
Offensive Security Defense Analyst Exam Report

OSDA Exam Report

student@youremailaddress.com, OSID: XXXX

2022-11-08

Contents

- 1 Offensive Security OSDA Exam Report 1**
 - 1.1 Introduction 1
 - 1.2 Objective 1
 - 1.3 Requirements 1

- 2 High-Level Summary 2**

- 3 Attacker Phases 3**
 - 3.1 Phase 1 3
 - 3.1.1 RDP Brute Force 3
 - 3.1.2 Persistence 4
 - 3.1.3 Summary 5
 - 3.2 Phase 2 6
 - 3.3 Phase 3 6
 - 3.4 Phase 4 6
 - 3.5 Phase 5 6
 - 3.6 Phase 6 6
 - 3.7 Phase 7 6
 - 3.8 Phase 8 6
 - 3.9 Phase 9 6
 - 3.10 Phase 10 6

1 Offensive Security OSDA Exam Report

1.1 Introduction

The Offensive Security Exam report contains all efforts that were conducted in order to pass the Offensive Security certification test. 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 Offensive Security Defense Analyst.

1.2 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.

1.3 Requirements

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

1. Overall High-Level Summary of level of compromise
2. Detailed walkthrough of attacker actions in each phase
3. 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 Offensive Security 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.



Figure 3.1: ImgPlaceholder

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.



Figure 3.2: ImgPlaceholder

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:

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:



Figure 3.3: ImgPlaceholder

```
process.name : "reg.exe"
```

As a result, we find the following event:

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`.



Figure 3.4: ImgPlaceholder

3.2 Phase 2

3.3 Phase 3

3.4 Phase 4

3.5 Phase 5

3.6 Phase 6

3.7 Phase 7

3.8 Phase 8

3.9 Phase 9

3.10 Phase 10