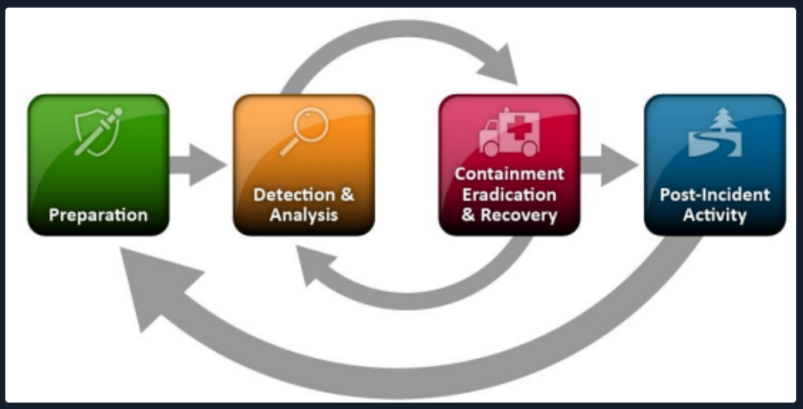
Incident Handling Process Overview

Now that we are familiar with the cyber kill chain and its stages, we can better predict/anticipate next steps in an attack and also suggest appropriate measures against them.

Just like the cyber kill chain, there are different stages, when responding to an incident, defined as the `incident handling process`. The `incident handling process` defines a capability for organizations to prepare, detect, and respond to malicious events. Note that this process is suited for responding to IT security events, but its stages do not correspond to the stages of the cyber kill chain in a one-to-one manner.

As defined by NIST, the incident handling process consists of the following four (4) distinct stages:



Incident handlers spend most of their time in the first two stages, `preparation` and `detection & analysis`. This is where we spend a lot of time improving ourselves and looking for the next malicious event. When a malicious event is detected, we then move on to the next stage and respond to the event `(but there should always be resources operating on the first two stages, so that there is no disruption of preparation and detection capabilities)`. As you can see in the image, the process is not linear but cyclic. The main point to understand at this point is that as new evidence is discovered, the next steps may change as well. It is vital to ensure that you don't skip steps in the process and that you complete a step before moving onto the next one. For example, if you discover ten infected machines, you should certainly not proceed with containing just five of them and starting eradication while the remaining five stay in an infected state. Such an approach can be ineffective because, at the bare minimum, you are notifying an attacker that you have discovered them and that you are hunting them down, which, as you could imagine, can have unpredictable consequences.

So, incident handling has two main activities, which are `investigating` and `recovering`. The investigation aims to:

- `Discover the initial 'patient zero' victim and create an (ongoing if still active) incident timeline`
- `Determine what tools and malware the adversary used`
- `Document the compromised systems and what the adversary has done`

Following the investigation, the recovery activity involves creating and implementing a recovery plan. When the plan is implemented, the business should resume normal business operations, if the incident caused any disruptions.

When an incident is fully handled, a report is issued that details the cause and cost of the incident. Additionally, "lessons learned" activities are performed, among others, to understand what the organization should do to prevent incidents of similar type from occurring again.

Let us now walk you through all stages of the `incident handling process`.

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

+1 True or False: Incident handling contains two main activities. These are investigating and reporting.

? Go to Questions

Table of Contents

Introduction

Incident Handling

Cyber Kill Chain

The Incident Handling Process

Incident Handling Process Overview

Preparation Stage (Part 1)

Preparation Stage (Part 2)

Detection & Analysis Stage (Part 1)

Detection & Analysis Stage (Part 2)

Containment, Eradication, & Recovery Stage

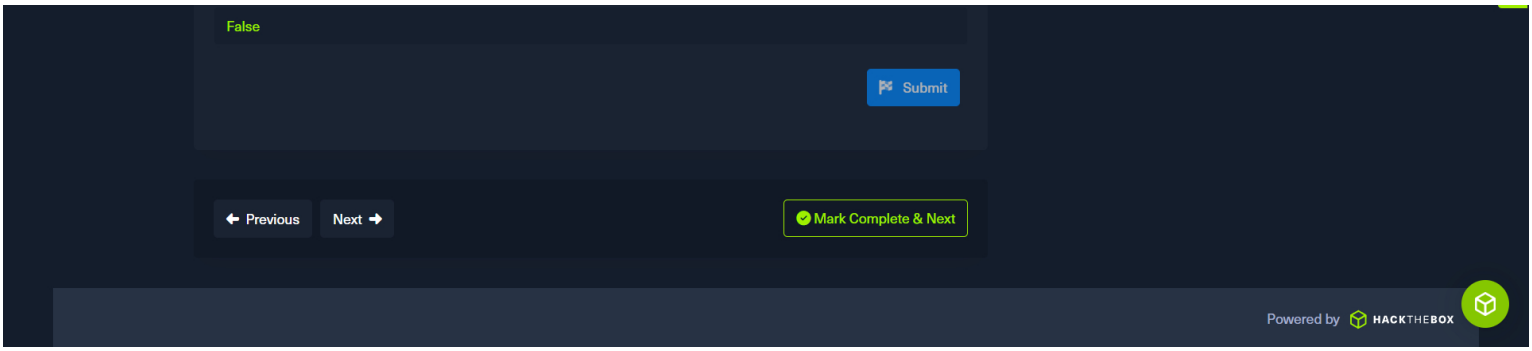
Post-Incident Activity Stage

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left


False
Submit
Previous
Next
Mark Complete & Next
Powered by HACKTHEBOX