Teacher Training

Red v Blue

Contents

1 Introduction

The concept behind this demo was to highlight to teachers both the importance of looking at cyber security exercises from a red, blue and purple team(s) perceptive as well as to showcase how a to get started with an exercise format that would make use of all 3 elements.

This exercise would have students split into 2 (or 3) groups, red or blue, with an optional third group, purple. The first thing to discuss are the key concepts that these groups or teams cover:

- Red team - This is the offensive cyber security team. They will play the role of attackers or penetration testers. Their goal is to manage to exploit vulnerabilities on the target.
- Blue team - This is the defensive cyber security team. They will play the role of a SoC (Secure Operations Centre). Their goal is to prevent or frustrate the red teams attacks and mitigate or patch the vulnerabilities which the red team are exploiting.
- Purple team (optional) - This is team can be considered optional, but have been successfully used in one implementation of this exercise by a school. They play a management role, directing the efforts of both red and blue, to make sure that neither stray beyond the confines of the exercise (only attack directed services, ports etc) and are their to help those that struggle to keep up with the pace of the exercise (provide hints in regards to ports being attacked, potential mitigation plans etc).

The ultimate goal would be to have the students work in at least the red and blue teams once, allowing them to work as both attackers and defenders. The purple team would be ideally suited to more advanced students, providing an exercise that works for multiple target student groups. Beyond exposing students to, and getting them familiar with, basic attack and defence cyber security skills,the exercise can be further expanded upon to include report writing and organisational / management skills (for the purple team).

2 Prerequisites

For the purpose of this exercise the following resource will need to be made available:

- Attack machine(s) - This can be a Virtual Machine (VM) or a dedicated machine (or a VM on a dedicated machine) - It should have sufficient software to facilitate the red teams efforts to enumerate, attack and exploit vulnerabilities on the target machine. We recommend either Kali or ParrotOS, both of which come pre-loaded with penetration testing aimed software and can be run inside VMs.
- Target machine(s) - This will **need** to be a VM as it will be under active attack and exploit by the red team. We recommend Metasploitable - Either 2 (Linux) or 3 (Windows). These are purposefully vulnerable machine, designed as entry level platforms for attacking. They come with multiple open ports and services which can be exploited, as well as multiple, pre-existing, online guides on how to both attack and harden (defend) them[1]
- Monitoring machine(s) - These can be standard Windows or Debian machines, as long as tey have at leats got the ability to monitor traffic on them (tools such as Wireshark). The blue and / or purple team would use these teams to monitor network traffic and try to identify enumeration of ports by the red team, as well as attacks in progress. They can then use this information to head of attacks or identify ports and protocols under attack (and therefore need securing).
- Blue attack machine(s) (Optional) - It is also feasible to have at least one of these machines be the same as or similar to the red team attacking machines. This would allow the blue (or purple) team to carry out ”in house” attacks against the target to try and head of the red team. This means that both the blue and red team are able to carry out offensive cyber security exercises in tandem and is representative of real world working practices (in house penetration testing, security audits etc).

[1] https://akvilekiskis.com/work/metasploitable/index.html

3 Implementation example

Here we will break down an example setup, covering student splits, example tasks and allocation of points for both teams.

If we assume a group of 20 students, we would have 8 each on the red and blue teams and 4 on the purple team. This is under the assumption that the 4 purple students are of the same year / skill group as the others but more advanced. However the same could apply if it was 16 students from 1 group and 4 from another.

We will not cover the setup of the machines as this will differ depending on the network and resources. We assume that all machines (attacking, target and monitoring) are on the same closed network, with no external internet access.

3.1 Setup - Pre exercise

We advise teachers (and / or purple team members) setup the target and at least one attacking and monitoring machine in advance to ensure that they can scan and attack the machine with no issues, as well as making sure that the traffic is visible on the monitoring machine.

It will also allow the open services and ports to be known in advance. This can then be used to collect information on them (using open source guides here if needed) and to also categorise services or ports into those that are going to be used in the first or second run of the exercise (see *Exercise - Round 2*, for more details). Once the network setup has been tested and the services identified and grouped the last thing to do would be to brief the teams.

The red team would be told that they are attacking, given the following information:

- The target IP
- The ports and protocols they are allowed to attack
- That the blue team will be working to stop them

The blue team would be told that they are defending, given the following information:

- The target IP
- The ports and protocols they are red team are allowed to attack / they need to focus on
- That the red team will be attacking and they need to stop them
- Login credentials for the target machine so they can access the machine to patch / mitigate the attacks

- That they will have access to monitor machines (optionally also their own attacking machines)

The purple team would be told that they are managing both teams, given the same information as both red *and* blue team, as well as, who is on what team and any appropriate material for attacking or defending (e.g. attacking or defending guides, such as the one linked above).

This information can be given in advance of the exercise and could then be used as a lead in to lessons that will ultimately build up to it, such as network monitoring (which will be utilised during the exercise).

3.2 Red team - During exercise

During the exercise the read team will seek to identify the open and vulnerable services on the target machine, using tools such as nmap:

INSERT EXAMPLE SCREENSHOT HERE

Once they have identified the open ports they will need to look at potential attacks or exploits. Assuming no internet access this can be through tolls pre-build on the attack machine(s), such as searchsploit, or through material made available to them by the teacher(s) or purple team. This can be through direct instruction (port x can be exploited by doing...) or by including the exploits in a larger corpus of material that is made available to them so that they have to research it themselves.

Assuming they have identified both the vulnerability and exploit they would then seek to actively exploit it and gain access to the target and provide evidence of their exploit, this can be screenshots of by simply making a teacher or purple team member aware and showing a live demo. AT this point the red team (or individual member) would be given a point or points.

INSERT EXAMPLE SCREENSHOT HERE

From here there are multiple options depending on the scope and scale of the exercise, that member of the red team may then have to do a write up (taking them out of the active exploit group, giving others a chance if resources are limited) or they may simply then be free to carry on searching for more exploits / points.

3.3 Blue team - During exercise

The blue team should either be directly monitoring the network traffic on the target or be in contact with a purple team member who is. If they identify an increase in traffic (or the purple team advise them of it) they should try and identify the port(s) / service(s) the traffic is aimed at and if possible the nature of the traffic (enumeration, under attack / exploit, brute force attempt, etc). Correctly identifying the traffic could be rewarded with points.

INSERT EXAMPLE SCREENSHOT HERE

If a service is under attack the blue should attempt to identify the attack and also mitigate it - As with the above we assume no internet access, so they can either be directly instructed or need to carry out research using material provided to them. If they manage to mitigate / patch an issue *before* the red team exploit it, they should get more points (and vice versa).

INSERT EXAMPLE SCREENSHOT HERE

If the patch is applied after the attack then red team should seek to validate the fix (re-try the original attack)

under the direction of the purple team. As with the red team there is then scope to pull that member of the blue team from the ”hot seat”, resource dependent, getting them to write up the attack and defence, while giving others a chance to do the more active roles.

3.4 Purple team - During exercise

The purple team should be able to monitor both the network traffic and the activity of the red and blue team. Their main job is to ensure that no team is too far ahead. For example that the red team are not able to actively exploit all of the target ports and protocols before the blue team is even aware of what is happening. Or that the blue team don’t start locking them out of every service / blocking their IPs before they have a chance to do anything.

This should be managed by providing hints on traffic and red team activity to the blue team and by ensure that the red team are made aware of some of the open and exploitable ports on the target.

Purple team are also in charge of managing and keeping track of the point allocations as well as any other tasks (such as write ups etc).

3.5 Exercise - Round 2

We would advise that this exercise should be run at least twice - Swapping the red and blue team members round. This will give each student a chance to experience both roles, it can also allow additional students to gain experience working as purple team members.

As such we advise (if using something like metasploitable) that open services and ports are split into two groups, with 1 group used per run of the exercise.

INSERT NMAP SCAN + TABLE BREAKDOWN HERE

This ensures that students are attacking and defending new ports and services and aren’t quickly able to defend or attack known services from the last round.

4 Comments

The ultimate management of this exercise will be dependent on several factors, such as:

- Resource available
- Student abilities
- Time available (prep, lesson plan, implementation, etc)

These notes are here as a guide and should not be considered as strict rules. If some of the concepts covered within here seem suitable, but not all, or the idea of breaking this exercise down into multiple, smaller component lessons and parts is deemed more suitable then we encourage you to make these choices. Ultimately the delivery of the ideas behind this exercise and how best to manage it will be a decision that is best left up to each teacher and / or institution.


UWE
Bristol
University
of the
West of
England