Redes de Computadores

Conceitos Gerais

1. Introdução

- Uma rede de computadores é caracterizada pela interconexão de estações de trabalho, periféricos, terminais ou outros dispositivos.

- Stallings define uma rede de computadores como: “quando dois ou mais computadores estão interconectados via uma rede de comunicação”.

Estrutura:

1. **Estações de trabalho**: desktops, laptops e dispositivos móveis em geral (smartphones, tablet, etc).
2. **Meios de Comunicação**: Cabos, ar, eletricidade etc.
3. **Equipamentos de infraestrutura de rede**: hubs, switches, roteadores etc.

1. Introdução

- Uma rede de computadores bem estruturada possibilita:

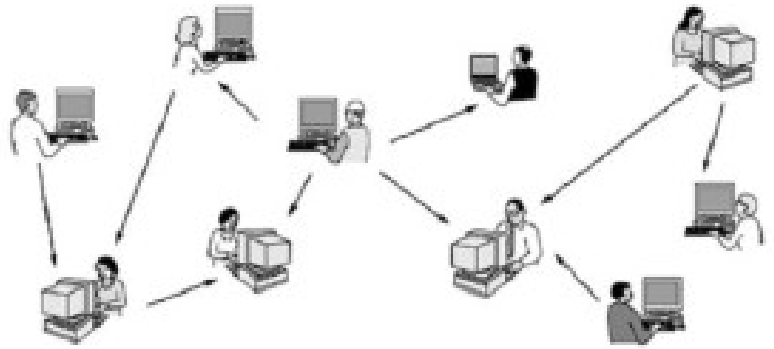
1. **Permitir aos usuários acesso remoto a serviços e aplicações**: correio eletrônico, comércio eletrônico e Internet Banking;

2. **Permitir comunicação entre os usuários**: Chat, voz sobre IP, Videoconferência e troca de arquivos;

3. **Compartilhamento de recursos**: Impressora de rede, armazenamento e processamento remoto (ex. grids computacionais). Explicaremos mais tarde alguns desses conceitos.

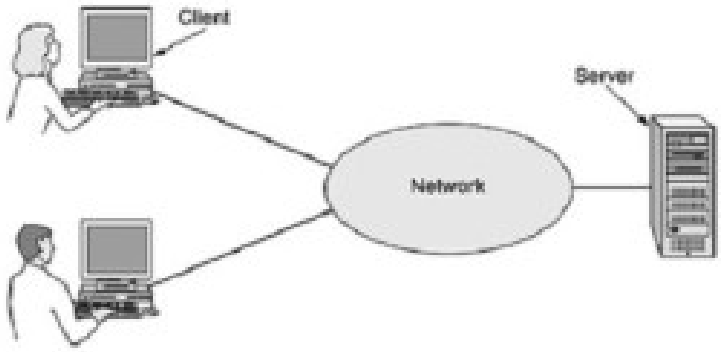
2. Tipos de Redes quanto a Forma de Interação

- **Rede Par-a-Par**: Cada usuário compartilha e coleta os dados que desejar. Podemos dizer que cada computador funciona como cliente e como servidor de forma dinâmica. Esse tipo de rede também é conhecida como ponto-a-ponto ou peer-to-peer (P2P).
- Um exemplo desta rede seria o Torrent.



2. Tipos de Redes quanto a Forma de Interação

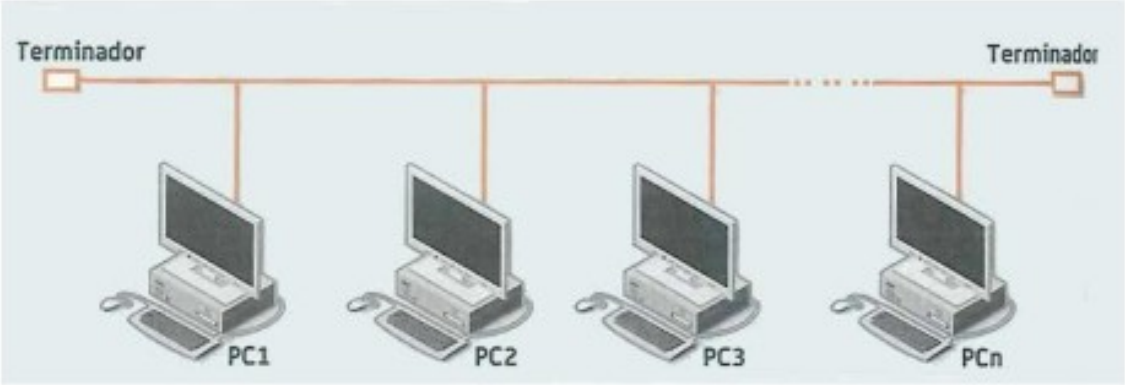
- **REDES CLIENTE-SERVIDOR**: Nessa categoria, surge o computador responsável por controlar e fornecer os dados e serviço da rede. É o tipo mais usado no meio corporativo, pois é necessário maior controle da rede.



3. Topologia de Redes

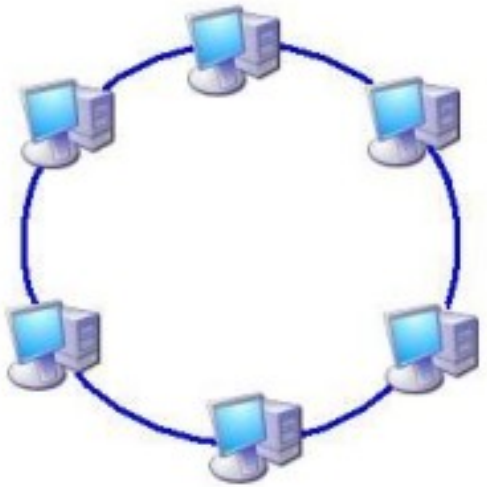
- **Barramento:** Quando um computador transmite todo o meio de transmissão é ocupado, impossibilitando os demais de transmitir naquele instante, para evitar colisão. A expansão da rede é complexa, e limitada pelo tamanho do barramento.

- Possui uma boa tolerância a falhas, pois caso algum computador pare de funcionar, não afetará os demais. Exemplo: TV por assinatura antigamente (NET)



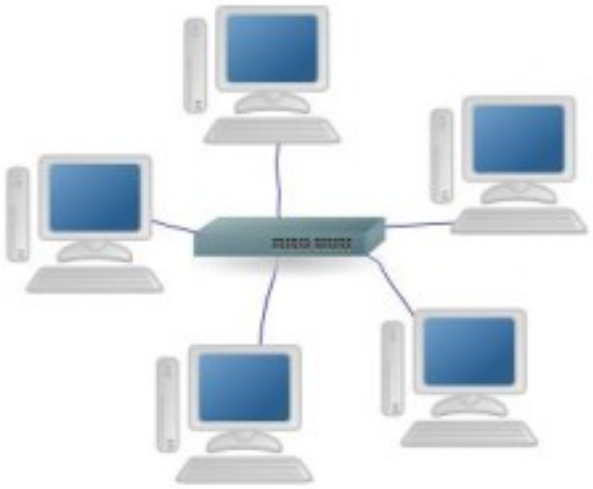
3. Topologia de Redes

- **Anel:** O protocolo mais usado nesta topologia é o TOKEN RING. Basicamente, um token é passado de estação a estação por um período determinado de tempo e enquanto se possui o token, há a liberação para transmissão dos dados. Isso evita a colisão.
- Geralmente os dados trafegam de forma unidirecional, mas pode ser bidirecional. Não é tolerante a falhas, pois um nó quebrado compromete a rede.



3. Topologia de Redes

- **Estrela:** É caracterizada por conexões ponto-a-ponto em torno de um nó central (hub, switch, roteador) o qual direcionará as mensagens. Possui uma capacidade de gerência na rede, permitindo controle de velocidade, permissões, etc.
- Se o nó central falhar, toda a rede torna-se inoperante.

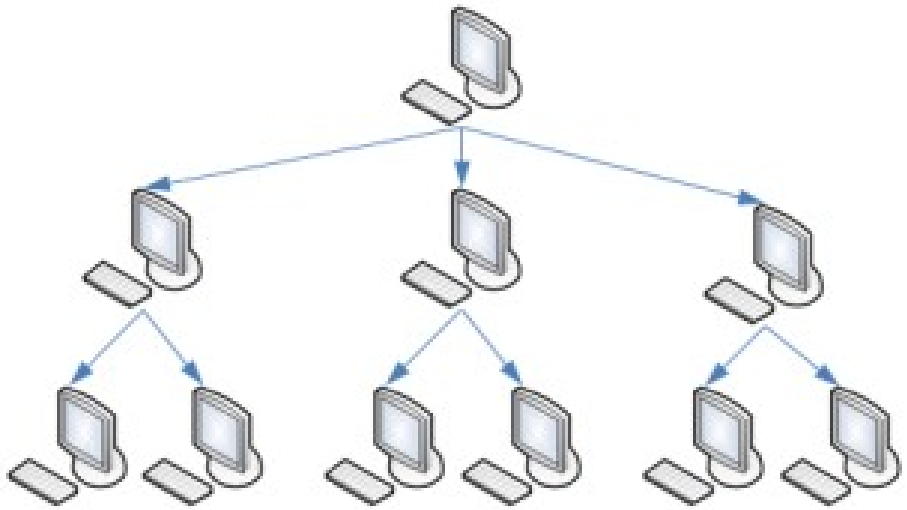


3. Topologia de Redes

- **Mesh:** Também conhecida como malha. É caracterizada pela interconexão entre quase todos os nós da rede entre si. Como cada nó conversa com todos os outros nós, não existe problema de colisão e o desempenho geralmente é bom (comunicação direta).
- Possui uma excelente tolerância a falhas. A expansão da rede é complexa e de alto custo.

3. Topologia de Redes

- **Arvore:** Seria uma conexão de forma hierárquica de várias redes estrelas. Atualmente, a interligação entre os roteadores e switches na Internet segue esse padrão. Possui uma boa escalabilidade além de uma boa tolerância a falhas.



4. Meios de Transmissão

- **Cabo Coaxial**: Cabo metálico (usado por TV a cabo). É mais grosso e difícil de ser manuseado. Sofre com interferência do meio. Aceita longas distâncias (100 até 500m). Velocidade de 10mbps.
- **Cabo Par Trançado**: É o padrão para redes locais. Possui várias categorias, com velocidades que passam facilmente dos 100Mbps. Possui blindagem contra interferência. Mais maleável e custo mais acessível. A distância máxima é de 100m (menos coaxial).
- **Fibra Óptica**: Utilizam tanto do fenômeno da refração e reflexão internas da luz na Fibra. A distância máxima pode passar de 70Km, com velocidade de ddd. São imunes a interferência.

5. Equipamentos de Rede

- Placa de Rede: Permite a conexão do computador com a rede. Cada placa possui um identificador único chamado de MAC. Esse endereço é formado por 48 bits e são expressos na forma hexadecimal, por exemplo: 24:6E:2A:91:41:D1
- HUB: Faz a interconexão entre os nós da rede. Entretanto, ele faz o envio dos dados para todos os nós (broadcast).
- Switch: Também faz a conexão dos nós, mas é capaz de isolar as portas e enviar os dados para o nó correto. Reduz o trafego de rede e possui melhor desempenho.

6. Protocolo TCP/IP

- O **TCP/IP** é como um conjunto de regras que os computadores usam para se comunicar entre si. Ele é dividido em dois principais protocolos:

  1. IP (Internet Protocol): é o responsável por endereçar as mensagens — como colocar o endereço do destinatário em uma carta.

  2. TCP (Transmission Control Protocol): é o que garante que a mensagem chegue direitinho, sem erros ou pedaços faltando — como se fosse um serviço dos Correios que garante a entrega completa e na ordem certa.

- Exemplo: Ao enviar uma foto para um amigo pelo WhatsApp, o IP garante que a foto vá para o celular certo, e o TCP garante que ela chegue inteira, mesmo que vá dividida em "pedacinhos".

6. Protocolo TCP/IP

- **IP** significa **Internet Protocol**. Ele pode ser associado como o "endereço da residencia de computador ou celular conectados a internet ou em uma rede local. Sem esse número, não tem como saber para onde enviar as mensagens.
- Um endereço IP pode parecer com isso: 192.168.1.10
- Cada número separado por ponto pode ir de 0 a 255.
- Existem dois tipos principais de IP:

  1. IPv4 (o mais comum): como o exemplo acima.

  2. IPv6 (mais novo, com números bem maiores): criado porque o IPv4 está ficando sem espaço.

6. Protocolo TCP/IP

- Outro conceito importante é a **máscara de sub-rede**. Definimos ela como uma forma de determinar o tamanho da rede. Ela permite saber se o destino da mensagem está na mesma rede local ou se precisa ser enviada para outro lugar (Internet por exemplo).
- Exemplo de máscara: 255.255.255.0
- Se o IP do seu computador é 192.168.1.10 e a máscara é 255.255.255.0, isso quer dizer que todos os IPs de 192.168.1.1 até 192.168.1.254 estão na rede local.

6. Protocolo TCP/IP

- Outro serviço importante de redes é o **DNS** (Domain Name System). Ele é como a "agenda de contatos" da internet.

- Ao invés do usuário decorar todos os IP’s, ele pode usar nomes mais fáceis, como google.com. O DNS faz a conversão do nome para IP

- Exemplo:

- Quando você digita www.youtube.com, o DNS traduz esse nome para o IP verdadeiro do servidor do YouTube, tipo 142.250.78.206. Aí sim o seu computador sabe para onde mandar o pedido para carregar o vídeo.

6. Protocolo TCP/IP

- Em resumo, quando o usuário acessa um site, temos a sequência:

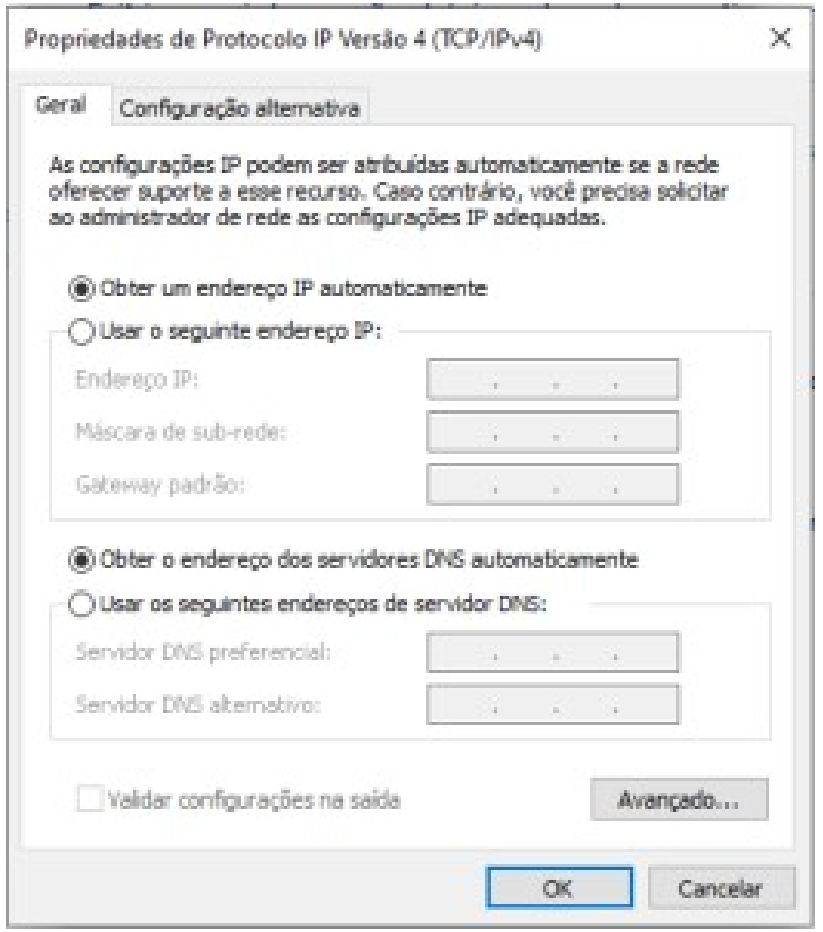
  1. Usuário digita um nome: (como www.exemplo.com).
  2. O DNS traduz esse nome para um endereço IP.
  3. O computador usa o IP e a máscara para saber se o destino está na mesma rede.
  4. Se não estiver, ele envia os dados para o gateway (roteador).
  5. O TCP/IP cuida para que a mensagem chegue certinho ao destino.

6. Protocolo TCP/IP

- **Gateway**: Um gateway (ou porta de enlace) é o ponto de saída da sua rede local para outra rede, geralmente a internet. Ele atua como uma ponte de comunicação entre redes diferentes.
- Mais tecnicamente, o gateway é um dispositivo (geralmente um roteador) que recebe os pacotes da sua rede local (LAN) e os envia para uma rede externa, como a internet.
- Imagine sua casa conectada à internet: Seu celular, PC e TV estão conectados ao roteador. Cada um desses dispositivos tem um IP local, como: Celular: 192.168.0.10, PC: 192.168.0.20 e TV: 192.168.0.30
- O roteador tem:
- Um IP interno (na rede local): 192.168.0.1
- Um IP externo (na internet): algo como 187.45.200.12
- O gateway padrão da rede é 192.168.0.1, ou seja, o endereço do roteador.

6. Protocolo TCP/IP

- No painel de controle do windows, temos a tela para configuração da rede:



7. Computação em Nuvem (Cloud)

- No painel de controle do windows, temos a tela para configuração da rede:
- **A computação em nuvem é a entrega de serviços de computação - incluindo servidores, armazenamento, bancos de dados, redes, software, análises e inteligência - pela Internet ("a nuvem").**

- **Principais Modelos de Serviço**

- **IaaS: Fornece infraestrutura básica de TI como serviço, permitindo que as empresas aluguem servidores virtuais e armazenamento. Exemplos: Amazon EC2.**

- **PaaS: Oferece uma plataforma para desenvolvimento e implantação de aplicativos, permitindo que os desenvolvedores se concentrem na codificação.**

7. Computação em Nuvem (Cloud)

- **Nuvem Pública**: Infraestrutura e serviços são disponibilizados ao público pela Internet. Exemplos: AWS, Azure.

- **Nuvem Privada**: Infraestrutura é utilizada exclusivamente por uma única organização. Exemplos: Nuvens privadas internas de grandes corporações.

- **Nuvem Híbrida**: Combinação de nuvens públicas e privadas, permitindo que dados e aplicativos sejam compartilhados entre elas. Exemplos: Empresas que utilizam serviços públicos para certas funções enquanto mantêm dados sensíveis em uma nuvem privada.

7. Computação em Nuvem (Cloud)

- **Principais serviços de Nuvem:**

- **Amazon Web Services (AWS)**: Maior e mais completo provedor de serviços em nuvem.

- **Microsoft Azure**: Integrado com produtos Microsoft, muito usado por empresas que já utilizam Windows Server.

- **Google Cloud Platform (GCP)**: Forte em análise de dados e aprendizado de máquina.

7. Computação em Nuvem (Cloud)

- **Vantagens dos serviços de Nuvem:**

- **Escalabilidade: Fácil ajuste de recursos conforme a demanda.**
- **Flexibilidade: Acesso a partir de qualquer lugar com conexão à internet.**
- **Redução de custos: Menos investimentos iniciais em hardware e manutenção.**
- **Manutenção automática: Atualizações e manutenções são gerenciadas pelo provedor.**
- **Acessibilidade e colaboração: Colaboração em tempo real entre equipes dispersas geograficamente.**

8. AWS

- **AWS é uma plataforma de serviços de computação em nuvem oferecida pela Amazon.**

- **Lançada em 2006, é atualmente uma das maiores e mais amplamente adotadas plataformas de nuvem do mundo.**

8.1 Serviços da AWS

- **Computação**:
- **1. Amazon EC2 (Elastic Compute Cloud): Serviço de máquinas virtuais escaláveis.**
- **2. AWS Lambda: Serviço de computação sem servidor que executa código em resposta a eventos.**

- **Armazenamento**:
- **1. Amazon S3 (Simple Storage Service): Armazenamento de objetos em nuvem.**
- **2. Amazon EBS (Elastic Block Store): Armazenamento de blocos para uso com EC2.**

- **Bancos de Dados:**
- **1. Amazon RDS (Relational Database Service): Bancos de dados gerenciados, como MySQL, PostgreSQL.**
- **2. Amazon DynamoDB: Banco de dados NoSQL totalmente gerenciado.**

8.1 Serviços da AWS

- **Redes:**
- **1. Amazon VPC (Virtual Private Cloud): Redes virtuais isoladas.**
- **2. Amazon Route 53: Serviço de DNS escalável e de alta disponibilidade.**

- **Segurança e Gerenciamento:**
- **1. AWS IAM (Identity and Access Management): Controle de acesso granular para serviços e recursos.**
- **2. AWS CloudTrail: Auditoria de conta e registro de atividades da API.**

8.2 Casos de USO da AWS

- **Casos de Uso da AWS**

- **Startups: Permite que pequenas empresas escalem rapidamente suas operações sem grandes investimentos iniciais.**

- **Empresas: Empresas como Netflix, Airbnb e Spotify utilizam AWS para gerenciar suas infraestruturas.**

- **Setor Público: Instituições governamentais e educacionais utilizam AWS para projetos de pesquisa, análise de dados e armazenamento seguro.**

9. Segurança de Redes

- Considerando a era da Informação em que nos encontramos atualmente, aspectos de Segurança digital são fundamentais em qualquer ambiente.

- Existem muitas empresas que possuem basicamente o centro dos seus negócios centrado em dados e informações (Google, Amazon). Alguns especialistas dizem que dados são o novo petróleo.

- Assim como o uso da computação e das redes de comunicação cresceram, também aumentaram de forma exponencial os golpes e ataques virtuais.

- A área de segurança da informação tem como objetivo identificar e elaborar técnicas que possam proteger servidores e sistemas destes ataques.

9. Segurança de Redes

- Podemos definir como os 3 pilares da segurança da informação como:

  1. **Confidencialidade**
  2. **Integridade**
  3. **Disponibilidade**

9. Segurança de Redes

- Alguns autores expandem estes 3 pilares da segurança com mais alguns pontos:

  4. **Autenticidade –** O princípio da autenticidade busca garantir que determinada pessoa ou sistema é, de fato, quem ela diz ser. Ex: Login e senha diz quem é o usuário.

  5. **Não-Repúdio (Irretratabilidade**) **–** Neste princípio, busca-se garantir que o usuário não tenha condições de negar o fato de que foi ele quem gerou determinada ação.

  6. **Irretroatividade**: Não deve ser possível reverter um evento ou ação uma vez que ele tenha sido executado e registrado. Ex: Uma transação bancária realizada não pode ter desfeita. Uma assinatura digital realizada não pode ser desfeita. Transações de um sistema empresarial não pode ter data e usuário modificados.

9.1. Varredura de Redes (Scan)

- A varredura em redes é uma técnica que geralmente antecede ataques. Essa técnica visa a obtenção de informações que subsidiarão as ações dos atacantes, como a busca de vulnerabilidades.
- Fazer a varredura fora da rede é mais complexo, pois o firewall costuma identificar e bloquear.
- Por isso, os hackers costuma infectar um computador interno da rede com um software de varredura para obter informações.
- Geralmente, a varredura é o primeiro passo para uma invasão mais agressiva.

9.2. Tipos de Ataques

- **Spoofing**: Se passar por alguma pessoa, instituição ou dispositivo que possua certo grau de confiabilidade para dar confiança à informação enviada. Por exemplo, posso enviar e-mails em nome da Receita Federal.

- **Man in the Middle**: Se inserir no meio da comunicação entre dois nós e capturar/modificar a informação trocada.

- **Sniffing**: É uma técnica que consiste em inspecionar os dados trafegados em toda a rede por meio do uso de programas chamados de sniffers (Ex. Wireshark).

- **Brute Force**: Tentar descobrir uma senha ou alguma outra informação através do método de tentativa e erro de forma exaustiva. Senha simples são quebradas facilmente.

- **Desfiguração (defacement)**: Técnica que consiste em alterar o conteúdo de uma página Web. Possui um caráter unicamente de vandalismo. Para isso explora vulnerabilidades na página ou no servidor.

9.2. Tipos de Ataques

- **Phishing**: Geralmente usado junto com o spoofing. O Spoofing induz o usuário a clicar em um link que irá direcionar para um site falso ou instalar um software malicioso.
- **Pharming**: Este tipo de ataque ocorre quando um tráfego que originalmente deveria ir para um site legítimo é redirecionado para outro. Geralmente um software malicioso altera este trafego em algum lugar da rede.
- **Ddos** (Negação de serviço): Gerar artificialmente um grande tráfego em determinado sistema/servidor e derrubar o serviço.
- **Engenharia Social:** Enganar usuários para que os demais ataques possam ser realizados.
- **Spyware**: Este tipo de malware foca na obtenção de informações de um host através do monitoramento de suas atividades. Em seguida envia para terceiros. Ex: keyloggers.
- **Botnet**: São programas que permitem a comunicação e controle do invasor sobre o sistema da vítima por intermédio de acessos remotos.

9.2. Tipos de Ataques

- **Ransomware**: Sequestro dos dados. O atacante criptografa os dados do computador, e libera a chave apenas mediante pagamento.

9.3. Tipos de Malwares (vírus)

- Os principais tipos de vírus são:

Vírus de Boot: Infecta a área de inicialização dos sistemas operacionais, também conhecido como MBR (Master Boot Record) do disco rígido. Esse tipo de vírus não corrompe arquivos específicos, mas sim, todo o disco. Os antivírus comuns de sistemas operacionais não são capazes de detectar esse tipo vírus, sendo necessário uma varredura antes da inicialização do sistema para sua detecção.

Vírus de Arquivo: Infecta arquivos de programas executáveis, geralmente, nas extensões .EXE e .COM. Ao se executar o referido programa, ativa-se o vírus.

Vírus Residente: Este é carregado diretamente na memória RAM do SO toda vez que o SO é iniciado. Este tipo de vírus pode ser extremamente danoso, bloqueando acessos à memória RAM, interromper determinados processos e funções a serem executadas e inclusive, alterar tais funções para fins maliciosos.

Vírus propagado por e-mail: recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no computador.

Vírus de script: escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página Web ou também por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador Web e do programa leitor de e-mails do usuário.