront – it seems to be using Content Delivery Network

(b) Finding out more about the networks: centurylink.com:

- 1) What are some IP addresses belonging to centurylink.com?
If using www.network-tools.com, do a Network Lookup for centurylink.com. An IP range 155.70.0.0 - 155.70.255.255 is returned
- 2) What are the live systems in the IP range (that belongs to centurylink.com)?
In Kali, can run "dig -t mx centurylink.com" to find mail servers belonging to centurylink.com and then dig for their IP addresses.
Can try "host 155.70.50.75" or "ping 155.70.32.51" to see which systems are up.
To test the whole range, a script can be used. If ping is used, remember that not all systems may reply to a ping echo request.
- 3) Any mail server in centurylink.com?
In Kali, can run "dig -t mx centurylink.com" to find mail servers belonging to centurylink.com and then dig for their IP addresses.

(c) Finding out about the company

- 1) Find career postings for IT staff for a company. What sort of technologies are listed in the job advertisement? This may also give you a clue on the technologies used at that company.

Example of a Job Posting**System Administrator****Job Description****Description:**

- Design and implemented Integration between Active Directory with Azure Active Directory using DirSync and Azure Active Directory Connect.
- Design and Implemented Active Directory Domain Consolidation and Tier0 Consolidation meeting EY business compliance.
- Collaboration and implemented Enterprise wide DNS Migration to Bluecoat proxy
- Review the solutions designed by the Technical Engineers

These may be the technologies used in the company

(d) Finding out more about a person:

Do a web search for a person's name.

You may be surprised by the amount of information available for a person on the Internet.

Read the following article on guessing email addresses:

http://email.about.com/od/addresssearchtip/qt/guess_address.htm

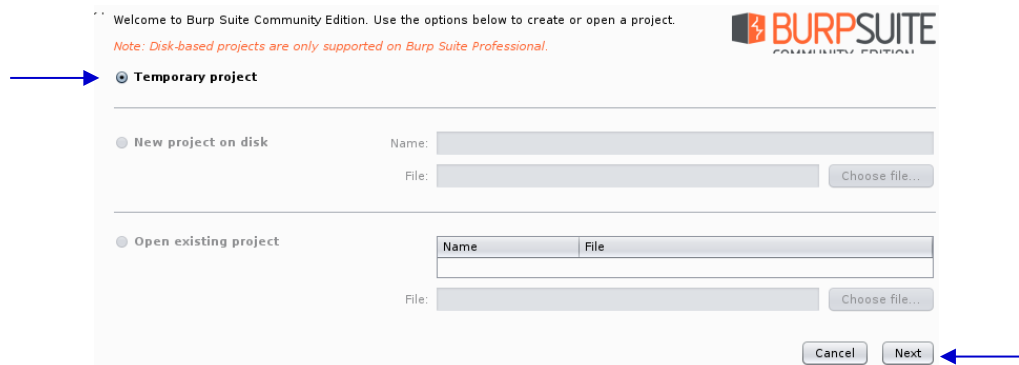
Exercise 5. Using Web Tools for fingerprinting

Description:

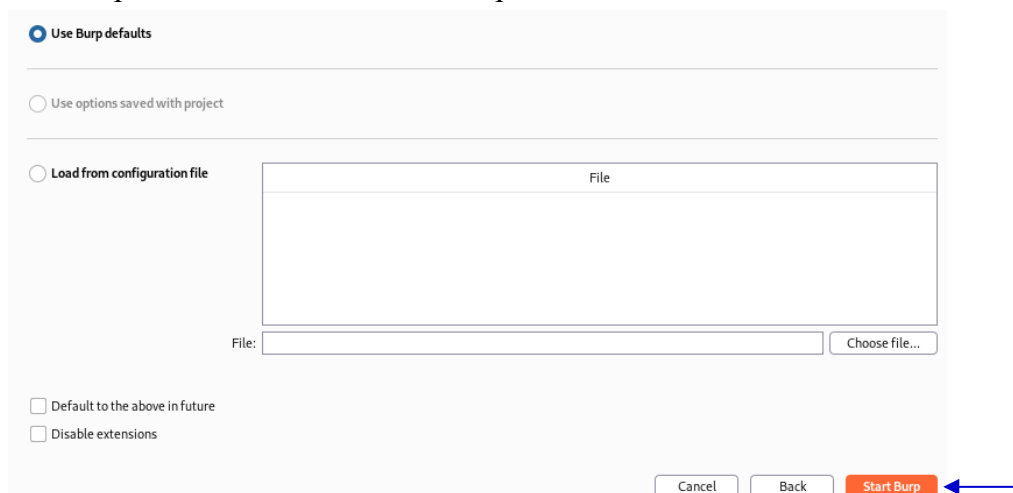
BurpSuite can be used for gathering information from a web site.

In Kali VM

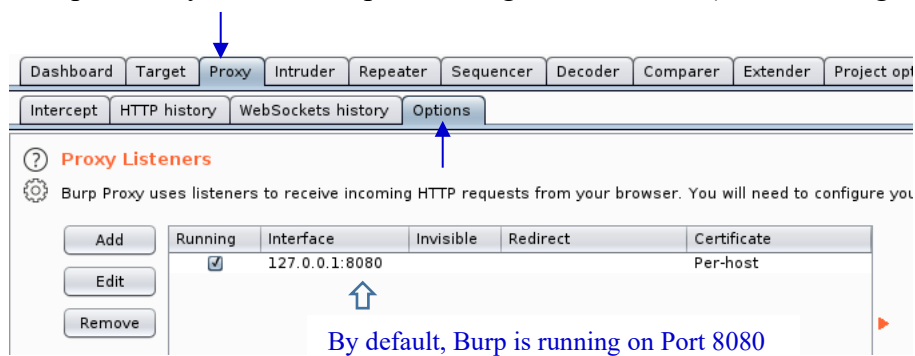
24. Click on the Kali icon in the top left corner and go to 03 Web Application Analysis -> burpsuite. Or in a terminal, type "burpsuite". If there is a message about the Java JRE, click OK. You will need to Accept the Terms and Conditions for the BurpSuite Community Edition. If asked to update the software, you can click Cancel.
25. Select Temporary Project and click Next. (see following diagram)



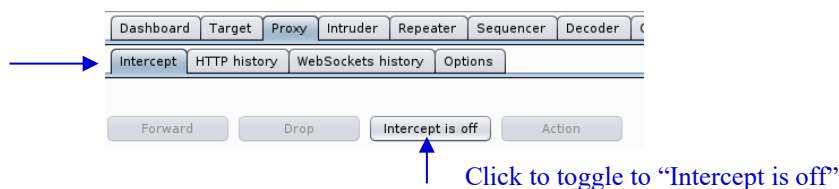
26. Use Burp Defaults and click Start Burp.



27. To see which port Burp is running on, click on the Proxy tab. Under the Proxy tab, click on Options. By default, Burp is running on Port 8080. (see following diagram)

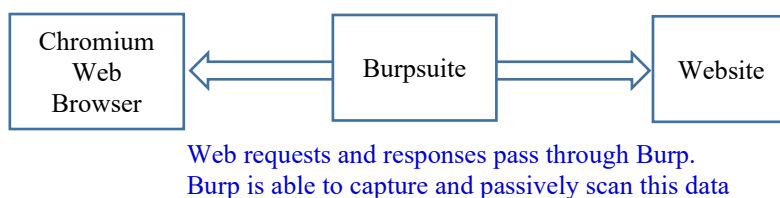


28. Under Proxy tab, click on Intercept tab. Click on the Intercept button to toggle to “Intercept is off”. (see following diagram)

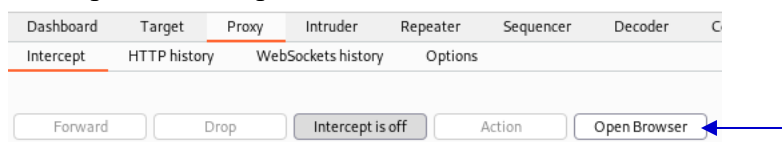


29. In a terminal, type “netstat -tuna” to check that Burp is running on port 8080.

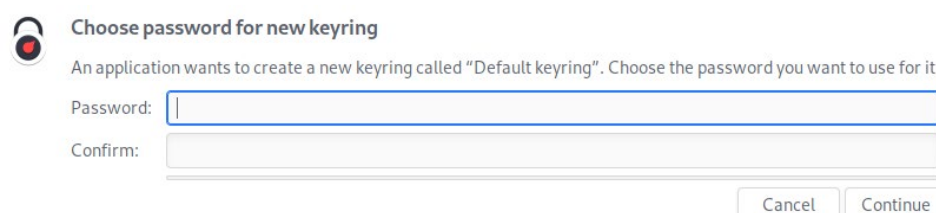
BurpSuite has provided an embedded Chromium Web Browser that we can use to browse the Internet. By using this Chromium Web Browser, all our web requests and responses will pass through Port 8080, where Burp is running. Burp is able to passively scan this data.



30. In Burp, click on Open Browser.



31. The Chromium Web Browser is started up. If the following dialog box about “keyring” appears, just click Cancel.



32. Browse to a web site (eg www.sp.edu.sg).
33. You may see a warning as the Web Browser has detected that Burp has intercepted and changed the certificate of the webpage. You can click to check the reason of the warning (the certificate is issued by PortSwigger, and not Singapore Polytechnic).
34. Browse a few pages in the website.
35. In Burp, click on the Target tab. Under the Site Map tab, you will see a list of the web resources mapped by Burp. (see following diagram)

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment
https://www.sp.edu.sg	GET	/		200	85534	HTML	Singapore Polytechnic	
https://www.sp.edu.sg	GET	/Cwp/assets/scripts/main.js		200	839380	script		
https://www.sp.edu.sg	GET	/Telarik.Web.UI.WebResource.axd?T...		200	145042	script		
https://www.sp.edu.sg	GET	/WebResource.axd?d=pynGmcFUVL...		200	24301	script		
https://www.sp.edu.sg	GET	/Cwp/assets/scripts/jquery.min.js		200	87730	script		
https://www.sp.edu.sg	GET	/js		200	70735	HTML	School of Business	
https://www.sp.edu.sg	GET	/sp/admissions/admissions-exercises		200	64056	HTML	Admissions Exercises	
https://www.sp.edu.sg	GET	/sp/admissions/admissions-exercise...		200	65083	HTML	Overview	
https://www.sp.edu.sg	GET	/sp/admissions/admissions-exercise...		200	64788	HTML	How to Apply	
https://www.sp.edu.sg	GET	/sp/education/schools		200	66690	HTML	Schools	
https://www.sp.edu.sg	GET	/Cwp/assets/fonts/icomoon.ttf?m0b9a1		200	538	HTML	301 Moved Permanently	

Request Response

Raw Headers Hex HTML Render ViewState

```

1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Date: Sat, 18 Apr 2020 04:30:42 GMT
5 Set-Cookie: rp_www.sp.edu.sg=2df1004f3ff6d70708982ea7255210ee; httponly; path=/; secure; HttpOnly
6 Set-Cookie: AWSALB=
/FH54d+u0XB1AFG5xHcxjsBgUM+vu0c+uWcj d0u3wPKFAa9f7E9yqtj;MhEkE68QkbKXp290Sc/Rz3eQ3HFFPOV+rEmHAAARHkEzzHh9xVWsoSp07gzruQnk;
Expires=Sat, 25 Apr 2020 04:30:40 GMT; Path=/
7 Set-Cookie: AWSALBCORS=
/FH54d+u0XB1AFG5xHcxjsBgUM+vu0c+uWcj d0u3wPKFAa9f7E9yqtj;MhEkE68QkbKXp290Sc/Rz3eQ3HFFPOV+rEmHAAARHkEzzHh9xVWsoSp07gzruQnk;
Expires=Sat, 25 Apr 2020 04:30:40 GMT; Path=/; SameSite=None
8 Strict-Transport-Security: max-age=31536000
9 X-FRAME-OPTIONS: SAMEORIGIN
10 X-Content-Type-Options: nosniff
11 Cache-Control: max-age=86400, public
12 X-XSS-Protection: 1; mode=block
13 X-Access-Control-Allow-Origin: *
14 Vary: Accept-Encoding
15 X-Cache: Miss from cloudfront

```

These are the HTTP Response headers of the Web Response packet.

36. In the above diagram, in the left hand pane, if you click on the hostname (for example, <https://www.sp.edu.sg>), you will see a list of the web requests sent to that host in the right top pane. Click on any of the web requests, and you can see the packet details of the Request and Response packets for that particular request.

Exercise 6. Viewing HTTP headers

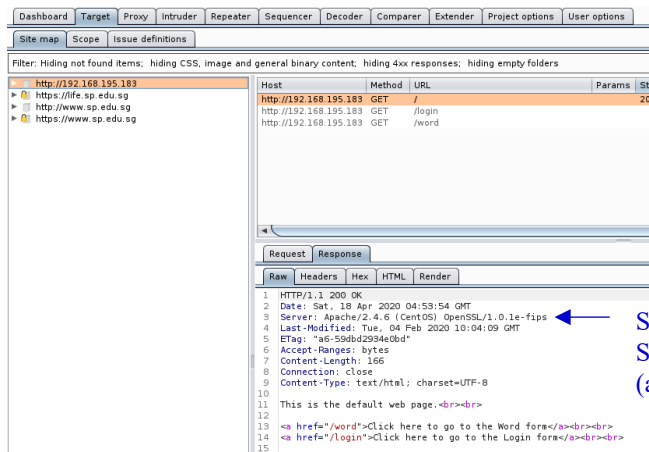
There are multiple ways to view the HTTP request and response headers sent by web browsers and web servers. One way is by using intercepting web proxies like BurpSuite like in the previous exercise. Many Web Browsers nowadays have built-in Developer Tools which can also allow us to view the HTTP request and response headers.

37. Power on the web-server2 VM.

In Kali

38. Run Burp. In the Proxy tab, check that "Intercept is off".
39. In Burp, under the Proxy tab, click Open Browser to start the Chromium Web Browser.
40. Browse to the IP address of your web-server2.

41. In Burp, under Target tab and Site Map tab, look at the HTTP response headers of the Response packet sent by web-server2. Can you tell which web server is being used?



Sometimes the HTTP response headers contain the Server field, which can tell us which web server (and even the operating system) is being used.

42. Close the Chromium Web Browser and exit Burp.

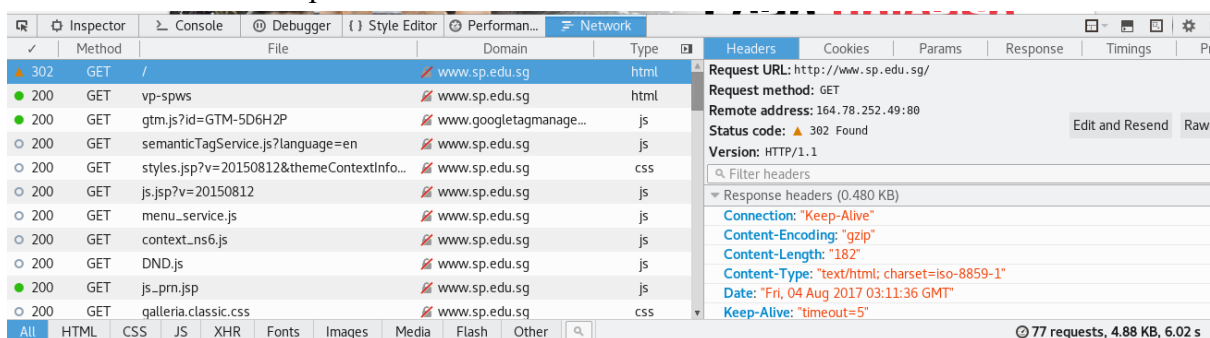
Using the Web Browser's built-in Developer Tools to view HTTP headers

Most web browsers nowadays have built-in Developer Tools that you can use to view network packets, and HTTP details.

In any system (Kali or Host PC)

43. In any Web Browser, press F12 to bring up the Developer Tools window.
 44. Click on Network tab.
 45. Browse to a website. You will see a list of network packets displayed in the Developer Tools window.
 46. Click on any network packet. In the right hand side, you can see the Request and Response headers.

Sometimes the Response headers will contain information about the Web Server.



47. Press F12 again to close the Developer Tools.

Exercise 7. Viewing Email headers

Description:

Email headers are useful when tracing the origins of an email. Email headers are normally hidden by most mail software, but there is usually an option to display them.

As an email is passed from one mail server to another, a new email header is added to the top.

The From and To headers in an email can be easily forged so the Received headers can provide a clue to where the email really comes from. However, hackers can add fake Received headers at the bottom of the list.

The X-Originating-IP header usually can tell us the IP address of the computer that had sent the email. If it is not present, however, the Received headers have to be checked.

Email header example 1

```
X-Apparently-To: customer@yahoo.com; Tue, 16 Apr 2019 19:06:14 +0000
Return-Path: <bounce@t.mail.coursera.org>
Received-SPF: pass (domain of t.mail.coursera.org designates 52.40.63.39 as
permitted sender)
X-Originating-IP: [52.40.63.39]
Authentication-Results: mta4121.mail.ne1.yahoo.com
  header.i=@t.mail.coursera.org; header.s=scph0616; dkim=pass (ok)
Received: from 127.0.0.1 (EHLO mta1b3.mail.coursera.org) (52.40.63.39)
  by mta4121.mail.ne1.yahoo.com with SMTPS; Tue, 16 Apr 2019 19:06:14 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=t.mail.coursera.org;
  s=scph0616; t=1555441574; i=@t.mail.coursera.org;
  bh=xfjjtNoG9cDwN2WG44diCEw3emOY/6LON5AtlyURhV4=;
  h=To:Message-ID:Date:Content-Type:Subject:From;
  b=WHtl3UbJz0zff4tOjGe9ZRcqjYftZHYu4E55DRfDdeqHM1EUCMhHhBsr8nGAYn2O1
  osBPZmd0Z3B69HtXUtGwLJa30gFVcIcflUNUXype6uvgyUPML5d387YCgn26lLoeXT
  2XnCWVulotBOWsSasyFaALwaqOPg2h9aSjaVNLPqE=
X-MSFBL: osnZjuM6KhUUNZX/3sop661yRvbwSeSFnsxb2c9j/6k=|eyJzdWJhY2NvdW50X2l
  kIjoIMCIsIm1lc3NhZ2VfaWQiOiIwMDI1YTtyN2I2NWNjODI2OTg5YiIsInRlbnM
  udF9pZCI6ImNvdXJzZXJhIiwiaWY3VzdG9tZXJfaWQiOiIwIiwiciI6InllaWx1ZW5
  AeWFob28uY29tIn0=
To: <customer@yahoo.com>
Message-ID: <89.B9.09928.6A726BC5@ak.mta2vrest.cc.pr.d.sparkpost>
Date: Tue, 16 Apr 2019 19:06:14 +0000
Content-Type: multipart/alternative; boundary="_----
OAYR0Q4FNgaDyh/WNUvXcQ===_09/B9-09928-6A726BC5"
MIME-Version: 1.0
Subject: Deadlines for Online Degrees
From: "University of Michigan" <no-reply@t.mail.coursera.org>
Content-Length: 47897
```

48. Determine the IP address where the above email came from.

Where is it from? (you can try nslookup, dig or whois)

Email header example 2

```
X-Apparently-To: customer@yahoo.com; Tue, 09 Apr 2019 07:34:33 +0000
Return-Path: <arleen@porcupinelampnet.com>
X-YahooFilteredBulk: 59.93.163.67
Received-SPF: none (domain of porcupinelampnet.com does not designate permitted sender hosts)
X-Originating-IP: [59.93.163.67]
Authentication-Results: mta4489.mail.bf1.yahoo.com from=porcupinelampnet.com; dkim=neutral (no sig)
Received: from 127.0.0.1 (EHLO arleen.porcupinelampnet.com) (59.93.163.67) by mta4489.mail.bf1.yahoo.com with SMTP; Tue, 09 Apr 2019 07:34:26 +0000
Date: 9 Apr 2019 13:3:51
From: Cherry Edwards <arleen@porcupinelampnet.com>
Reply-To: arleen@porcupinelampnet.com
X-Priority: 3 (Normal)
To: customer@yahoo.com
Subject: Save 80% from this Pharmacy
```

49. Determine the IP address where the above email came from.
50. You can also try online email header analysers. For example, browse to the following URL and paste the email headers of one of your emails to find out where the email is from.

<https://www.whatismyip.com/email-header-analyzer>

Exercise 8. What information am I giving to websites?**Description:**

When we browse websites, we are also giving information about our client setup to the web servers.

51. On your Host PC, go to www.ipgoat.com. The public IP address that you are providing to the Internet is listed, plus other details.
52. Click on the link “More Info” to see more information that your web browser can provide to the web server.

End of Practical

Practical 4b

Objectives: Use nmap and other port scanning software
 Try ping sweeps
 Use hping to craft packets

Exercise 1. Use nmap and inspect the packets sent

Description :

You will be running nmap against your web-server2 VM. Your web-server2 will have several services running, but not the Telnet server. The firewall on the web-server2 will allow clients to connect to a number of ports, including the Telnet port 23.

In web-server2

1. Check that the firewall configuration file /etc/firewalld/zones/public.xml contains the following line to allow incoming connections to Telnet port 23.

```
<service name="telnet"/>
```

If the above line is not in the file, add it in. Run “systemctl restart firewalld” to restart the Firewall.

2. Edit the file /etc/xinetd.d/telnet. Change the following line to disable telnet

```
disable = yes
```

3. Restart the xinetd service if it is not already running.

```
systemctl restart xinetd
```

In Kali Linux

4. Look at the options available for nmap.

```
nmap -h
```

What is the option for running a SYN Scan? (Ans : -sS)

5. Start a Wireshark capture.

6. Use nmap to run a SYN scan against your web-server2.

```
sudo nmap -sS 192.168.10.100
```

← Change to the IP of your web-server2

7. Stop Wireshark when nmap has finished running.

8. Look at the results of nmap. Port 21 and other ports are reported as “opened”, while Port 23 is reported as “closed”.

9. In Wireshark, apply the following filter to see only the SYN packets.

Filter: `tcp.flags.syn == 1`

10. Scroll through the filtered packets to see the ports targeted. Look for any SYN packet going to port 21 (ftp).

You can either search manually or you can apply a filter

Filter: `tcp.flags.syn == 1 and tcp.dstport == 21`

11. To see all the packets going to or coming from port 21, try the following filter :

Filter: `tcp.port == 21`

How did your web-server2 respond to the SYN packet sent to the opened port 21? What kind of packet did it send back?

How did nmap respond to the packet sent by the web-server2 VM?

(Answer : example of a packet capture below)

No.	Time	Source	Destination	Protocol	Length	Info
13	0.033154000	192.168.248.132	192.168.248.130	TCP	58	47179 > ftp [SYN] Seq=0 Win=1024 Len=0
18	0.033945000	192.168.248.130	192.168.248.132	TCP	60	ftp > 47179 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
19	0.033975000	192.168.248.132	192.168.248.130	TCP	54	47179 > ftp [RST] Seq=1 Win=0 Len=0

Packet 13 is the SYN packet sent to port 21. In Packet 18, the web-server2 responded with a SYN/ACK packet. In Packet 19, nmap responded with a RST packet.)

12. Change the filter to see all the packets going to or coming from port 23.

How did your web-server2 respond to the SYN packet sent to the closed port 23? What kind of packet did it send back?

(Answer : example of a packet capture below)

No.	Time	Source	Destination	Protocol	Length	Info
8	0.032948000	192.168.248.132	192.168.248.130	TCP	58	47179 > telnet [SYN] Seq=0 Win=1024 Len=0
17	0.033701000	192.168.248.130	192.168.248.132	TCP	60	telnet > 47179 [RST, ACK] Seq=1 Ack=0 Win=0 Len=0

In Packet 17, the web-server2 responded with a RST packet. This RST packet also has the ACK flag set.)

13. Change the filter to see all the packets going to or coming from port 445.

How did your web-server2 respond to the SYN packet sent to port 445 which is blocked by the firewall? Did it send any packet back?

(Ans : It did not send back any packet. Sometimes the firewall blocking the port may send back an ICMP destination unreachable packet)

Use the table below to record whether a SYN/ACK packet or a RST packet was returned or no packet was returned at all.

	Response from web-server2
Port 21 (service running and not blocked by firewall)	[RST]
Port 23 (service not running and port not blocked by firewall)	[RST, ACK]
Port 445 (service not running and port blocked by firewall)	[SYN]

Exercise 2. FIN Scan

Description :

You will now use Nmap to send FIN packets to a range of ports on a range of IP addresses.

Pick a range of IP addresses that include your web-server2.

For example, if your web-server2 IP is 192.168.10.100, you can pick the range 192.168.10.97 to 192.168.10.102

In Kali Linux

14. Start a Wireshark capture.
15. Use nmap to run a FIN scan against your range of IP addresses. This time, to reduce network traffic, only scan ports 21,23,25,53, 80 and 110. For example, if your target network range is 192.168.10.97 – 192.168.10.102, you will run :

```
sudo nmap -sF -p 21,23,25,53,80,110 192.168.10.97-102
```

16. Stop the Wireshark capture when nmap has finished running.
17. Using the Wireshark capture, find out how the different systems in your range of IP addresses responded to the FIN packet on the different ports. Use the table below to record whether each system replied with a SYN/ACK or a RST packet or did not reply at all. Sometimes the firewall blocking the ports may send back an ICMP destination unreachable packet.

	web-server2	
Port 21	ICMP Destination unreachable	
Port 23		
Port 25		
Port 53		
Port 80		
Port 110		

Exercise 3. ACK Scan


Description :

ACK scans can be used to detect the presence of stateful firewalls.

In Kali Linux

18. Start a Wireshark capture.
19. Run an ACK scan against your web-server2 VM. Currently the firewall on web-server2 is blocking some ports while allowing other ports.

```
sudo nmap -sA 192.168.10.100
```

 Change to the IP of your web-server2
20. Stop Wireshark when nmap has finished running.

21. An ACK scan can be used to find if there a firewall blocking the ports. In the screenshot below, the ten ports listed as “unfiltered” are not blocked by the firewall. Another 990 ports have also been scanned and are listed as “filtered” (blocked by firewall).

```

└─$ sudo nmap -sA 192.168.153.165
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-30 22:04 EDT
Nmap scan report for 192.168.153.165
Host is up (0.00091s latency).
Not shown: 990 filtered ports
PORT      STATE      SERVICE
21/tcp    unfiltered  ftp
22/tcp    unfiltered  ssh
23/tcp    unfiltered  telnet
25/tcp    unfiltered  smtp
53/tcp    unfiltered  domain
80/tcp    unfiltered  http
110/tcp   unfiltered  pop3
443/tcp   unfiltered  https
993/tcp   unfiltered  imaps
995/tcp   unfiltered  pop3s
MAC Address: 00:0C:29:41:54:D8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.60 seconds

```

← 990 ports found to be blocked by firewall (filtered)

← These ports are not blocked by firewall (unfiltered)

22. Using the Wireshark capture, find out how your web-server2 VM responded to the ACK packets. Use the table below to record whether a RST packet was returned or no packets were returned at all. If a RST packet is received, the firewall allowed the ACK packet to that port to go through.

Sometimes the firewall blocking the ports may send back an ICMP destination unreachable packet.

	Your web-server2 VM	Is the port blocked by firewall?
Port 21		
Port 22		
Port 23		
Port 25		
Port 445		
Port 3389		

In web-server2

23. Run the following command to turn the firewall off.
- ```
systemctl stop firewalld
```

### In Kali Linux

24. Start the Wireshark capture again. Repeat the ACK scan.
25. Stop Wireshark when nmap has finished running.
26. Using the Wireshark capture, find out how your web-server2 responded to the ACK packets. This time, with no firewall enabled, a RST packet should be returned to every ACK packet sent by nmap.

```

└─$ sudo nmap -sA 192.168.153.165
Starting Nmap 7.91 (https://nmap.org) at 2021-04-30 22:12 EDT
Nmap scan report for 192.168.153.165
Host is up (0.00023s latency).
All 1000 scanned ports on 192.168.153.165 are unfiltered
MAC Address: 00:0C:29:41:54:D8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds

```

← Nmap reports that all 1000 scanned ports are not blocked by firewall (unfiltered)

In web-server2

27. Run the following command to turn the firewall on again.  
`systemctl start firewalld`

**Exercise 4. UDP Scans****Description :**

UDP ports can also be opened on a system, and attackers can also scan for these opened UDP ports. Note that UDP port scanning can take much longer than TCP port scanning. This is because many opened UDP ports only responds to UDP packets containing specific data. When Nmap send generic UDP packets in the UDP scan, it may not receive replies from most of the UDP ports, and spends a while waiting for the time out.

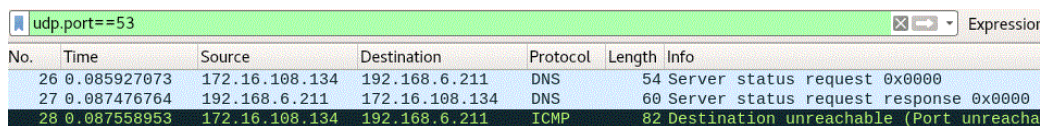
In Kali Linux

28. Start a Wireshark capture.
29. Run a UDP scan on ports 21,53, 80 and 161 against your web-server2.

```
sudo nmap -sU -p 21,53,80,161 192.168.10.100
```

← Change to the IP of your web-server2

30. Stop Wireshark when nmap has finished running.
31. Which UDP ports are opened? What services are normally running on these ports?



| No. | Time        | Source         | Destination    | Protocol | Length | Info                                   |
|-----|-------------|----------------|----------------|----------|--------|----------------------------------------|
| 26  | 0.085927073 | 172.16.108.134 | 192.168.6.211  | DNS      | 54     | Server status request 0x0000           |
| 27  | 0.087476764 | 192.168.6.211  | 172.16.108.134 | DNS      | 60     | Server status request response 0x0000  |
| 28  | 0.087558953 | 172.16.108.134 | 192.168.6.211  | ICMP     | 82     | Destination unreachable (Port unreacha |

(UDP Port 53 replied to the UDP scan)

32. In the screenshot below, UDP port 53 is reported to be opened. Nmap is not sure if UDP port 161 is opened or blocked by firewall, as it did not receive any reply from UDP port 161.

```
$ sudo nmap -sU -p21,53,80,161 192.168.153.165
Starting Nmap 7.91 (https://nmap.org) at 2021-04-30 22:47 EDT
Nmap scan report for 192.168.153.165
Host is up (0.00082s latency).

PORT STATE SERVICE
21/udp filtered ftp
53/udp open domain
80/udp filtered http
161/udp open|filtered snmp
```

## Exercise 5. Other nmap scans

33. In Kali Linux, try other nmap options. For example, the -sV option to determine the version number of the service.

```
sudo nmap -sV 192.168.10.100
```

← Change to the IP of your web-server2

34. Try the -sV option with UDP port scanning to increase the chances of finding out if the UDP ports are opened, plus the version number of the UDP service.

```
sudo nmap -sV -sU -p21,53,80,161 192.168.10.100
```

↑  
Change to the IP of your web-server2

35. If you do a UDP scan without specifying any ports, Nmap will scan 1000 most-frequently ports, which will take a long time

```
sudo nmap -sU 192.168.10.100
```

← Change to the IP of your web-server2

Press Control-C to stop the UDP scan.

36. You can add the -v or -vv option (verbose or more verbose) to see what Nmap is doing during the scan.

```
sudo nmap -sU -vv 192.168.10.100
```

← Change to the IP of your web-server2

Press Control-C to stop the UDP scan.

37. You can add the --reason option to see what kind of packet the scanned port returned (or did not return) for Nmap to make its deduction if the port is open, closed or filtered.

```
sudo nmap -sS --reason 192.168.10.100
```

← Change to the IP of your web-server2

The following screenshot shows an example of using the --reason option.

```

└─$ sudo nmap -sS --reason 192.168.153.165
Starting Nmap 7.91 (https://nmap.org) at 2021-04-30 22:49 EDT
Nmap scan report for 192.168.153.165
Host is up, received arp-response (0.00089s latency).
Not shown: 990 filtered ports
Reason: 978 no-responses and 12 host-prohibiteds
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack ttl 64
22/tcp open ssh syn-ack ttl 64
23/tcp closed telnet reset ttl 64
25/tcp open smtp syn-ack ttl 64
53/tcp open domain syn-ack ttl 64
80/tcp open http syn-ack ttl 64
110/tcp open pop3 syn-ack ttl 64
443/tcp open https syn-ack ttl 64
993/tcp open imap syn-ack ttl 64
995/tcp open pop3s syn-ack ttl 64

```

← 990 ports are listed as filtered because 978 ports did not respond, and another 12 ports replied with an ICMP Destination Unreachable "Host Prohibited" packet

← These ports are listed as open or closed because Nmap received these packets

38. Try the -O option to guess the operating system.

```
sudo nmap -O 192.168.10.100
```

← Change to the IP of your web-server2

You can also try the nmap -O option against your Win10 VM or your Host PC. Note : it is only a best-guess of the operating system.

39. View the file `/usr/share/nmap/nmap-services` to see the list of common ports, their service names and frequencies.
40. Try the `--top-ports` option to scan the top 10 most frequently ports according to the `nmap-services` file.
- ```
sudo nmap --top-ports 10 192.168.10.100
```
- ← Change to the IP of your web-server2

Exercise 6. Ping Sweeps and other methods to discover hosts in network

Description :

Fping can be used to ping a group of IP addresses. However, it may not always work as firewalls may block the ping packets.

Netdiscover and Nmap can be used to send ARP requests to discover alive hosts in the current network.

In Kali Linux

41. Use `fping` command to ping the range of addresses from 8.8.8.1 to 8.8.8.10. Which system is up?

```
fping -g 8.8.8.1 8.8.8.10
```

```
kali@kali:~$ fping -g 8.8.8.1 8.8.8.10
8.8.8.8 is alive
8.8.8.1 is unreachable
8.8.8.2 is unreachable
8.8.8.3 is unreachable
8.8.8.4 is unreachable
8.8.8.5 is unreachable
8.8.8.6 is unreachable
8.8.8.7 is unreachable
8.8.8.9 is unreachable
8.8.8.10 is unreachable
```

You may see results like this. 8.8.8.8 is the IP address of Google's public DNS Server

42. Use Netdiscover to send ARP broadcast requests to the subnet of your Kali. Which system is up?

```
sudo netdiscover -i eth0 -r 172.16.108.0/24
```

← Replace with the subnet of your Kali.
For example, if your Kali IP is 192.168.23.4 with netmask 255.255.255.0 then replace with 192.168.23.0/24

In this example, two IP addresses are discovered : 192.168.195.144 and 192.168.195.185 →

Currently scanning: Finished!		Screen View: Unique Hosts			
5 Captured ARP Req/Rep packets, from 5 hosts.		Total size: 300			
IP	At MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.195.1	00:50:56:c0:00:08	1	60	VMware, Inc.	
192.168.195.2	00:50:56:e8:f8:33	1	60	VMware, Inc.	
192.168.195.144	00:0c:29:ab:e9:96	1	60	VMware, Inc.	
192.168.195.185	00:0c:29:7c:f3:aa	1	60	VMware, Inc.	
192.168.195.254	00:50:56:e0:7a:70	1	60	VMware, Inc.	

192.168.195.1 is the Host PC

192.168.195.2 is the VMware Gateway and DNS Server

192.168.195.254 is the VMware DHCP Server

Note : Netdiscover may take a while to display the results.

43. Use Nmap to do host discovery by sending ARP broadcast requests to the local network. Which system is up?

```
sudo nmap -sn 172.16.108.0/24
```

← Replace with the subnet of your Kali.
For example, if your Kali IP is 192.168.23.4 with netmask 255.255.255.0 then replace with 192.168.23.0/24

Exercise 7. Crafting packets

You will use hping to craft ICMP packets with a spoofed source IP.

In Kali Linux

44. Start a Wireshark capture.
45. Type “icmp” in the Filter textbox to see only ICMP packets.
46. Use hping to send 2 ICMP packets to your Win10 VM or web-server2 VM.

```
sudo hping3 -c 2 --icmp 192.168.10.100
```

← Change to the IP of your Win10 or web-server2 VM

47. While Wireshark is running, look at the ICMP packets captured. Note that the ICMP echo request packets have the source IP of your Kali.

48. Use hping to send 2 ICMP packets to your Win10 VM or web-server2 VM with a spoofed IP

```
sudo hping3 -c 2 -a 192.168.20.20 --icmp 192.168.10.100
```

↑
This is the fake IP

↑
Change to the IP of your Win10 or web-server2 VM

49. Look at the ICMP packets captured. This time the ICMP echo request packets have the fake source IP.

(Important : Do not scan other people's systems or networks without their permission!)

End of Practical