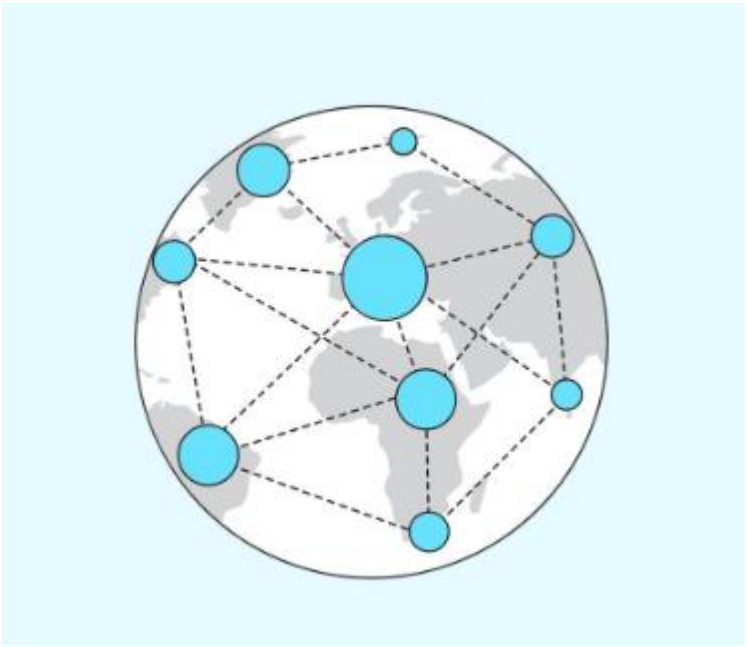


TRAFFIC ANALYSIS

Carlos Almeida (1181132)
André Teixeira (1190384)
SEGSI – Segurança de Sistemas e Informação

Índice

Índice de Figuras

Introdução

A análise de tráfico de rede é um processo de monitorização de inspeção de padrões de tráfego de rede.

Ao identificar anomalias ou comportamentos suspeitos, esta análise de tráfego de rede pode ajudar as equipas de segurança e operações de redes a detetar alguma possível ameaça. A análise de tráfego pode ser útil para solucionar problemas de desempenho como altas taxas de perda de pacotes ou de alta latência de rede.

O propósito de analisar o tráfego de redes é obter insights baseados em padrões de tráfego de rede que possam ajudar as equipas de segurança a encontrar e corrigir problemas de desempenho e segurança da rede. Esta análise é também importante, porque os padrões de tráfego de rede podem variar amplamente. As rotas que os pacotes percorrem à medida que se movem entre segmentos de rede e pontos finais podem variar, resultando em diferentes níveis de desempenho dependendo da eficiência das diversas rotas. Da mesma forma, atividade maliciosas de rede, como “port scanning” ou ataques de negação de serviço (DoS), geralmente criam padrões de tráfego incomuns. Ao detetar estas anomalias, as organizações/empresas podem identificar os potenciais riscos de segurança e bloqueá-los antes que ocorra qualquer violação.

Para este primeiro trabalho prático o objetivo era, que cada aluno do grupo, analisasse o tráfego normalmente encontrado numa rede. Para isso, foi nos fornecido um conjunto de capturas de pacotes feitas através do Wireshark, e cada aluno teria de analisar duas dessas capturas.

Na análise destas capturas teríamos de ser capazes de encontrar: os intervenientes, o protocolo principal, as operações realizadas pelo protocolo principal, problemas de segurança que podem ocorrer e como mitigá-los e por último, se possível, outras considerações que achássemos importantes.

Os Intervenientes

Os intervenientes refere-se às partes envolvidas na comunicação de rede, os dispositivos, hosts ou servidores que trocam pacotes de dados. Numa rede TCP/IP, isso refere-se aos endereços IP das máquinas que estão a enviar e receber informações.

Protocolo Principal

O protocolo principal é o conjunto de regras ou normas usadas para estabelecer e conduzir a comunicação entre dois ou mais dispositivos. Alguns exemplos mais comuns incluem o TCP, UDP, HTTP, FTP, DNS, entre outros. Este protocolo dita a forma como os pacotes são formatados, enviados e recebidos.

Operações realizadas pelo protocolo principal

São as ações específicas que ocorrem durante a comunicação na rede. Na análise de tráfego de redes, as operações realizadas pelo protocolo principal referem-se ao conjunto de ações e mecanismos que um protocolo utiliza para garantir a comunicação entre dispositivos na rede. Cada protocolo possui uma função específica no modelo de camadas da rede, como o TCP/IP, e define regras para a formatação, transmissão e receção de dados entre os nós da rede. Estas operações podem incluir o estabelecimento de conexões, a troca de pacotes, o controlo de erros, a fragmentação de dados, e a autenticação.

Problemas de segurança que podem ocorrer e como mitigá-los

No contexto das redes de comunicação, diversos problemas de segurança podem surgir durante a transmissão de dados entre dispositivos. Estes problemas estão relacionados a vulnerabilidades intrínsecas aos protocolos utilizados, à má configuração dos dispositivos de rede, ou à ação de cibercriminosos que exploram falhas para comprometer a integridade, confidencialidade e disponibilidade da informação.

Parte Prática

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 interceções 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.

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 interceção 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.

Considerar também o uso de protocolos mais recentes como IMAP com SSL/TLS ou até mesmo o uso de serviços de email mais seguros que garantam criptografia até ao fim dos dados.

CAP 3

Intervenientes

Segundo a análise de tráfego feita à captura podemos dizer:

- **Fonte (source):** 192.168.2.101, este parece ser o cliente, pois inicia a comunicação com um pedido SYN para estabelecer a conexão
- **Destino (destination):** 192.168.2.100, este parece ser o servidor, pois responde ao pedido do cliente com um SYN-ACK e fornece arquivos requisitados.

Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.2.101	192.168.2.100	160	80 kB	0	69	4 kB	91	76 kB	0.000000	52.3330	657 bits/s	11 kbps

Figura 1: Intervenientes CAP 3

Principal Protocolo

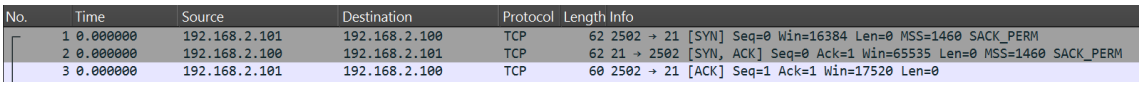
O protocolo principal nesta categoria é o FTP (File Transport Protocol), que é utilizado para transferir ficheiros entre o cliente e o servidor. Através do Wireshark, é claramente usado na coluna do Protocol o FTP ou o FTP-DATA.

Consequentemente à utilização deste protocolo, vemos também o uso de TCP, pois o FTP opera sobre o TCP para garantir uma entrega confiável de pacotes.

Operações de protocolo

As operações realizadas entre a comunicação cliente-servidor são para transferir ficheiros.

- **Handhsake TCP**: A captura começa com uma comunicação TCP (pacotes SYN, SYN-ACK, ACK) entre o cliente e o servidor (nas 3 primeiras linhas). Este processo de "three-way handshake" estabelece a conexão confiável para o FTP.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.101	192.168.2.100	TCP	62	2502 → 21 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.000000	192.168.2.100	192.168.2.101	TCP	62	21 → 2502 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM
3	0.000000	192.168.2.101	192.168.2.100	TCP	60	2502 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0

Figura 2: Three-Way Handshake

- **Autenticação no FTP**: o cliente conecta-se ao servidor FTP e envia um comando USER administrator (linha 6), seguido por PASS 123456 (linha 9), para se autenticar. O servidor responde com um "230 Login successful" (linha 12), dizendo assim que a autenticação foi bem-sucedida.
- **Conexão para transferir informação:** o cliente usa o comando PORT para iniciar uma conexão com o servidor para transferir informação, como ficheiros ou listagens de diretórios. Assim antes do uso de qualquer comando abaixo referidos, é sempre estabelecida uma conexão para estas transferências, onde lhe é especificado o IP ao qual o servidor se deve conectar e a porta onde querem comunicar. Quando este pedido é aceite, o servidor informa que o pedido foi bem-sucedido e antes de qualquer transferência, o cliente e o servidor estabelecem uma nova conexão, para que possam ser transferidos os pedidos do cliente. Depois da transferência ser concluída esta conexão é encerrada.
- **Listagem arquivos**: o cliente através do comando NLST requisita a lista de arquivos no diretório atual (linha 16), onde podemos ver que existem ficheiros do tipo executável e do tipo dynamic link library (dll), o que pode sugerir que

estaremos a comunicar com um sistema operativo Windows.

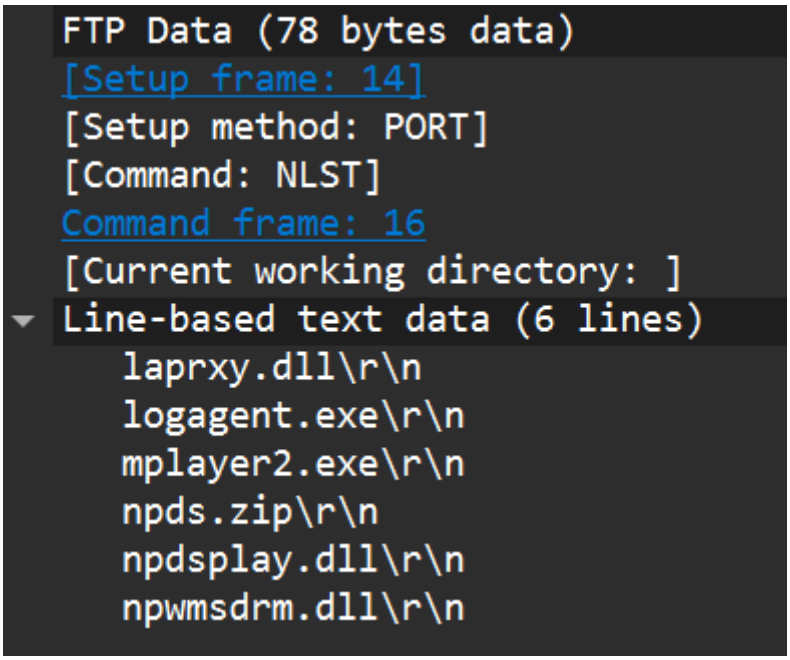


Figura 3: Listagem de ficheiros

- **Transferência de ficheiros**: o cliente solicita a transferência de ficheiros por meio de comandos RETR:
    - **RETR logagent.exe**: o cliente fez uma solicitação para baixar o ficheiro "logagent.exe" (linha 46).
    - **RETR mplayer2.exe**: o cliente fez uma solicitação para baixar o ficheiro "mplayer2.exe" (linha 126).
    - Estes ficheiros são transferidos para o cliente através do protocolo FTP-DATA, com pacotes de dados de 1460 bytes sendo trocados. O fluxo de dados é visto na sequência dos pacotes FTP-DATA, onde vemos o servidor a enviar conteúdo para o cliente.
    - O servidor informa o cliente que as transferências foram bem-sucedidas enviando um "226 Transfer complete" (linhas122,141).
- **Finalização das operações**: após a transferência de ficheiros, o cliente executa o comando XPWD (linha 143) para listar o diretório atual, na qual o servidor lhe responde que o diretório atual é o "/" (linha 144) e de seguida o cliente solicita o comando NLST (linha 148) para obter a lista de ficheiros do diretório, na qual o servidor lhe mostra os arquivos disponíveis (linha 153).
- **Encerramento da Conexão**: o processo de encerramento é visível nos pacotes TCP com o FIN-ACK, onde ambas as partes terminam a conexão (linhas 154, 155, 156).

Problemas de segurança

Os problemas potenciais encontrados nesta captura acerca da comunicação seria o uso de FTP sem criptografia. O FTP não criptografa os dados, o que significa que todas as

informações, incluindo credenciais de login e arquivos transferidos, são enviadas em texto plano/limpo.

Isto pode ser facilmente intercetado por um atacante com acesso à rede. As credenciais do utilizador são expostas durante a captura, o que sugere um grande risco.

Além disso, um dos aspetos mais cruciais encontrados aqui é a consulta dos ficheiros ao qual encontramos ficheiros do tipo executável (.exe), que pode trazer vulnerabilidades, pois com o download desses mesmos ficheiros pode implicar o risco de serem alvo de ataques. Os ficheiros executáveis são o tipo mais comum de vetor de ataque para malware, trojans (cavalos de troia) e vírus. Assim sendo se um invasor conseguir intercetar este tipo de ficheiros pode comprometê-los e subjacentemente comprometer os sistemas que depois recebem este ficheiro e o executam.

Como mitigar os problemas de segurança

Umas das soluções que encontramos para conseguir mitigar estes problemas seriam:

Senhas fortes e autenticação multifator: A autenticação FTP poderia ser melhorada através do uso de senhas mais fortes e a introdução de um segundo fator de autenticação.

O uso de SFTP ou FTPS: Invés de FTP seria melhor usar SFTP (Secure FTP), que é baseado no protocolo de SSH e criptografa a sessão inteira. Outra alternativa seria o FTPS, que adiciona o suporte de SSL/TLS ao FTP para garantir a segurança dos dados.

Uso de uma VPN: Implementar uma VPN para criptografar toda a comunicação seria uma solução adicional para proteger as transferências de arquivos. Assim poderia se garantir que mesmo que alguém conseguisse capturar os pacotes, os dados estariam criptografados

CAP 4

Intervenientes

Segundo a análise de tráfego feita à captura podemos dizer:

- **Fonte (source):** 192.168.251.1, este parece ser o cliente, pois inicia a comunicação com um pedido SYN para estabelecer a conexão
- **Destino (destination):** 192.128.251.11, este parece ser o servidor, pois responde ao pedido do cliente com um SYN-ACK.

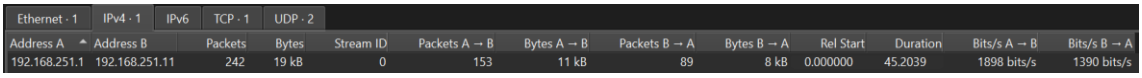


Figura 4: Intervenientes CAP 4

Principal Protocolo

O protocolo TELNET é o principal nesta captura. Este protocolo é utlizado para acesso remoto a dispositivos permitindo que o cliente (neste caso 192.168.251.1) interaja com o servidor (neste caso 192.168.251.11).

Para além deste protocolo também está evidenciado o uso do protocolo TCP usado para estabelecer e manter a conexão. Existe ainda alguns protocolos ICMP que é usado para relatar erros de comunicação e DHCP que oferece configuração dinâmica de terminais, que no caso desta captura parece alocar um endereço IP.

Operações de protocolo

Handhsake TCP: A captura começa com uma comunicação TCP (pacotes SYN, SYN-ACK, ACK) entre o cliente e o servidor (nas 3 primeiras linhas). Este processo de “three-way handshake” estabelece a conexão cliente/servidor.

De seguida vemos um protocolo TELNET, com vários comandos fornecidos, que fazem parte de uma negociação de opções TELNET, onde o cliente e o servidor ajustam parâmetros para garantir que a sessão TELNET funcione de acordo com as capacidades do cliente.

Na linha 5 o servidor envia um protocolo NBNS para o cliente. Este protocolo é usado para mapear nomes NetBIOS a endereços de IP numa rede, normalmente usado em redes Windows.

Na linha 6 o cliente envia um protocolo ICMP ao servidor indicando que o destino não está acessível, neste caso que a porta solicitada não está a ser atingida.

Este processo repete-se 3 vezes, até que na linha 12 o servidor envia um protocolo DHCP pedindo uma atribuição ou renovação de endereço IP. Seguidamente (linha 13) o cliente responde positivamente com um DHCP ACK, afirmando que o servidor pode usar o endereço IP atribuído.

Na captura vemos que na linha 19 o servidor a avisar o cliente que está num serviço TELNET e pede para que faça o login.

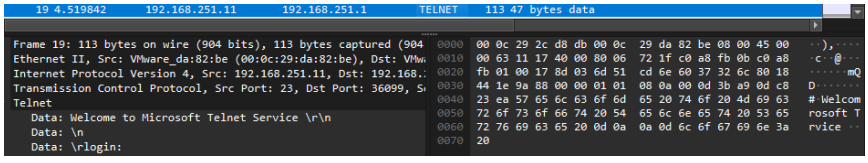


Figura 5: Mensagem de bem-vindo e início de sessão

De seguida vemos uma comunicação feita através de pequenos pacotes de dados transmitidos na conexão TELNET. Estes pacotes são típicos da transmissão de comandos ou dados entre um cliente e um servidor TELNET. Vemos vários pacotes de 1 byte de

dados, o que pode corresponder a comandos ou teclas pressionadas durante a sessão. Pela análise feita à captura, percebemos que seriam teclas pressionada.

Ao pedido de login o cliente escreveu, pela análise feita, “esegi-boss”, e na linha 52 o servidor requisitou que fosse introduzida a password.

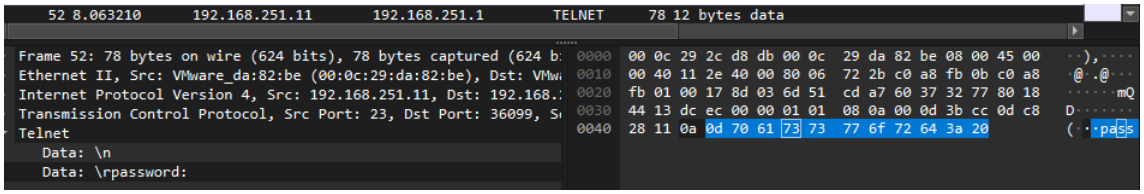


Figura 6: Pedido para inserir password

Na resposta por parte do cliente a este pedido, o cliente inseriu a password “segredo”, na qual o servidor respondeu-lhe que estava errado e pediu para repetir.

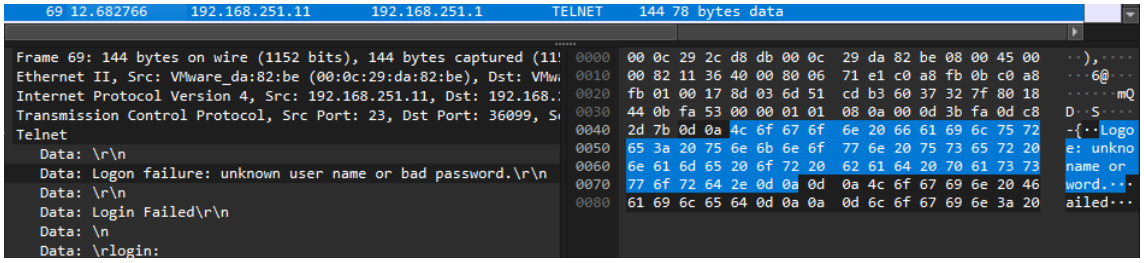


Figura 7: Mensagem de erro

De seguida o utilizador inseriu de novo “esegi-boss” com a password “segred0”, conectando-se.

Depois o servidor na linha 124, informa o cliente de novo que esta no servidor da TELNET e diz lhe também em que diretório se encontra.

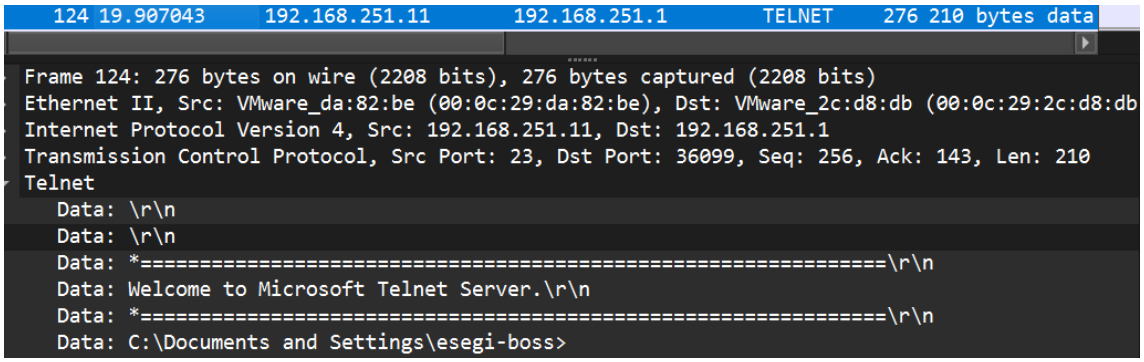


Figura 8: Informação sobre diretório atual

Seguidamente o cliente insere o comando “cd\” e na linha 136 o servidor informa que se encontra no diretório de raiz.

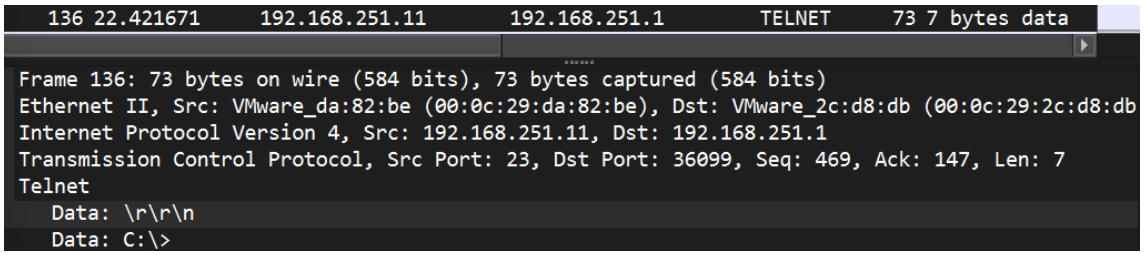


Figura 9: Informação que se encontra no diretório raiz

Na sequência, o cliente insere o comando “dir” para ver os diretórios/ficheiros presentes no diretório raiz e o servidor apresenta-lhe a informação (linha 148).

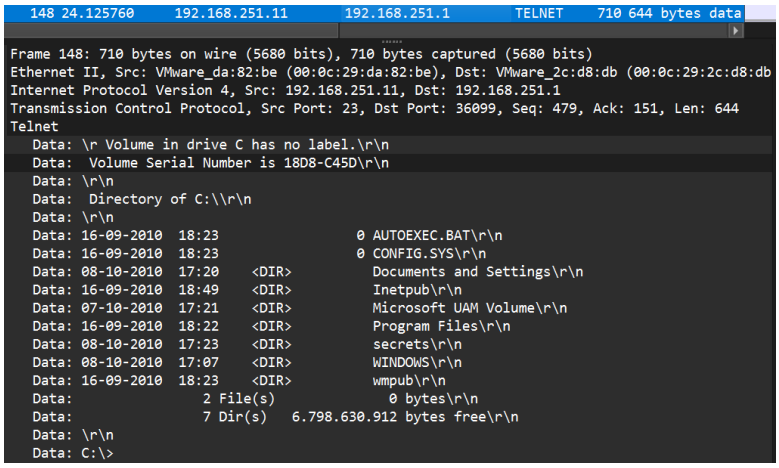


Figura 10: Listagem dos diretórios/ficheiros no diretório raiz

O cliente entra no diretório “secrets” e executa de novo o comando “dir” para ver os ficheiros e o servidor mostra.

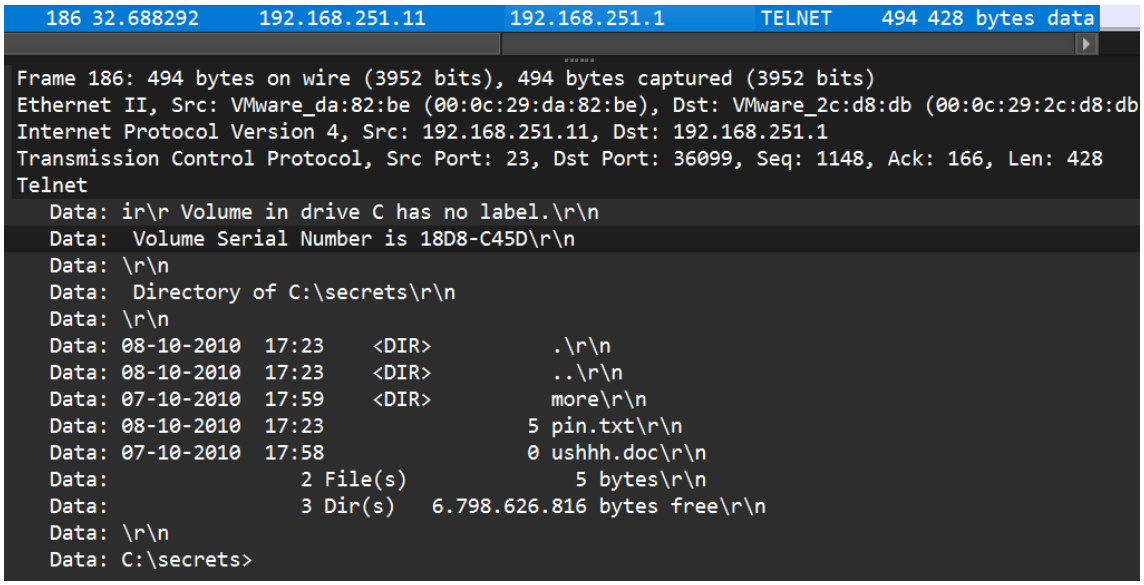


Figura 11: Listagem dos ficheiros no diretório "secrets"

Consequentemente o cliente insere o comando “type pin.txt” para ver a informação dentro do ficheiro e o servidor mostra-lhe o conteúdo do ficheiro na linha 225, podendo ver a informação “89384”.

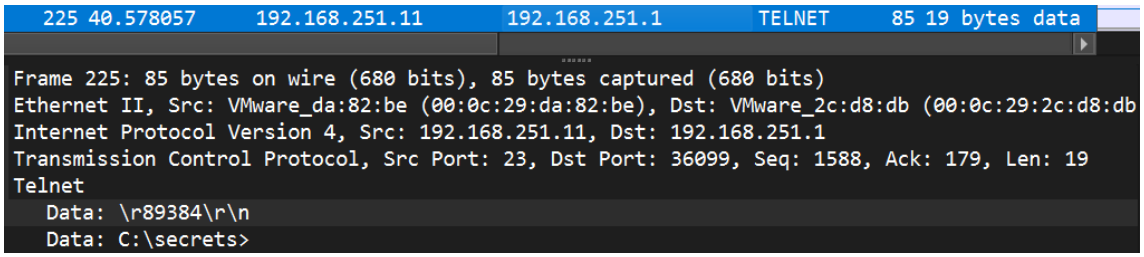


Figura 12: Informação dentro do ficheiro "pin.txt"

No final o cliente insere o comando “exit” e terminam a conexão (últimas 3 linhas).

Problemas de segurança

O uso do TELNET é uso de um protocolo inseguro, pois este protocolo transmite todos os dados, incluindo credenciais em texto claro, o que torna vulnerável a ataques de sniffing e interceção. Alguém que capture este tráfego pode facilmente ver senhas e outros dados quaisquer.

A autenticação deste protocolo é feita através de utilizador e palavra-passe que são transmitidos em texto simples. Além disso, o TELNET não oferece suporte a métodos avançados de autenticação como certificados ou tokens multifator.

Como mitigar os problemas de segurança

Para mitigar estes problemas o uso de SSH é amplamente recomendado, já que o uso de SSH oferece criptografia forte, autenticação robusta, muitas proteções que o TELNET não possui. O SSH traz vantagens tais como:

- Criptografia de dados.
- Proteção contra ataques “Man-in-the-Middle” e modificação de dados.
- Suporte a autenticação multifator.

Pode também se usar um VPN para criptografar o texto claro, assim garante que os dados que são transmitidos através de TELNET não sejam intercetados por terceiros.

CAP5

Esta análise detalha o tráfego capturado durante um processo de autenticação utilizando o protocolo RADIUS (Remote Authentication Dial-In User Service), amplamente usado em redes organizacionais para fornecer autenticação, autorização e contabilidade (AAA). Foram inspecionados dois pacotes principais, Access-Request e Access-Accept, trocados

entre um cliente e um servidor RADIUS, que são utilizados para solicitar e aceitar uma tentativa de autenticação.

Intervenientes

Cliente (IP de Origem): 192.168.170.135

Servidor (IP de Destino): 192.168.170.131

Principal Protocolo

O protocolo principal utilizado é o RADIUS sobre UDP o que, embora eficiente em termos de velocidade e simplicidade, apresenta vulnerabilidades, especialmente em ambientes que exigem maior segurança.

Há dois pacotes capturados:

- Access-Request (ID=240): Enviado do cliente ao servidor solicitando autenticação.
- Access-Accept (ID=240): Resposta do servidor ao cliente, aceitando a tentativa de autenticação.

Além disso, no contexto da autenticação, o MS-CHAPv2 (Microsoft Challenge-Handshake Authentication Protocol versão 2) é o protocolo utilizado para validar as credenciais do utilizador. O MS-CHAPv2 é baseia-se num sistema de desafio-resposta, no qual o servidor gera um Challenge (desafio) e o cliente responde com um Response (resposta) gerado a partir da combinação da sua palavra-passe e do desafio.

Operações do Protocolo

O processo de autenticação utilizando o protocolo RADIUS envolve várias etapas importantes, que serão detalhadas a seguir:

O processo inicia com o envio de um pacote Access-Request pelo cliente ao servidor. Este pacote contém informações essenciais para a autenticação, incluindo o nome de utilizador(bob) e a resposta criptografada ao desafio enviado pelo servidor utilizando MS-CHAPv2.

- Service-Type: Login (1): Este campo especifica que o serviço solicitado é um login de rede, indicando ao servidor que o cliente está a tentar autenticar-se.

MS-CHAP Challenge: Após o envio do pacote Access-Request, o servidor gera um Challenge (valor), que é essencial para verificar a resposta do cliente.

MS-CHAP Response: Em seguida, o cliente envia a MS-CHAP Response, que é o hash gerado pela passe enviada, utilizado no processo de autenticação. E que será desencriptado posteriormente.

Informações do NAS:

- NAS-IP-Address: 192.168.170.135 - O IP do NAS (Network Access Server), que iniciou o pedido de autenticação.
- NAS-Identifier: pfSense.home.arpa - O identificador do NAS é pfSense.home.arpa. O pfSense é um dispositivo que permite configurar funcionalidades avançadas de firewall, roteamento e VPN, oferecendo segurança adicional à rede.

O pacote Access-Accept confirma que a autenticação foi bem-sucedida e inclui as chaves criptográficas que serão utilizadas para proteger a sessão subsequente.

- MS-CHAP-MPPE-Keys: Indica que as chaves de criptografia para MPPE (Microsoft Point-to-Point Encryption) foram geradas, permitindo a proteção da comunicação.
- MS-MPPE-Encryption-Policy: Valor = Encryption Allowed (1), indicando que a criptografia é permitida para esta sessão.
- MS-MPPE-Encryption-Types: Define os tipos de criptografia permitidos, neste caso RC4-40 ou RC4-128.

Análise de Autenticação MS-CHAPv2 e Crack da palavra-passe

A fim de determinar a palavra-passe utilizada no tráfego capturado, foi realizada uma tentativa de "cracking" do hash utilizando a ferramenta John the Ripper e a wordlist rockyou.txt, que contém uma extensa lista de passes comuns.

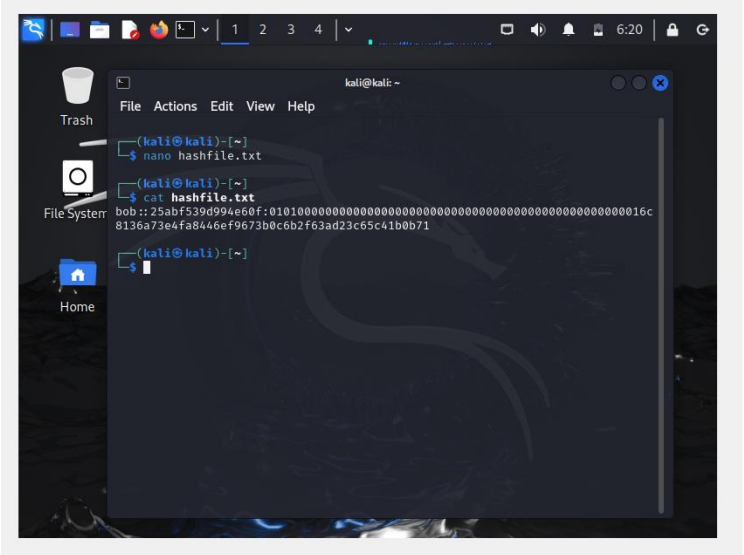


Figura 13: Criação e introdução de informação no ficheiro "hashfile.txt"

Como demonstrado pela imagem anterior, inicialmente foi criado um ficheiro denominado “hashfile.txt” através do comando “nano”, onde foram introduzidos os seguintes elementos:

- O nome de utilizador, neste caso, “bob”, seguido de “::”. Entre estes dois pontos será o espaço onde a senha crackada aparecerá.
- Em seguida, foi inserido o valor “25abf539d994e60f”, que representa o MS-CHAP Challenge — um valor aleatório de 16 caracteres em hexadecimal gerado pelo servidor e enviado ao cliente como parte do processo de autenticação.
- Por fim, foi adicionado o MS-CHAP Response, que é o hash criptografado gerado pelo cliente ao combinar a passe do utilizador e o valor recebido do servidor. Este valor prova ao servidor que o cliente conhece a password correta.

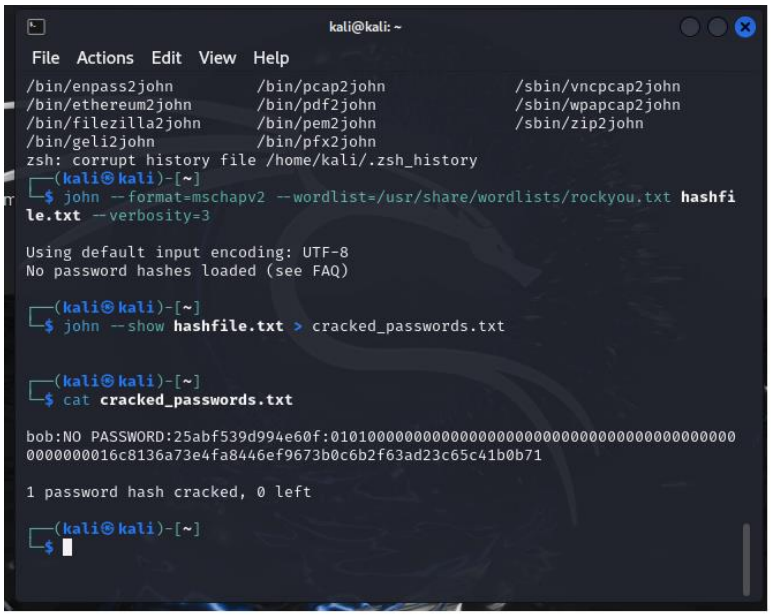


Figura 14: Password crakada

Posteriormente, iniciámos o John the Ripper e utilizámos o seguinte comando para tentar crackar o hash e encontrar a password:

john --format=mschapv2 --wordlist=/usr/share/wordlists/rockyou.txt hashfile.txt --verbosity=3

Neste comando, especificámos o formato do hash (MS-CHAPv2), utilizámos a wordlist popular “rockyou.txt”, juntamente com o ficheiro de hash previamente criado (hashfile.txt).

Após a execução do comando, guardámos o resultado num ficheiro de texto chamado “cracked_passwords.txt” e, para visualizar o conteúdo, utilizámos o comando “cat”. O resultado revelou que a palavra-passe era “NO PASSWORD”.

Portas utilizadas

- Porta UDP 1812: É a porta padrão utilizada pelo servidor RADIUS para receber pacotes de autenticação. Essa porta é amplamente conhecida

e, sem proteção adicional (como IPsec ou TLS), pode ser vulnerável a ataques de interceção.

- Porta 58157 (temporária): Essa porta foi atribuída temporariamente pelo cliente para esta sessão específica de comunicação. O único propósito é diferenciar essa sessão de outras conexões que o mesmo cliente pode estar a estabelecer. Ao encerrar a sessão, a porta será libertada e pode ser reutilizada em futuras conexões.

Problemas de segurança

1. O uso de UDP para transporte de mensagens RADIUS traz algumas vulnerabilidades significativas que precisam ser mencionadas:
   a. Falta de Confiabilidade: UDP não garante a entrega dos pacotes nem a sua ordem correta, o que significa que pacotes de autenticação podem ser perdidos sem que o cliente ou servidor percebam imediatamente. Isso pode causar falhas na autenticação ou permitir que um atacante explore o processo como interrupções e ataques de falsificação.
   b. Vulnerabilidade a Ataques de Spoofing: Como o UDP não mantém estado de conexão, é suscetível a falsificação de pacotes (spoofing). Um atacante pode enviar pacotes falsos ao servidor ou cliente fingindo ser o cliente ou o servidor. Isso pode permitir que o atacante intercete ou redirecione as comunicações, levando a um comprometimento da rede.
   c. Ataques de Replay: Como o UDP não protege contra retransmissão de pacotes, é possível que um atacante capture um pacote legítimo e o retransmita posteriormente para tentar obter acesso indevido.
   d. Porta UDP 1812 (Autenticação): A captura revela que o servidor RADIUS está a utilizar a porta 1812, que é a porta padrão para autenticação RADIUS. Este é um padrão amplamente conhecido, e como tal, se não houver medidas de segurança adicionais (como IPsec ou TLS), a comunicação pode ser intercetada por um atacante experiente.

2. MS-CHAPv2: Embora seja amplamente utilizado para autenticação, apresenta vulnerabilidades bem documentadas. Um atacante que capture pacotes contendo a MS-CHAP Response pode, com ferramentas apropriadas, tentar recuperar a password do utilizador com relativa facilidade. Isso torna o MS-CHAPv2 uma escolha insegura para autenticação sem medidas de proteção adicionais, como TLS ou IPsec.
3. A análise do tráfego capturado revela o uso de RC4-40/128, um método de criptografia de fluxo, para proteger a comunicação. Entretanto, a criptografia

RC4 possui várias vulnerabilidades conhecidas, principalmente em sessões de longa duração, como por exemplo ataques de Long-Term Key onde o fluxo de chaves pode começar a repetir padrões ou revelar regularidades no texto cifrado, tornando-a insegura para proteger dados sensíveis. O uso de RC4 já foi amplamente desaconselhado em favor de criptografias mais robustas, como AES (Advanced Encryption Standard).

4. A utilização de uma password fraca ou facilmente adivinhável (como "123456", "password", ou "qwerty") também torna o sistema vulnerável a ataques de força bruta, onde um atacante tenta múltiplas passes comuns ou gera combinações até encontrar a correta.

Como mitigar os problemas de segurança

1. Impor o uso de palavras-passes fortes para mitigar o risco de acessos não autorizados, isso inclui:
   a. Mínimo de 8-12 caracteres.
   b. Uso obrigatório de caracteres especiais, como @, #, %, &.
   c. Inclusão de números, letras maiúsculas e minúsculas.
   d. Proibição de passes vazias ou fracas como "123456" ou " NO PASSWORD".

2. Migrar para TLS ou IPsec: Uma das formas mais eficazes de mitigar os riscos associados ao UDP é configurar o RADIUS para funcionar sobre TLS ou IPsec. Esses protocolos fornecem confidencialidade, integridade e autenticação para os pacotes, protegendo a comunicação de espionagem e ataques de spoofing.
3. Substituir MS-CHAPv2: Recomenda-se a substituição do MS-CHAPv2 por métodos de autenticação mais seguros, como EAP-TLS, que utiliza certificados digitais em vez de passwords. O EAP-TLS oferece um nível de proteção muito mais elevado contra ataques de captura de pacotes, evitando que um atacante recupere palavras-passe mesmo que consiga capturar o tráfego.
4. A criptografia RC4 deve ser substituída por AES (Advanced Encryption Standard), que é muito mais segura e amplamente aceita como o padrão para proteger comunicações sensíveis. O AES protege a integridade e a confidencialidade da comunicação com maior eficácia.
5. Monitorização da Rede: Implementar ferramentas de monitorização ativa para identificar tentativas de spoofing, replay attacks, ou qualquer outro comportamento anômalo é fundamental para proteger a rede. A monitorização contínua pode detetar e responder rapidamente a ameaças, minimizando o impacto de potenciais ataques.

Considerações adicionais

O tempo entre os dois pacotes é muito curto (0.000964 segundos), o que sugere uma rede local com baixa latência e resposta rápida do servidor de autenticação.

Os endereços MAC mostrados são de dispositivos virtuais (VMware), o que indica que a captura foi feita num ambiente virtual.

O Access-Request tem um tamanho de 209 bytes, enquanto o Access-Accept tem um tamanho de 126 bytes.

Conclusão

O trabalho desenvolvido ao longo desta análise de tráfego de rede demonstrou a importância de avaliar cuidadosamente os protocolos utilizados e as vulnerabilidades associadas ao ambiente de rede. Foi possível identificar problemas relacionados ao uso de protocolos inseguros, como o MS-CHAPv2, RC4, UDP, FTP, TELNET e no transporte de mensagens RADIUS, que são suscetíveis a ataques como spoofing, replay e cracking de senhas.

Para mitigar esses riscos, foram feitas recomendações claras, como a migração para protocolos mais seguros, que são mudanças essenciais para garantir um nível mais elevado de segurança nas comunicações de rede.

Em suma, a análise de tráfego e as vulnerabilidades encontradas mostram a necessidade de atualização contínua dos protocolos e políticas de segurança em ambientes organizacionais, promovendo a proteção contra ataques e garantindo a confidencialidade, integridade e disponibilidade dos dados.