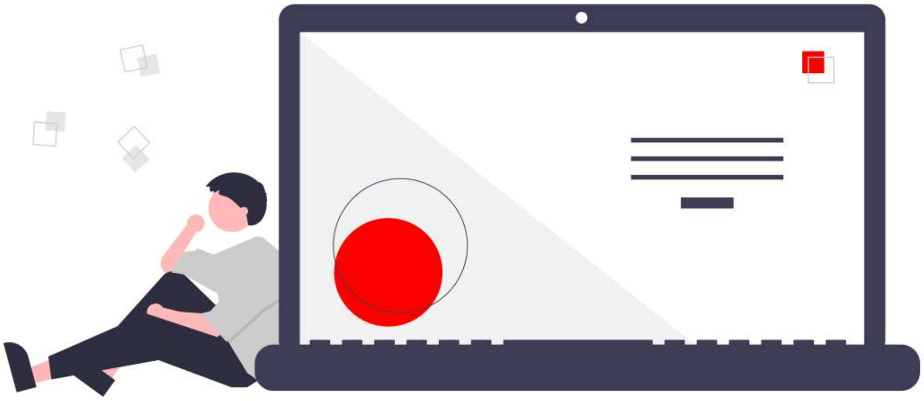
Secure IDE for Red Teaming



COMPX576 – Programming project

Venkatasubramanian Sankaranarayanan

Student ID: 1649356

Table of contents

Project proposal

Introduction

We all know that there are Integrated Development Environment customized testing environment for Software Development. What about Security testing? Here I have proposed a secure environment for practicing various attacking skills for Red teaming with few challenges. It can help attackers enhance their skills in various attacking methodologies inside a secure environment without disturbing the real world devices.

Methodology

I am including the methodologies, which include developing the environment, customization, deployment and testing.

1. Choosing suitable Operating system for the room (environment)
2. Setting up server
3. Installation of LAMP stack architecture
4. Building CMS (Content Management System) on top of LAMP stack
5. Creating custom plugin for CMS
6. Implementing Access management to make privilege escalation attack more challenging
7. Creating and hiding relevant 'flags' as a part of the challenge
8. Deployment and testing
9. Final product submission

Requirements

1. Hypervisor – Oracle VirtualBox
2. Operating System – Debian Based architecture
3. Attacking machine (another os in the hypervisor within the NAT network)

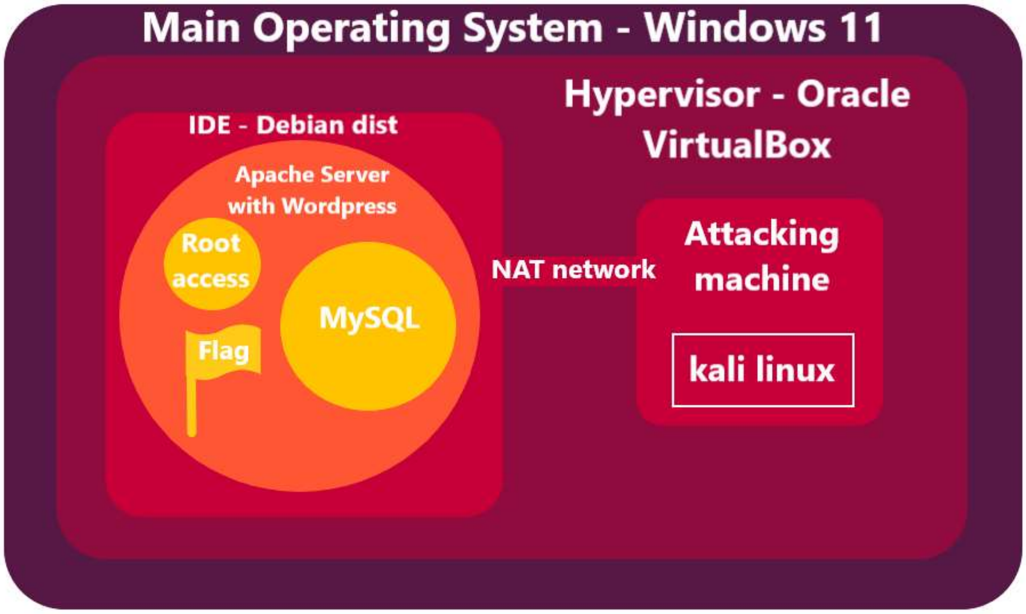
Technologies

1. Hypervisor – Oracle VirtualBox
2. Operating System (Debian based OS)
3. Webserver – Apache/Ubuntu
4. Database – MySQL
5. Scripting Language – PHP/Bash
6. Content management System – Wordpress
7. Secure Shell with RSA/passwd login
8. Networking - TCP/IP and NAT
9. IDE (Code) – nano/Vim

What I am learning for this project?

1. Server configuration
2. Custom CMS plugin development
3. PHP – Server side programming language
4. Access level definition – Custom Linux automations

Architecture


Main Operating System - Windows 11
Hypervisor - Oracle VirtualBox
IDE - Debian dist
Apache Server with Wordpress
Root access
Flag
MySQL
NAT network
Attacking machine
kali linux

Conclusion

This project helps in Cybersecurity training bridging the gap between theoretical and practical implementations especially designed for the Red team. This allows people who have keen interest on red teaming and are ready to take up tough challenges without disturbing the real world entities. Ultimately, it contributes to the Cybersecurity community who are ethically bound to the compliances.

Week – 2

Weekly target

1. Choosing apt Linux distribution
2. Installation of Server and it's configuration
3. Implementation of LAMP Stack over the server
4. Prepare the internal network (Network Address translation and port forwarding)

Challenges

1. Initially I chose Kubuntu for Base Operating system. I noticed that it consumes a lot of graphics for virtualization because of KDE-Plasma setup. The environment crashed repeatedly. Therefore, I chose to go with "A platform which consumes less graphics and allows user to have Super user permission in ease". I chose "kali Linux" which uses GNOME-2, which consumes less graphics.
2. After the installation of Kali Linux, I started to install "Ubuntu Server" where the installation of CMS is going to take place. But the server crashed at first due to misconfiguration issues. Then I re-installed that and started executing the CMS. I was implementing the server installation and setup every time whenever I need to develop and test the plugin code. So, I decided to install "Docker" container.
3. After the installation of Docker, I wrote a custom "yml" file for the docker build. I got errors due to version mismatch. After going through the errors, I noticed that, I have installed V3 of "docker-compose" to build the instance. I downgraded the mentioned service to V2 to create and run the instances.

Conclusion

Though I faced many challenges, I managed to complete this week’s tasks. It helped me to learn a new technology “Docker” for container management. The challenges I faced helped me to get to know about how important version of software is.

Week 3-4 Target

Creating custom Plugin for CMS (Wordpress)

References (Week-2)

1. https://appsecexplained.gitbook.io/appsecexplained/scripts/docker-compose.yml-files/wordpress - Docker instance creation for WordPress and Database connection
2. Few YouTube videos on tutorials to install Ubuntu server, Docker and fixing errors.

Week – 3

Weekly target

1. To create an user flag and root flag which must be captured by the attacker

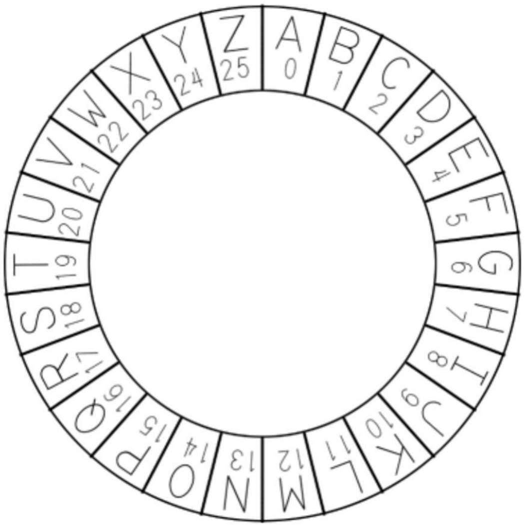
Flag Specification

1. The flag must be encrypted with any algorithm or cipher
2. We must provide hint to decrypt the cipher and algorithm
3. Both local user and root user must have separate flags

Local user flag creation

For Local user, we are implementing ROT13 cipher. For hint, we are going to name the text file which contains user flag as '13.txt'

Encryption	**C = O + 13**
Decryption	**O = C - 13**



Credit - https://www.researchgate.net/figure/Circular-positional-alphabet-and-position-values_fig1_330521841

Root user flag creation

For Root user, we are implementing Vigenère cipher. For hint, we are going to name the text file, which contains root flag as 'le_chiffrage_indéchiffrable.txt'

This encryption method requires a key to decrypt the cipher. So I am going to put a hint below the encryption as 'userflag'.

Encryption	$C_i = (P_i + K_i) \bmod 26$
Decryption	$P_i = (C_i - K_i + 26) \bmod 26$

Challenges faced

1. Understanding and implementing the cipher and encryption techniques. Written code for the above mentioned encryptions.

Conclusion

Initially, I was about to complete the CMS plugin creation. Then I decided to create flags first so that it can be with uploaded once the plugin is created. We have few more challenges to face during the development.

Week 4

Weekly Target

1. To write a custom Wordpress plugin with php which can be run over docker container with Ubuntu
2. Test whether the plugin runs and gets an input from the user

Plugin Specs

1. Take input from the user
2. Can take “any” input from the user
    a. This is a processed threat that needs to be exploited by the attacker.
    b. This is termed as “Command Injection Vulnerability”

Code

```
function report_reader_include_file($atts) {
//user logged in
if (!current_user_can('manage_options')) {
return 'You do not have sufficient permissions to access this content.';
}
// get shortcode params
extract(shortcode_atts(array(
'path' -> '',
), $atts));
// $path = sanitize_text_field($path);
// construct the full path
$full_path = ABSPATH . $path;
if (!file_exists($full_path)) {
    return 'The specified file does not exist.';
}
// return the file contents
return file_get_contents($full_path);
add_shortcode('include_report',report_reader_include_file');

//Code needs be sanitized more and few bugs needs to be fixed.
```

Week 5

Weekly Target

1. Complete the PHP code and sanitize the code more
2. Deploy and execute it under wordpress environment

Challenges faced

1. Faced challenges with logic of the program and keywords (As I am learning php now)
2. Deployed in wordpress environment which has problem with Docker container

Requests submitted

1. To help with the Docker container version issue via mail

Overall progress

This code is the base code for the entire application which is the entry point for the attacker to access the machine. So I'm concentrating it on more to better experience and making sure no other vulnerability other than scope is open.

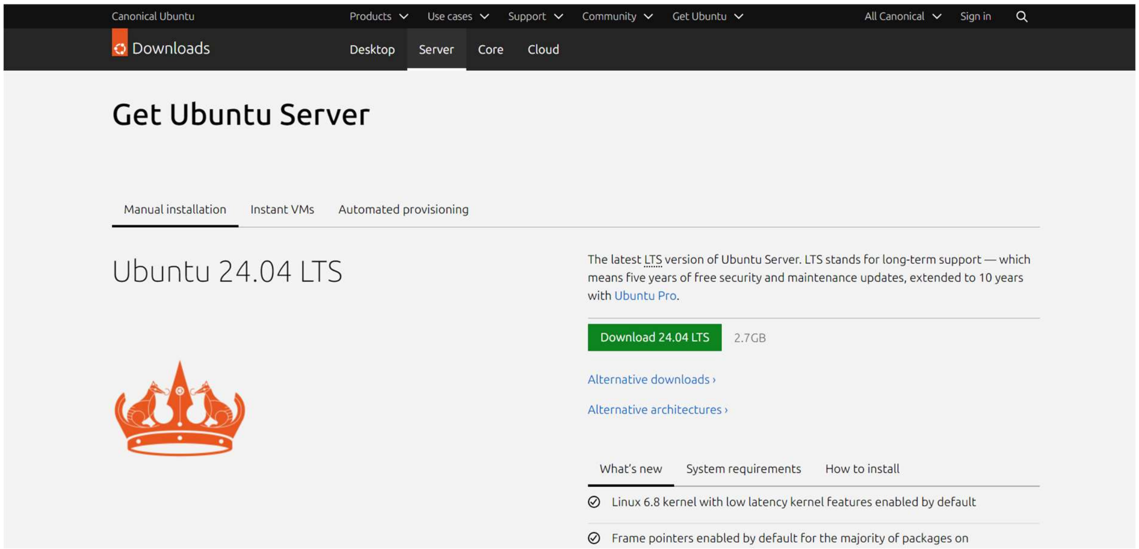
Week 6

Weekly Target

1. Setting up Ubuntu server for opening “Local File inclusion” vulnerability

Challenges faced

1. Version compatibility issues with Docker and Wordpress



Get Ubuntu Server

Ubuntu 24.04 LTS

The latest LTS version of Ubuntu Server. LTS stands for long-term support — which means five years of free security and maintenance updates, extended to 10 years with Ubuntu Pro.

- Linux 6.8 kernel with low latency kernel features enabled by default
- Frame pointers enabled by default for the majority of packages on

Overall progress

This Ubuntu server port forwards the current running Wordpress site in Docker to the other systems in the internal network with the NAT 10.0.2.0/24 with DHCP. It will be open for the attacker to scan and gain access the running Wordpress site.

Week 7

Changes in the project

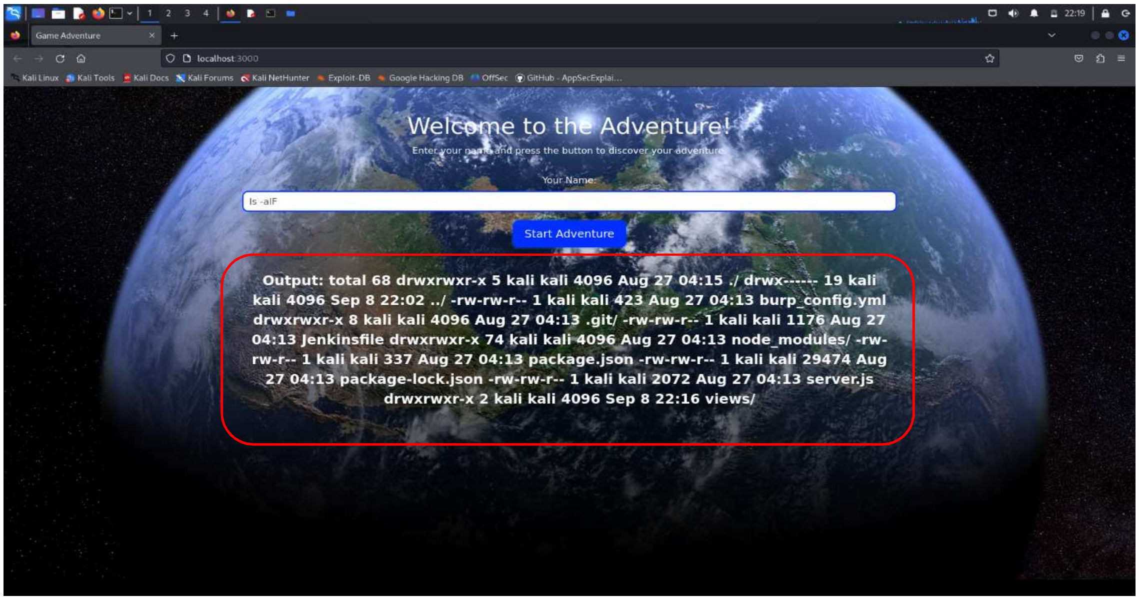
1. Used Jenkins instead of WordPress inside Docker.
2. Used Node instead of Ubuntu server for pre-fetched libraries

Things done in the recession week

1. Installed all the required and configured for Jenkins and Node
2. Wrote own “.ejs” file for front-end part
3. Made the frontend like a gamified experience and gave hint for the interrupter.
4. Mentioned as “Enter your name” asking from a “commander”
5. Sanitized input for taking commands and executing it on server
6. Both proper and improper input is given and screenshot is attached below.

Screenshots

Right command



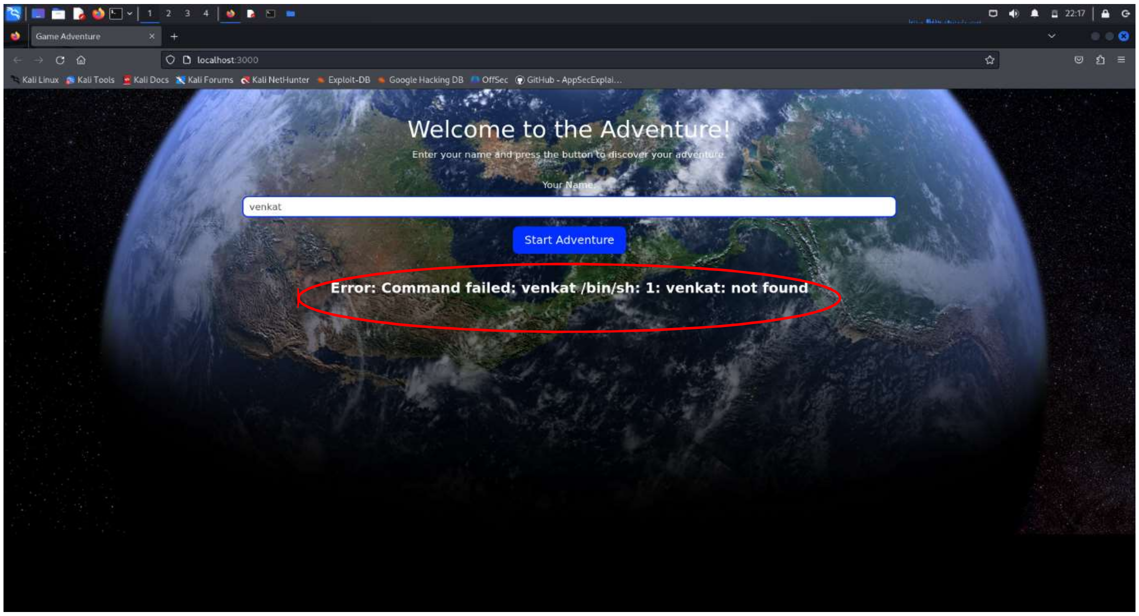
Welcome to the Adventure!

Enter your name and press the button to discover your adventure

Your Name: ls -alF

```
Output: total 68 drwxrwxr-x 5 kali kali 4096 Aug 27 04:15 ./ drwx------ 19 kali
kali 4096 Sep 8 22:02 ../ -rw-rw-r-- 1 kali kali 423 Aug 27 04:13 burp_config.yml
drwxrwxr-x 8 kali kali 4096 Aug 27 04:13 .git/ -rw-rw-r-- 1 kali kali 1176 Aug 27
04:13 Jenkinsfile drwxrwxr-x 74 kali kali 4096 Aug 27 04:13 node_modules/ -rw-
rw-r-- 1 kali kali 337 Aug 27 04:13 package.json -rw-rw-r-- 1 kali kali 29474 Aug
27 04:13 package-lock.json -rw-rw-r-- 1 kali kali 2072 Aug 27 04:13 server.js
drwxrwxr-x 2 kali kali 4096 Sep 8 22:16 views/
```

Wrong command



Welcome to the Adventure!

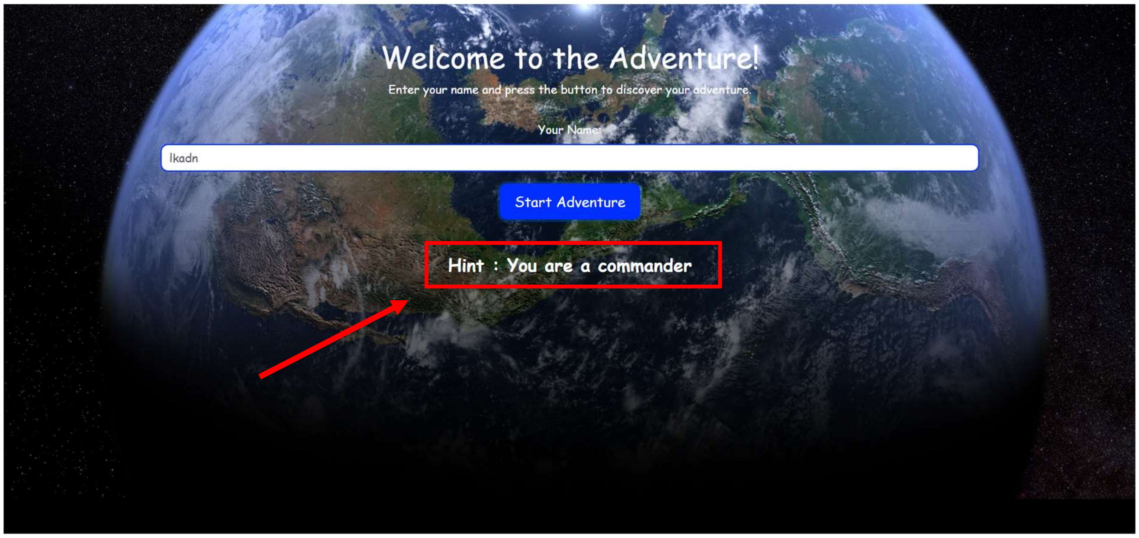
Enter your name and press the button to discover your adventure.

Your Name:

venkat

```
Error: Command failed: venkat /bin/sh: 1: venkat: not found
```

If any other input is given which the input can’t handle the argument, then the below “Hint” will be displayed



Welcome to the Adventure!

Enter your name and press the button to discover your adventure.

Your Name:

lkadn

Hint : You are a commander

Next week target

1. Configure a private “Network Address Translation” network
2. Attach “Flag” files inside the server

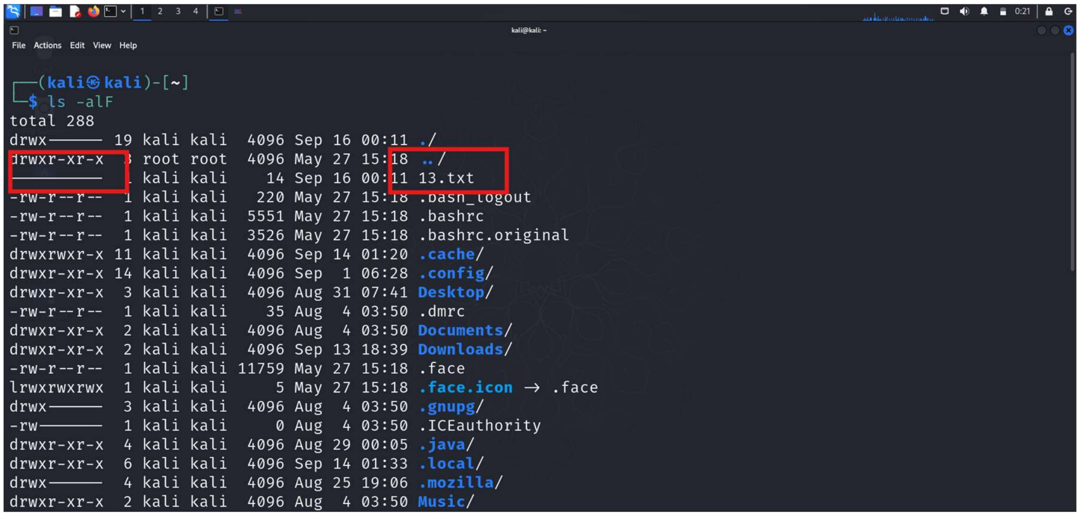
Week 8

Week's Target

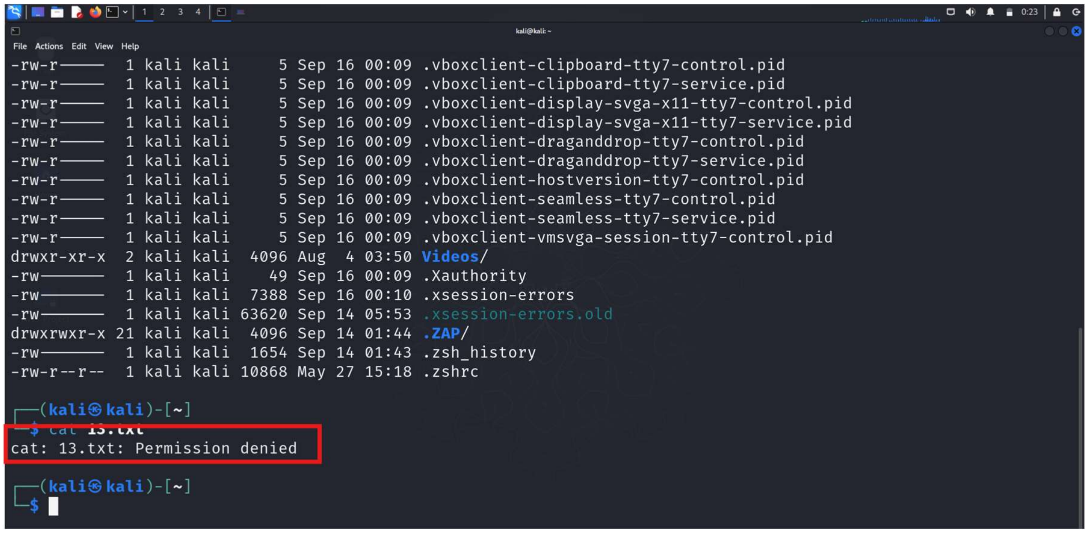
1. Encrypt and place root and user flags on according folder
2. Change access permission to make sure the attacker is set to gain access to super user permission

Achieved targets for the week

1. User flag is placed in the default user of the system. The file is not given any permission viz read, write and execute.



```
┌──(kali㉿kali)-[~]
└─$ ls -alF
total 288
drwx------ 19 kali kali  4096 Sep 16 00:11 ./
drwxr-xr-x  3 root root  4096 May 27 15:18 ../
----------  1 kali kali    14 Sep 16 00:11 13.txt
-rw-r--r--  1 kali kali   220 May 27 15:18 .bash_logout
-rw-r--r--  1 kali kali  5551 May 27 15:18 .bashrc
-rw-r--r--  1 kali kali  3526 May 27 15:18 .bashrc.original
drwxrwxr-x 11 kali kali  4096 Sep 14 01:20 .cache/
drwxr-xr-x 14 kali kali  4096 Sep  1 06:28 .config/
drwxr-xr-x  3 kali kali  4096 Aug 31 07:41 Desktop/
-rw-r--r--  1 kali kali    35 Aug  4 03:50 .dmrc
drwxr-xr-x  2 kali kali  4096 Aug  4 03:50 Documents/
drwxr-xr-x  2 kali kali  4096 Sep 13 18:39 Downloads/
-rw-r--r--  1 kali kali 11759 May 27 15:18 .face
lrwxrwxrwx  1 kali kali     5 May 27 15:18 .face.icon → .face
drwx------  3 kali kali  4096 Aug  4 03:50 .gnupg/
-rw-------  1 kali kali     0 Aug  4 03:50 .ICEauthority
drwxr-xr-x  4 kali kali  4096 Aug 29 00:05 .java/
drwxr-xr-x  6 kali kali  4096 Sep 14 01:33 .local/
drwx------  4 kali kali  4096 Aug 25 19:06 .mozilla/
drwxr-xr-x  2 kali kali  4096 Aug  4 03:50 Music/
```



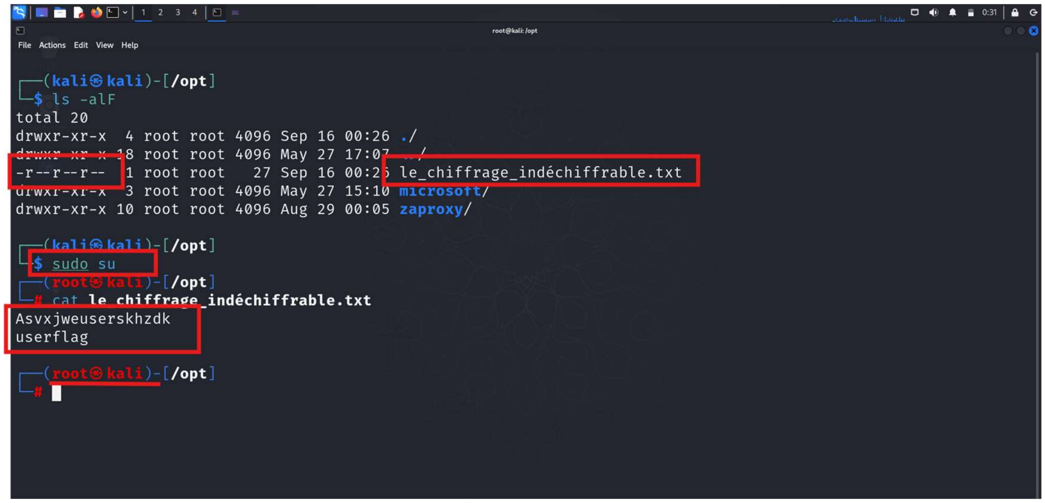
```
-rw-r-----  1 kali kali     5 Sep 16 00:09 .vboxclient-clipboard-tty7-control.pid
-rw-r-----  1 kali kali     5 Sep 16 00:09 .vboxclient-clipboard-tty7-service.pid
-rw-r-----  1 kali kali     5 Sep 16 00:09 .vboxclient-display-svga-x11-tty7-control.pid
-rw-r-----  1 kali kali     5 Sep 16 00:09 .vboxclient-display-svga-x11-tty7-service.pid
-rw-r-----  1 kali kali     5 Sep 16 00:09 .vboxclient-draganddrop-tty7-control.pid
-rw-r-----  1 kali kali     5 Sep 16 00:09 .vboxclient-draganddrop-tty7-service.pid
-rw-r-----  1 kali kali     5 Sep 16 00:09 .vboxclient-hostversion-tty7-control.pid
-rw-r-----  1 kali kali     5 Sep 16 00:09 .vboxclient-seamless-tty7-control.pid
-rw-r-----  1 kali kali     5 Sep 16 00:09 .vboxclient-seamless-tty7-service.pid
-rw-r-----  1 kali kali     5 Sep 16 00:09 .vboxclient-vmsvga-session-tty7-control.pid
drwxr-xr-x  2 kali kali  4096 Aug  4 03:50 Videos/
-rw-------  1 kali kali    49 Sep 16 00:09 .Xauthority
-rw-------  1 kali kali  7388 Sep 16 00:10 .xsession-errors
-rw-------  1 kali kali 63620 Sep 14 05:53 .xsession-errors.old
drwxrwxr-x 21 kali kali  4096 Sep 14 01:44 .ZAP/
-rw-------  1 kali kali  1654 Sep 14 01:43 .zsh_history
-rw-r--r--  1 kali kali 10868 May 27 15:18 .zshrc

┌──(kali㉿kali)-[~]
└─$ cat 13.txt
cat: 13.txt: Permission denied

┌──(kali㉿kali)-[~]
└─$ 
```

The attacker cannot access the file without gaining full access to the user's profile.

2. The user flag is placed inside /opt/ folder of victim machine. The flag file is set to “read-only” by “root”. So the attacker needs to take over super user access to read and decrypt this file.



```
┌──(kali㉿kali)-[/opt]
└─$ ls -alF
total 20
drwxr-xr-x  4 root root 4096 Sep 16 00:26 ./
drwxr-xr-x 18 root root 4096 May 27 17:07 ../
-r--r--r--  1 root root   27 Sep 16 00:25 le_chiffrage_indéchiffrable.txt
drwxr-xr-x  3 root root 4096 May 27 15:10 microsoft/
drwxr-xr-x 10 root root 4096 Aug 29 00:05 zaproxy/

┌──(kali㉿kali)-[/opt]
└─$ sudo su
┌──(root㉿kali)-[/opt]
└─# cat le_chiffrage_indéchiffrable.txt
Asvxjweuserskhzdk
userflag

┌──(root㉿kali)-[/opt]
└─# 
```

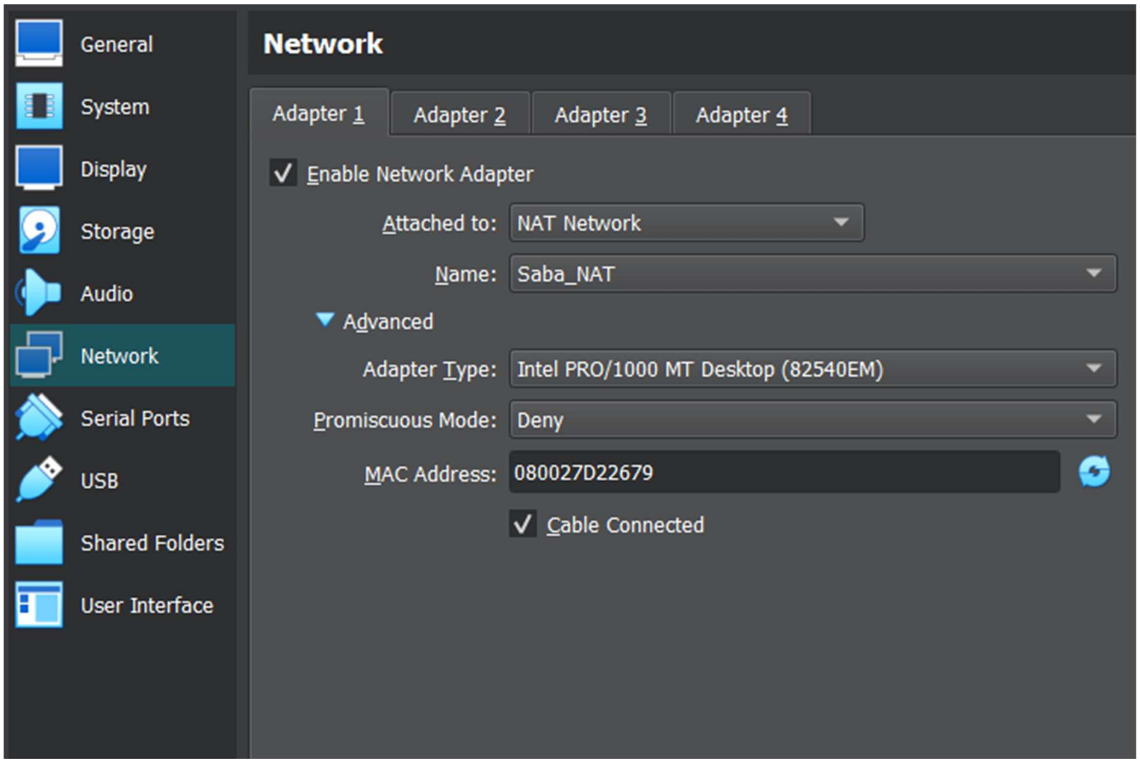
Conclusion

The flag which was created on “Week-3” is placed according to the plan on the victim machine and user permission is also set. The Hint according to plan is also given.

Week 9

Target of the week

1. Configure Network address translation between the local virtual machines
2. Assign DHCP and Port forwarding to Victim machine



Network

☑ Enable Network Adapter

Attached to: NAT Network

Name: Saba_NAT

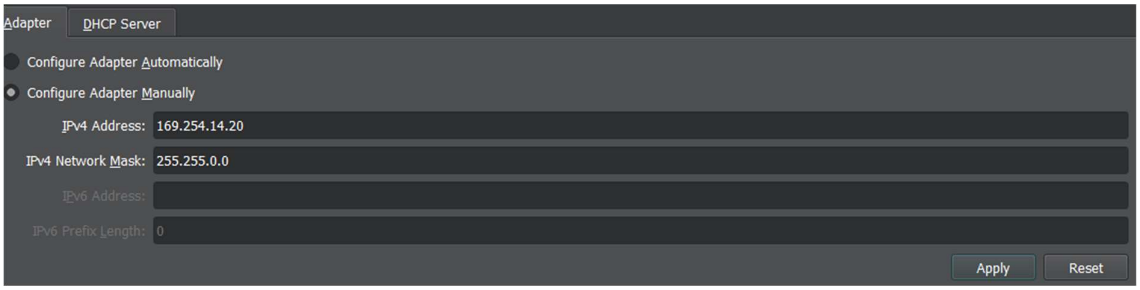
Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027D22679

☑ Cable Connected



○ Configure Adapter Automatically

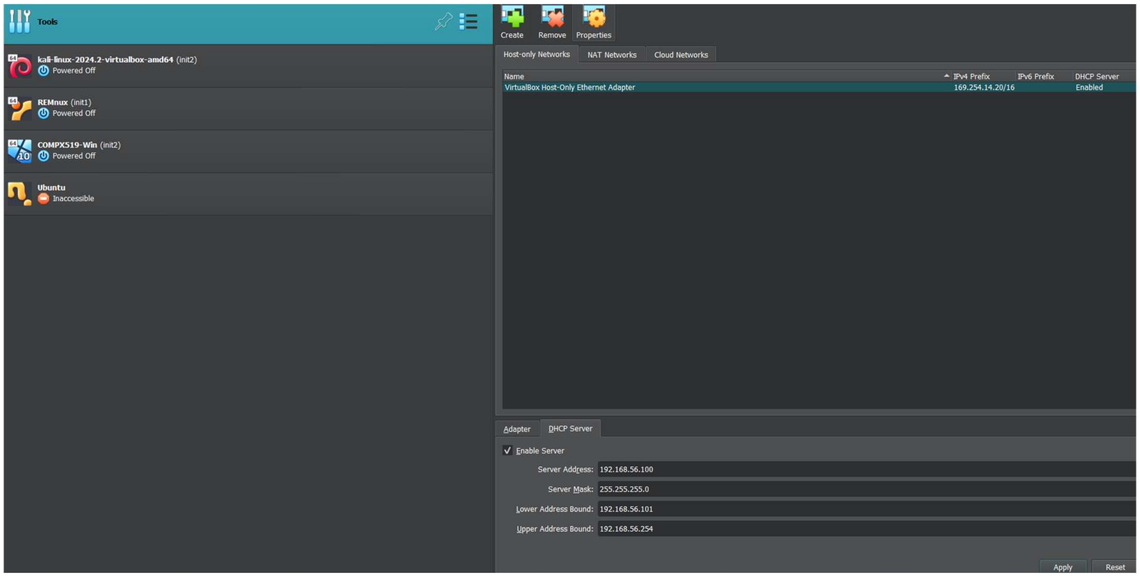
● Configure Adapter Manually

IPv4 Address: 169.254.14.20

IPv4 Network Mask: 255.255.0.0

IPv6 Address:

IPv6 Prefix Length: 0



kali-linux-2024.2-virtualbox-amd64 (init2)
Powered Off

REMnux (init1)
Powered Off

COMPX519-Win (init2)
Powered Off

Ubuntu
Inaccessible

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
VirtualBox Host-Only Ethernet Adapter	169.254.14.20/16		Enabled

☑ Enable Server

Server Address: 192.168.56.100
Server Mask: 255.255.255.0
Lower Address Bound: 192.168.56.101
Upper Address Bound: 192.168.56.254

Conclusion

The network host and Ip configured are done which operates only between the virtual machines. This helps attacker to connect to victim machine, scan, discover and exploit the system