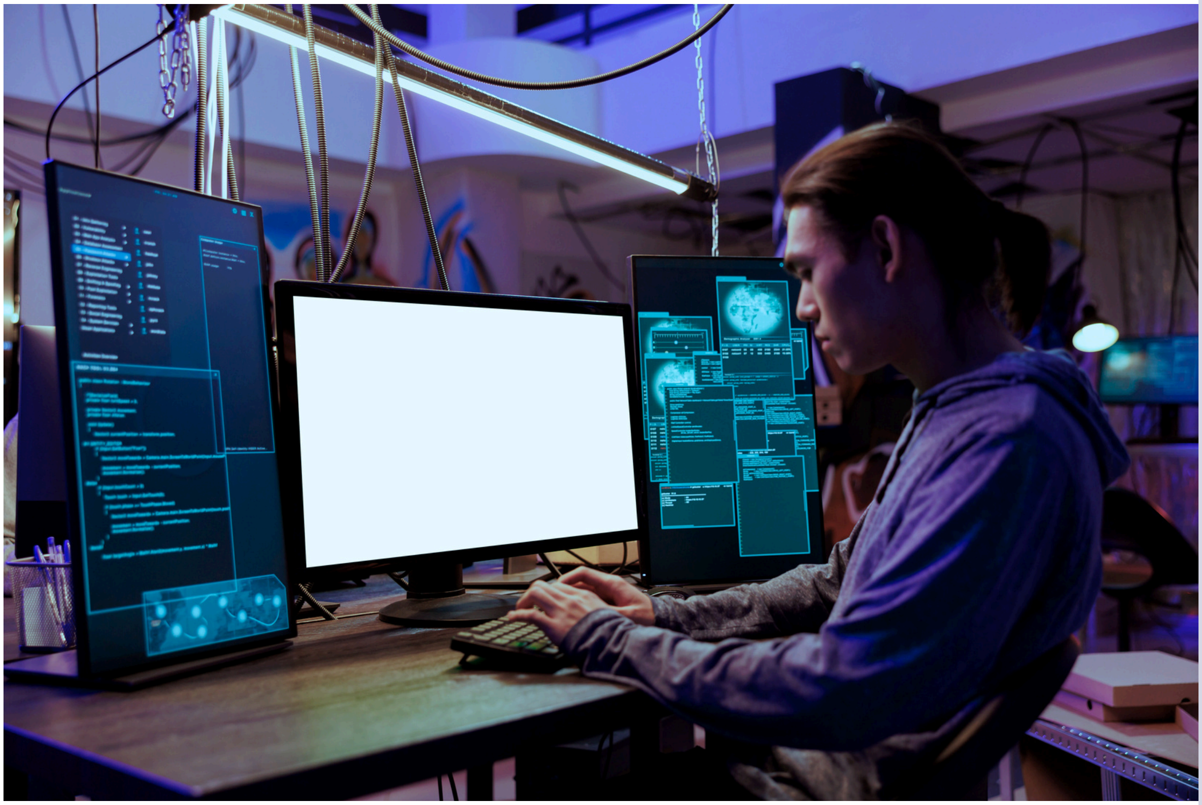
HIGH-LEVEL DEFENSE PLAN

High-level defense plan to counter a cyber offensive operation from a nation-state attacker

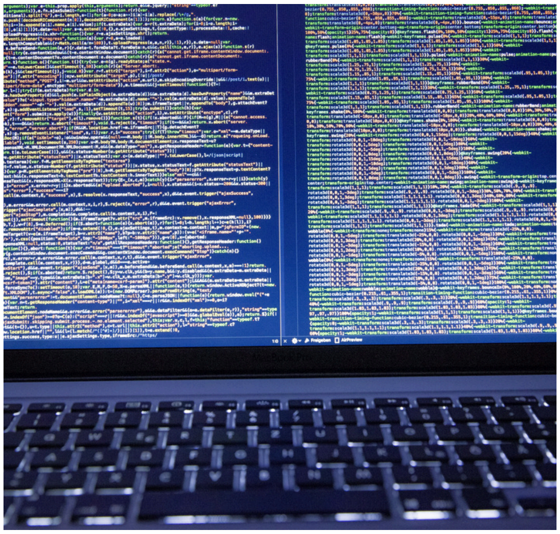
2/21/2024

Liela Pressley
Grand Canyon University- College of Engineering and Technology
ITT-340 | Information Assurance

TABLE OF CONTENT



HOW TO PROTECT AGAINST RECONNAISSANCE



Recon is the act of an actor looking to find more information about their target hoping to use this info to exploit vulnerabilities or even use social engineering to get past security protocols and gain unauthorized access.

To prevent or reduce the ability for attackers to try and gain unauthorized information about our organization such as OS types, devices, network activity, user credentials and permissions, etc. It is imperative that a reliable and well managed IDS (Intrusion Detection System) is in place as it can be used by management to detect incorrect, anomalous activity both on the computers and the network.

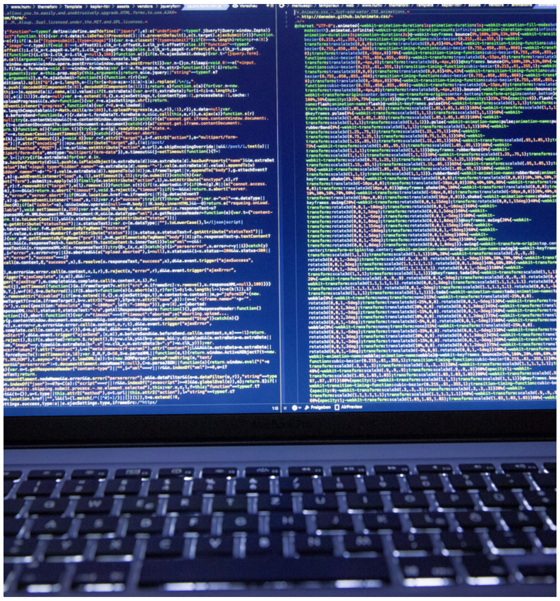
Next having a prioritized log managment tool establihsed so that logs of actvity are filtered, stored and analyzed which can be used to find attack or unauthorized access patterns.

Next is having a SIEM or a Security Information and Event Management software which can import the logs and correlate events and create a report among system from the given data.

Ensure that physical controls are set in place to ensure that systems and data are not easily accessed in case of a natural or intentional disaster. These include having sensor, alarms, smoke/fire detectors, motion detectors and close-circuit tv and monitors. In addition, implementing internal penetration test and personnel monitoring tools to reduce the risk of having attacks within the organization’s permimeter.

Time to take defensive action, honeypots are a computer system that is set up with intentional/known vulnerabiltie used to entice hackers who are targeting the organization. This can allow the organization to study the hacker’s behavious, motivation, strategy and tools. Pairing this with malware detection, signature detection, change detection, and state detection are necessary proactive ways to deter and reduce recon against a organization.

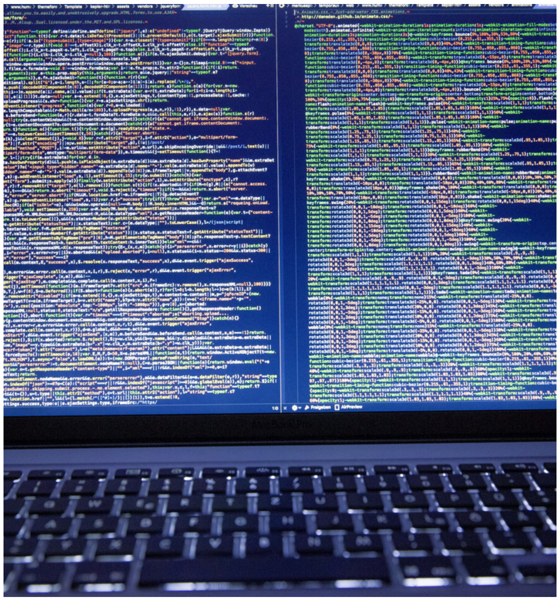
WEAPONIZATION & DELIVERY, EXPLOITATION, & COMMAND/CONTROL OPERATIONS



Weaponization is when the malicious actor takes all the recon information they have accumilated and implements their knowledge into an attack or a series of attacks on the organization. A well organized and built security team should have preperations in place not if but when an attack occurs. Though great efforts were made to prevent as much attacks as possible by following the guide for preventing recon-here is a list of necessary steps when an actor takes weaponized action against the organization. Incident handling is the first step to a successful recovery; its important to be as quick, efficient and accurate as possible in order to minimize damage. Incidents will test communicaiton between the security team, leadership, management, administrators, system owners, public relations, third party vendors, and legal teams.
The first step is ensuring that incident reporting is done accurately with evidence such as records, sources, referencing the incident response policy, operational procedures and more.

Ensure that our security team, management and the organization as a whole is aware of a clear/ emergency and crisis communication plan and failure to report these can be determental to the organization. Identifying an incident needs to be handled through a chain of custody to ensure that all information relevant to the event has evidence, is well documented, preserved, and protected. Next, containment needs to be acted upon as immediately as possible to prevent the incident/attack rom spreading or escalating. Eradicating the event is the hardest part of incident handling espeically with intricately exploited attack but this is the most crucial as it typically entails identifying and eliminationg vulnerabilities while carefully extracting malicious code and malware safely.

WEAPONIZATION & DELIVERY, EXPLOITATION, & COMMAND/CONTROL OPERATIONS



Lastly, if the incident handling team feels that all signs of malware and exploits are officially eradicated then it is time to rebuild the system and bring them back to operations. This is where good backups and baseline configurations will help the transition be that much more smoother. Once the system is restored then management needs to verify that restoration and recovry was a success and begin the review process.

The review is a follow up report reflecting on the incident, the pros, cons of how the situation was handled and what can be done to better the security posture of the organziation to make it stronger and what improvements can be made by the incident handling team. If done right this will help the organization set in place better and improved controls and management protocols to prevent recurrence,