# *IT Security (420-F30-HR)*

# *Lab 02a – Setup & Introduction*

Date assigned: Tuesday, January 28

Date Due: Tuesday, January 28 (end of lab)

**Objectives:**

1. Understand the IT Sec Lab setup

**References:**

420-F30-HR Lab configuration (Moodle – Reference Material)

**To be handed in:**

1. Your ***username*\_F30\_L01b\_LabEnv** doc should be filled in and uploaded to **Moodle**. (individual submission)

# Theory

**Objectives:**

Recap:

1. The CIA Triad of IT Security

Find an article that describes the difference between IT Security and Cyber security that’s consistent with our course material (yes, don’t be quoting some random guy found on the internet):

<URL> (My example [here](https://digital.com/information-security-vs-cybersecurity/#:~:text=IT%20security%20covers%20a%20broader,that%20could%20compromise%20the%20system.), you find your own)

<Your interpretation (not cut and paste): What is CyberSecurity>

<Your interpretation (not cut and paste): What is IT Security? Explain the difference between IT Security and CyberSecurity>

<Your interpretation (not cut and paste): Explain CIA in the context of IT Security, include the terms “asset” and “threat”>

# IP networking

Complete the following table:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IP Address | Subnet mask | CIDR prefix length | First host in subnet | Last host in subnet | # of hosts in subnet |
| 64.55.89.97 |  | 30 |  |  |  |
| 233.192.87.12 | 255.255.248.0 |  |  |  |  |

What’s the maximum prefix size for a subnet that holds 500 hosts? \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Provide the netmask for such a subnet in dotted decimal: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Reference:

A screenshot of a cell phone

Description automatically generated

# IT Security Lab environment

**Objectives:**

Learn:

1. The Lab environment used in this course.
2. Familiarize the student with Kali Linux
3. Familiarize the student with Web Application Vulnerability tools
4. Familiarize the student with DVWA

Warning: You are not to run any of these tools against school equipment. Intrusion detectors will come down hard on you. Do not use this knowledge for evil.

Read the “Lab VM Config” document. Hint: You will find this in MS Teams/W25 IT Sec/General/Files/Class Materials/Reference/

Your goal is to run OWASP ZAP from the Kali linux box (Kalibox), point it to the DVWA running on one of the target machines (checkout the “Lab setup” document, some research and thinking required).

To do this, startup the Kalibox and the VM running DVWA for Configuration 1.

## From Kalibox startup a browser. Type in the URL for the DVWA. (Figure it out)

## Login as admin/password into DVWA and set the security level to the lowest setting. (This should all be review from Web IV.)

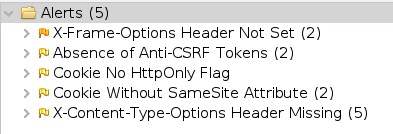
## Run OWASP ZAP from Kalibox targeted to DVWA.

Answer:

## Provide a screen shot of the DVWA security setting to low

## 

## Provide a screen shot of the vulnerabilities discovered by OWASP ZAP on the DVWA.



## Research and explain in a sentence or two. What is the OWASP ZAP and what is the purpose of it? (Do not cut and paste, use your own words).

<answer>

## Analyze. How would you use a tool like OWASP ZAP if you were a web application developer planning deployment (say , like in a Dev Projects course….)

<answer>

## Research and explain in a sentence or two. What is Kali Linux and what is the purpose of it? (Do not cut and paste, use your own words).

<answer>

## Research and explain in a sentence or two. What is DVWA and what is the purpose of it? (Do not cut and paste, use your own words).

<answer>

## In our lab environment which are the attack machine(s) and which are the targets for the attacks in Configuration 1?

<answer>

## Analyze the lab setup. What are the benefits of setting up the IT Sec lab machines this way instead of having physical servers/hosts (like CSDEV, CSTEST) to play on?

<answer>

# IT Security Lab recon

**Objectives:**

Learn:

1. Host recon
2. Port and Service Recon

Startup up config 1 of your lab environment.

Assume you broke into KaliBox and had no idea what other machines existed in your network.

In order to attack any network, you have to do a reconnaisance. i.e. Find the hosts and the ports that they have open.

You will do this all just from KaliBox

Hints:

ifconfig – cmd line to determine interface configuration

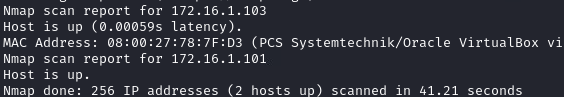
man – cmd line manuals, i.e. man ifconfig

nmap – network map tool

## Figure out what subnet you’re in.

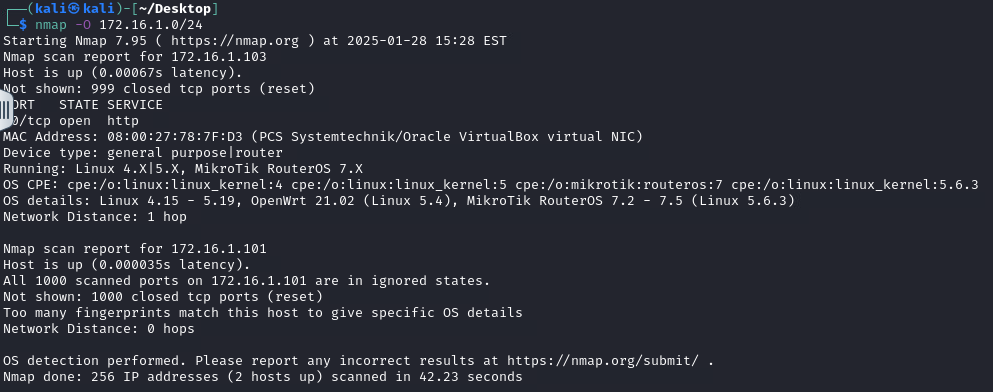


## Scan that subnet for hosts.



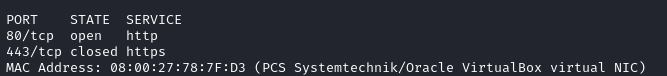
## Using nmap determine what OS is running on each host. [hint](https://nmap.org/book/man-os-detection.html)

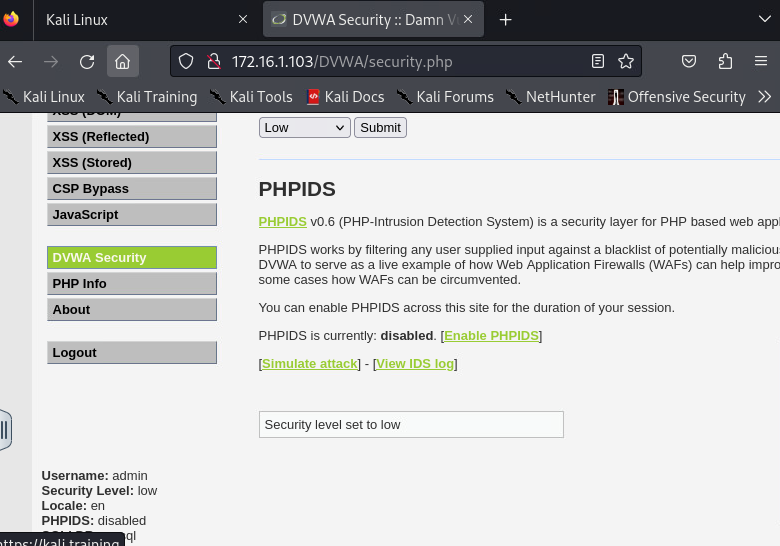
Fill in the following table:



|  |  |
| --- | --- |
| Host | OS |
| 172.16.1.101 | Linux 4.X/5.X |
| 172.16.1.103 | MikroTik RouterOS 7.X |
|  |  |
|  |  |

## Which host is running DVWA?





## How long did the scan take?



**Marking Scheme**

|  |  |  |
| --- | --- | --- |
|  | **Mark** | **Out of** |
| **Part A: Theory Recap** |  |  |
| URL |  | 2 |
| CyberSecurity |  | 2 |
| IT Security and difference |  | 2 |
| CIA |  | 4 |
|  |  |  |
| **Part B** |  |  |
| Subnet table |  | 8 |
| Prefix and netmask |  | 2 |
|  |  |  |
| **Part C: IT Security Lab** |  |  |
| OWASP ZAP Run |  | 2 |
| DVWA screen shot |  | 2 |
| OWASP ZAP screen shot |  | 2 |
| OWASP ZAP purpose |  | 2 |
| OWASP ZAP applied to web projects |  | 2 |
| Kali Linux purpose |  | 2 |
| DVWA purpose |  | 2 |
| Attack vs Target machines |  | 2 |
| Lab Setup Analysis |  | 2 |
|  |  |  |
| **Part D: Networks Discovery** |  |  |
| subnet |  | 2 |
| scan |  | 4 |
| OS table |  | 4 |
| DVWA |  | 2 |
| duration |  | 2 |
|  |  |  |
| English/Handed in properly |  | 4 |
| **Total** |  | **56** |