1.Protocolos seguros

Seja enviando tráfego por uma rede com fio ou sem fio, é essencial garantir que todas as informações transmitidas estejam protegidas. Uma das melhores formas de proteger o tráfego da rede é criptografando todos os dados. No entanto, a criptografia nem sempre foi uma prática comum, e ainda existem muitos protocolos que enviam dados sem qualquer tipo de proteção.

Alguns dos protocolos mais utilizados no dia a dia, como **Telnet, FTP, SMTP e IMAP**, transmitem informações sem criptografia, permitindo que qualquer pessoa com acesso à rede intercepte esses dados. Para entender melhor o quanto do tráfego da sua rede está sendo enviado de forma segura, é possível capturar os pacotes de dados. Dentro desses pacotes, os cabeçalhos devem ser visíveis, mas todo o conteúdo interno deveria estar criptografado. Se for possível visualizar os dados enviados dentro dos pacotes, isso significa que o protocolo em uso não está protegendo as informações adequadamente.

Um exemplo de como esse problema pode ser exposto ocorre na conferência de segurança **DEFCON**, onde existe um painel chamado **Wall of Sheep**. Esse painel exibe uma lista de participantes que usaram protocolos inseguros, revelando seus nomes de usuário, parte de suas senhas (com os últimos caracteres ocultados), endereços IP e os protocolos utilizados. Entre os serviços mais frequentemente expostos no Wall of Sheep estão **IMAP, HTTP e POP3**, todos considerados inseguros.

O objetivo deve ser sempre utilizar protocolos seguros que protejam os dados transmitidos por meio de criptografia. Se não for possível utilizar um protocolo seguro, é preferível não usar o aplicativo correspondente. Por exemplo, ao acessar um dispositivo remotamente, em vez de utilizar **Telnet**, que é inseguro, deve-se optar pelo **SSH (Secure Shell)**. Da mesma forma, em navegação web, é recomendável utilizar **HTTPS** em vez de **HTTP**. Para e-mails, em vez de utilizar **IMAP**, é preferível configurar o cliente de e-mail para utilizar o IMAPS, que protege os dados por criptografia. Para transferências de arquivos, **SFTP** é uma alternativa segura ao **FTP** tradicional.

Uma maneira de identificar se um protocolo é seguro ou não é observar a **porta** utilizada. Alguns protocolos possuem versões seguras e inseguras utilizando portas diferentes. Por exemplo, se um tráfego de rede estiver utilizando a **porta 80**, ele provavelmente está usando **HTTP**, que transmite dados sem criptografia. Já se estiver utilizando a **porta 443**, é provável que o tráfego esteja sendo transmitido via **HTTPS**, que automaticamente criptografa os dados.

No entanto, apenas verificar a porta não é suficiente para garantir que o tráfego esteja seguro. Algumas implementações podem utilizar a porta correta, mas sem ativar as configurações de segurança adequadas. Por isso, é importante verificar as

configurações do servidor e, se necessário, capturar pacotes de rede para confirmar que os dados estão sendo transmitidos de forma criptografada.

Por exemplo, ao capturar o tráfego de um site que utiliza a porta **80**, é possível visualizar todo o conteúdo transmitido em **HTTP** sem criptografia, tornando as informações legíveis dentro da captura de pacotes.

Com tantas diferenças entre protocolos seguros e inseguros, uma alternativa para garantir que todos os dados sejam transmitidos de forma protegida é **criptografar o tráfego da rede como um todo**, independentemente do aplicativo utilizado.

Se uma rede sem fio **802.11** estiver configurada como um **ponto de acesso aberto**, todo o tráfego será transmitido sem criptografia. Para resolver isso, pode-se configurar o roteador para utilizar **WPA3** ou outro protocolo de criptografia, garantindo que todas as informações enviadas estejam protegidas.

Outra forma de proteger a transmissão de dados é utilizando uma **VPN (Virtual Private Network)**, que cria um túnel criptografado entre o dispositivo do usuário e um **concentrador de VPN**. Com essa abordagem, todo o tráfego entre o usuário e a VPN será protegido. O concentrador descriptografa os dados antes de enviá-los para o destino final, garantindo que ninguém na rede local possa interceptar as informações.

Embora uma VPN forneça uma camada adicional de segurança, ela pode exigir a instalação de um software específico no dispositivo do usuário e, em alguns casos, pode ser necessário configurar um **servidor VPN próprio** ou contratar um serviço terceirizado.