Estudo de Ataque Man-in-The-Middle com Software Cain&Abel

Man-in-The-Middle Attack Study with Cain&Abel Software

Gabriel Gonçalves Ferreira, Fatec e

gabriel.ferreira62@fatec.sp.gov.br Andre Giovanni Castaldin, Fatec

e andre.castaldin@fatec.sp.gov.br

Resumo

Atualmente, com o crescente avanço da Internet, os usuários aproveitam cada vez mais desses recursos, contudo, não deixam de estar vulneráveis e suscetíveis ataques e seus dados podem ser capturados ou monitorados. Esse artigo e´ fundado no ataque *Man-in- The-Middle*, que captura informações de dois computadores conectado em uma rede .
É criado um ambiente virtual controlado para realizar esse estudo de caso qualitativo,
usando como ferramenta de ataque Caim e Abel. O resultado, a avaliação e descrição de quão eficiente é esse ataque, mostrando suas facilidades e procurando formas de se prevenir contra esse tipo de ataque.
Palavras-chave: Ataque, Caim e Abel, Man-in-The-Middle, Rede, Segurança

Abstract

Currently, with the increasing advancement of the Internet, users are increasingly taking advantage of these advances, however, they are still vulnerable to susceptible attacks and their data can be captured or monitored. This article will be based on the Man-in-The- Middle attack, which captures information from two computers connected in a network. A controlled virtual environment was created to carry out this qualitative case study, using Cain e Abel as an attack tool. The result will be evaluated and will describe how efficient this attack is, showing its facilities and looking for ways to prevent against this type of attack.
Keywords: Attack, Cain and Abel, Man-in-The-Middle, Network, Security

1. Introdução

A quantidade de internautas e empresas na *Internet* vem aumentando no Brasil e no mundo a fora principalmente em meio a pandemia, dessa forma cresceu também a quan- tidade de dispositivos vulneráveis a suscetíveis ataques.

De acordo com InforChanel (2021) a empresa de segurança cibernética industrial *TI Safe* aponta entre julho e setembro um aumento de 860% de tentativas de invasões no Brasil. Segundo o CEO da *TI Safe* Marcelo Branquinho, muitas empresas permitiram-se trabalharem remotamente, mas não tomando as devidas precauções e cuidados com a segurança e então, colocando suas redes de Tecnologia da Informação e Comunicações em risco.

O ataque conhecido como *Man-in-The-Middle* (O Homem no Meio) tem como principal função capturar dados importantes de suas vítimas, como usuário e senha, de modo que a vítima não fique sabendo.

Neste trabalho é realizado um estudo de caso, com simulação de um ataque em ambiente controlado, visando o aprendizado com duas máquina *Windows* e um *Linux*, fazendo uso do *software* Caim e Abel como as principais ferramentas de intrusão e captura de dados.

2. Referencial Teórico

2.1. Ataques Man-In-the-Middle

Para entendermos o que e´ um ataque de *MITM*, podemos usar como exemplo um carteiro que abre uma carta e coleta informações contidas nela ou faz algum tipo de alteração no conteúdo da carta. Segundo Gangan (2015), o ataque*MITM* permite que o atacante bisbilhote os dados da sua vítima através do *backdoor* (Método que permite escapar de uma autênticação ou criptografia).

2.2. ARP Cache Poisong

Segundo Botti e Martins (2015) Esse tipo de ataque *MITM* e´ considerado o mais antigo e eficiente para ataques em redes locais, ele permite que o atacante, conectado na mesma rede consiga espionar todo o tráfego da rede, ou de dois *Hosts* distintos. Tem como foco o envenenamento do cache *ARP*.

Segundo Gangan (2015) Em uma situação normal, o *host* enviará um pacote com o endereço *IP* de origem e destino dentro do pacote e esse será transmitido para todos os dispositivos conectados na rede, como pode ser facilmente falsificado, o pacote de resposta pode ser enviado para a máquina que solicitou o *ARP*.

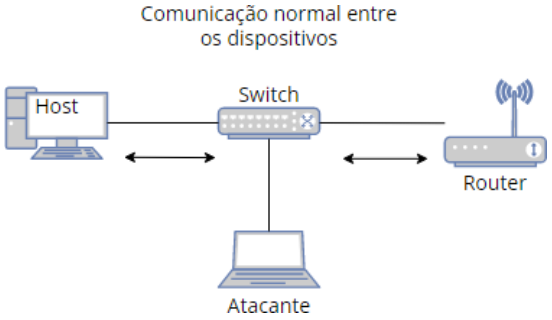
Ainda fazendo citação Gangan (2015), descreve que existem diferentes tipos de ferramentas no mercado para envenenamento de *cache ARP*, sendo alguns deles *Ettercap*, *Dsniff* e Cain e Abel etc. Uma forma de podermos controlar o envenenamento de *cache ARP*, é usando *Dynamic ARP Inspection* (DAI). O recurso de segurança DAI, é usado para validar os pacotes *ARP* na rede e descartar ligações inválidas de *IP* para endereço *MAC* Essa inspeção é realizada em *Switchs Ethernet* que são compativeis com a inspeção, fazendo sua configuração manualmente. A Figura 1 exemplifica o fluxo de tráfego regular entre dois computadores.

Figure 1. Fluxo de tráfego regular entre dois computadores.

Fonte: Elaborado pelo próprio autor.

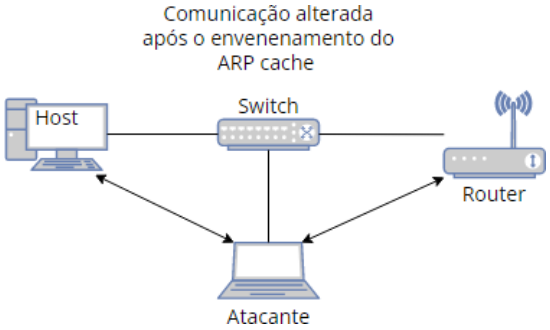
Segundo Silva (2019) o envenenamento do *ARP cache* explora uma falha de segurança no protocolo *ARP*, que permite atualizações de qualquer dispositivo, e em qualquer momento. Desse modo, um *Host* pode enviar resposta *ARP* para outro *Host* e forçá-lo atualizar seu *cache ARP* com o novo valor passado. Dessa forma, o atacante pode alterar o *IP* e *MAC* de destino se colocando no meio da comunicação, sem que a v´ıtima saiba, como mostra a Figura 2 e a Figura 3.

Figure 2. Rede antes do envenenamento ARP Cache.



Fonte: Elaborado pelo próprio autor.

Figure 3. Rede após o envenenamento ARP Cache.



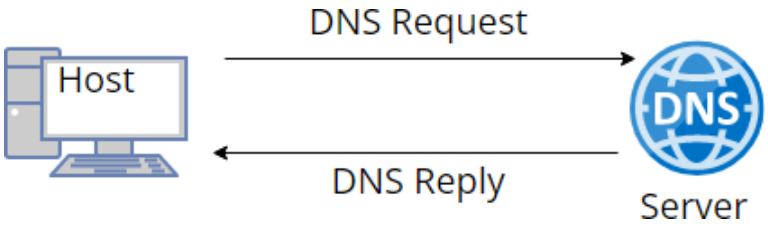
Fonte: Elaborado pelo próprio autor.

2.3. Falsificação de DNS

Esse tipo de ataque altera informações do protocolo *DNS* que são fornecidos aos dispositivos conectados em redes de computadores.

Toda vez que um usuário tenta se conectar em um site em seu computador, é feita uma requisição ao servidor *DNS*, solicitando o endereço *IP* deste site, dessa forma, encaminhando o usuário até o endereço *IP* solicitado. O processo é mostrado na Figura 4.

Figure 4. Comunicação entre host DNS server.



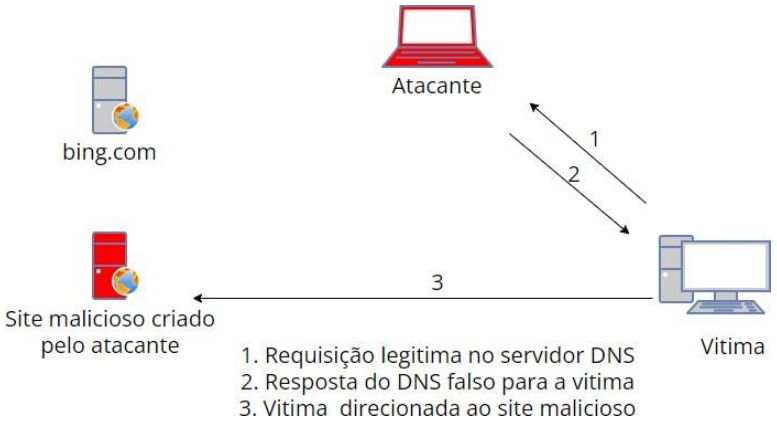
Fonte: Elaborado pelo próprio autor.

Segundo Gangan (2015) as solicitações e respostas *DNS* são mapeadas em conjunto com um número de identificação exclusivo. Se o invasor conseguir esse número, enganando a vítima com um pacote corrompido contendo o número de identificação, conseguirá lançar o ataque. Com isso, o atacante redireciona a vítima para um site falso e se a mesma acreditar que está em um site seguro e colocar suas informações como e-mail e senha, elas poderão ser capturadas pelo atacante.

Para o atacante conseguir usar o *DNS Spoofing*, ele primeiramente deve utilizar a

técnica de *ARP Cache Poisoning*, que permite interceptar todo o tráfego de dados entre o servidor *DNS* com a v´ıtima. Com isso, quando a v´ıtima faz uma consulta *DNS* ao servidor *DNS*, devido ao ataque *MITM*, e´ redirecionada ao site falso, consequentemente, tera´ suas credenciais roubadas. A Figura 5 traz um exemplo de como e´ realizado o ataque.

Figure 5. Ataque de falsificação do DNS.



Fonte: Elaborado pelo próprio autor.

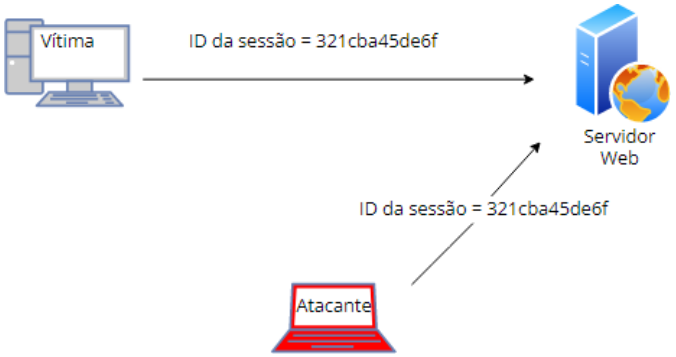
2.4. Sequestro de sessão (Session Hijacking)

Sessão relaciona a conectividade de um usuário a um site, como exemplo, em uma rede social, onde voceˆ entra utilizando suas credenciais de *Login* e Senha, desse modo se estabelece uma sessão de comunicação entre usuário e servidor *web*. A sessão se manterá estabelecida enquanto o usuário estiver conectado, após o usuário se desconectar do site a sessão é desfeita (BAITHA; VINOD, 2018).

Esse tipo de expressão é utilizada em muitos ataques e é voltado para sequestro de sessão por roubo de *cookie* que utiliza *HTTP*. Segundo Gangan (2015), a partir do momento em que se estabelece uma sessão entre PC *host* e servidor *web*, através da captura de *cookies* (pequeno arquivo armazenado no computador que contém informações como *login* e senha quando um usuário acessa um *site*), o invasor pode obter partes do estabelecimento da sessão. A Figura 6 mostra o início do ataque.

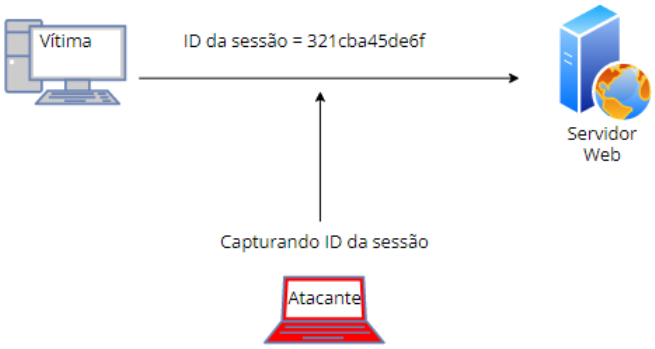
Utilizando o ID capturado, o atacante pode iniciar uma comunicação com o servidor, assim se passar pela v´ıtima, e concluir o ataque, conforme a Figura 7 demonstra.

Figure 6. Sequestro de sessão.



Fonte: Elaborado pelo próprio autor.

Figure 7. Capturando ID de sessão.



Fonte: Elaborado pelo próprio autor.

2.5. Sequestro de SSL

Segundo Botti e Martins (2015) esse é o tipo de ataque *MITM* mais potente, pois ele permite explorar os serviços que fazem a segurança na troca de informações, como os protocolos *HTTP* e *HTTPS*. Segundo Augusto (2014) *Secure Socket Layers* (SSL) e´ um protocolo de criptografia projetado para Internet, que permite a comunicação segura entre cliente e servidor de uma aplicação *web*.

Segundo Silva (2019), o ataque *SSL Hijacking* e´ realizada da seguinte forma: Primeiro é necessário que o atacante faça a interceptação do tráfego de dados entre o usuário e o servidor *web*, utilizando a técnica de *ARP Cache Poisoning*. Em seguida, quando solicitado o acesso ao site no servidor *web* via protocolo *HTTP*, a solicitação irá chegar ao atacante, que ira´ repassar ao servidor. Dessa forma, o servidor respondera´ a

solicitação do atacante fazendo o redirecionamento ao site *HTTPS*, e enviará o certificado digital de autenticidade, iniciando a comunicação. Então, o servidor pensará que estará se comunicando de forma segura e criptografada com o usuário, e vice e versa. Todas as mensagens serão recebidas pelo atacante sem criptografia via *HTTP*, enviadas pelo usuário ao servidor web, então, após serem salvas, serão envidas criptografadas via *HTTPS* ao servidor *web*. Com isso, o servidor *web* ira´ responder as mensagens via HTTPS enviando ao atacante, que conseguirá ler através do certificado digital, após salvá-las, o usuário receberá a mensagem sem criptografia. A Figura 8 nos ajuda a entender melhor sobre esse ataque.

Figure 8. Protocolo HTTPS

Fonte: Elaborado pelo próprio autor.

2.6. Cain & Abel

Segundo Donda (2020) Caim e Abel e´ um *software* originalmente criado para monitorar o tráfego, capturar pacotes de dados para verificar sua confiabilidade, recuperar senhas no Sistema Operacional *Windows*.

É desenvolvido com o objetivo de ser útil para profissionais de segurança, equipe forense, administradores de rede, professores, fornecedores de software de segurança, consultores, testadores de penetração profissional e qualquer outra pessoa que planejasse usá-lo de forma ética.

2.6.1. Pricipais Caracter´ısticas da Ferramenta Cain & Abel

Segundo Vieira (2008) com um programa desse, e´ poss´ıvel buscar senhas facilmente através de *sniffer* de rede em qualquer sistema de vários tipos de senhas, mesmo quando elas estão criptografadas, pois, ele pode descriptografá-las encontrando a chave real que fica escondida atrás do *hash*, com essa ferramenta ainda é possível detectar a rede, gravar conversas VoIP, recuperar chaves de rede sem fio, descobrir senhas em cache, revelar caixas de senhas, recuperar chaves de rede sem fio, analisar o roteamento de protocolos,

decifrar senhas criptografadas usando ataques de *Brute-Force, Dictionary* e de *Cryptanalysis*.

Sua última versão, conforme SegInfo (2013) possibilita analisar protocolos criptografados como *SSH-1* e *HTTPS*. Com esse *software* também conseguimos espionar qualquer rede, além de permitir capturar todas as senhas que são enviadas através dela. Do mesmo modo, permitindo fazer engenharia reversa de qualquer senha, mas isso se forem das mais prováveis ou utilizadas.

Conforme Mills (2020) o *software* ja´ esta´ presente entre os usuários há muito tempo. Porém, visto a sua funcionalidade, é normal que os *softwares* de segurança como os antiv´ırus, o detectem como um programa perigoso. O *Avast*, o reconhece como um programa potencialmente perigoso chamado *Win32: Cain – B* e o *Windows Defender* como *Win32 / Cain! 4.9: 14* e classifica-o como *software* de comportamento potencialmente perigoso.

Ainda fazendo referência a Mills (2020) o *software* por ser utilizado por *hackers*, acabou sendo considerado pelos programas de segurança como perigoso. Mesmo sendo afirmado pelo seu desenvolvedor em varias ocasiões que o *software* não possui *malware* ou não esconde portas traseiras, infelizmente, não é possível afirmar que é um programa 100% seguro, já que seu código fonte não foi colocado às disposição de empresas de auditoria para que saibamos que e´ realmente seguro. Deste modo, o programa e´ como qualquer outro *software* proprietário, útil, mas no qual devemos ter cuidado.

Com a ferramenta e´ poss´ıvel: Descobrir as senhas *Web* dos roteadores *Wi-Fi*; Utilizar técnicas de injeção de pacotes que acelerar a captura de pacotes em uma rede; Decifrar todos os tipos de senhas fortes; Melhorar a velocidade de quebra de senhas ele calcula *hashes* rapidamente; Capturar tráfego da rede, pois ele usa técnicas de *ARP Spoofing*; Encontrar o endereço *MAC* de qualquer *IP*; Calcular uma rota precisa de seu dispositivo para qualquer destino e Ler o conteúdo dos arquivos de senha *PWL* do *Windows*.

Além de ter todas essas funções, esse programa é possível hacker senhas dos protocolos a seguir: *APOP – MD5; Cisco IOS – MD5; Cisco PIX – MD5; CRAM – MD5; Hashes* de banco de dados *Oracle* e *SIP*; *Hashes* de chave compartilhada *RADIUS IKE PSK; Kerberos 5;LM e NTLM; MADURA MD – 160; MD2; MD4; MD5; MSSQL; MySQL; NTLMv2; OSPF – MD5; RIPv2 MD5; SHA – 1; SHA – 2 e VNC Triplo DES* -

HMAC.

2.7. Mac Binding Switch

De acordo com Yashee (2020), tem a função de vincular o endereço *MAC* ao endereço *IP*, de modo que as solicitações desse endereço *IP* sejam respondidas apenas pelo computador que possuir esse endereço *MAC*. Com isso, caso o endereço *MAC* ou *IP* mude, o dispositivo não poderá acessar a *Internet*.

2.8. Client Isolation

Conforme Mirzoev, White et al. (2014), a *Cisco Systems*, líder mundial na fabricação de equipamentos de rede, implementou a tecnologia *PSPF*, em tradução livre, Encaminhamento Público Seguro de Pacotes. *PSPF* é uma tecnologia de isolamento de cliente que impede que um cliente sem fio converse com o outro. Usa-se essa técnica para evitar ataques diretos *client-on-client* (Cliente-a-Cliente), mas sendo poss´ıvel impedir o sequestro de sessão, impedindo que pacotes *ARP* falsificados cheguem a vítima.

2.9. Virtual Box

Conforme a Oracle (2015), é um *software* de virtualização de plataforma cruzada em código aberto, também denominado como *software* de máquina virtual. Em outras palavras utilizado na criação de servidores e dispositivos virtuais.

3. Materiais e Métodos (ou Metodologia)

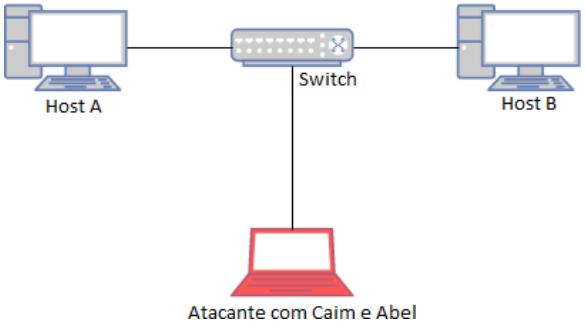
Essa parte do trabalho foi realizada através de um estudo de caso, em um ambiente controlado, com a intenção de monitorar e entender como é realizado um ataque de *Man-in-The-Middle*.

O ambiente foi construído através do *Virtual Box*. Dessa forma foram criadas três *VMs* (máquinas virtuais) em uma *LAN*, *Host A* instalado com *Windows 7 Professional*, *Host B* um *Debian 11* e Atacante que faz o uso de um *Windows 7 Professional*. A Figura 9 e´ uma topologia da rede criada no *Virtual Box*.

O esquema da Figura 10 exemplifica como e´ uma rede antes e depois de ser invadida pelo homem do meio.

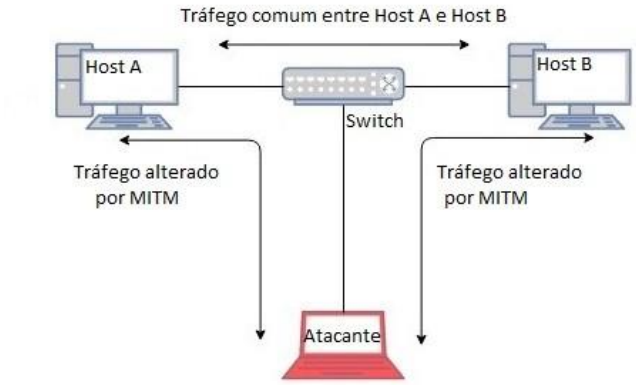
Em uma *LAN* com *swtichs*, para dois ou mais hosts se comunicarem é necessário que os pacotes passem pelo *switch* para depois chegarem ate´ o outro *host*, estabelecendo assim, um tráfego comum entre eles.

Figure 9. Topologia do ambiente de ataque.



Fonte: Elaborado pelo próprio autor.

Figure 10. Topologia do ambiente antes e no momento do ataque.



Fonte: Elaborado pelo próprio autor.

Com o in´ıcio de um ataque do Homem do Meio na rede local, e´ alterado o caminho dos pacotes, fazendo com que ao invés deles terem que passar pelo *switch* eles começam a passar pelo atacante e então o atacante nesse caso se passa pelo *switch* e envia os pacotes para outro *host* da rede, isso tudo sem que o *Host A* e o *Host B* saibam que existe um invasor e que seus dados estão sendo capturados.

Ainda que, Cain e Abel é considerado como um único programa, na verdade ele é composto por duas partes. Cain é o primeiro, no qual é responsável por quebrar as senhas. E o segundo é Abel, o serviço do *Windows NT* que faz a proteção do envio de senhas em redes locais.

O programa ocupa apenas *10 MB*, a não ser que tenha problemas com o antivírus,

sua instalação e inicialização não possui segredos. Além de não esconder publicidade indesejada ou *softwares*. Mas ainda deve ser levado em consideração que é *software* utilizado por *hackers*, então se não deseja prejudicar seu equipamento, faça as instalações em uma *VM*(Máquina Virtual).

Após o programa estar instalado, podemos usá-lo. Ao iniciar o Cain, observamos sua interface simples, onde temos todas as nossas ferramentas.

A interface do programa, como mostra a Figura 11, e´ dividida em abas, e em cada aba encontramos diferentes módulos: Decodificadores, *Network, Sniffer, Cracker, Traceroute, CCDU, Wireless* e *Query*.

Em cada aba, encontramos tudo o que é necessário para que possamos localizar as senhas e decifrá-las. Algumas técnicas são muito simples que qualquer *script kiddie* (Pessoa inexperiente que realiza ativades semelhantes a de *hackers*) pode realizar, ja´ outras são complicadas e, então é necessário ser um usuário avançado, para que não tenha problemas.

O tempo para quebrar a senha pode variar, dependendo do tipo de senha que estamos tentando quebrar.

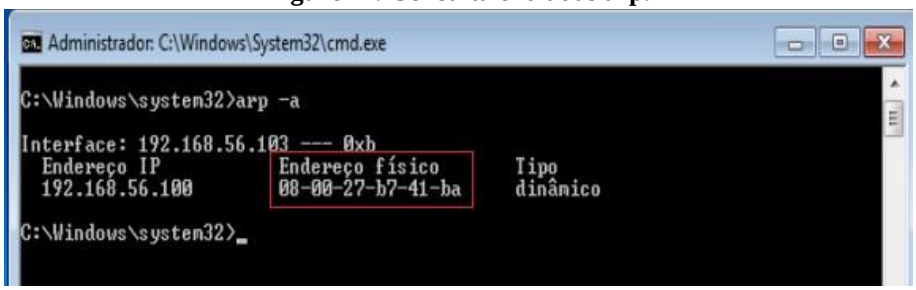
Figure 11. Interface Cain & Abel.

Fonte: Elaborado pelo próprio autor.

3.1. Tabela ARP

O início deu-se com a exibição das entradas para a tabela *arp*, vide a Figura 12. Visto qual *Mac Address* pertence ao servidor da rede após ter sido feita a verificação, fomos para uma outra etapa do ataque de *Man-in-The-Middle*.

Figure 12. Consulta entradas arp.

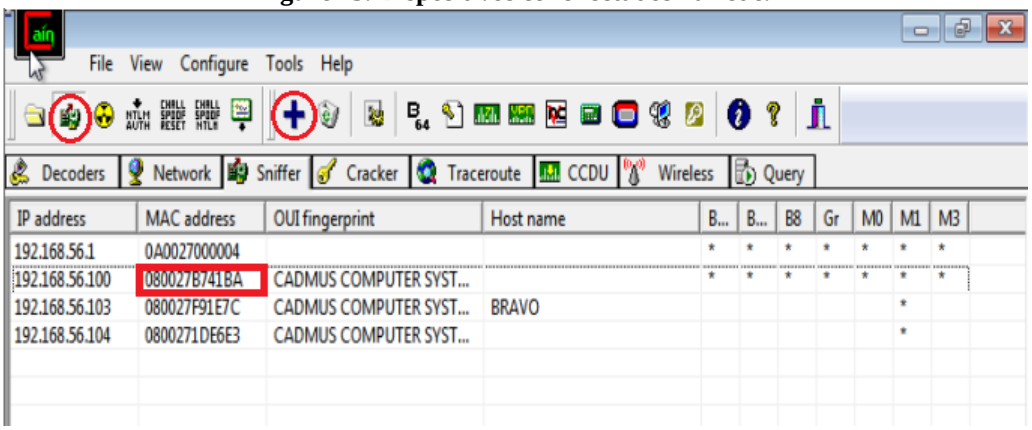


Fonte: Elaborado pelo próprio autor.

3.2. Ataque MITM

O ataque de *MITM* foi realizado apenas com a ferramenta Cain que fez o envenenamento do *ARP cache*, e para isso foi necessário descobrir quais sãos os dispositivos conectados nessa rede para então escolher quem seria a vítima do ataque. Para fazer isso, por ser uma ferramenta gráfica tivemos a vantagem em utilizar botões conforme pode ser visto na Figura 13.

Figure 13. Dispositivos conenectados na rede.



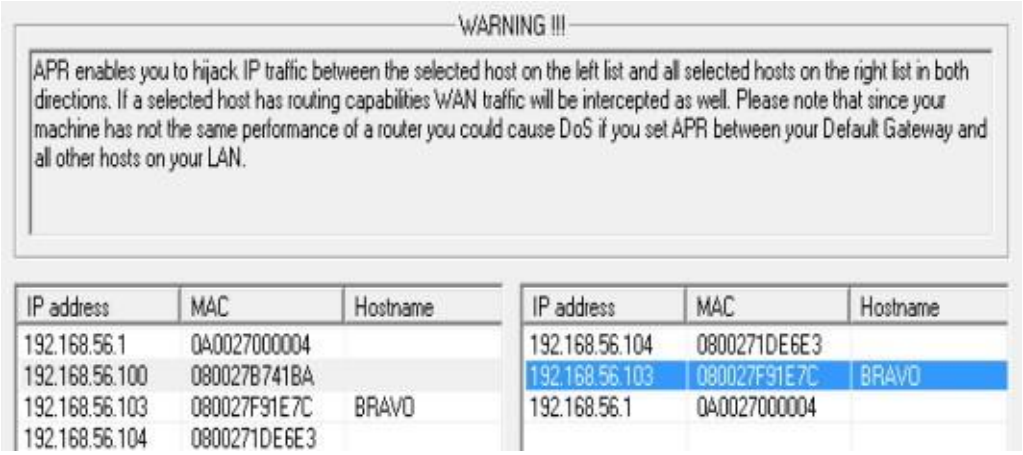
Fonte: Elaborado pelo próprio autor.

Nota-se que o endereço *Mac* é 080027b741ba, tanto para a vítima quanto para o atacante, com o decorrer do ataque esse endereço foi alterado.

A próxima fase foi executada com o envenenamento do dispositivo que foi a vítima do ataque de envenenamento de *ARP cache*. Conforme a Figura 14 na janela esquerda e´ onde podemos escolher qual *IP* do *gateway* que foi configurado para a rede, que por vez

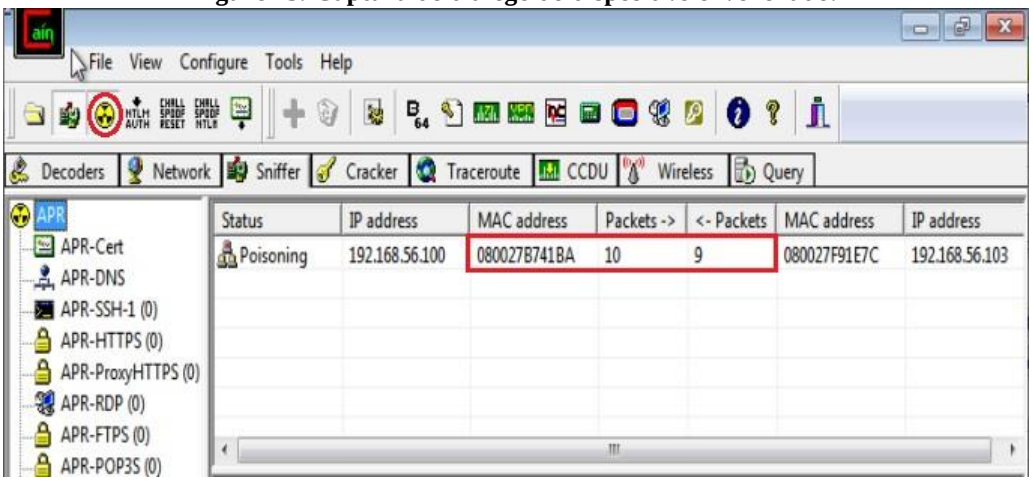
foi o *switch* (192.168.56.100), e na janela da direita foi onde se escolheu o *IP* da v´ıtima. Foi selecionado o *IP* 192.168.56.103 e em seguida na Figura 15 foi efetuado o ataque clicando no ´ıcone amarelo de radioativo no canto superior.

Figure 14. Envenenamento do ARP cache.



Fonte: Elaborado pelo próprio autor.

Figure 15. Captura do tráfego do dispositivo envenenado.

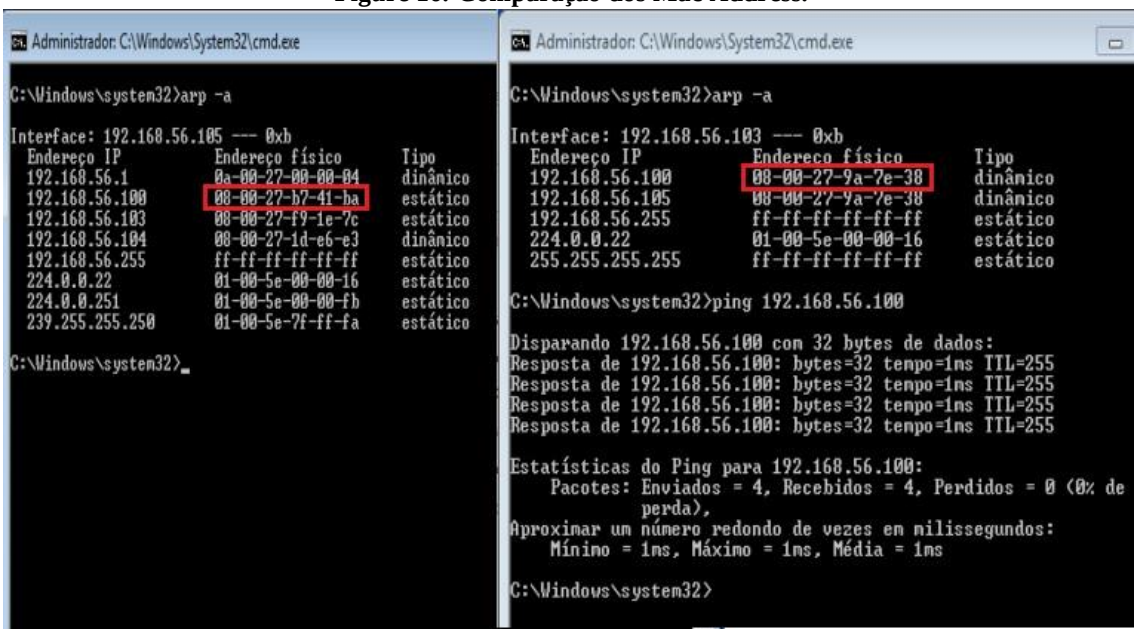


Fonte: Elaborado pelo próprio autor.

Nessa fase a ferramenta capturou as requisições do *Host A* que imaginou estar se comunicando diretamente com o *Host B*, mas na verdade tudo o que ele enviou estava passando pelo Atacante e então após a captura dos dados o Atacante repassou para o *Host B*.

Nota-se na Figura 16, que para o atacante, o *Mac Address* não foi alterado e continuou o mesmo (080027b741ba) após o ataque e com o comando *arp -a* executado no *prompt de comando* nos dois *Hosts*. Podemos observar a efetividade do ataque.

Figure 16. Comparação dos Mac Address.



Fonte: Elaborado pelo próprio autor.

4. Resultados e Discussões

Conforme demonstrado durante o desenvolvimento deste trabalho, existem possibilidades de sofrer ataques do tipo *Arp Poisioning*, em especial ao se conectar a` Redes desconhecidas, portanto, é boa prática, manter os Sistemas Operacionais de nossos dispositivos sempre atualizados, bem como utilizar ferramentas Antivírus e de proteção de *Internet* e da Rede. Quando for possível, conhecer as configurações dos dispositivos da Rede, utilizar os comandos *arp -d* e *arp -s* (ambos Windows), para, respectivamente, excluir endereçamento suspeito e adicionar endereçamento estático na tabela *ARP*, a qual relaciona endereçamento *MAC* e *IP*. Evitando assim o *ARP Request* e *ARP Response*, como forma de pesquisa automática dos dispositivos na rede. Na questão física da implantação da rede, para evitar o *ARP Poisioning*, deve-se optar pelo uso de *Switches* com a funcionalidade *Mac Binding Switch*, que associa um endereçamento *MAC* a uma porta, impedindo a "injeção" de novo endereço causado pela tentativa de um ataque. Na rede *Wi-Fi* também é

possível habilitar o *Client Isolation*, que não permite que dois dispositivos conectados em um mesmo *Access Point* troquem informações diretamente, visto que o servidor de acesso costuma estar na parte cabeada da rede, sendo obrigatório que o dispositivo que deseja se conectar à Internet, primeiro se conecte à *Wi-Fi* e na sequência envie pacotes para a Rede Cabeada após o *Wi-Fi* do *Access Point*. Como o *ARP Poisioning* é uma das bases para o desvio, ou roteamento de pacotes, para ação do ataque de *Man-in-The-Middle*, prevenir-se contra esta base, torna muito mais difícil a execução do ataque de *Man-in-The-Middle* e a perda da confidencialidade, principalmente de usuários e senhas de sistemas.

O objetivo do trabalho foi fazer um estudo de caso da ferramenta Cain & Abel, listar os principais tipos de ataques do tipo *Man-in-The-Middle* e propor formas de evitar esse tipos de ataques.

O software Cain & Abel, por mais que seja antigo, conseguiu cumprir com seu objetivo, e foi poss´ıvel capturar alguns pacotes de uma rede formada por um *Switch*. Dessa forma podemos observar a necessidade de proteger uma rede, visto as chances de ataques, vindo da utilização das técnicas disponíveis, e com isso podendo ter os dados monitorados e roubados nas redes que estiverem conectados.

Referências

AUGUSTO, E. *Como funciona o protocolo SSL/TLS*. 2014. Https://www.ecommercebrasil.com.br/artigos/seguranca-como-funciona-o-protocolo-ssltls/.

BAITHA, A. K.; VINOD, S. Session hijacking and prevention technique. *International Journal of Engineering & Technology*, v. 7, n. 2.6, p. 193–198, 2018.

BOTTI, C. F.; MARTINS, D. M. S. Análise comparativa entre ferramentas de ataque man in the middle. *Caderno de Estudos em Sistemas de Informação*, v. 2, n. 2, 2015.

DONDA, D. *Cain & Abel*. 2020. Https://danieldonda.com/cain-abel/.

GANGAN, S. A review of man-in-the-middle attacks. *arXiv preprint arXiv:1504.02115*, 2015.

INFORCHANEL. *Ataques cibernéticos no Brasil crescem 860% na pandemia*. 2021. Https://inforchannel.com.br/2021/03/03/ataques-ciberneticos-no-brasil-crescem-860-na-pandemia/.

MILLS, M. *Cain e Abel: programa para crackear e hackear senhas*. 2020. Https://itigic.com/pt/cain-and-abel-program-to-crack-and-hack-passwords/.

MIRZOEV, D.; WHITE, S. et al. The role of client isolation in protecting wi-fi users from arp spoofing attacks. *arXiv preprint arXiv:1404.2172*, 2014.

ORACLE, V. *VirtualBox*. 2015.

SEGINFO. *Tutorial Cain Abel: Ferramenta de recuperação de senha para Sistemas Operacionais Microsoft*. 2013.

SILVA, C. A. S. Análise de vulnerabilidades em redes wireless: proposta de soluções para ataques do tipo mitm. 2019.

VIEIRA, L. *Cain e Abel: Cain Abel – Segurança e monitoramento de tráfego*. 2008. Https://imasters.com.br/devsecops/cain-e-abel-seguranca-e-monitoramento-de-trafego/.

YASHEE. *Mac Binding Addresss*. 2020. Https://indianexpress.com/article/explained/explained-what-is-mac-binding-the-condition-specified-for-using-the-internet-in-jk-6299406/.