# 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.

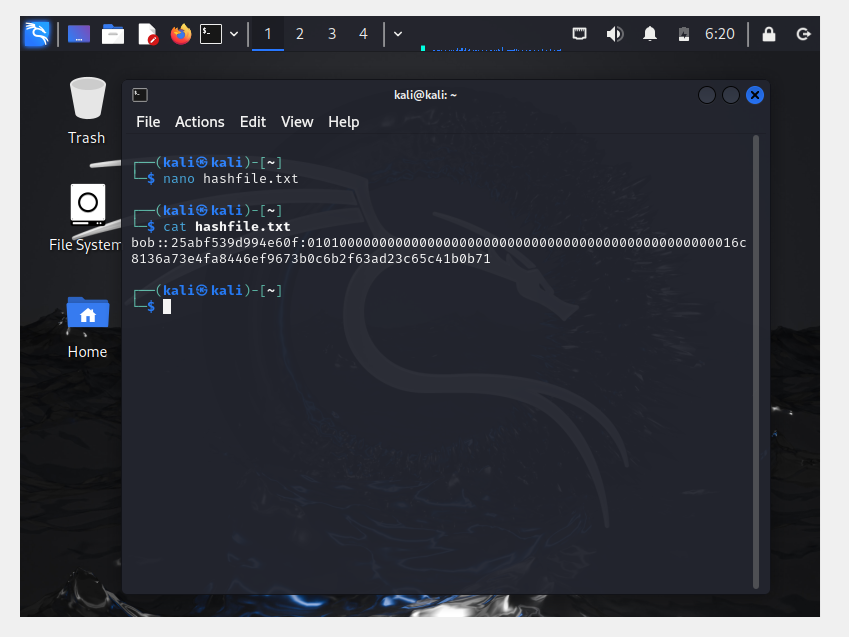
Informações do NAS:

* 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.

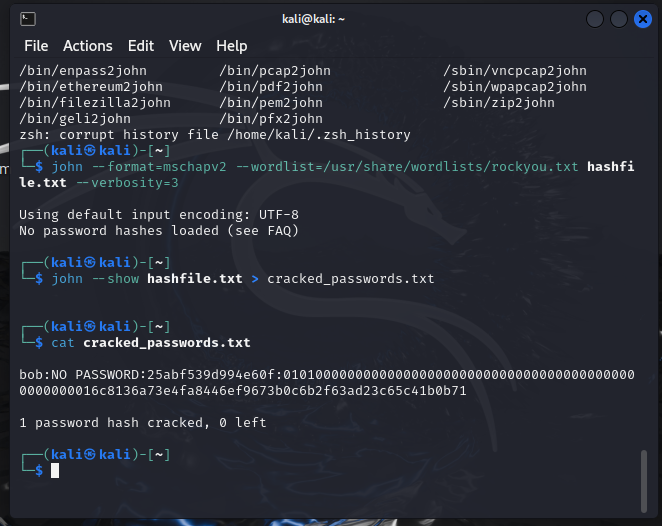
* MS-CHAP-MPPE-Keys: Indica que as chaves de criptografia para MPPE (Microsoft Point-to-Point Encryption) foram geradas, permitindo a proteção da comunicação.
* MS-MPPE-Encryption-Policy: Valor = Encryption Allowed (1), indicando que a criptografia é permitida para esta sessão.
* MS-MPPE-Encryption-Types: 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.

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.



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:

* 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.
* 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.
* 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.
* 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.

1. 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.
2. 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).
3. 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:

* Mínimo de 8-12 caracteres.
* Uso obrigatório de caracteres especiais, como @, #, %, &.
* Inclusão de números, letras maiúsculas e minúsculas.
* Proibição de passes vazias ou fracas como "123456" ou " NO PASSWORD".

1. 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.
2. 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.
3. 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.
4. 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.