Lectures Notes on Data Preservation and Security

Camilo de Lellis

October 21, 2025

Contents

1 Lecture - 09/09/2025

Content taught: Apresentação da Disciplina — Fundamentos de Segurança

1.1 Ementa da Disciplina

Curso: Curso Superior de Tecnologia em Sistemas para Internet **Disciplina:** Segurança e Preservação de Dados **Carga-Horária:** 60h (80h/a) **Pré-Requisito(s):** Aplicações de Redes de Computadores **Número de créditos:** 4

EMENTA

Visão geral da segurança da informação; incidentes de segurança (ataques); criptografia e esteganografia; segurança em ambientes de rede; análise de vulnerabilidades de segurança; computação forense; políticas de segurança da informação.

PROGRAMA

Objetivos

Conhecer os principais conceitos e terminologia da área de segurança da informação;

- Conhecer e aprender a utilizar técnicas de criptografia e esteganografia;
- Aprender a identificar e responder aos principais incidentes de segurança (ataques) a sistemas computacionais;
- Aprender a identificar e corrigir as principais vulnerabilidades de segurança em sistemas computacionais;
- Conhecer e exercitar a configuração de ativos de redes de computadores relacionados a segurança da informação;
- Conhecer e praticar técnicas de segurança em redes de computadores;
- Conhecer técnicas e ferramentas comumente utilizadas no ataque e defesa de sistemas de informação;
- Conhecer e praticar técnicas e ferramentas de computação forense;
- Conhecer normas e critérios para implementação de políticas segurança da informação.

Bases Científico-Tecnológicas (Conteúdos)

- 1. Visão geral da segurança da informação
  - 1.1. Contextualização, principais conceitos e terminologia;
  - 1.2. Princípios básicos da segurança da informação;
  - 1.3. As 5 dimensões da segurança;
  - 1.4. Novos princípios/objetivos da segurança da informação.
- 2. Incidentes de Segurança (Ataques)
  - 2.1. Ameaças x Vulnerabilidades x Riscos;
  - 2.2. Principais tipos de ataques;
  - 2.3. Identificação, combate e resposta a incidentes.
- 3. Criptografia e Esteganografia
  - 3.1. Criptografia: Visão geral;
  - 3.2. Criptografia simétrica e assimétrica;
  - 3.3. Funções hash;
  - 3.4. Criptografia em serviços de rede;
  - 3.5. Esteganografia.

- 4. Segurança em Ambientes de Rede
  - 4.1. Firewalls;
  - 4.2. Sistemas de detecção de intrusões (IDS);
  - 4.3. Redes privadas virtuais (VPNs).
- 5. Análise de Vulnerabilidades de Segurança
  - 5.1. Vulnerabilidades em sistemas computacionais e serviços;
  - 5.2. Testes de intrusão (pentests).
- 6. Computação Forense
  - 6.1. Introdução à análise forense computacional;
  - 6.2. Técnicas de recuperação de dados;
  - 6.3. Introdução à análise forense em redes.
- 7. Políticas de Segurança da Informação
  - 7.1. Principais normas de segurança da informação;
  - 7.2. Implementação de uma política de segurança.

Procedimentos Metodológicos

Aulas teóricas expositivas; aulas práticas em laboratório; desenvolvimento de projetos; leitura de textos, palestras, seminários, visitas técnicas, pesquisas bibliográficas.

Recursos Didáticos

Quadro branco, computador, projetor multimídia e vídeos.

Avaliação

Avaliações escritas e práticas; trabalhos individuais e em grupo (listas de exercícios, estudos dirigidos, pesquisas); apresentação dos projetos desenvolvidos.

Bibliografia Básica

- 1. NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. Segurança de redes em ambientes cooperativos. São Paulo: Novatec, 2007. 482 p. il.
- 2. STALLINGS, William; BROWN, Lawrie. Segurança de computadores: princípios e práticas. 2. ed. Rio de Janeiro: Elsevier, 2014. 726 p. il.
- 3. STALLINGS, William; VIEIRA, Daniel. Criptografia e segurança de redes: princípios e práticas. 4. ed. São Paulo: Pearson Prentice Hall, 2010. 492 p. il. Bibliografia Complementar

Bibliografia Complementar

- 1. FARMER, Dan; VENEMA, Wietse. Perícia forense computacional: teoria e prática aplicada: como investigar e esclarecer ocorrências no mundo cibernético. São Paulo: Pearson Prentice Hall, 2007.
- 2. TANENBAUM, Andrew S. et al. Redes de computadores. 5. ed. São Paulo: Pearson Prentice Hall, 2011. 582 p. il.
- 3. BEAL, Adriana. Segurança da informação: princípios e melhores práticas para proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.
- 4. GUIMARÃES, Alexandre Guedes; LINS, Rafael Dueire; OLIVEIRA, Raimundo Corrêa. Segurança com redes privadas virtuais – VPNs. Rio de Janeiro: Brasport, 2006.

- 5. KIZZA, Joseph Migga. Computer network security and cyber ethics. 2nd ed. Jefferson: McFarland and Company, 2006.

Software(s) de Apoio:

- Sistemas operacionais Linux e Windows;
- Ferramentas específicas para exercícios e testes de segurança em sistemas computacionais.

2 Lecture - 15/09/2025

Content taught: Fundamentos de Segurança

2.1 Fundamentos de Segurança

3 Lecture - 16/09/2025

Content taught: Incidentes de Segurança

3.1 Incidentes de Segurança

4 Lecture - 22/09/2025

Content taught: Incidentes de Segurança

4.1 Incidentes de Segurança

5 Lecture - 23/09/2025

Content taught: Práticas de Fixação: Incidentes de Segurança (Footprinting + Portscan)

5.1 Práticas de Fixação: Incidentes de Segurança (Footprinting + Portscan)

6 Lecture - 29/09/2025

Content taught: Incidentes de Segurança

6.1 Incidentes de Segurança

7 Lecture - 30/09/2025

Content taught: Práticas de Fixação: Incidentes de Segurança (Scanning)

7.1 Práticas de Fixação: Incidentes de Segurança (Scanning)

8 Lecture - 06/10/2025

Content taught: Incidentes de Segurança

8.1 Incidentes de Segurança

9 Lecture - 07/10/2025

Content taught: 1a Avaliação do 1o Bimestre

Figure 1: An example of steganography. Data embedded into an image.

9.1 1a Avaliação do 1o Bimestre

10 Lecture - 13/10/2025

Content taught: Criptografia e Esteganografia

10.1 Criptografia e Esteganografia

11 Lecture - 14/10/2025

Content taught: Criptografia e Esteganografia

11.1 Criptografia e Esteganografia

12 Lecture - 20/10/2025

Content taught: Esteganografia

12.1 Introduction to Steganography

A lot of people know cryptography even when they never implemented it in their life. Steganography, however, is much less common to the popular knowledge. Steganography consists in occulting a message into diverse media formats.

The historical context to steganography dates to the communications of old age emperors. Examples brought by the professor are:

- 480 BC Greece x Persia
- Histiaeus communicating through bald heads
- Chinese wax ball
- Invisible ink
- Boiled egg message

Steganography starts being used in computers when people realized that file formats such as images took a big amount of bits. There was, then, a big opportunity to hid messages in between the data. First this knowledge was used to compress images. That was done by removing the least significant bits from a file. They then realized that we could take this gap created by removing those bits to insert news information. We could then insert messages inside images. We then took notice that another kind of files could be to store those messages. We could then store messages inside sound files.

With the advance of tech and the tools for steganography, we can now basically store anything inside anything. For example, we could take an audio and record then into image files or store image into sound.

Some of the tools used for steganography are:

- Steghide
- Camouflage(?)
- S-tools
- Invisible Secrets
- Gifshuf
- Hideseek
- Gifclean (not found)
- HIP (Hide in Picture)

For the practice example we did in class, we first had to download a **docker-compose.yml**:

```
wget http://10.49.10.70/cripto01/docker-compose.yml
```

TO-DO: Later, I'll share the content of the **.yml** here. To run it, just execute the following command:

```
docker compose up
```

After running the container, just access localhost:10001/acesso.html with a password of **password**
To extract the image, just run:

```
steghide extract -sf rk_01.jpg
```

The passphrase is "agua". The professor hid an image inside another.

To suspect if an image is an object to steganography, there is an area in the field of security called steganalysis. You can use image editors to search for filters inside an image file and see where is there a "shadow" inside an image.

Bin Laden was a great user of such techniques. The professor just gave an example of hiding images inside a gigantic amount of pornography. Even images without steganography are big. Higher resolution

Stegcracker is a brute force tool that can crack the password of steganography applied into a image. An example of such tool being used:

```
stegcracker camilo.jpg senhas
```

To see if an image is not compromised, we can check it's hash to see if it is like the original:

```
md5sum camilo.jpg
```

13 Lecture - 21/10/2025

Content taught: Asymmetric Cryptography

13.1 Asymmetric Cryptography

Asymmetric cryptography consists of using a pair of keys when encrypting and decrypting data.

Installing **gpg**:

```
# being sudo
apt update && apt install gnupg
```

I send someone my public key, they send me and I decrypt it with my private key. To make sure that someone sent someone, they need to sign someone with their private key, and with their public key, through a keychain, they can be sure that someone encrypted it. keys.openpgp.org is a public keychain. This website generate public keys that can be used by everyone. You cannot have two certificates in the same keychain using the same e-mail.

The first step is to add the keyserver to our gnupg installation:

```
mkdir ~/.gnupg
touch ~/.gnupg/gpg.conf
vim ~/.gnupg/gpg.conf
```

Inside the file, write the following:

```
keyserver hkps://keys.openpgp.org
```

The difference between a remote to a local keychain is that the local keychain only has keys I used before, not the ones I did never use.

To encrypt data asymmetrically:

```
gpg --full-generate-key
```

Expected output:

If some problem arises when you set your key to never expire, you can revoke your key.

To see if the keys was really created, you just need to take a look at the **/.gnupg**

```
$ ls ~/.gnupg/
S.gpg-agent
S.gpg-agent.ssh
S.gpg-agent.browser
gpg.conf
S.gpg-agent.extra
openpgp-revocs.d
private-keys-v1.d
trustdb.gpg
pubring.kbx
pubring.kbx-
```

To see the keys:

To export your key as text to later upload to the public keychain:

```
gpg --export --armor lellis.m@escolar.ifrn.edu.br > minha_chave.asc
```

Then we can go to openpgp and upload our key.

References