Threat Hunting Methodology

Module 4

4.1 Methodology

4.2 Reporting

Methodology

In this module we'll discuss:

- A threat hunting methodology that you can follow to start hunting in your environments.

Survey the Hunting Ground

First we must begin by surveying the network. We need to understand where the high value assets are in our environment. This would be the machines and/or subnets that we'll hunt for signs of an adversary in.

There are different factors in determining which assets would be considered high value. Lets go over some.

Survey the Hunting Ground

Factors that would make an asset high value:

- A sysadmin's computer/laptop
  - Reason: compromise his/her machine then you'll have admin privileges throughout the environment.
- Server containing and/or processing sensitive information
  - Reason: this might be the end goal of a potential adversary.
- A necessary server running legacy software
  - Reason: it might be vulnerable and easily exploitable.

Survey the Hunting Ground

A risk assessment report can assist you in this phase.

This report will (should) list the organization's critical IT functions and group them by their priorities.

We can use this as guidance at defining the high value assets and for prioritization.

Survey the Hunting Ground

Next, we would put measures in place to ensure we have visibility to the asset(s). This would include network and host monitoring and data collection. The monitoring sensors need to be fine tuned to grab the type of information we'll need later when we're hunting.

As we discuss later in the course, these logs should be at a central repository and we, as hunters, need access to these logs if we don't already have it.

Securing the Assets

This phase entails securing an unsecured asset, if possible, or assets. It is a known concept that an adversary will not use their most advanced payload/tactic if they can use their least advanced instead.

Why use version 25 of their malware, which they perfected through time, when they can simply use version 3?

Securing the Assets

If you find a well-known adversary in your environment, depending on the TTPs that were used, it will give you an understanding of your security posture.

If they had to used version 25 of their malware instead of their version 3 then your security posture is better than most. You forced them to use their most advanced tactic to accomplish their task.

Securing the Assets

One of our goals is to make the objective of the adversary harder for them to achieve.

For example, if you're hunting for PTH and you find out that PTH will successfully be exploited in a particular high value asset, why not mitigate that so it makes it more difficult for the adversary to move laterally within the environment?

Securing the Assets

Another goal of securing the asset is to ensure that your monitoring tools are protected from the adversary.

For example, if Sysmon is on a device, the adversary will be able to tell and possibly disable and/or remove Sysmon altogether. We need to ensure that this does not happen and our monitoring tools stay intact on the asset.

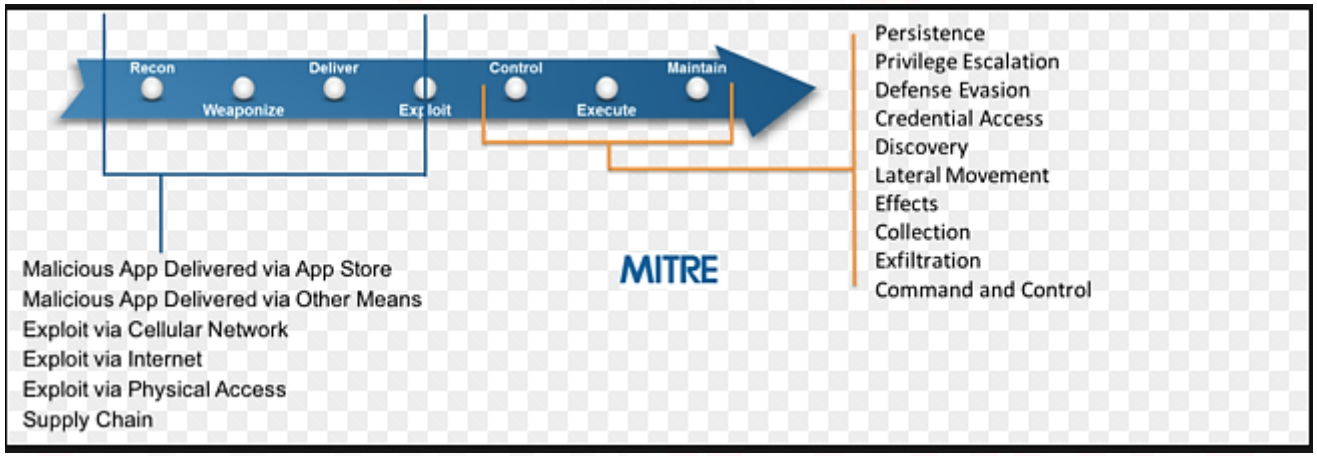
Attack Models

Before we begin hunting we need to choose an attack model.

We discussed a few attack models within the course. We made, and will make, a lot of references to Mitre's ATT&CK lifecycle so we'll use that attack model.

Attack Models

MITRE ATT&CK MODEL



Attack Models

Using that attack model we can identify activities of high impact, medium impact, and low impact.

Activities of high impact is the most devastating and can lead to data exfiltration if the adversary is successful.

This is where our focus should begin when hunting on the high value assets.

Hypothesis

Using the ATT&CK model as our guide, we need start identifying what activities you wish to hunt for. Activities, such as:

- C2 communication
- DNS Tunneling
- Lateral Movement
- Pass The Hash
- DLL Injection, etc.

We also need to create a **hypothesis** as to what type of activity **might be happening** in the high value asset and **hunt for it**.

Hypothesis

At this point you know that DNS Tunneling is a technique being used by malicious threat actors and you have identified this as an activity you want to hunt for.

Now you have to learn the various tools and techniques as to how this is accomplished by the adversary.

Hypothesis

This is necessary to understand how the attack takes place to effectively hunt for it. You might need to create an isolated environment within the network so you can create these simulations. In doing so, you can monitor what occurs at the network level and at the endpoint level. You can also search online for research papers or blog posts revealing such information.

Hypothesis

When you're hunting for the specific activity, you're actually proving or disproving your hypothesis. In all actuality you're not always going to get a hit but you might have other interesting patterns or anomalies that you find during your hunt. These findings should be documented.

Depending on the finding, other hunts can be scheduled and/or our detection rules can be updated.

Hypothesis

For example, we might be hunting for C2 activity and discover strange internal communication between 2 nodes. This information can be gathered and added to our detection rules to catch it if it happens again.

Now we no longer have to worry about hunting for that activity because we know our appliances will catch it and we don't have to waste our time hunting for it. We just secured the asset and hunting ground.

Hunting Schedule

Before we start hunting, we need to set a hunting schedule for our hunt team. There has to be some organization and tracking. Why is this necessary?

This will prioritize your hunts and ensure that an activity (whatever technique you're hunting for) isn't overlooked.

Hunting Schedule

A possible hunting schedule could be on the first week and second week of the month; hunters can hunt for high impact activities (based on the MITRE'S ATT&CK Model).

The last couple of weeks in the month can be dedicated to hunting medium impact activities.

Hunting Phase

At this point, we have:

- Identified the high value assets.
- Placed our monitoring capabilities where they need to be.
- Decided on the attack model that we'll use.
- Identified the different attack activities that fall within the different phases of the kill chain, by levels of severity (high, medium, low).
- A hunting schedule set.

Time to go hunting.

Hunting Phase

In this phase, the hunters will use various tools, techniques, and platforms to hunt for these activities.

Tools such as Bro, Network Miner, and PowerShell.

Techniques such as stacking, frequency analysis, and time correlation.

Platforms like ELK, Splunk, etc.

Respond Phase

This phase covers if you, the hunter, have found something. It can be active malware, dormant malware, an active C2 channel, etc. for example.

If its active malware, you can choose to monitor the activities of the adversary but you must contain the adversary to ensure that the adversary will not reach their objective.

Respond Phase

By monitoring the adversary you can discover the adversaries techniques, motives, and goals.

This will allow you to learn more about the adversary so you that you will be able to put more defensive measures in place.

Respond Phase

Don’t forget that documentation is crucial. It’s not enough that you found evidence of DLL Injection, you found active malware, you watched the adversary pivot throughout the network, and removed all traces of them from the network.

Respond Phase

The Diamond Model can be used to document any findings on all the hunts. This can later be used to see if there are any correlation between different sets of findings, meaning if it can be the same threat actor/group.

If you're not comfortable with the Diamond Model, find a method that will work for you.

Respond Phase

Alternatively, you can use a template created by Lenny Zeltser called Report Template for Threat Intelligence and Incident Response.

You can read more about it and download it here.

Respond Phase

This form of documentation is good among the hunt team and maybe can be shared with other teams, like the SOC analysts, but it will not be good enough to present to management.

The next section will propose a format in which you can generate a report to submit to management regarding the findings from your team's hunts.

REPORTING

The next few slides will outline what should be detailed in your report that you submit to management, or even the C-Suite.

Executive Summary

The executive summary is the first part of the report.

It should be no longer than a few pages and should sum up, at a high level (without the use of jargon), the overall outcome of the hunt.

Executive Summary

A report of this magnitude should only be required when the hunter actually finds something in their hunts and the hunter had to take action.

You will not submit a report after every hunt if there is not anything significant to report.

Scope of Compromise

In this section, the following should be detailed:

- What was affected (business process, users, data sets, machines, etc.).
- In what ways were they affected and for how long (dwell time).
- A timeline of the activities involving the compromise should be noted in this section.

Adversary Identification

If we have enough information to successfully identify the threat actor/group, it would be disclosed in this section.

Along with supporting information to validate your theory. You may reference other reports in this section too.

Timeline of Discovery

In this section, the following should be detailed:

- Each step of your hunt, indicating your finding(s)
- Tools and/or techniques used in the steps
- Any other pertinent information, such as adversary monitoring, modifications to the network to contain the adversary, etc.

Remediation Plan

Lastly, this section should outline how the adversary was able to succeed through the different steps of the kill chain and remediation steps to ensure that the techniques used will be monitored and/or ineffective by making adjustments in the network where necessary.

Remember, this report will be submitted to individuals that are probably not technical, don't understand the jargon, and don't care about the latest TTPs.

We have to do our best to convey our findings in a report that they understand and are interested in hearing/reading.

This section by no means is an official reporting outline.

It’s merely a recommendation based on the input of many within the threat hunting community.

Feel free to use or come up with an outline that you see fit to report your findings.

4.3 Module Conclusion

MAP REF

This concludes the module on Threat Hunting Methodology.

We have covered:

- ✓ How to start threat hunting in your environment
- ✓ How to construct a report to disclose your findings to management and C-Suite personnel

References

[Report Template for Threat Intelligence and Incident Response]