RED-BLUE TEAM EXERCISE

BLUE TEAM GET A HIGH MARK AND END THE GAME!!!

INTRODUCTION

Red-blue team exercises offer a simulated approach to uncover vulnerabilities effectively.

- Red team: offensive side
- Blue team: defensive side

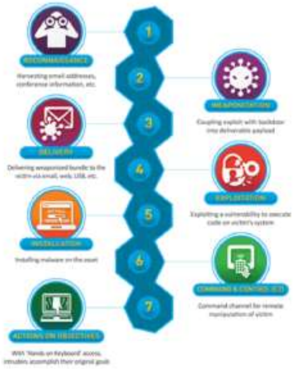
There is a playbook about the marks deduction and addition related to the attack and defense.

OBJECTIVE

In this exercise, the security of 3 critical IT systems in one of the HKSAR Government departments will be examined and represented by the mark.

METHODOLOGY

The following cyber kill chain could be a good reference for the attack path when establishing the strategy.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With "Hands on Keyboard" access, intruders accomplish their original goals

Moreover, the incident response team would be divided into L1 and L2.

- L1: monitor some simple HTTP requests and other network traffic
- L2: verify the findings of L1

KEY FINDINGS

The client's blue team received a higher mark than the initial mark, showing the success of defending.

1 critical vulnerability: **misconfiguration of the Spring Boot**

Numerous sensitive actuator endpoints could be accessed:

1. env
2. heapdump
3. mapping
4. beans

ANALYSIS

The domain is believed to be too narrow, causing the defense to become easy. Most of the vulnerability may be hidden due to the limited scope.

CONCLUSION

This red-blue team exercise shows that the blue team and IT system can detect and respond to the attack appropriately.

Recommendation: broaden the scope to examine the security of more systems in future exercises.