**UNIVERSIDADE FEDERAL DE UBERLÂNDIA**
**FEELT – FACULDADE DE ENGENHARIA ELÉTRICA**

PAULO JOSÉ CARMONA TEIXEIRA
11611ECP018

# SEGURANÇA EM REDES DE COMPUTADORES

Modelos e regras sobre segurança em redes de computadores

Uberlândia - MG
2019

## Sumário

## 1. **OBJETIVO**

Mostrar de forma simples e sucinta conceitos de segurança em redes de computadores, diferenciando e exemplificando meios de violações e proteção existentes.

## 2. **INTRODUÇÃO**

Quando ouvimos a palavra redes de computadores, imaginamos uma quantidade imensurável de computadores conectados, compartilhando todo tipo de informações o tempo todo, criando um vinculo entre eles, que assim denominamos de rede. E essa troca de informações são dadas de simples mensagens de texto, até transações bancarias, dados pessoais.

Com essa troca de informações frequentes e a grande dependência pessoal que a internet criou, ocasionou em um grande crescimento do numero de tentativas de roubo dos dados pessoais, invasões a computadores alheios, infecções por vírus, entre outras. Sendo assim, surge a necessidade de alto investimento e mercado na área de segurança de redes e consequentemente segurança de dados. Estima-se que hoje em dia um Ethical Hacker (responsável por realizar ataques e testar a segurança de uma dada empresa) receba valores de até R$100.000,00 se escolhido o modo BlackBox.

Esses investimentos são focados em: estruturas de segurança, como na criptografia dos dados, estudos de técnicas de ataques e invasões, sendo assim possível criar ferramentas de combate.

## 3. **SEGURANÇA DE REDES**

Se formos analisar desde os primórdios da Internet, das redes de computadores, falar de segurança era quase que um tema não falado, pois, antigamente, onde era o ponto das informações de valor, não se tinha acesso, e quando tinha, não era de fácil acesso. O acesso era feito localmente, pois essas estavam isoladas de qualquer acesso externo, então para se acessar, era necessário estar no local.

Hoje em dia, temos uma enorme diferença. A Internet foi capaz de nos proporcionar uma acessibilidade imensurável, hoje podemos conectar a maioria dos computadores, celulares, e produtos que possuem acesso a internet, e esses dispositivos compartilham dados frequentemente, e com isso a segurança ficou comprometida, se tornando assim um ponto crucial de pesquisa e trabalho. Um exemplo de uma grande empresa que é especializada no ramo é a CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil).

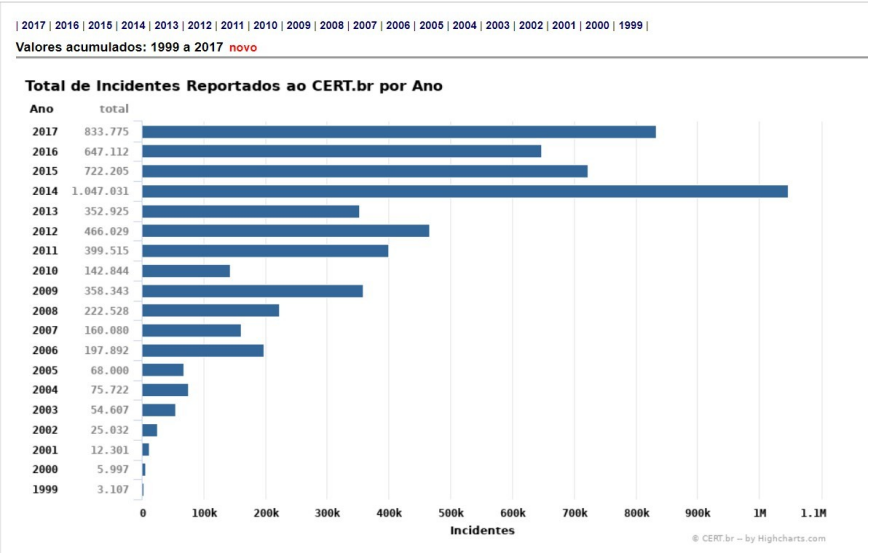


*Figura 1 – Total de incidentes segundo a CERT.br*

Segundo a CERT.br tivemos um grande avanço de invasões até 2014, e após essa data uma variação menor. Na Figura 1 podemos acompanhar a evolução dessas ameaças ao longo dos anos.

## 4. **TÉCNICAS DE INVASÃO**

Existem vários meios e tipos de invasão, cada um com suas principais técnicas, e a cada um aplicamos uma classificação ao invasor, que geralmente são Hackers, Crackers, Carders e entre outros. Cada profissional dessa área possui conhecimento específicos, porem todos possuem amplo conhecimento à segurança de redes e de sistemas operacionais, que são os requisitos essenciais para estudar e aplicar as técnicas de invasão.

- Keyloggers: São aplicativos que ficam em execução em um determinado computador para monitorar todas as entradas do teclado. É por isso que é dado o nome de Loggers.
- Spoofing: O invasor convence alguém de algo que não é, sem ter permissão para isso, conseguindo autenticação.
- FakeMail: Técnica mais comum utilizada, onde é enviado um e-mail ao receptor, como forma de propaganda, e ao clicar, se instala programas indevidos que coletam informações e dão acesso externo aos computadores de forma remota.
- Sniffer: É um programa de computador que monitora passivamente o tráfego de rede, ele pode ser utilizado legitimamente, pelo administrador do sistema para verificar problemas de rede ou pode ser usado ilegitimamente por um intruso, para roubar nomes de usuários e senhas. Este tipo de programa explora o fato dos pacotes das aplicações TCP/IP não serem criptografados.

- **SQL Injection:** É um ataque contra o banco de dados de uma empresa via web site. Nesse ataque, os crackers executam comandos não autorizados de SQL ao aproveitar sistemas inseguros que estão conectados na internet. O SQL Injection é a segunda mais comum vulnerabilidade em aplicações web, de acordo com o Open Web

  Application Security Project.

- **Code Injection e Script Injection:** Code injection nada mais é do que injetar código em um processo e fazer com que este processo execute determinado código. O Script Injection é um tipo de Code Injection, porém é um ataque específico da web.

## 5. **TECNICAS DE PROTEÇÃO**

As técnicas de proteção, foram desenvolvidas para que os usuários tenham uma segurança satisfatória. Dado as diversas técnicas e meios de invasão atuais, que continuam em constante crescimento, as técnicas de proteção não encobrem totalmente, apenas parte das técnicas, sendo necessário que o usuário busque constantemente apoio e auxilio de Anti-Malwares.

Dentre as diversas técnicas, destacam-se Assinatura Digital, Autenticação, Controle de Roteamento, Hardwares e Softwares de confiança, Criptografia e diversas outras.

- Assinatura Digital: Garante que a mensagem assinada teve suas informações geradas com a privacidade de quem as assinou. Sendo assim, garante a confiança dos dados, sem que haja adulterações.
- Autenticação: Próprio nome informa, identifica os usuários e mensagens.
- Controle de Roteamento: Determina quais rotas os dados devem seguir, ou seja, serem transmitidas. Muito usado no desenvolvimento Web onde deixamos na pasta public os dados a serem a mostra, e na parte externa da pasta no servidor os dados

importantes da regra de negócio. E o controle de roteamento é responsável por fazer essa ligação entre as pastas.

- Hardware e Softwares de confiança: Demonstram garantias de funcionalidades, segurança satisfatória, e notas altas em benchmarks.
- Criptografia: É uma codificação (alteração da mensagem no envio do host) no qual apenas o destinatário consegue decodificar, garantindo assim que terceiros não consigam acesso as informações corretas.

## 6. **MERCADO DE TRABALHO**

O mercado de trabalho é muito amplo, possuindo diversos profissionais, e diversos tipos de contrato, uma vez que cada contrato interliga preço, dificuldade, conhecimento e mercado, entre as principais profissões da área se destaca o Ethical Hacking, que é responsável por efetuar diversos testes, quebras de informações, ataques com as técnicas descritas e demais, todos esses passos são feitos, e em seguida são descritos em um relatório, que será entregue de forma combinada com o contratante.

O salário inicial varia de R$2.000,00u a R$5.000,00 fixos, e contratos podem variar e chegar a preços de R$100.000,00.

O Ethical Hacking é uma profissão cujo é obrigatório diversos certificados.

## 7. **CONCLUSÃO**

Com todas essas informações, entendemos os problemas e algumas soluções possíveis para se planejar uma rede de computadores, independente da finalidade. Devemos projetar um sistema capaz de suprir todos as necessidades de segurança, para prevenir ataques externos e vazamento de informações sensíveis. E como empresa, descobrimos um meio (Ethical Hacking) de sempre testar as seguranças de forma segura, visando assim melhorias no sistema da mesma.

## 8. **REFERENCIAS BIBLIOGRÁFICAS**


[1] DE SOUZA, Ricardo José Cabeça. Segurança de Redes de Computadores.

[2] KUROSE, James F.; ROSS, Keith W. Redes de Computadores e a Internet.

[3] MORENO, Daniel; Introdução ao Pentest. Ediitora Novatec.

[4] NAKAMURA, Nakamura Emilio Tissato & Geus Paulo Lício de Segurança de Redes – em ambientes cooperativos, Segunda Edição, São Paulo, Novatec Editora, 2010.


**Obs:** Link dos arquivos do trabalho armazenado no Github

https://github.com/Paulojct1/REDES_2019_1