Satiex’s Penetration Test Report Template

Lab Penetration Test Report

and

Course Module Exercises

Version 1.0  
xx/xx/xxxx

Name

XX-XXXXX

[satiex@satiex.net](mailto:satiex@satiex.net)

# Table of Contents

[Table of Contents 2](#_Toc15575237)

[Introduction 3](#_Toc15575238)

[Objective 3](#_Toc15575239)

[Requirements 3](#_Toc15575240)

[High-Level Summary 4](#_Toc15575241)

[Recommendations 4](#_Toc15575242)

[Methodology 4](#_Toc15575243)

[Reporting 4](#_Toc15575244)

[Information Gathering 6](#_Toc15575245)

[Penetration Test 7](#_Toc15575246)

[Hostname - x.x.x.x 7](#_Toc15575247)

[Summary 7](#_Toc15575248)

[Exploits/Vulnerabilities & Recommendations 8](#_Toc15575249)

[References 8](#_Toc15575250)

[Maintaining Access 9](#_Toc15575251)

[House Cleaning 9](#_Toc15575252)

[Appendices 10](#_Toc15575253)

[Appendix A – Course Exercises 10](#_Toc15575254)

[Intro to … 10](#_Toc15575255)

[1.1.1.1 10](#_Toc15575256)

[Appendix B – PoC Code 11](#_Toc15575257)

[Hostname (Vulnerability Name) 11](#_Toc15575258)

# Introduction

# Objective

# Requirements

# High-Level Summary

## Recommendations



# Methodology

The methodology used in this engagement followed a robust penetration testing methodology based on the Cyber Kill Chain to enumerate and exploit each host. This report details each step …

The methodology is as follows:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **011-magnifying-glass** | Illustration of a black right arrow : Free Stock Photo | **022-bomb** | Illustration of a black right arrow : Free Stock Photo | **020-virus-3** | Illustration of a black right arrow : Free Stock Photo | **028-browser** | Illustration of a black right arrow : Free Stock Photo | **047-user** | Illustration of a black right arrow : Free Stock Photo | **033-file-1** |
| **Reconnaissance** | **Weaponisation** | **Delivery** | **Exploit** | **Privilege Escalation** | **Action on Objectives** |

**Reconnaissance**

The start of every engagement begins with performing reconnaissance on each target. The goal is to…

Tools and techniques used in this stage include …

**Weaponisation**

This stage of the Kill Chain is performed once enough is known about the target from the reconnaissance stage to …

Tools and techniques used in this stage include

**Delivery**This stage of the attack involves delivering …

Tools and techniques used in this stage of the attack include…

**Exploit**This stage of the attack is where a vulnerability in an application …

Tools and techniques used in this stage of the attack include …

**Privilege Escalation**This stage of the attack involves escalation privilege to a …

Tools and techniques used in this stage of the attack include …

**Action on Objectives**This stage of the attack typically occurs only after fully compromising a …

Tools and techniques used in this stage of the attack include c…

## Reporting

In the Penetration Test section of the report, each host has been separated into its own section, with a summary, Kill Chain report detailing each step, and some recommendations. This way of organising the report will allow system administrators to ….

# Information Gathering

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Host IP Address | Hostname | Ports Open | Operating System | Services & Applications |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Penetration Test

## Hostname - x.x.x.x

|  |  |
| --- | --- |
| **Hostname** |  |
| **IP Address** |  |
| **Operating System** |  |
| **Ports Open** |  |
| **Services & Applications** |  |
| **Credentials** |  |
| **Proof** |  |

### Summary

|  |  |
| --- | --- |
| **What worked?** | **What didn’t work?** |
|  |  |

|  |  |
| --- | --- |
| **Kill Chain – Phase 1** | |
| 011-magnifying-glass Reconnaissance |  |
|  |
| 022-bomb Weaponisation |  |
|  |
| 028-browser  Exploit |  |
|  |
| **Kill Chain – Phase 2** | |
| 011-magnifying-glass Reconnaissance | Sometimes, once you gain access to a host, you will want start from the reconnaissance stage again. In these cases, you can break up the report into Phase 1 and Phase 2. |
|  |
| 022-bomb Weaponisation |  |
|  |
| 020-virus-3 Delivery |  |
|  |
| **047-user**  Privilege Escalation |  |
|  |
| 033-file-1  Action on Objectives |  |
|  |

### Exploits/Vulnerabilities & Recommendations

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **Exploit/Vulnerability** | **Description** | **Recommendation** |
|  |  |  |  |
|  |  |  |  |

### References

# Maintaining Access

On each host that was compromised, …

# House Cleaning

Once we had completely compromised a host, …

# Appendices

## Appendix A – Course Exercises

### Intro to …

1.1.1.1 **Research …**

## Appendix B – PoC Code

### Hostname (Vulnerability Name)

#!/usr/bin/python

#

#

Source - https://www.exploit-db.com/...