OFFENSIVE SECURITY

OSEP Exam Documentation

v.1.0

student@youremailaddress.com

OSID: XXXXX

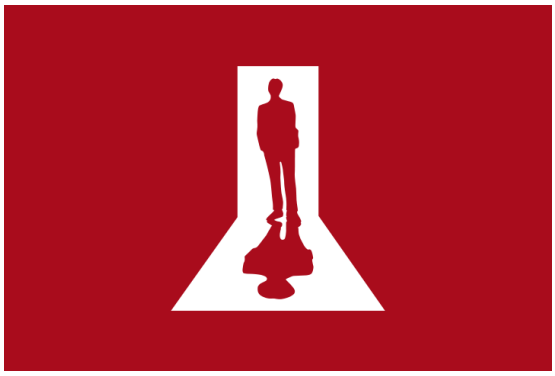

Table of Contents

1.0 Offensive-Security OSEP Exam Documentation 3
1.2 Requirements 3
2.0 High-Level Summary 4
3.0 192.168.XX.XX / Hostname 4
3.1 Local.txt / Proof.txt / Secret.txt 4
3.2 Pre-Compromise Enumeration Steps 4
3.3 Compromise 4
3.4 Post-Exploitation Enumeration Steps 4
3.5 Local Privilege Escalation 5
3.6 Screenshots 5

1.0 Offensive-Security OSEP Exam Documentation

The Offensive Security OSEP exam documentation contains all efforts that were conducted in order to pass the Offensive Security Experienced Penetration Tester exam. This report 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 the technical knowledge required to pass the qualifications for the Offensive Security Experienced Penetration Tester certification.

1.1 Objective

The objective of this assessment is to perform an external penetration test against the Offensive Security Exam network. The student is tasked with following methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including enumeration and post-exploitation. The exam report is not meant to be a penetration test report, but rather a writeup of the steps taken to locate, enumerate and compromise the network.
Enumeration and post-exploitation actions that lead to subsequent attacks with successful compromises should be included in the report.
An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this exam. 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 exam documentation fully and to include the following sections:

- High level summery of findings, including the depth of compromise.
- Methodology walkthrough and detailed outline of steps taken including enumeration.
- Each finding with included screenshots, walkthrough, sample code or reference.
- Screenshot of any local.txt, proof.txt or secret.txt.

2.0 High-Level Summary

A brief description of the attack chain with machine names, including the depth of compromise should be included here.

3.0 192.168.XX.XX / Hostname

3.1 Local.txt / Proof.txt / Secret.txt

Provide the contents of local.txt, proof.txt or secret.txt

3.2 Pre-Compromise Enumeration Steps

Provide relevant techniques and methods used to perform enumeration prior to initial compromise, the steps taken should be able to be easily followed and reproducible if necessary. Include any custom code or references to public tools.

3.3 Compromise

Provide a description of exploitation steps to compromise the machine and obtain shell access, the steps taken should be able to be easily followed and reproducible if necessary. Only the steps that ended up working are required. Include any custom code or references to public tools.

3.4 Post-Exploitation Enumeration Steps

Provide relevant post-exploitation enumeration steps related to the network or local privilege escalation, the steps taken should be able to be easily followed and reproducible if necessary. Include any custom code or references to public tools.

3.5 Local Privilege Escalation

Provide a description of exploitation steps to escalate privileges on the machine if applicable, the steps taken should be able to be easily followed and reproducible if necessary. Include any custom code or references to public tools.

3.6 Screenshots

The exam control panel contains a section available to submit your proof files. The contents of the local.txt, proof.txt and secret.txt files obtained from your exam machines must be submitted in the control panel before your exam has ended. Note that the control panel will not indicate whether the submitted proof is correct or not.

Each local.txt, proof.txt and secret.txt found must be shown in a screenshot that includes the contents of the file, as well as the IP address of the target by using ipconfig, ifconfig or ip addr.