Incident Handling Process:

Link to challenge: https://academy.hackthebox.com/module/148/

(log in required)

Class: Tier I | Fundamental| General

Introduction

Cyber Kill Chain:

Question: In which stage of the cyber kill chain is malware developed?

Answer: weaponize

Method: according the module, in weaponize stage the malware for initial access is developed.

The Incident Handling Process

Incident Handling Process Overview:

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

Answer: False

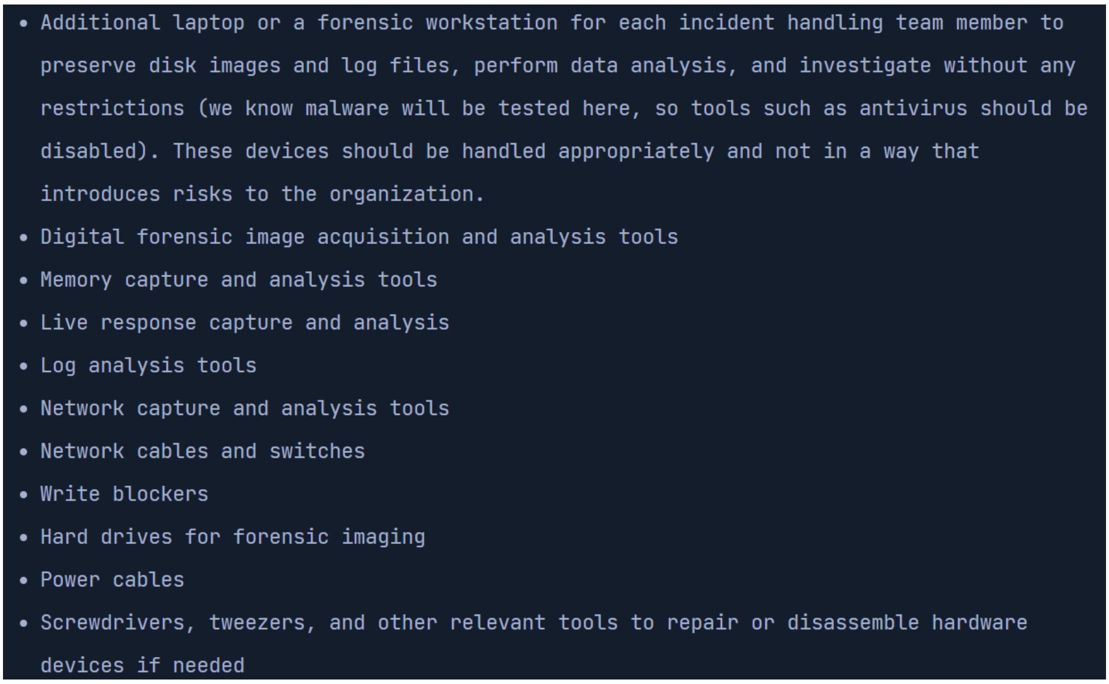
Method: In practice, there are 4 stages to incident handling: Preparation, Detection & Analysis; Containment, Eradication & Recovery; Post-Incident Activity

Preparation Stage (Part 1):

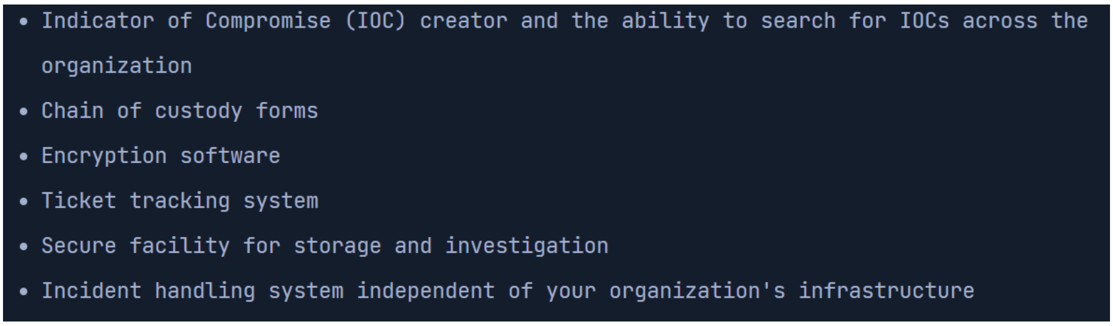
Question: What should we have prepared and always ready to 'grab and go'?

Answer: jump bag

Method: jump bag is a collection of various tools that are used for incident response, which include and not limited to:



- Additional laptop or a forensic workstation for each incident handling team member to preserve disk images and log files, perform data analysis, and investigate without any restrictions (we know malware will be tested here, so tools such as antivirus should be disabled). These devices should be handled appropriately and not in a way that introduces risks to the organization.
- Digital forensic image acquisition and analysis tools
- Memory capture and analysis tools
- Live response capture and analysis
- Log analysis tools
- Network capture and analysis tools
- Network cables and switches
- Write blockers
- Hard drives for forensic imaging
- Power cables
- Screwdrivers, tweezers, and other relevant tools to repair or disassemble hardware devices if needed



- Indicator of Compromise (IOC) creator and the ability to search for IOCs across the organization
- Chain of custody forms
- Encryption software
- Ticket tracking system
- Secure facility for storage and investigation
- Incident handling system independent of your organization's infrastructure

Question: 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.

Answer: True

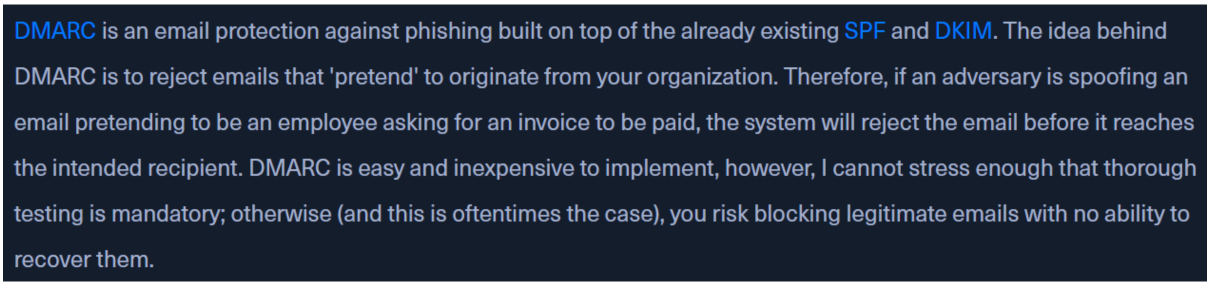
Method: Golden Image is a copy of a reference computer's virtual or hard disk drive and its contents. When we know that as baseline, we can discover any deviations from the golden image.

Preparation Stage (Part 2):

Question: What can we use to block phishing emails pretending to originate from our mail server?

Answer: DMARC

Method:



DMARC is an email protection against phishing built on top of the already existing SPF and DKIM. The idea behind DMARC is to reject emails that 'pretend' to originate from your organization. Therefore, if an adversary is spoofing an email pretending to be an employee asking for an invoice to be paid, the system will reject the email before it reaches the intended recipient. DMARC is easy and inexpensive to implement, however, I cannot stress enough that thorough testing is mandatory; otherwise (and this is oftentimes the case), you risk blocking legitimate emails with no ability to recover them.

Question: True or False: "Summer2021!" is a complex password.

Answer: True

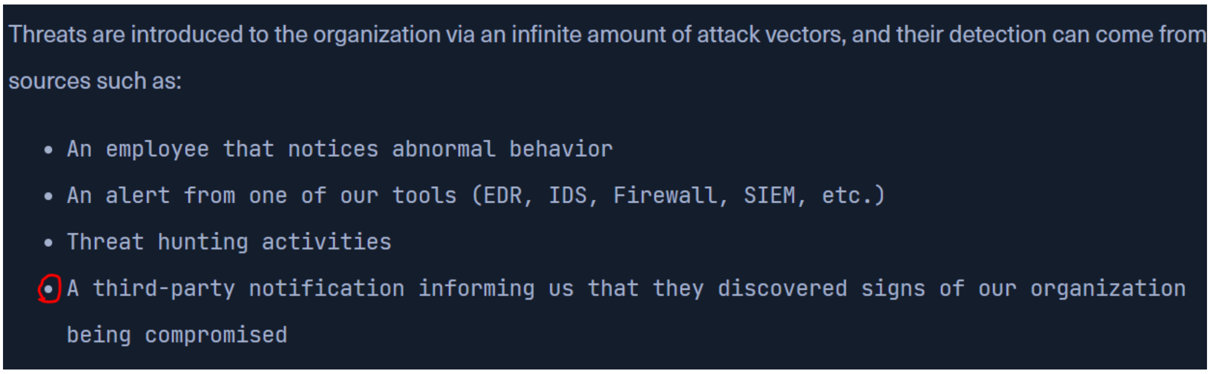
Method: the official module answer is True but I disagree, “summer2021!” is not complex enough as it is comprised of a common word ‘summer’, a common recent year ‘2021’ and common symbol ‘!’ (which os the often first to be guessed as it is shift+1 in the keyboard

Detection & Analysis Stage (Part 1):

Question: True or False: Can a third party vendor be a source of detecting a compromise?

Answer: True

Method:



Threats are introduced to the organization via an infinite amount of attack vectors, and their detection can come from sources such as:

- An employee that notices abnormal behavior
- An alert from one of our tools (EDR, IDS, Firewall, SIEM, etc.)
- Threat hunting activities
- A third-party notification informing us that they discovered signs of our organization being compromised

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

Answer: IOC

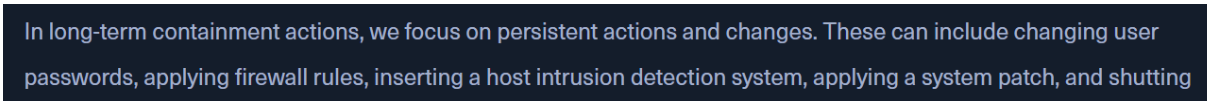
Method: IOC – indicator of compromise, is a sign that some incident has occurred. Detection of malicious file hash is regarded as such.

Containment, Eradication, & Recovery Stage:

Question: True or False: Patching a system is considered a short term containment.

Answer: False

Method:



In long-term containment actions, we focus on persistent actions and changes. These can include changing user passwords, applying firewall rules, inserting a host intrusion detection system, applying a system patch, and shutting

Patching a system is often falls under the category of taking mitigating steps to ensure a breach to our system will not re-occur.

Post-Incident Activity Stage:

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

Answer: True

Method: **“**This stage is also a great place to train new team members by showing them how the incident was handled by more experienced colleagues.**”**