# CAP2

Intervenientes

Foi realizada a captura de tráfego de uma sessão de correio eletrónico utilizando o protocolo POP3 (Post Office Protocol v3). A sessão POP3 analisada funciona sobre o protocolo TCP (Transmission Control Protocol) na porta 110, entre dois intervenientes:

* **Fonte (Source):** 192.168.2.100 (um dispositivo na rede local)
* **Destino (Destination):** 64.246.26.20 (um servidor remoto)

Principal Protocolo

O protocolo principal utilizado é o POP3 (Post Office Protocol v3),como é demonstrado na linha 4. O POP3 é um protocolo amplamente utilizado para receber emails, permitindo que o utilizador descarregue emails de um servidor remoto para o seu dispositivo local.

O POP3 opera num modelo de cliente-servidor, onde o cliente solicita ao servidor o conteúdo da caixa de correio. É considerado um protocolo "pull", no sentido em que o cliente inicia as conexões e requisita as mensagens. Embora este seja um protocolo eficiente para transferir emails, o mesmo apresenta limitações em termos de segurança, pois a comunicação é transmitida em texto simples, tornando-a suscetível a intercetações e outros ataques.

Operações do Protocolo

A comunicação inicia-se com o estabelecimento de uma conexão TCP (linhas 1 e 2), onde o cliente (192.168.2.100) envia um SYN para iniciar a conexão e o servidor responde com um pacote SYN, ACK confirmando a receção. Finalmente, o cliente responde com um pacote ACK estabelecendo a conexão TCP. De salientar que estes 3 passos fazem parte do **three-way handshake** e são fundamentais para garantir uma conexão confiável antes da transmissão dos dados.

Após o estabelecimento da conexão, há a troca de comandos POP3, transmitidos em texto simples e sem criptografia:

* O comando USER test2@colasoft.com (linha 5) é utilizado para fornecer o nome de utilizador ao servidor.
* O servidor responde com uma mensagem de confirmação (**+OK**), indicando que o nome de utilizador foi aceite solicitando a password.
* O comando PASS test2123 (linha 8) é utilizado para fornecer a palavra-passe do utilizador.
* O servidor responde com mensagens de confirmação (**+OK**), indicando que as credenciais foram aceites e a caixa de entrada está disponível.

Após a autenticação, o cliente começa a interagir com o servidor com os seguintes comandos adicionais:

* UIDL (linha 14): O cliente utiliza este comando para obter uma lista de IDs únicos das mensagens no servidor, permitindo identificar quais mensagens já foram processadas.
* LIST (linha 16): O comando LIST é utilizado para obter uma listagem das mensagens na caixa de correio, juntamente com os respetivos tamanhos.
* RETR 1 (linha 18): O cliente solicita o download da primeira mensagem da caixa de entrada. O servidor responde com o tamanho da mensagem em octetos(984) e, posteriormente, transfere o conteúdo da mensagem para o cliente.
* DELE 1 (linha 20): O cliente utiliza este comando para marcar a mensagem descarregada para exclusão, que será realizada ao finalizar a sessão.
* QUIT (linha 22): O cliente encerra a sessão com o servidor, e o servidor responde com uma mensagem de despedida ("Sayonara").

Por último a comunicação TCP entre o cliente e o servidor é finalizada com uma troca de pacotes FIN e ACK, sinalizando o encerramento da conexão de forma adequada.

Problemas de segurança

Uma vulnerabilidade crítica associada ao uso do POP3 é a transmissão de credenciais e dados em texto simples. Neste caso tanto o nome de utilizador como a palavra-passe são transmitidos sem qualquer criptografia, como se pode observar com a palavra-passe "test2123" exposta na linha 8. Isto torna a comunicação suscetível a ataques onde um atacante pode facilmente intercetar e ler as credenciais, comprometendo a conta de email.

Além disso, o POP3 não possui mecanismos robustos de proteção contra tentativas repetidas de login, o que o torna vulnerável a ataques de força bruta. Neste tipo de ataque, o invasor tenta inúmeras combinações de nomes de utilizador e palavra-passes até conseguir acesso. Como as credenciais são transmitidas em texto simples no POP3, o atacante com acesso à comunicação pode observar e ajustar as tentativas com base nas respostas do servidor.

Outra vulnerabilidade observada é o uso de uma senha fraca. A senha capturada ("test2123") é previsível e de baixa complexidade, o que a torna especialmente vulnerável a ataques de força bruta. O uso de senhas curtas ou que seguem padrões simples facilita a descoberta por parte de um atacante.

Como mitigar os problemas de segurança

A principal recomendação para mitigar este tipo de vulnerabilidade é a migração para o protocolo **POP3S**, que utiliza **SSL/TLS** para criptografar toda a comunicação entre o cliente e o servidor. Com o **POP3S**, todas as informações trocadas, incluindo credenciais de login e o conteúdo das mensagens, são protegidas contra a intercetação por parte de terceiros, prevenindo ataques de **Man-in-the-Middle (MITM)** e outras formas de comprometimento.

Outra medida de segurança recomendada é a implementação de **Autenticação Multifator (MFA).** Mesmo que as credenciais de acesso sejam comprometidas, o uso de um segundo fator de autenticação (como um código enviado por SMS ou através de uma aplicação autenticadora) adiciona uma camada extra de segurança, dificultando que o atacante consiga finalizar o ataque.

Adicionalmente, a implementação de uma **política de senhas fortes** é essencial. Essa política deve exigir que os utilizadores criem senhas com pelo menos 8-12 caracteres, incluindo uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Isso aumenta a complexidade da senha e torna mais difícil a sua descoberta.