
Offensive Security Experienced Penetration Tester Exam Report

OSEP Exam Report

foo@bar.com, OSID: 12345

2022-01-25

Contents

1	Offensive-Security OSEP Exam Documentation	1
1.1	Objective	1
1.2	Requirements	1
2	High-Level Summary	2
2.1	DOMAIN_NETWORK	2
2.2	DOMAIN_NETWORK_X	2
2.2.1	Compromise through VECTOR_X	2
3	Flow of Attack	3
3.1	DOMAIN_NETWORK	3
3.1.1	192.168.X.X / HOSTNAME - Low & And High Priv. User's	3
3.1.1.1	Local.txt / Proof.txt	3
3.1.1.2	Pre-Compromise Enumeration Steps	3
3.1.1.3	Compromise	3
3.1.1.4	Post-Exploitation Enumeration Steps	3
3.1.1.5	Local Privilege Escalation	4
3.1.2	192.168.X.X / HOSTNAME - High Priv. User's	4
3.1.2.1	Proof.txt / Secret.txt	4
3.1.2.2	Pre-Compromise Enumeration Steps	4
3.1.2.3	Compromise	4
3.1.2.4	Post-Exploitation Enumeration Steps	4
3.1.2.5	Local Privilege Escalation	5
3.2	DOMAIN_NETWORK_X	5
3.2.1	Compromise through VECTOR_X	5
4	Additional Items	6
4.1	Appendix - AMSI Bypass code	6
4.2	Appendix - Powershell Shellcoderunner	6
4.3	Appendix - ANOTHER_SHELLCODE_USED Shellcoderunner Code	6
4.4	Appendix - Proof and Local Contents	6
4.5	Appendix - Credentials obtained	6
4.5.1	NTLM Hashes	6
4.5.2	Passwords	6
4.5.3	Credential's files	6

1 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 summary 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 High-Level Summary

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

2.1 DOMAIN_NETWORK

Server IP Address	Hostname	Compromised	Low-Privilege User	High-Privilege User
192.168.X.X	HOSTNAME	No	N/A	N/A
192.168.X.X	HOSTNAME	Yes	jperez	root
192.168.X.X	HOSTNAME	Yes	N/A	root

The chain of attack followed for getting into the machines from above in the network DOMAIN was as follows:

- 1 -
- 2 -
- 3 -
- 4 -
- N -
- 9 -

2.2 DOMAIN_NETWORK_X

2.2.1 Compromise through VECTOR_X

Briefly description of how the DOMAIN_NETWORK_X was compromised throughout the VECTOR_X.

3 Flow of Attack

3.1 DOMAIN_NETWORK

3.1.1 192.168.X.X / HOSTNAME - Low & And High Priv. User's

3.1.1.1 Local.txt / Proof.txt

Local.txt

```
1 foo
```

Proof.txt

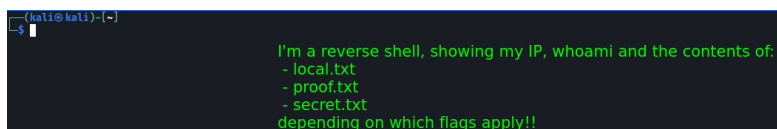
```
1 bar
```

3.1.1.2 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 reference to public tools, if custom code then reference it in the Appendix, for example “Code for AMSI Bypass in Appendix 4.1”.

3.1.1.3 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 reference to public tools, if custom code then reference it in the Appendix, for example “Code for AMSI Bypass in Appendix 4.1”.



```
(kali@kali)-[~]  
└─$   
I'm a reverse shell, showing my IP, whoami and the contents of:  
- local.txt  
- proof.txt  
- secret.txt  
depending on which flags apply!!
```

3.1.1.4 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 reference to public tools, if custom code then reference it in the Appendix, for example “Code for AMSI Bypass in Appendix 4.1”.

3.1.1.5 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 reference to public tools, if custom code then reference it in the Appendix, for example “Code for AMSI Bypass in Appendix 4.1”.

```
(kali@kali)-[~]  
└─$  
I'm a reverse shell, showing my IP, whoami and the contents of:  
- local.txt  
- proof.txt  
- secret.txt  
depending on which flags apply!!
```

3.1.2 192.168.X.X / HOSTNAME - High Priv. User's

3.1.2.1 Proof.txt / Secret.txt

Proof.txt

```
1 bar
```

Secret.txt

```
1 foobar
```

3.1.2.2 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 reference to public tools, if custom code then reference it in the Appendix, for example “Code for AMSI Bypass in Appendix 4.1”.

3.1.2.3 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 reference to public tools, if custom code then reference it in the Appendix, for example “Code for AMSI Bypass in Appendix 4.1”.

```
(kali@kali)-[~]  
└─$  
I'm a reverse shell, showing my IP, whoami and the contents of:  
- local.txt  
- proof.txt  
- secret.txt  
depending on which flags apply!!
```

3.1.2.4 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 reference to public tools, if custom code then reference it in the Appendix, for example “Code for AMSI Bypass in Appendix 4.1”.

3.1.2.5 Local Privilege Escalation

Local Privilege Escalation doesn't apply as the initial access was already an elevated one.

3.2 DOMAIN_NETWORK_X

3.2.1 Compromise through VECTOR_X

Detailed explanation of how the DOMAIN_NETWORK_X was obtained throughout the VECTOR_X this section belongs to.

4 Additional Items

4.1 Appendix - AMSI Bypass code

4.2 Appendix - Powershell Shellcoderunner

4.3 Appendix - ANOTHER_SHELLCODE_USED Shellcoderunner Code

4.4 Appendix - Proof and Local Contents

Hostname	local.txt Contents	proof.txt Contents
HOSTNAME	foo	bar
HOSTNAME	foo	bar

4.5 Appendix - Credentials obtained

4.5.1 NTLM Hashes

Username	NTLM Hash	Found in
Administrator	HASH	HOSTNAME

4.5.2 Passwords

Found in	Corresponds to	Password
HOSTNAME	USER BELONGS	SoyUnaPassword!

4.5.3 Credential's files

Found in	File	Type
HOSTNAME	FILE FROM WHERE IS IT	Example: SSH Priv. Key>
