CodePath

Week 8

CS 4760 F18
Christopher Raley

Homework

Week 8 Lab report 10/28 @ 11:59 PM

- Submit on **Collab**

CodePath Assignment

- Submit on **Collab** and **CodePath**

Topics

Week 8

Readings on course website

- Enumeration
- Footprining
- Fingerprinting
- IDOR
- XSS
- CSRF

Goals

- Building off of last week
  - More sophisticated attacks
- Prerequisites
  - Vagrant
  - WPDistillery
    - Able to access “wpdistillery.vm” on Kali and Host

Vagrant/WP

- If you are **stuck**, remove the current VM you have and start a fresh one
  - “vagrant destroy --force”
  - “rm -rf public” <- Need to delete “public” folder
    - In Windows use “del”
- Remember to set version to “4.2” in config.yml file

Vagrant/WP

```yaml
setup:
  wp: true
  settings: true
  theme: false
  plugins: false
  cleanup: false
  # adjust what data you want to be deleted within the cleanup (required `cleanup: true`)
  comment: false
  posts: false
  files: false
  themes: false
```

Metasploit

- Exploitation framework
  - On Kali by default
  - Contains ~1600 exploits for many devices
  - Many different pre-loaded payloads
- Straightforward syntax
  - You will become familiar with this during the Lab

Metasploit

```
Available targets:
  Id  Name
  --  ----
  0   Reflex Gallery 3.1.3

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOST                       yes       The target address
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /                yes       The base path to the wordpress application
  VHOST                       no        HTTP server virtual host

Payload information:

Description:
  This module exploits an arbitrary PHP code upload in the WordPress
  Reflex Gallery version 3.1.3. The vulnerability allows for arbitrary
  file upload and remote code execution.
```

CodePath Assignment

- You will be pentesting **live** targets
- There are 3 targets from the link
  - Red, Blue, Green
- Each has 2 vulnerabilities

ID	Link
Mirror 1	https://35.184.88.145/
Mirror 2	https://104.198.208.81/

Week 8: Globitek Targets

Blue Target

Red Target

Green Target

Welcome to Globitek!

Globitek is a world-wide industry leader with many award-winning products which have become well-known household names. Our staff of experts are dedicated to finding synergies across a wide variety of vertical markets and integrating technology into everyday life.

Find a Salesperson

Use the list below to find a salesperson nearby. We are ready to serve you!

UNITED STATES

Alabama (AL)
- Daron Burke

Alaska (AK)
- Robert Hamilton

Arizona (AZ)
- Irene Boling

Arkansas (AR)
- Elizabeth Olson

California (CA)
- Northern California
  Robert Hamilton
- Southern California
  Sherry Trevino

Colorado (CO)
- Irene Boling

Connecticut (CT)
- Barbara Hinckley

Delaware (DE)
- Barbara Hinckley

Florida (FL)
- Daron Burke

Contact Us

Use the feedback form below to let us know how we can serve you better.

Your name:

Your email:

Feedback:

Submit

Home About Globitek Find a Salesperson Contact Login

Log in

Username:

Password:

Submit

Menu

Users

Salespeople

Countries, States, & Territories

Feedback

CodePath Assignment

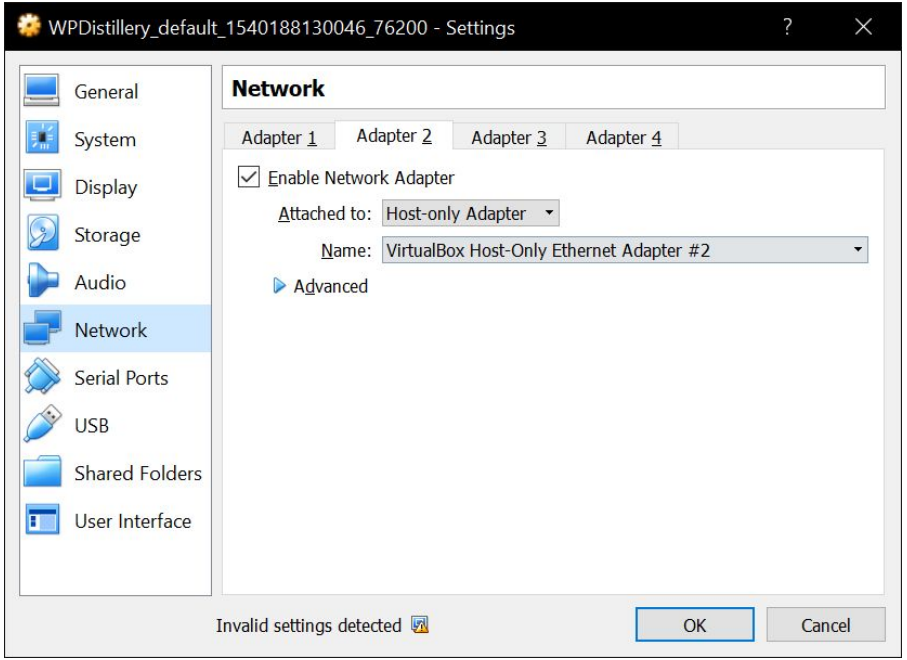
- Each website looks identical (besides the color)
  - However, they each have 2 different vulnerabilities
- Overall you need the carry out the following in **total**:
  - User enumeration
  - IDOR
  - SQLi
  - XSS
  - CSRF
  - Session Hijacking/Fixation

Setup Notes

- This week we are going to use Kali to attack WordPress
- In order to do this we will place Kali and WordPress in the same network, so that they can communicate with each other
- The next couple of slides will show the changes in the VM settings (full walkthrough on CodePath)

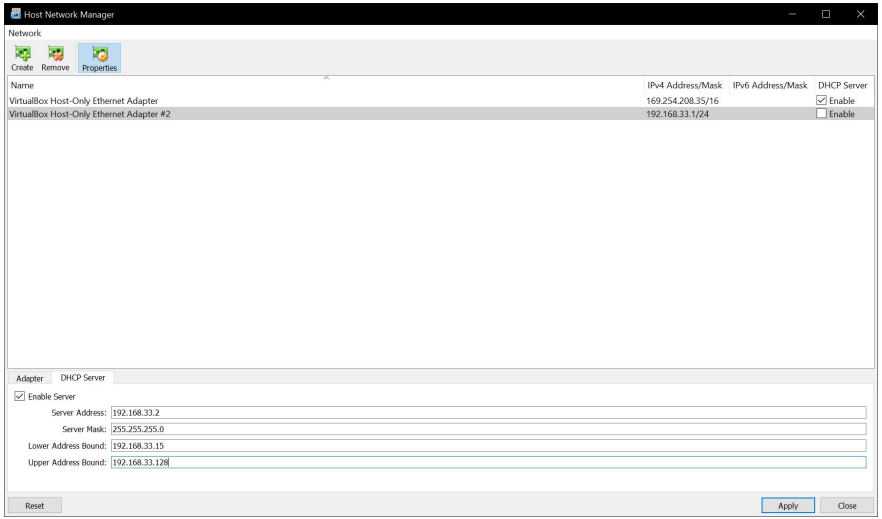
Setup Notes

- Determining the host adapter of the VM
- Doesn’t have to have the name “vboxnet3” like they have in the directions



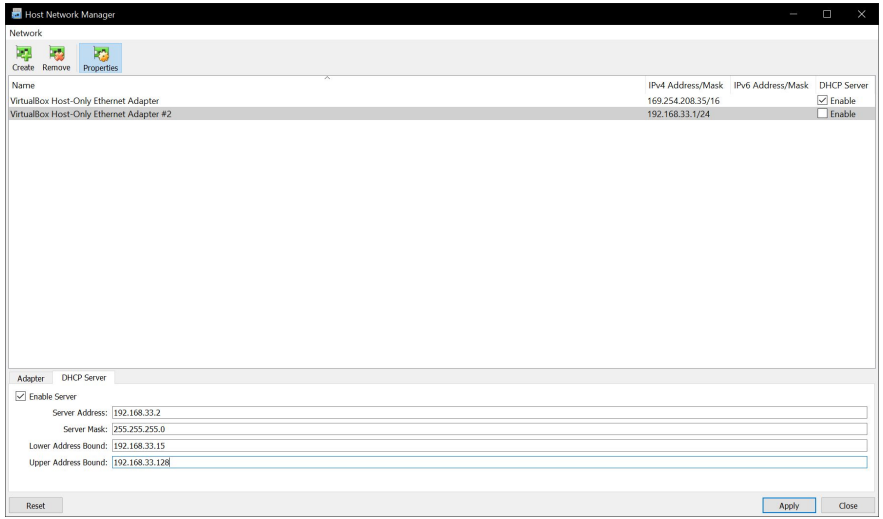
Setup Notes

- In VirtualBox go to:
  - File -> Host Network Manager
- Make sure “Enable Server” in DHCP is checked



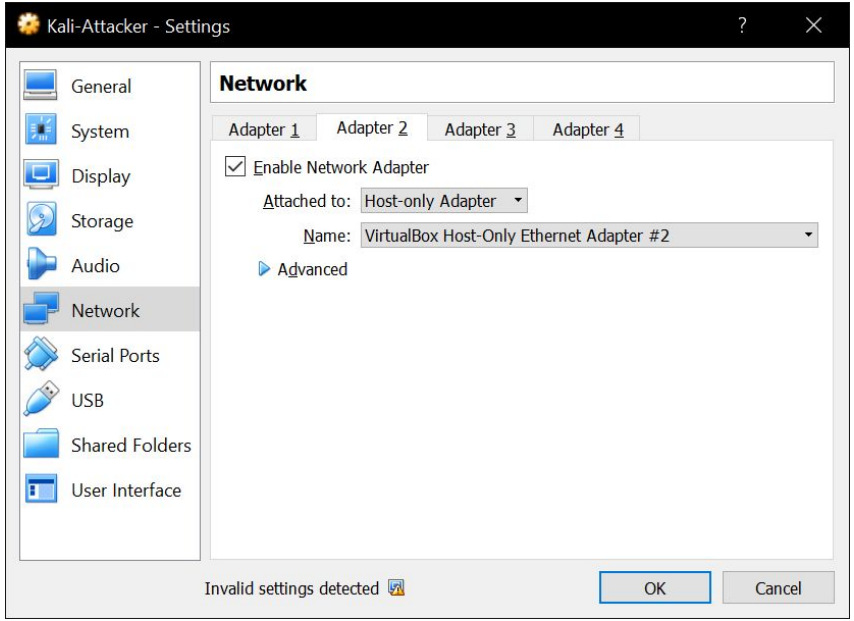
Setup Notes

- Values in “DHCP Server” tab should match up with CodePath directions



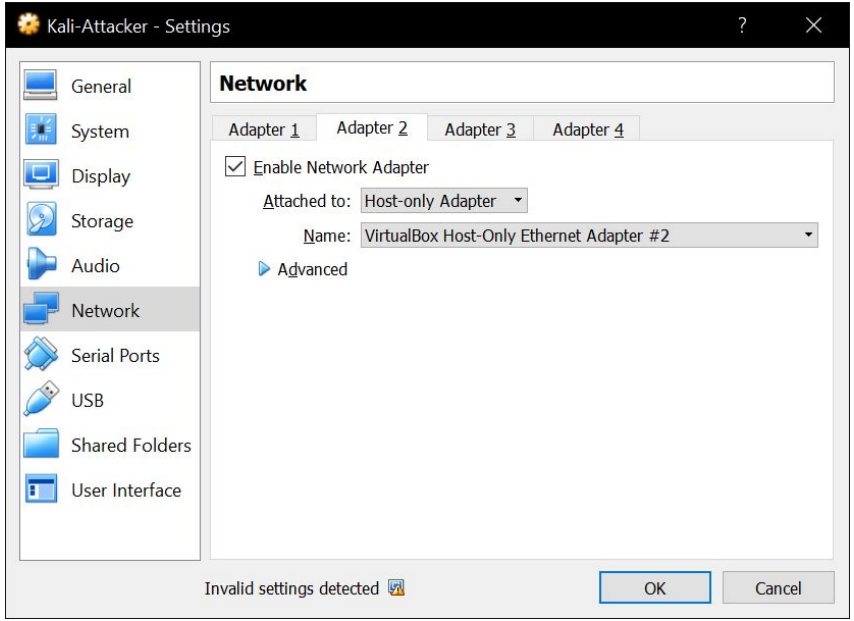
Setup Notes

- Go to Network settings for Kali-Attacker and set the second adapter as shown in the image



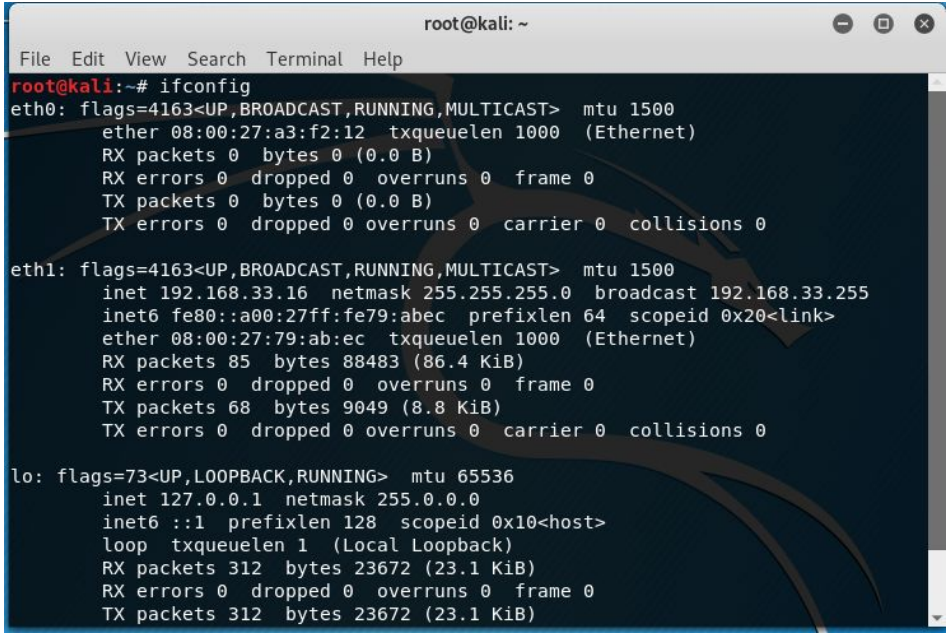
Setup Notes

- **“VirtualBox Host-Only Ethernet Adapter #2”** should be whatever the WPDistillery VM was using for their second adapter



Setup Notes

- This should appear in Kali if everything was setup correctly
  - Important part is the “inet” value



Important Notes

- Necessary to read through everything on the CodePath website carefully
- Start early, some of you **will** encounter technical difficulties
- Windows users must run everything as an administrator
- Document as you go
  - In case you make a mistake

Important Notes

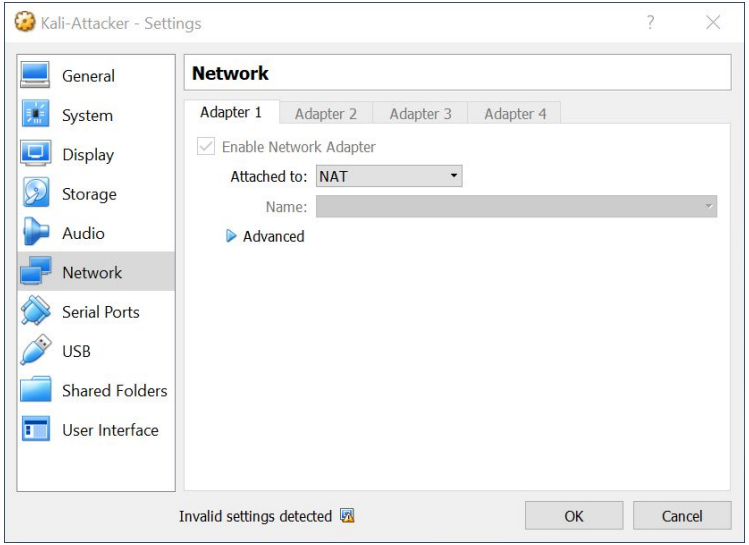
- If you plan on using the course's copy of Kali...
  - You need to run: `apt-key adv --keyserver hkp://keys.gnupg.net --recv-keys 7D8D0BF6`

Important Notes

- If you plan on using the course's copy of Kali...
  - `apt-get update && apt-get upgrade`
    - This will take some time
  - https://guides.codepath.com/websecurity/Running-Kali-Linux-in-VirtualBox

Important Notes

- If you plan on using the course's copy of Kali…



Important Notes

- Kali by default already this installed, so you should be able to run all commands listed in the Lab with no problems

Lab Report

- Walkthrough of Milestone 5/6 in the Lab **and** the Assignment as well
  - View rubric on Collab for details
- Make sure to submit a PDF in the format as described in the write-up
- Try and solve all technical issues you encounter (make sure to document these)

CodePath Assignment Submission

- Following the submission guidelines
  - https://courses.codepath.com/courses/cybersecurity_university/pages/submitting_assignments
- You need to create a public repo with your GitHub account you used to sign up for CodePath
- Read all directions/requirements carefully

Office Hours

Monday / Thursday / Sunday : 5 - 7 PM @ Rice 226