ITT 450
INFORMATION AND NETWORK SECURITY

(REPORT ANALYSIS OF TWO DOMAINS ASSIGNMENT)

Instructor: Sir Mohd Ali	
Name	**Zaimah Binti Jamaluddin**
Matric ID	**2017917675**
Group	**M3CS2453A**

TABLE OF CONTENTS

No	Contents	Page
1	SUMMARY OF FINDINGS sabah.uitm.edu.my fixi.com.my	3-5
2	SUMMARY OF RECOMMENDATIONS sabah.uitm.edu.my fixi.com.my	6
3	DETAIL FINDINGS sabah.uitm.edu.my fixi.com.my	7-12
4	REFERENCES	13

1. Summary of Findings

The two domains which I choose for this assignment are:

a) sabah.uitm.edu.my

b) fixi.com.my

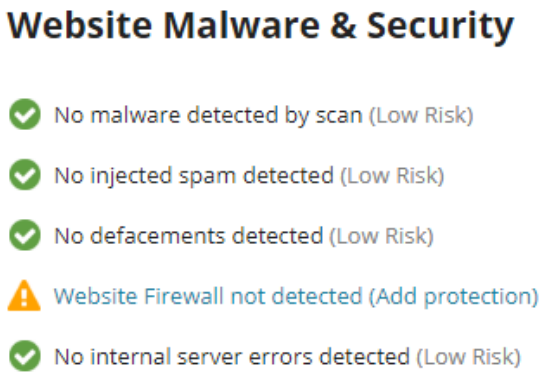
The findings that I got on these two websites are based on the result of a few online web scanners and the use of the Nmap in Kali Linux to scan the domains.

Below are the results:

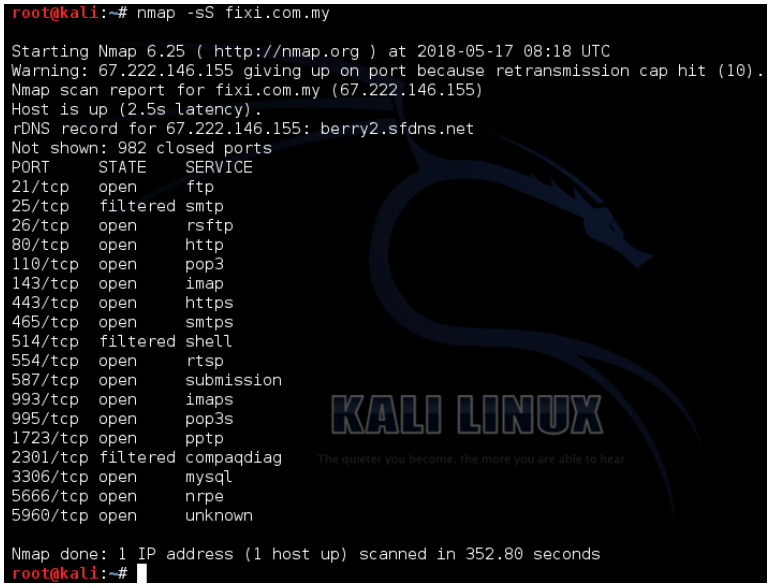
Domains	Summary of findings
sabah.uitm.edu.my	One of the primary findings of all the result is that this domain is using an outdated version of Joomla which is Joomla Version 3.6.0. **Site is Outdated** (using Joomla Version 3.6.0 found at: 'http://sabah.uitm.edu.my/v2//administrator/manifests/files/joomla.xml') This was found by using Sucuri Website Scanner. Besides that, I also found that the domain does not have a website firewall. All the online website scanners that I used have not detected any sort of firewall for their website. **Website Malware & Security** No injected spam detected (Low Risk) No defacements detected (Low Risk) Website Firewall not detected (Add protection) No internal server errors detected (Low Risk) Site is outdated (Medium Risk) (More details)

	Lastly, by using Nmap in Kali Linux, I have found that this domain has several open ports such as tcp port 21, 80 and 443. The vulnerabilities that the open port will be discussed in details in the Detail Findings part of this report. root@kali:~# nmap -sS sabah.uitm.edu.my Starting Nmap 6.25 (http://nmap.org) at 2018-05-17 07:39 UTC Nmap scan report for sabah.uitm.edu.my (202.58.80.225) Host is up (0.017s latency). Not shown: 983 filtered ports PORT STATE SERVICE 21/tcp open ftp 80/tcp open http 84/tcp closed ctf 443/tcp open https 554/tcp open rtsp 1723/tcp open pptp 1812/tcp closed radius 2522/tcp closed windb 3333/tcp closed dec-notes 4550/tcp closed gds-adppiw-db 5862/tcp closed unknown 6129/tcp closed unknown 6881/tcp closed bittorrent-tracker 8080/tcp closed http-proxy 9593/tcp closed cba8 10082/tcp closed amandaidx 34572/tcp closed unknown Nmap done: 1 IP address (1 host up) scanned in 105.38 seconds
fixi.com.my	After I have done many online web scanners on this domain, this website is relatively secure as most of the results show that it does not have any major weakness or vulnerabilities that those online scanners can find. For example, here is one of the results from Sucuri website scanner that i found which is the security risk also still in good conditions. No Malware Found Our scanner didn't detected any malware Site is not Blacklisted 9 Blacklists checked 90 URLs Scanned Pages scanned: 86 Javascript files scanned: 3 Other files: 1 Low Security Risk Medium

But unfortunately, I found that the domain does not have a website firewall.



Other than that, by using Nmap in Kali Linux, I found for this domain has several ports that is open.



```
root@kali:~# nmap -sS fixi.com.my

Starting Nmap 6.25 ( http://nmap.org ) at 2018-05-17 08:18 UTC
Warning: 67.222.146.155 giving up on port because retransmission cap hit (10).
Nmap scan report for fixi.com.my (67.222.146.155)
Host is up (2.5s latency).
rDNS record for 67.222.146.155: berry2.sfdns.net
Not shown: 982 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
25/tcp   filtered smtp
26/tcp   open     rsftp
80/tcp   open     http
110/tcp  open     pop3
143/tcp  open     imap
443/tcp  open     https
465/tcp  open     smtps
514/tcp  filtered shell
554/tcp  open     rtsp
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
1723/tcp open     pptp
2301/tcp filtered compaqdiag
3306/tcp open     mysql
5666/tcp open     nrpe
5960/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 352.80 seconds
root@kali:~#
```

I also have obtained some important information regarding the domain by using Who.is such as registrant and administrative contact information. Besides that, it also shows me the servers name and ip addresses.

2. Summary of Recommendations

Based on the result that I have found on the two domains, this is a few recommendations on how to improve their security website and decrease their risk on being hack.

Domains	Summary Recommendations
sabah.uitm.edu.my	The important thing that needs to be done first is to update the domain to the latest version of Joomla as this is the first thing that an attacker would try to access the data in the domain. Therefore, below is the other recommendations are: • Create a firewall for their website. • Update their site regularly. • Manage the security of open ports correctly.
fixi.com.my	The admin must take an action to this domain to hide their domain information on who.is because the attacker can easily use their information such as their server ip, to make an attack on this domain. So, here other recommendations are: • Close unnecessary open ports. • Update the domain operating system to the latest version. • Create a firewall to this website to make it more secure.

3. Detail Findings.

The domain of sabah.uitm.edu.my is less secure when compared to the domain fixi.com.my due to a few causes after all of the results have been checked. Thus, below are the results that I have found with the recommendations to secure the website.

Detail Findings and Recommendations for sabah.uitm.edu.my	
Information about the domain	SITE http://sabah.uitm.edu.my/v2/ DOMAIN sabah.uitm.edu.my IP 202.58.80.225 CMS Joomla NOTICE Apache Redirects to: http://sabah.uitm.edu.my/v2 INFO Application: Joomla! - Open Source Content Management,http://www.joomla.org VERSION Joomla Version 3.6.0 found at: 'http://sabah.uitm.edu.my/v2//administrator/manifests/files/joomla.xml' WARN Joomla version outdated: Upgrade required.

Site	http://sabah.uitm.edu.my	**Netblock Owner**	Universiti Teknologi MARA
Domain	uitm.edu.my	**Nameserver**	ns2.uitm.edu.my
IP address	202.58.80.225	**DNS admin**	postmaster@salam.uitm.edu.my
IPv6 address	*Not Present*	**Reverse DNS**	seladang.uitm.edu.my
Domain registrar	mynic.net.my	**Nameserver organisation**	whois.mynic.net.my
Organisation	Universiti Teknologi MARA, Pusat Sistem Maklumat Bersepadu Tkt 5, Bangunan Menara, Universiti Teknologi MARA40450 Shah Alam Selangor, Malaysia	**Hosting company**	*unknown*
Top Level Domain	Malaysia (.edu.my)	**DNS Security Extensions**	*unknown*
Hosting country	MY		

Netblock owner	IP address	OS	Web server	Last seen Refresh
Universiti Teknologi MARA Education Center	202.58.80.223	Linux	Apache/2.2.31 Unix mod_ssl/2.2.31 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 PHP/5.6.28	29-Sep-2017
Universiti Teknologi MARA Education Center	202.58.80.223	Linux	Apache/2.2.19 Unix mod_ssl/2.2.19 OpenSSL/1.0.0-fips mod_auth_passthrough/2.1 mod_bwlimited/1.4 PHP/5.3.5	25-Aug-2012
Universiti Teknologi MARA Education Center	202.58.80.223	Linux	Apache/2.0.63 Unix mod_ssl/2.0.63 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.3.3	7-Jun-2011

Site is outdated	**Risk Rating** High **Analysis** The domain is outdated with a Joomla version of 3.6.0. This can make attacker find the weakness and vulnerabilities of the old version in order to try and hacked into the domain. **Recommendation** The admin should update the website to avoid the domain from hackers.
Communication is not secure	**Risk Rating** High **Analysis** The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data). **Recommendation** It is recommended to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

<table>
<tr>
<td>Server software and technology found</td>
<td>
<table>
<tr><th>Software / Version</th><th>Category</th></tr>
<tr><td>Apache</td><td>Web Servers</td></tr>
<tr><td>Joomla</td><td>CMS</td></tr>
<tr><td>Twitter Bootstrap</td><td>Web Frameworks</td></tr>
<tr><td>Google Font API</td><td>Font Scripts</td></tr>
<tr><td>MooTools</td><td>JavaScript Frameworks</td></tr>
<tr><td>jQuery</td><td>JavaScript Frameworks</td></tr>
</table>
Risk Rating
Medium

Analysis
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation
Recommended to eliminate the information which permit the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.
</td>
</tr>
<tr>
<td>No Website Firewall</td>
<td>
Risk Rating
Medium

Analysis
This domain has no firewall for their website. Any connections done with user will not be sterilized of any suspicious activities.

Recommendation
Install the firewall for the website in order to have another layer of protection and also in order to monitor and sterilize any connection that is suspicious.
</td>
</tr>
</table>

Detail Findings and Recommendations for
fixi.com.my

Information about the domain

SITE http://fixi.com.my/

DOMAIN fixi.com.my

IP 67.222.146.155

NOTICE Apache
Powered by: PHP/5.5.38

Site	http://fixi.com.my	**Netblock Owner**	ServerFreak Technologies Sdn Bhd
Domain	fixi.com.my	**Nameserver**	dns1.serverfreak.biz
IP address	67.222.146.155	**DNS admin**	monitor2@serverfreak.biz
IPv6 address	*Not Present*	**Reverse DNS**	berry2.sfdns.net
Domain registrar	mynic.net.my	**Nameserver organisation**	whois.biz
Organisation	Buku Fixi, B-8-2A OPAL DAMANSARA, JALAN PJU 3/27 47810 Petaling Jaya Selangor, Malaysia	**Hosting company**	Tailor Made Servers
Top Level Domain	Malaysia (.com.my)	**DNS Security Extensions**	*unknown*
Hosting country	MY		

```
a [Domain Name]                 fixi.com.my
b [Registration No.]            D1A160284
c [Record Created]              24-FEB-2011
d [Record Expired]              24-FEB-2016
e [Record Last Modified]        18-SEP-2014
f [Invoicing Party]                             R0110
  Lee Cheng Yew
  Serverfreak Technologies Sdn Bhd
  12A, Jalan Teluk Pulai KS/1
  41100 Klang
  Selangor
  Malaysia
  domreg@serverfreak.com
  (Tel) 603-33712564
  (Fax) 603-50219149

g [Registrant Code]                             RKEY0000029237
  Buku Fixi
  (002016254-V)
  B-8-2A OPAL DAMANSARA, JALAN PJU 3/27
  47810 Petaling Jaya
  Selangor
  (Tel) 012-2311584
  (Fax) -
```

Netblock owner	IP address	OS	Web server	Last seen Refresh
ServerFreak Technologies Sdn Bhd 12A JALAN TELUK PULAI KLANG SE MY 41100	67.222.146.155	Linux	Apache	17-May-2018

Did Not Hide Their Information on Who.Is	**Risk Rating** Low **Analysis** The important information about the domain can be seen on Who.is as the administrator did not choose to hide it. Thus, the attackers can try to hack based on the information that they have especially about the name and ip of their server. **Recommendation** Recommended for the admin to hide the important information because the chance of the attackers to stealing the data is high.
Communication is not secure	**Risk Rating** High **Analysis** The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data). **Recommendation** It is recommended to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

No Website Firewall	**Risk Rating** Medium **Analysis** This domain has no firewall for their website. Any connections done with user will not be sterilized of any suspicious activities. **Recommendation** Install the firewall for the website in order to have another layer of protection and also in order to monitor and sterilize any connection that is suspicious.

4. References

a) Who.Is Information

- ✓ fixi.com.my

b) Sucuri Website Scanners

c) Website Vulnerability Scanner

d) Nmap Scans (Kali Linux)

- ✓ Stealth Scans
- ✓ Operating System Type Scan

```
root@kali:~# nmap -O sabah.uitm.edu.my

Starting Nmap 6.25 ( http://nmap.org ) at 2018-05-17 09:17 UTC
Nmap scan report for sabah.uitm.edu.my (202.58.80.225)
Host is up (0.043s latency).
Not shown: 984 filtered ports
PORT      STATE  SERVICE
21/tcp    open   ftp
80/tcp    open   http
443/tcp   open   https
554/tcp   open   rtsp
1723/tcp  open   pptp
3301/tcp  closed unknown
3800/tcp  closed pwgpsi
5440/tcp  closed unknown
6129/tcp  closed unknown
6580/tcp  closed parsec-master
7435/tcp  closed unknown
8010/tcp  closed xmpp
8080/tcp  closed http-proxy
8192/tcp  closed sophos
16080/tcp closed osxwebadmin
41511/tcp closed unknown
Device type: general purpose|storage-misc
```

```
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 2.4.X (95%), Microsoft Windows 7 (95%), BlueArc e
mbedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.4 cpe:/o:microsoft:windows_7:::enterprise cp
e:/h:bluearc:titan_2100
Aggressive OS guesses: DD-WRT v24-sp2 (Linux 2.4.37) (95%), Microsoft Windows 7
Enterprise (95%), BlueArc Titan 2100 NAS device (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 186.86 seconds
```