



Métodos de Invasão de Redes e Sistemas

Prof. Érico José Ferreira

ericonet@ericonet.com.br

Material disponível em <http://www.ericonet.com.br>

Métodos de Invasão de Redes e Sistemas

HACKERS





Métodos de Invasão de Redes e Sistemas Histórico

- Durante as primeiras décadas de sua existência, as redes de computadores foram principalmente usadas pelos usuários para enviar mensagens de correio eletrônico e para compartilhar impressoras.

SEGURANÇA NÃO PRECISAVA DE CUIDADOS




Métodos de Invasão de Redes e Sistemas Histórico

Uso crescente das redes

- operações bancárias
- e-commerce
- Serviços públicos em geral

segurança precisa de muitos cuidados

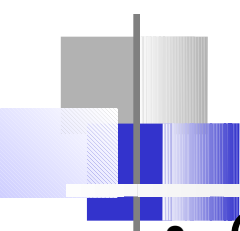


Métodos de Invasão de Redes e Sistemas

Segurança

- A segurança se preocupa em garantir que pessoas mal-intencionadas não leiam ou, pior ainda, modifiquem mensagens enviadas a outros destinatários. Outra preocupação da segurança se volta para pessoas que tentam ter acesso a serviços remotos, os quais elas não estão autorizadas a usar.
- A maior parte dos problemas de segurança são intencionalmente causados por pessoas que tentam obter algum benefício ou prejudicar alguém.

HACKERS




Métodos de Invasão de Redes e Sistemas

Origem do Termo

- O termo hacker designava qualquer pessoa que fosse extremamente especializada em uma determinada área. Qualquer fera em qualquer assunto, poderia ser considerado um hacker.
- Foi com o cinema americano que o termo passou a ser usado largamente.

FILMES – WAR GAMES / CÓDIGO PARA O INFERNO



Métodos de Invasão de Redes e Sistemas

Origem do Termo

- O mercado americano abarrotou as prateleiras de livros como Cyberpunk, e mais tarde, qualquer nota sobre invasão de sistemas ou crimes relacionados a computadores ganhavam um espaço cada vez maior na mídia.

DESPERTOU A CURIOSIDADE



Métodos de Invasão de Redes e Sistemas

Hackers Antigos


- Os hackers eram pessoas que trabalhavam em projetos de computadores e técnicos altamente especializados. Mas também existiam aqueles garotos que estudavam muito e hoje, grande parte trabalha na área de segurança de computadores. O resto está preso ou respondendo processo.



Métodos de Invasão de Redes e Sistemas

Hackers Atuais

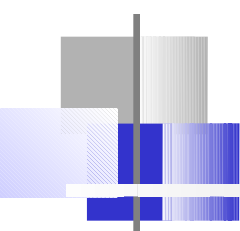
- Hoje, a grande maioria dos hackers é jovem. Dizem que é uma fase da vida de cada micreiro. E além do mais o jovem tem muito mais tempo para estudar e aprender.



Métodos de Invasão de Redes e Sistemas

Hacker - Definição

- Hacker é aquela pessoa que possui uma grande facilidade de análise, assimilação, compreensão e capacidades surpreendentes de conseguir fazer o que quiser com um computador. Ele sabe perfeitamente que nenhum sistema é completamente livre de falhas, e sabe onde procurar por elas, utilizando técnicas das mais variadas.

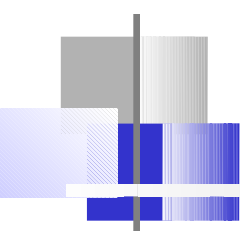


Métodos de Invasão de Redes e Sistemas

Cracker - Definição

- Possui tanto conhecimento quanto os hackers, mas com a diferença de que, para eles, não basta entrar em sistemas, quebrar senhas, e descobrir falhas. Eles precisam deixar um aviso de que estiveram lá, geralmente com recados malcriados, algumas vezes destruindo partes do sistema, e até aniquilando com tudo que vê pela frente.

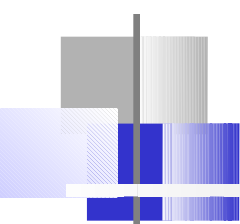
HACKER MALIGNO



Métodos de Invasão de Redes e Sistemas

Lamer - Definição

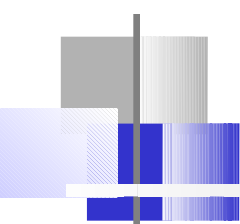
- É aquele cara que quer aprender sobre hackers, e sai perguntando para todo mundo. Os hackers, ou qualquer outra categoria, não gostam disso, e passam a lhe insultar, chamando-o de lamer, ou seja, novato.



Métodos de Invasão de Redes e Sistemas

Wannabe - Definição

- É o principiante que aprendeu a usar algumas receitas de bolo (programas já prontos para descobrir senhas ou invadir sistemas), entrou em um provedor de fundo de quintal e já acha que vai conseguir entrar nos computadores da Nasa.



Métodos de Invasão de Redes e Sistemas

Arackers - Definição

- Esses são os piores. Os “hackers de araque” são a maioria absoluta no submundo cibernético. Algo em torno de 99,9%. Finge ser os mais ousados e espertos usuários de computador, planejam ataques, fazem reuniões durante as madrugadas, mas no final das contas vão fazer downloads de sites pornográficos ou jogar em Rede.



Métodos de Invasão de Redes e Sistemas

Métodos de Invasão - Hackers

- Cavalo de tróia – O hacker infiltra em seu alvo um programa semelhante a um vírus. Mas, em lugar de destruir programas e arquivos, ele tem a função de descobrir senhas. O cavalo de tróia pode ser enviado escondido numa mensagem na Internet ou num disquete que o hacker passa, com jogos ou outros programas, para usuários do computador que quer invadir. Como é programado para se conectar com seu criador, por meio de modem, em dia e hora marcados, ele transmite os dados que copiou.



Métodos de Invasão de Redes e Sistemas

Métodos de Invasão - Hackers

- Farejamento de redes – Para acelerar a sua transmissão, os dados que entram nas redes, provenientes de vários computadores, são agrupados em pacotes. O hacker cria programas farejadores que monitoram a circulação desses pacotes nas redes e procuram neles palavras como password e senha. Quando as encontra, o programa copia o pacote e o envia para o computador do hacker.



Métodos de Invasão de Redes e Sistemas

Métodos de Invasão - Hackers

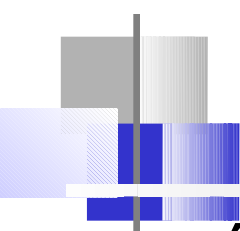
- Engenharia Social – É uma espécie de espionagem. Senhas com datas de nascimento, sobrenome ou nome dos filhos são muito comuns. Se o hacker tiver acesso a essas informações do usuário, vai tentá-las, como primeira opção, para descobrir sua senha. Alguns chegam a arrumar emprego temporário na empresa que pretendem invadir. Ninguém cobre o teclado na hora de digitar a senha.



Métodos de Invasão de Redes e Sistemas

Métodos de Invasão - Hackers

- Quebra-cabeça – Um jeito simples de desvendar senhas é a velha tentativa e erro. Para isso, o hacker cria programas capazes de montar todo tipo de combinação de letras e números. O sistema funciona bem para senhas de 06 caracteres. No Brasil era um método muito difundido, pois as senhas em geral eram simples e dificilmente os computadores possuíam sistema de proteção



Métodos de Invasão de Redes e Sistemas

Phreaker - Definição

- É especializado em telefonia. Faz parte de suas principais atividades as ligações gratuitas (tanto local como interurbano e internacional), reprogramação de centrais telefônicas, instalação de escutas.



Métodos de Invasão de Redes e Sistemas

Métodos de Invasão - Phreakers

- Fraudando orelhões com aparelho comum – Primeiro o Phreaker arruma um telefone comum bem pequeno e compacto. Depois ele tem que descascar os fios do orelhão e os do telefone. Ele entrelaça-os e fica ligado para a polícia não ver.
- Nota pessoal: no meu tempo de engenharia eletrônica os orelhões eram com ficha e alguns alunos usavam um diodo retificador de meia onda com “jacarés” soldados nas pontas e colocavam os “jacarés” nos fios descascados e faziam ligações de graça.



Métodos de Invasão de Redes e Sistemas

Métodos de Invasão - Phreakers

- Fraude em caixa de verificação – As caixas de verificação são caixas de ferro, que geralmente ficam localizadas em vias públicas, e são utilizadas para se fazer a checagem das linhas e detectar problemas antes que chegue a central. O phreaker conecta um telefone comum a uma dessas linhas e liga gratuitamente.



Métodos de Invasão de Redes e Sistemas

Métodos de Invasão - Phreakers

- Enganando o telefone público – O phreaker bota o cartão, assim que a pessoa falar ALÔ! Segura o número 9 e retira o cartão. Ele tem que ficar segurando o 9, até acabar de falar.
- Mito ????



Métodos de Invasão de Redes e Sistemas

Métodos de Invasão - Phreakers

- Grafite – O grafite é um material super condutor que conduz energia, e o cartão funciona assim, ele tem 50 fusíveis, cada ligação gasta ele queima um fusível, então o nosso amigo grafite que é condutor de eletricidade, não deixa queimar os fusíveis. Então o phreaker deve rabiscar o grafite com força no fundo do cartão e usá-lo a vontade.
- Mito ???



Métodos de Invasão de Redes e Sistemas

Métodos de Invasão - Phreakers

- Esmalte de unha incolor – O esmalte de unha evita que os fusíveis dos cartões telefônicos queimem.
- Mito ???

OBS: ESTES EXEMPLOS SÃO APENAS ILUSTRATIVOS E NÃO DEVEM SER SEGUIDOS PELOS LEITORES DESTE MATERIAL.



Métodos de Invasão de Redes e Sistemas

Realidade

- Não existe segurança a 100%!
- Existirão sempre vulnerabilidades e ataques capazes de explorá-las e pessoas dispostas a fazê-lo, etc...
- Questões chave:
 - Quanto se deve investir em segurança?
 - Qual a relação custo benefício compensadora?
- O custo da segurança não deve ser superior ao custo da informação protegida.



Métodos de Invasão de Redes e Sistemas

Segurança de Perímetro x Profundidade

- Segurança pressupõe atitude defensiva
- Defesa de perímetro :
 - Consiste em definir um perímetro protegido englobando um conjunto de máquinas e redes.
 - Evitar as interações indesejáveis entre os dois lados desse perímetro.
 - Restringir interações entre domínios de segurança.



Métodos de Invasão de Redes e Sistemas

Segurança de Perímetro x Profundidade

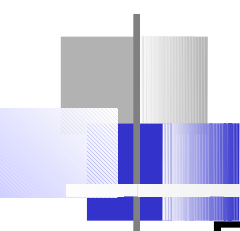
- Defesa em profundidade :
 - Atua em todos os níveis e não apenas nas fronteiras entre domínios.
 - Particularmente útil para detectar problemas internos.
 - Mais complexa de gerir.



Métodos de Invasão de Redes e Sistemas

Políticas e Mecanismos de Segurança


- Políticas de segurança: definem o foco da segurança e o que se deve garantir.
- Mecanismos de segurança: tecnologia que permite implementar as políticas de segurança.
- Domínio de segurança: universo de recursos (máquinas, redes) e pessoas sujeitos à mesma política de segurança.



Métodos de Invasão de Redes e Sistemas Políticas e Mecanismos de Segurança

Exemplo :


- Política: O computador A só pode ser acessado por pessoas do Setor de Informática
- Mecanismos (para implementar esta política): barreiras físicas, mecanismos de autenticação, registros, etc...



Métodos de Invasão de Redes e Sistemas

Mecanismos de Segurança


- Mecanismos de confinamento: criam barreiras à difusão de atividades para além das barreiras de segurança
 - Ex: sandboxes, firewalls e as zonas desmilitarizadas (DMZ) , etc...
- Mecanismos de controle de acesso: permitem aferir se uma determinada pessoa pode ou não realizar uma determinada tarefa
 - Ex: proteção dos arquivos, proteção do acesso a outras máquinas da rede, etc...



Métodos de Invasão de Redes e Sistemas

Mecanismos de Segurança


- Mecanismos de execução privilegiada: destinam-se a conceder privilégios a usuários que habitualmente não os têm.
 - Ex: setuid, setgid
- Mecanismos de filtragem: servem para identificar atividades não autorizadas e evitar que as mesmas sejam levadas a efeito.
 - Ex: filtragem de tráfego na rede através de firewall



Métodos de Invasão de Redes e Sistemas

Mecanismos de Segurança

- Mecanismo de registo: produzem relatórios sobre as atividades solicitadas ou realizadas. Servem, fundamentalmente, para observar se o sistema está operando normalmente.
 - Ex: Logs
- Mecanismos de auditoria: servem para fazer inspeção e análise de registros que “permitem” retirar conclusões após ter acontecido algo de inesperado.



Métodos de Invasão de Redes e Sistemas

Mecanismos de Segurança

- Algoritmos criptográficos: servem para proteger informação que possa ser fisicamente devassada.
- Protocolos criptográficos: são trocas ordenadas de dados entre entidades em que parte ou a totalidade dos dados úteis são cifrados.



Métodos de Invasão de Redes e Sistemas

Ação dos Mecanismos de Segurança

- Prevenção de ataques
 - Evitar que tenham sucesso
 - perturbação da operação normal?...
- Detecção de ataques
 - Percebê-los o mais cedo possível
 - nem sempre é possível a prevenção (vírus...)
- Recuperação de ataques
 - Repor a situação inicial
 - mas eliminar o ponto de entrada do ataque



Métodos de Invasão de Redes e Sistemas

Leis Federais

LEI 9610/98 – LEI DE DIREITOS AUTORAIS

LEI 9609/98 – LEI DO SOFTWARE

LEI 9279/96 – CÓDIGO DE PROPRIEDADE
INDUSTRIAL

LEI 10695/03

SQL BÁSICO

- O modelo relacional encontra-se padronizado pela indústria de informática. Ele é chamado de *padrão SQL* (Structured Query Language).
- O padrão SQL define precisamente uma *interface SQL* para a definição de tabelas, para as operações sobre as mesmas (seleção, projeção, junção, e outras) e para a definição de regras de integridade de bancos de dados.
- A interface SQL é portanto implementada em *todos* os sistemas de bancos de dados relacionais existentes.
- Por quê a indústria tem interesse em padronizar os sistemas de bancos de dados? A razão é muito simples: a existência de padrões facilita a interoperabilidade (comunicação entre máquinas, entre programas).



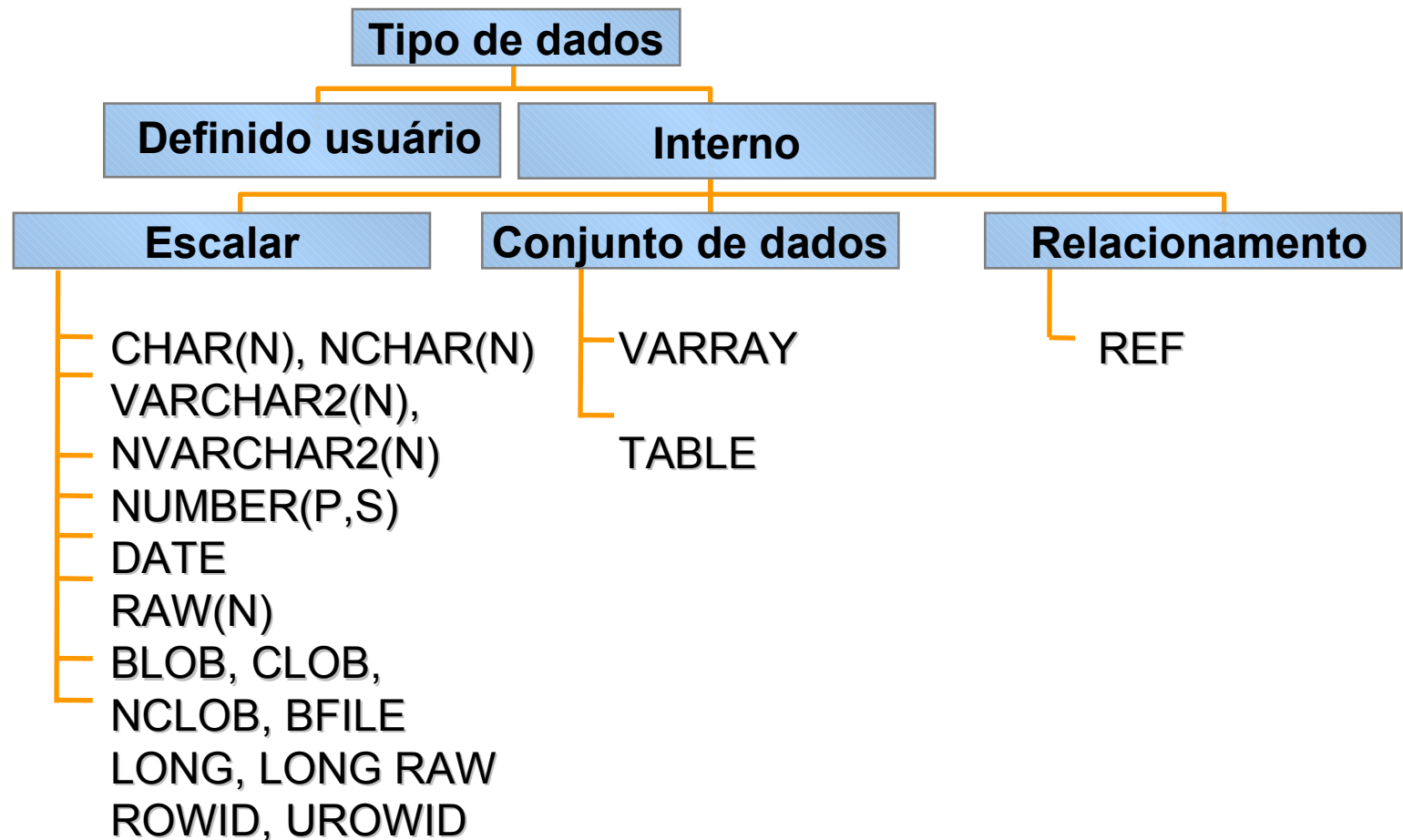
Métodos de Invasão de Redes e Sistemas

SQL BÁSICO

- A linguagem SQL tem diversas partes:
 - Linguagem de Definição de Dados (DDL)
 - fornece comandos para definições de esquemas de relação, criação/remoção de tabelas, criação de índices e modificação de esquemas.
 - Linguagem de Manipulação de Dados (DML)
 - inclui uma linguagem de consulta baseada na álgebra relacional e cálculo relacional de tupla. Compreende comandos para inserir, consultar, remover e modificar tuplas num BD.

Métodos de Invasão de Redes e Sistemas

SQL BÁSICO



SQL BÁSICO - DDL

- Os comandos SQL para definição de dados são:
 - CREATE
 - DROP
 - ALTER
- CREATE TABLE: especifica uma nova tabela (relação), dando o seu nome e especificando as colunas(atributos) (cada uma com seu nome, tipo e restrições)_
- Sintaxe:
 - CREATE TABLE tabela_base (colunas tabela_base + constraints)

SQL BÁSICO - DDL

- As definições das colunas têm o seguinte formato:
 - coluna tipo[NOT NULL [UNIQUE]][DEFAULT valor]
- Onde:
 - coluna: nome do atributo que está sendo definido
 - tipo: domínio do atributo
 - NOT NULL: expressa que o atributo não pode receber valores nulos
 - UNIQUE: indica que o atributo tem valor único na tabela. Qualquer tentativa de se introduzir uma linha na tabela contendo um valor igual ao do atributo será rejeitada. Serve para indicar chaves secundárias
 - DEFAULT: indica um valor default para a coluna



Métodos de Invasão de Redes e Sistemas

SQL BÁSICO - DDL

- Constraints (Restrições de Integridade e de domínio):
 - Integridade de Chave:
 - PRIMARY KEY(atributos_chave)
 - Integridade Referencial:
 - FOREIGN KEY (atributos) REFERENCES
tabela_base(atributos)
 - Restrição de Integridade:
 - CHECK(condição)



Métodos de Invasão de Redes e Sistemas

SQL BÁSICO - DDL

- Exemplo:
 - Create table CD (
 - cod_cd integer not null,
 - cod_gravadora integer null,
 - nome_cd varchar(60) null,
 - preco_venda decimal(6,2) null,
 - cd_indicado integer null,
 - Primary Key (cod_cd),
 - Foreign Key (cod_gravadora) references Gravadora(cod_gravadora),
 - Check (preco_venda > 0)



Métodos de Invasão de Redes e Sistemas

SQL BÁSICO - DDL

- **ALTER TABLE**
 - usado para alterar a estrutura de uma tabela para:
 - Acrescentar novas colunas
`ALTER TABLE cliente add email varchar(80) unique`
 - Acrescentar novas constraints
`ALTER TABLE cliente add Primary Key (cd_cliente)`
 - Modificar colunas
`ALTER TABLE cliente Modify Column
email varchar(100) not null`



Métodos de Invasão de Redes e Sistemas

SQL BÁSICO - DDL

- ALTER TABLE

- Excluir colunas

- ```
ALTER TABLE cliente Delete (drop) email
```

- Trocar nomes de colunas

- ```
ALTER TABLE cliente Rename (change)
```

- ```
nome_cliente To nm_cliente (tipo)
```

\* Valores entre parenteses usados no MySQL

## SQL BÁSICO - DDL

---

- DROP TABLE
  - Usado para eliminar uma tabela
    - DROP TABLE cliente



# Métodos de Invasão de Redes e Sistemas

## SQL BÁSICO - DML

---

- INSERT INTO
  - Para incluir dados em uma tabela

INSERT INTO AUTOR

Values (1, 'Vinicius de Moraes'),  
(2, 'Tom Jobim'),  
(3, 'Toquinho')



# Métodos de Invasão de Redes e Sistemas

## SQL BÁSICO - DML

---

- UPDATE TABLE
  - Para alterar o conteúdo de uma ou mais colunas, ou o conteúdo de uma coluna em diversas linhas.

```
UPDATE CD Set preco_venda = 15
Where cod_gravadora = 1;
```

## SQL BÁSICO - DML

- DELETE FROM

- Usado para excluir linhas de uma tabela

DELETE FROM AUTOR

Where cd\_autor = 1;

DELETE FROM CD

Where cod\_gravadora = 2;

DELETE FROM MUSICA

- Nesse caso, todas as músicas serão excluídas (a tabela ficará vazia)



## SQL BÁSICO - DML

- Pesquisa Básica em Tabelas – o comando SELECT
- A sintaxe mais simples do SELECT é:

```
SELECT [DISTINCT | ALL] { * | coluna [,coluna, ...] }
```

```
FROM tabela;
```

- Para visualizar todas linhas e colunas de uma tabela:

```
SELECT * FROM CD;
```

- Para filtrar apenas algumas colunas:

```
SELECT cod_cd, nome_cd FROM CD;
```



# Métodos de Invasão de Redes e Sistemas

## SQL BÁSICO - DML

---

- Pesquisa Básica em Tabelas – o comando SELECT

- Ordenando o resultado:

```
SELECT cod_cd, nome_cd FROM CD ORDER BY
nome_cd;
```

- Agrupando o resultado:

```
SELECT cod_cd, nome_cd FROM CD GROUP BY
nome_cd;
```



# Métodos de Invasão de Redes e Sistemas

## SQL BÁSICO - DML

---

- Filtrando linhas
  - Para filtrar linhas em uma pesquisa, utilizamos a cláusula WHERE, onde definimos uma expressão lógica(condição) que será avaliada e mostrará apenas as linhas que atenderem ao critério estabelecido.

```
SELECT nome_cd, preco_venda
FROM CD
WHERE preco_venda > 10;
```



# Métodos de Invasão de Redes e Sistemas

## SQL BÁSICO - DML

---

- Operadores Relacionais
  - Definem um tipo de condição básica. Podemos usar os seguintes operadores:
    - = igual
    - < menor que
    - <= menor ou igual que
    - > maior
    - >= maior ou igual que
    - != ou <> diferente

## SQL BÁSICO - DML

- Operadores Lógicos
  - Utilizados quando apenas uma condição não é o suficiente para determinarmos o critério de busca. Podemos usar os seguintes operadores:
    - AND e condição1 e condição2
    - OR ou condição1 ou condição2
    - NOT ou !negação não-condição

```
SELECT nome_cd, preco_venda, cod_gravadora
FROM CD
WHERE preco_venda > 11 AND cod_gravadora = 3.
```



# Métodos de Invasão de Redes e Sistemas

## SQL BÁSICO - DML

---

- Operadores Especiais

- IS NULL : para saber se o conteúdo de uma coluna foi ou não inicializado.

```
SELECT nome_gravadora From GRAVADORA
WHERE endereco IS NULL;
```

- IS NOT NULL : negação do operador anterior.

```
SELECT nome_gravadora, endereco From GRAVADORA
WHERE endereco IS NOT NULL;
```

## SQL BÁSICO - DML

- Operadores Especiais

- BETWEEN : serve para determinar um intervalo de busca. Muito usado para simplificar a utilização do operador lógico AND.

```
SELECT nome_cd, preco_venda FROM CD
```

```
WHERE preco_venda BETWEEN 10 AND 20;
```

- De outra forma teríamos que utilizar:

```
SELECT nome_cd, preco_venda FROM CD
```

```
WHERE preco_venda >= 10 AND preco_venda <= 20;
```

## SQL BÁSICO - DML

- Operadores Especiais

- LIKE : usado para comparar cadeias de caracteres utilizando padrões de comparação para um ou mais caracteres.

|            |                                          |
|------------|------------------------------------------|
| LIKE 'A%'  | palavras iniciadas com A                 |
| LIKE '%A'  | palavras que terminem com A              |
| LIKE '%A%' | palavras com A em qualquer posição       |
| LIKE 'A_'  | string de 2 caracteres iniciado com A    |
| LIKE '_A'  | string de 2 caracteres terminado em A    |
| LIKE '_A_' | string de 3 caracteres sendo A o segundo |
| LIKE '%A_' | palavras com A na penúltima posição      |
| LIKE '_A%' | palavras com A na segunda posição        |





# Métodos de Invasão de Redes e Sistemas

## SQL BÁSICO - DML

---

- Operadores Especiais

```
SELECT * FROM AUTOR
```

```
WHERE nome_autor LIKE 'V%';
```

```
SELECT * FROM AUTOR
```

```
WHERE nome_autor LIKE '_I%';
```

```
SELECT * FROM AUTOR
```

```
WHERE nome_autor LIKE 'C_R%';
```

```
SELECT * FROM AUTOR
```

```
WHERE nome_autor LIKE 'V%';
```



# Métodos de Invasão de Redes e Sistemas

## SQL BÁSICO - DML

---

- Operadores Especiais
  - IN : permite comparar o valor de uma coluna com um conjunto de valores. Usado para substituir uma série de comparações seguidas usando a cláusula OR.

```
SELECT * FROM AUTOR
```

```
WHERE cod_autor IN (1,12,27);
```



# Métodos de Invasão de Redes e Sistemas

## SQL BÁSICO - DML

---

- Manipulação de Cadeias
  - LENGTH : retorna o número de caracteres contidos em uma cadeia de caracteres.

```
SELECT LENGTH('Renato Russo') From Autor
```

Retorna 12



# Métodos de Invasão de Redes e Sistemas

## SQL BÁSICO - DML

---

- Manipulação de Cadeias
  - UPPER e LOWER : usado quando não sabemos exatamente como a cadeia de caracteres foi armazenada no banco. O conteúdo do campo é comparado literalmente com a cadeia informada, levando-se em conta maiúsculas e minúsculas.
  - Se em nome\_autor tivermos ‘Vinicius’, a seguinte query não retorna nenhuma linha:  

```
SELECT * From AUTOR Where nome_autor = ‘VINICIUS’;
```



# Métodos de Invasão de Redes e Sistemas

## SQL BÁSICO - DML

---

- Manipulação de Cadeias
  - Para solucionar podemos utilizar:  
`SELECT * From AUTOR`  
`Where UPPER(nome_autor) = 'VINICIUS';`
  - Ou ainda:  
`SELECT * From AUTOR`  
`Where LOWER(nome_autor) = 'vinicius';`

## SQL BÁSICO - DML

- Manipulação de Datas
  - Quando criamos colunas com tipo de dado Data, podemos realizar uma série de cálculos e operações cronológicas.
  - O SQL especifica quatro tipos de dados relacionados a data e hora:
    - DATE            Apenas Data
    - TIME            Apenas Hora
    - TIMESTAMP    Data e Hora
    - INTERVAL      Intervalo entre os dois tipos de dados anteriores

## SQL BÁSICO - DML

- Manipulação de Datas

SELECT \* From CD

Where data\_lancamento = CURRENT\_DATE;

- Retorna os CDs lançados no dia de hoje.
- Uma coluna do tipo data é composta de seis elementos:
  - YEAR (ano)
  - MONTH (mês)
  - DAY (dia)
  - HOUR (hora)
  - MINUTE ( minuto)
  - SECOND (segundo)

## SQL INJECTION

---

- Uma das técnicas de fraude mais conhecida pelos desenvolvedores web é a SQL Injection. Trata-se da manipulação de uma instrução SQL através das variáveis que compõem os parâmetros recebidos por um script server-side, tal como PHP, ASP, ColdFusion e outros.



## SQL INJECTION

- O principal motivo pelo qual deve-se impossibilitar a utilização da SQL Injection está no fato de que, através de uma simples instrução SQL, como por exemplo, uma projeção de dados, outras operações podem ser executadas, podendo impactar sobre o esquema das tabelas, os dados armazenados, e até mesmo sobre elementos do sistema operacional, tendo em vista que alguns bancos de dados permitem a execução de comandos do shell do próprio sistema operacional.

# Métodos de Invasão de Redes e Sistemas

## SQL INJECTION

- Para ilustrar o conceito de SQL Injection, a seguinte simulação pode ser realizada.
- Imaginemos que um script de validação de acesso de usuários tenha sido desenvolvido como segue:

```
1 <?php
2
3 $usuario = $_POST['usuario'];
4 $senha = $_POST['senha'];
5
6 $query_string = "SELECT * FROM usuarios
7 WHERE codigo = '{ $usuario }' AND senha = '{ $senha }' ";
8
9 ?>
10
```

## SQL INJECTION

---

- Nas linhas 3 e 4, as variáveis \$usuario e \$senha, respectivamente, recebem o conteúdo submetido por um formulário através do método POST.
- É aí que mora o perigo !

# Métodos de Invasão de Redes e Sistemas

## SQL INJECTION

- Suponha que a seguinte entrada tenha sido informada no campo usuário no formulário chamador do script de validação.

Usuário:

Senha:

' or 1='1

- A query SQL resultante será:

```
SELECT * FROM usuarios WHERE codigo = ' ' AND senha = ' ' or 1='1'
```

entrada do usuário  
(\$senha)



# Métodos de Invasão de Redes e Sistemas

## SQL INJECTION

---

- Usando esta técnica, pode-se promover grandes estragos como demonstrado em alguns exemplos a seguir:

*SELECT fieldlist*

*FROM table*

*WHERE field = 'x' AND email IS NULL; --';*

- -- inicia um comentário em SQL o que faz a instrução desconsiderar o '; final da instrução original.

## SQL INJECTION

*SELECT email, passwd, login\_id, full\_name*

*FROM table*

*WHERE email = 'x' AND 1=(SELECT COUNT(\*) FROM  
tabname); --';*

*SELECT email, passwd, login\_id, full\_name*

*FROM members*

*WHERE email = 'x' OR full\_name LIKE '%Bob%';*



# Métodos de Invasão de Redes e Sistemas

## SQL INJECTION

---

```
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'x'; DROP TABLE members; --'; -- Boom!
```

```
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'x';
INSERT INTO members ('email','passwd','login_id','full_name')
VALUES ('steve@unixwiz.net','hello','steve','Steve Friedl');--';
```



# Métodos de Invasão de Redes e Sistemas

## SQL INJECTION

---

```
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'x';

UPDATE members
SET email = 'steve@unixwiz.net'
WHERE email = 'bob@example.com';
```



## SQL INJECTION

---

- Para que se esteja livre da utilização da SQL Injection, certas providências devem ser tomadas.
- Algumas das ações serão realizadas no servidor de banco de dados, outras devem ser garantidas pelo código fonte.

## SQL INJECTION

---

- Deve-se tomar cuidado com a configuração do usuário que estabelece a conexão com o banco de dados.
- O ideal é que as permissões de acesso deste usuário estejam restritamente limitadas às funções que irá realizar, ou seja, para a exibição de um relatório, a conexão com o banco de dados deve ser realizada por um usuário com permissões de leitura e acesso somente às tabelas necessárias para sua operação.

## SQL INJECTION

---

- Todos os valores originados da coleta de dados externos, devem ser validadas e tratadas a fim de impedir a execução de eventuais instruções destrutivas ou operações que não sejam as esperadas.

# Métodos de Invasão de Redes e Sistemas

## SQL INJECTION

- Um tratamento básico para a execução de queries com variáveis contendo valores informados pelo usuário:

```
1 <?php
2
3 $usuario = $_POST['usuario'];
4 $senha = $_POST['senha'];
5 $usuario_escape = addslashes($usuario);
6 $senha_escape = addslashes($senha);
7
8 $query_string = "SELECT * FROM usuarios
9 WHERE codigo = '{$usuario_escape}'
10 AND senha = '{$senha_escape}'";
11
12 ?>
```

# Métodos de Invasão de Redes e Sistemas

## SQL INJECTION

- Com a utilização da função addslashes() será adicionada uma barra invertida antes de cada aspa simples e aspa dupla encontrada, processo conhecido como escape.
- Abaixo, a query SQL resultante da aplicação desta função:

```
SELECT * FROM usuarios WHERE codigo = ' ' AND senha = '\ ' or 1='\ 1'
```

entrada do usuário  
após tratamento (\$senha)

## BUFFER OVERFLOW

---

- Para entender o que é um overflow, a tradução da palavra ajuda muito. Overflow significa inundação e, quando aplicada como termo da informática, significa um transbordamento que causa uma inundação.
- Os computadores possuem chips especiais chamados de memória. Estes chips especiais recebem o nome de memória porque guardam informações em forma de bits.

## BUFFER OVERFLOW

---

- Quando um programa está sendo executado, a sequência de instruções que deve ser seguida, a instrução que está sendo executada no momento, endereços, valores de constantes, valores de variáveis, etc, ficam armazenados na memória.

## BUFFER OVERFLOW

---

- Para que não haja bagunça, a memória é “loteada”, ou seja, são definidas áreas da memória para guardar cada coisa em seu lugar.
- Estas áreas, assim como em qualquer loteamento, possuem limites e são conhecidas como buffers.



## BUFFER OVERFLOW

- Cada “terreno” da memória (ou buffer), por sua vez, é dividido em células ou posições de memória.
- Cada uma destas posições é identificada por um número, o chamado endereço de memória.
- Em cada células pode ser guardado apenas um bit.

## BUFFER OVERFLOW

---

- Quando é preciso guardar bits na memória, o que geralmente é feito em grupos de 8 (byte), 16 (word), 32 (double word) ou 64 (quadword), também é preciso indicar o endereço no qual os bits devem ser colocados.

## BUFFER OVERFLOW

---

- Quando, por exemplo, o valor de uma variável de 32 bits é enviada para um endereço no finzinho do buffer onde, digamos, há apenas 20 células disponíveis, os bits da variável dão uma de MST e 12 deles invadem o terreno de algum vizinho, ou seja, causam um overflow.

## BUFFER OVERFLOW

---

- Resumindo: um overflow acontece sempre que alguns bits transbordam e invadem uma área que não lhes pertence.
- A sequência de execução de um programa

## BUFFER OVERFLOW

---

- Esta é uma falha de segurança comumente encontrada em software.
- Apesar de ser uma falha bem-conhecida e bastante séria, que se origina exclusivamente na incompetência do programador durante a implementação do programa, o erro repete-se sistematicamente a cada nova versão ou produto liberados.

## BUFFER OVERFLOW

---

- Alguns programas já são famosos por freqüentemente apresentarem a falha, como o Sendmail, módulos do Apache, e boa parte dos produtos da Microsoft, incluindo obviamente o infame Internet Information Services (IIS).
- Mesmo software considerado seguro, como o OpenSSH, já apresentou o problema.

## BUFFER OVERFLOW

---

- Um buffer overflow é resultado do armazenamento em um buffer de uma quantidade maior de dados do que sua capacidade .
- É claro que apenas linguagens de programação que não efetuam checagem de limite ou alteração dinâmica do tamanho do buffer são frágeis a este problema.

## BUFFER OVERFLOW

- O princípio é estourar o buffer e sobrescrever parte da pilha, alterando o valor das variáveis locais, valores dos parâmetros e/ou o endereço de retorno.
- Altera-se o endereço de retorno da função para que ele aponte para a área em que o código que se deseja executar encontra-se armazenado (código malicioso dentro do próprio buffer estourado ou até algum trecho de código presente no programa vulnerável).



## BUFFER OVERFLOW

---

- Pode-se assim executar código arbitrário com os privilégios do usuário que executa o programa vulnerável.

## CONCLUSÃO

---

- Cabe ao desenvolvedor estar atento às possíveis brechas de segurança existentes nos códigos fonte que produz, principalmente quando o que está em jogo é um bem de grande valia: a informação.



# Métodos de Invasão de Redes e Sistemas

## Sites Interessantes

---

<http://jarlsberg.appspot.com/>

<http://perso.crans.org/raffo/papers/phdthesis/thesisch1.html>

<http://securityhacker.org/>

[http://www.cic.unb.br/docentes/pedro/trabs/buffer\\_overflow.htm](http://www.cic.unb.br/docentes/pedro/trabs/buffer_overflow.htm)

<http://www.cert.br/>

<http://www.rnp.br/cais/>

<http://www.vivaolinux.com.br/artigo>

<http://www.invasao.com.br>

<http://www.invasao.com.br/2010/01/09/curso-de-tecnicas-de-intrusao-hackers/>