Cybersecurity Case study

Task 1: Response to a malware attack

Background information

You are an information security analyst in the Security Operations Centre at Telstra Australia. A common task and responsibility of information security analysts in the SOC is to respond to triage incoming threats and respond appropriately, by notifying the correct team depending on the severity of the threat. It's important to be able to communicate the severity of the incident to the right person so that the organisation can come together in times of attack.

The firewall logs & list of infrastructure has been provided, which shows critical services that run the Spring Framework and need to be online / uninterrupted. A list of teams has also been provided, which depending on the severity of the threat, must be contacted.

It's important to note that the service is down and functionality is impaired due to the malware attack.

Your task

Your task is to triage the current malware threat and figure out which infrastructure is affected.

First, find out which key infrastructure is currently under attack. Note the priority of the affected infrastructure to the company - this will determine who is the respective team to notify.

After, draft an email to the respective team alerting them of the current attack so that they can begin an incident response. Make sure to include the timestamp of when the incident occurred. Make it concise and contextual.

The purpose of this email is to ensure the respective team is aware of the ongoing incident and to be prepared for mitigation advice.

Resources to help you with the task

https://www.cisa.gov/uscert/ncas/current-activity/2022/04/01/spring-releases-security-updates-addressing-spring4shell-and

https://tanzu.vmware.com/security/cve-2022-22965

Task 1_2 - Firewall_Infrastructure List.xlsx

T1 – Email Template.docx

Task 2: Analysing the attack

Background information

Now that you have notified the infrastructure owner of the current attack, analyse the firewall logs to find the pattern in the attacker's network requests. You won't be able to simply block IP addresses, because of the distributed nature of the attack, but maybe there is another characteristic of the request that is easy to block.

An important responsibility of an information security analyst is the ability to work across disciplines with multiple teams, both technical and non-technical.

In the resources section, we have attached a proof of concept payload that may be of interest in understanding how the attacker scripted this attack.

Your task

First, analyse the firewall logs in the resources section.

Next, identify what characteristics of the Spring4Shell vulnerability have been used.

Finally, draft an email to the networks team with your findings. Make sure to be concise, so that they can develop the firewall rule to mitigate the attack. You can assume the recipient is technical and has dealt with these types of requests before.

Resources to help you with the task

https://github.com/craig/SpringCore0day/blob/main/exp.py

Task 1_2 - Firewall_Infrastructure List.xlsx

T2 – Firewall request Template.docx

Task3: Mitigate the malware attack

background information

Work with the networks team to implement a firewall rule using the Python scripting language. Python is a common scripting language used across both offensive and defensive information security tasks.

In this task, we will simulate the firewall's scripting language by using an HTTP Server. You can assume this HTTP Server has no computational requirements and has the sole purpose of filtering incoming traffic.

In the starter codebase, you will find a test script that you can use to simulate the malicious requests to the server.

You can check out the Readme file in the starter codebase for more information on how to get started.

Your task:

Use Python to develop a firewall rule to mitigate the attack. Develop this rule in `firewall_server.py`.

You may use `test_requests.py` to test your code whilst the firewall HTTP server is running.

Resources to help you with the task

https://github.com/craig/SpringCore0day/blob/main/exp.py

https://docs.python.org/3/library/http.server.html

T3 – Firewall_Starter_codebase.zip

Task4: Incident Postmortem

background information

The firewall rule worked in stopping the malware attack, 2 hours after the attack began.

After an incident has occurred, it's best practice to document and record what has happened. A common report written after an incident is a postmortem, which covers a timeline of what has occurred, who was involved in responding to the incident, a root cause analysis and any actions which have taken place.

The purpose of the postmortem is to provide a 'paper trail' of what happened, which may be used in future governance, risk, or compliance audits, but also to educate the team on what went down, especially for those on the team who weren't involved.

In the resources section, you will find some educational content about what is an incident postmortem and why it's important to create one.

Your task

For this task, create an incident postmortem of the malware attack, covering the details you have picked up in the previous tasks.

Make sure to include when the incident started and the root cause. Remember, the more detail the better.

Resources to help you with the task

https://www.pagerduty.com/resources/learn/incident-postmortem/

T4_Postmortem Template.docx