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

Table of Contents

Introduction

Objective

Requirements

High-Level Summary

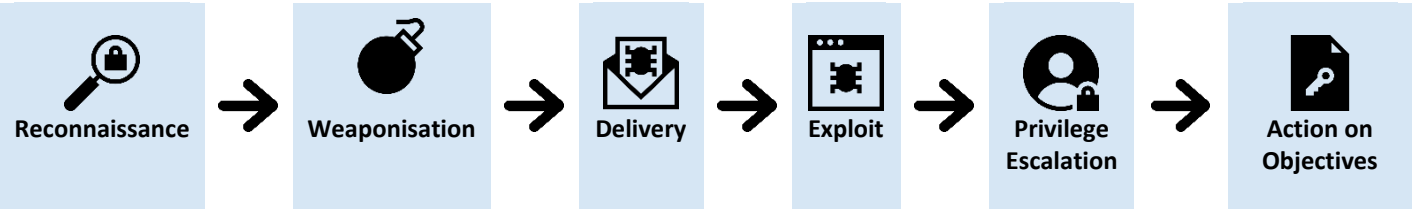
Recommendations

-
-

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:



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	
 Reconnaissance	
 Weaponisation	
 Exploit	
Kill Chain – Phase 2	
 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.
 Weaponisation	
 Delivery	
 Privilege Escalation	

 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/...