CSCI 6706 – TERM PROJECT

Given: June 30th, 2020
Due: August 4th, 2020

Objective:
To understand and experience network management in practice via "Blue team vs Red team" kind of a game!

Term Project:

During this term project, everyone will have a Kali VM and a target network with services in GNS3 (as labs 6-7) on their machines. The Kali VM will represent the attacker (Red Team) and the target network with services in GNS3 will represent the defender (Blue Team).

In this case, Blue Team represents a start-up small business for this project. Therefore, each student will need to provide a service to set up and maintain on the target network for the purpose of this project.

It is the responsibility of the student to install the software necessary depending on the service they choose as well as to back up anything they install and/or store against any system crashes. Please remember these activities are all part of network / service operations and management. Please note that to make it an interesting learning experience for everyone; each student will defend his / her service as well as perform penetration testing (attack) against his / her service.

Service: Each person will perform one of the following services on his/her Blue Team:

(i) Installation and configuration of a ***web*** service as well as generating data for such service for the enterprise.
(ii) Installation and configuration of an ***e-mail*** service as well as generating data for such service. In this case, it is up to you to decide which mail server you will install for the enterprise.
(iii) Installation and configuration of a ***File Transfer Protocol*** service as well as generating data for such service for the enterprise
(iv) Installation and configuration of a ***Secure Shell*** service as well as generating data for such service for the enterprise
(v) Or any other service of your choice, after discussing it with Dr. Zincir-Heywood.

For all the above services, ***please make sure that you define at least four accounts on your Blue Team with easy passwords*** (for the first part to play the game under weak defenses)!

Additionally, ***please define scenarios for your service to create normal traffic and normal data***. This is **very important**, otherwise the monitoring and analysis you make becomes irrelevant. Please note that creating normal traffic component affects your term project grade by 15%. Moreover, it has also a

big effect in the Part-1 and Part-2 analysis, given that any anomalous behaviour is defined relative to the normal behaviour.

Furthermore, all the log files (such as *pcap* etc.) should be stored on the corresponding machine. Please note that part of the ***project expects you to think about how to protect your own service and Red team vs Blue team environment and plan*** (in terms of what to install and configure as defense tools) accordingly! ***Remember with this project you are exploring and demonstration how to do the network operations and management in general, and 3 of the 5 components of network management in particular. These are: Configuration, Performance, and Security.***

Finally, since part of the game is learning and understanding ***penetration testing*** by doing it, you are also allowed to launch any type of penetration testing from your Red team to your Blue team. In this case, I expect you to ***perform 3 penetration testing activities***. Please note that when you put your penetration tester hat on, **the overall objective of penetration testing** is to find the vulnerabilities on the Blue Team and exploit them. Indeed, you can use any automated tool on your Red Team and/or your own scripts to search for vulnerabilities on the Blue Team. **In all the above cases**, it is each person's own responsibility to collect the relevant evidence to make a case that the objectives given above are achieved.

In summary, **the overall objective of defense** is to show how to protect a small organization with the different tools – IDS/IPS, Argus and firewalls - used and to make sure that no important data files (your assets) are lost. After the penetration activities (attacks), you should be able to analyze the log files ***(minimum case: pcap and your service's log file)*** and trace the behavior of the penetration testing activities.

It should be noted here that the first 5 days (**July 20th – July 24th**) of the Red Team vs Blue Team game, you will play the game under **No Security conditions**. In other words, firewall does not close any ports, no traffic is blocked, no IDS / IPS is run, and you do anything you can to loosen Kali's security on the Blue Team.

However, during the following 5 days (**July 27th – July 31st**), you will play the game under **as Secure as possible conditions!** So, the Firewall should have only the ports of the services set as open, all the other ports should be closed and all the other security measures such as IDS / IPS etc. should be up and running.

<u>Schedule for the main milestones of the project:</u>

Project start date: July 7th, 2020

Planning and design of Red and Blue Teams: July 7th - July 9th (By midnight)
On July 9th by midnight: Please submit a personal-PDF-report (max one page) on your service as well as explaining your plans for your Red and Blue Team environments: Please include which service will be done, how it will be done as well as the penetration testing tools you plan to use. Last but not the least, make sure that you explain how you plan to generate normal traffic / data on your Blue Team in this report. This is called as Report-1.

Installation and configuration of the software: July 10th – July 16th
During this period, set up and configure your Ted and Blue teams, all the tools and services you plan to use for this project. ***After this point, you must disable Kali VM's Internet connection, so that if mistakes happen, your attacking traffic would not leak to the Internet!***

On July 17th by midnight, please submit a personal-PDF-report (max two pages including the reference list without the code for the scripts) regarding the implementation and the installation of the software listed in the previous report for your Red and Blue Teams. In this report, explain if there are any changes, and why – compared to the Planning and Design report you submitted on July 9th. Moreover, explain your strategy for the penetration testing and defense sessions: What you will do and how the evidence will be collected etc. This is called as Report-2.

Starting from July 20th (10:00AM) until July 31st (4:00PM), the game will be played in two parts. These parts are:

(i) Starting from at 10:00AM on July 20th until 10:00AM on July 24th, you will play the game using the ***minimum firewall and defense mechanisms possible***.

(ii) Then on July 25th and 26th, you take back ups and prepare all the necessary components to harden your defences on the Blue Team for the rest of the game. This way you will play the game using harder defenses starting from July 27th at 10:00AM.

(iii) The game will finish on July 31st at 10:00AM. So, please stop all your penetration testing and defending activities at that time!

In both parts, penetration testing and defending will be in parallel. **Please remember though that you should not have any Internet connection from your VM from July 20th until August 1st.**

We will meet at our regular class and office times throughout July so we continue our lectures as well as answer any questions you might have related to the term project.

Live penetration testing and defending Presentation Time: Meeting on **July 30th starting** at 10:00AM on Teams. Each student will give a 5-minute presentation on his/her project! Each student should ***submit a PowerPoint slide deck (max 5 slides) on Brightspace***.

Game finishes: on July 31st at 10:00AM

Final Report is due: on ***August 4th, 2019 (midnight***), Submit the report on Brightspace in PDF format. Together with this report you should also submit your log files. ***PLEASE KEEP IN MIND THAT THIS IS A FIRM DEADLINE***!

The Final report (maximum 8 pages) should include an explanation of what / how you did to achieve your objectives for the term project. You should demonstrate how you achieved your objectives by the supporting data and the evidence you collected. Moreover, in your report, you should elaborate (discuss) on your experience and what you learned through this project.

In other words, your final report should include:

1. The description and details of the systems (for attacking or defending) you use
2. The results you collect (screen shots, tables, figures, graphs etc.)
3. The conclusions that you draw based on your systems and results

4. The report should focus on explaining how you get to the state of keeping it safe when you are a defender and how you penetrate a system and what exactly you do when you are a penetration tester.

GRADING CRITERIA FOR THE PROJECT:

- Report-1 and Report-2: 5% (2.5% each)
- Keeping all services running and creating normal traffic / data: 30%
- Part-1 activities and analysis (both attack and defend): 15%
- Part-2 activities and analysis (both attack and defend): 15%
- Integration of configuration, performance and security management components: 20%
- Uniqueness and creativeness: 15%

If you have any questions or need any help, please see me.

(Preferably earlier than the day before the project is due ☺)