

PROTOCOLO XMPP

- O Protocolo XMPP (Extensible Messaging and Presence Protocol) é um protocolo aberto e extensível baseado em XML (Linguagem de Marcação Extensível), que promove a segurança digital e a privacidade online. Ele facilita a troca de mensagens em tempo real e a gestão de presença entre sistemas de comunicação.
- XMPP atua como um middleware crucial para ambientes de nuvem, além de ser compatível com a Internet das Coisas (IoT).
- Sua arquitetura é semelhante a outros protocolos de aplicação, como SMTP.
- Funciona através da troca distribuída de mensagens instantâneas em tempo real entre usuários e outras aplicações, operando sobre sockets TCP e utilizando mensagens XML para comunicação assíncrona.
- Devido à sua eficiência em termos de largura de banda e assincronia, a conexão TCP reduz o custo de banda, congestionamento de rede, latência, uso de CPU e memória. Além disso, por ser aberto, qualquer pessoa pode implementar um cliente ou servidor XMPP.
- A segurança do XMPP é reforçada com suporte a criptografia TLS/SSL, garantindo a confidencialidade e integridade das comunicações.
- O princípio de gateways permite a comunicação entre redes XMPP e outras redes com diferentes protocolos, como MSN e ICQ.
- É amplamente utilizado em aplicativos de mensagens instantâneas, redes sociais e serviços de Voz sobre IP (VoIP), como Google Talk.
- Mensagens são entregues aos usuários quando online e offline, as mensagens ficam em espera até que o usuário se conecte.

- Servidores XMPP também são conhecidos como servidores Jabber, nome dado pela comunidade que desenvolveu o XMPP.

PROTOCOLO DNS sobre HTTPS

- O Protocolo DNS sobre HTTPS (DoH) é um protocolo que visa melhorar a privacidade e segurança das consultas DNS, criptografando tanto as consultas quanto as respostas. Ele requer autenticação, tornando mais difícil a invasão por terceiros, sendo uma alternativa ao Protocolo DoT.
- Funciona através de consultas e respostas DNS enviadas via protocolos HTTP ou HTTP/2.
- Os usuários podem configurar seus dispositivos para usar um servidor DNS com suporte a DoH. No entanto, DoH pode apresentar desafios para administradores de rede ao dificultar a implementação de políticas de segurança e a detecção de ameaças estabelecidas, como censura e filtros baseados em DNS. É aconselhável avaliar se a aplicação do DoH é necessária antes de implementá-lo.

PROTOCOLO NFS

- O Protocolo NFS (Network File System) é um protocolo de padrão aberto que funciona no modelo cliente-servidor, permitindo que sistemas operacionais compartilhem arquivos de forma transparente através de redes locais e remotas.
- O funcionamento do NFS é realizado através da montagem de diretórios remotos como parte da árvore de diretórios local, permitindo que vários usuários compartilhem os mesmos arquivos sem conflitos de dados.
- Os arquivos podem ser acessados para leitura, escrita ou gerenciamento, dependendo das permissões concedidas pelo responsável pelo armazenamento dos arquivos.

- É amplamente utilizado em ambientes Unix/Linux, com suporte também para outros sistemas operacionais e softwares.
- A versão mais recente, NFSv4, oferece melhorias significativas em segurança, gerenciamento de sessões e suporte a IPv6. No entanto, ainda requer configurações como suporte a autenticação Kerberos e criptografia, além de políticas de acesso e firewalls.

PROTOCOLO BitTorrent

- O Protocolo BitTorrent é um sistema de compartilhamento e download de arquivos entre usuários através de uma rede descentralizada, utilizando comunicação peer-to-peer (P2P).
- Quando um usuário baixa um arquivo pelo BitTorrent, ele baixa partes do arquivo (chunks) de vários outros usuários que já possuem essas partes, reduzindo a carga nos servidores centralizados e facilitando o download.
- Torrents são arquivos de metadados que contêm informações sobre o arquivo compartilhado, como nome, tamanho, número de chunks e endereços de onde os arquivos estão sendo compartilhados.
- Para usar o protocolo BitTorrent, é necessário seguir as regras e procedimentos estabelecidos para garantir uma comunicação eficaz, evitando perdas na troca de chunks, congestionamentos e assegurando a integridade dos dados baixados.
- Um exemplo de uso do protocolo é na distribuição de atualizações de software em sistemas como Linux e na distribuição de conteúdo de domínio público.

Link vídeo protocolos em uso no linux:

https://drive.google.com/file/d/19rk-yO0TRFG080Yj6eS311koiNuM-w-R/view?usp=drive_link