Computer Security – Lab 2
Network Security

Thomas Kerber

October 29, 2016

1 Packet-Sniffing with Wireshark

1.1 VM Setup

For this exercise, you will be utilising a virtual machine, similar to coursework 1. Import the file '`/group/teaching/cs/wireshark-lab.ova`' into VirtualBox. Remember to change the path of the hard disk from

`/afs/inf.ed.ac.uk/user/sXX/sXXXXXX/VirtualBox VMs/Wireshark Lab/wireshark-lab.vdi`

to

`/tmp/sXXXXXX/VirtualBox VMs/Wireshark Lab/wireshark-lab.vdi`.

You may need to create the directory `/tmp/sXXXXXX` first. This is due to disk quote limits on student home directories.

1.2 Packet Sniffing

Start up the VM, and login as `root`, with the password `toor`. Then, launch **Wireshark**. An error may pop up when starting Wireshark, this can safely be ignored. A window with a list of hardware devices to capture from will open. Double click on **any**, and the window view should change. At this point, there should be no internet traffic in the VM, and the screen should remain blank. Open a terminal and run:

```
# run-conversation
```

This is a small program which will simulate a very simple HTTP(S) exchange. The client sends messages with a delay, so you should see the capture window filling up more as the conversation progresses. Take a while to familiarise yourself with the packets being captured. What information can you find in them?

1.3 Decrypting TLS

You will no doubt have noticed that parts of the communication are encrypted using TLS, and that you can't see the unencrypted content of these packets. Normally, there is little that can be done about this, but as that would be boring, you can find the server's private RSA key hidden somewhere in the unencrypted transmissions. Find the key, and save it as a plain text file '`private.pem`' (Note: you can use **mousepad** as a text editor in the VM).

Private RSA keys in the PEM format look something like this:

```
-----BEGIN PRIVATE KEY-----
MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpAgEAAoICAQC6fDDIdm6iMnDY
n0Xyg74JHYRtAV0gaKRh5XrDyZM9sAkMZJ/78XMi2i8zUvS2ukTh3yAnH3vtD9ji
...
OWo+pSjHke0evevfF3vm24Rk3755f7W9rNBvjBZ4/cunVZlJeHSeO+VOn2/whA9j
V4U3iQWZiCYr0cW+6po/BEJ+KPRzXZE=
-----END PRIVATE KEY-----
```

Next, in wireshark, navigate to **edit > Preferences > Protocols > SSL**, and press the **Edit** button for the RSA key lists. Add a new key, with IP address **127.0.0.1**, port **443**, protocol **http**, and select the key file '`private.pem`'.

You should now be able to inspect the TLS packets as well, and find the top secret project.

2 Executing HTTP with Netcat

For this exercise, you will have to retrieve the course web page (`http://www.inf.ed.ac.uk/teaching/courses/cs/`) using **netcat**. The command you will need to use is **ncat**, and is installed on dice. **ncat** opens a TCP (or UDP) stream with a server at a specific port. Running '`ncat www.inf.ed.ac.uk 80`' opens a TCP stream with the informatics HTTP server. Anything you type in the terminal with this command running will be sent to the server via TCP, and any packet the server sends back will be printed to the terminal.

Look up the format of a HTTP request, and make one to request the course web page. Hint: The informatics servers require the HTTP header '**Host**' to be set (but all other headers are optional).