CY702 Project: Network Penetration Testing and Defense

	Part 1	Part 2
Due date	Dec. 14, 2023	Jan. 14, 2023
Weight	30%	25%

Overview

Saturn Security Ltd. is a provider of network security solutions. The company has a website for its employees and customers, and a private network accessible only by the employees. To prevent security breaches, which could be very damaging for the company's brand, your pentest company has been hired to perform a test on Saturn's internal network and recommend appropriate mitigation solutions.

Part I: Penetration Testing

As a penetration tester you've access only to the public website of the company, and no access to the private network.

The project will be performed using Kali as attack machine and a virtual image that mirrors as much as possible the target network. You must download the image at the following link:

The Vulberable Network.

Install it on your own machine. The installation guidelines are available on a single PDF file that will be sent separately.

Phase 1: Information gathering (10%)

1.1 Using network scanners, extract the topology information of the company's private network. Identify available hosts, and for each host, find the IP address, Operating System, running services and open ports. Ensure that you specify the exact versions. (6%)

1.2 Identify vulnerable services; briefly explain why you think these services are vulnerable. (4%)

Phase 2: Exploitation (20%)

2.1 Review the *network* scanning results and other information obtained in the previous phase, and exploit one or more of the vulnerable services to gain access to the private network. Justify the adopted strategy (6%).

2.2 After gaining access to the private network, collect the following company confidential files (14%):

(i) Company financial history statement – (3%)

(ii) Company confidential business strategy document prepared by *Frost & Sullivan* (a market research firm) – (3%)

(iii) Company online banking accounts information (accounts details and credentials) stored in a file– (4%)

(iv) Credentials for lock to the company *safe deposit box* stored in a file. (4%).

The above document must all be located and retrieved (i.e. downloaded or transferred) and the content must be recovered if necessary.

Hints:

- The safe deposit box is a physical appliance that allows the company to store safely offline, several important pieces of paper-based and electronic documents (i.e. USB drives containing secret information, contracts documents, etc.).
- Saturn has a public website which can be accessed at http://<IP_address>:8080 The site runs on port 8080, and the IP address of the server is one the machines running a web server.
- Some of the documents are stored in the network accounts, while others can be found in restricted areas in the website (i.e. login to authorized web account is required). Some important piece of information that can help in recovering some of the documents were communicated by email.
- The credentials for web accounts uses the format: *email address/password*. Saturn's employee email addresses has the format j.doe@saturn.com (for employee John Doe). E-mail accounts are password-protected and can be accessed only using a mail client (i.e. no webmail). E-mail accounts and web accounts have the same credentials. It is recommended for the project to use the *Evolution* Mail client; guidelines for configuring the *Evolution* mail client are available in the project guideline document. You can use a different mail client, but would have to figure out on your own how to configure it.
- The credentials for network accounts use the format: jdoe/password (for employee John Doe). Saturn's Security Officer has advised employees against using the same password for network and web accounts, but it is unclear whether they really follow such recommendation.
- Many account passwords are dictionary words (characters/digits), but not all. You can start using the password dictionary available **here**.

  This can help with some of the key accounts, but not all. So alternatively, you can generate your own dictionary or use some of the default dictionaries on Kali or online.

Important Notes:

- Document your answer using screenshots of your scanning activities and explain the scanning methods you used. Report both your successful and failed attempts.
- It is assumed that the attacker does not have physical access to the target network. So all access should be performed (remotely) through the attack machine (i.e. Kali). Results obtained by analyzing directly the target machine are invalid, and will be assigned **zero**.
- The project must be done by groups of two (except the only group of three people). Any collaborative or plagiarism activities will be sanctioned (i.e. Groups are not allowed to collaborate).
- Your submissions need to be typeset as a PDF file. You also need to prepare a PowerPoint presentation for the project discussion on the first lecture after the due date.
- Project reports should be submitted on or before the deadline by email at **mseifeldin@adj.aast.edu**

Part 2: Defense Strategies

In the second part of the project, you will use the attack intelligence obtained in part 1 to implement adequate defense strategy to prevent or detect similar attacks in the future. As part of the protection mechanisms, you'll setup snort IDS on the machine SaturnR and IPTables on the machine SaturnN.

Phase 1: Intrusion Detection (15%)

By reviewing the network scans, select two high risk vulnerabilities (other than password cracking or unsupported OS version), for which you can identify exploit code and execute the exploits using Metasploit.

A straightforward solution to prevent attacks based on these vulnerabilities could simply be to install more recent versions of the services. But the goal here is to go beyond such obvious solution, as variations on the attack patterns may still be successful (even after installing the upgrades).

1. Explain briefly the generic attack scenarios associated with each of these vulnerabilities (2 paragraphs maximum per vulnerability); graphical sketches (in addition of the explanations) are required (1.5%).
2. Define new Snort rules (as many as you think are necessary) to detect these attacks, and add these rules to the snort rule set. Justify the rationale for the rules. Make sure your Snort rules do not over-fit the attack scenarios (8%).

3. Configure Snort (on the **SaturnR** machine) and run it in intrusion detection mode. Execute the relevant exploit for each of (the two) vulnerabilities using your attack machine (i.e. Kali) (4%).
4. Analyze the Snort alerts log generated after each of these attacks, and discuss the results in terms of false positives and false negatives (in principle the snort configuration must successfully alerts on all suspicious packets, while not raising alerts on legitimate traffic) (1.5%).

Note: It matters that the exploit be relevant (you cannot pick one at random), and you must complete all the proper steps in Metasploit (initializing, launching, and completion). Provide screenshots documenting the different steps.

Phase 2: Intrusion Prevention (10%)

In order to protect against the above attacks, we would like to reinforce the IDS protection using IPTables firewall. The protection scope (in this phase) will be the **SaturnN** machine, i.e., the IPTables rules will be deployed on **SaturnN**. Since this part of the project focuses on protection, it is assumed that you'll have direct access to the internal network. This means you can update the firewall rules on the machine directly. The default root credentials for SaturnN will be given after Part 1.

Note that snort will run only in non-inline mode. That is, it does detection only, and does not actively prevent anything. We use IPTables for that.

1. Define the IPTables rules and provide rationale for each of the rules. You should minimize false negatives and false positives so that a legitimate client is allowed access, but a client that attempts the aforementioned attacks is blocked. (6%).
2. Test the firewall rules by executing the attacks (in metasploit, when relevant exploit exists); provide screenshots documenting the results. (3%).
3. By reviewing the scan results (obtained in project – part 1), suggest and briefly describe any additional defense strategy to protect the target systems (4 paragraphs maximum in total) (1%).