

PACKET-SNIFFING BACKDOOR

Testing

Danny Lieu

A00831407 | MAY 22, 2018

Table of Contents

Test outline.....	2
Test description	4
Test #1	4
Test #2	4
Test #3	5
Test #4	6
Test #5	8
Test #6	9

Test outline

Test #	Description	Tools	Expected Results	Actual Results	Status
1	Root privilege checking for attacker script.	Python3	A message will be printed to ask for root access.	The message is printed for the normal user.	Pass. See test description for more details.
2	Root privilege checking for backdoor script.	Python3	A message will be printed to ask for root access.	The message is printed for the normal user.	Pass. See test description for more details.
3	The port knocking procedure is done with correct sequence.	Python3/ Wireshark	The attacker will knock the backdoor 3 times with given ports.	After 3 knocks, the backdoor is ready to	Pass. See test description for more details.

				receive command.	
4	The attack is able to send encrypted command to the backdoor. After that, the backdoor decrypt the payload to get the command and print to stdout.	Python3/ Wireshark	Looking at Wireshark capture, the payload of the packet should be encrypted. The backdoor is able to print the command to stdout.	The backdoor printed out the command.	Pass. See test description for more details.
5	The backdoor sends the encrypted result of the command to the attacker. After that, the attacker decrypts the payload to get the result of the command and print to stdout.	Python3/ Wireshark	Looking at Wireshark capture, the traffic between backdoor and attacker should be encrypted. The attacker should be able to print the result to stdout.	The attacker printed the result to stdout.	Pass. See test description for more details.
6	The communication between the attacker and the backdoor will be	Python3	After the attacker send "close" command, both	Both the attack and the	Pass. See test description

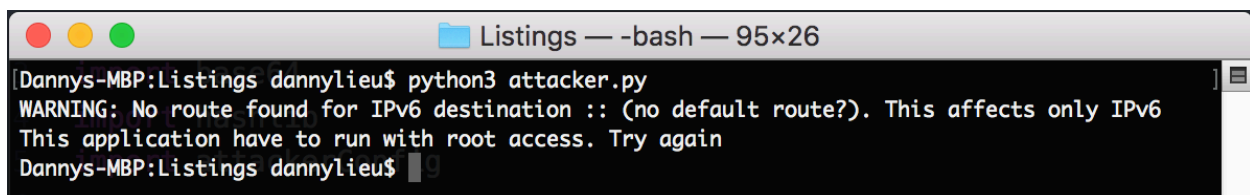
	stopped by “close” command.		script will print an appropriate message and exit.	backdoor printed out the closing messages.	for more details.
--	--------------------------------	--	--	--	----------------------

Test description

Test #1

Root privilege checking for attacker script.

To test for root privilege, the username is dannylieu which is not the root user. We run the script under dannylieu username:



```

Dannys-MBP:Listings dannylieu$ python3 attacker.py
WARNING: No route found for IPv6 destination :: (no default route?). This affects only IPv6
This application have to run with root access. Try again
Dannys-MBP:Listings dannylieu$

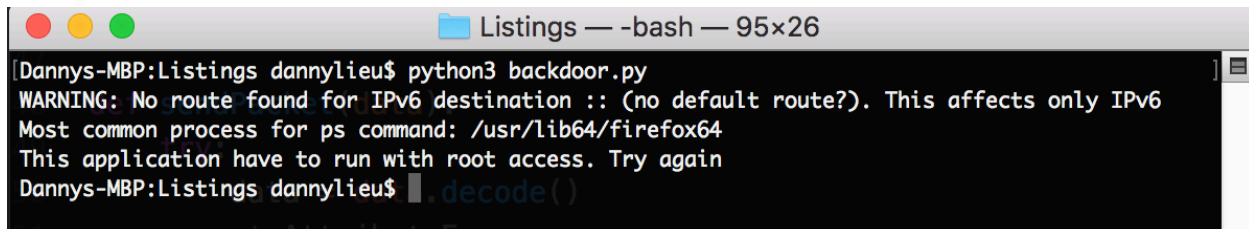
```

The script is unable to run and ask for root access.

Test #2

Root privilege checking for backdoor script.

To test for root privilege, the username is dannyliu which is not the root user. We run the script under dannyliu username:



```

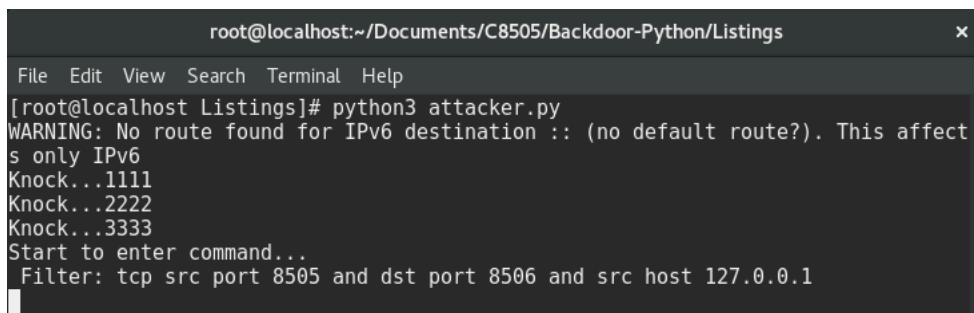
Dannys-MBP:Listings dannyliu$ python3 backdoor.py
WARNING: No route found for IPv6 destination :: (no default route?). This affects only IPv6
Most common process for ps command: /usr/lib64/firefox64
This application have to run with root access. Try again
Dannys-MBP:Listings dannyliu$ .decode()
```

As expected, the script is unable to run because the user is not root user.

Test #3

The port knocking procedure is done with correct sequence.

For port knocking, the configuration files for both attacker and backdoor need to have the same list of knocking ports such as [1111, 2222, 3333]. The listener port on the backdoor side will also need to define in the backdoorConfig in order for the backdoor to listen.



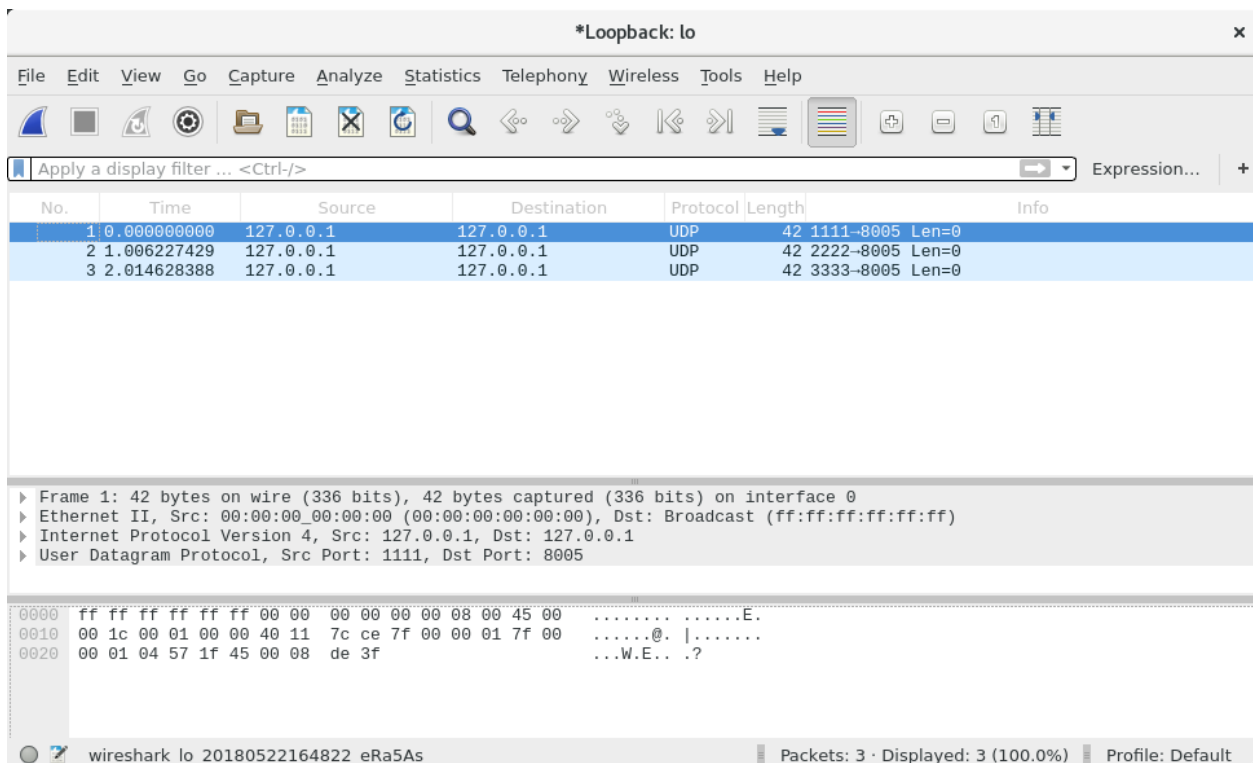
```

root@localhost:~/Documents/C8505/Backdoor-Python/Listings
File Edit View Search Terminal Help
[root@localhost Listings]# python3 attacker.py
WARNING: No route found for IPv6 destination :: (no default route?). This affects only IPv6
Knock...1111
Knock...2222
Knock...3333
Start to enter command...
Filter: tcp src port 8505 and dst port 8506 and src host 127.0.0.1
```

The backdoor will print a message indicating that the authentication procedure is completed.

```
root@localhost:~/Documents/C8505/Backdoor-Python/Listings
File Edit View Search Terminal Help
[root@localhost Listings]# python3 backdoor.py
WARNING: No route found for IPv6 destination :: (no default route?). This affects only IPv6
Most common process for ps command: /usr/lib64/firefox64
127.0.0.1 : Knock 1
127.0.0.1 : Knock 2
127.0.0.1: Knock 3. Authentication succeed.
```

In Wireshark, we can also see the procedure happen. The attacker will send three packets with the source port is 1111, 2222, and 3333 to port 8005 of the backdoor program.



Test #4

The attack is able to send encrypted command to the backdoor. After that, the backdoor decrypt the payload to get the command and print to stdout.

After the pork knocking procedure, the user will be asked to enter a command. The command will encrypt using AES encryption and the **masterkey** (Note: the **masterkey** is the hash using md5). The payload of the packet will contain the password + the actual command.

In Wireshark, the payload of the packet will show as a random combination of character which cannot be read.

```
root@localhost:~/Documents/C8505/Backdoor-Python/Listings
File Edit View Search Terminal Help
[root@localhost Listings]# python3 attacker.py
WARNING: No route found for IPv6 destination :: (no default route?). This affects only IPv6
Knock...1111
Knock...2222
Knock...3333
Start to enter command...
Filter: tcp src port 8505 and dst port 8506 and src host 127.0.0.1
pwd
Result: /root/Documents/C8505/Backdoor-Python/Listings
Result: /root/Documents/C8505/Backdoor-Python/Listings
python3 --version
Result: Python 3.5.3
Result: Python 3.5.3
```

*Loopback: lo

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	UDP	42	1111-8005 Len=0
2	1.008710391	127.0.0.1	127.0.0.1	UDP	42	2222-8005 Len=0
3	2.016390905	127.0.0.1	127.0.0.1	UDP	42	3333-8005 Len=0
4	5.607027112	127.0.0.1	127.0.0.1	TCP	98	8506-8505 [SYN] Seq=0 Win=8192 Len=44
5	5.616963973	127.0.0.1	127.0.0.1	TCP	162	8505-8506 [SYN] Seq=0 Win=8192 Len=108
6	13.013762194	127.0.0.1	127.0.0.1	TCP	118	[TCP Retransmission] 8506-8505 [SYN] Seq=0 ...
7	13.024072230	127.0.0.1	127.0.0.1	TCP	118	[TCP Retransmission] 8505-8506 [SYN] Seq=0 ...

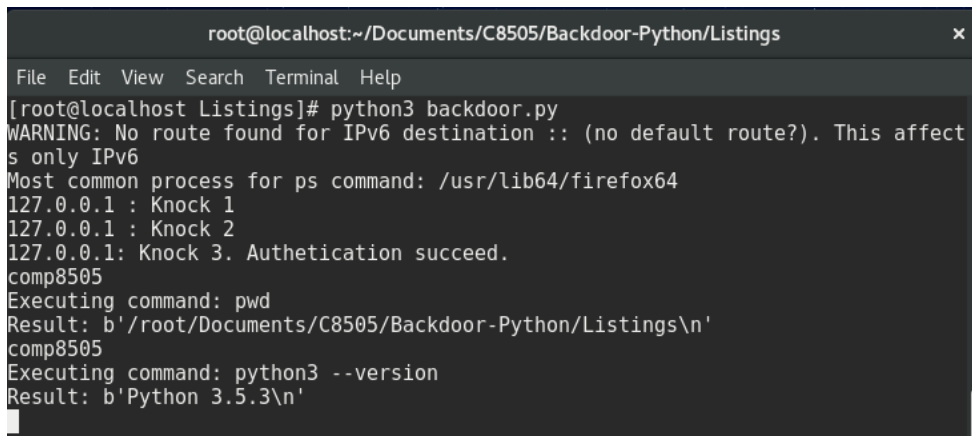
Frame 5: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 0
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 8505, Dst Port: 8506, Seq: 0, Len: 108
Data (108 bytes)

```
0000 ff ff ff ff ff ff 00 00 00 00 00 00 08 00 45 00 .....E.
0010 00 94 00 01 00 00 40 06 7c 61 7f 00 00 01 7f 00 .....@. |a.....
0020 00 01 21 39 21 3a 00 00 00 00 00 00 00 00 50 02 ..!9!... ..P.
0030 20 00 42 8d 00 00 56 4c 6b 78 7a 73 30 6b 69 50 .B...VL kxzs0kiP
0040 47 6f 4d 64 45 41 52 30 76 4c 50 75 53 6f 34 43 GoMdeAR0 vLPuSo4C
0050 6a 42 4b 79 2b 31 73 75 61 67 4f 4d 48 66 6a 76 jBK y+1su agOMHfjv
0060 72 70 49 5a 44 68 50 58 30 78 58 77 62 46 74 6f rpIZdHPX 0xXwbFto
0070 34 37 79 69 56 66 4a 4d 4f 4b 44 4a 57 36 77 66 47yiVfJM OKDJW6wf
0080 37 7a 41 77 70 43 72 7a 58 49 5a 62 6c 75 33 39 7zAwpCrz XIZblu39
0090 45 78 65 42 6a 4e 65 56 48 36 31 7a 77 59 38 6b ExeBjNeV H61zwY8k
00a0 51 3d Q=
```

wireshark_lo_20180522165218_JZWYMY Packets: 7 · Displayed: 7 (100.0%) Profile: Default

On the backdoor side, when it received the packet that contain the command. It will decrypt the packet using AES encryption and the same masterkey.

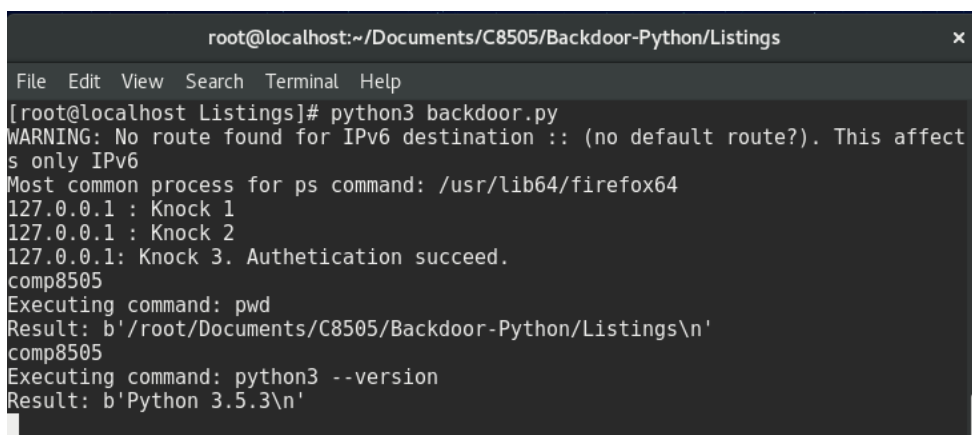
The command is printed to stdout and will be executed.

A terminal window titled 'root@localhost:~/Documents/C8505/Backdoor-Python/Listings' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output shows the execution of 'python3 backdoor.py'. It starts with a warning about IPv6, then prints 'Most common process for ps command: /usr/lib64/firefox64'. It receives three knocks from 127.0.0.1, with the third one succeeding authentication. It then executes 'pwd' and prints the result: '/root/Documents/C8505/Backdoor-Python/Listings'. Finally, it executes 'python3 --version' and prints 'Python 3.5.3'.

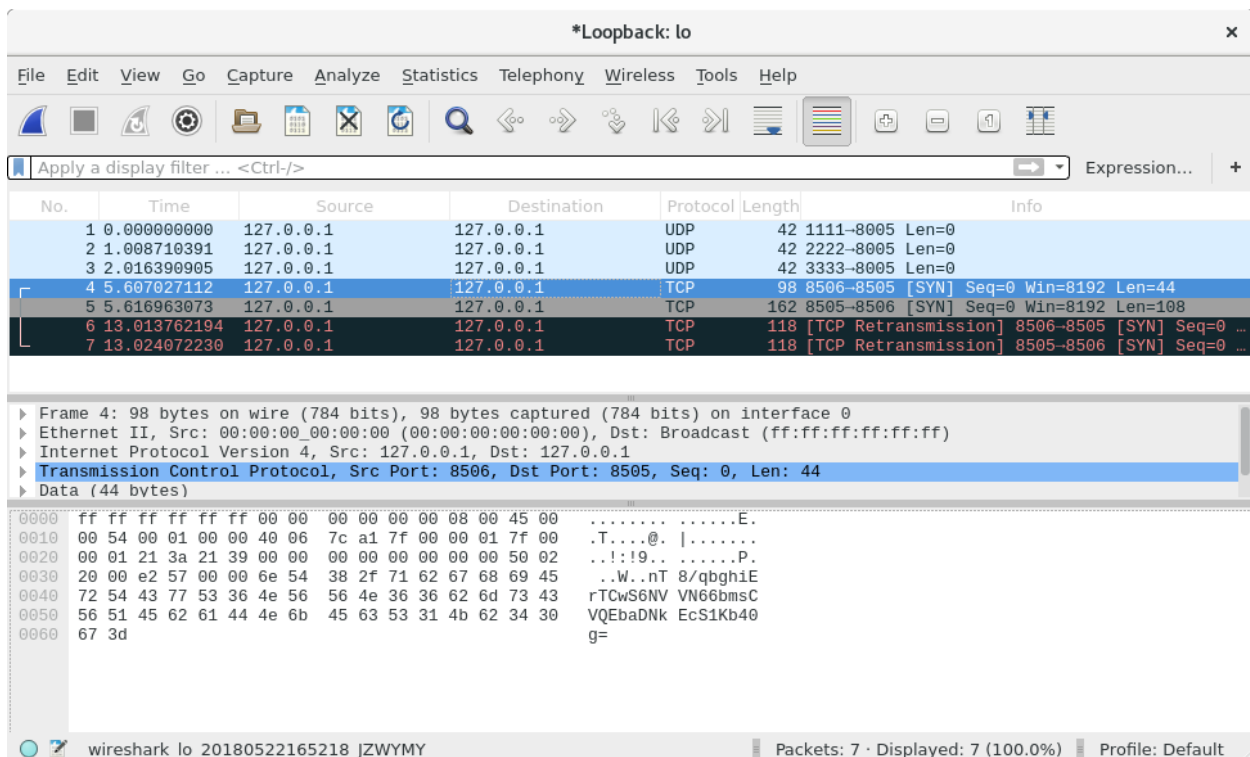
Test #5

The backdoor sends the encrypted result of the command to the attacker. After that, the attacker decrypts the payload to get the result of the command and print to stdout.

After the command is executed, the result will be encrypted using the same encryption scheme when receiving. A copy of the result is also printed to stdout.

A terminal window titled 'root@localhost:~/Documents/C8505/Backdoor-Python/Listings' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output shows the execution of 'python3 backdoor.py'. It starts with a warning about IPv6, then prints 'Most common process for ps command: /usr/lib64/firefox64'. It receives three knocks from 127.0.0.1, with the third one succeeding authentication. It then executes 'pwd' and prints the result: '/root/Documents/C8505/Backdoor-Python/Listings'. Finally, it executes 'python3 --version' and prints 'Python 3.5.3'.

In Wireshark, payload of the packet will show as a random combination of character which cannot be read.



When the attack receives the result, it will decrypt the payload to get the result and print out to stdout.

```

root@localhost:~/Documents/C8505/Backdoor-Python/Listings
File Edit View Search Terminal Help
[root@localhost Listings]# python3 attacker.py
WARNING: No route found for IPv6 destination :: (no default route?). This affect
s only IPv6
Knock...1111
Knock...2222
Knock...3333
Start to enter command...
Filter: tcp src port 8505 and dst port 8506 and src host 127.0.0.1
pwd
Result: /root/Documents/C8505/Backdoor-Python/Listings
Result: /root/Documents/C8505/Backdoor-Python/Listings
python3 --version
Result: Python 3.5.3
Result: Python 3.5.3

```

Test #6

The communication between the attacker and the backdoor will be stopped by “close” command.

Using the close command, both attacker and backdoor script will exit and print out the appropriate closing message.

Attacker

```
root@localhost:~/Documents/C8505/Backdoor-Python/Listings x
File Edit View Search Terminal Help
[root@localhost Listings]# python3 attacker.py
WARNING: No route found for IPv6 destination :: (no default route?). This affects only IPv6
Knock...1111
Knock...2222
Knock...3333
Start to enter command...
Filter: tcp src port 8505 and dst port 8506 and src host 127.0.0.1
close
Attacker closed...
```

Backdoor

```
root@localhost:~/Documents/C8505/Backdoor-Python/Listings x
File Edit View Search Terminal Help
[root@localhost Listings]# python3 backdoor.py
WARNING: No route found for IPv6 destination :: (no default route?). This affects only IPv6
Most common process for ps command: /usr/lib64/firefox64
127.0.0.1 : Knock 1
127.0.0.1 : Knock 2
127.0.0.1: Knock 3. Authentication succeed.
comp8505
Executing command: close
Backdoor closed...
```