OffSec Defense Analyst

Exam Report

OSID: OS-XXXXX
student@example.com

September 30, 2025

v2.0

Table of Contents

1 OffSec Defense Analyst Exam Report 3

1.1 Objective 3

1.2 Requirements 3

2 High-Level Summary 4

3 Attacker Phases 5

3.1 Phase 1 5

3.1.1 RDP Brute Force 5

3.1.2 Persistence 7

3.1.3 Summary 8

3.2 Phase 2 9

3.2.1 TODO Action 9

3.3 Phase 3 10

3.3.1 TODO Action 10

3.4 Phase 4 11

3.4.1 TODO Action 11

3.5 Phase 5 12

3.5.1 TODO Action 12

3.6 Phase 6 13

3.6.1 TODO Action 13

3.7 Phase 7 14

3.7.1 TODO Action 14

3.8 Phase 8 15

3.8.1 TODO Action 15

3.9 Phase 9 16

3.9.1 TODO Action 16

3.10 Phase 10 17

3.10.1 TODO Action 17

1 OffSec Defense Analyst Exam Report

The OffSec Defense Analyst 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 security detection methodologies as well as the technical knowledge to pass the qualifications for the OffSec Defense Analyst.

1.1 Objective

The objective of this assessment is to perform detections and analysis on the simulated exam network in order to determine which attacker actions took place in each of the 10 phases.

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.

1.2 Requirements

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

- Overall High-Level Summary of level of compromise
- Detailed walkthrough of attacker actions in each phase
- Each finding with included screenshots, explanations, event / log entries, and KQL queries if applicable

2 High-Level Summary

This report details and documents the attacks observed against the OffSec OSDA exam network.

The attacker organization started by performing a brute force against an internet accessible RDP server called APPSRV02 and obtained administrative access. This led to a complete compromise of the server.

Next the attacker performed lateral movement to the internal server APPSRV02 by reusing stolen credentials from APPSRV02, this also led to a complete compromise of APPSRV03.

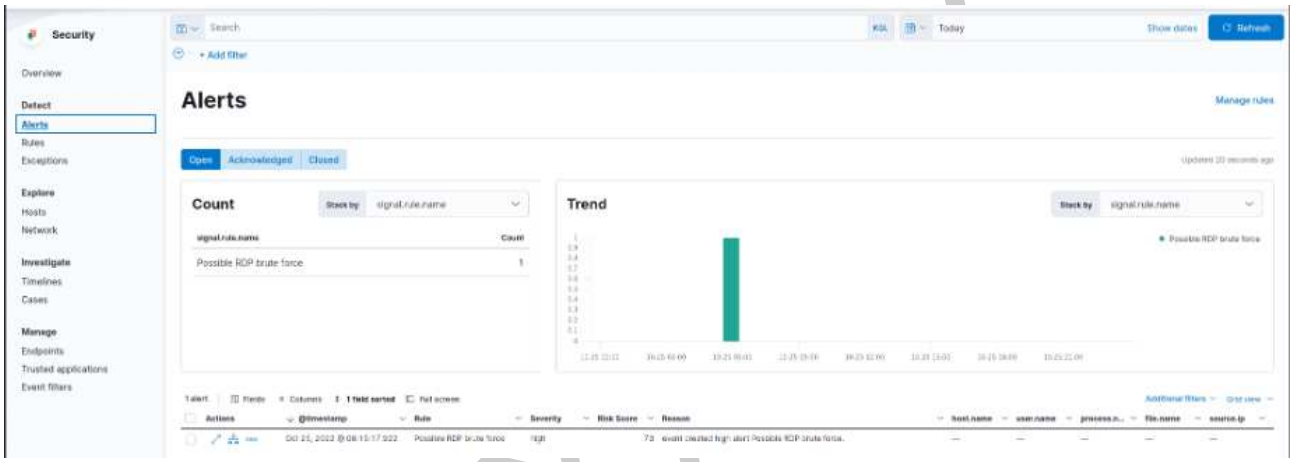
...

3 Attacker Phases

3.1 Phase 1

3.1.1 RDP Brute Force

The initial indicator of an attack happening was the triggering of a pre-defined threshold rule called “Possible RDP brute force” as shown below.



By looking at how the rule was defined, it is triggered by more than 100 instances of event ID 4625, which is a failed logon. This could align with a brute force attack where the attacker makes use of a user and/or password list.

When we inspect some of the events that triggered the alert, as shown below, we notice that the server reporting the events is APPSRV02.

Given that an attacker may have attempted to brute force the server, we should search for a subsequent successful log on event to APPSRV02 to determine if they obtained access.

We do this with the following KQL query:

event.code : "4624" and NOT user.name : SYSTEM and NOT user.name : DWM-2

From this query we find the following event entry:

t host.name	appsrv02
t host.os.build	17763.2565
t host.os.family	windows
t host.os.kernel	10.0.17763.2565 (WinBuild.160101.0800)
t host.os.name	Windows Server 2019 Standard
t host.os.platform	windows
t host.os.type	windows
t host.os.version	10.0
t input.type	winlog
t log.level	information
t message	› An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: -
t process.executable	-
t process.name	-
# process.pid	0
IP related.ip	192.168.67.69
t related.user	Peter
t source.domain	-
IP source.ip	192.168.67.69

This shows that the user Peter did a successful logon to APPSRV02 shortly after the suspected brute force attack. The source IP of the logon event was 192.168.67.69 which means its not a local logon, but remotely.

At this point we have a strong suspicion that the account with the username Peter was compromised and a malicious actor obtained access to APPSRV02 coming from the IP address 192.168.67.69. We should escalate this to an incident and contact the user to verify whether this was a legitimate logon.

3.1.2 Persistence

After suspicion of a compromise, additional investigation should be performed. One area is looking for persistence and a common way attackers employ is through the registry.

To try and determine if this happed, we can use the KQL query:

process.name : "reg.exe" As a result, we find the following event:

process.args	reg, add, HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, /f, /v, UpdateService, /t, REG_SZ, /d, C:\Windows\System32\update.exe
process.args_count	10
process.command_line	reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" /f /v UpdateService /t REG_SZ /d "C:\Windows\System32\update.exe"
process.entity_id	{ae2f0756-bfd2-6357-0c01-000000001100}
process.executable	C:\Windows\SysWOW64\reg.exe
process.hash.md5	dacac17455d4eefe433b41ba02cd106f
process.hash.sha256	e3046d83648d114af89c6b7738f69b14ec188ece999573489a7d3386e4abab b5
process.name	reg.exe
process.parent.args	cmd.exe

This shows that a registry change was performed. An entry for the Run key was added. The Run registry key is used when a user logs on to the computer and thus is often used for persistence.

In particular we notice that the file “C:\Windows\System32\update.exe” will be executed when a user logs on to APPSRV02.

We should escalate this to investigate what the file update.exe is.

3.1.3 Summary

In this phase we have strong suspicions that a malicious actor performed a brute force attack against APPSRV02 and managed to compromise the user account with the username “Peter”. Additionally, we suspect that persistence was set up through a Run key in the registry to execute the file “C:\Windows\System32\update.exe”.

3.2 Phase 2

3.2.1 TODO Action

TODO Action Details

3.3 Phase 3

3.3.1 TODO Action

TODO Action Details

3.4 Phase 4

3.4.1 TODO Action

TODO Action Details

3.5 Phase 5

3.5.1 TODO Action

TODO Action Details

3.6 Phase 6

3.6.1 TODO Action

TODO Action Details

3.7 Phase 7

3.7.1 TODO Action

TODO Action Details

3.8 Phase 8

3.8.1 TODO Action

TODO Action Details

3.9 Phase 9

3.9.1 TODO Action

TODO Action Details

3.10 Phase 10

3.10.1 TODO Action

TODO Action Details

End of Report

This report was rendered
by SysReptor with
♥