# Penetration Test Initial Assessment Template

## Reconnaissance

* Describe the methodology and process you used to perform research and recon on the target (at least one paragraph and screenshots)

Google common password that have been leaked using the username. And use and download the provided database 10GB of password list to try to login. And marlinspike have build-in backdoor vulnerability.

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, application

Description automatically generated

## Scanning / Enumeration

* Describe the scanning and enumeration you performed against the target
* (at least one paragraph and screenshots)

Scan the addresss and know that vtcsec available to the public

Text

Description automatically generatedf

## Gaining Access

* How did you gain access?
* (at least one paragraph and screenshots)

Modify the hosts file in order to access the websites.

Text

Description automatically generated

Use Metasploit to find build-in backdoor of the website

Text

Description automatically generated

Use the reverse payload to try to access the box

Text

Description automatically generated

After setting the LHOST, RHOST and payload. I could exploit the box successfully.

Graphical user interface, text

Description automatically generated

Use the leaked database password and add to rockyou filfe and Using hydra to access ssh attack

Text

Description automatically generated

The password is marlinspike as indicate in the leaded database

Text

Description automatically generated

## Maintaining Access

* What did you do to be persistent on the target host?
* (at least one paragraph and screenshots)

Create sudo user account and reconfigure the password to maintain access.

Text

Description automatically generated

## Covering Tracks

* What steps did you take to remove the evidence you were there?
* (at least one paragraph and screenshots)

Kills the ssh connection and reconfigure the original password

Text

Description automatically generated

## Summary

* Describe what you learned during the course of your attack
  + Screenshots and at least 2 paragraph

First, using the nmpap, and nitko to find the info. During the recons showed that it has build-in backdoor and there’s vulnerability on ssh, you can ssh attack the using hydra. To access the backdoor using metasploite.

A screenshot of a computer

Description automatically generated