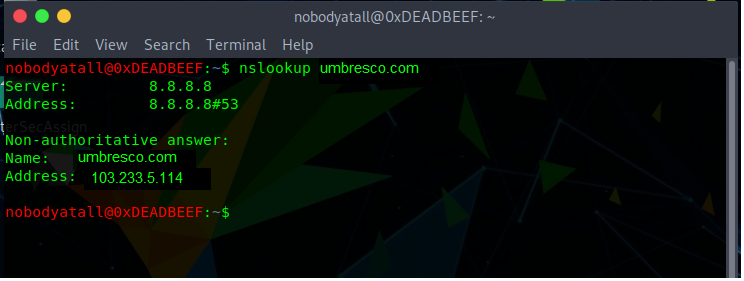
**1.4 Footprinting**

1. **NSlookup**

****

*Figure 3.1 query umbresco.com DNS record with nslookup*

So we have perform nslookup on the domain name to get the public IP address. Nslookup is a command line tool which let the network administrator to query the Domain Name Server (DNS) to gather the public IP address, or any other DNS queries from the given domain name.

In figure 3.1 shown, we have use our linux terminal with bash shell with the nslookup command line tool to query the domain name “umbresco.com”. In our case we will be using the default flag since we only need the public IP address of “umbresco.com” querying from the DNS server. So as we can see that the nslookup return the IPv4 public address of “umbresco.com”. The IPv4 public address of “umbresco.com” will be 103.233.5.114. So in our case we have now gathered the public IP address of Umbresco IT Sdn Bhd for our penetration testing and vulnerability testing that will be done later.

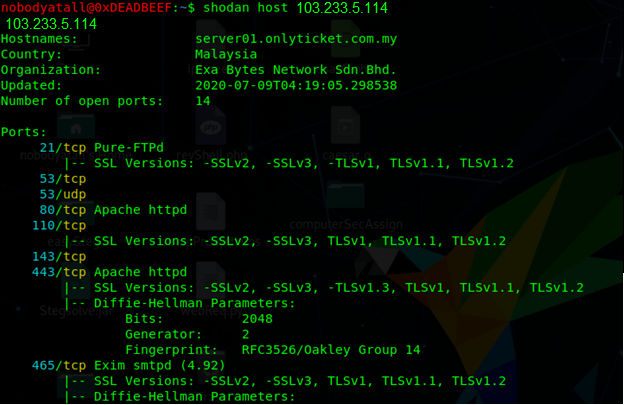
**Summary**

Tool: Linux Terminal

Method: “nslookup” command line tool

Aim: perform DNS query to gather public IP

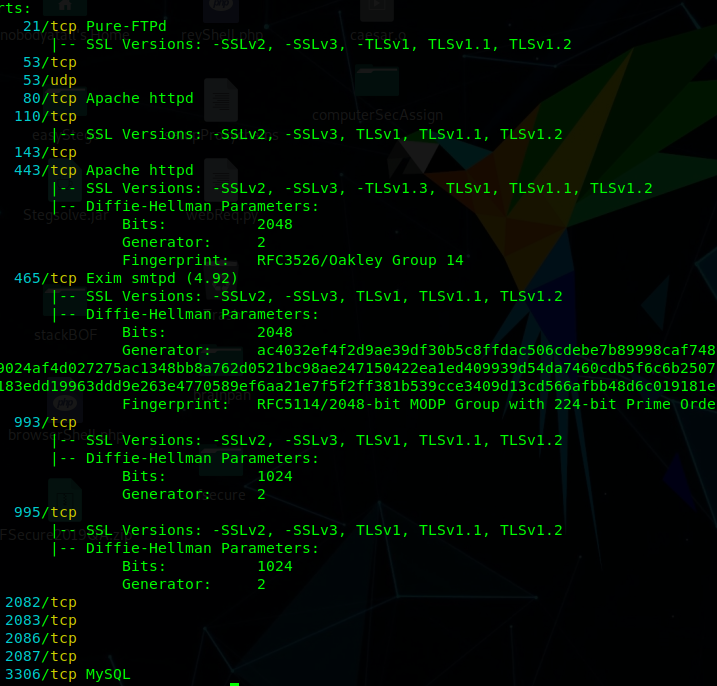
1. **Shodan**

****

*Figure 3.2.1 shodan perform port scanning of umbresco.com (public IP: 103.233.5.114)*

So we have use shodan to perform port scanning to find for any open ports and the services that it used on the port that available on umbresco.com. Shodan is a search engine that cyber security expert used to scan for devices that connected to the internet to gather information of the devices during their reconnaissance phase. Shodan have 2 version which is the web interface version which is shodan.io and the CLI version which will be the one that we will be using in our footprinting phase. Shodan will return the open ports of the public IP provided, the country the server at, the Internet Service Provider that the server subscribed, etc.

Based on the shodan result that shown Figure 3.2.1, we will notice that the location that the server hosting are based on Malaysia country. The Internet Service Provider (ISP) that the company subscribed are Exa Bytes Network Sdn. Bhd. The result did show us that it had found 14 open ports at the server.

****

*Figure 3.2.2 open ports and the services running on the port*

In Figure 3.2.2 we had found some interesting ports which will be the File Transfer Protocol (FTP) port 21, web server port 80 and 443 and the MySQL Database running on port 3306. From this information gathered, we can plan our penetration testing strategy on finding the vulnerability and attacking on these ports. Example like the web service port, we can try to enumerate on the website to find any misconfigurations, perform web directory fuzzing to find hidden directories, checking for poor user input sanitization, etc. that likely the attacker will be using to compromise the server. We also know that the backend websites codes will likely to be connected to MySQL server too, so we can utilize this part to perform SQL Injection with MySQL syntaxes. As for the FTP port, we can try to login as anonymous without entering the password to check and see whether anonymous login is available or not. If we managed to access the FTP server, then most likely we can gather more information that the system administrator left on the FTP server then.

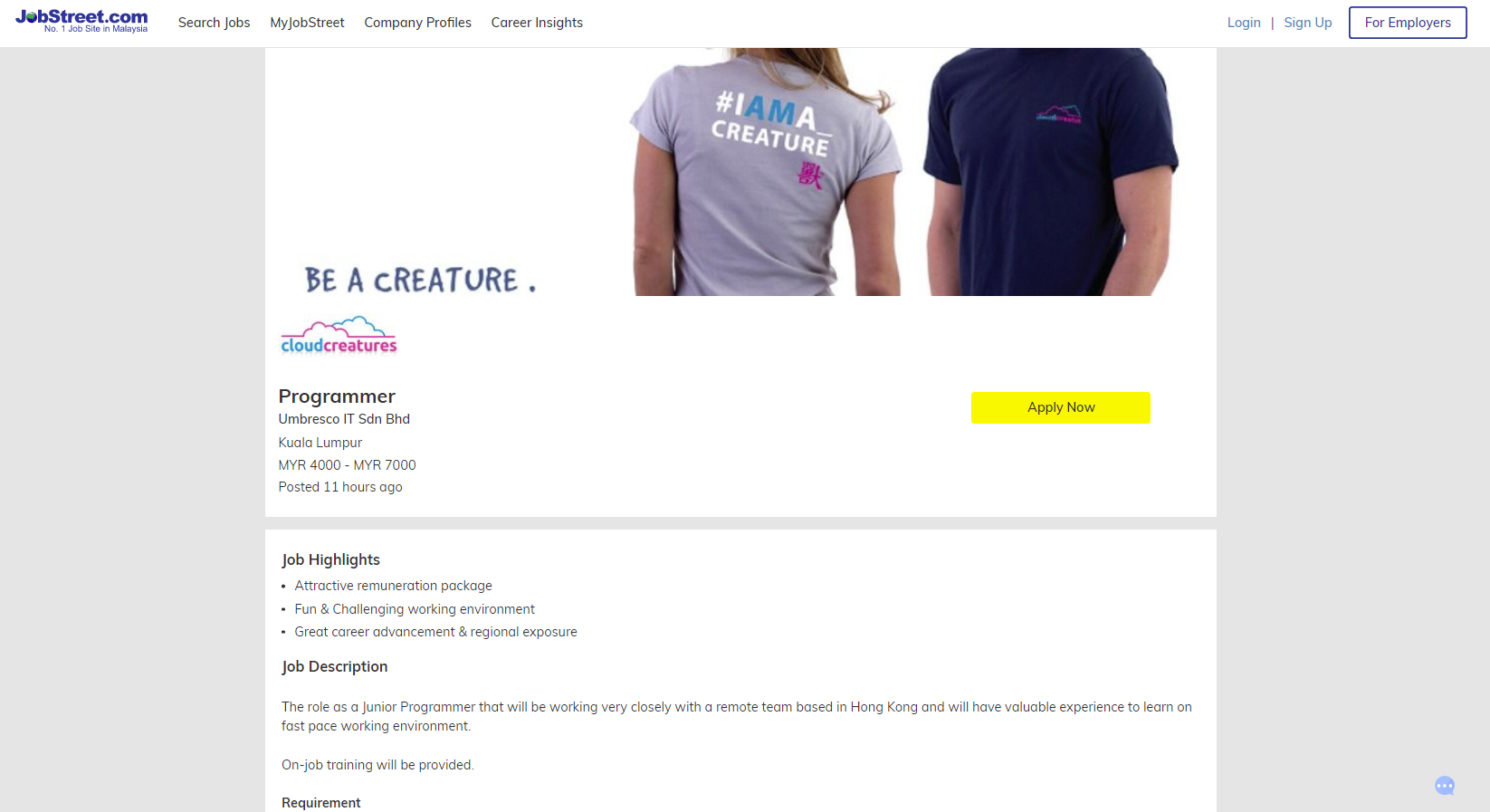
**Summary**

Tool: Linux Terminal

Method: “shodan” command line tool

Aim: gather information about the server and open ports that will be tested during the penetration testing phase to find vulnerabilities to perform attacks.

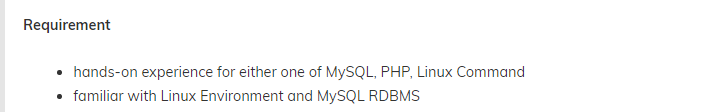
1. **Job Postings**

****

*Figure 3.3.1 Job Posting of Umbresco IT Sdn Bhd on JobStreet*

Since we know that Umbresco IT Sdn Bhd is a company in Malaysia, so we search for job posting in Malaysia JobStreet website. JobStreet is a website that user can use to find jobs online. It will provide the details that the recruiter requires the applicant to have before applying for the job.

In figure 3.3.1 shows the job posting of Umbresco IT Sdn Bhd which finding for a programmer in Kuala Lumpur. It shows that the HR posted the job post 11 hours ago which we can assume that the recruiter is posting up to date job posting with the require skills the company need currently.



*Figure 3.3.2 required skills that needed to apply for the job*

Based on figure 3.3.2, it shows that the skills that the programmer require are MySQL, PHP and Linux Command. From these results we can gather some information of what software and operating system that will be used in the company. So here we will know that the web service that hosting used PHP Programming Language to code the website. Other than that, the MySQL skill and familiar with MySQL RDBMS require will shows that the database that they are using will be MySQL database. Then the experience on Linux Command and familiar with Linux Environment will shows that the devices operating system will be running Linux operating system. With these results gathered, we will gain more information about the software and operating system that using in Umbresco IT Sdn Bhd. In this phase, identifying the software and the operating system that used we need to have IT knowledge in order to identify it when we saw the skills that needed.

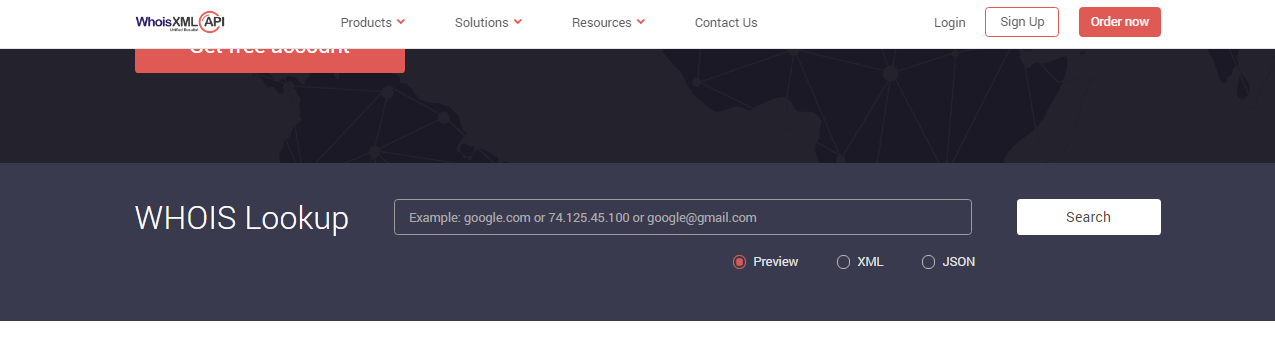
**Summary**

Tool: JobStreet website

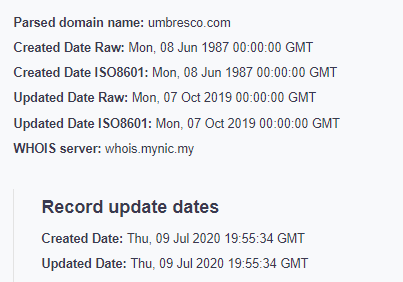
Method: IT knowledge to identify software and operating system

Aim: Find out the software and operating system that used

1. **Whois**

****

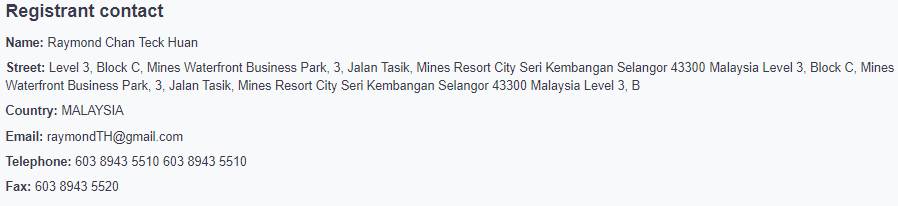
*Figure 3.4.1 looking for domain name details with whois lookup*

******

*Figure 3.4.2 umbresco.com domain name information in whois server*

Whois is a tool to gather the information of the domain name registrant that the registrant provided when they register the domain name. In figure 3.4.1 we will be using the online whois lookup tool (<https://www.whoisxmlapi.com/>) to gather the domain name registrant information in our footprinting process.

In figure 3.4.2, we gathered some domain name information of umbresco.com. It shows that the date the registrant register for the domain name is on the 8th of June 1987 12am, and the whois details of the domain name has been updated in 7th of October 2019 12am.

****

*Figure 3.4.3 umbresco.com domain name registrant details in whois server*

Based on Figure 3.4.3, we gathered some information about the registrant contact including the registrant’s name, address, country, email, telephone and fax. These information are useful for us to determine what are the people that might be in the company, the email “raymondTH” might be a possible username that used during the login process, the telephone number and the address of the company to tell us the location of the company and the contact that we can used to reach the company, country which shows that the company is a Malaysia company. This information can be used when we perform password spraying on the login page too. Like we can try with telephone number as the password, the combination of username follows by some random 4-5 digit numeric, etc.

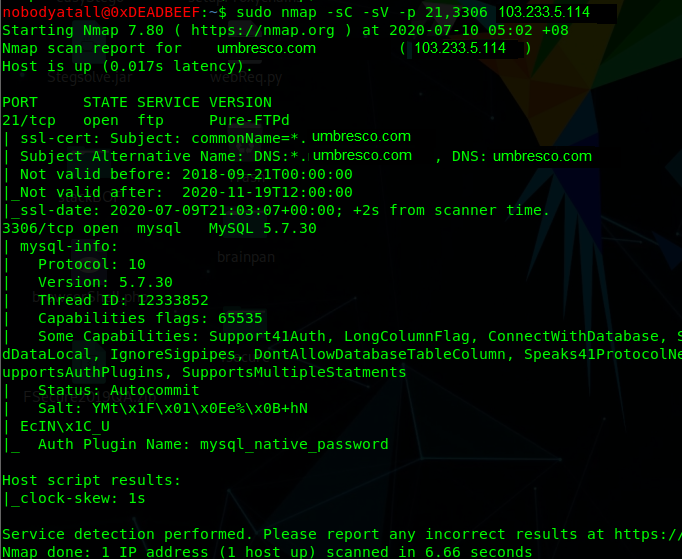
**Summary**

Tool: Internet tool

Method: Whois Server

Aim: Registrant contact and domain name information

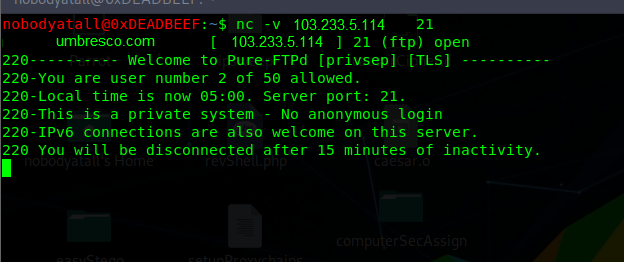
1. **Banner Grabbing (MySQL and FTP)**

****

*Figure 3.5.1 nmap banner grabbing result for MySQL and FTP server*

Banner grabbing is a technique that used to gain information about the device services that running on its open ports. In this case we will be utilizing nmap -sV flag which will show the version and the service name of the services running on the open port, and netcat to grab FTP banner.

In figure 3.5.1, we used nmap with the -sV flag set to grab the banner of mysql and ftp service. In the figure 3.5.1, it shows that the FTP server that is running are Pure-FTPd FTP server and the mysql version that running are MySQL 5.7.30. With these information we can do some research on what are the vulnerability that some cyber security experts had found previously and published the public exploits to shows as the Proof of Concept of the attack. GitHub and Exploit-db are one of the common place that we can find for public exploits. If the vulnerability have Common Vulnerabilities and Exposures (CVE) for the particular version or service then we can do research on that particular CVE to plan our strategy that needed to carry out during the penetration testing and vulnerability testing phase.

****

*Figure 3.4.2 FTP banner grabbing with netcat*

Based on figure 3.4.2 results, we use netcat to grab the FTP banner. we can see that the FTP server have show some details in their banner. Starting from the 220 line, the 1st line shows the FTP server software name. The 2nd line shows the counter of user number that are allowed to enter into the FTP server. 3rd line shows the server time. 4th line shows that anonymous login are disabled, so we would not be able to access the FTP server anonymously. 5th line shows that IPv6 connection are allow to connect into the FTP server too and the last line shows that if the user are inactive for 15minutes, it will be disconnected from the FTP server.

**Summary**

Tool: Linux Terminal

Method: Nmap and netcat banner grabber

Aim: Gather information about the software version, software name and FTP banner’s information