IN715 Networks 3
Capture The Flag
Scoring Plan

Introduction

We'll conclude our exploration of network security topics by playing a game of network *Capture the Flag*. The game will run from 9:00 AM on Tueday, 4 November until 9:00 AM the following day. Your objective is to defend your network against attack and maintain the uptime of network services while at the same time attacking your classmates' networks. You will maintain a log of your acticities and findings during this exercise and your score will be based upon this log. The game will have three parts:

Preparation Prior to the day of the game you can take whatever measures you see fit to harden your network against attack. This may include installing and configuring firewalls and intrusion detection systems, configuring services to operate more securely, and updating software. Document all steps you take to earn up to 35 points for this work. If you want to add any systems to your virtual network at this time, make arrangements with the lecturer to do so.

Defence Your defensive goal is to operate the servers securely and keep the services online[1]. You will earn points by identifying network attacks, by taking steps to block network atacks, and by keeping your services accessible to legitimate use. Note that some network traffic you may observe during the game is legitimate, so blocking everything or regarding any traffic as an attack will not work.

Offence You will be provided with an IP address range in which to look for systems to attack. You may launch scans and attacks from any virtual systems in your control. Your offensive goals are to gather information about systems in the target address range and to plan and launch attacks intended to disrupt network services or to gain control of target systems.

You will score points in the game, and hence earn marks on the assignment, based on the objectives you achieve and the degree to which you achieve them.

The rules for the game are very simple. Basically, you can do anything to attack or defend systems, with two exceptions:

1. You can't do anything unlawful.

[1] The specific services you are expected to keep online will be identified in your individual competition spec.

2. You can't scan. probe, or attempt to compromise any computer other than those in the specified target ip address range.

Your scored output for this assessment will be an activity log document. You should log every offensive or defensive action you take or observation you make. Include the date and time with each log entry. Your log entries may be verified by the lecturer by inspecting the systems involved or by real time monitoring of network activity. Note that you will not receive points for anything that is not logged, even if the lecturer sees other evidence of the activity. Thorough and clearly written logs are more likely to score points than poorly written ones.

Defensive objectives

- **System and network hardening** (35 points) Awarded for actions you take to make your systems less vulnerable by configuring firewalls, shutting down unnecessary services, tightening weak passwords, etc. You may perform these activities both during and prior to the active competition period.
- **Maintaining network services** (12 points) Awarded for keeping required network services online and functioning properly during the competition period[2].
- **Identify the source IP addresses of attacks*** (2 points)
- **Identify the types of attacks*** (5 points) Examples of attack types include port scans, dictionary attacks, or code injection attacks.
- **Block attacks*** (5 points) You might do this by adding a specific firewall rule, for example.

Offensive objectives

- **Identify hosts in your target range*** (2 points) Awarded for identifying. by ip address, what hosts are online and may be subject to attack.
- **Identify open ports on target systems*** (3 points)
- **Fingerprint OS and running services on target systems*** (5 points) For example, determining that 192.168.1.10 is running Apache on port 80 and is using it to run a Wordpress site
- **Identify a known vulnerability on a target system*** (10 points) For example, you may find that the particular version of Wordrpess above has a known vulnerability.
- **Launch a specific attack*** (10 points) Awarded for attempting an attack against a known (or reasonably possible) vulnerability you have identified on a target system.

[2]Note that you may not shut down required services to reduce your vulnerability. You may shut down a service briefly to fix a problem. The shutdown must be logged.

- **Disrupt a network service*** (10 points) Awarded for an attack that renders a network service unavailable, or nearly so, for a brief period of time (i.e., long enough to be logged by nagios - about 15 minutes).
- **Penetrate a target host*** (15 points) Awarded for demonstrating that you gained access by placing a text file with a distinct string in it on a target host. Note that the defender may find and remove the file, so you should try to conceal it. If you do this, send an email to the lecturer immediately so that he can verify the attack's success.

Note that items above marked with asterisks may be awarded multiple times. For example, you score two points for every host you identify in the target range.

Bonus points

The lecturer may award bonus points at his discretion for exceptional events. For example, if a defender successfully blocks a particularly clever and well executed attack, she may be awarded bonus points.