

Christopher Smith

Assignment Example

Abstract

Examine network traffic to determine what information is exposed in transit. Sample traffic is generated and sent. The packets are observed and examined for content. The results demonstrate that all information sent is clear to read by an attacker.

Introduction

Kali Linux will be used in a VirtualBox Virtual machine. Netcat will be used to send and receive unencrypted data. Wireshark will be used for packet analysis.

Netcat listener commands used:

```
nc -l 127.0.0.1 -p 31337
```

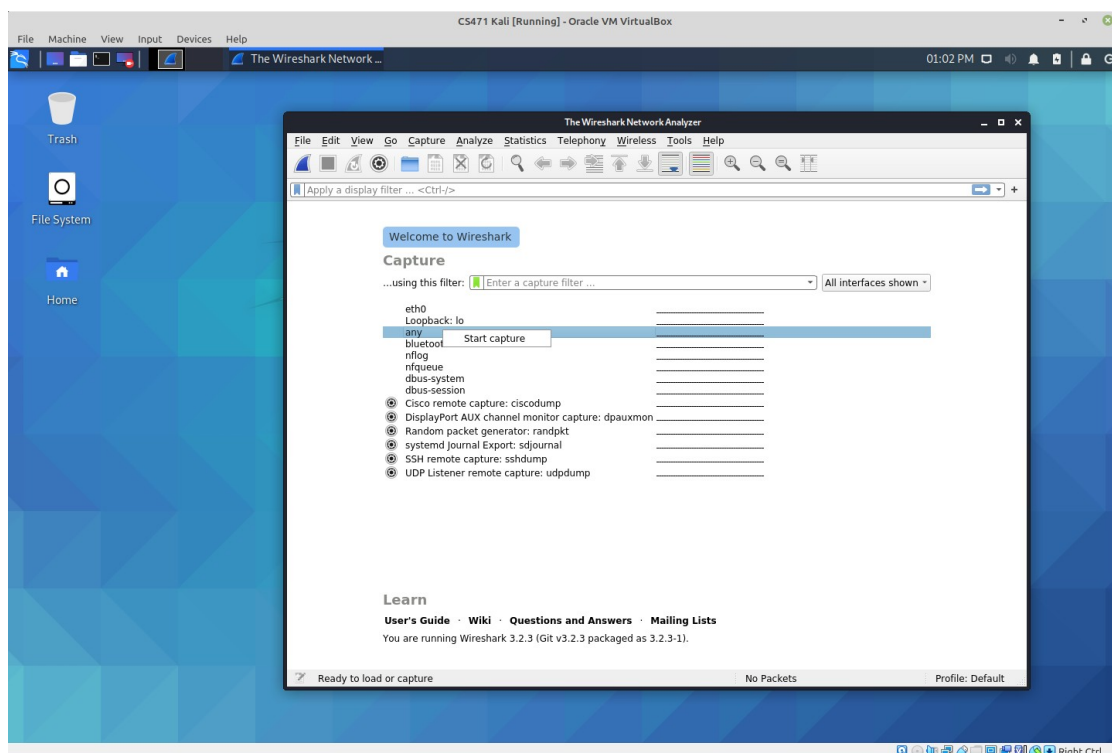
Netcat sender commands:

```
nc 127.0.0.1 -p 31337
```

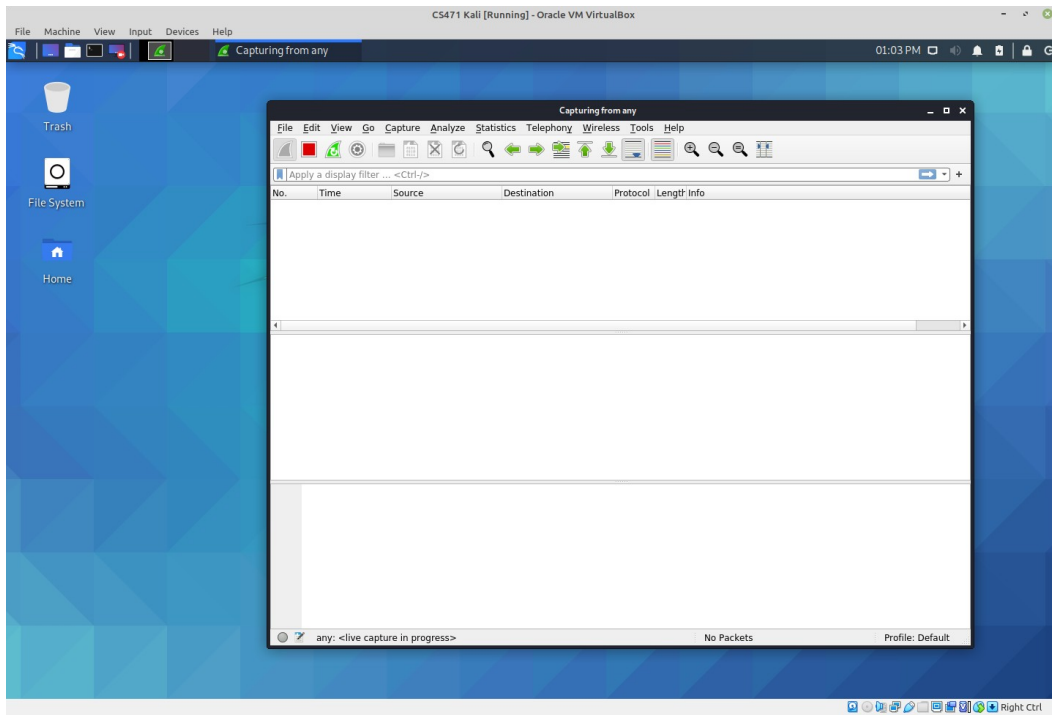
Wireshark run as root while capturing on the 'any' adapter.

Summary of Results

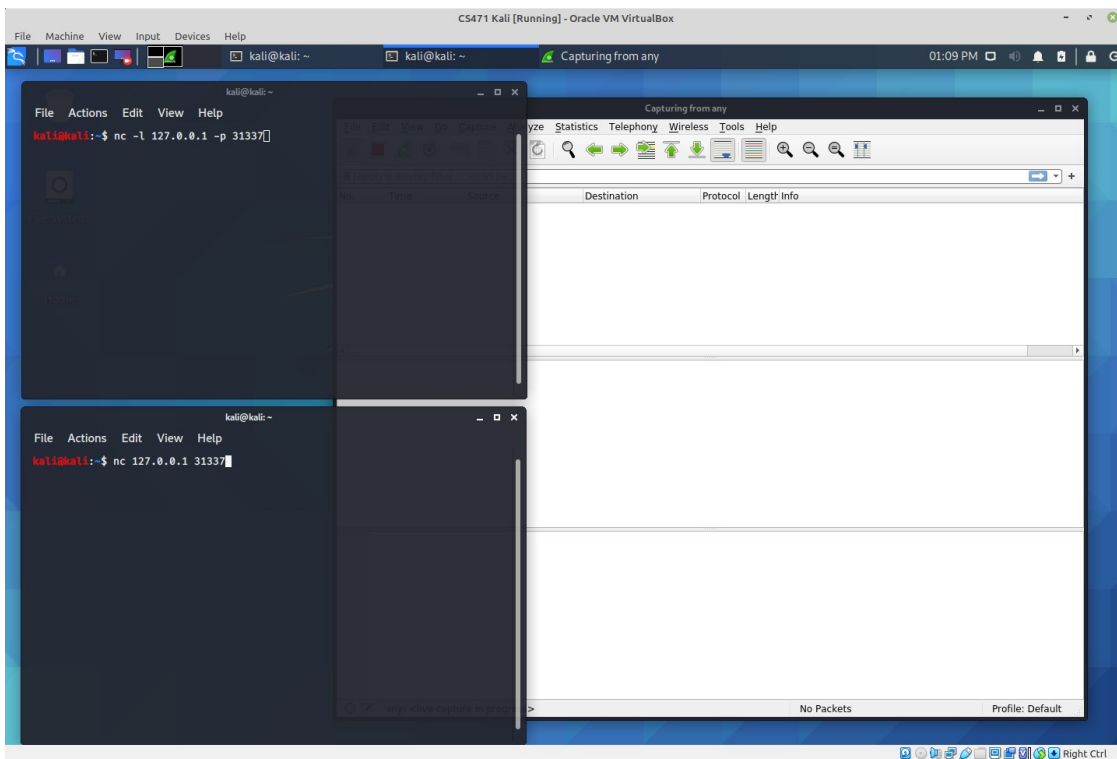
Starting Wireshark in Kali Linux. Selecting the 'any' interface for packet capture.



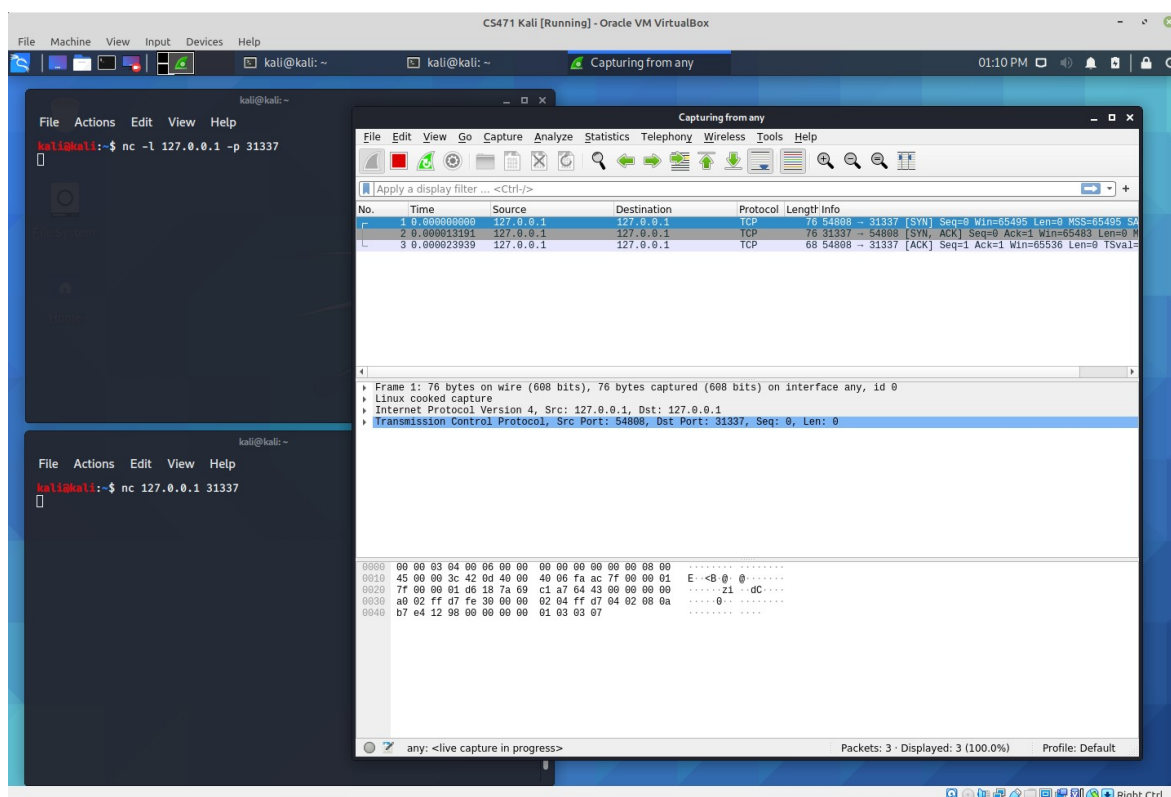
Now Wireshark is listening. No packets heard.



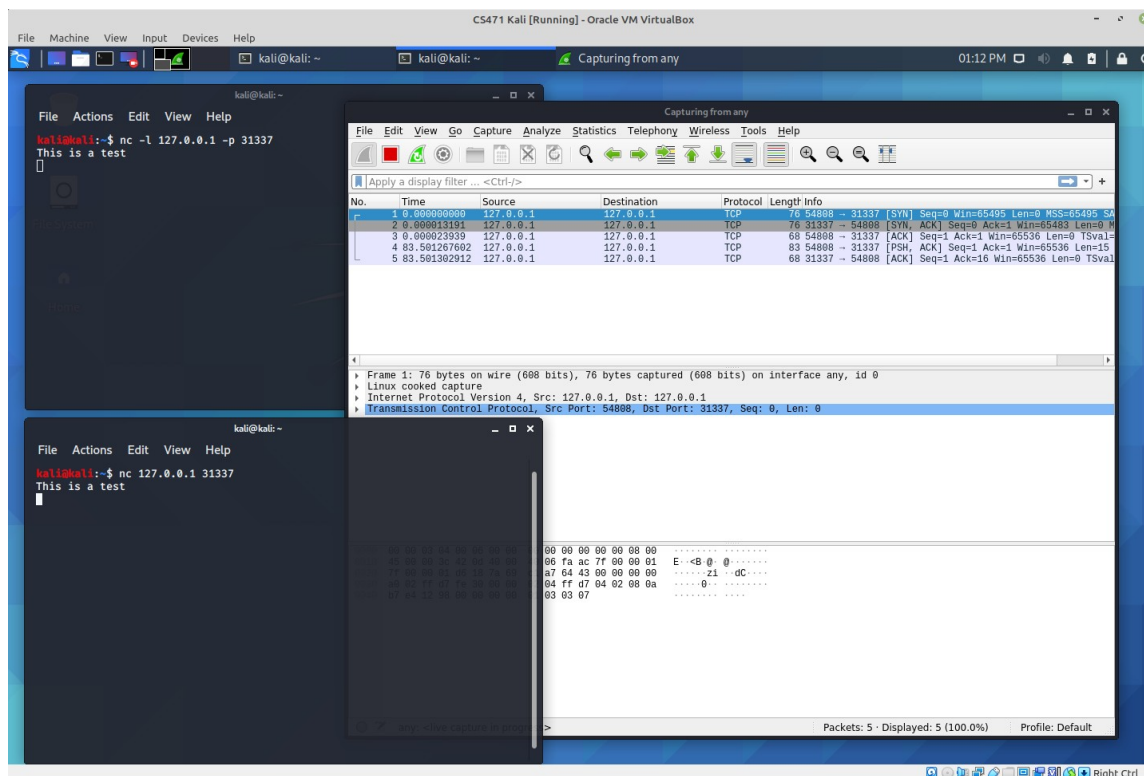
Next open two terminals. One as a netcat listener first, then another as a Netcat sender.



This reveals the TCP setup connection packets, but no intentional data has been sent.



Type some text into the sender terminal. Netcat sends this text to the listener over the network. Wireshark captures these packets also.



Notice the text sent over the network was found in the Wireshark capture. The text was easily intercepted and revealed.

CS471 Kali [Running] - Oracle VM VirtualBox

FileMachineViewInputDevicesHelp

kali@kali: ~kali@kali: ~Capturing from any01:14 PM

Capturing from any

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000...	127.0.0.1	127.0.0.1	TCP	76	54808 → 31337 [SYN] Seq=0 Win=6...
2	0.000...	127.0.0.1	127.0.0.1	TCP	76	31337 → 54808 [SYN, ACK] Seq=0 ...
3	0.000...	127.0.0.1	127.0.0.1	TCP	68	54808 → 31337 [ACK] Seq=1 Ack=1...
4	83.50...	127.0.0.1	127.0.0.1	TCP	83	54808 → 31337 [PSH, ACK] Seq=1 ...
5	83.50...	127.0.0.1	127.0.0.1	TCP	68	31337 → 54808 [ACK] Seq=1 Ack=1...

Frame 4: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface any, id 0

Linux cooked capture

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Transmission Control Protocol, Src Port: 54808, Dst Port: 31337, Seq: 1, Ack: 1, Len: 15

Data (15 bytes)

Data: 54686973206973206120746573740a

[Length: 15]

0000	00 00 03 04 00 06 00 00	00 00 00 00 00 00 08 00
0010	45 00 00 43 42 0f 40 00	40 06 fa a3 7f 00 00 01	E..CB.@. @.....
0020	7f 00 00 01 d6 18 7a 69	c1 a7 64 44 15 3c 5b d2zi ..dD.<[.
0030	80 18 02 00 fe 37 00 00	01 01 08 0a b7 e5 58 c57.....X.
0040	b7 e4 12 98 54 68 69 73	20 69 73 20 61 20 74 65	...This is a te
0050	73 74 0a		st.

Data (data.data), 15 bytes

Packets: 5 · Displayed: 5 (100.0%)

Profile: Default

Right Ctrl

Conclusion

Packets sent over the network are clear to read by any device that intercepts them. Additional measures are required to secure private information.

NOTE TO STUDENTS:

This is an example of the format to use when submitting assignments. Be sure to include more substance than this example.

Abstract: The abstract is a very short executive summary of the entire document. This includes result. 3-4 sentences only. This should clearly summarize the entire purpose and result of the document as succinctly as possible.

Introduction: This includes the tools used and any background information needed to understand your report.

Summary of Results: This includes your work in a *reproducible* way. Explain all of your work here. Include screenshots with descriptions. There should be more words here than pictures....

Conclusion: This should be a cogent explanation of the results. This should explain what the results imply and what the importance of this is. If prompted for a specific conclusion topic, include this, but do not exclude your explanation of results.

If specific questions are presented in the assignment description, answer them in the conclusion.

Last, try to avoid editorializing and using marketing jargon. Be clear and support your claims with results.