IN2011 Computer Networks : Courswork 1

March 11, 2022

1 Fictional Back Story

The University's new student finance system is about to be launched! Just before giving a demonstration to the University President, one of our team logged in to the system from their laptop. All they did was log in and then log back out, but somehow someone was able to change their financial details, apply for a grant and steal the money! This shouldn't be possible as it uses a 2 factor authentication.

Thankfully the network team managed to record the traffic going to and from the attacker's machine. You have been asked to work out how they stole the money.

2 Tasks

- It is important that you use the right file; you will loose a lot of marks if you don't. If your student number is even then use:
  `coursework-for-even-student-numbers.pcapng`
  If your student number is odd then use:
  `coursework-for-odd-student-numbers.pcapng`
- Download the relevant file from Moodle and open it in Wireshark (either in the virtual machine image or on your own computer).
- Using your knowledge of network protocols and the features of Wireshark work out what has happened.
- Write a short report (*4.5 pages max!* and PDF) which covers the following three topics:

  What Happened Describe what happens in the captured network traffic. Give all of the relevant details. You need to work out what is relevant.

  The Attack Identify the different steps used in the attack. Explain how each step of the attack works.

Prevention Give defences which would prevent this attack. They must be specific to this attack and not general security improvements. Say which steps of the attack they would stop.

- Every claim or observation you make *must* be linked to one or more packets or parts of packets in the `pcap` file. Use the packet number (on the far left of the main display) to identify packets. Screen shots are not required but you can include them if you feel it is the best way of explaining something.

3 Deadline

Sun 3rd April 2022 17:00:00

4 Mark Scheme

This is individual coursework. Each of the three areas is worth 15% of the course mark and will be marked out of 15 according to the following criteria:

Correctness Are the technical claims you are making correct?
Completely → 5, mostly right → 3, mostly wrong → 1, completely wrong → 0

Completeness Have you identified all of the relevant information?
Everything → 5, most → 4, some → 2, one or two things → 1, nothing → 0.

Referencing Are all claims supported by references to packets or parts of packets?
Everything referenced → 5, some references → 2, few references → 0.

A further 5% of the course mark will be awarded for the general quality of the report.

5 Hints

- In Wireshark filters are very important for narrowing down what you are looking for and hiding things that you have already understood.
- To fully understand what is happening you will need information from several protocol layers. As the course is covering these in order, not all of the relevant information has been taught before the coursework is set. If things don't immediately make sense, don't panic and pay attention to future lectures and reading.
- One approach to the coursework is to divide the captured traffic into a series of time-slices based on the type of traffic. Then work out what happens in each time slice.
- Another approach is to work by protocol layers. For each layer what protocols are used, what addresses are used, what kind of services are used.
- Just like real traffic captures, there is some noise and irrelevant packets. Not everything is the file is important.
- Also there may be information that is not included in the file or is not readable due to encryption. This is common in real uses and something you will have to work around.
- The practicals contain some relevant exercises to get you started with Wireshark.
- Many of the tools needed to generate the attack file are on the virtual machine image so it should be possible to test out different ideas and see what packets they generate.
- Don't just look at the protocol information, the pattern and amount of data exchanged may be useful, especially if some of the packets are encrypted.