



CERTIFICADO DIGITAL

19

I Certificado digital

- Problema da criptografia simétrica: qual é?

20

I Certificado digital

FIAP

- Problema da criptografia simétrica: qual é?
- Visualização de um certificado digital

21

I Certificado digital

FIAP

- Problema da criptografia simétrica: qual é?
- Visualização de um certificado digital
 - Observar:
 - Emissor/Issuer
 - Chave pública do emissor/Subject's Public Key
 - Há outros campos:
 - Prazo de validade
 - ...

22

I Certificado digital

FIAP

- Uma **Autoridade Certificadora (AC)** é responsável por emitir o certificado (e somente a AC emite um certificado digital)
- A AC garante a legitimidade do negócio
- Exemplos de ACs:
 - Verisign
 - Certisign
 - SERASA
 - SERPRO
 - Let's Encrypt
 - ...



23

I Certificado digital

FIAP

- A AC gera um par de chaves:
 - Chave pública (Public Key)
 - Chave privada (Private Key)
- Chave pública:
 - Emissor a distribui publicamente
- Chave privada:
 - De conhecimento e armazenamento exclusivo do titular do certificado
 - Nunca deve ser divulgada

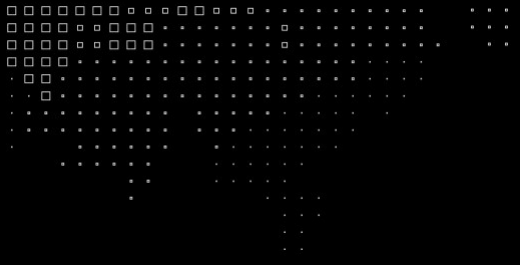
24

I Certificado digital

FIAP

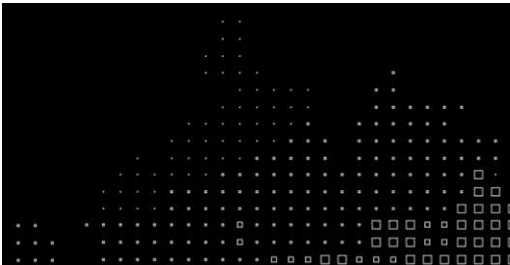
- Chave pública:
 - Usada para que os outros criptografem o conteúdo e enviem para o titular do certificado
- Chave privada:
 - Titular do certificado recebe a mensagem cifrada e a decifra com a chave privada

25



Demonstração

- Certificado digital
 - HTTP e HTTPS
 - Usando o Kali



26

I Site HTTP simples

FIAP

- Diretório (**site_inseguro**)
 - Há nesse diretório um arquivo (index.html):

```
<!DOCTYPE html>
<html lang="pt-BR">
<head>
  <meta charset="UTF-8">
  <title>Site HTTP Simples</title>
</head>
<body>
  <h1>Bem-vindo ao Site HTTP!</h1>
  <p>Este é um site *SEM* criptografia. Veja como o conteúdo é visível no Wireshark!</p>
  <form>
    <label>Senha secreta:</label>
    <input type="text" name="senha">
    <input type="submit" value="Enviar">
  </form>
</body>
</html>
```

- Iniciando o servidor web:

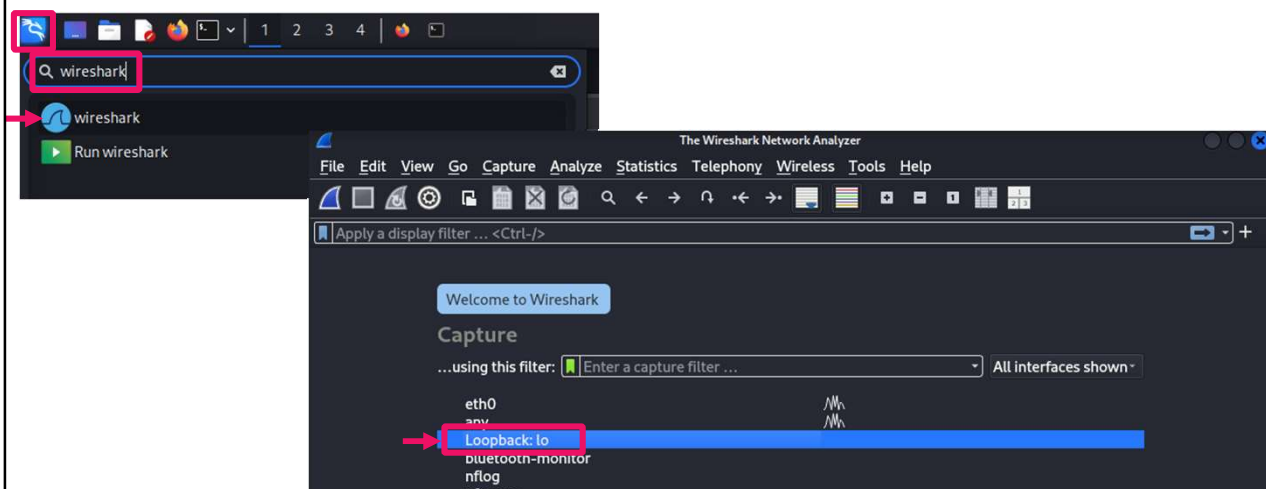
python -m http.server 80

27

I Certificado digital

FIAP

- Abrindo o Wireshark para capturar o tráfego da interface loopback

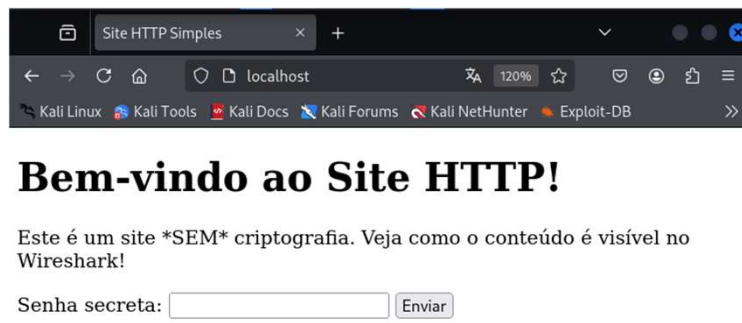


29

Certificado digital

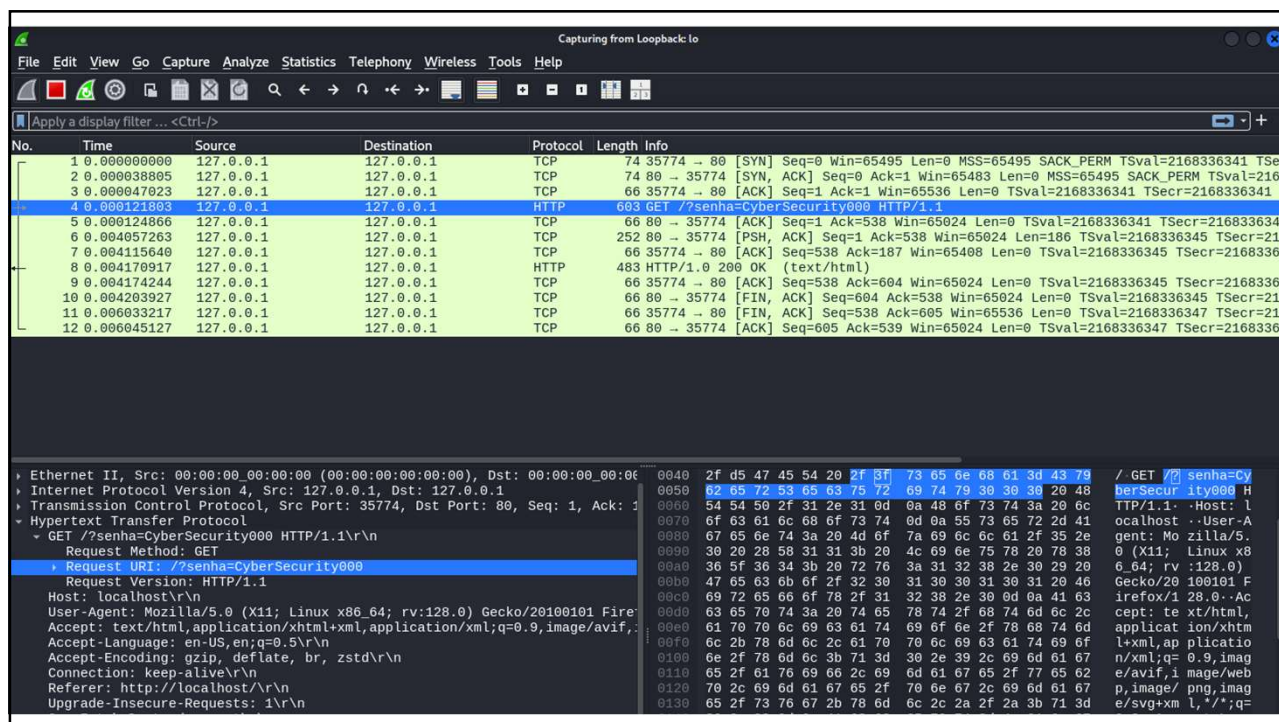
FIAP

- Acessando a página:
 - <http://localhost>



- Ao digitar a senha, vemos o seguinte resultado no Wireshark:

30



32

I Certificado digital



- Agora veremos um site com certificado digital

33

I Certificado digital



- No diretório (**site_seguro**)
 - Há o arquivo (index.html):

```
<!DOCTYPE html>
<html lang="pt-BR">
<head>
  <meta charset="UTF-8">
  <title>Site HTTPS Simples</title>
</head>
<body>
  <h1>Bem-vindo ao Site HTTPS!</h1>
  <p>Este é um site *COM* criptografia. O conteúdo está protegido no Wireshark!</p>
  <form>
    <label>Senha secreta:</label>
    <input type="text" name="senha">
    <input type="submit" value="Enviar">
  </form>
</body>
</html>
```

34

I Certificado digital

FIAP

- Usando o python, há o código do servidor web (site-seguro.py):

```
import http.server
import ssl
import os

# Configurações do servidor
PORT = 443
DIRECTORY = "."

# Define o manipulador de requisições
Handler = http.server.SimpleHTTPRequestHandler
Handler.directory = os.path.abspath(DIRECTORY)

# Cria o servidor
httpd = http.server.HTTPServer(("localhost", PORT), Handler)

# Configura o SSL/TLS com os certificados
ssl_context = ssl.SSLContext(ssl.PROTOCOL_TLS_SERVER)
ssl_context.load_cert_chain(certfile="cert.pem", keyfile="key.pem")

# Aplica o SSL ao servidor
httpd.socket = ssl_context.wrap_socket(httpd.socket, server_side=True)

# Inicia o servidor
print(f"Servidor HTTPS rodando em https://localhost:{PORT}")
httpd.serve_forever()
```

35

I Certificado digital

FIAP

- Precisamos, agora, gerar as chaves:
 - Chave pública
 - Chave privada
- Uso do openssl
 - Software para geração de chaves
 - O openssl é usado para gerar o par de chaves no mesmo diretório em que estão os arquivos **site_seguro/index.html** e **site_seguro/site-seguro.py**:

```
openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out cert.pem
```

- Serão gerados 2 arquivos:
 - cert.pem (contém a chave pública)
 - key.pem (contém a chave privada)

36

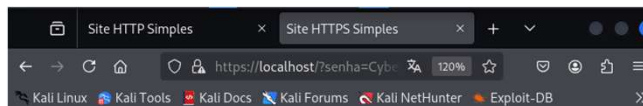
Certificado digital

FIAP

- Inicialização do servidor usando o certificado digital
 - Denominado auto-assinado

python site-seguro.py

- Ao acessar a página <https://localhost>
(avance e prossiga quando receber o aviso do navegador)



Bem-vindo ao Site HTTPS!

Este é um site *COM* criptografia. O conteúdo está protegido no Wireshark!

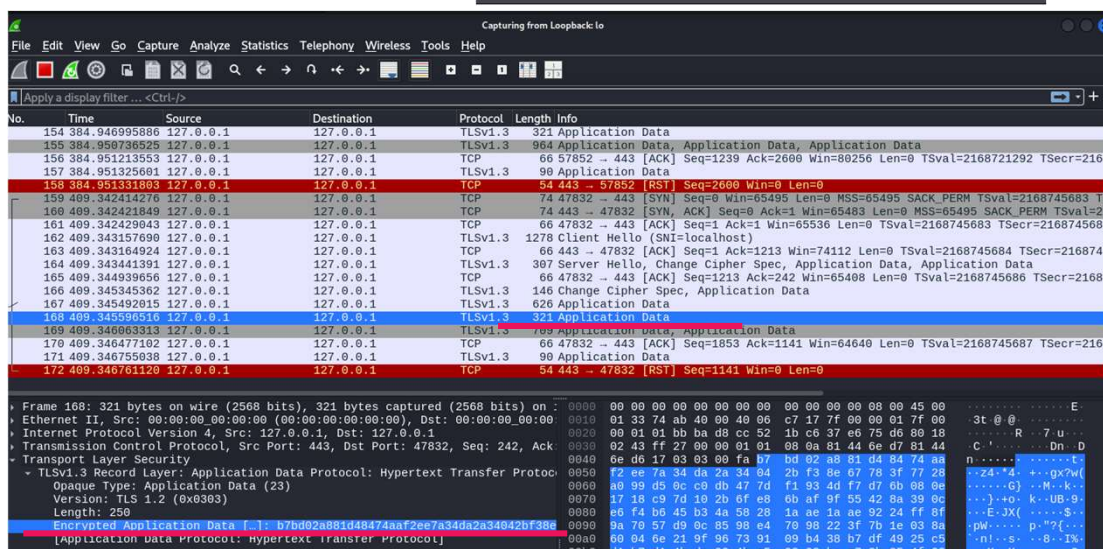
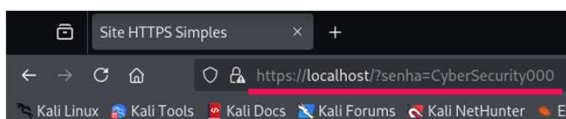
Senha secreta:

E digitar a senha, vemos no Wireshark:

37

Certificado digital

FIAP



39



ENVENENAMENTO DE DNS + HTTPS

40

I DNS poisoning + HTTPS

• Kali

- 1 - Acessar o website `www.exemplo.com` (feche o navegador depois de acessar)
- 2 - Executar o comando `ping` no site `www.exemplo.com`
- 2 - Consultar o DNS (comando `dig`)
- 3 - Wireshark: Observar a requisição e a resposta
- 4 - Modificar o arquivo `/etc/hosts` (executar como superusuário: `sudo mousepad /etc/hosts`):
 - Inserir o IP 127.0.0.1 para o endereço do website (salvar o arquivo):
 - `127.0.0.1 www.exemplo.com`
- 5 - Iniciar o servidor HTTPS local
- 6 - Abra um novo navegador e acesse o website novamente (*atualize a página se necessário CTRL+F5, pois o navegador pode ter feito cache da página*)
- 7 - Executar o comando `ping` no site `www.exemplo.com`
- 8 - Executar o comando `dig` no site `www.exemplo.com`
- 9 - Modificar o arquivo `/etc/hosts` (executar como superusuário - root):
 - Remover a linha inserida no passo 4 anterior (salvar o arquivo)

41



42

 A screenshot of a news article from G1. The header is red with a white 'G1' logo and the text 'TECNOLOGIA E GAMES'. On the right is the 'FIAP' logo. The article text is as follows:

06/09/2011 19h21 - Atualizado em 06/09/2011 19h21

Invasão a empresa invalida 'cadeados' de segurança de sites legítimos

DigiNotar sofreu ataque em sua rede interna.
Atualização do Internet Explorer remove empresa de lista 'confiável'.

Altieres Rohr
Especial para o G1


Relatório de Segurança



Cadeado deixará de funcionar em sites com certificados da DigiNotar (Foto: Reprodução)

A companhia de segurança holandesa DigiNotar foi removida da lista de autoridades certificadoras (ACs) do Internet Explorer. As ACs são as organizações que emitem os certificados digitais que fazem aparecer o "cadeado de segurança" em sites de internet. A DigiNotar também emite certificados digitais para o governo holandês, que realizou uma auditoria na qual foram identificados diversos problemas com os sistemas da empresa.

Social media icons for Facebook, Twitter, Google+, and Pinterest are visible.

43



 MENU
 

TECNOLOGIA E GAMES

FIAP

08/08/2011 19h21 - Atualizado em 08/08/2011 19h21

Invasão a empresa invalida 'cadeados' de segurança de sites legítimos

DigiNotar usava senhas fracas e software desatualizado

A auditoria realizada pela empresa Fox-It afirma que os computadores da DigiNotar estavam todas no mesmo domínio (rede) e que as senhas usadas pela empresa "não eram muito fortes e poderiam ser adivinhados por força bruta". Força bruta é o método que um software testa senhas uma por uma, rapidamente.

Havia softwares desatualizados na rede da empresa.

Esses problemas, somados, permitiriam que qualquer invasor que obtivesse acesso a uma parte da rede da empresa avançasse até o servidor que realizava a emissão dos certificados.

