Labs - Incident Handling Process

Introduction

Cyber Kill Chain

Question

- In which stage of the cyber kill chain is malware developed?
  -> The weaponize stage.

Incident Handling Process Overview

Question

- True or False: Incident handling contains two main activities. These are investigating and reporting.
  -> False, Incident handling contains four activities in a cyclic manner, preparation, analysis, containment eradication & recovery and post-incident activity.

Preparation Stage (Part 1)

Question

- What should we have prepared and always ready to 'grab and go'?
  -> An Jump bag, we need to always have all the tools required ready to 'grab and go'.
- True or False: Using baselines, we can discover deviations from the golden image, which aids us in discovering suspicious or unwanted changes to the configuration.
  -> True, we can compare and observe the difference made in configuration (e.g. attacks might enable restricted admin mode to use rdp through adding the `DisabledRestrictedAdmin` registry key `HKLM\System\CurrentControlSet\Control\Lsa`)

Question

- What can we use to block phishing emails pretending to originate from our mail server?
  -> We can use tools like DMARC to block phishing emails pretending to originate from

our email server, which can also be extended to domains we do not own if extensive testing has been done.

- True or False: "Summer2021!" is a complex password.
  -> True, it is an complex password yet a weak one, as it often appears on common wordlists or mutations of common wordlists that can then be used to perform a password attack.

Detection & Analysis Stage (Part 1)

Question

- True or False: Can a third party vendor be a source of detecting a compromise?
  -> True, for example, EDR products like crowdstrike are effective programs that performs detection at the endpoint level.

Detection & Analysis Stage (Part 2)

Question

- During an investigation, we discovered a malicious file with an MD5 hash value of 'b40f6b2c167239519fcfb2028ab2524a'. How do we usually call such a hash value in investigations? Answer format: Abbreviation
  -> We would call it an IOC (indicator of promise), as it represents aspect of the malware that caused the incident.

Containment, Eradication, & Recovery Stage

Question

- True or False: Patching a system is considered a short term containment.
  -> False, patching a system requires time and is usually considered as a long-term containment which improves the overall security posture of the company.

Post-Incident Activity Stage

Question

- True or False: We should train junior team members as part of these post-incident activities.

-> True, it showcases how the incident were handled by more experienced members and the juniors could learn from it.