RSA Conference 2016

Learning Labs

Performing Advanced Incident Response – Interactive Exercise

Post-Conference Summary

Merlin Namuth

Robert Huber

Performing Advanced Incident Response – Interactive Exercise

Incident response is more than just acknowledging an alert in a security tool and having a workstation reimaged. A large amount of information can be gathered to create a picture of how the incident occurred, the goal of the attack, if any sensitive information was stolen, and how to prevent a similar incident from happening again. The goal of this Learning Lab was to learn from each other on how to approach incident response answering these questions. A total of four scenarios were presented one at a time. Participants were given the opportunity to work the incident with their table partners. Everyone came back together to discuss and learn from each other.

Scenario 1 - Phishing Emails

It is common for people to receive phishing emails. When an employee forwards a phishing email to the incident response team, it must be analyzed to determine if an incident has occurred.

Analysis

- Collect metadata
  - SMTP – display name, originating IP address, attachment name, boundary, receiver, X-Mailer, encoding, language, and timezone are some examples
  - File – filesize, author, creation date, language set, hash, and mutex are some data points
- Language/Timezone settings
  - Is this a region where your company conducts business?
- Can use automated analysis platforms to determine if the attachment is malicious
- Find patterns of the recipients, such as department, same level of access to information, job title, and publicly available information about them
- Determine if this sender has sent other emails before
- We learned there are several data points to pivot to and from. Pivot on all metadata into other logs such as DNS, firewall, proxy, host, and security.

Mitigations

- Implement proxy block on malicious domain
- Implement DNS Blackhole
- Log for other hosts attempting to reach the same malicious site
- Ensure SIEM, IDS, and/or Flow are updated to alert for IP or DNS requests to the bad site

Scenario 2 - IDS Alert for psexec

IDS systems can alert on a wide variety of different malicious activity. For this scenario, we focused on psexec activity. The different analysis activities can be applied to most alerts from IDS systems, as well as other security tools.

Analysis

- Track down the host. Ensure before incident you have retention of at least 1 month's worth of DHCP logs
  - Were there any alerts for psexec on other hosts or did this host have IDS alerts for other activity?
- Determine how psexec was installed on host
  - Trace back to the first compromised system.
  - What was the method of compromise?
- How was psexec used?
  - It may have been used for exfiltration of sensitive company information
  - Psexec could have copied other attack tools to the victim system and other computers
- Pivoting
  - Correlate network and host-based forensics to determine timelines and method of compromise

Scenario 3 - Threat Hunter

This scenario was focused on the security tools functioning properly and how the incident responder can use the tools to find problems the security devices are missing. It can be overwhelming to know where to start. We discussed different data points.

Analysis

- Look for systems trying to communicate to the Internet bypassing the proxy
- Patterns of traffic to regions your company does not conduct business can be an indicator of an issue
- Determine if there are large file transfers after hours
- Multiple failed logins may indicate an attacker trying to brute force a password
- Binaries copied to critical servers may be a sign of an attacker copying malicious tools as well as repeated occurrences of the same filesize
- Search across network, endpoint, and security analytic solutions to gain a wide perspective using available threat intelligence

Scenario 4 - Employee Investigation

Sometimes incident response teams are called upon to support an internal investigation, as they have the tools and experience on using the tools to gather data. It is important to understand the sensitivity and documentation requirements for these efforts.

Analysis

- Determine the requester is authorized, such as HR or Legal
- Maintain strict confidentiality, such as using a different ticketing system only the IR team uses
- Document forensically sound process including date, time, and all actions performed
- Establish chain of custody of the evidence to prove it was not tampered
- Write a report with details and explanation of the technical aspects

Lessons Learned

- Incident response is more than responding to individual alerts
- It is not a helpdesk job and just acknowledging alerts
- Pivoting off of different data points can reveal a more complete and detailed picture

Application in first month

- Review your organization's incident response capabilities
- Start researching and reading more about incident response and threat hunting
- Get or create your own threat intelligence

Application within 3 months

- Create incident response plan, if you don't have one
- Search for examples
- Create incident response procedure

Application within 6 months

- Test incident response plan and procedure
- Create tracking metrics