CSE 345/545: Foundations to Computer Security

Assignment #2 [90 +10pts]

Due on March 28 2025, 11:59 PM

Plagiarism policies will be strictly enforced

Instructions:

- Make necessary assumptions and follow submission instructions for every question carefully.
- Keep your code efficient, make sure output matches the requirements.
- Post your queries on Google Classroom.
- Strict plagiarism checks will be conducted for each question. The assignment must be done individually

Part I – Intrusion Detection [20 points]

1. Install Snort on VM/Local machine. Get familiarized. Answer below questions with necessary justifications.

   a. What is a zero-day attack? Can Snort catch zero-day network attacks? If not, why not? If yes, how?

   b. Given a network that has 1 million connections daily where 0.1% (not 10%) are attacks. If the IDS has a true positive rate of 95%, and the probability that an alarm is an attack is 95%. What is false alarm rate?

2. Write a rule that will fire when you browse to craigslist.org or another particular website from the machine Snort is running on; it should look for any outbound TCP request to craigslist.org and alert on it.

   a. The rule you added (from the rules file)

   b. A description of how you triggered the alert

   c. The alert itself from the log file (after converting it to readable text)

Extra Credit (5pt): Write and add a snort rule for detecting VPNs; it should trigger an alert when a VPN service is running on your machine

Part II [20 points]

Kindly answer the question within 500 words

Use any web security application testing tool that serves as a middle man for intercepting browser web requests and web server replies.

1. With the tool turned on, go to your favourite Web sites and interact with them, such as logging and downloading files. Explain the kinds of information that can be captured.

2. List two vulnerabilities/possible attacks that can occur by exploiting the data obtained.

3. List two techniques (if they exist) the website has used to prevent any security exploits. (give a two-line description at max)

4. If you were a developer, what could you do to prevent misuse of data (assume the vulnerabilities you found in point 2)? Also, provide justification on why your approach would prevent the misuse of the data.

A tool you can use is OwaspZap /WebScarab /Burp Suite /Wireshark

Some tutorial links are here:

Burp Suite: https://www.youtube.com/watch?v=fVLD_eao9nQ

Webscarab; : http://yehg.net/lab/pr0js/training/webscarab.php

Wireshark: https://www.lifewire.com/wireshark-tutorial-4143298

Part III – Anonymization [20 points]

Download the ToR source code(https://www.torproject.org/download/tor/). Don't download the ToR Browser Bundle, build only ToR from Source Code. Run the binary on the command line, and configure your browser to use it. The configuration should be such that your computer should accept connections from any computer on IIITD-LAN. Access website of your choice on browser configured with ToR, intercept ToR packets on Wireshark, and provide interesting findings if any.

Bonus [5pts] for using bridges and any transport method like obs4 etc .

Part IV [30 points] - Metasploitable

Attack Machine with Metasploitable: You can use Kali Linux or Ubuntu as the attacking machine. Kali Linux comes with a suite of applications pre-installed. Unless specified, you will perform the following exercise on the attacking machine.

Report format:

1. Background of the attack (3 bullet points on why / how / outcome).
2. Steps followed to perform the attack.
3. Appropriate screenshots for each command/attack.
4. Other deliverables are specific to the questions.

Problems:

a. Use Nmap to identify the OS version of the metaspoiltable system. [5 pts]

b. List the open ports on the metaspoiltable system. What commands did you use? What are the ports used for by default? What applications did you find running on the open ports? [10 pts]

c. Metasploitable contains a backdoor on its FTP server. Exploit the same and report the following:

i. What tool(s) did you use? [2.5 pts]

ii. What command(s) did you execute? [5 pts]

iii. What is the outcome of the exploit? [2.5 pts]

d. Metaspoiltable has Mutillidae running on the VM. Mutillidae contains the top-10 vulnerabilities on OWASP. You are required to exploit the “Add blog for Anonymous” vulnerability on the “Cross Site Request Forgery (CSRF) page.” [5 pts]

Submission details:

All the codes/pdf files must be compressed in a zip file which is to be uploaded to the GC. The name of the zip file must be **<first_name>_<rollnumber>_FCS_Assignment_2.zip** (for eg. john_2022000_FCS_Assignment_2.zip). Instructions to run the code (along with the question number) must also be included (in a text file called ‘instructions.txt’). This time around, you are required to make a single pdf report for all 4 parts and must be named as: **<first_name>_<rollnumber>.pdf(for eg. john_2022000.pdf)**
Do not send any assignment by email! No email submissions will be entertained.

NO HANDWRITTEN ASSIGNMENTS SHALL BE ACCEPTED.