Offensive Security Threat Hunter Exam Report

OSTH Exam Report

student@youremailaddress.com, OSID: XXXXX

2024-10-19

Contents

1 Offensive Security Threat Hunter Exam Report

1.1 Introduction

The OffSec Threat Hunter exam report contains all efforts that were conducted in order to pass the OffSec certification examination. This report should contain all items that were used to pass the exam and it will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of threat hunting methodologies as well as the technical knowledge to pass the qualifications for the OffSec Threat Hunter.

1.2 Objective

The objective of this assessment is to perform a threat hunting sprint in the Megacorp One environment. The student is tasked with following a methodical approach to identify all compromised systems and detect if sensitive data was exfiltrated or encrypted. An example page has already been created for you at the latter portions of this document that should demonstrate the amount of information and detail that is expected in the exam report. Use the sample report as a guideline to get you through the reporting.

1.3 Requirements

The student will be required to fill out this threat hunting report fully and to include the following sections:

- Executive Summary
- Methodology
- Hunt Narrative
  - A detailed walkthrough of the entire threat hunting sprint.

  - The walkthrough should contain an explanation of all steps, assumptions, and decisions supported by screenshots and Splunk queries if applicable.
  - The walkthrough should be thorough enough that the complete threat hunting sprint can be replicated step-by-step by a technically competent reader.

- Findings
  - A timeline of all key activities related to the attacker's actions
- Conclusion
- IoC Lists in the Appendix

2 Executive Summary

2.1 Overview

The threat hunting sprint began with the assignment of reviewing the threat intelligence report of an APT group known as “We Are Garfield” (WAG) and proactively hunting for indicators of a compromise within the Megacorp One systems. The primary objectives were to identify all compromised systems and assess the impact of the attacker’s actions, such as determining whether data has been exfiltrated or encrypted.

During the threat hunt, we identified three compromised systems within the Megacorp One environment:

- PC1
- PC2
- PC3

The threat actor accessed and exfiltrated the secret recipe for our chocolate muffins, which could have catastrophic consequences if leaked or sold to competitors.

2.2 High-Level Attack Path

The threat hunt revealed the following high-level path the threat actor took to compromise the Megacorp One environment:

1. PC1 was used as the initial entry vector by the threat actor by trying numerous passwords against several user accounts. The threat actor finally succeeded and got access to this machine with administrative privileges.
2. PC2 was configured to use the same password for the local administrator account and the threat actor used it to get access to it. On the machine, the attacker obtained credentials from logged on users by using Mimikatz.
3. PC3 was accessed using one of the obtained sets of credentials from PC2. The threat actor accessed and exfiltrated the secret chocolate muffin recipe from this machine.

2.3 Recommendations

The threat hunt revealed the following high-level path the threat actor took to compromise the Megacorp One environment:

1. **Escalate Incident to Incident Response Team:**
    - Escalate the incident to the incident response team to conduct a thorough investigation of the identified compromises. The focus should be on assessing the full scope of the incident and understanding its impact on the organization's systems and data.
    - Collaborate closely with the incident response team to share findings, provide context, and support their efforts in containing and remediating the security incidents.
2. **Continued Support and Analysis:**
    - Remain actively involved in supporting other defensive teams, particularly during the incident detection and identification phase of the incident management process.
    - Conduct further analysis of the malware samples to extract additional IoCs and behavioral patterns, providing valuable insights for ongoing threat detection and mitigation efforts.
3. **Continuous Improvement and Training:**
    - Implement policies to ensure that users do not reuse passwords across different accounts.
    - Develop and deploy detection rules to identify and prevent successful password attacks.
    - Add access control mechanisms to prevent unprivileged user accounts from accessing sensitive files.
    - Implement security awareness training for all users, emphasizing strong password usage and best practices.

3 Methodology

For the scheduled threat hunting sprint, we utilized the following tools, scripts, commands, and resources:

- Splunk
- WAG Threat Intelligence Report
- PowerShell on DEV (Deobfuscation)

We performed an intelligence-based threat hunting sprint based on the information provided in the WAG threat intelligence report. This approach led us to detect the usage of Mimikatz on PC2, which revealed several additional indicators for further investigation. By analyzing these indicators, we were able to identify lateral movement to PC3 by correlating login and Sysmon events in Splunk with the known tools and techniques categorized under the “Lateral Movement” column. Through this analysis, we also discovered that after compromising PC3, the attacker exfiltrated a sensitive document.

After exhausting our list of IoCs and other information from the intelligence-based phase, we transitioned to hypothesis-based threat hunting. This shift provided us with the flexibility to investigate how PC2 was accessed and how the perimeter was breached, considering that this is not a publicly accessible machine.

Our hunting hypothesis was:

We suspect that PC3 and PC2 are not the only systems compromised by the WAG threat actor. While we couldn’t identify any further indicators that revealed additional compromised systems using the credentials obtained from PC2, or following the compromise of PC3, it is likely that PC2 was not the initial system compromised by WAG, given that it is not externally accessible. Therefore, we suspect that at least one other machine is compromised. We will validate this by investigating the events preceding the use of Mimikatz to obtain credentials and by identifying the vector the threat actor used to access PC2 and breach the perimeter.

4 Hunt Narrative

The threat intelligence report covering TTPs of the threat actor We Are Garfield provided a list of IoCs including SHA-256 hashes. We used the following query in Splunk to hunt for these hashes:

```
index="*" ("EEAAFA68236BD1629E36E81C5A8EC2CE8804C9798B5C84FEE55F6128CCBA8FB0" OR
"4ED877F6F154EB6EBB02EE44E4D836C28193D9254A4A3D6AF6236D8F5BAB88D2" OR
"11EBBAA2EDA3CCD4B7F1BB2C09AC7DCA0CD1F4B71B7E0CFCEDE36861E23DA034" OR
"8507FFC7EA1953F66D8441180C281D456889F93CF3F6CBB01F368886F9D8C097"
```

This search query resulted in only a single event with the timestamp 01/11/2024 1:11:11 AM:

Figure 4.1: ImgPlaceholder

The matching SHA-256 hash is referred to as “Mimikatz” in the threat intelligence report. We then reviewed the event in more detail.

Figure 4.2: ImgPlaceholder

The event provides us several important information that can be leveraged in our hunt:

- Username: Administrator
- Filename: Zwetsch.exe
- Directory: `C:\hackingtools\`

Based on the matching SHA-256 hash of the threat intelligence report and the characteristic command-line argument “sekurlsa::logonpasswords”, we can be certain that this is Mimikatz.

[...]

5 Findings

Timestamp	Observation	Affected Assets
01/09/2024 3:25:00 PM	Beginning of Password Spraying with Password Password1!	Host: PC1
01/09/2024 3:58:00 PM	End of Password Spraying.	Host: PC1
01/09/2024 3:58:15 PM	Successful login for local Administrator user	Host: PC1 User: Administrator (local)
01/09/2024 3:59:00 PM	Download of meterpreter.exe from `<IP>` via Browser	Host: PC1 User: Administrator
01/09/2024 3:59:49 PM	Process Creation of meterpreter.exe	Host: PC1 User: Administrator (local)
01/09/2024 4:05:11 PM	Process Creation of PsExec	Host: PC1 User: Administrator (local) Target Machine: PC2 Target User: Administrator (local) Password: Password1!”
[…]	[…]	[…]
01/11/2024 1:11:11 AM	Process Creation of Zwetsch.exe	Host: PC2 User: Administrator (local)
[…]	[…]	[…]

6 Conclusion

Our threat hunting sprint successfully uncovered three compromised systems within the Megacorp One enterprise, along with the exfiltration of our secret chocolate muffin recipe.

Based on our findings and actionable insights, the incident response team can now initiate the necessary steps for incident detection and identification, containment, and restoration of the compromised systems. In addition, any policy- or regulation-driven actions can be initiated to ensure compliance and further secure the organization.

For comprehensive guidance on potential remediation steps and enhancing detection capabilities, please refer to the compiled list of IoCs provided in the Appendix of this report. These IoCs serve as a valuable reference and baseline for improving our organization's overall security resilience against similar threats in the future.

7 Appendix

7.1 IOCs

Attached is a compiled list of the resulting IOCs found during the threat hunting sprint.

File Hashes

File Name	SHA256
Zwetsch.exe	4ED877F6F154EB6EBB02EE44E4D836C28193D9254A4A3D6AF6236D8F5BAB88D2
meterpreter.exe	DF99BBABE7BD0E7A1D96CF370B78FDCF250AF380065A3D51F57EDE6A571E2C15
[…]	[…]

Network Communications

Type	Value
C&C	192.168.1.1:9999 (meterpreter.exe)
Exfiltration	192.168.1.1:80 (WebDAV Share “looty”)
File Download	192.168.1.1:80 (meterpreter.exe)
File Download	192.168.1.1:80 (Zwetsch.exe)
[…]	[…]