Lab 2: Reconnaissance Skills and Tools

Preliminaries

Refer to Lecture slides in Week 2.

Tasks

Write your answers for all questions to your lab report.

1. **Google Fu.** Use the Chrome browser on a Lab computer or your personal computer. No need to use VMs.
   1.1 Find webpages in which the title contains "zone" and the url contains "dns". Write the search string you use into your lab report.
   1.2 Visit the following website: http://www.googleguide.com/advanced_operators_reference.html . Using it as a reference, explain what the operator "allintext:" does in your lab report. Then, enter **`allintext: western Sydney ethical hacking`** into Google and check whether the results reflect what "allintext:" should do. Take a screenshot of the Google search results and include this screenshot into your lab report. Since this screenshot is not related to VM use, you don't need to include VM ID in your screenshot. This rule will apply to future encounters of such scenarios.

2. **Google Hacking.** Use the Chrome browser on a Lab computer or your personal computer. No need to use VMs.
   2.1 The search string **`inurl:"ViewerFrame?Mode="`** allows you to find public webcams on the Internet. Please try it and grab a screenshot of your search results, and include the screenshot into your lab report.
   2.2 Try the search string **`filetype:xls username password -example`** in Google. Explain in your lab report what this search string does, especially, what the operator "-" before "example" does by consulting the googleguide.com link mentioned above.

3. **Whois for domain name.** Log into your Kali VM, and start a terminal.
   3.1 Execute the command 'whois smh.com.au'. Examine the output on ‘Registrant’, which means the company that registers this domain name. Write the company name into your lab report.
   3.2 Execute the command 'whois transportnsw.info > whois.txt'. Explain what this command does in your lab report. (Hint: for the meaning of the operator ‘>’, refer to lecture 1 slides.)
   3.3 Execute the command 'grep -i registrant whois.txt'. Explain what this command does in your lab report. Especially, what does the option '-i' means?
   3.4 Based on the output of the above command, which organisation registers the domain 'transportnsw.info'?

4. **Whois for IP address.** Use the Chrome browser on a Lab computer or your personal computer. No need to use VMs.
   - 4.1 Visit the website 'www.apnic.net'. The first web page will show your IP address. Also, run an 'ipconfig' on your computer. Do you see the same IP address?
   - 4.2 If not, please explain why you see this difference in your lab report.
   - 4.3 Enter the IP address '13.8.8.8' into the top 'whois' search box in the www.apnic.net website. You'll notice that the authoritative answer comes from 'whois.arin.net'. Which “Regional Internet Registry” is this website responsible for?
   - 4.4 Also answer the following questions regarding '13.8.8.8' in your lab report:
     - a) Which company does this IP address belong to?
     - b) What's the range of IP addresses does this company own?

5. **nslookup.** Use the Windows OS on a Lab computer or your personal computer. No need to use VMs. Start a command window.
   - 5.1 Enter the interactive mode of nslookup. Write your default DNS server hostname into your lab report.
   - 5.2 Use the commands under nslookup to find out the email server IP addresses for the domain 'gmail.com'. Write your steps and results into your lab report. (hint: you need to query 'MX' record to get email server hostnames first, and then query 'A' record to obtain IP addresses.)
   - 5.3 Change the DNS server for query to '8.8.8.8'. Write the command you use for this into your lab report.
   - 5.4 Repeat 5.2. Do you get the same results? If not, include the differences in your lab report.

6. **dig.** Log into your Kali VM, and start a terminal.
   - 6.1 Run the command 'dig gmail.com mx +short'. Explain what this command does in your lab report, especially the meanings of the three arguments to 'dig'.
   - 6.2 Run the command 'dig @8.8.8.8 gmail.com mx'. Explain the meaning of the argument '@8.8.8.8' in your lab report.
   - 6.3 In the 'Answer Section' of the above output, how many email servers are returned for the domain 'gmail.com'?

Last but very important: First shutdown and then power off all your three VMs. Our school's cloud is under heavy load, as you can see your VMs may not respond to you quickly. Therefore, if you are not using them, you should have them shutdown and power off.