Chad Ballay

CYBR430-342

1/27/2020

Week 7 Module 2 – Indications of Intrusion

Happy Accident Labs

222 South 15th Street

Omaha, NE 68102

(402) 915-0985

<http://www.happyaccidentlabs.com/>

1. SIEM
   1. Much of the analysis points to the initial precondition of no central point to aggregate security related activities for correlation. *A comprehensive review of the existing SIEM or acquiring a SIEM and the ancillary infrastructure needed to make use of it should be the first priority before proceeding.*
2. Physical Location
   1. Location is in a crowded downtown area. Identifying threat actors from the human traffic in the local environment is unlikely. *Low priority should be given here since it is unlikely to identify network intruders.*
   2. Internal office space is restricted from public access and therefore should be prioritized. Non-company employees and other such guest should not be unescorted. Medium priority should be given so as to discourage rogue devices being added to enable remote access to network. Unused ports should be disabled. All hardware should have company supplied inventory tag for identification/confirmation. *High priority should be given with an ongoing timeline.*
   3. After hours access should be monitored and investigated as part of daily or weekly review. Badge swipe logs vs recordings compared to validate the badge matches the employee. Activity and movement should trigger response to prevent rogue device from being installed after hours. *Medium priority should be given with a focus for turnkey solutions.*
3. Wifi
   1. Wifi signal propagation outside of office space should be addressed to discourage threat actors from readily accessing the network. This should be added to the next Wifi site survey performed. *Low priority should be given since this only reduces not prevents likelihood of attack.*
   2. Our initial breach was trigged by capturing a WPA handshake. Low priority should be given on monitoring the frequency of these since they occur due to multiple reasons. A single one is often enough. *Low priority since it is unlikely to be a large enough event to trigger.*
   3. The recording of the WPA was useful in that it allowed offsite attacking. *High priority should be given to Wifi’s password policy due to discovering it was a known password.*
   4. *Invalid authentication attempts should also be given a low priority.* This is due to low ROI on focus due to it is unlikely to be noticed or catch an attacker.
4. Network
   1. The enumeration of hosts on the network was accomplished using NMAP to scan the network. Each host identified then was probed for identifying OS and open ports/services. This proved immensely valuable. *High priority should be given to reviewing your IDS solution or attaining an IDS solution*
   2. The network was extremely flat in that all systems breached where on a single Class C subnet. *High priority should be given to compartmentalizing the network into logical groups that are better segregated.*
   3. Much of these breaches follow predictable patterns using common tools. *High priority should be given to reviewing your IPS solution or attaining an IPS solution.*
5. Systems
   1. A honey pot system can act as an efficient use of resources due to narrowing the areas of high intensity focus while still giving the same benefit of security. *High priority should be given to implementing a honeypot system.*
   2. Invalid login attempts are a likely indicator for further investigation. *High priority should be given to getting this into a SIEM.*
   3. Much of our activity would behaviorally differ from your employee’s nominal behavior. Copying/running netcat. High volume copying of files. Etc, etc…. *Medium priority should be given to review acceptable use policies and other policies that govern system usage and to implement monitoring for this to identify non-standard usage.*
   4. System metrics for CPU, network traffic, disk activity should be monitored for a variety of reasons. *Low priority should be given to establish a monitoring/alerting system to sudden spikes in these metrics based off of established trends.*
   5. Patch management failed at keeping the breached systems current on security patches. System inventory software and other tools for identifying devices that are out of compliance with patch levels should be highly prioritized with a focus for non-compliant system reporting.