**Practical 3**

**Objectives:** Use dig, host, nslookup and zone transfers for footprinting

Gather information from the Internet

**Exercise Gathering Information from the Internet**

1. 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.

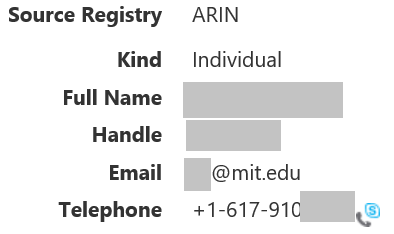
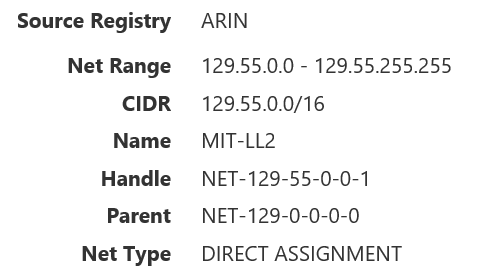
1. In Google, search for “site:.sp.edu.sg email” to search for the word “email” appearing in sp.edu.sg website.

Search for “site:.sp.edu.sg login” to search for the word “login” appearing in sp.edu.sg website, including login forms.

1. You can also use Google Advanced Search. Visit www.google.com/advanced\_search to see how detailed your search can be.
2. 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.

1. Try searching the Whois databases.
2. Go to https://search.arin.net/rdap.
3. In the Search Whois textbox, type “MIT” (or Massachusetts Institute of Technology)
4. 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.

1. Go to www.network-tools.com.
2. 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.
3. 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.
4. 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?

1. You can also make whois queries through a command line. In Kali, type the following command :

whois sp.edu.sg

1. The website ipinfo.io provides information on IP addresses. The free service is limited to 1000 requests per day.
2. Go to https://ipinfo.io. You will see your current IP address that is seen by the Internet.
3. 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.
4. 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

1. 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 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.

1. In Kali Linux, look at the man pages for dig and host.

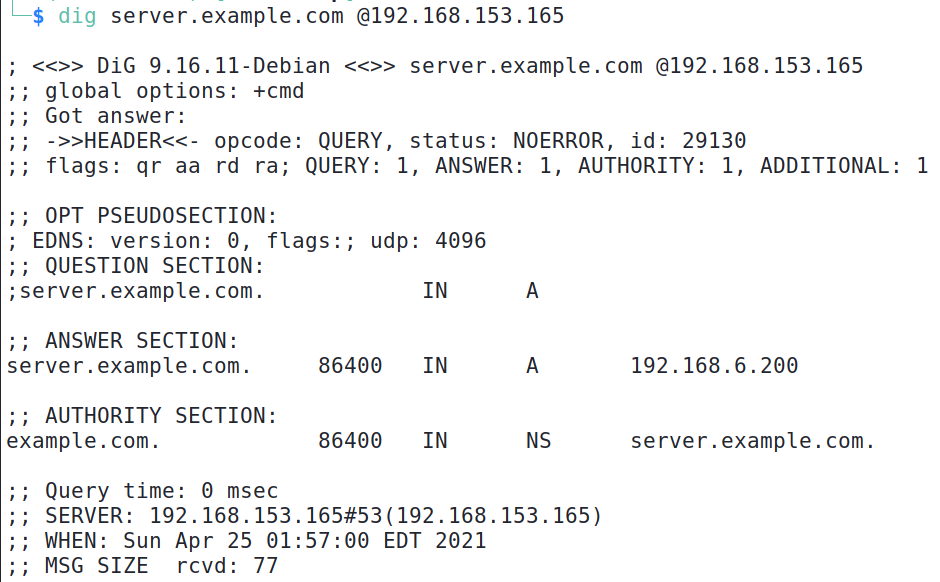
man dig

man host

1. 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.

Change to web-server2 IP

dig server.example.com @192.168.13.100



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

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

Change to your web-server2 IP

host server.example.com 192.168.13.100

1. 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

Set the DNS Server to your web-server2

**>server 192.168.13.100**

Default Server: [192.168.13.100]

Address: 192.168.13.100

**>server.example.com**

.... IP address displayed

**>quit**

1. 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:

Change to web-server2 IP

dig –x 192.168.6.201 @192.168.13.100

Or the host command:

Change to web-server2 IP

host 192.168.6.201 192.168.13.100

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

Set the DNS Server to your web-server2

**>server 192.168.13.100**

Default Server: [192.168.13.100]

Address: 192.168.13.100

**>set type=ptr**

**>192.168.6.201**

.... hostname displayed

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

Remember to set the DNS Server to web-server2 IP

dig @192.16.13.100 example.com axfr

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

Text

Description automatically generated

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 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.

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

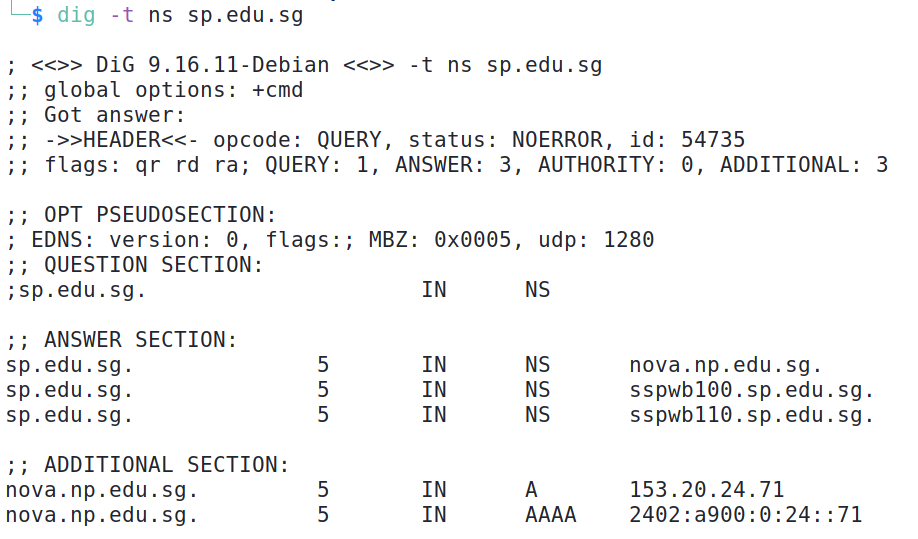
dig www.sp.edu.sg

1. 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)*

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.



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

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

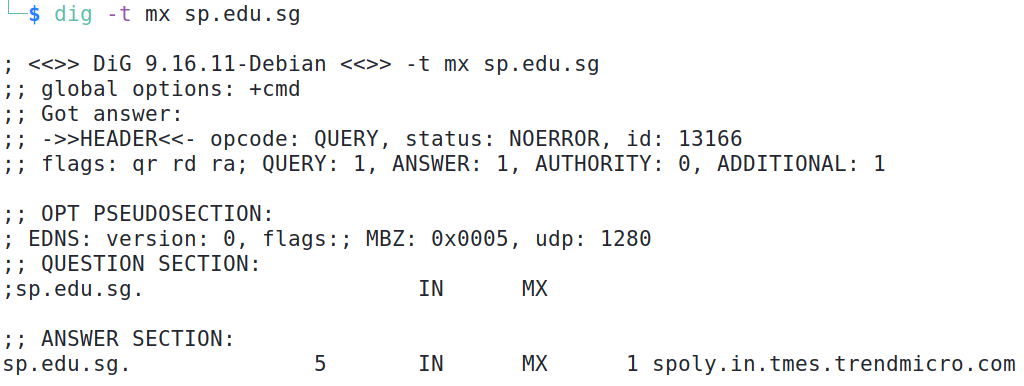
1. In the screenshot above, the IP addresses for the DNS Server sspwb100.sp.edu.sg and sppwb110.sp.edu.sg are not listed. Use the dig command to find their IP addresses.

dig sspwb100.sp.edu.sg

1. 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)*



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

1. 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 :

You can also use [www.network-tools.com](http://www.network-tools.com) and do a Network Lookup on the IP address

whois 164.78.252.50

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

1. 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)

1. 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.

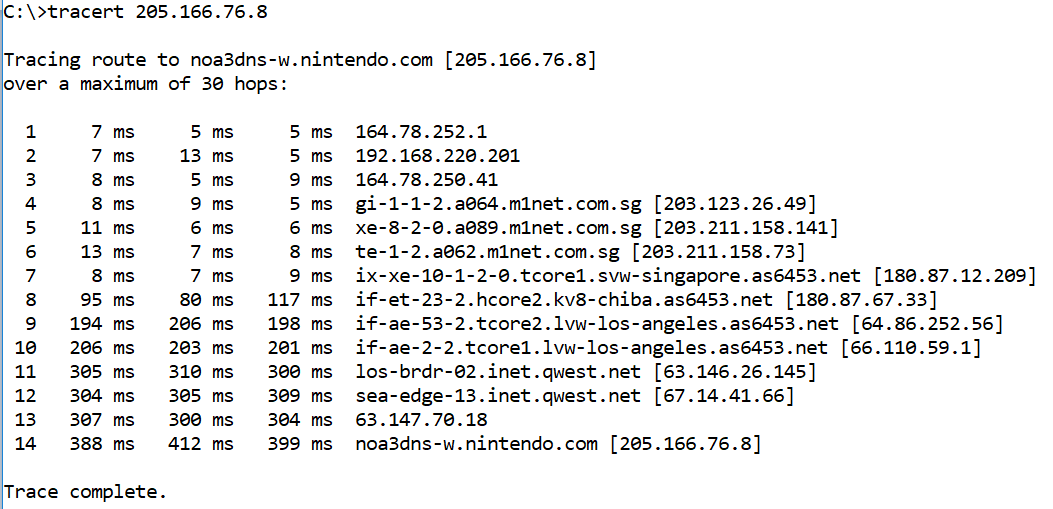
**Exercise Finding information on intermediate nodes**

1. 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.

traceroute 205.166.76.8 (you can use any reachable IP)

1. 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)

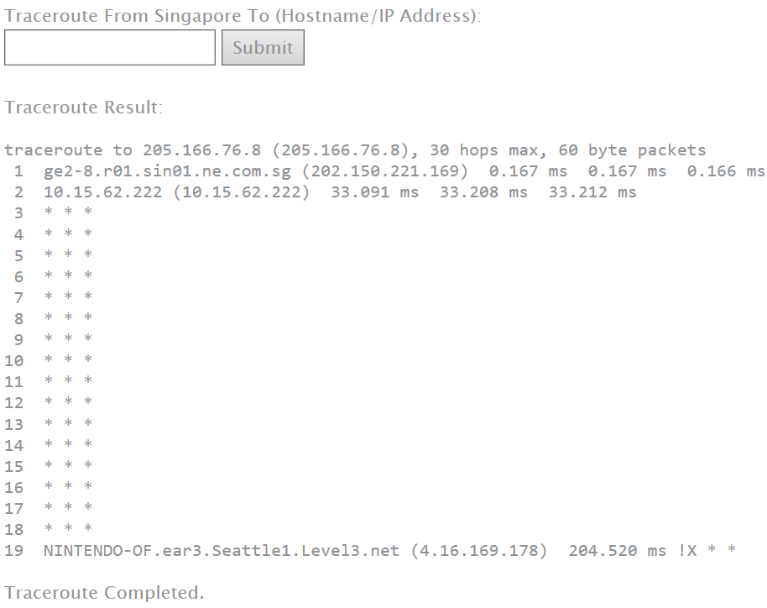


Sample output of a traceroute. Sometimes the intermediate routers do not return any info, so you see a series of \* instead.

1. Alternatively, you can use online traceroute websites.

Go to www.traceroute.org

1. Choose a server near you and start tracing to the target IP. Traceroute will return a list of IP addresses.
2. 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.
3. You can use various methods to learn more about the IP addresses listed (eg whois, dig, online search).



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)

Text

Description automatically generated

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

Text

Description automatically generated

(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.

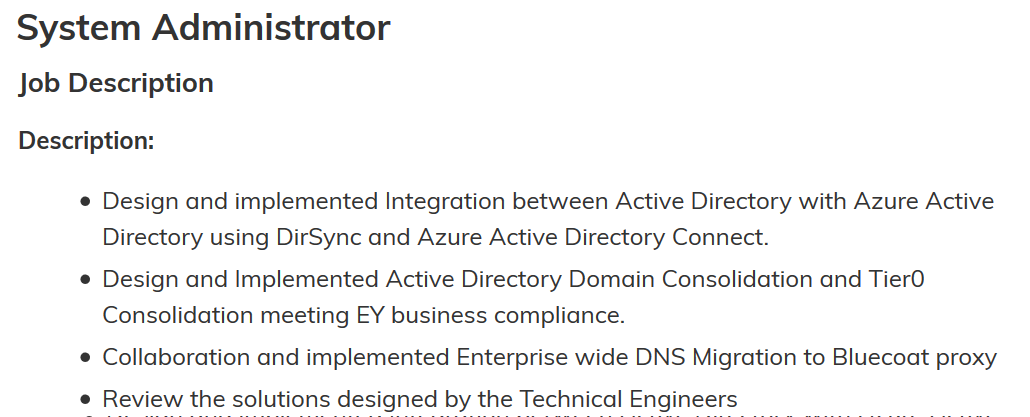
3) Any mail server in centurylink.com?

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



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

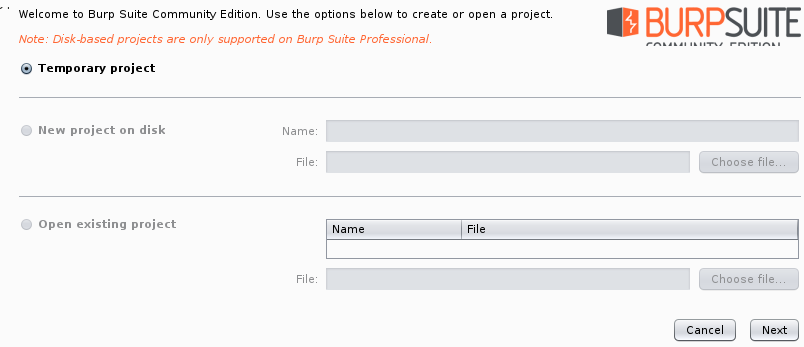
**Exercise Using Web Tools for fingerprinting**

**Description:**

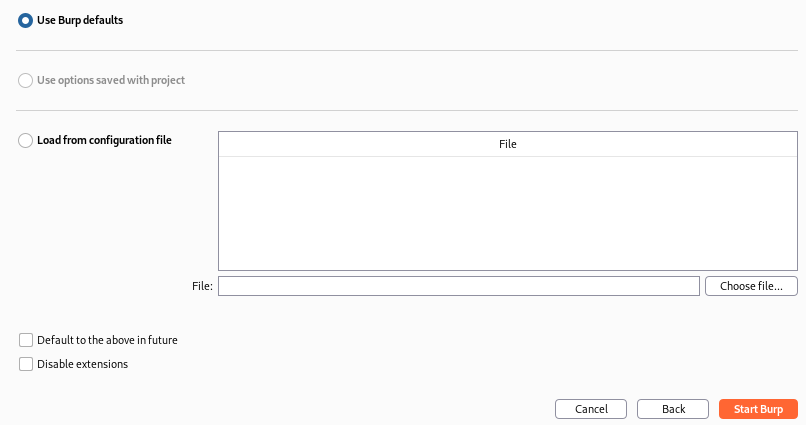
BurpSuite can be used for gathering information from a web site.

In Kali VM

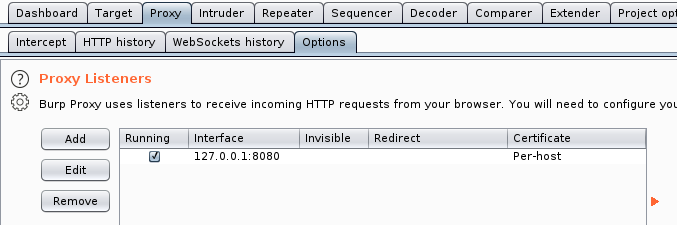
1. Click on the Kali icon in the top left corner and go to 03 Web Application Analysis -> burpsuite. Or in a terminal, type “burpsuite”. If there is a message about the Java JRE, click OK. You will need to Accept the Terms and Conditions for the BurpSuite Community Edition. If asked to update the software,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



1. Use Burp Defaults and click Start Burp.



1. 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)



By default, Burp is running on Port 8080

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



Click to toggle to “Intercept is off”

1. 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.

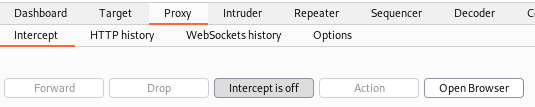
Chromium Web Browser

Website

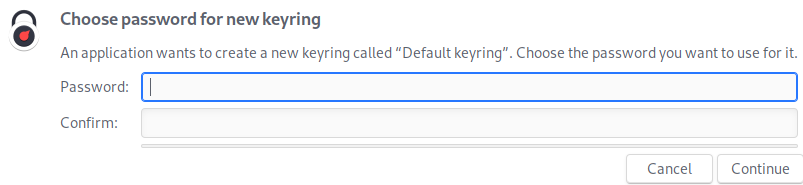
Burpsuite

Web requests and responses pass through Burp. Burp is able to capture and passively scan this data

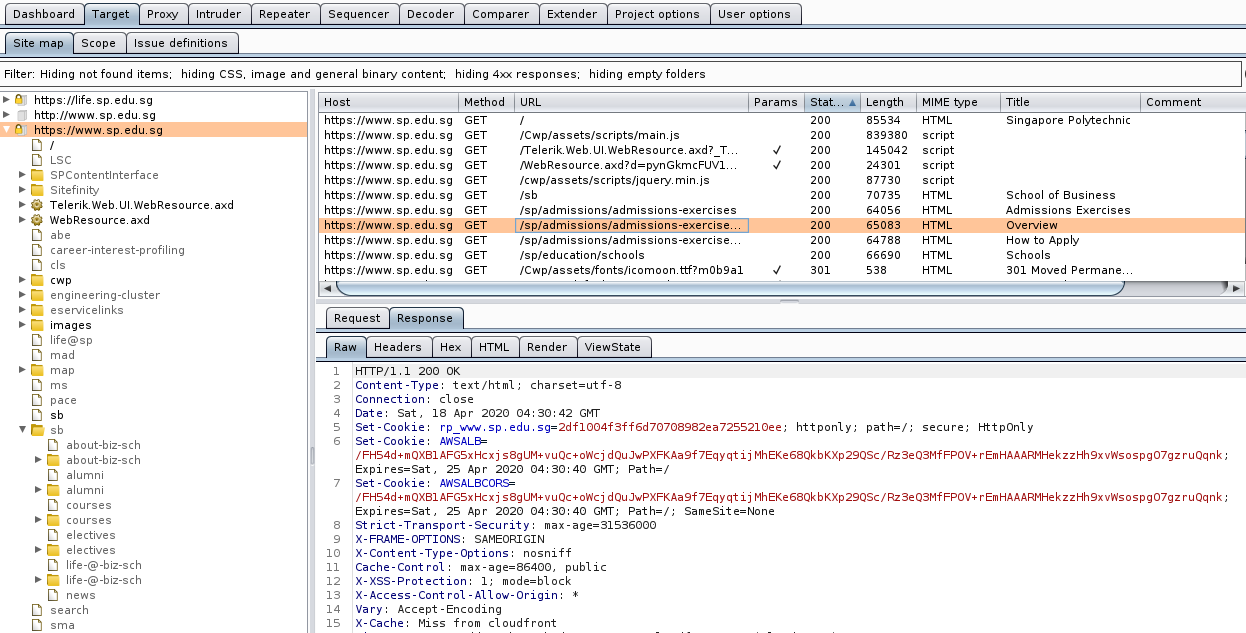
1. In Burp, click on Open Browser.



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



1. Browse to a web site (eg [www.sp.edu.sg](http://www.sp.edu.sg)).
2. 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).
3. Browse a few pages in the website.
4. 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)



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

1. 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.

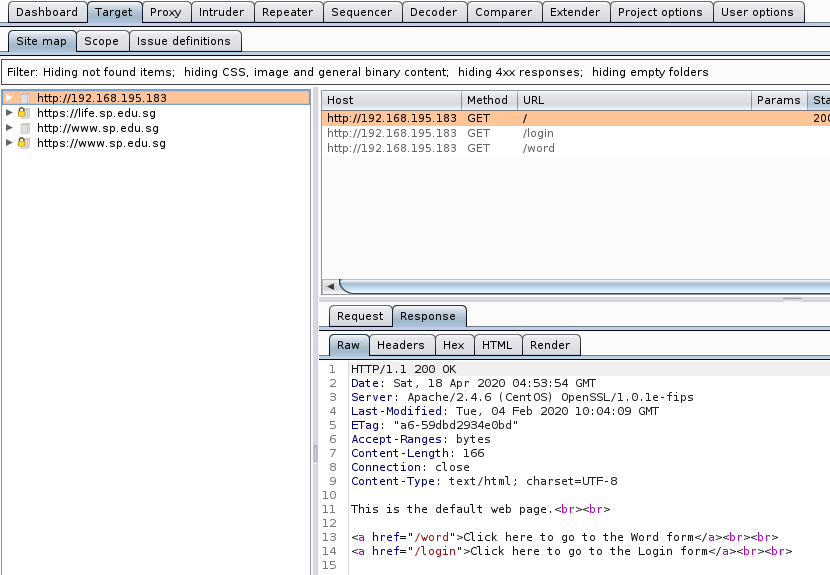
**Exercise Viewing HTTP headers**

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.

1. Power on the web-server2 VM.

In Kali

1. Run Burp. In the Proxy tab, check that “Intercept is off”.
2. In Burp, under the Proxy tab, click Open Browser to start the Chromium Web Browser.
3. Browse to the IP address of your web-server2.
4. 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.

1. Close the Chromium Web Browser and exit Burp.

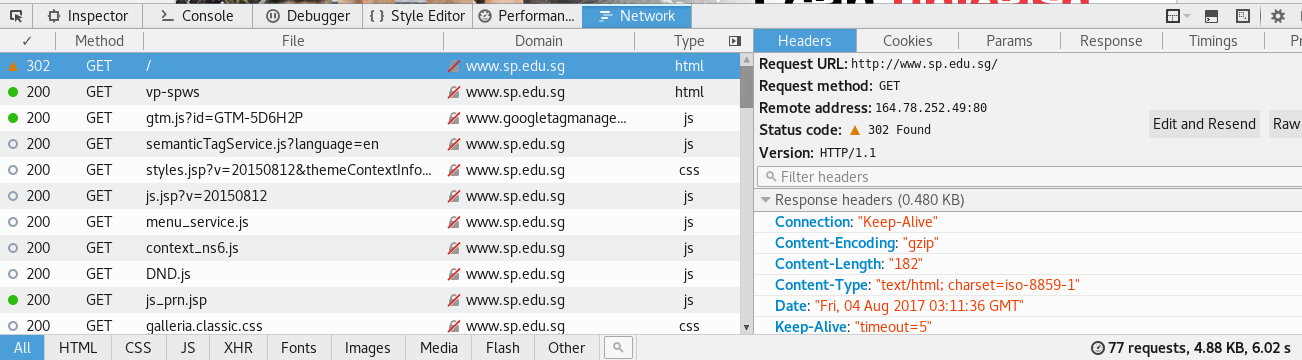
Using the Web Browser’s built-in Developer Tools to view HTTP headers

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)

1. In any Web Browser, press F12 to bring up the Developer Tools window.
2. Click on Network tab.
3. Browse to a website. You will see a list of network packets displayed in the Developer Tools window.
4. 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.



1. Press F12 again to close the Developer Tools.

**Exercise 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/6L0N5AtlyURhV4=;

h=To:Message-ID:Date:Content-Type:Subject:From;

b=WHtl3UbJz0zfF4tOjGe9ZRcqjYftZHYu4E55DRfDdeqHMlEUCMhHhBsr8nGAYn2O1

osBPZmd0Z3B69HtXUtGwLJa30gFVcIcf1uNUXype6uvgYUPML5d387YCgn26lLoeXT

2XnCWVulotBOwSasyFaALwaqOPg2h9aSjaVNLPqE=

X-MSFBL: osnZjuM6KhUUNZX/3sop661yRvbwSeSFnSxb2c9j/6k=|eyJzdWJhY2NvdW50X2l

kIjoiMCIsIm1lc3NhZ2VfaWQiOiIwMDI1YTYyN2I2NWNjODI2OTg5YiIsInRlbmF

udF9pZCI6ImNvdXJzZXJhIiwiY3VzdG9tZXJfaWQiOiIxIiwiciI6InllaWxlZW5

AeWFob28uY29tIn0=

To: <customer@yahoo.com>

Message-ID: <89.B9.09928.6A726BC5@ak.mta2vrest.cc.prd.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

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

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

**Amazon Technologies Inc. (AT-88-Z)**

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

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

Bharat Sanchar Nigam Limited

1. 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 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.

1. 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.
2. Click on the link “More Info” to see more information that your web browser can provide to the web server.

*End of Practical*