Packet Sniffing Backdoor Testing

William Murphy and Benny Wang

Table of Contents

Escalate Privileges

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

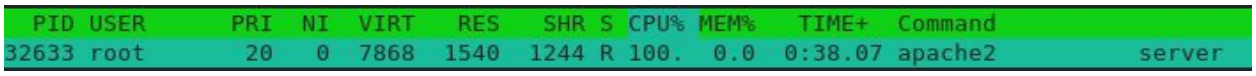
Inputs

Run the backdoor.

Expected Results

The backdoor is run as root.

Test Results



Status

Pass.

Mask Process Name

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

Process

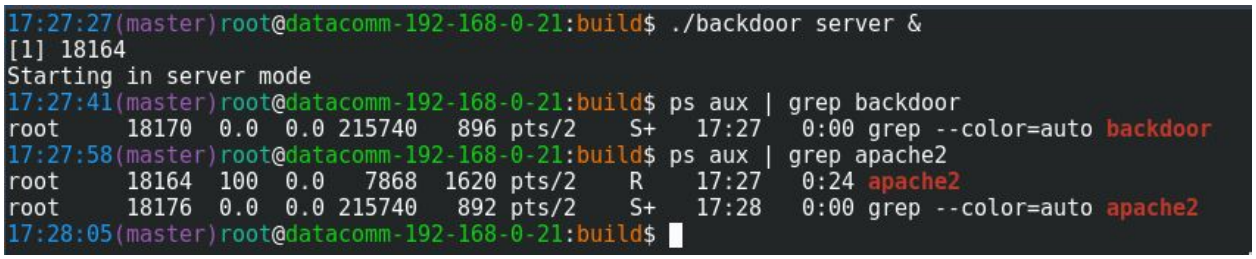
Invoking the program in server mode.

Expected Results

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

Test Results

The screenshot below shows the result.



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

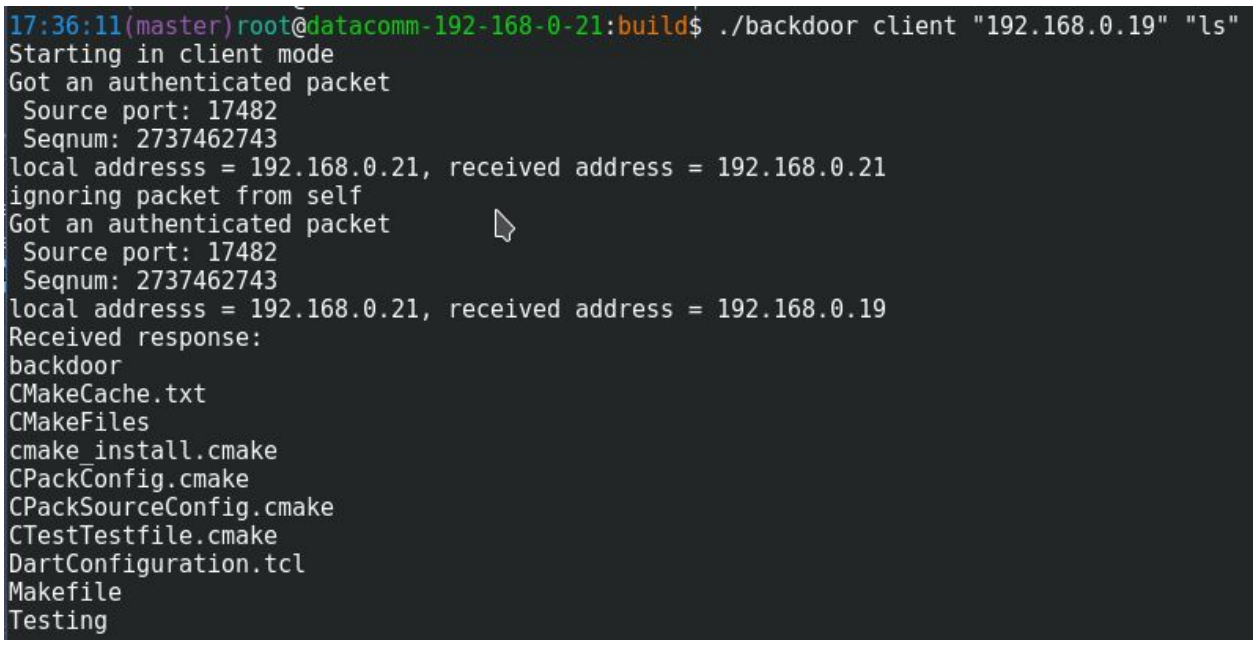
The backdoor server is running on the machine using 192.168.0.19. The client sends a command to the server.

Expected Results

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

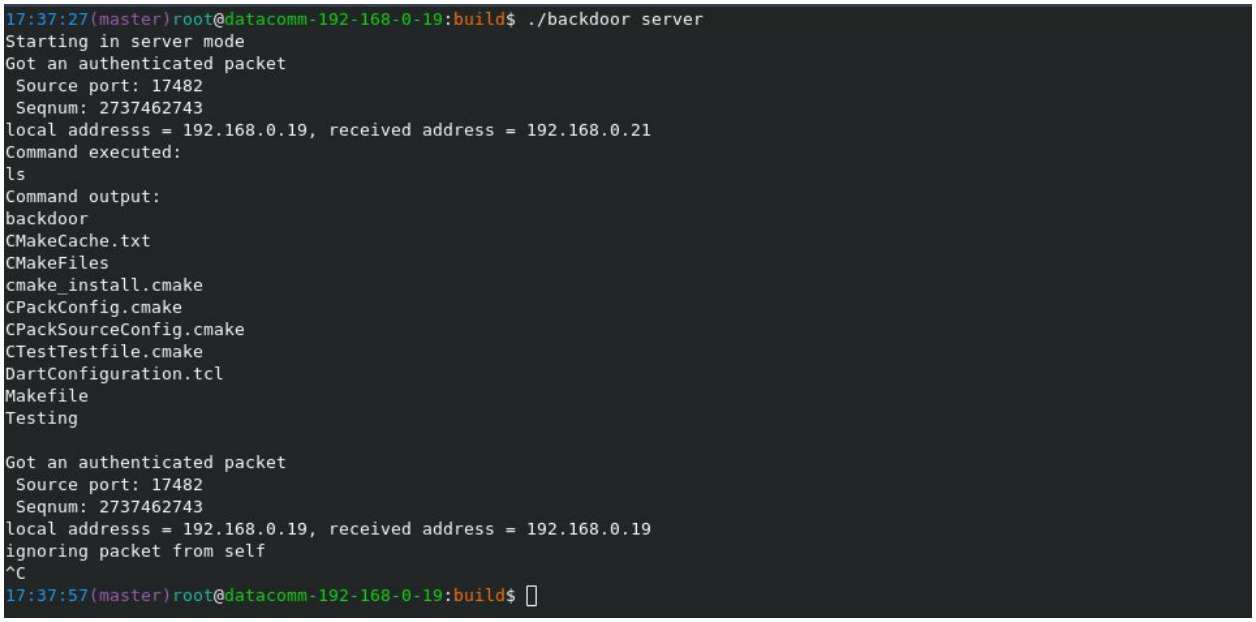
Test Results

Client side after sending “ls” to the backdoor server:



The server replies with the command’s output.

Server side:



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

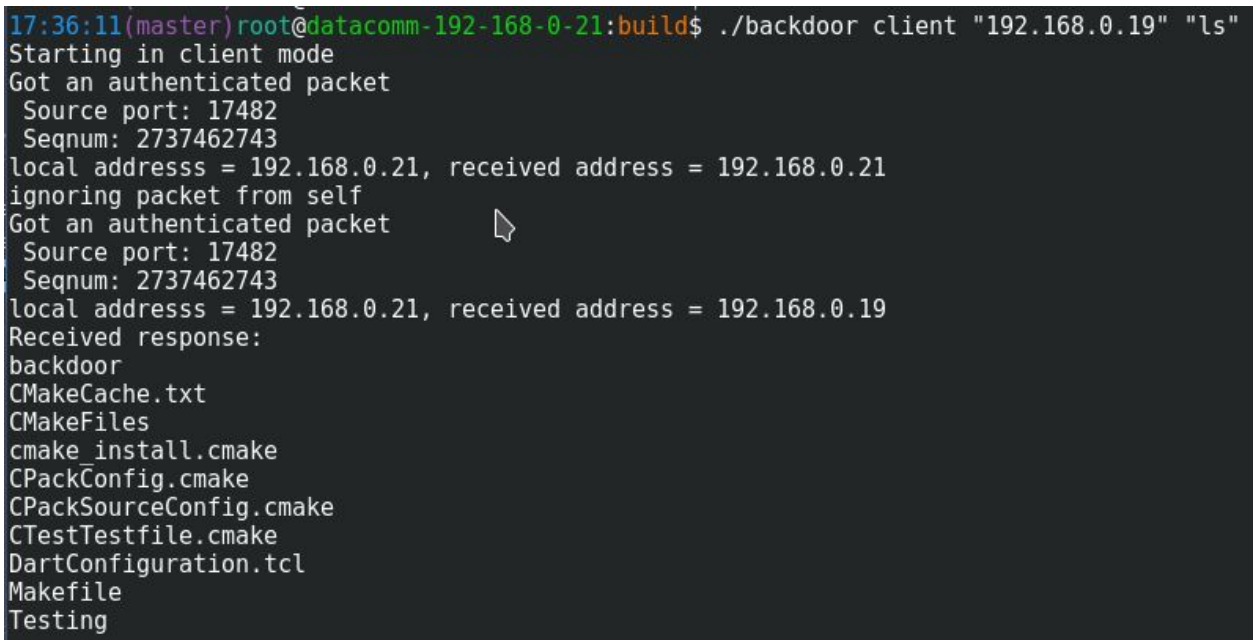
A backdoor is run on machine A. Packets are sent out on the same interface that the backdoor is sniffing.

Expected Results

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

Test Results

The client rejects the packet from itself.



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:

The server does not reply.

Server rejection:

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.