UNIVERSITI KEBANGSAAN MALAYSIA

National University of Malaysia

TX6224: Individual Lab Assignment

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT

UNIVERSITI KEBANGSAAN MALAYSIA

Pusat Pengajian Sains Komputer

School of Computer Science

TX6244: **Ethical Hacking and Penetration Testing**	**SEMESTER 2**	**SESI 2015/2016**

Lecturer/Instructor:

Mr Zamri Bin Murah

NAMA	**NO DAFTAR**
1. Warhamni Binti Jani @ Mokhtar	GP04294

CONTENTS

INDIVIDUAL LAB ASSIGNMENT

1. FOOT PRINTING AND RECONNAISSANCE

Question:
Learning objective:
1. Use external system to gather info about the target system.
2. Use and familiar with various tools.
3. Able to access the data and summarize the finding.
4. Any interesting finding? (e.g 20% sites use Linux 2.3, and old version. etc.)

You have been assigned to do *foot printing* and *reconnaissance* for **ukm.my** domain. You are required to find out all subdomains, the services available, and the types of servers, the operating system and the topology of the domain. Use 3 relevant tools for these tasks.
You can use other domain that you have access to like *gmi.edu.my*, sites from your previous university. Please do not use any military or security sites.
Please indicate the steps you have taken, the tools used, and your conclusions. Please use table to summarize your finding. Please include screen shots and relevant outputs.

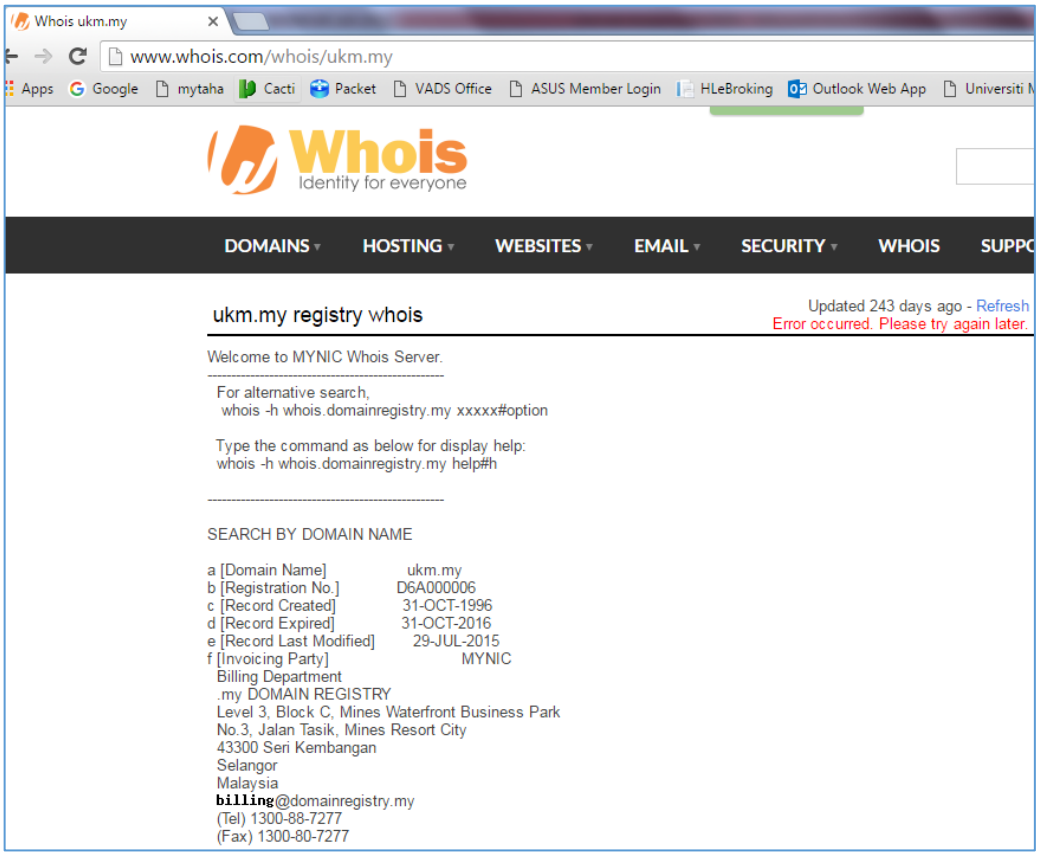
The target domain chosen is www.ukm.my. The relevant tools for these tasks are:

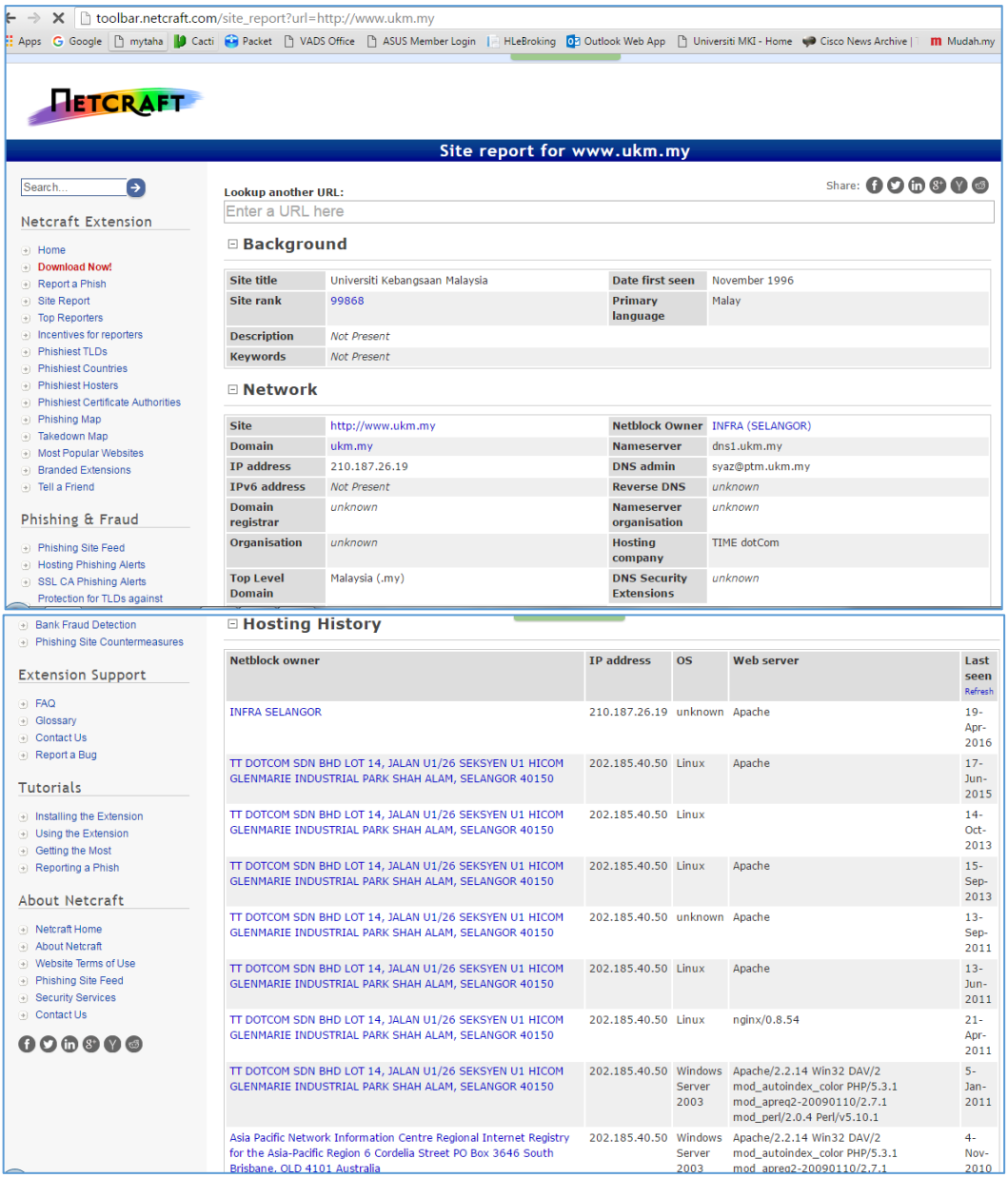
a) Whois and Netcraft

b) Nmap

c) Zenmap

Using whois and Netcraft




toolbar.netcraft.com/site_report?url=http://www.ukm.my
Apps Google mytaha Cacti Packet VADS Office ASUS Member Login HLeBroking Outlook Web App Universiti MKI - Home Cisco News Archive Mudah.my
NETCRAFT
Site report for www.ukm.my
Search...
Netcraft Extension
Home
Download Now!
Report a Phish
Site Report
Top Reporters
Incentives for reporters
Phishiest TLDs
Phishiest Countries
Phishiest Hosters
Phishiest Certificate Authorities
Phishing Map
Takedown Map
Most Popular Websites
Branded Extensions
Tell a Friend
Phishing & Fraud
Phishing Site Feed
Hosting Phishing Alerts
SSL CA Phishing Alerts
Protection for TLDs against
Bank Fraud Detection
Phishing Site Countermeasures
Extension Support
FAQ
Glossary
Contact Us
Report a Bug
Tutorials
Installing the Extension
Using the Extension
Getting the Most
Reporting a Phish
About Netcraft
Netcraft Home
About Netcraft
Website Terms of Use
Phishing Site Feed
Security Services
Contact Us
Lookup another URL:
Enter a URL here
Share:
Background
Site title Universiti Kebangsaan Malaysia
Date first seen November 1996
Site rank 99868
Primary language Malay
Description Not Present
Keywords Not Present
Network
Site http://www.ukm.my
Netblock Owner INFRA (SELANGOR)
Domain ukm.my
Nameserver dns1.ukm.my
IP address 210.187.26.19
DNS admin syaz@ptm.ukm.my
IPv6 address Not Present
Reverse DNS unknown
Domain registrar unknown
Nameserver organisation unknown
Organisation unknown
Hosting company TIME dotCom
Top Level Domain Malaysia (.my)
DNS Security Extensions unknown
Hosting History
Netblock owner
IP address
OS
Web server
Last seen
Refresh
INFRA SELANGOR 210.187.26.19 unknown Apache 19-Apr-2016
TT DOTCOM SDN BHD LOT 14, JALAN U1/26 SEKSYEN U1 HICOM GLENMARIE INDUSTRIAL PARK SHAH ALAM, SELANGOR 40150 202.185.40.50 Linux Apache 17-Jun-2015
TT DOTCOM SDN BHD LOT 14, JALAN U1/26 SEKSYEN U1 HICOM GLENMARIE INDUSTRIAL PARK SHAH ALAM, SELANGOR 40150 202.185.40.50 Linux 14-Oct-2013
TT DOTCOM SDN BHD LOT 14, JALAN U1/26 SEKSYEN U1 HICOM GLENMARIE INDUSTRIAL PARK SHAH ALAM, SELANGOR 40150 202.185.40.50 Linux Apache 15-Sep-2013
TT DOTCOM SDN BHD LOT 14, JALAN U1/26 SEKSYEN U1 HICOM GLENMARIE INDUSTRIAL PARK SHAH ALAM, SELANGOR 40150 202.185.40.50 unknown Apache 13-Sep-2011
TT DOTCOM SDN BHD LOT 14, JALAN U1/26 SEKSYEN U1 HICOM GLENMARIE INDUSTRIAL PARK SHAH ALAM, SELANGOR 40150 202.185.40.50 Linux Apache 13-Jun-2011
TT DOTCOM SDN BHD LOT 14, JALAN U1/26 SEKSYEN U1 HICOM GLENMARIE INDUSTRIAL PARK SHAH ALAM, SELANGOR 40150 202.185.40.50 Linux nginx/0.8.54 21-Apr-2011
TT DOTCOM SDN BHD LOT 14, JALAN U1/26 SEKSYEN U1 HICOM GLENMARIE INDUSTRIAL PARK SHAH ALAM, SELANGOR 40150 202.185.40.50 Windows Server 2003 Apache/2.2.14 Win32 DAV/2 mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1 5-Jan-2011
Asia Pacific Network Information Centre Regional Internet Registry for the Asia-Pacific Region 6 Cordelia Street PO Box 3646 South Brisbane, QLD 4101 Australia 202.185.40.50 Windows Server 2003 Apache/2.2.14 Win32 DAV/2 mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 4-Nov-2010

Security

Netcraft Risk Rating [FAQ]	0/10		
On Spamhaus Block List	No	**On Exploits Block List**	No
On Policy Block List	No	**On Domain Block List**	No

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.

This host does not have a DMARC record.

Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

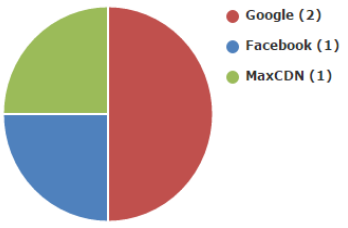
4 known trackers were identified.

Web Trackers

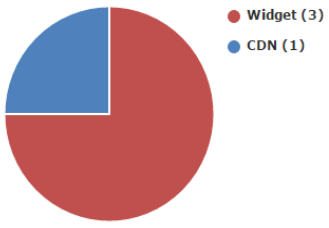
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

4 known trackers were identified.

Companies



Categories



Company ▲	Primary Category	Tracker	Popular Sites with this Tracker
Facebook	**Widget**	Facebook	www.nfl.com, www.gazeta.pl, www.ynet.co.il
Google	**Widget**	Googleplus	www.cnn.com, www.repubblica.it, www.wp.pl
		Googlewidget	www.idealo.de, www.fanfiction.net, www.welt.de
MaxCDN	**CDN**	Bootstrapcdn	www.gocomics.com, www.geek.com, www.gamefaqs.com

Site Technology

Fetched on 5th April 2016

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
PHP	PHP is supported and/or running	www.pcwelt.de , www.xnxx.com , www.mediafire.com
XML	*No description*	vk.com , platform.twitter.com
SSL	A cryptographic protocol providing communication security over the Internet	login.salesforce.com
PHP Enabled	Server supports PHP	www.lepoint.fr , www.bom.gov.au , www.northamericanweather.net

Client-Side

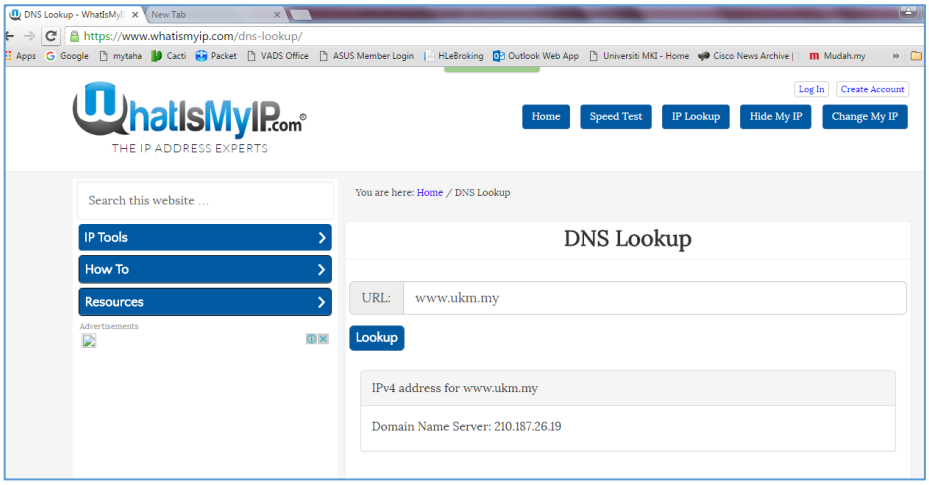
Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Open source programming language commonly implemented as part of a web browser	accounts.google.com , login.live.com , facebook.com
Client Pull	*No description*	www.repubblica.it , www.ilfattoquotidiano.it , www.ampparit.com

Client-Side Scripting Frameworks

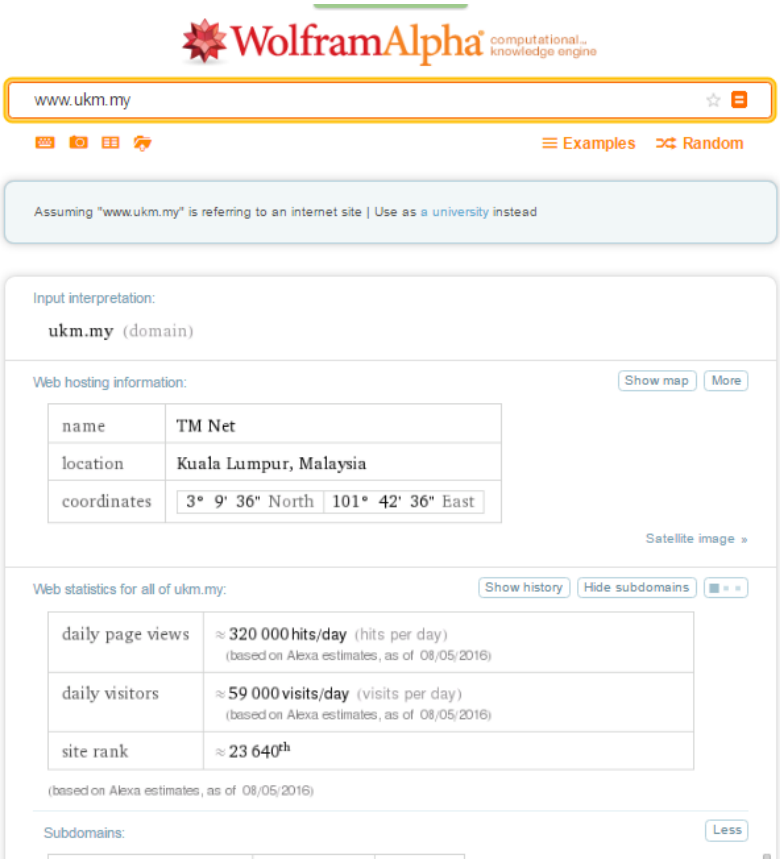
Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	www.linkedin.com , www.spiegel.de , www.xvideos.com
Google Hosted Libraries	Google API to retrieve JavaScript libraries	www.orange.fr , www.google.co.in ,



i. All subdomains ukm.my

Result from http://www.wolframalpha.com/input/?i=www.ukm.my



Subdomains: Less

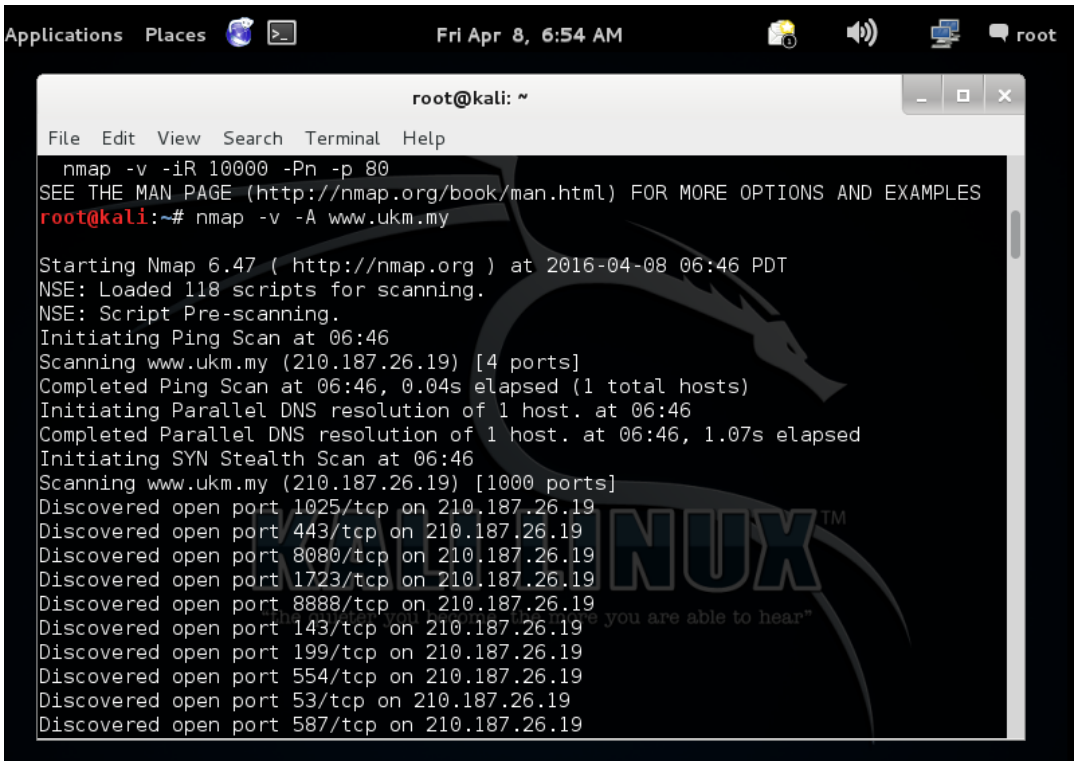
subdomain	daily visitors	fraction
ukm.my	28 000	34.1%
ifolio.ukm.my	20 000	24.36%
smp.ukm.my	6200	7.55%
portalewarga.ukm.my	4100	4.99%
smk.ukm.my	3900	4.75%
journalarticle.ukm.my	2700	3.29%
guest.ukm.my	2400	2.92%
ewarga.ukm.my	2100	2.56%
gemilang.ukm.my	2000	2.44%
ezplib.ukm.my	1600	1.95%
ejournal.ukm.my	1500	1.83%
spdukm.ukm.my	1100	1.34%
ftsm.ukm.my	1000	1.22%
ehebahan.ukm.my	800	0.97%
smpphp.ukm.my	700	0.85%
ekew.ukm.my	700	0.85%
hukm.ukm.my	600	0.73%
ppukm.ukm.my	600	0.73%
ejournals.ukm.my	600	0.73%
ewarga2.ukm.my	600	0.73%
pkukmweb.ukm.my	500	0.61%
appsmu.ukm.my	400	0.49%

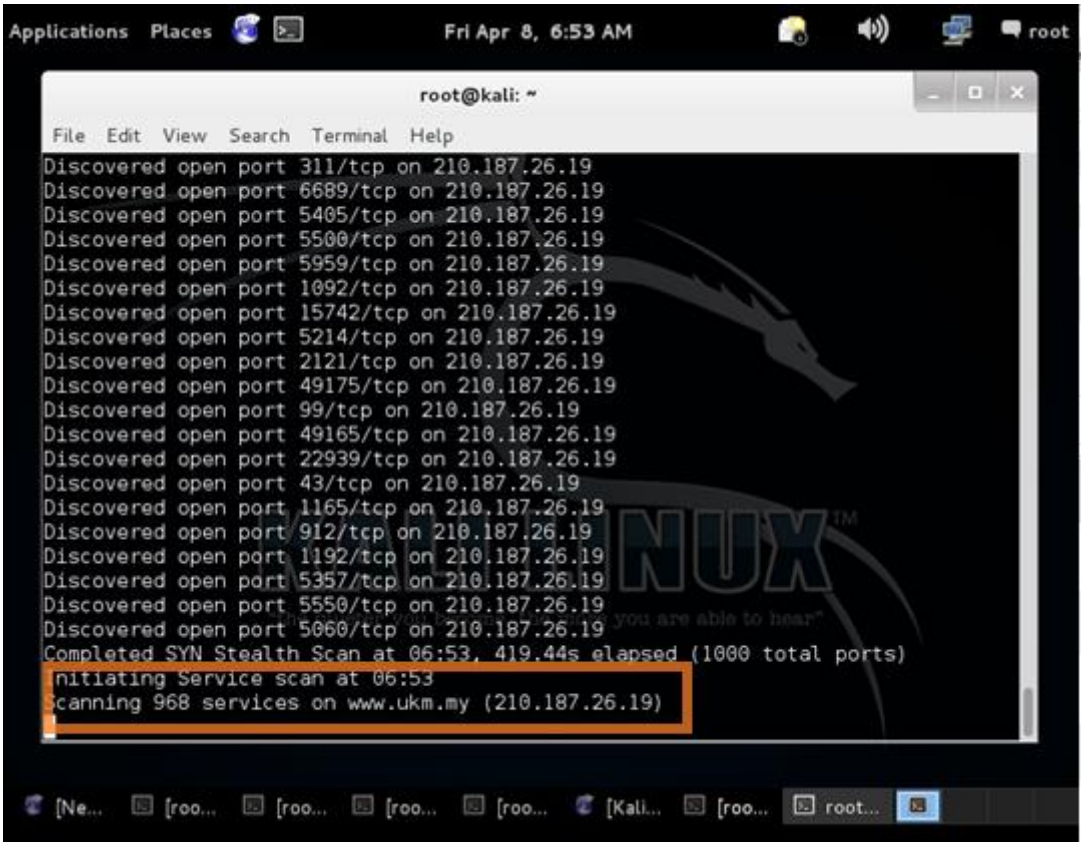
Sources Download page POWERED BY THE WOLFRAM LANGUAGE

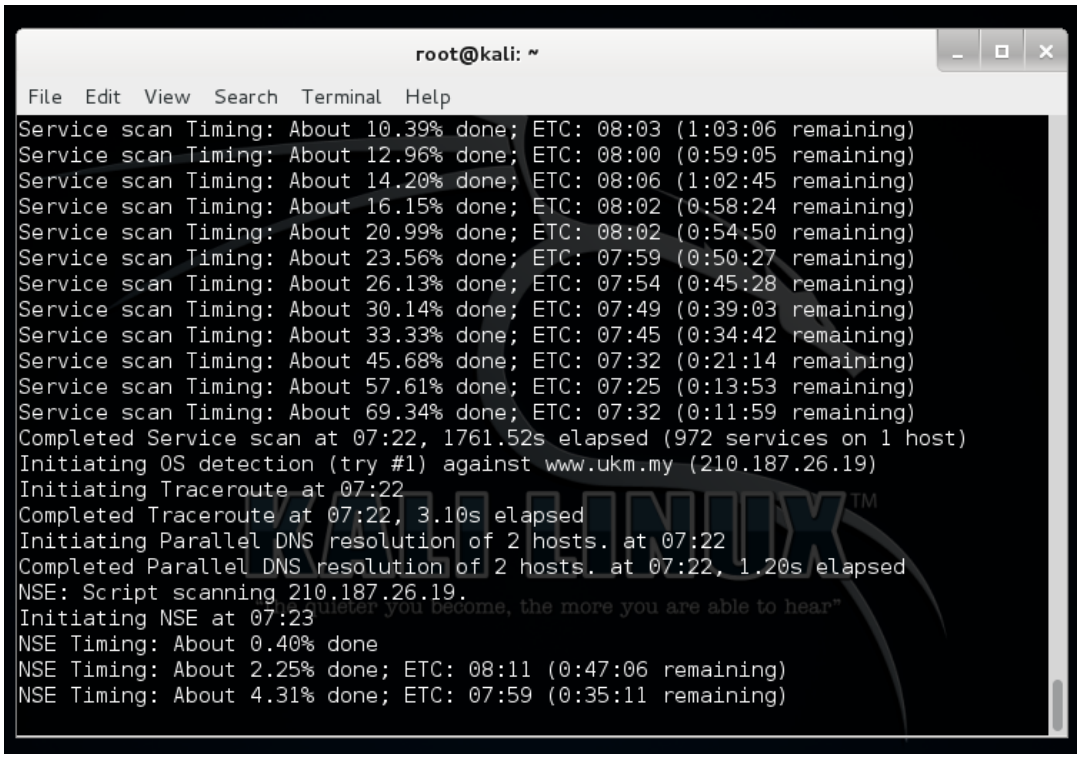
Based on the figure above, all the subdomains are listed.

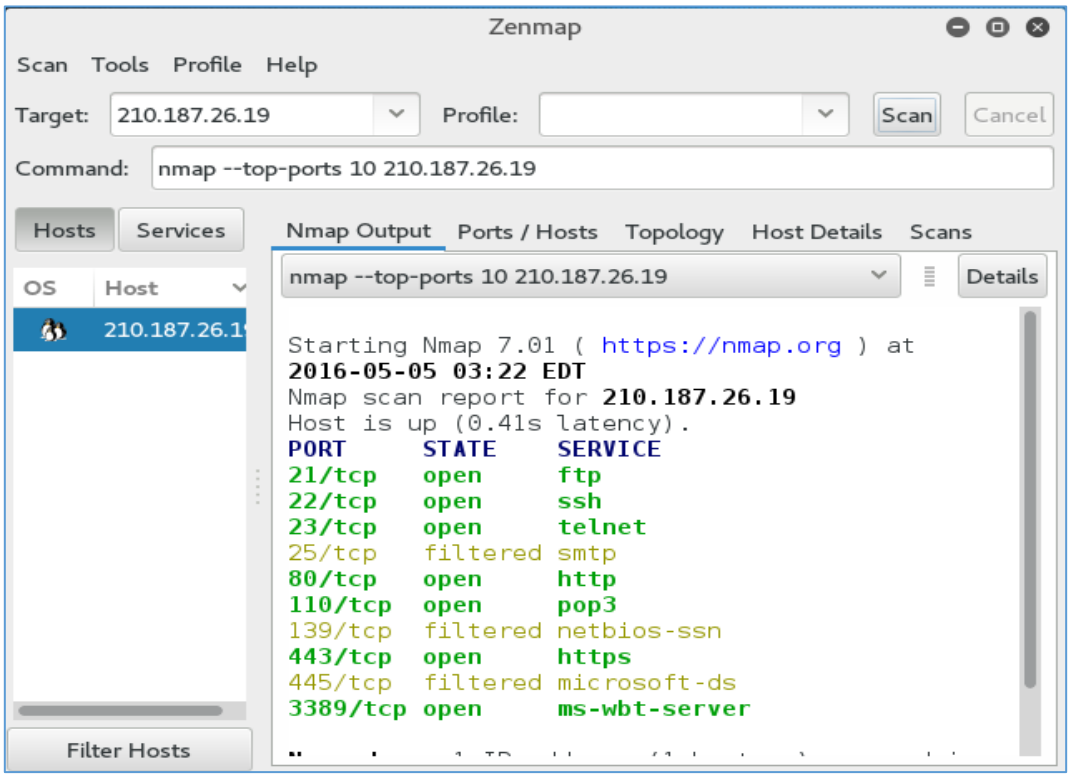
ii. Services available

There are 968 services available

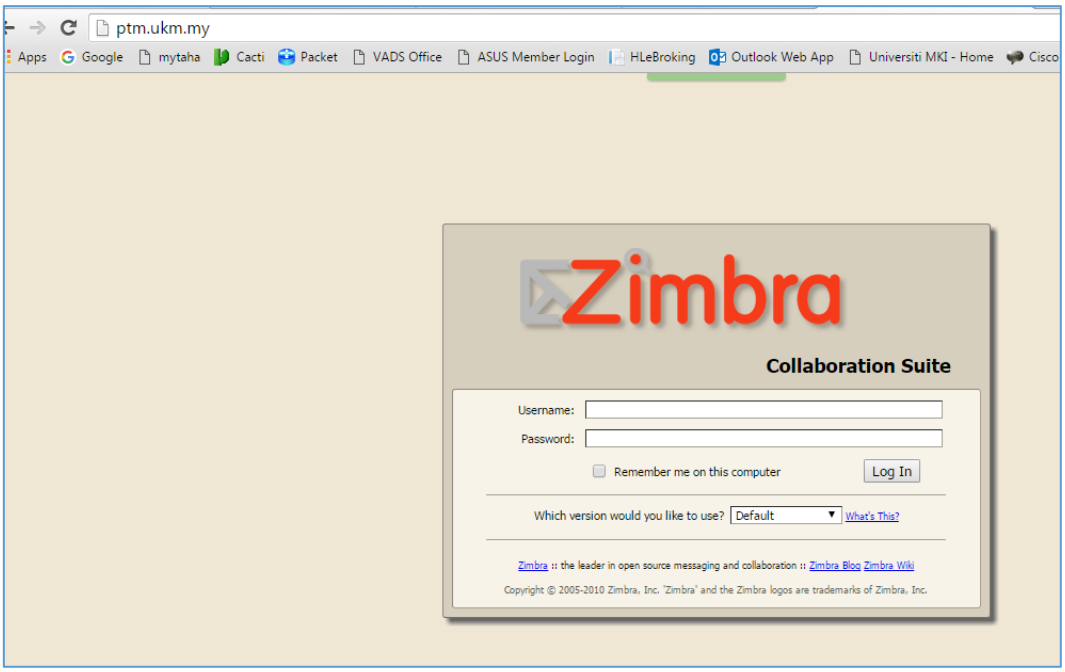






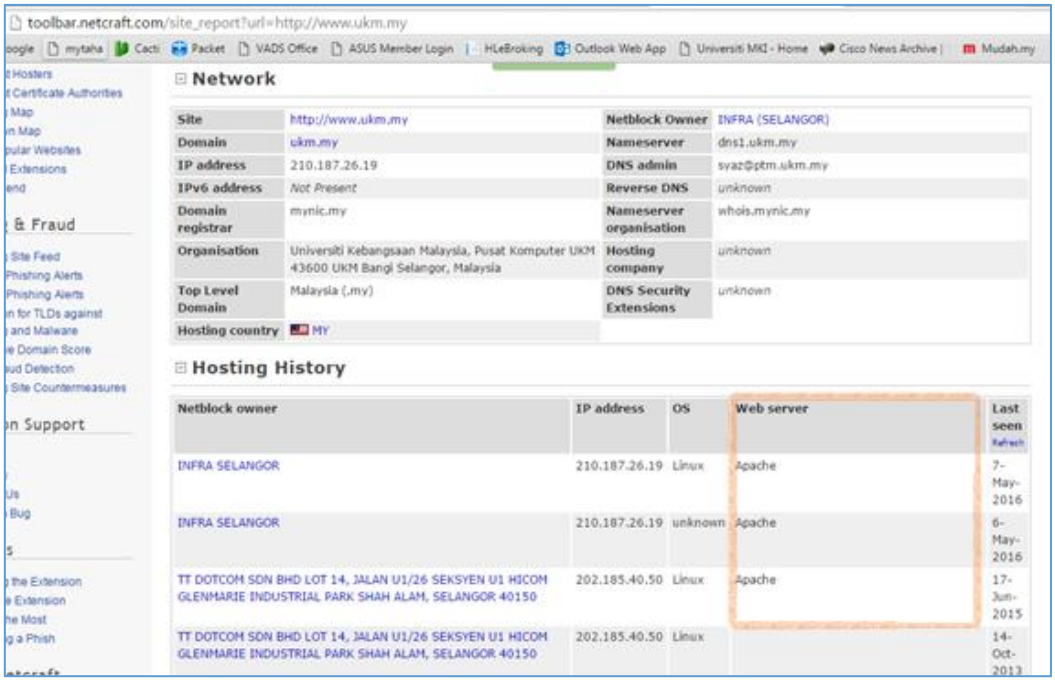


Top service from Zenmap



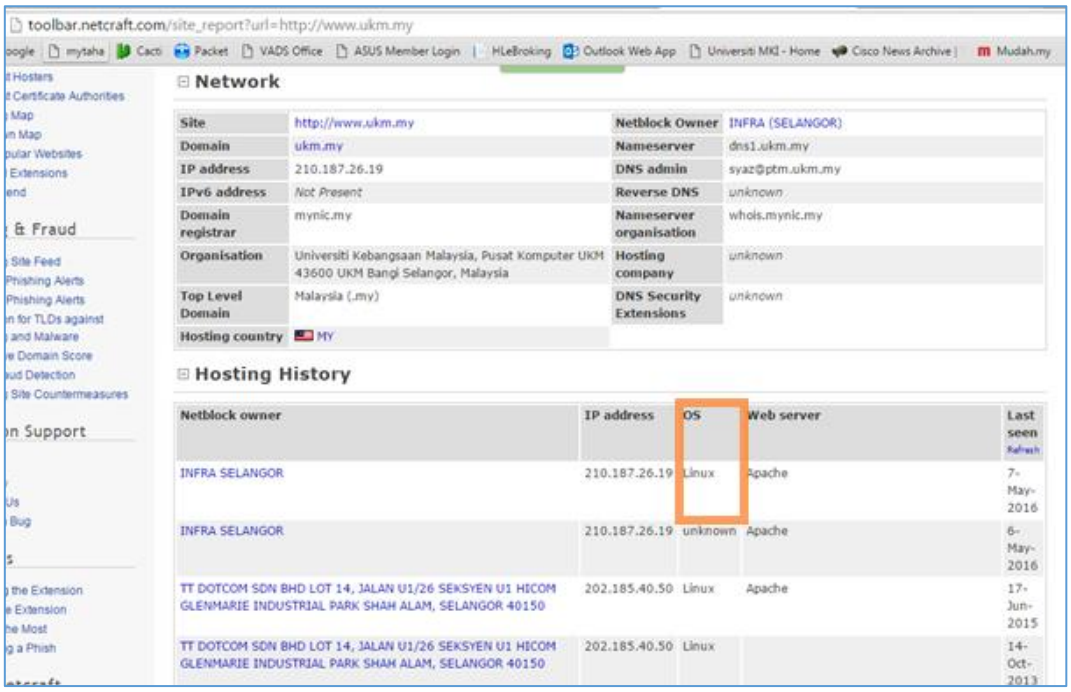
Email using Zimbra open source.

iii. Type of servers

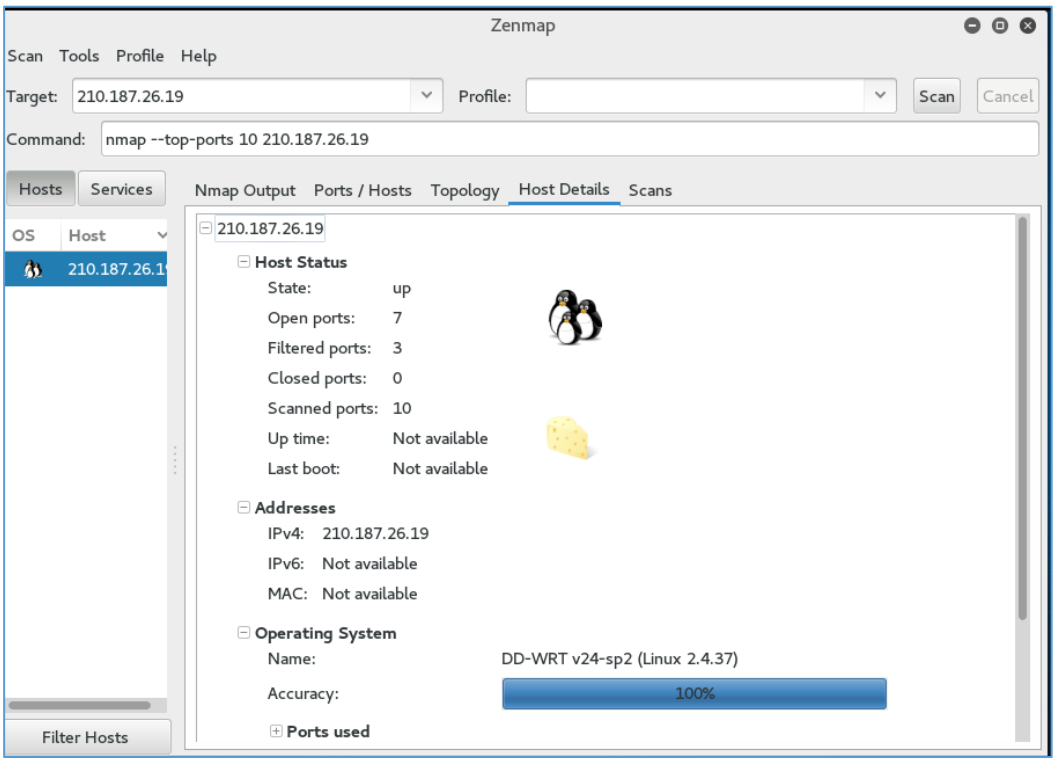


Using Netcraft, we can see that the type of server is Web Server.

iv. Operating systems

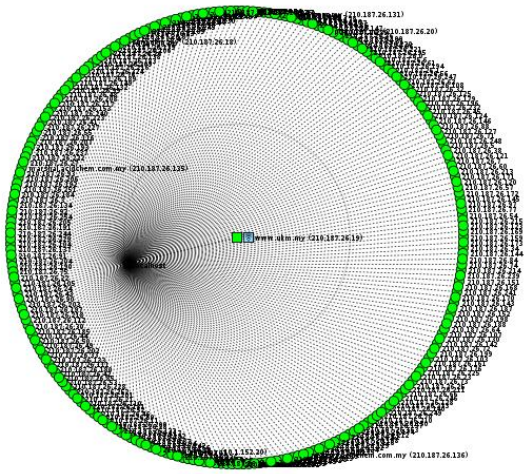


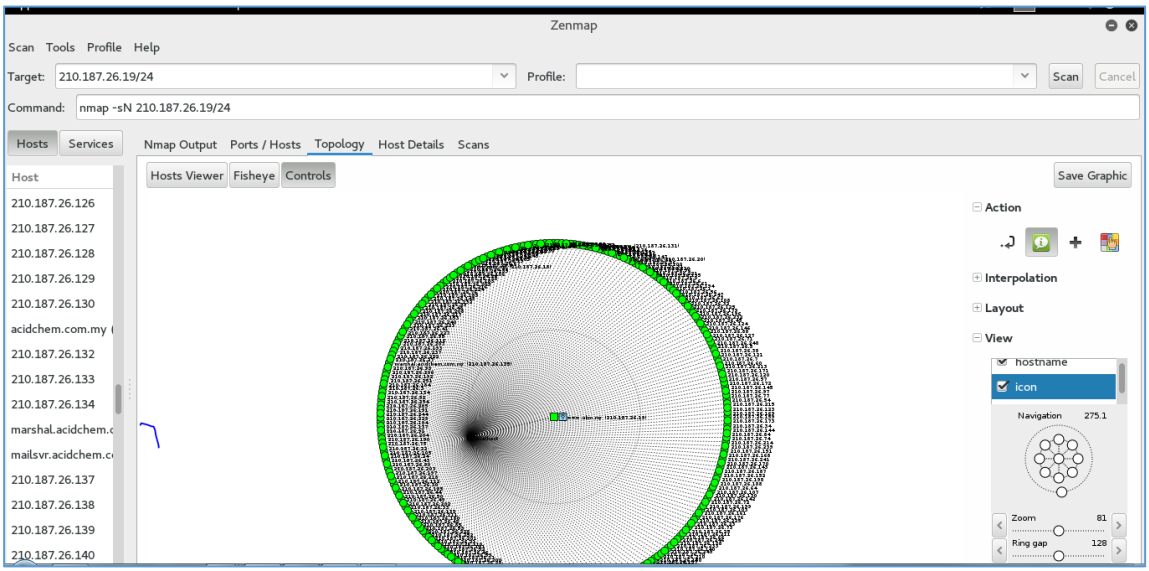
Using Netcraft, we can see that the operating system is Linux.



From Zenmap, the result is also same with 100% accuracy

v. Topology of the domain





The topology was derived from Zenmap using the following command: nmap -sN 210.187.26.19/24

Summarize finding are details in the above table.

1. Step taken	➢ We find information for www.ukm.my using whois and netcraft ➢ To get the list of **subdomains**, by using WolframAlpha http://www.wolframalpha.com/input/?i=www.ukm.my it shows **22** subdomains for ukm.my. ➢ Using nmap, there are 968 **services** available. ➢ Next, using Netcraft (www.netcraft.com), we get more detail information for like the **type of servers** is Web Servers and the **operating system** is Linux. Also from nmap we get 100% accuracy on the OS is Linux. ➢ For **topology**, the command is nmap -sN 210.187.26.19/24. By using this command, we find out the topology is ring topology.
2. Tools used	Nmap, Netcraft, Zenmap, Whois, WolframAlpha
3. Conclusion	Using various tools described above, www.ukm.my is 210.187.26.19 in IP translate. There are 22 subdomains found. The services found is 968.The type of server is Web Server and the operating system found to be Linux by 100% accuracy using nmap. The emel system used is zimbra open source.

2. WIRELESS PENETRATION TESTING

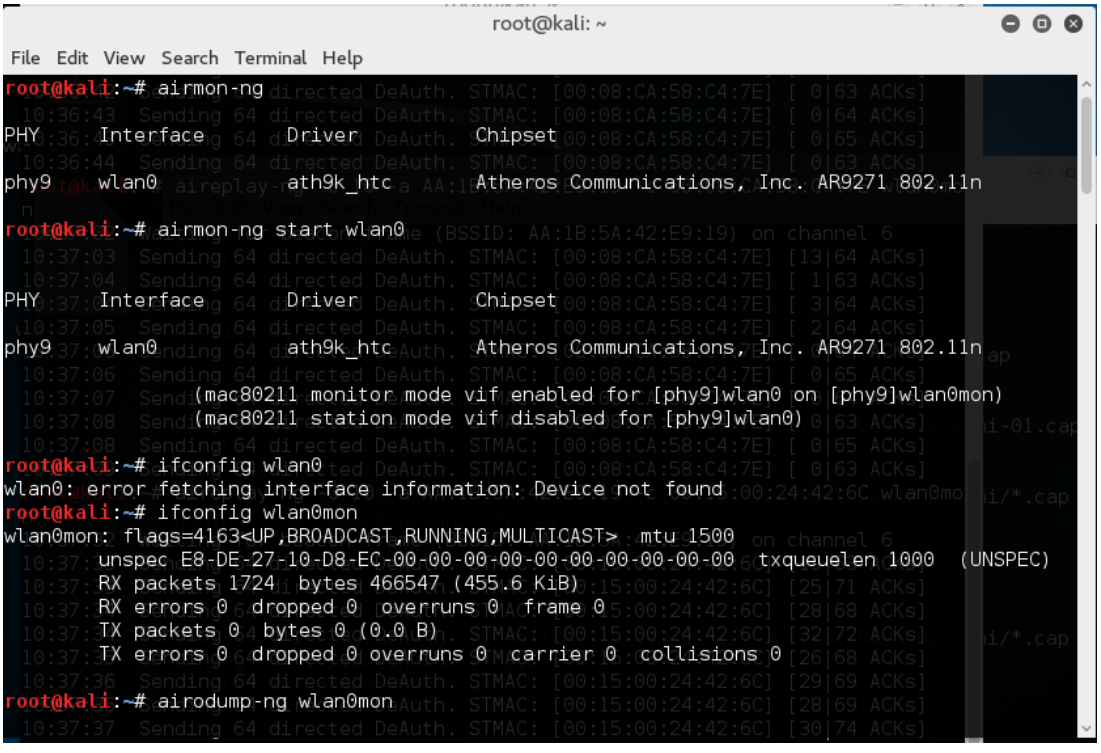
Question:
Learning objective:

1. Setup system to capture packet. (Some computer need external USB wifi adapter to capture packets. Setup requirement.)
2. What can you learn from the packets?
3. How do you analysis the packets?

Use *wireshark* or *aircrack-ng*, *kismet* or other packet capture tools to capture wireless packets. You can do this at the faculty or at home.
At the faculty, capture wireless traffic or UKM-warga or UKM-pelawat. See if you can obtain password or other sensitive information, various sites access and other interesting info.
At home, capture local wireless traffic such as unifi or maxis. Again, see what you can analysis about the traffic. Is the password easily available? What do people browse in the Internet? Can you do 'man-in-the-middle-attack'?
For the network, find all wireless networks available. Find the BSSID. Can you penetrate the wireless network? Please include relevant steps and out.
Please include relevant output (e.g from airmon-ng, kismet) as supplementary files.
In short, pick any wireless network, and try to penetrate the network. What are the steps?

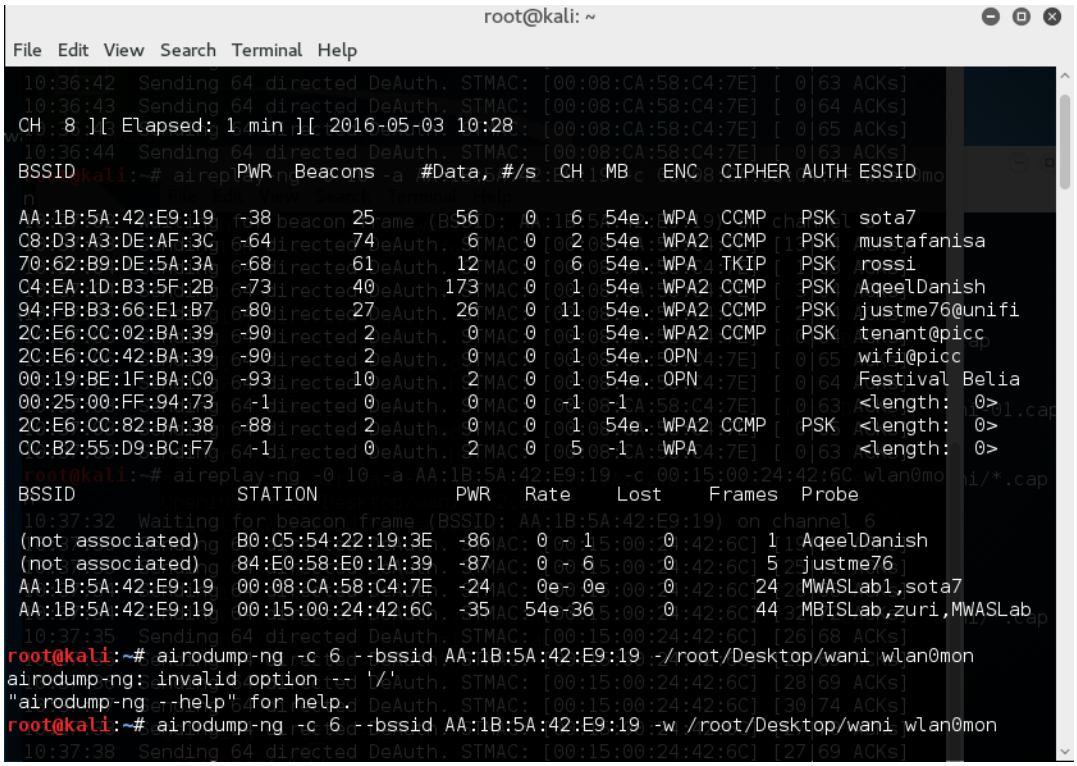
i. Setting to capture packet.

Open new terminal in Kali Linux. Plug-in the TP-Link wireless adapter and connect the device to Kali Linux. Type 'airmon-ng' and see the listed interface. Next configure the interface into monitor mode for capturing purposes. Refer figure below.



ii. Packet capture information

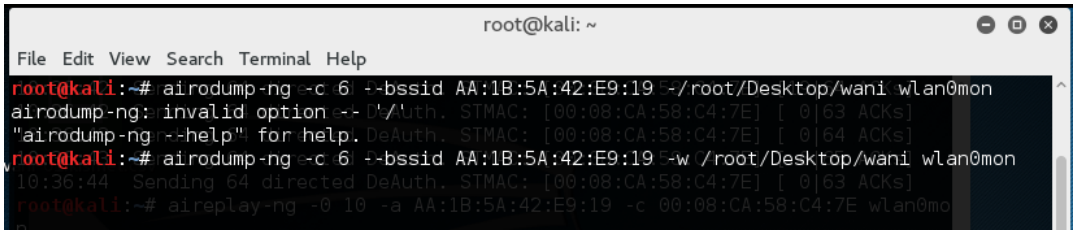
The BSSID found in the home wireless network at Presint 5.



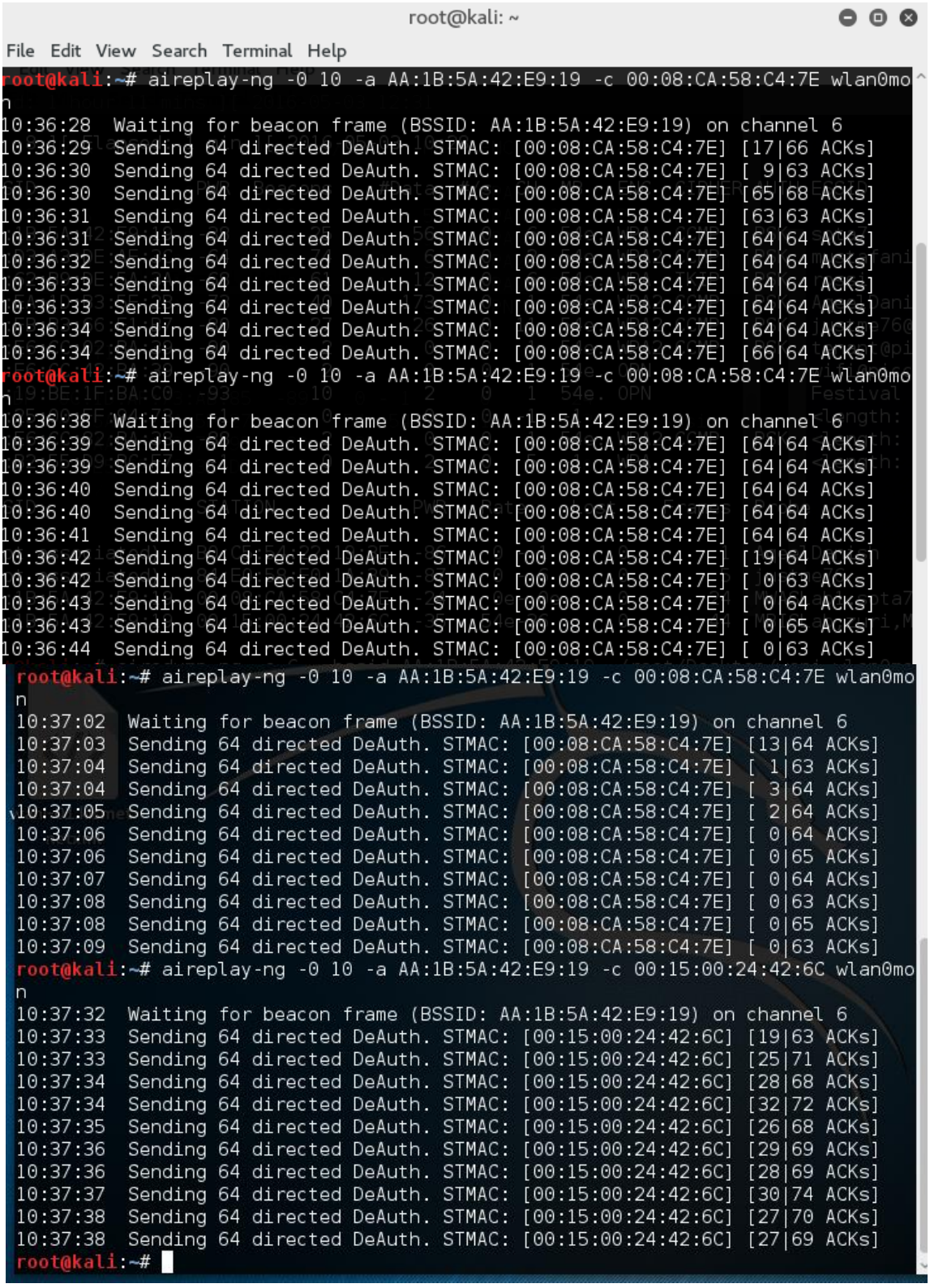
The selected BSSID is AA:1B:5A:42:E9:19 with ESSID named as '*sota7*'. This BSSID was chosen because there is a bigger advantage on WPA encryption. The channel used is 6.

iii. Penetrate the wireless network chosen

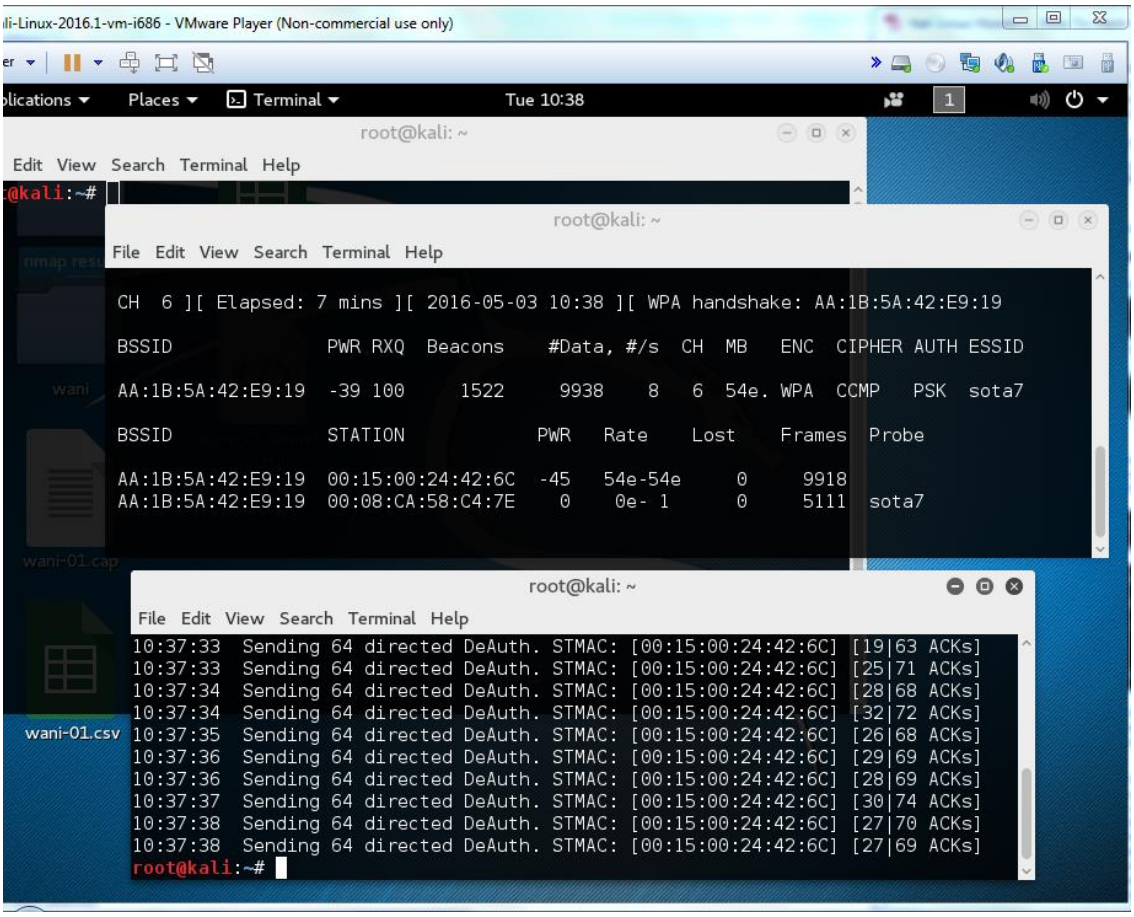
File for saving the capture packet purposes.

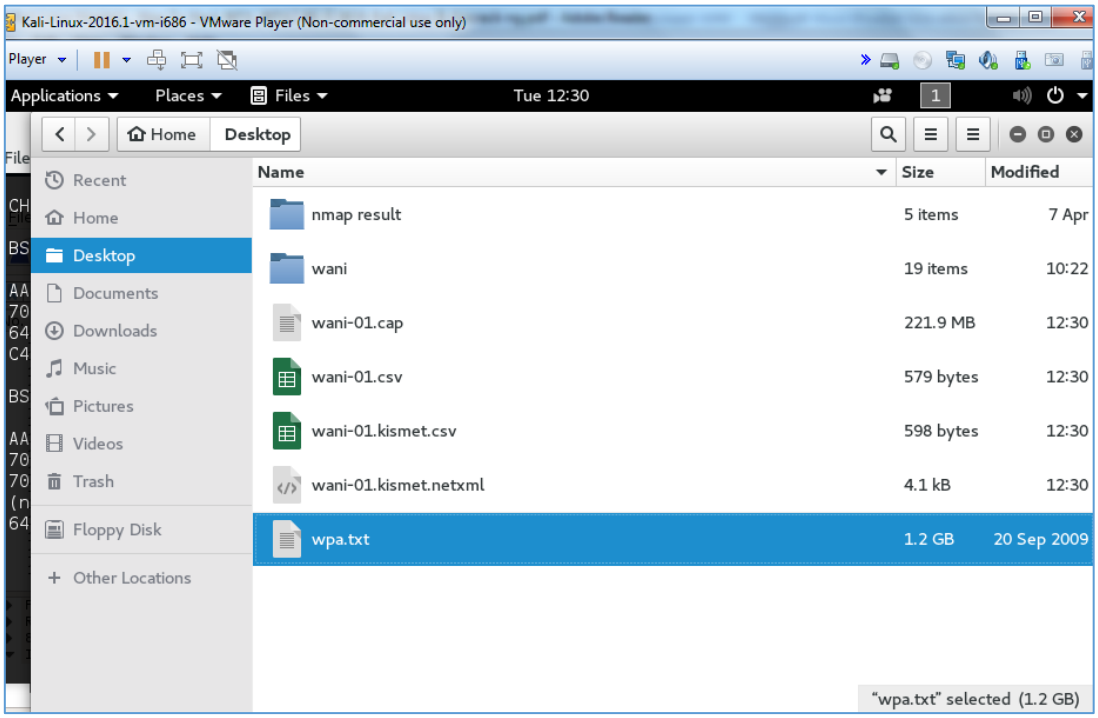


The deauthorization process was being sent in below capture.

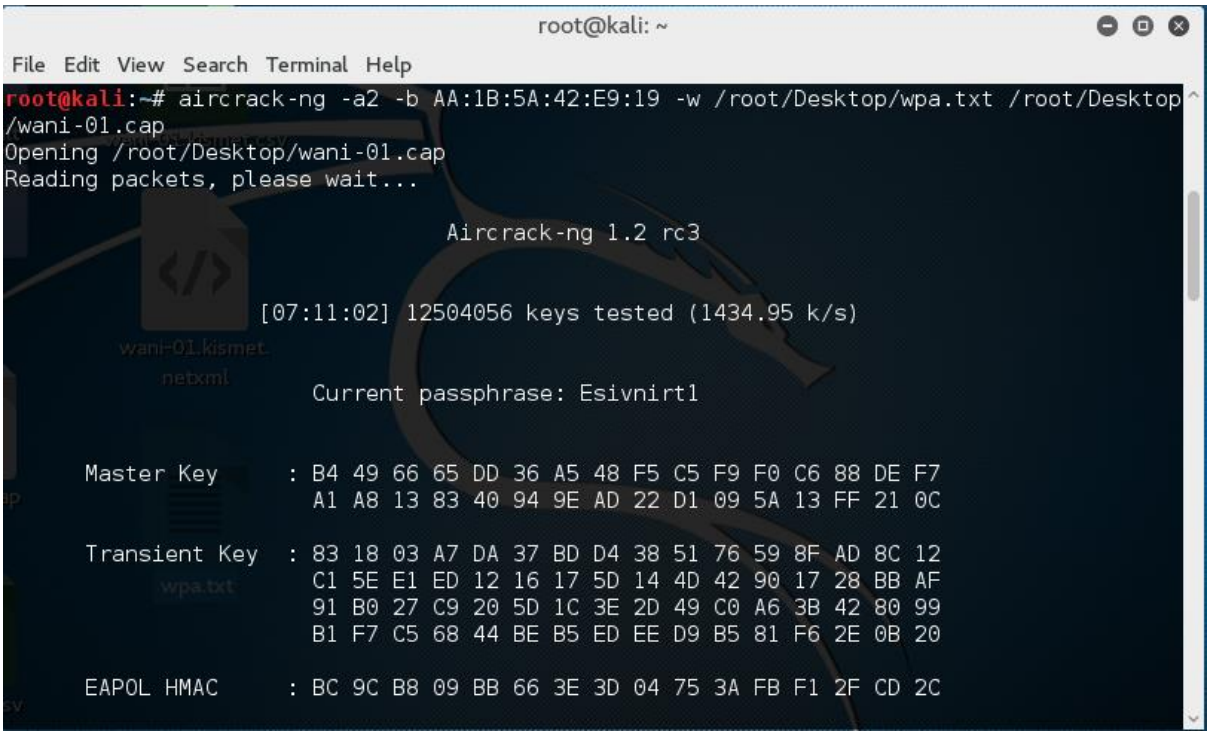


Repeat the process until the handshake shown in previous screen. After the success of deauth, the handshake was shown in the figure below:

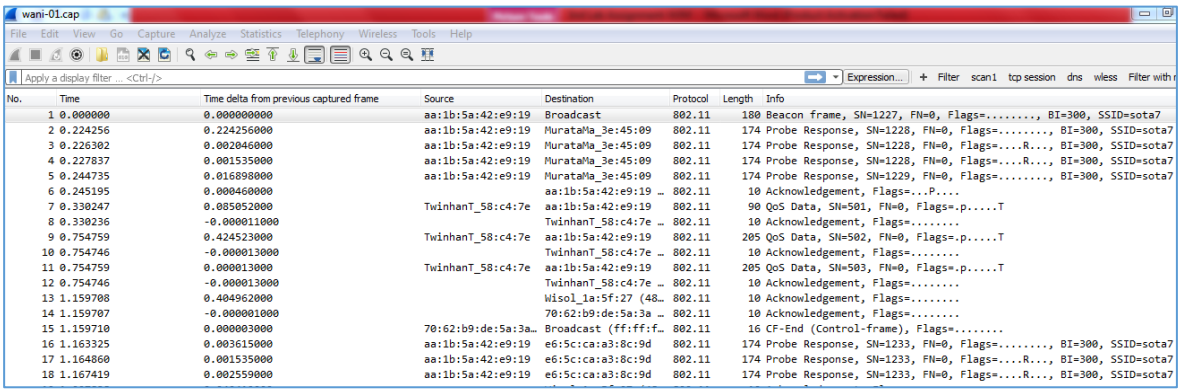




Access the file location for the .cap and the wordlist to try cracking the password. Sample of the cracking process is shown below.



Unfortunately, the password was not able to be crack even the process has taken almost 1 day. This may due to the length of the password.



Using Wireshark, we see the traffic of home wireless network.

1. Step taken	➢ In Kali Linux, plug-in the TP-Link Wireless Adapter. ➢ Configure the interface to monitor mode and make sure the interface is in 'up' state. Command: **airmon-ng start wlan0**. ➢ Start scanning the wireless network by using command **airodump-ng wlan0**.The list of available wireless network will be displayed. ➢ Select the target that has least security encryption. Copy the BSSID and channel. ➢ **Airodump-ng -c <channel> --bssid<bssid> -w<location to save file> wlan0**. This command will save the 4-way intercepted handshake in it. ➢ See if any client connected to it. If yes, send command to deauth the handshake.Command: **aireplay-ng 0 10 -a <router bssid> -c <client bssid> wlan0**. The '10' refers to total deauth packets send. ➢ If successful, the handshake will be visible in the previous screen. ➢ Open new terminal and type this **command aircrack-ng -a2 -b<router bssid> -w<path to wordlist> <path to .cap file>** ➢ To monitor the packet capture, open the packet in Wireshark and try to find the any password inside it.
2. Tools used	Kali Linux, Aircrack-ng, TP-Link Wireless Adapter, Wordlist (download from internet), Wireshark.
3. Conclusion	Based on the activity describe above, it is possible to crack the password of wireless especially those that have weak encryption. The process was not long and any determined hackers will eventually have the password. It is advisable to use tighten security in wireless technology to avoid loss in future.

3. WEB APPLICATION VULNERABILITIES

Question:
Learning objectives:

1. Learn how to access web sites vulnerabilities.
2. Apply necessary tools.
3. Get summarize of web sites status.

Discover **3** web hosting host from the Internet, e.g *ftsm.ukm.my* or *ukm.my*. You can choose any sites. Please do not use something big like www.google.com or www.amazon.com. Please use your judgement. If you still confuse, just use ftsm.ukm.my or ukm.my.
How would you test whether the web hosts for vulnerabilities. Use any relevant tools for these tasks.
Please indicate the steps you have taken, the tools used, and your conclusions. Please use table to summarize your finding. Please include screen shots and relevant output.

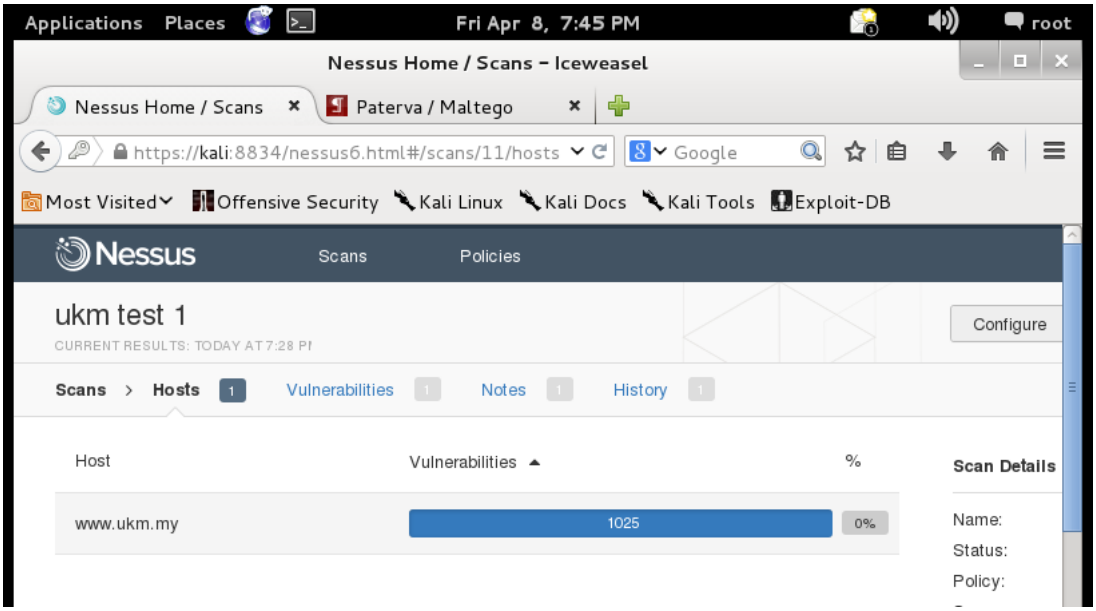
There are 3 webpages that have been chosen for the web application vulnerabilities test and that are:

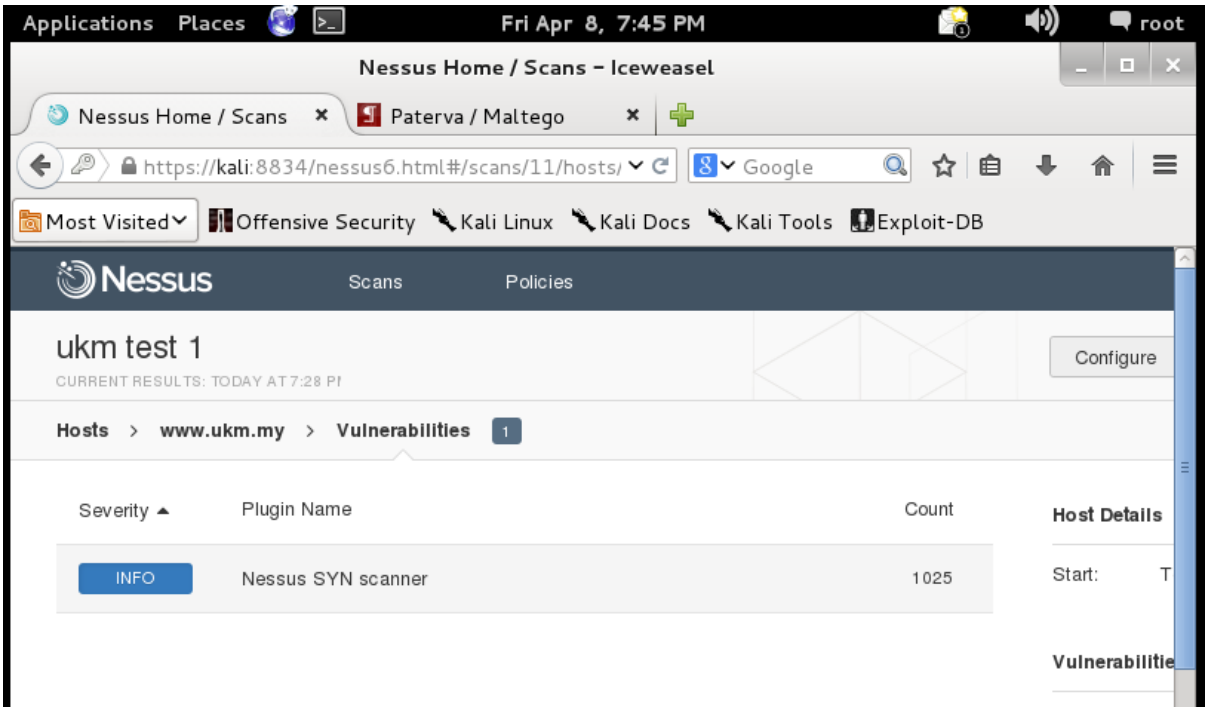
i. www.ukm.my
ii. ftsm.ukm.my
iii. ifolio.ukm.my

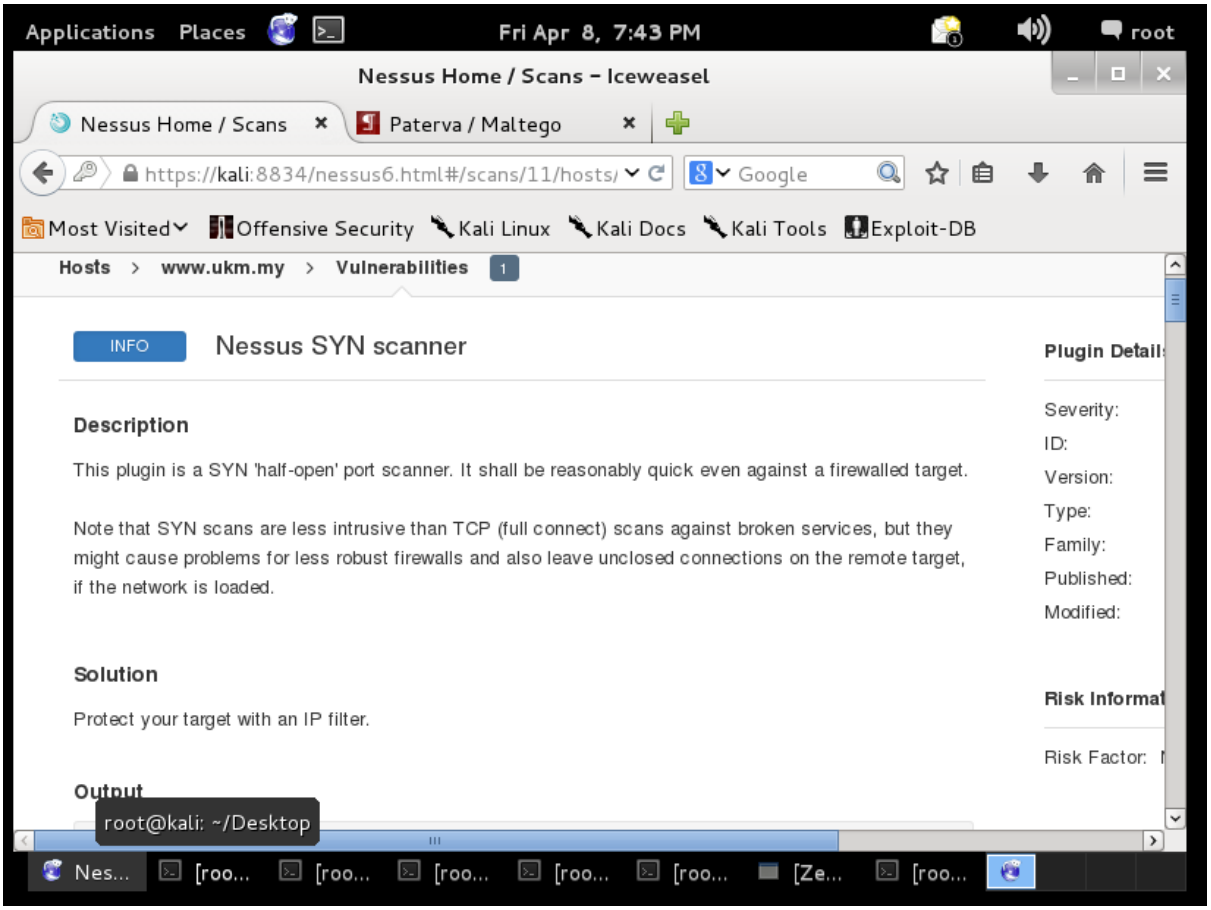
Web Application vulnerability discovery

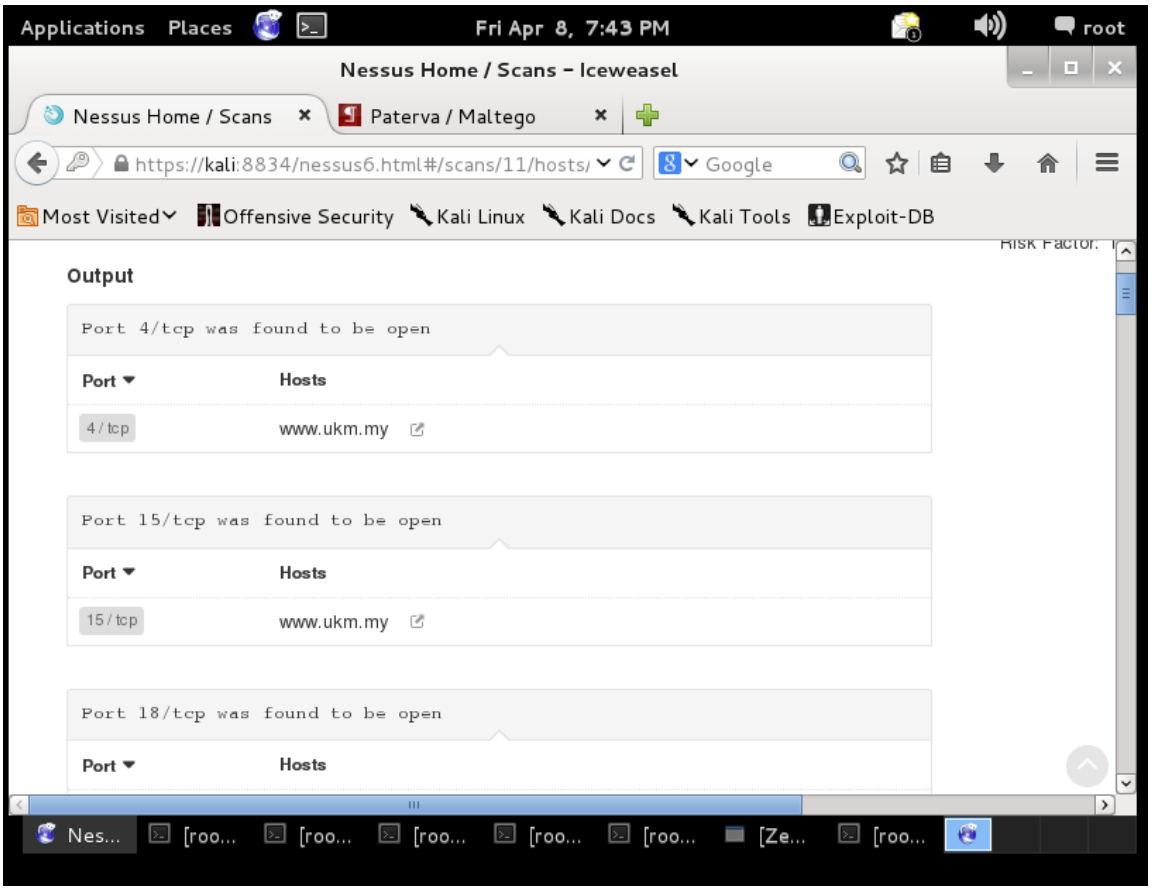
The test was conducted using Nessus. Below are the results of the conducted test:

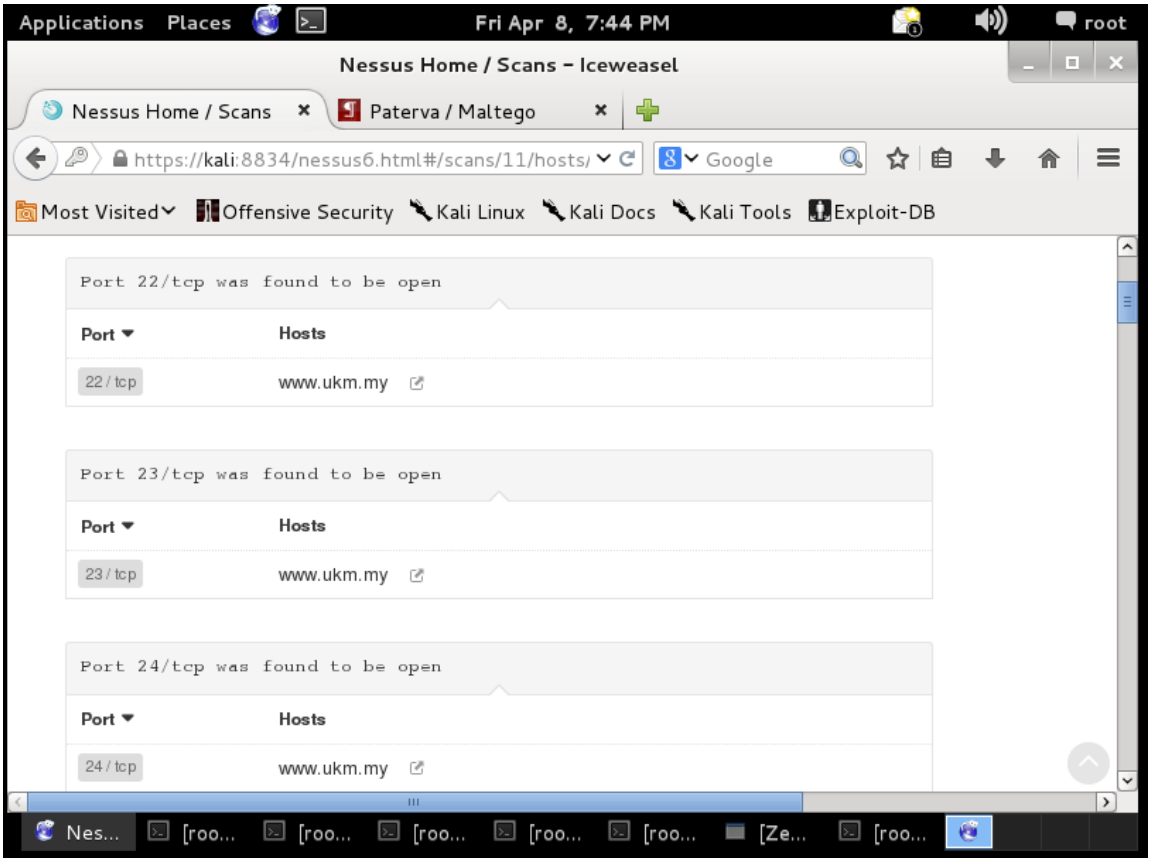
For www.ukm.my



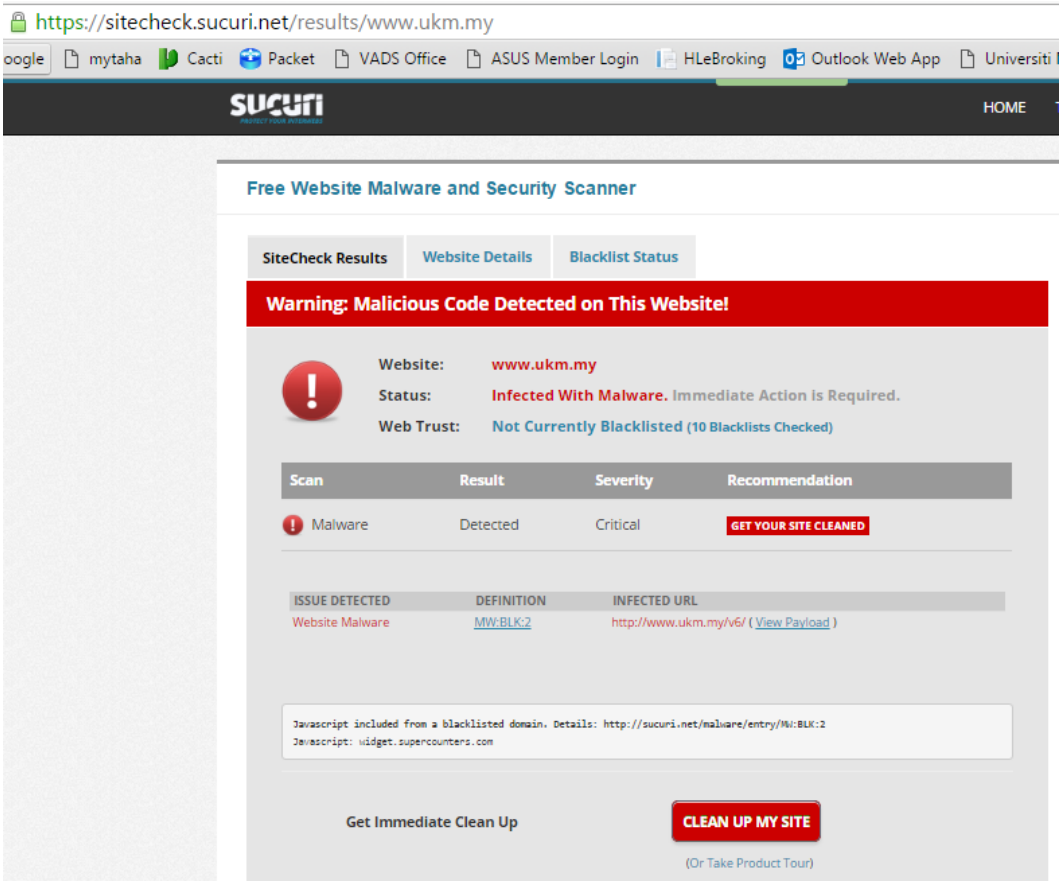

Applications Places
Fri Apr 8, 7:45 PM
root
Nessus Home / Scans - Iceweasel
Nessus Home / Scans
Paterva / Maltego
https://kali:8834/nessus6.html#/scans/11/hosts/
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Nessus
Scans
Policies
ukm test 1
CURRENT RESULTS: TODAY AT 7:28 PM
Configure
Hosts > www.ukm.my > Vulnerabilities 1
Severity
Plugin Name
Count
INFO
Nessus SYN scanner
1025
Host Details
Start:

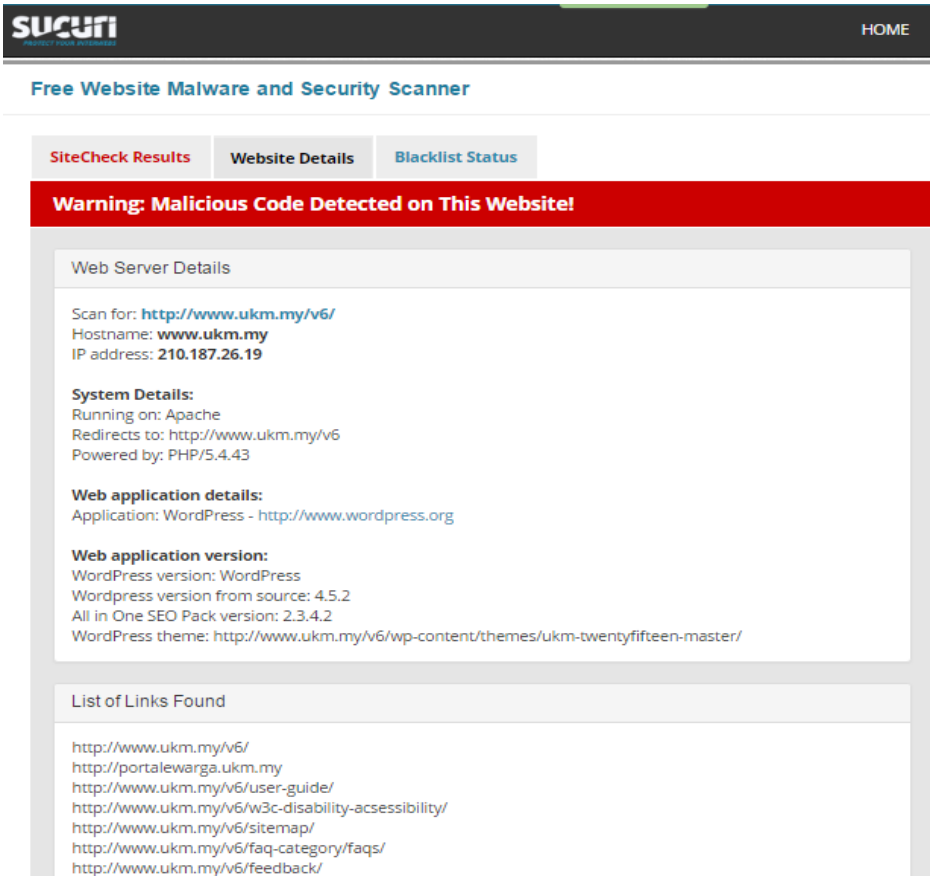

Applications Places
Fri Apr 8, 7:43 PM
root
Nessus Home / Scans - Iceweasel
Nessus Home / Scans
Paterva / Maltego
https://kali:8834/nessus6.html#/scans/11/hosts/
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Hosts > www.ukm.my > Vulnerabilities 1
INFO
Nessus SYN scanner
Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.
Solution
Protect your target with an IP filter.
Output
Plugin Details
Severity:
ID:
Version:
Type:
Family:
Published:
Modified:
Risk Information
Risk Factor:
root@kali: ~/Desktop


Applications Places Fri Apr 8, 7:43 PM root
Nessus Home / Scans – Iceweasel
Nessus Home / Scans
Paterva / Maltego
https://kali:8834/nessus6.html#/scans/11/hosts/
Google
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB
Output
Port 4/tcp was found to be open
Port Hosts
4 / tcp www.ukm.my
Port 15/tcp was found to be open
Port Hosts
15 / tcp www.ukm.my
Port 18/tcp was found to be open
Port Hosts

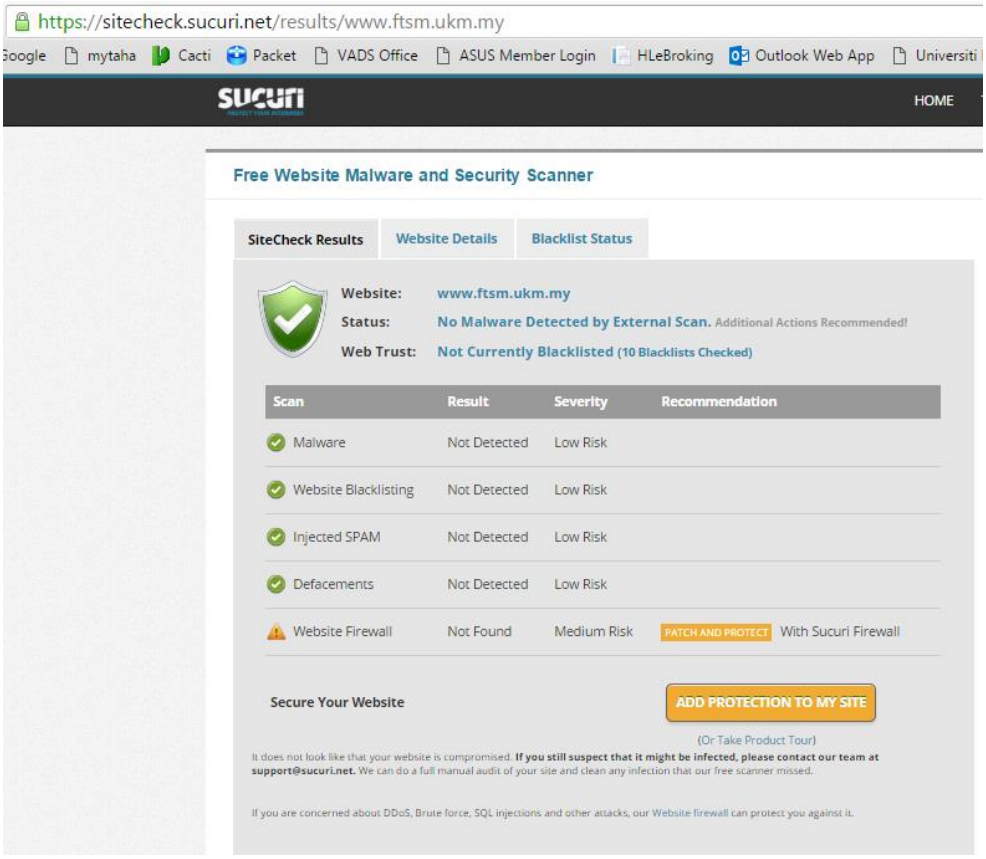

Applications Places Fri Apr 8, 7:44 PM root
Nessus Home / Scans – Iceweasel
Nessus Home / Scans
Paterva / Maltego
https://kali:8834/nessus6.html#/scans/11/hosts/
Google
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB
Port 22/tcp was found to be open
Port Hosts
22 / tcp www.ukm.my
Port 23/tcp was found to be open
Port Hosts
23 / tcp www.ukm.my
Port 24/tcp was found to be open
Port Hosts
24 / tcp www.ukm.my

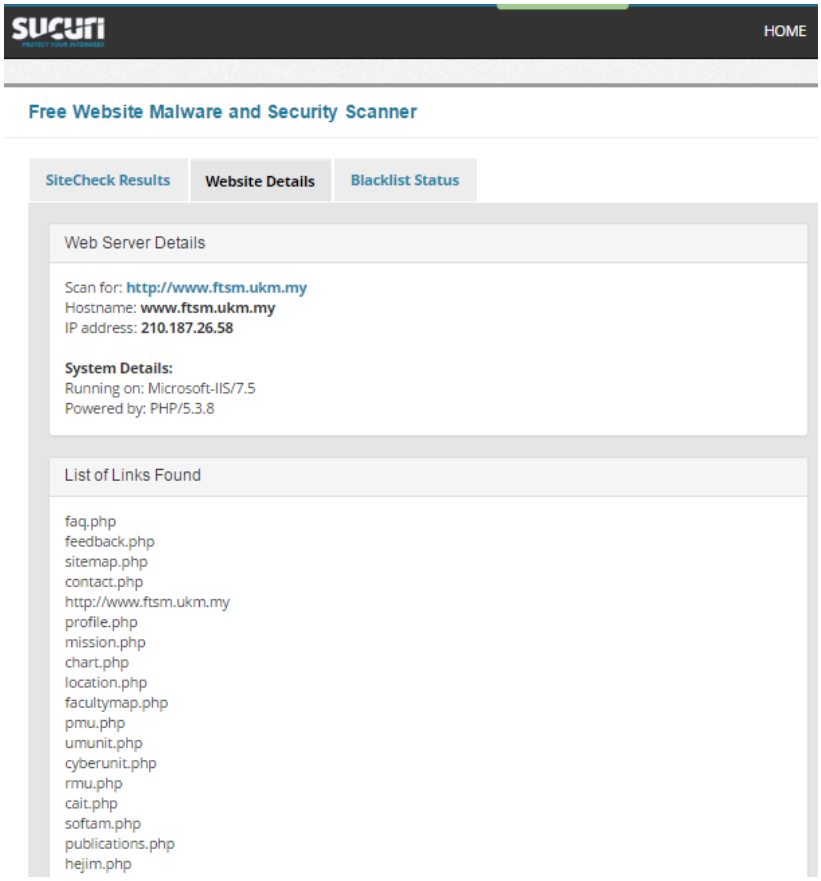
Using succuri for www.ukm.my



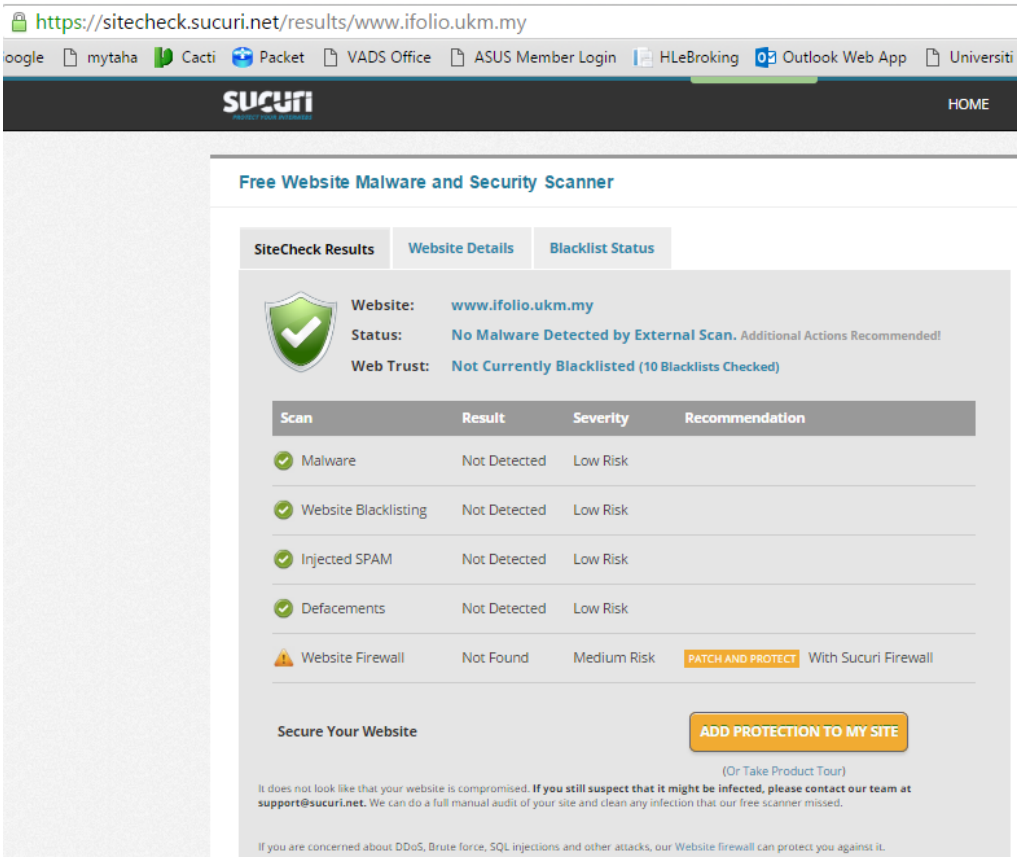


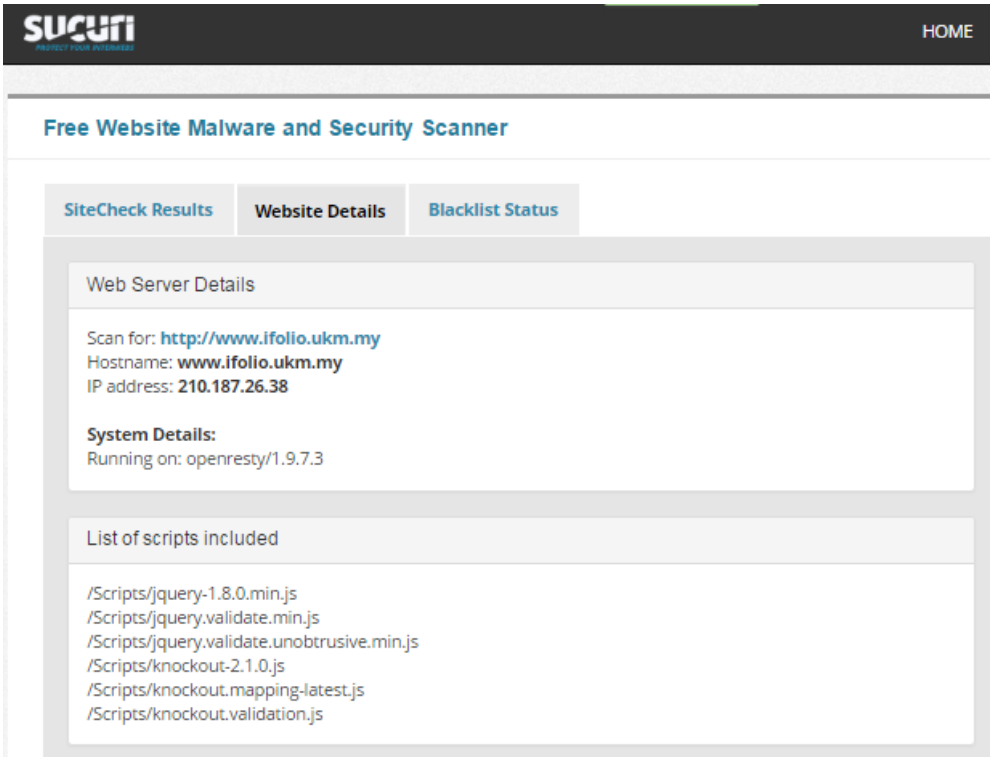
Using succuri for www.ftsm.ukm.my

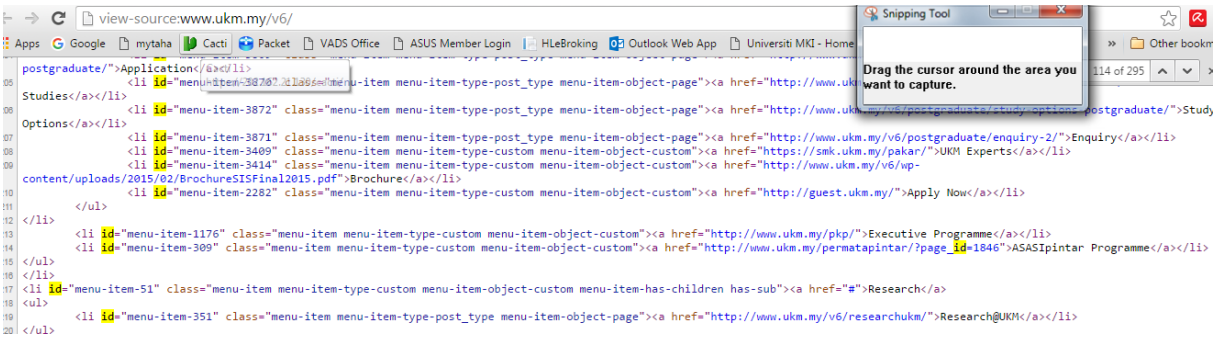




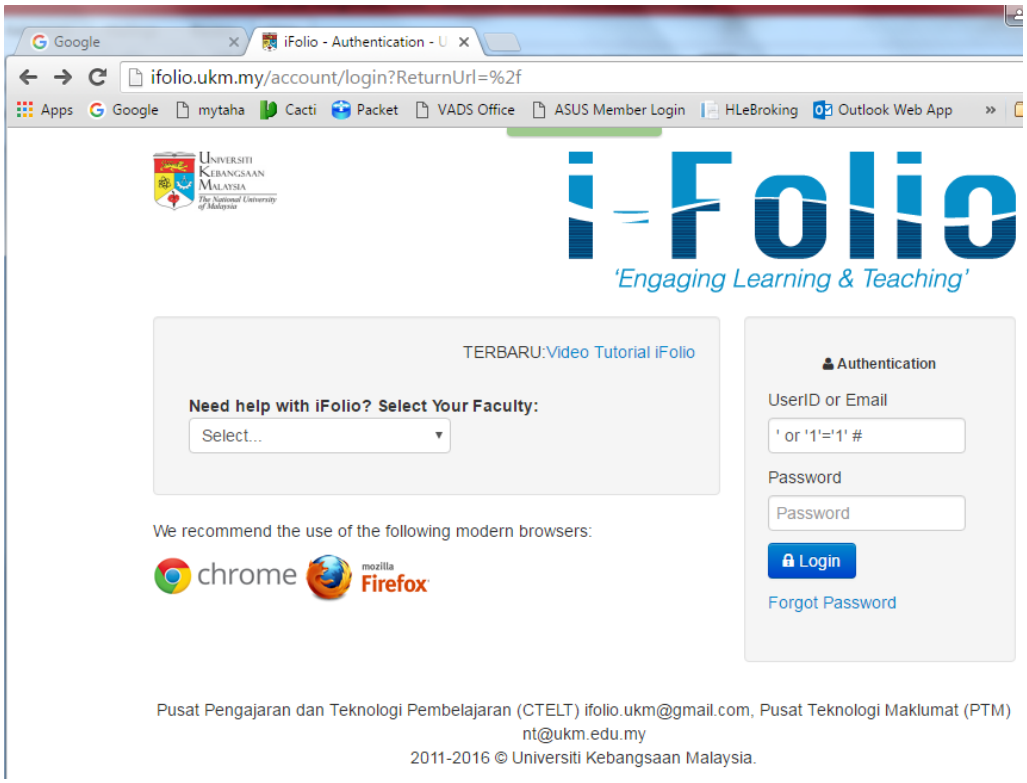
Using succuri for www.ifolio.ukm.my

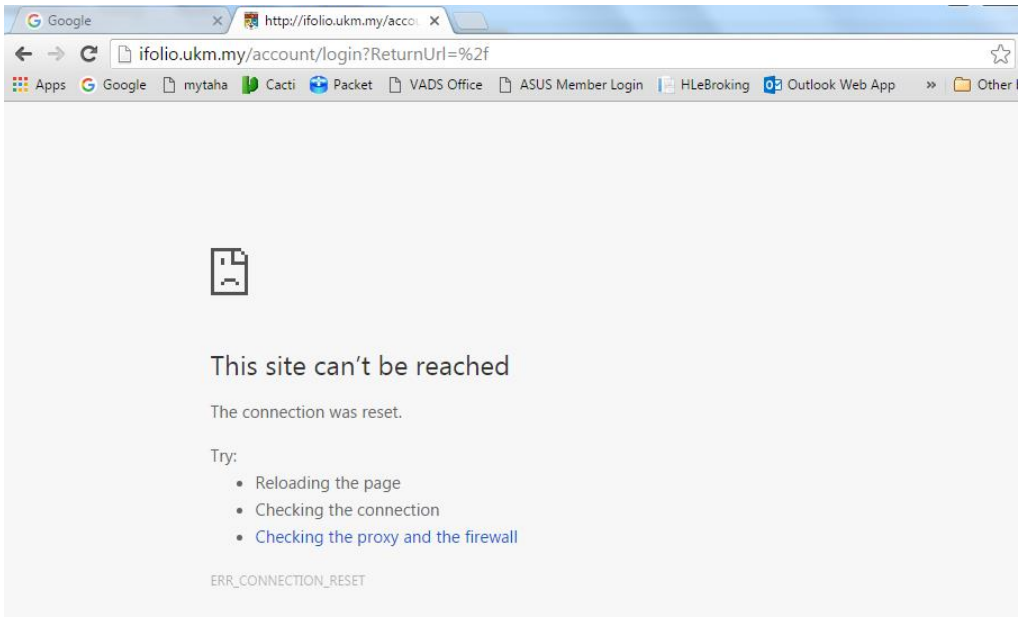


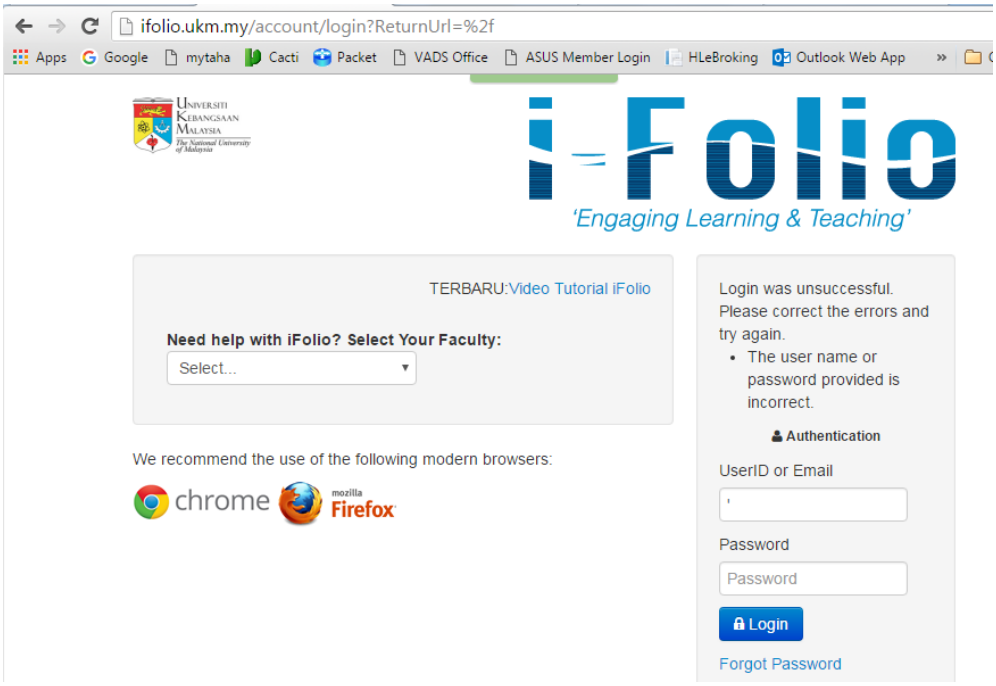




SQL Injection testing

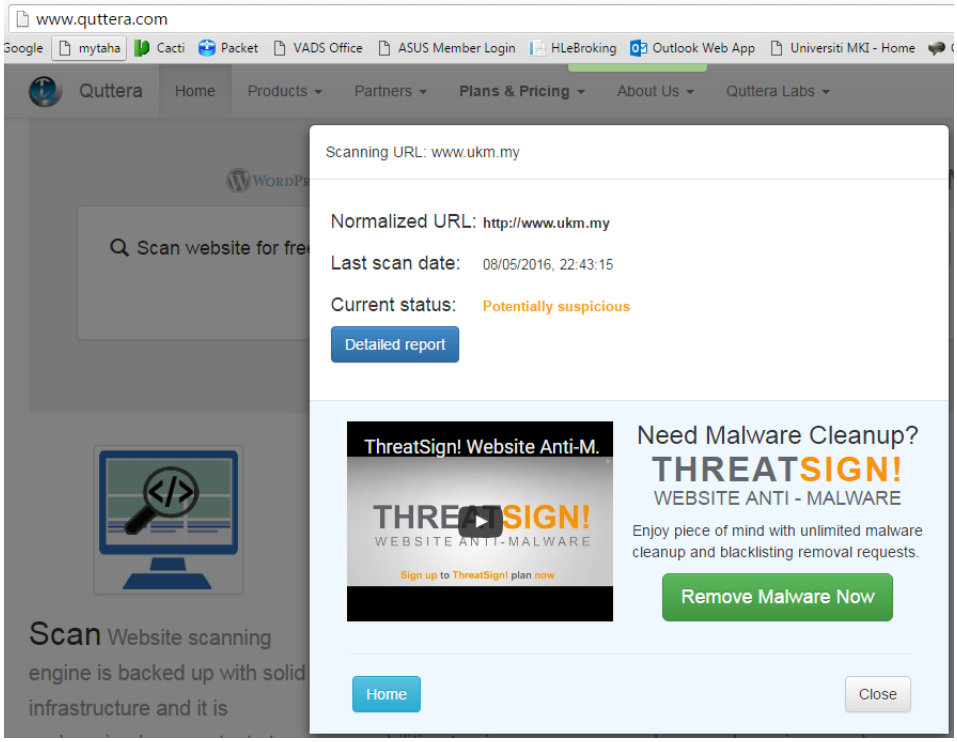






While inputting ' this is the error.

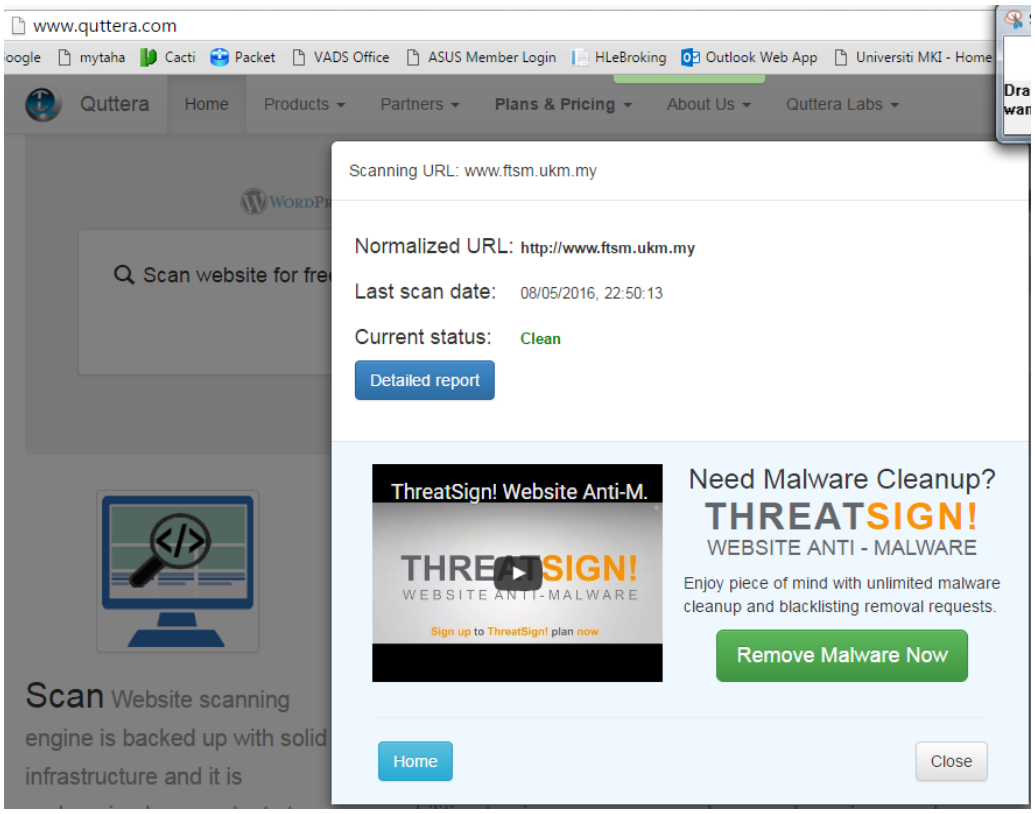
Using Quterra for www.ukm.my



It says that this website is potentially suspicious.

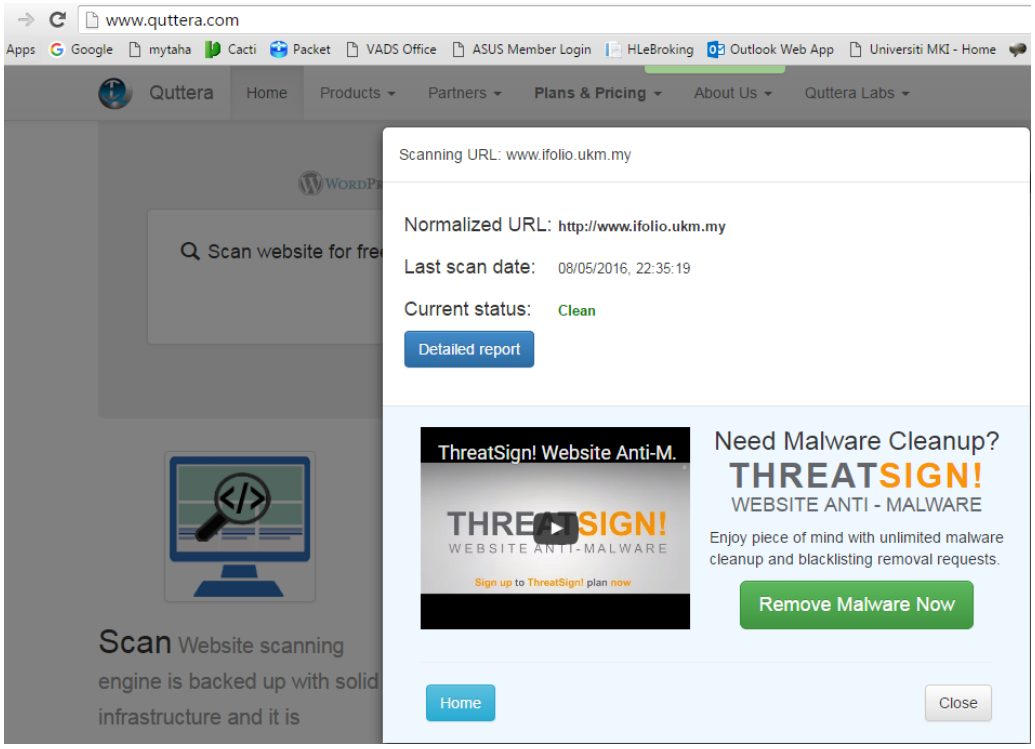
Normalized URL:	http://www.ukm.my:80
Submission date:	Sun May 8 16:43:15 2016
Server IP address:	210.187.26.19
Country:	Malaysia
Server:	Apache
Malicious files:	0
Suspicious files:	0
Potentially Suspicious files:	1
Clean files:	30
External links detected:	100
Iframes scanned:	2
Blacklisted:	No

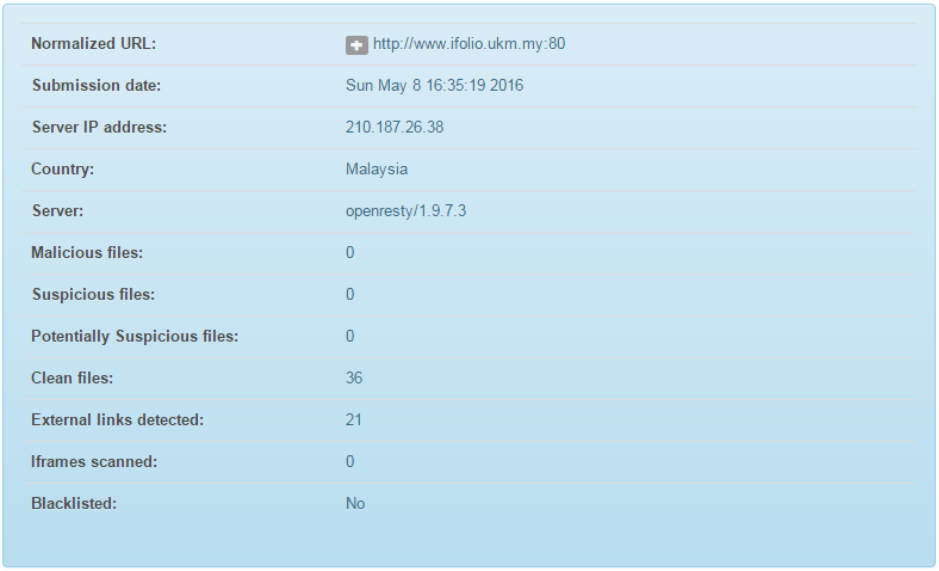
Using Quterra for www.ftsm.ukm.my



Normalized URL:	http://www.ftsm.ukm.my:80
Submission date:	Sun May 8 16:50:13 2016
Server IP address:	210.187.26.58
Country:	Malaysia
Server:	Microsoft-IIS/7.5
Malicious files:	0
Suspicious files:	0
Potentially Suspicious files:	0
Clean files:	101
External links detected:	84
Iframes scanned:	7
Blacklisted:	No

Using Quterra for www.ifolio.ukm.my





Normalized URL:	http://www.ifolio.ukm.my:80
Submission date:	Sun May 8 16:35:19 2016
Server IP address:	210.187.26.38
Country:	Malaysia
Server:	openresty/1.9.7.3
Malicious files:	0
Suspicious files:	0
Potentially Suspicious files:	0
Clean files:	36
External links detected:	21
Iframes scanned:	0
Blacklisted:	No

1. Step taken	Using Nessus and online tools like Succuri, Quterra by inputting the url of www.ukm.my, www.ftsm.ukm.my and www.ifolio.ukm.my
2. Tools used	Nessus, sql injection, Succuri, Quterra
3. Conclusion	Based on the ttols used, one alert from succuri tools mention there is a malware threat on www.ukm.my and none for the other two sites. However by using sql injection to www.ifolio.ukm.my it seems that the site was not fully protected due to the error it was showing (this site can't be reached) error.

4. EXPLOITATION

Learning objective:

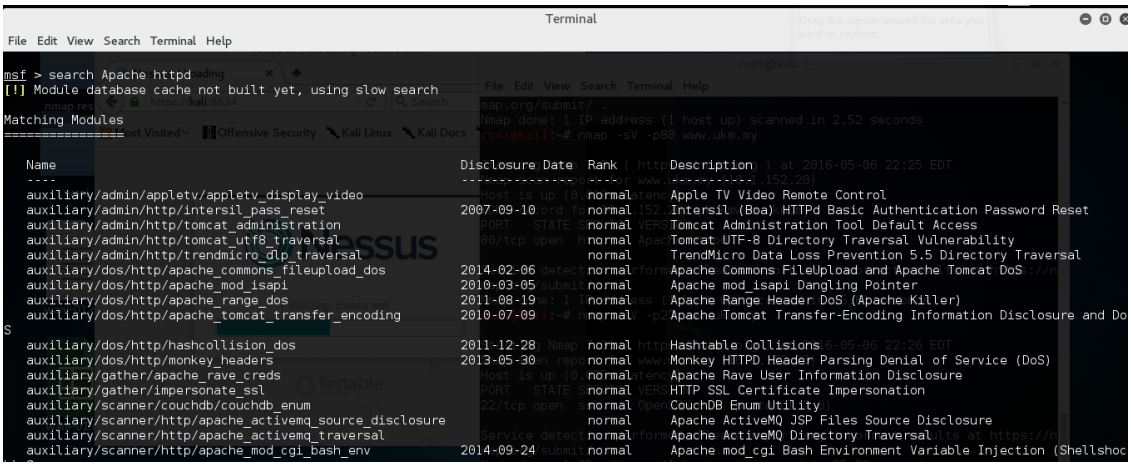
1. How to search for exploitation for a site.
2. Search the severity of the exploitation
3. Do not exploit. Just mention, what you find.

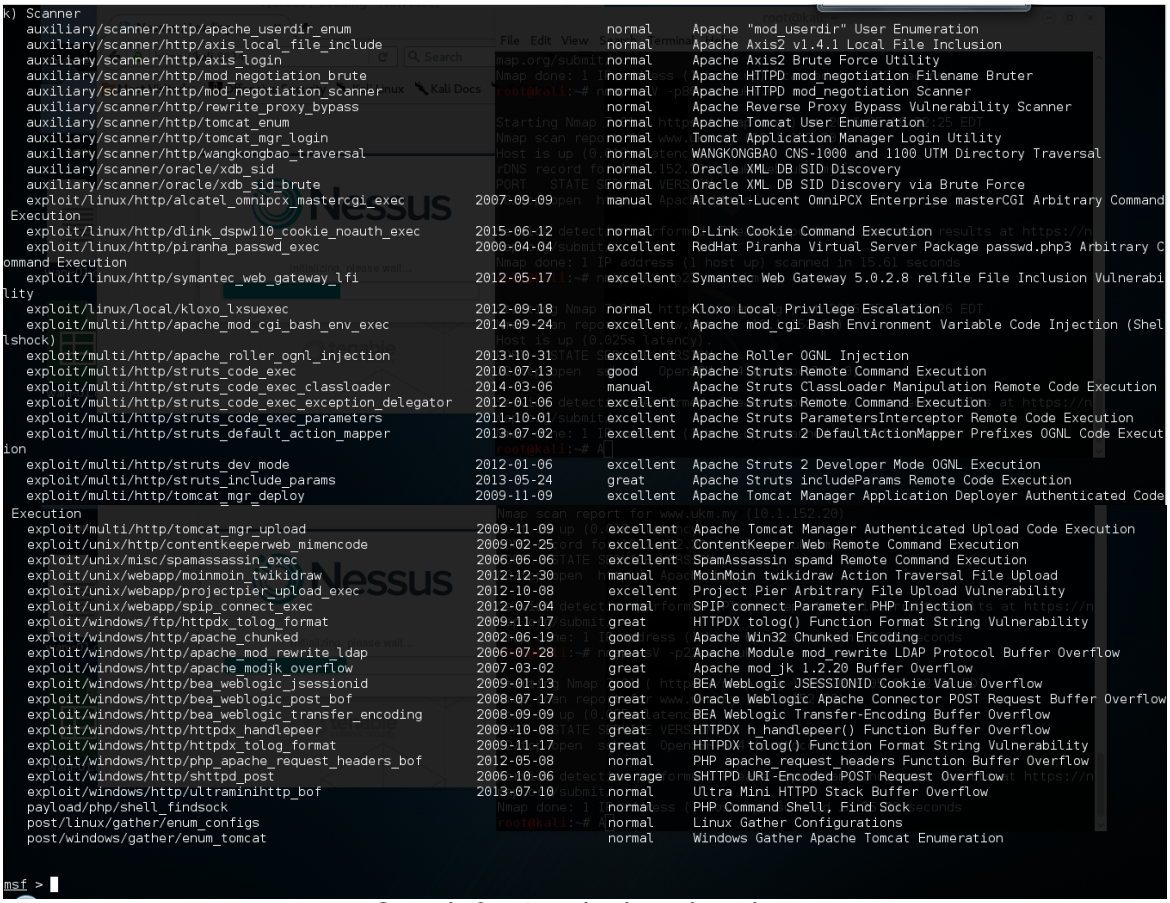
Pick *one* host from ***ukm.my*** domain. You can use your result from previous work. (you can use your result from question 1.)
Search for 5 possible exploitation on the hosts. See the severity of the exploit. Is exploitation possible? Why do the exploitation possible? (System not patchs, etc.)
Explain how to use the exploitations.
Please indicate the steps you have taken, the tools used, and your conclusions. Please use table to summarize your finding. Please include screen shots and relevant outputs.
Please treat this lab assignment as a learning process, ask questions if you need clarification and encourage knowledge sharing. However, end result is yours.

Based on nmap scan in Question 1, above port is open and service was listed. The potential exploitation was search using the Metaspoilt in Kali Linux.

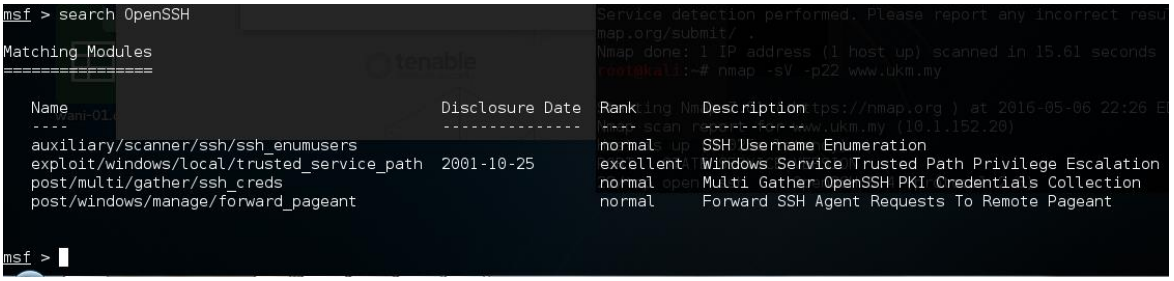
```
root@kali:~# nmap -sS -sV www.ukm.my

Starting Nmap 7.01 ( https://nmap.org ) at 2016-05-06 22:18 EDT
Nmap scan report for www.ukm.my (10.1.152.20)
Host is up (0.038s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Pure-FTPd
22/tcp open  ssh     OpenSSH 6.4 (protocol 2.0)
80/tcp open  http    Apache httpd

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.63 seconds
root@kali:~#
```

By using this tool, we can search the exploit in by typing search follows by the service found earlier. Refer figure below for each services exploit search.

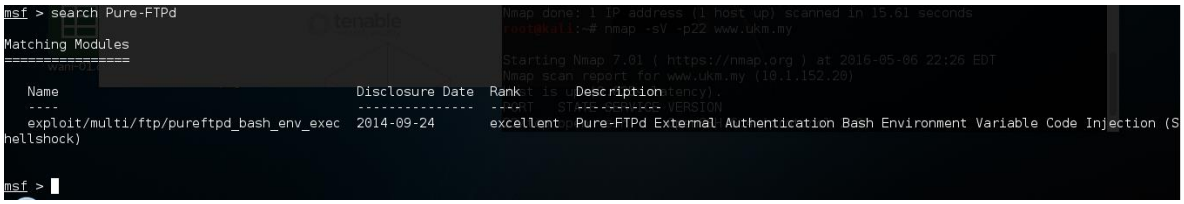




Search for Apache httpd exploit



Search for OpenSSH exploit



Searching for Pure-FTPd exploit

Based on the result found, we can use the listed exploit above to instruct Metaspoilt to do the exploitation. The severity of the exploit is listed under 'Rank' column. One of the reasons of the exploit is the system not being patched accordingly. Sometimes this is due to either two reasons, one is because the user or system administrator neglectful to do the

update and two; because the system will have problem and if the update being carried out. Usually the historical system or software that the manufacturer have stopped the support and updated their services will also facing this vulnerabilities.

1. Step taken	Using nmap to scan the services that have potential to be exploit using command: *nmap -sS -sV www.ukm.my*. Search the listed services in metaspoilt. Type *search <services>* The listed exploit are ready to be use. Type command *use <selected exploit> IP* and click enter. Set the variable needed like IP, port number and host. Type '*exploit*' to start the process.
2. Tools used	Nmap and Metaspoilt
3. Conclusion	By combining Nmap and Metaspoilt program, we can take advantage on the listed vulnerable port and services.