**Lab 4: Information Gathering**

Name: Van Linh Ha

Student ID: 116.592.171

**PART 1:**

**Table 2: Domain Name and IP Address Lookup**

|  |  |  |  |
| --- | --- | --- | --- |
| IP ADDRESS | FQDN | Point of Contact | Location |
| 129.119.70.168 | Smu.edu | info@verisign-grs.com | Dallas, Texas |
| 162.21.1.112 | Ripe.net | [abuse@ripe.net](mailto:abuse@ripe.net) | Amsterdam, NL |
| 200.74.207.19 | www.dj.com.ve | Cdn.ceo@gmail.com | Venezula |
| 70.86.89.34 | Softlayer.com | [abuse@softlayer.com](mailto:abuse@softlayer.com) | Dallas, Texas |
| 202.131.95.30 | www.hackthestack.com | Stress\_test@hotmail.com | Melbourne, Australia |
| 211.64.175.201 | qdu.edu.cn | nicadmin@qdu.edu.cn | Qingdao, China |

I was using cmd tool built in Windows to ping the IPs and whois lookup website to lookup the IP address and the location. Using website to find the domain contact information.

**How would you defend against this type of information gathering by potential attackers?**

Normally use company contact to register domain instead of using personal information. Buying subscription to make your domain become private.

**PART 2: Information Gathering**

|  |  |
| --- | --- |
| ITEM |  |
| Domain Name | www.redflagdeals.com |
| Address and phone number of corporate HQ | 111 Peter St, Suite 901, Toronto ON M5V 2H1 CA - +1.4163418950 |
| Location of Internet Presence | Canada |
| Co-location or branches | 111 Peter St, Suite 901, Toronto ON M5V 2H1 CA |
| Types of Technology | https |
| Name of CEO | Rob Laidlaw |
| Home Address of CEO | 111 Peter St, Suite 901, Toronto |
| Background of CEO | Computer Science MIT |
| CEO Alma Mater | Arizona State University |
| Job Listing | http://forums.redflagdeals.com/careers-f58/ |
| Other information | Bachelor's Degree 1983  Arizona State University |

**Part 3: Google Hacking**

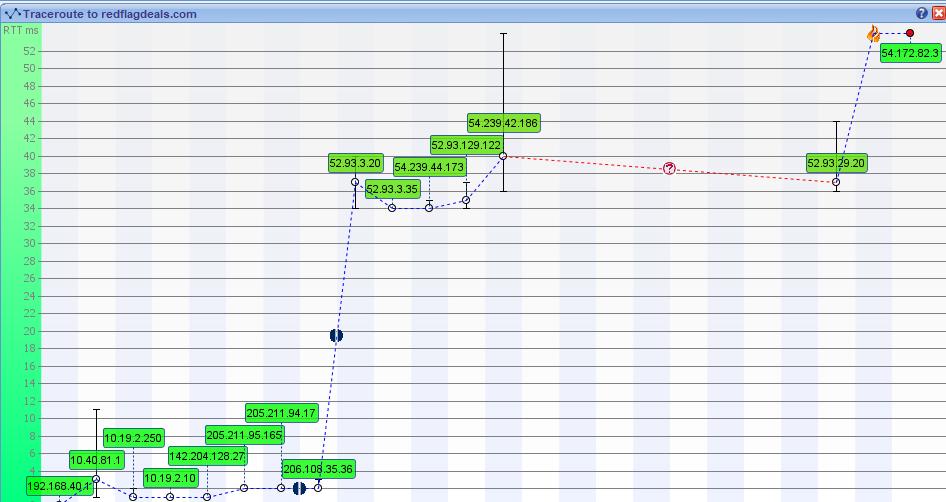
|  |  |  |
| --- | --- | --- |
| Directive | Example | Description |
| intext | intext:password filetype:xlsx | Displays hits within page text |
| intitle | intitle:"index of /backup" | Displays hits within the page title |
| inurl | inurl:dyn\_sensors.htm | Displays hits within the page URL |
| filetype | filetype:log intext:password | Return results with a specific file type (e.g., passwords within log files) |
| site | site:edu filetype:key intext:private | Show resultswithin a particular domain (e.g., RSA private keys within the EDU top-level domain) |

|  |  |  |
| --- | --- | --- |
| Directive | Example | Description |
| intitle | site:facebook.com & intext:dvdrip | Looks for dvdrip on Facebook |
| filetype | filetype:htaccess | Looks for filetype htaccess |
| ext | ext:csv intext:"password" | Looks for passwords in CSV |

**Part 4: Banner Grabbing**

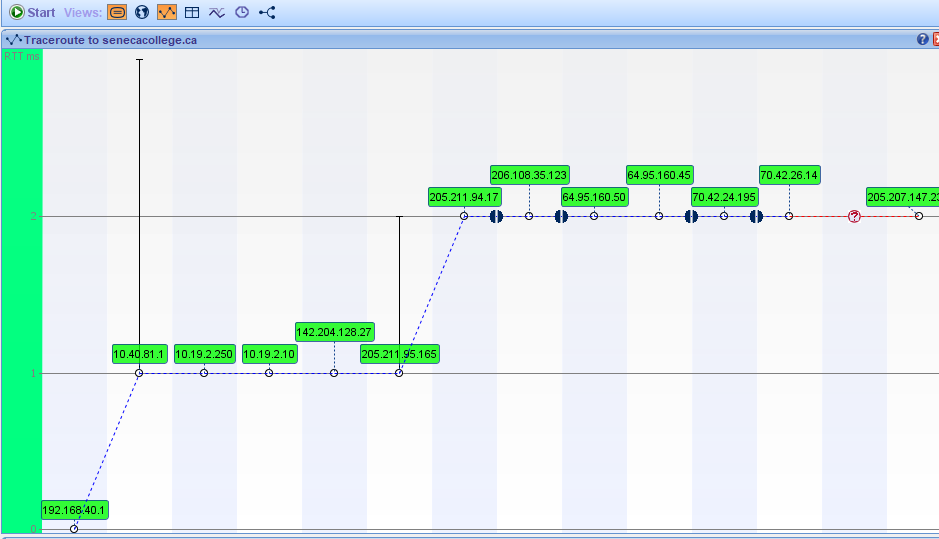
Banner Grabbing – is used to penetration the system to find all the vulnerability possibility of the system to help administrator prepare all the solution to protect the whole network. HTTP, FTP and SMTP are used on their ports 80, 21, and 25. We can use Telnet, Nmap, Zmap, and Netcat to perform Banner Grabbing.

**Part 5: Visual Route**



RedFlagDeals.com

Seneca:



Google.ca

