PEntest workstation

One machine using different snapshots.

# Overview

Build a vulnerable virtual machine in the format of snapshots to educate students in the field of professional penetration testing. There are many different flags to find in various locations on different snapshots. This will let the user practice different penetration testing tools.

## Draft 1

|  |  |
| --- | --- |
|  | This will be our first draft, ideas might be altered in some way. |

* Aim #1: Build one machine that has multiple snapshots
* Aim #2: Each Snapshot is for practicing exploiting a vulnerability or using different ethical hacking tools.
* Aim #3: Once you exploit the machine using your tool of choice, your presented with a flag. This indicates your exploit was successful.

## Ideas

* Snapshot #1:
  + This snapshot will be based around web exploitation.
  + Ports 80/tcp and 443/tcp will be open for exploitation.
  + There will be a web page available with company details
  + The details will help for some brute force attacks for every snapshot.
    - Flag 1 will be hidden on site.
    - Flag 2 will be in source code or javascript code.
    - Flag 3 will be on https site.
* Snapshot 2:
  + Snapshot one will be based around FTP exploitation.
  + Port 21/tcp will be open.
    - Flags will be hidden and viewable after different brute forcing attacks, anonymous login.
* Snapshot 3:
  + Snapshot one will be based around SSH exploitation.
  + Port 22/tcp will be open.
    - Flag 1 will be in the banner.
    - Flag 2 is Metasploit version attack.
    - Flag 3 is the password you receive with a bruteforce attack
* Snapshot 4:
  + Is based around using burp suite and wireshark.
    - Flags will be hidden in wireshark data
* Snapshot 5:
  + Is based on udp scanning
  + A random udp port will be open.
    - Flags will be hidden as ssh passwords
    - And hidden on the machine somewhere
* Snapshot 6:
  + Is based on using different vulnerability scanners
    - Flags are hidden in misleading places
* Snapshot 7:
  + Is based on breaking hashes.
  + You have to break into user 1 to get roots password
  + And user 2 contains roots username.
    - Flags when you enter root will be ciphered
* Snapshot 8:
  + Is based on gaining a reverse shell.
    - Flags are hidden everywhere.
    - All flags are a section of a flag to make one flag
* Snapshot 9:
  + Is based on firewall exploitation.
    - Get passed the firewall to gain access and retrieve flags
* Snapshot 10:
  + This will be the hardest snapshot and contains elements of all of the previous snapshots