Offensive Security

Penetration Test Report for Exam

*Templates By Jewel591, Just For OSCP Exam*

[*https://github.com/Jewel591/OSCP-Pentest-Methodologies*](https://github.com/Jewel591/OSCP-Pentest-Methodologies)

*记得删除这部分*

youreamil@email.com

OSID: XXXXX



**©**

All rights reserved to Offensive Security, 2014

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Offensive Security.

# Table of Contents

[Table of Contents 2](#_Toc52884369)

[1. Offensive Security Exam Penetration Test Report 3](#_Toc52884370)

[1.1. Introduction 3](#_Toc52884371)

[1.2. Objective 3](#_Toc52884372)

[1.3. Requirements 3](#_Toc52884373)

[2. High-Level Summary 4](#_Toc52884374)

[2.1. Recommendations 4](#_Toc52884375)

[3. Methodologies 5](#_Toc52884376)

[3.1. Information Gathering 5](#_Toc52884377)

[3.2. Penetration 6](#_Toc52884378)

[3.2.1. System IP: 192.168.1.1 6](#_Toc52884379)

[3.2.2. System IP: 192.168.1.2 10](#_Toc52884380)

[3.2.3. System IP: 192.168.1.3 12](#_Toc52884381)

[3.2.1. System IP: 192.168.1.4 14](#_Toc52884382)

[3.2.1. System IP: 192.168.1.5 16](#_Toc52884383)

# Offensive Security Exam Penetration Test Report

## Introduction

The Offensive Security Lab and Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security course. This report should contain all lab data in the report template format as well as all items that were used to pass the overall exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the lab and exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

## Objective

The objective of this assessment is to perform an internal penetration test against the Offensive Security Lab and 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 the overall 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 course. Use the sample report as a guideline to get you through the reporting.

## Requirements

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

* Overall High-Level Summary and Recommendations (non-technical)
* Methodology walkthrough and detailed outline of steps taken
* Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
* Any additional items that were not included

# High-Level Summary

Student OS-XXXXX Lin was tasked with performing an internal penetration test towards Offensive Security Exam. An internal penetration test is a dedicated attack against internally connected systems. Student OS-XXXXX’s overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Offensive Security’s network. When performing the attacks, Student OS-XXXXX was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, Student OS-XXXXX had administrative level access to multiple systems. All systems were successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

* Exam 192.168.1.1 – Got Local.txt and Proof.txt
* Exam 192.168.1.2 – Got Proof.txt
* Exam 192.168.1.3 – Got Proof.txt
* Exam 192.168.1.4 – Got Local.txt and Proof.txt
* Exam 192.168.1.5 – Got Local.txt and Proof.txt

## Recommendations

Student OS-XXXXX recommends patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

# Methodologies

Student OS-XXXXX utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Labs and Exam environments are secure. Below is a breakout of how Student OS-XXXXX was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

## Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, Student OS-XXXXX was tasked with exploiting the exam network. The specific IP addresses were:

**Exam Network**

* 192.168.1.1
* 192.168.1.2
* 192.168.1.3
* 192.168.1.4
* 192.168.1.5

## Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this exam penetration test, Student OS-XXXXX was able to successfully gain access to 5 out of the 5 systems.

### System IP: 192.168.1.1

#### Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

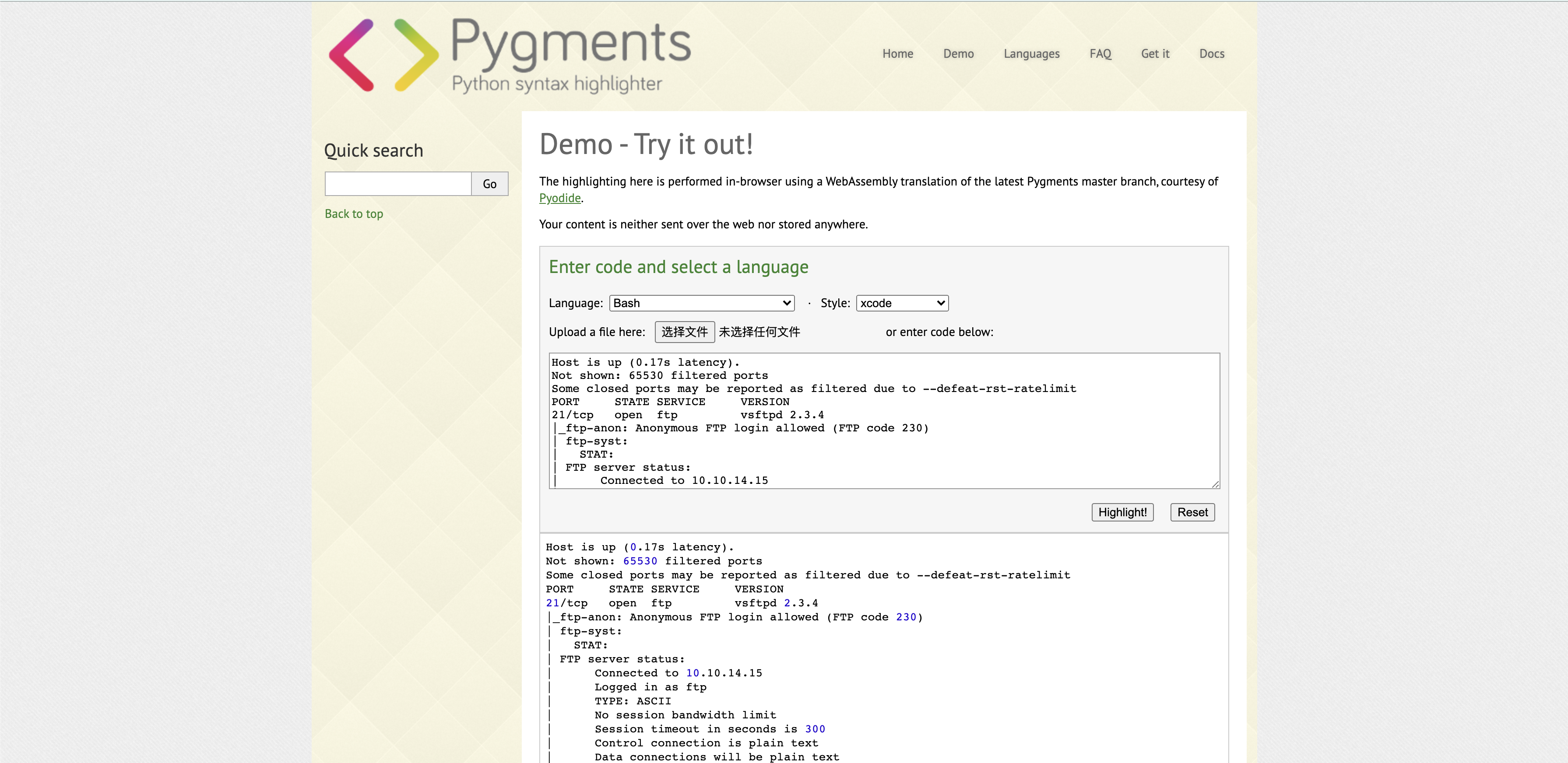
|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168.1.1 | **TCP:** 22,80 |

*------------------------------------------------------------------------------------------*

*代码使用这个网站来格式化，再复制贴入表格，表格底纹选择浅灰:*

[*https://pygments.org/demo/#try*](https://pygments.org/demo/#try)

*------------------------------------------------------------------------------------------*



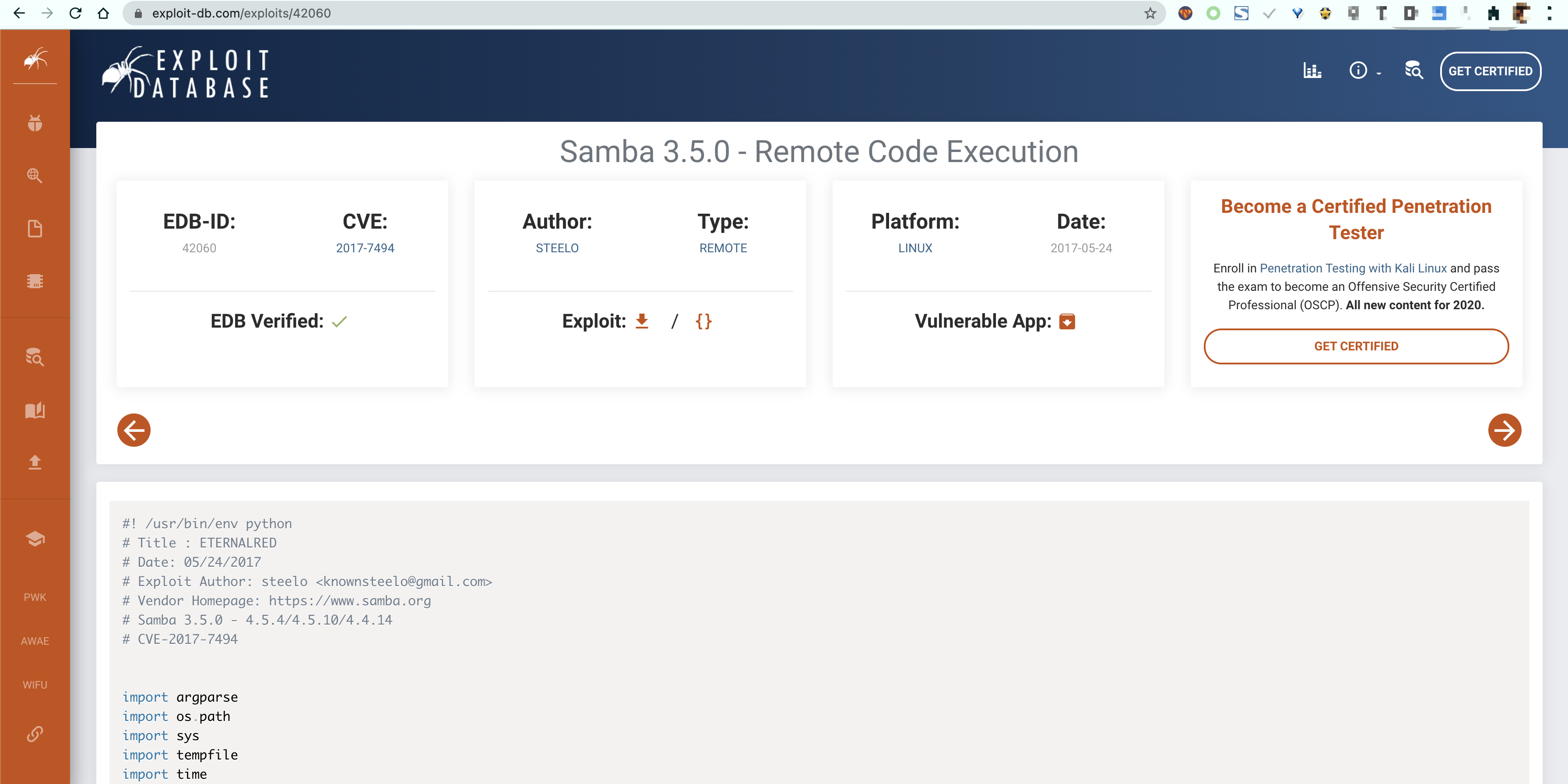
Using Nmap for scanning：

|  |
| --- |
| sudo nmap -A 192.168.1.1 |

The results are as follows:

|  |
| --- |
| Host is up (0.17s latency).  Not shown: 65530 filtered ports  Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  PORT STATE SERVICE VERSION  21/tcp open ftp vsftpd 2.3.4  |\_ftp-anon: Anonymous FTP login allowed (FTP code 230)  | ftp-syst:  | STAT:  | FTP server status:  | Connected to 10.10.14.15  | Logged in as ftp  | TYPE: ASCII  | No session bandwidth limit  | Session timeout in seconds is 300  | Control connection is plain text  | Data connections will be plain text  | vsFTPd 2.3.4 - secure, fast, stable  |\_End of status  22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  | ssh-hostkey:  | 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)  |\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)  139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))  Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel  Host script results:  |\_ms-sql-info: ERROR: Script execution failed (use -d to debug)  |\_smb-os-discovery: ERROR: Script execution failed (use -d to debug)  |\_smb-security-mode: ERROR: Script execution failed (use -d to debug)  |\_smb2-time: Protocol negotiation failed (SMB2) |

Using exploitdb to view Samba 3.x public vulnerabilities:



The details of the vulnerability are as follows:

|  |
| --- |
| https://www.exploit-db.com/exploits/42060 |

… etc.

#### Local.txt Screenshot

*<ScreenShot Here>*

#### Local.txt Content

|  |
| --- |
| 5201c103ce |

#### Privilege Escalation

nmap was found to have s privileges and used the SUID method to elevate them.

Use the following command to elevate privileges:

|  |
| --- |
| nmap --interactive |

Enter the !sh to successfully get the root privileges shell:



#### Proof.txt Screenshot

Proof.txt was successfully obtained:

*<Screenshot Here>*

#### Proof.txt Content

|  |
| --- |
| 99fgcc4 |

#### summary and overview

The initial shell was obtained by exploitdb by …

### System IP: 192.168.1.2

#### Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168.1.2 | **TCP:** 21,80 |

Using Nmap for scanning：

|  |
| --- |
| sudo nmap -A 192.168.1.2 |

The results are as follows:

#### Local.txt Screenshot

#### Local.txt Content

#### Privilege Escalation

#### Proof.txt Screenshot

Get to proof.txt:

#### Proof.txt Content

|  |
| --- |
| a5921bc4 |

#### summary and overview

### System IP: 192.168.1.3

#### Debug Buffer Overflow Poc

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168.1.3 | **TCP:** 4567 |

…etc…

#### Completed Buer Overflow Code

The final code is as follows:

|  |
| --- |
| import sys, socket |

#### Proof.txt Screenshot

Proof.txt was successfully obtained:

#### Proof.txt Content

|  |
| --- |
| a4asfeae1 |

#### summary and overview

### System IP: 192.168.1.4

#### Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168.1.4 | **TCP:** 21,80 |

Using Nmap for scanning：

|  |
| --- |
| sudo nmap -A 192.168.1.4 |

The results are as follows:

#### Local.txt Screenshot

#### Local.txt Content

#### Privilege Escalation

#### Proof.txt Screenshot

Get to proof.txt:

#### Proof.txt Content

|  |
| --- |
| a5921bc487 |

#### summary and overview

### System IP: 192.168.1.5

#### Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168.1.5 | **TCP:** 21,80 |

Using Nmap for scanning：

|  |
| --- |
| sudo nmap -A 192.168.1.5 |

The results are as follows:

#### Local.txt Screenshot

#### Local.txt Content

#### Privilege Escalation

#### Proof.txt Screenshot

Get to proof.txt:

#### Proof.txt Content

|  |
| --- |
| a592 |

#### summary and overview