INTRODUCTION TO PRACTICAL WORK

2DV702 – Internet Security

Paolo Molinaro

pm222py@student.lnu.se

FACTS AND LOGISTICS

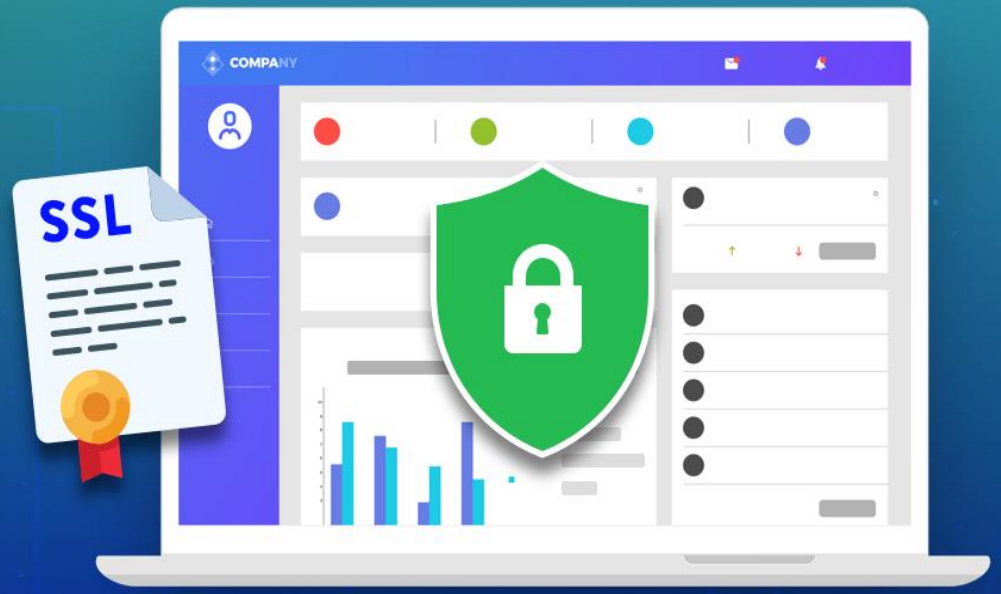
- Only one TA (it’s me).
- Four assignments including theoretical and practical tasks.
- Grading scheme: Pass (A-E) || Fail (F).
- MyMoodle as e-learning platform.
- **Slack** as a main channel of communication.
- Plagiarism is forbidden! Reports will be checked!

WHAT IS EXPECTED FROM YOU?

- A report in PDF - use the “Report Template” as basis.
- Follow our naming convention, “Firstname_Lastname_Assign#” E.g., “Harald_Gormsson_Assign1.pdf”.
- Well structured report, easy to follow, good language.
- Referencing is a must.
- Meet the deadlines.
- Refer to “Introduction to Practical Work”, section “IV. Assignment Rules”.

WHAT IS EXPECTED FROM US?

- Tutoring sessions: (check TimeEdit to be sure)
  - Tuesday 15:15 – 16:00, 16:15 – 17:00
  - Thursday 13:15-14:00, 14:15-15:00
- There will be on campus tutoring sessions.
- Help with the tasks is given at tutoring sessions.
- Grades with feedback comments.



ASSIGNMENT 1

Certificates, Authentication, Confidentiality and SSL/TLS

Paolo Molinaro
pm222py@student.lnu.se

TOOLS AND REQUIREMENTS

- A GNU/Linux system, e.g., Ubuntu (recommended).
- How to use? Hypervisor (VirtualBox, VMware), Live CD, local installation (Use WSL if possible).
- OpenSSL: Command-line tool.
- s_client: SSL/TLS client program (part of OpenSSL).
- Wireshark: Network protocol analyzer.
- Firefox web browser.
- Chromium web browser.
- 10-pages limit!

```
OPENSSL(1)                        OpenSSL                       OPENSSL(1)

NAME
       openssl - OpenSSL command line tool

SYNOPSIS
       openssl command [ command opts ] [ command args ]

       openssl [ list-standard-commands | list-message-digest-commands | list-
       cipher-commands ]

       openssl no-XXX [ arbitrary options ]

DESCRIPTION
       OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer
       (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and
       related cryptography standards required by them.

       The openssl program is a command line tool for using the various
       cryptography functions of OpenSSL's crypto library from the shell.  It can
       be used for

        o  Creation of RSA, DH and DSA key parameters
        o  Creation of X.509 certificates, CSRs and CRLs
        o  Calculation of Message Digests
        o  Encryption and Decryption with Ciphers
        o  SSL/TLS Client and Server Tests
        o  Handling of S/MIME signed or encrypted mail

COMMAND SUMMARY
       The openssl program provides a rich variety of commands (command in the
       SYNOPSIS above), each of which often has a wealth of options and arguments
       (command opts and command args in the SYNOPSIS).

       The pseudo-commands list-standard-commands, list-message-digest-commands,
       and list-cipher-commands output a list (one entry per line) of the names
       of all standard commands, message digest commands, or cipher commands,
       respectively, that are available in the present openssl utility.

       The pseudo-command no-XXX tests whether a command of the specified name is
       available.  If no command named XXX exists, it returns 0 (success) and
       prints no-XXX; otherwise it returns 1 and prints XXX.  In both cases, the
       output goes to stdout and nothing is printed to stderr.  Additional
       command line arguments are always ignored.  Since for each cipher there is
       a command of the same name, this provides an easy way for shell scripts to
       test for the availability of ciphers in the openssl program.  (no-XXX is
:
```

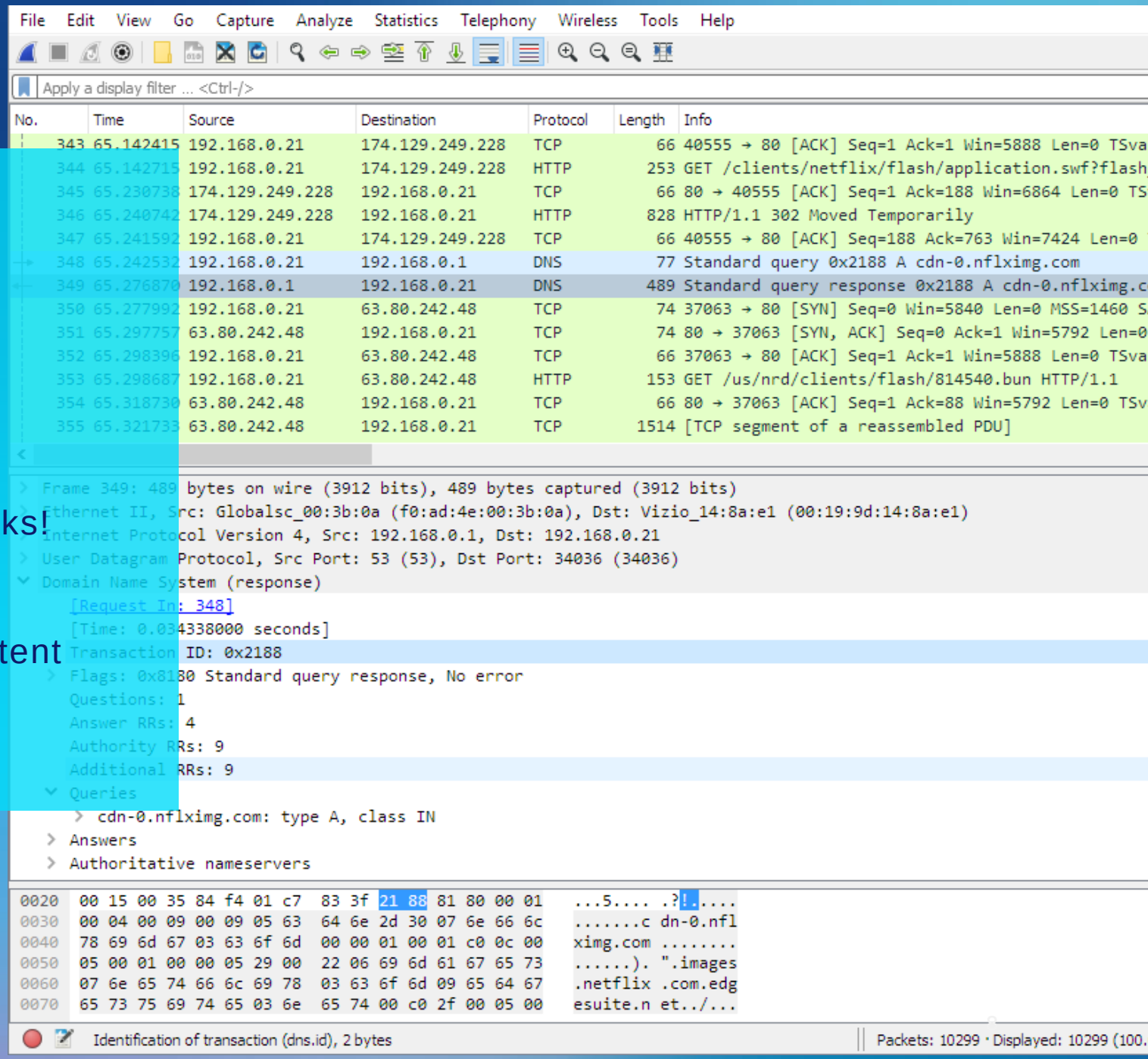
STRATEGY

- Work with terminal => Bash
- Use embedded help functionality
  - man <command>
  - <command> --help
  - <command> -h
- Search the web.
- Extra material, online tutorials, etc …
- ’**tldr**’ tool is excellent for quick references

POST-MORTEM TRACE ANALYSIS

- Wireshark for network traffic traces
- Very capable tool => Learn how it works!
- Trace collection workflow:
- Capable of decrypting SSL/TLS traffic
- Capable of decoding compressed content

[Wireshark Masterclass by Chris Greer]



USEFUL LINKS

- OpenSSL
- s_client
- Wireshark
- Wireshark Masterclass by Chris Greer
- VirtualBox, VMWare, UTM (Mac)
- Firefox, Chromium
- WSL