Shri G. S. Institute of Technology & Science, Indore

Department of Computer Engineering

Lab Assignment - I

Subject: Information & Network Security (CO 44701)
Class: BE IVth Year
Session: Jan-June 2021
Duration: 1 week

Q1. Visit to the website **https://threatmap.checkpoint.com/** and answer the following questions:

I. How many numbers of attacks are performed in all over the world when you visited this website? Attach the screenshot.
II. Write the various malware type trends in India in last 30 Days with percentage of affected organization?
III. Explain the working of threat cloud map?
IV. Write the name of any five websites which is similar to the thread cloud and attach their screenshots.

Q2. Visit to the website **https://web.archive.org/** and perform the following operation on the target website i.e. **www.sgsits.ac.in** -

I. Search the target website on wayback machine and count the number of captures with duration. Also attach the screenshot of your result.
II. Try the following filters on wayback machine for checking the vulnerabilities in the target website: **?, ?id=, .zip, readme.php, readme.txt, .csv, password, /admin/, .js, /api/, .config, msg=** etc. Also attach the screenshot for each filter and/or your result.

Q3. Visit to the website **https://www.netcraft.com** and perform the following operation on the target website: **www.sgsits.ac.in** –

I. Write the names of various domains associated with the target website.
II. Write the IP version 4 and version 4 ranges associated with the target website.
III. What is the name and location of the server of the target website?
IV. Can you detect the OS name? if yes then also write the name of the OS.

Q4. Visit to the website **https://builtwith.com** and perform the following operation on the target website**: www.sgsits.ac.in** –

I. Write the name of various technology used in designing the target website.
II. Write the name of CMS used for designing the target website.
III. Write the description about the security certificates used in the target website.
IV. Write the name of other websites or tools which can be used for website technology lookup.

Q5. Perform the following operations:

I. Setup the following virtual machine in VirtualBox or VmWare environment:
   1) Kali Linux/Parrot security
   2) Metasploitable 2
   3) Windows XP or Vista or 7

II. Assign the static IP to each of the above virtual machine. Make sure that they are also having the active internet connection.

Q6. Execute the following commands on/in the virtual machine:

I. Run the ifconfig/ipconfig/iwconfig in each of the virtual machine and write the IP, MAC and subnet mask details.
II. Run the ping command in each of the virtual machine and ping to each other.
III. Run the traceroute command from one virtual machine to another virtual machine's IP and give the explanation of the output.
IV. Run the traceroute command for the target website i.e. www.sgsits.ac.in and give the explanation of the output.
V. Run the nslookup on the target website i.e. www.sgsits.ac.in and write the name/IP of the server, mail server, IP address of the target website etc.
VI. Run the dig on the target website i.e. www.sgsits.ac.in and give the explanation of the output. Execute the dig command to get the name of the name servers and mail servers etc.
VII. Run the netstat/route command and print the routing table of each of the virtual machine.
VIII. Run the arp command and give the explanation of the output.

Q7. Execute the nmap command and answer the following questions:

I. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and give the explanation of the output.
II. Execute the nmap on target website i.e. www.sgsits.ac.in and give the explanation of the output.
III. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and display the open port in detail.
IV. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and display the OS.
V. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and display the services running on various open ports.
VI. Execute the nmap in the given IP range and display the services running at specified ports i.e. port 80, 20, 21 etc. in that IP range.

Q8. Setup the Maltego application in Kali Linux and perform the following operations:

I. Select a target website/domain and perform the required transformation like email, phone no, name etc. transformations. Generate the report for all the transformation.
II. Select a particular name/mobile number/email id and perform the email, phone number and social media account details etc. transformations. Generate the report for all the transformation.
III. List the name of any 5 general transformations which can be performed on a particular target to get the required information.

Q9. Setup the Nessus Vulnerability Scanner application in Kali Linux/any other OS and perform the following operations:

I. Perform a basic network scan on target VM i.e. Metasploitable2. Write the name of critical vulnerabilities discovered by the Nessus.
II. Perform a malware scan on target VM i.e. Windows XP, Vista or 7. Write the name of critical vulnerabilities discovered by the Nessus.

Q10. Download and setup the Damn Vulnerable Web Application(DVWA) in your OS. Also install the Burpsuite software and perform the following operations:

I. Configure the proxy setting in Burpsuite. Use the proxy tab of Burpsuite and record the HTTP request/response for a target web application i.e. DVWA, do some changes in the session id and check the result. Attach the suitable screenshot of this activity.

II. Use the Sitemap tab and generate the sitemap for target web application i.e. DVWA. Attach the suitable screenshot of this activity.

III. Use the Intruder tab and apply the brute force attack to crack the login password of target web application i.e. DVWA login page.

IV. Write the name of other tabs/tools given in the Burpsuite and also write about their uses/applications.

++++++++++++++++++++++++