

**REPORT ANALYSIS ON THE SECURITY OF TWO DOMAINS ASSIGNMENT**

**ITT 450**

**INFORMATION AND NETWORK SECURITY**

**INSTRUCTOR: SIR MOHD ALI**

**Group: M3CS2453A**

**Name: Adzli Firdaus Bin Adha Fikris**

**Student ID: 2017116905**

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| No. | Title | Page |
| 1.0 | Summary of Findings | 3 |
|  | 1.1 Summary Findings for “puncakperdana.uitm.edu.my” | 3 |
|  | 1.2 Summary Findings for “shahalamantlers.com” | 3 |
| 2.0 | Summary of Recommendations | 4 |
|  | 2.1 Summary Recommendations for “puncakperdana.uitm.edu.my” | 4 |
|  | 2.2 Summary Recommendations for “shahalamantlers.com” | 4 |
| 3.0 | Details Findings | 5 |
|  | 3.1 Details Findings for “puncakperdana.uitm.edu.my” | 5-7 |
|  | 3.2 Details Findings for “shahalamantlers.com” | 8-11 |
| 4.0 | References | 12-22 |

**1.0 Summary of Findings**

The domains that has been chosen to carry out this assignment is “puncakperdana.uitm.edu.my” and “shahalamantlers.com”. The findings on these two domains are based on the chosen web scanners and also by using the Nmap software. Below are the results:

**1.1 Summary Findings for “puncakperdana.uitm.edu.my”**

On this domain, it is relatively secured as most of the results shown that this domain does not have many major weaknesses or vulnerabilities such as malware or injected spam. However, it is detected that this domain does not have website firewall. Besides, there are also open ports on this domain. The vulnerabilities that can be caused by these open ports will be discussed details in the “Details Findings”.

**1.2 Summary Findings for “shahalamantlers.com”**

The main findings on this domain is an outdated version of WordPress Version 4.7. This finding is found by using the Sucuri Sitecheck Web Scanner. Other than that, it is also detected that this domain does not have website firewall. Besides, by using the Nmap in Kali Linux, it is proven that this domain has several open ports which is port 21, 25, 26, 80, 1723 and 3306. Other than that, it is proven that some of the private information such as registrant and administrative contact information also is shown. These findings are detected by using “Who.is”. Further explanation will be discussed in “Details Findings”.

**2.0 Summary of Recommendations**

Based on the results that have been found, a few recommendations need to be taken in order to improve the security of those two domains and to decrease the risk for that domains to be hacked by the hackers. Below are some of the suggested recommendations that have been done.

**2.1 Summary Recommendations for “puncakperdana.uitm.edu.my”**

The main thing that need to be done is to build a firewall for the website to protects it from being attacked by hackers, viruses and worms. Besides, there are also some of the other recommendations that need to be taken such as:

* Manages the open ports properly
* Keep updating the website regularly
* Keep updating and patching the domain operating system to the latest version

**2.2 Summary Recommendations for “shahalamantlers.com”**

For this domain, it is a wise action for the admin to hide their important information on “Who.is” because attackers can use this information such as the server ip to launch an attack. Besides, there are also some of the other recommendations that need to be taken such as:

* Close the unnecessary ports
* Build a firewall for the website
* Keep updating the website regularly
* Close the unnecessary ports
* Always patching the domain operating system to the latest version

**3.0 Details Findings**

After all the results have been checked and gathered together, it is seen that the domain “puncakperdana.uitm.edu.my” is more secure than domain “shahalamantlers.com”. All of the results found is shown below, paired with any recommendations to a better performance and security if it any.

**3.1 Details Findings and Recommendations for domain “perlis.uitm.edu.my”**

Information Gained About Domain:

Website Name : <https://puncakperdana.uitm.edu.my>

Domain : puncakperdana.uitm.edu.my

Scanned IP : 202.58.80.220

Server type : Apache

Country : Malaysia

City : Shah Alam, Selangor

Open Ports : -> TCP port-21 (ftp)

-> TCP port-80 (http)

-> TCP port-443 (https)

-> TCP port-1723 (pptp)

**There Is No Website Firewall:**

|  |
| --- |
| **Risk Rating** |
| High |

**Analysis**

The online scanner results show that this domain has a total lack of a firewall for their website. It is a big risk for not put a firewall because without it, any connections done with user will not be sterilize of any suspicious activities which is most primarily done by hackers.

**Recommendation**

Install the firewall for the website in order to have another layer of protection and also to monitor and sterilize any connection that is suspicious.

**TCP Port 21-FTP Is Open:**

|  |
| --- |
| **Risk Rating** |
| Low |

**Analysis**

It cannot be deny that this port needs to be open to transfer the data from user to host. However, this port is also associated with a lot of vulnerabilities especially Trojans such as ADM worm, Back Construction, BlueFire and CC Invader.

**Recommendation**

The administrator should scan the port and also check the logs at least once a week in order to identify any anomaly that may occur due to intrusion from hackers. Closing off the port is not viable if the website is a source of data that users can download from.

**TCP Port 80-HTTP 443-HTTPS Is Open:**

|  |
| --- |
| **Risk Rating** |
| Medium |

**Analysis**

It is not recommended to open port 80 and port 443 because according to most of security experts, these two ports perform the same action but port 443 is more secure than port 80. The vulnerabilities that mostly found in port 80 is Trojans.

**Recommendation**

It is suggested that the admin open port 443 redirect every user to port 443. If port 80 had to be opened, make sure the server and website is up to date with the same thing goes for the antivirus.

**TCP Port 1723-PPTP Is Open:**

|  |
| --- |
| **Risk Rating** |
| Medium |

**Analysis**

This port is a Point-to-Point Tunneling Protocol(PPTP) which use MS-CHAPv2 to encrypt and decrypt the connection between host and users. PPTP has a number of known vulnerabilities. It is no longer considered secure, as cracking it can be brute-force in a short period of time. It is also prone to man in the middle (MITM) attacks.

**Recommendation**

The admin should use other type of tunneling or encryption method that is more secure at other ports and close this single port to avoid from being intruded by the hackers.

**3.2 Details Findings and Recommendations for domain “shahalamantlers.com”**

Information Gained About Domain:

Website Name : https:/shahalamantlers.com

Domain : shahalamantlers.com

Scanned IP : 220.158.200.81

Server type : LiteSpeed

Country : Malaysia

City : Kajang, Selangor

Open Ports : -> TCP port-21 (ftp)

-> TCP port-80 (http)

-> TCP port-443 (https)

-> TCP port-1723 (pptp)

-> TCP port-3306 (mysql)

**Site is outdated:**

|  |
| --- |
| **Risk Rating** |
| Critical |

**Analysis**

The online scanners shown that this domain is outdated with a WordPress Version 4.7. It is a dangerous risk because an attacker can find the weakness and vulnerabilities from this old version in order to launch an attack and hacked into the domain.

**Recommendation**

The admin must keep updating the website as soon as possible to avoid the domain from being accessed by the unauthorized users such as hackers.

**There Is No Website Firewall:**

|  |
| --- |
| **Risk Rating** |
| High |

**Analysis**

The online scanner results show that this domain has a total lack of a firewall for their website. It is a big risk for not put a firewall because without it, any connections done with user will not be sterilize of any suspicious activities which is most primarily done by hackers.

**Recommendation**

Install the firewall for the website in order to have another layer of protection and also to monitor and sterilize any connection that is suspicious.

**TCP Port 21-FTP Is Open:**

|  |
| --- |
| **Risk Rating** |
| Low |

**Analysis**

It cannot be deny that this port needs to be open to transfer the data from user to host. However, this port is also associated with a lot of vulnerabilities especially Trojans such as ADM worm, Back Construction, BlueFire and CC Invader.

**Recommendation**

The administrator should scan the port and also check the logs at least once a week in order to identify any anomaly that may occur due to intrusion from hackers. Closing off the port is not viable if the website is a source of data that users can download from.

**TCP Port 80-HTTP and Port 443-HTTPS Is Open:**

|  |
| --- |
| **Risk Rating** |
| Medium |

**Analysis**

It is not recommended to open port 80 and port 443 because according to most of security experts, these two ports perform the same action but port 443 is more secure than port 80. The vulnerabilities that mostly found in port 80 is Trojans.

**Recommendation**

It is suggested that the admin open port 443 redirect every users to port 443. If port 80 had to be opened, make sure the server and website is up to date with the same thing goes for the antivirus.

**TCP Port 1723-PPTP Is Open:**

|  |
| --- |
| **Risk Rating** |
| Medium |

**Analysis**

This port is a Point-to-Point Tunneling Protocol(PPTP) which use MS-CHAPv2 to encrypt and decrypt the connection between host and users. PPTP has a number of known vulnerabilities. It is no longer considered secure, as cracking it can be brute-force in a short period of time. It is also prone to man in the middle (MITM) attacks.

**Recommendation**

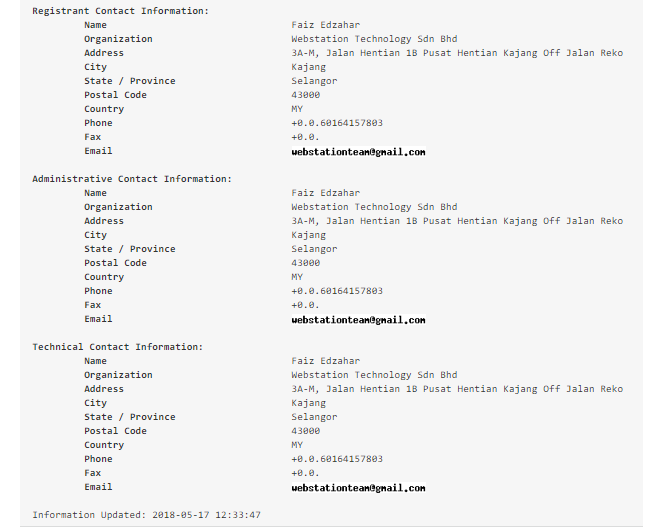
The admin should use other type of tunneling or encryption method that is more secure at other ports and close this single port to avoid from being intruded by the hackers.

**4.0 References**

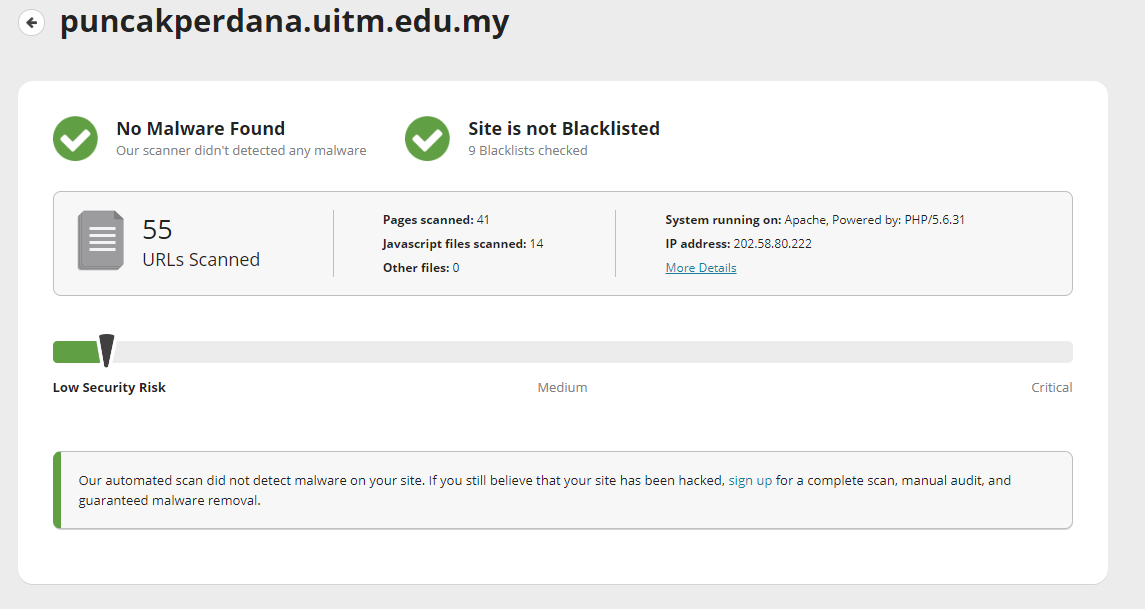
i) “Who.is” Information for “puncakperdana.uitm.edu.my”



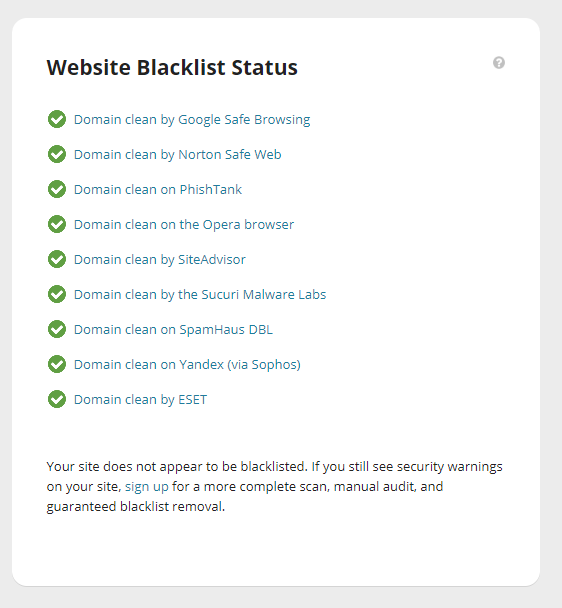
ii) “Who.is” Information for “shahalamantlers.com”



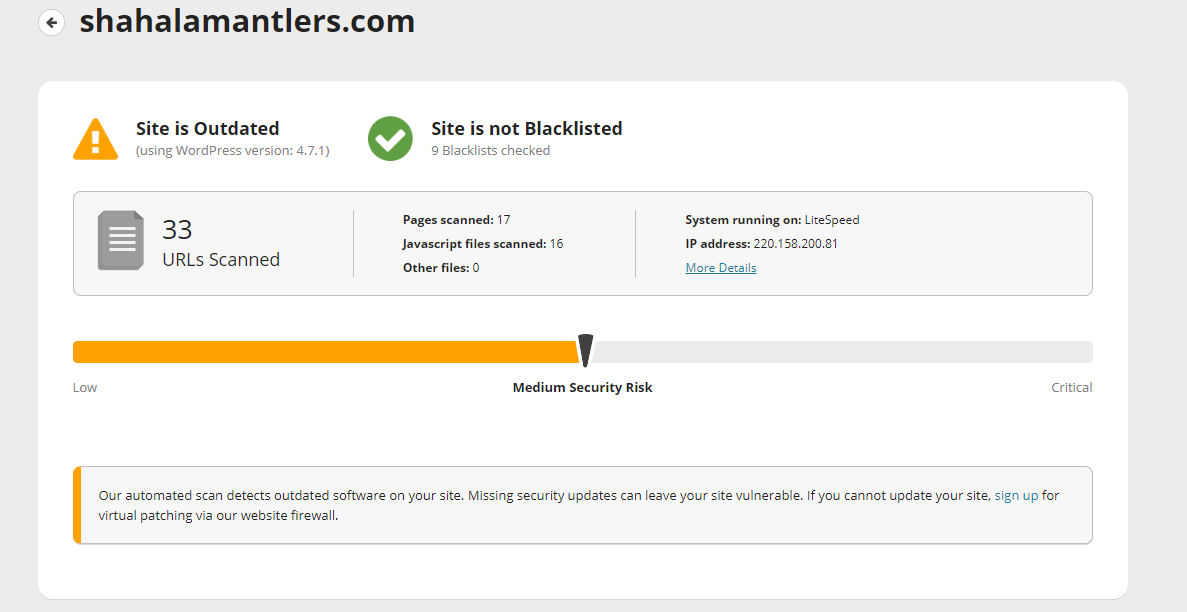
iii) Sucuri Sitecheck Web Scanner for “puncakperdana.uitm.edu.my

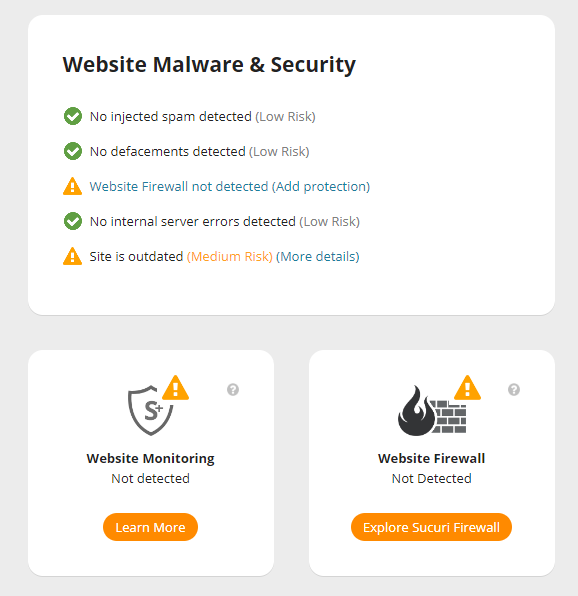


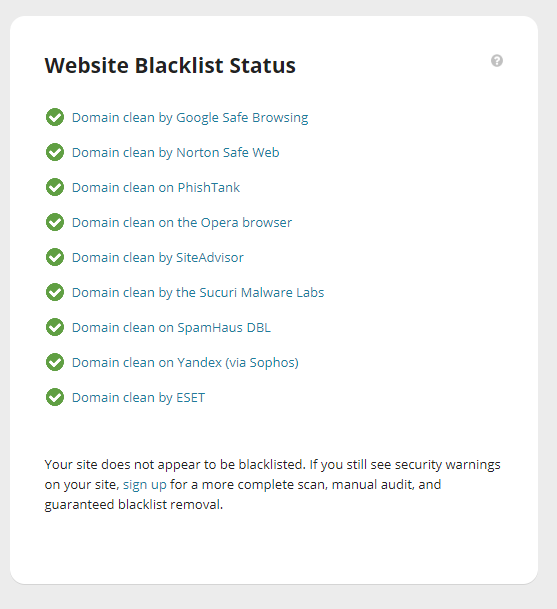




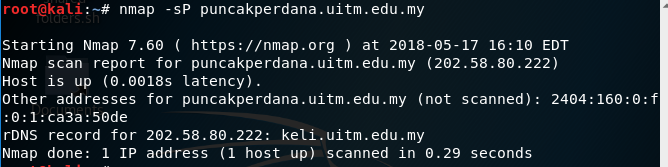
iv) Sucuri Sitecheck Web Scanner for “shahalamantlers.com”



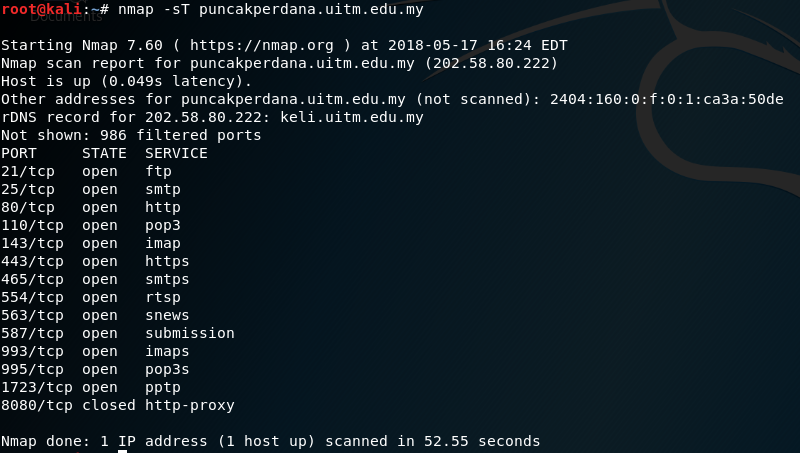




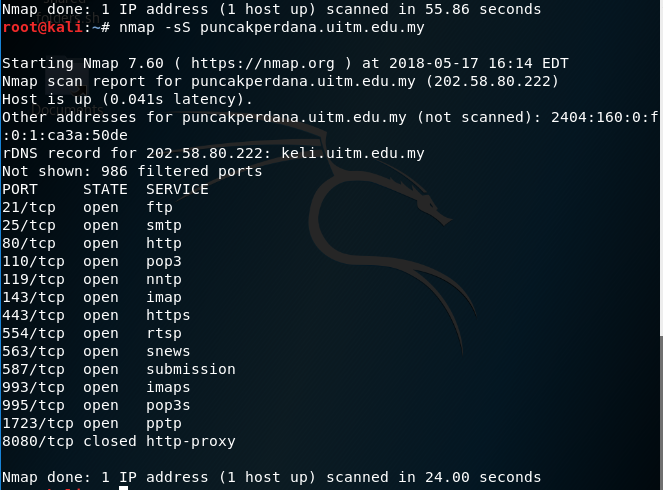
v) Nmap scanning for “puncakperdana.uitm.edu.my”



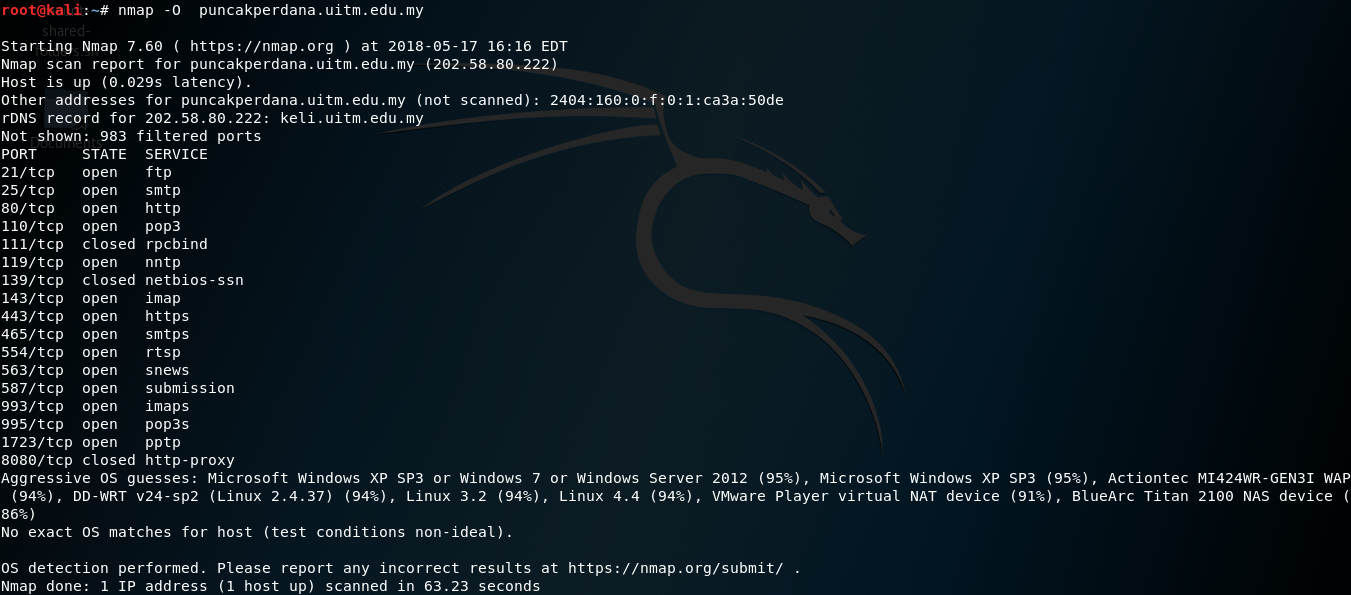
*Figure 1: nmap –sP puncakperdana.uitm.edu.my*



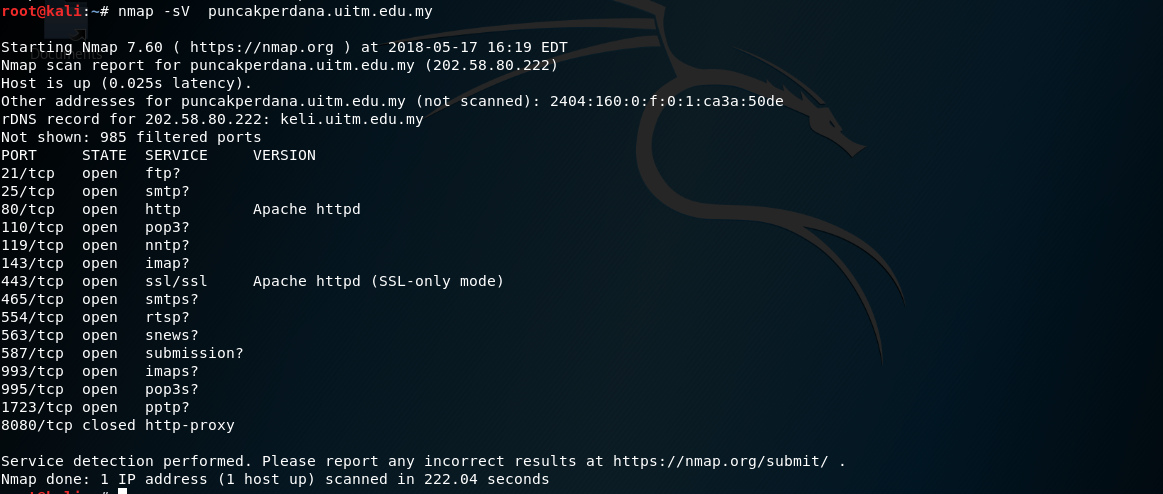
*Figure 2: nmap –sT puncakperdana.uitm.edu.my*



*Figure 3: nmap –sS puncakperdana.uitm.edu.my*

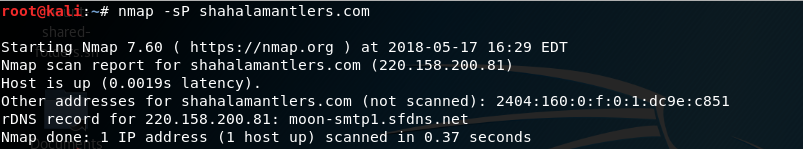


*Figure 4: nmap –O puncakperdana.uitm.edu.my*

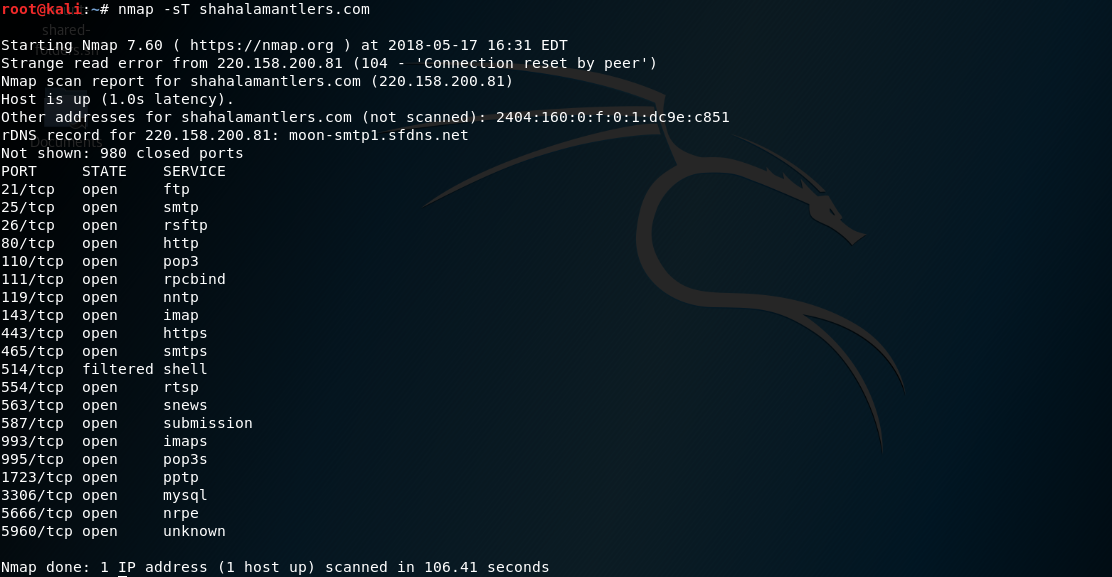


*Figure 5: nmap –sV puncakperdana.uitm.edu.my*

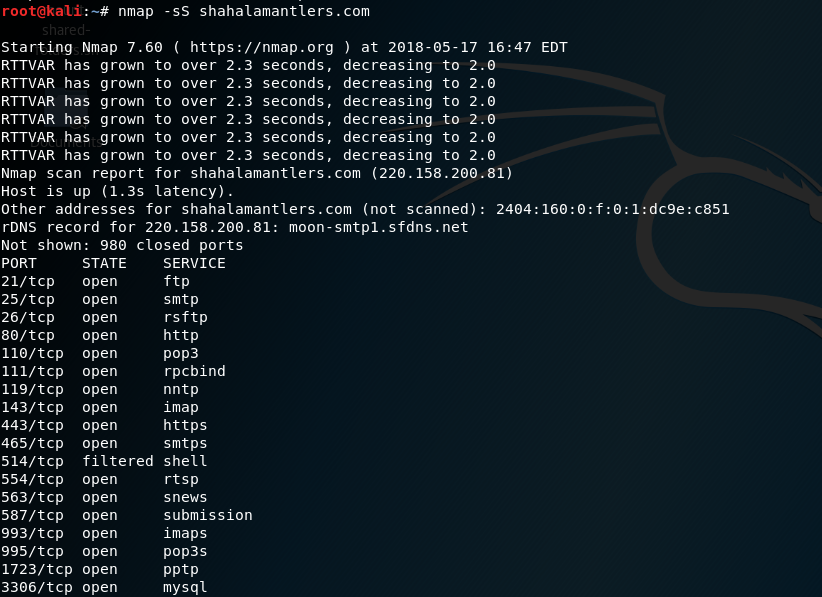
v) Nmap scanning for “shahalamantlers.com”



*Figure 6: nmap –sP shahalamantlers.com*



*Figure 7: nmap –sT shahalamantlers.com*

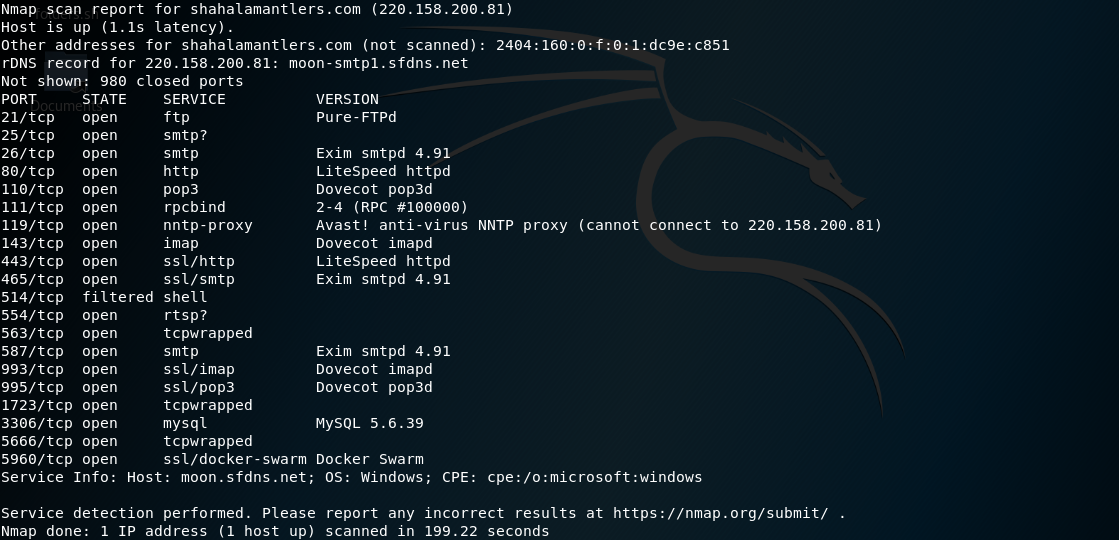


*Figure 8: nmap –sS shahalamantlers.com*



*Figure 9: nmap –O shahalamantlers.com*





*Figure 10: nmap –sV shahalamantlers.com*