Análise comparativa entre ferramentas de ataque Man in the middle

Caio Fernandes Botti, Daves Márcio Silva Martins

Sistemas de Informação – Centro de Ensino Superior de Juiz de Fora (CES/JF)
36016-000 – Juiz de Fora – MG – Brasil

caiofbotti@gmail.com

Resumo: *Nos dias atuais, com o avanço da Internet, cada vez mais os usuários estão usufruindo deste avanço tecnológico, mas os usuários estão em constante risco de sofrerem um ataque e ter seus dados capturados ou monitorados. Nesse artigo será abordado um tipo de ataque, conhecido como Man In the Middle, que intercepta a comunicação entre dois computadores interligados por uma rede, como por exemplo a internet. Um ambiente computacional foi preparado para realização de um estudo de caso utilizando duas ferramentas de ataque Man in the middle, o Kali Linux e Cain&Abel. Os resultados dessa simulação de ataque foram comparados e é apresentada uma discussão sobre as ferramentas. O artigo mostra a facilidade de uso das ferramentas para o ataque.*

Abstract: *Nowadays, with the advent of the Internet, more and more users are taking advantage of this technological advance , but users are at constant risk of suffering an attack and have your data captured or monitored. In this paper is discussed a type of attack, known as a man in the middle , which intercepts the communication between two computers connected by a network such as the Internet . A computational environment was prepared to conduct a case study using two attack tools Man in the middle . The tools selected KaliLinux and Cain & Abel. The results of this attack simulation were compared and a discussion of the tools is presented . The article shows the ease of use of the tools for attack.*

.

1 Introdução

No mundo atual é crescente o número de pessoas conectadas na Internet, com esse aumento cresce as possibilidades de sofrer algum tipo de ataque e ter suas informações capturadas. A preocupação por segurança não tem crescido na mesma proporção, com isso são cada vez mais frequentes histórias de pessoas que tiveram seus dados roubados e usados de maneira ilícitas. As pessoas se preocupam com a segurança do seu próprio computador, mas esquecem da segurança da rede a qual está conectada. Um antivírus ou um firewall pode proteger os dados de uma máquina mais não podem proteger os dados que trafegam na rede.

Um dos ataques mais utilizados na atualidade são os ataques man in the middle (MITM), cujo o objetivo é interceptar os dados que saem de uma máquina até o servidor, muitas vezes o usuário não sabe que seus dados foram capturados, ou que ele tenha sofrido um ataque segundo Sanders (2010).

Neste artigo será apresentado um ambiente virtual controlado, onde o objetivo é realizar um ataque MITM simulado, comparando duas ferramentas, a Kali Linux e Cain&abel. Ao final será apresentado um comparativo dos resultados obtidos e como se proteger de algumas variações do ataque MITM.

2 Ataque Man in the middle (MITM)

Neste tipo de ataque segundo Cunha (2006), o atacante é capaz de ler, inserir e modificar, mensagens entre duas entidades sem que estas tenham conhecimento que a ligação entre ambas está comprometida. Tipicamente o atacante insere-se no meio da comunicação entre dois hosts, fazendo parte do canal de comunicação como é mostrado na figura 1.

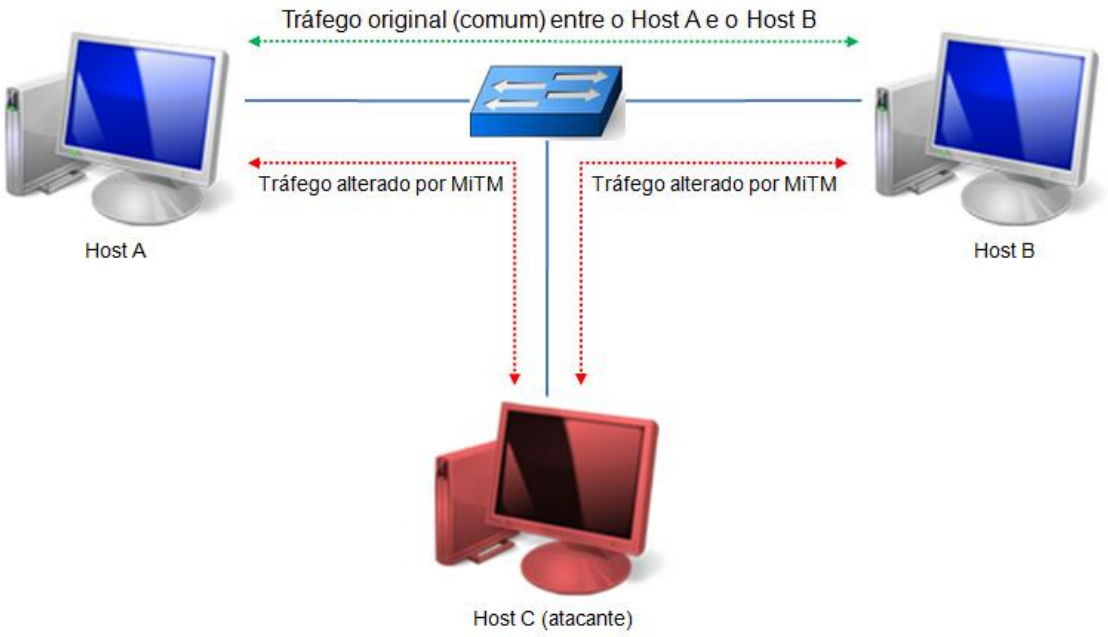

Figura 1. Ataque Man in The Middle. Fonte: Autor

O autor do ataque pode se comportar de duas maneiras, passivo, onde os dados das vítimas são apenas monitorados e ativo, onde os dados são monitorados e podem sofrer alterações antes de chegar no servidor de destino.

Nesse ataque, muitas vezes a vítima nem fica sabendo que está sendo monitorada ou sendo atacada. Este tipo de ataque é simples, porém muito eficiente em redes locais. Por isso é importante sempre ficar atento em qual rede se conectar, e garantir que seja uma rede confiável.

É muito comum hoje em dia, estabelecimentos como shoppings, restaurantes e locais públicos possuírem uma rede *WIFI* aberta, por falta de informação o usuário que se conecta nessa rede está exposto a vários tipos de ataques, como por exemplo, o roubo de sessão, o usuário pode ter sua máquina invadida a partir de um *backlog* e sofrer um ataque MITM.

O artigo aborda a técnica de ataque MITM comparando duas ferramentas de plataformas distintas. Uma é o Cain&Abel que é da plataforma Windows e a outra é o

Kali Linux, que é um sistema operacional, baseado na plataforma Linux, que possui diversas ferramentas para a realização de ataques.

2.1 Tipos de ataque man in the middle.

Segundo Sanders (2010), as técnicas de ataque MITM mais utilizadas são: *ARP cache poisoning, dns spoofing, http session hijacking e ssl hijacking*.

2.1.1 ARP CACHE POISONING

Esse é o tipo de ataque MITM mais antigo e eficiente para redes locais, esse tipo de ataque permite que o atacante, conectado na mesma rede possa espionar todo o trafego da rede, ou de dois *Hosts* distintos. O foco desse tipo de MITM é o envenenamento do cache ARP.

O protocolo ARP foi desenvolvido para a resolução de endereços IP[1] em endereço físico (MAC[2]). Segundo Souza (2010), para solucionar o problema de mapear o endereço de nível superior (IP) para endereço físico (Ethernet) foi proposto através da RFC826 o *Address Resolution Protocol* (ARP). O ARP permite que um Host encontre o endereço físico de um host destino, tendo apenas o seu endereço IP. Para um Host se comunicar com outro Host, que possui um endereço IP qualquer , ele envia um pacote de broadcast[3] na rede, para descobrir quem possui um endereço IP especifico, essa é uma ARP *request* (Requisição ARP), o Host que possuir o endereço IP solicitado ,vai enviar uma ARP *reply* (Resposta ARP) com o seu Mac (endereço físico) como pode ser visto na figura 2.

1 IP: Internet Protocol é o principal protocolo de comunicação da internet.

2 MAC: Media Access Control é um endereço físico e único, que é associado à interfaces de comunicação utilizadas em dispositivos de rede.

3 Broadcast: Pacote transmitido a todos os hosts de uma rede.

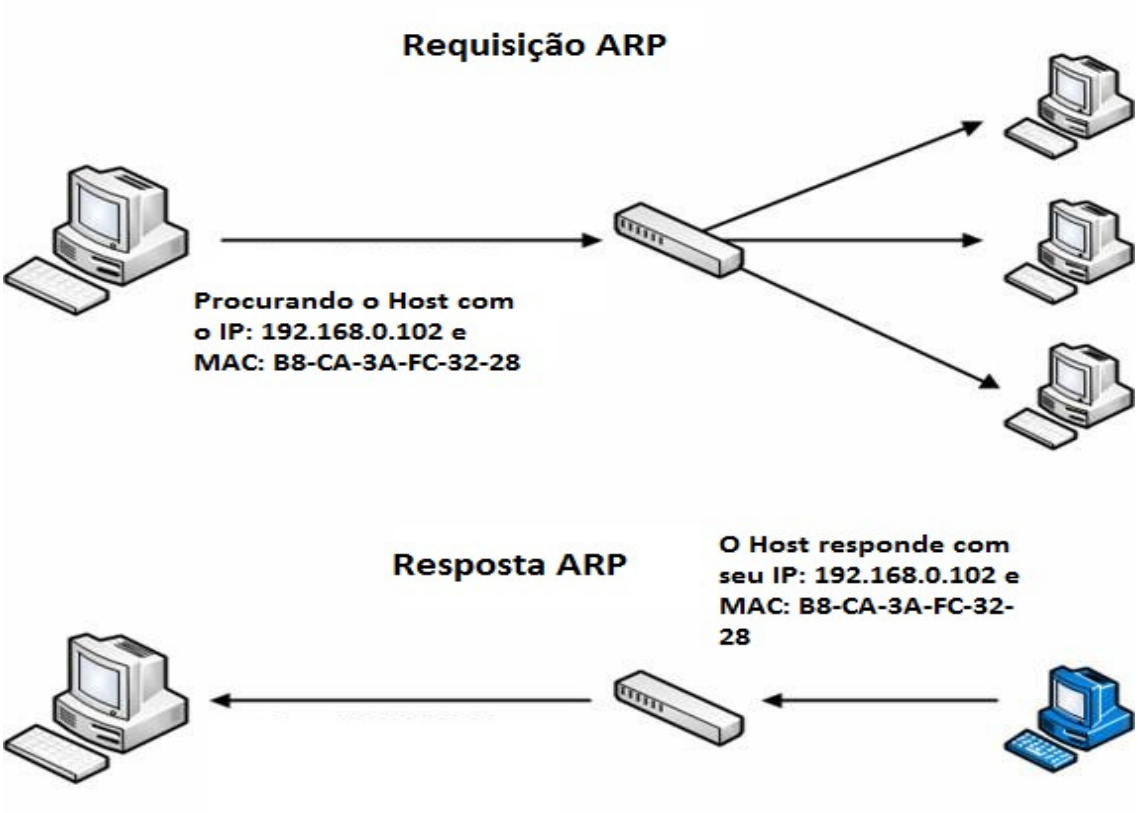

Figura 2. Consulta e resposta na comunicação ARP. Fonte: Autor**.**

Em uma rede de grande porte e altamente utilizada, o envio de pacotes em broadcasting interromperá todos os hosts para que eles processem cada pacote da rede. Essa interrupção prejudicará de maneira significativa a eficiência da rede e a tornaria mais lenta. Para reduzir os broadcasts, os hosts de redes utilizam o ARP, mantêm uma lista de endereços IP e Ethernet que correspondem a eles obtidos por solicitações anteriores. Isto é chamado de Cache ARP, e esse cache é atualizado sempre que uma solicitação for enviada segundo Souza (2010).

Segundo Sanders (2010) o envenenamento do ARP cache explora uma falha de segurança no protocolo ARP, em que este aceita atualizações de qualquer dispositivo a qualquer momento. Com isso um *Host* pode enviar resposta ARP para outro *Host* e força-lo a atualizar seu cache ARP com o novo valor passado. Com isso o atacante consegue alterar o IP e MAC de destino se colocando no meio da comunicação, sem que a vítima se dê conta. A figura 3 mostra o atacante se colocando no meio da comunicação do *Host* A e *Host* B. Após alterar o cache ARP todas as informações estão passando por ele sem que a vítima saiba.

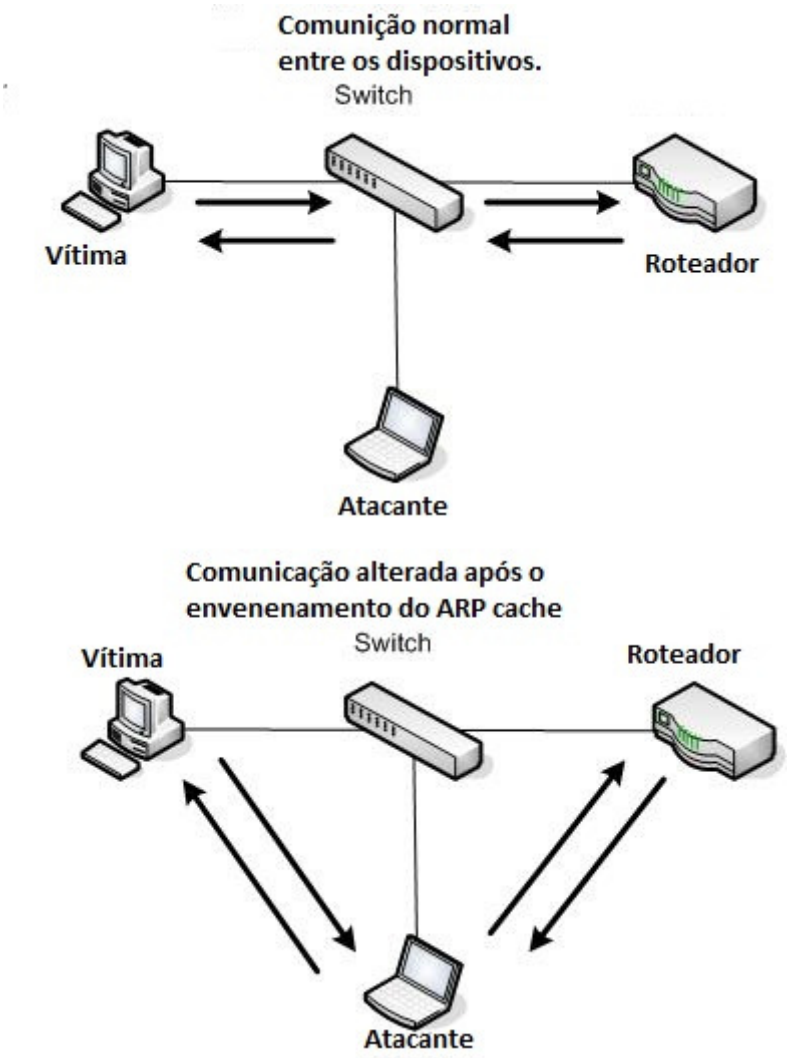

Figura 3. Envenenamento do ARP cache.

2.1.2 DNS spoofing (falsificação de DNS)

Esta é uma técnica de ataque MITM usada para fornecer informações falsas de DNS para um host de uma rede local.

Segundo Silva (2014) o *Domain name System* (DNS) é o responsável por localizar e traduzir para números IP os endereços dos sites que é passado nos navegadores. Para saber qual o IP de um determinado site é enviado uma consulta DNS, que possui um ID que tem por objetivo indexar consultas e respostas.

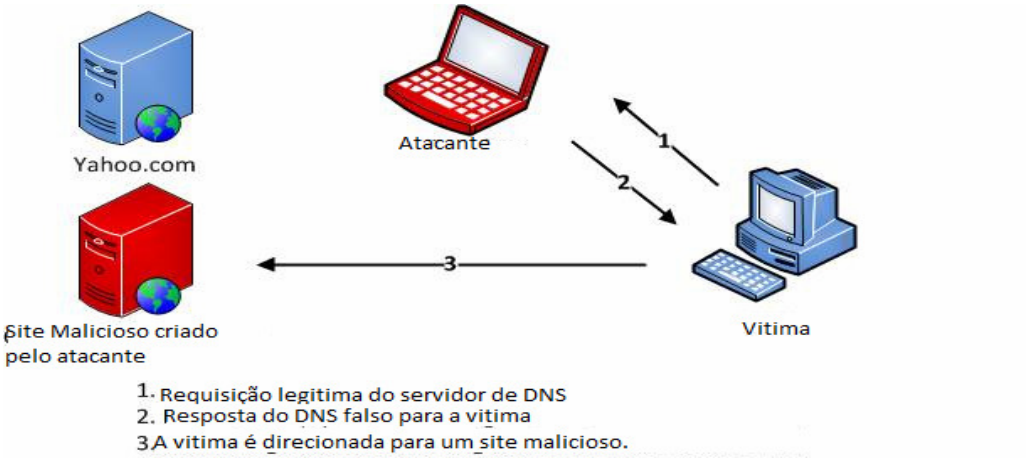

Figura 4. Ataque de falsificação do DNS.

Nessa técnica o atacante intercepta o trafego da rede para capturar uma consulta DNS e modifica-la, fazendo com que a vítima seja direcionada para uma página falsa da internet. A figura 4 mostra que a vítima está fazendo uma consulta de DNS de um determinado site, ao invés da consulta ser feita para o servidor de DNS ela é direcionada para o atacante, que em posse dessa informação, pode direcionar a vítima para um site malicioso. Se a vítima acessar essa página falsa o ataque já foi realizado e a partir daí a vítima acha que está em um site seguro e insere suas informações como e-mail, senhas. Com posse das credenciais da vítima o atacante pode usa-las para fins maliciosos.

2.1.3 Session Hijacking (sequestro de sessão)

A expressão sequestro de sessão é utilizada em muitos ataques que adotam a exploração de sessões. O termo sessão é relacionado a uma conexão entre dispositivos em que não há estado, o que significa que há um diálogo estabelecido no qual uma conexão foi formalmente constituída. A conexão é mantida e um processo definido vai encerrar a ligação. Esse tipo de ataque é voltado para o sequestro de sessão através do roubo de *cookie*[4] que utilizam HTTP.

Um exemplo de uso de sessões é quando você deve ser autenticado pelo *site* com seu nome de usuário e senha para definir formalmente a sessão. O *site* mantém alguma forma de rastreamento de sessão para garantir que o usuário acesse algum conteúdo sem ter estabelecido a sessão. Quando a sessão está terminando, as credenciais são apagadas. Nesse ataque, a vítima não sabe que está sendo monitorada e faz um acesso a um servidor qualquer que vai gerar o ID da sessão. Nesse momento, o atacante consegue o ID e se comunica com o servidor com esse ID, se passando pela vítima, como é mostrado na figura 5.

4 Cookie: pequeno arquivo que é armazenado no computador quando um usuário acessa um site, contém informações sobre o usuário, como nome de usuários e senhas.

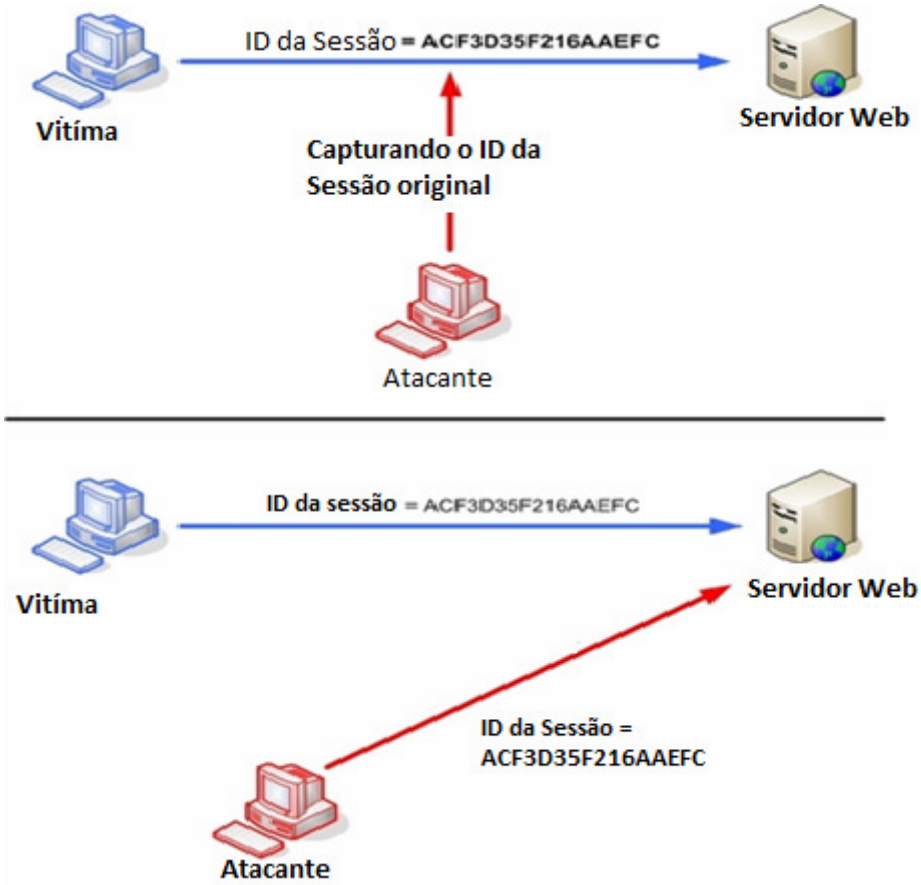

Figura 5. Roubo do ID da sessão. Fonte: Autor.

2.1.4 SSL Hijacking

Esse é o tipo de ataque MITM mais potente, pois permite a exploração dos serviços que têm como finalidade a segurança na troca de informações. Segundo Augusto (2014), *Secure Socket Layers* (SSL) é um protocolo de criptografia projetado para internet. Permite a comunicação segura entre os lados cliente e servidor de uma aplicação Web.

O Ataque SSL é feito através do HTTP ou do HTTPS, nos quais o uso de SSL é muito comum, segundo Sanders (2010). Muitos sites que usam HTTPS visam garantir que a comunicação entre cliente e servidor seja criptografada. No Kali Linux, há uma ferramenta que é utilizada para atacar o protocolo SSL ,é o SSLStrip[5] ,essa ferramenta faz o sequestro das sessões e vai ser mostrada no ataque no final do artigo.

3 Ferramentas para o ataque Man in the middle.

5 Disponível em: http://sectools.org/tool/sslstrip/

O ataque MITM é um ataque simples, porém muito perigoso, para realização do ataque foi utilizada algumas ferramentas que trabalham em paralelo para realizar a captura do trafego na rede.

Neste artigo vão ser comparadas duas ferramentas que realizam este tipo de ataque o Cain&Abel e o Kali Linux além de outras que complementam o ataque.

- **Cain & abel:** O Cain & Abel é uma ferramenta de recuperação de senhas para sistemas operacionais Microsoft, segundo Vieira (2008) ela permite fácil recuperação de vários tipos de senhas através de sniffer de rede, desencriptação de senha usando dicionários, força bruta, decodificações de senhas codificadas, recuperação de senhas armazenadas em cachê e analise dos IP. Uma característica que foi levada em consideração para a escolha deste programa é sua opção de habilitar o sniffing em redes com switch e ataques MITM.

- **Kali Linux:** O Kali Linux é um projeto *open source* que é mantido e financiado pela Segurança Ofensiva, um fornecedor de treinamento de segurança da informação de classe mundial e de serviços de teste de penetração. Segundo o site oficial, esse sistema possui mais de 300 ferramentas de testes de intrusão e é muito utilizado para estudos de prevenção de ataques.

- **Ettercap:** É uma ferramenta voltada para esse tipo de ataque na rede (MITM), o Ettercap possui interface gráfica e linha de comando. Essa ferramenta funciona colocando uma interface de rede em modo promiscuo e realiza o envenenamento ARP da vítima, se colocando no meio da comunicação. Com essa ferramenta é possível realizar outros tipos de ataque MITM como: *DNS SPOOFING e ARP POISON.*

- **SSLSTRIP:** Essa ferramenta foi desenvolvida na linguagem python e é utilizada para no ataque MITM de *SSL Hijacking* para burlar sessões HTTPs, nessa ferramenta a comunicação entra a vítima e o atacante é feita via HTTP, já a comunicação entre o atacante e o servidor é feita via HTTPs.

- **VirtualBox:** Software de virtualização da Oracle que é capaz de simular um sistema computacional completo. Assim, é possível instalar vários sistemas operacionais em uma mesma máquina e simular uma rede local. Esse Software foi utilizado para simular o sistema Kali linux.

4 Ambiente do ataque

Para realizar o ataque foi configurado um ambiente controlado para que não seja preciso roubar dados de terceiros já que o intuito do artigo é para aprendizagem.

O ataque vai ser realizado por duas maquinas virtuais, onde uma delas será uma máquina virtual com o sistema operacional Windows, que terá a ferramenta Cain&Abel já que essa ferramenta só roda nesta plataforma. A outra máquina virtual terá o sistema operacional KaliLinux instalado, com suas diversas ferramentas de ataque e monitoramento embutidas nela como o ETTERCAP e SSLSTRIP.A vítima que sofrerá o ataque é um notebook com sistema operacional Windows 7 Professional. As duas maquinas virtuais utilizadas para realizar o ataque possuem a mesma configuração de hardware, com 2 GB de memória cada, ficando mais objetivo o critério de comparação de tempo.

A figura 6 mostra o ambiente que foi configurado para realizar o ataque MITM, pode-se notar que a vítima (192.168.0.100) está acessando um site da WEB e insere suas credenciais como Email e senha. Como o atacante se coloca no meio da comunicação cliente/servidor, ele conseguirá capturar os dados da vítima que acredita estar se comunicando diretamente com o servidor WEB.

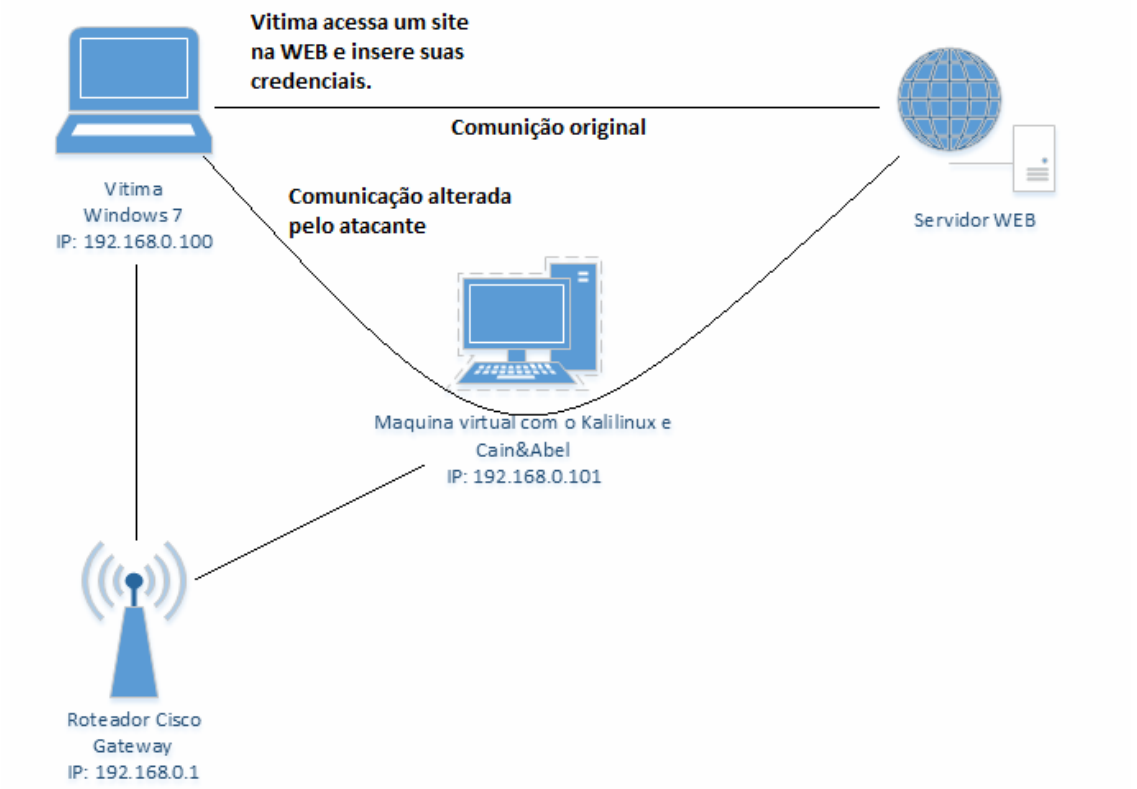

Figura 6. Ambiente configurado para realizar o ataque MITM. Fonte: Autor.

5 Execução do ataque com Cain&Abel e Kali linux.

O ataque que será realizado com as duas ferramentas será o ataque MITM de envenenamento do ARP cache, para começar o ataque com ambas as ferramentas é necessário descobrir os dispositivos conectado nessa rede e escolher um para ser a vítima do ataque. Para descobrir os dispositivos conectados nessa rede pelo Cain&Abel, é utilizado apenas botões como pode ser visto na figura 7. No Kalilinux é utilizado linha de comando, no terminal de controle é inserido o comando *ROUTE*, para descobrir o *gateway* da rede, com o IP do *gateway* já é possível começar a fazer um escaneamento dessa rede para descobrir os *Hosts* conectados com o comando *NMAP 192.168.0.1* que é o IP do nosso roteador. O resultado do comando *NMAP* é mostrado na figura 7.

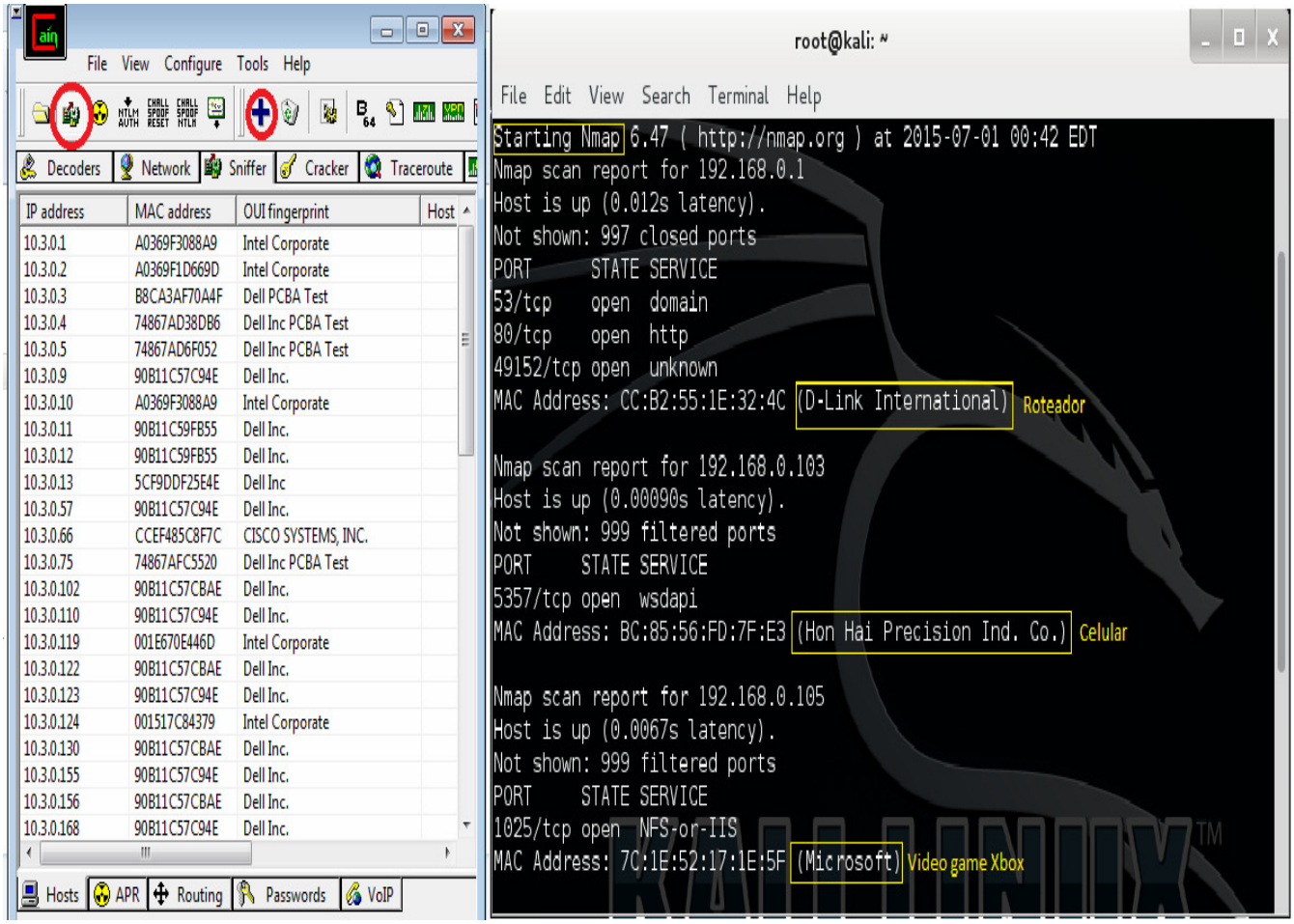

Figura 7. Dispositivos conectados na rede. Fonte: Autor.

O próximo passo é envenenar o dispositivo que sofrerá o ataque de envenenamento de ARP cache. Nas duas ferramentas é possível realizar este tipo de ataque MITM. O Cain&Abel possui uma interface gráfica o que o torna mais amigável e de fácil compreensão quanto ao uso, mas isso pode limitar as operações a serem realizadas, como pode ser visto na figura 8.

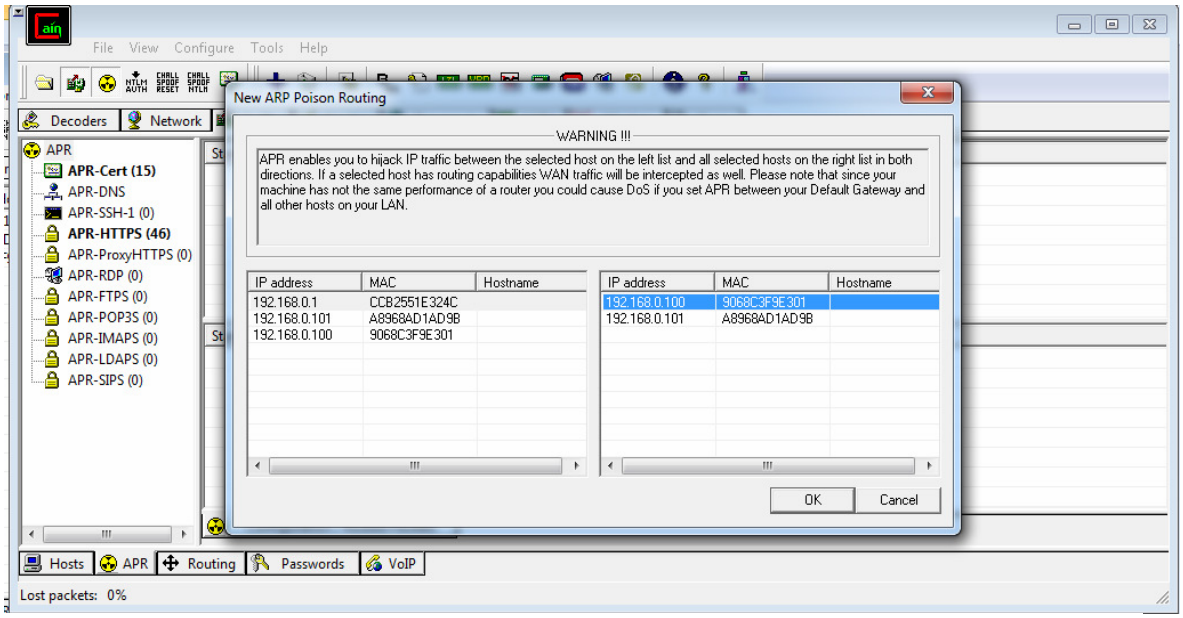

Figura 8. Tela do Cain&Abel onde é feito o ataque de envenenamento do ARP cache. Fonte: Autor.

Nessa tela do Cain&Abel, na janela esquerda é onde se pode escolher o IP do *gateway* que foi configurado para essa rede, que no caso é o roteador (192.168.0.1) e na janela da direita é onde se escolhe o IP da vítima, a vítima escolhida foi o 192.168.0.100.A vítima já foi selecionada e agora para efetuar o ataque é preciso clicar no ícone amarelo de radioativo no canto superior. Na figura 9 é visto que o roteador foi envenenado e que o trafego já foi alterado.

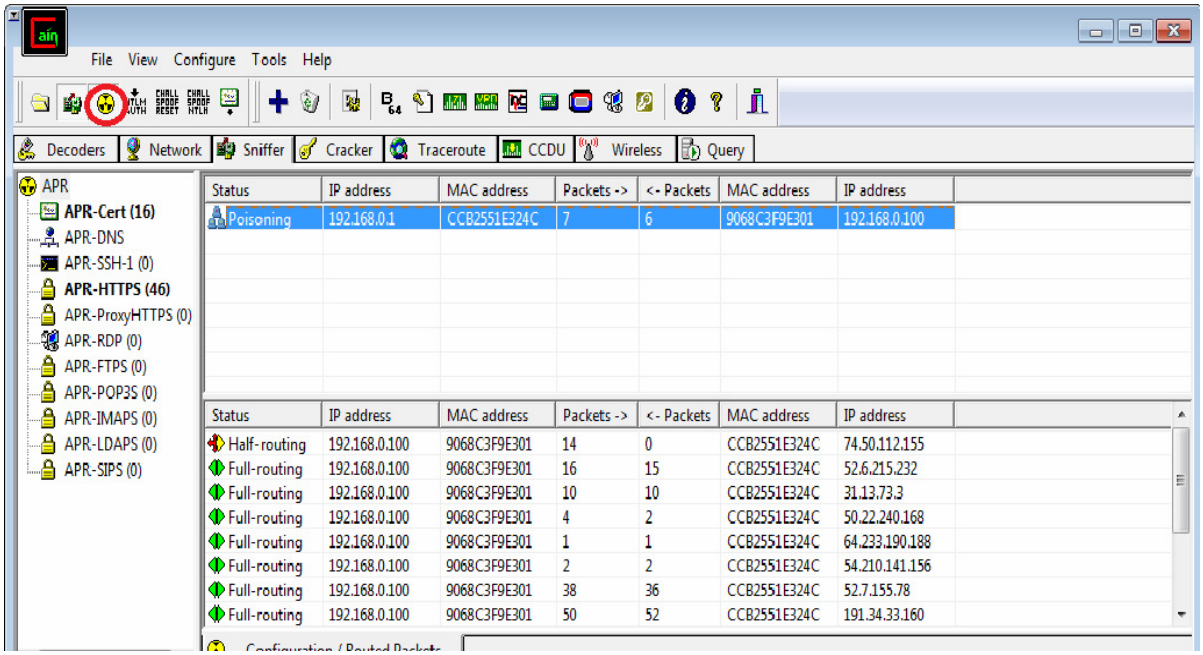

Figura 9.O ataque foi realizado e trafego do disposto envenenado já está sendo capturado. Fonte: Autor.

Esse mesmo ataque feito com o Kali linux é um pouco mais complicado por não ter uma interface gráfica, com isso todo o ataque é feito por linha de comando no terminal.

Para realizar o ataque no Kali Linux é preciso habilitar uma função que já vem embutida no sistema operacional por padrão que é o encaminhamento de IP e pacotes com o comando:

echo 1 >> /proc/sys/net/ipv4/ip_forward.

Com esse comando o computador vai trabalhar como um roteador. Com isso é possível forçar todo o trafego HTTP que está sendo interceptado e encaminhá-lo para uma porta especifica onde o SSLSTRIP vai ser executado. Para encaminhar o trafego para uma porta específica é utilizado o comando:

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000.

Para ler os dados que foram direcionados para porta 10000 é utilizado o SSLSTRIP, para executar a ferramenta é usado o comando:

SSLSTRIP –L 10000

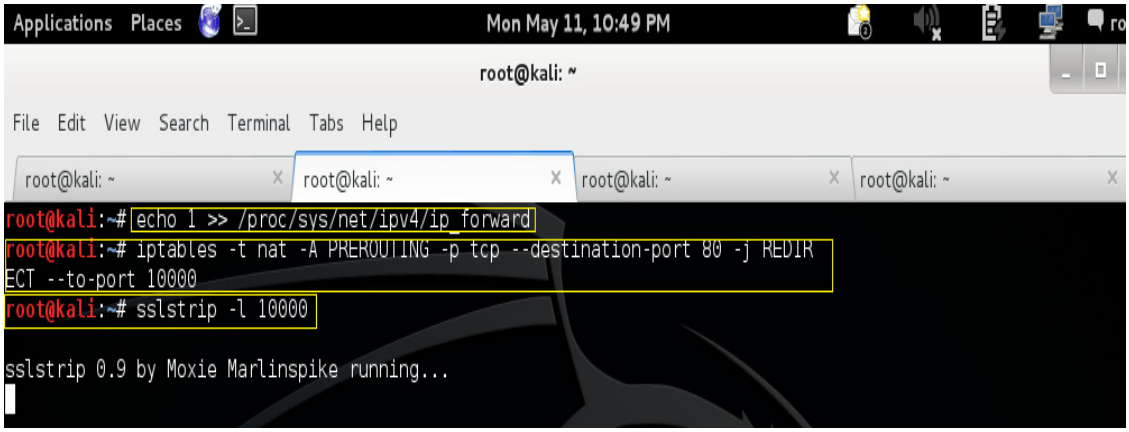

Figura 10. Comandos utilizados no terminal do Kalilinux para realizar o ataque MITM.

Para realizar o ataque MITM no protocolo ARP no Kali Linux, é necessário executar uma ferramenta que auxilia nesse tipo de ataque que é o Ettercap.

Para executar a ferramenta é usado o comando:

ettercap -T -q -i wlan0 -M arp: remote /192.168.0.1/ /192.168.0.100/

Onde os parâmetros do comando são:

-T: modo texto.

-q: modo silencioso.

-i wlan0: interface de rede.

-M arp: remote: Será feito um ataque MITM no protocolo ARP.

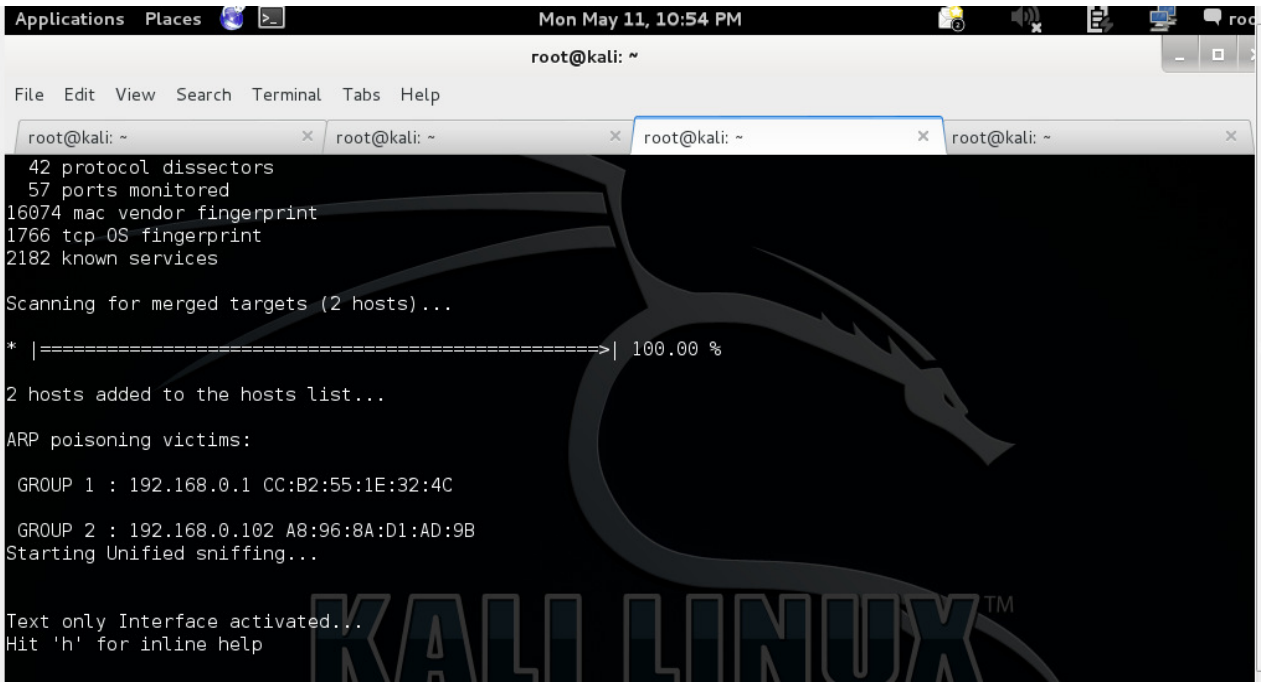

Figura 11. Resultado do comando ETTERCAP no Kali Linux. Fonte: Autor.

Após rodar o comando ETTERCAP o terminal retorna uma mensagem informando que o Host escolhido foi atacado e o roteador foi envenenado, como pode ser visto na figura 11, agora o ataque foi realizado e já é possível capturar todo o trafego HTTP desse dispositivo. Com as duas ferramentas, após o envenenamento do host o atacante tem acesso a todo trafego HTTP que a vítima está acessando em seu dispositivo, com isso o atacante pode capturar todas as informações trocadas entre vítima e roteador sem que a vítima saiba, pode se observar na figura 12, o trafego HTTP sendo monitorado pelo Kali Linux, os sites acessados pela vítima estão destacados de amarelo.

Na figura 13 é mostrado o trafego HTTP sendo monitorado pelo Cain&Abel, além de exibir o site acessado, ainda possui uma aba para capturar login/senha que foram acessados via HTTP, na figura 13 pode-se notar que a vítima acessou o site do CESJF e logou no portal do aluno, com posse dessas informações o atacante pode usa-las para fins maliciosos.

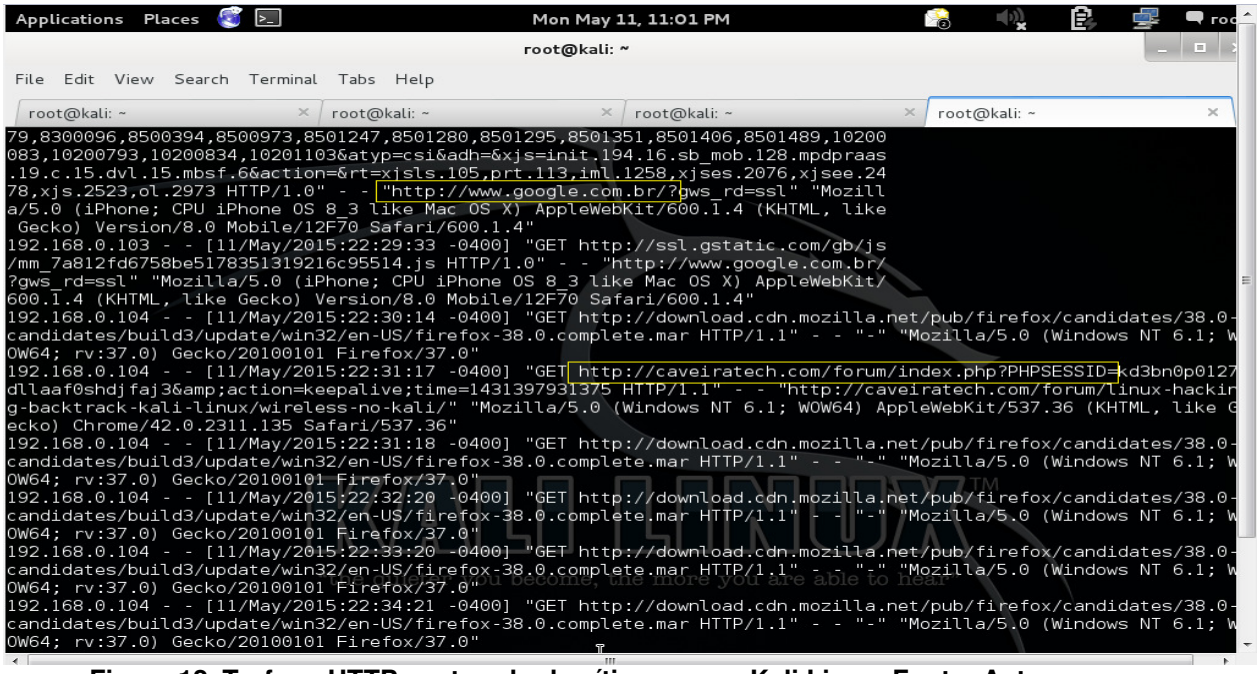

Figura 12. Trafego HTTP capturado da vítima com o Kali Linux. Fonte: Autor.

U

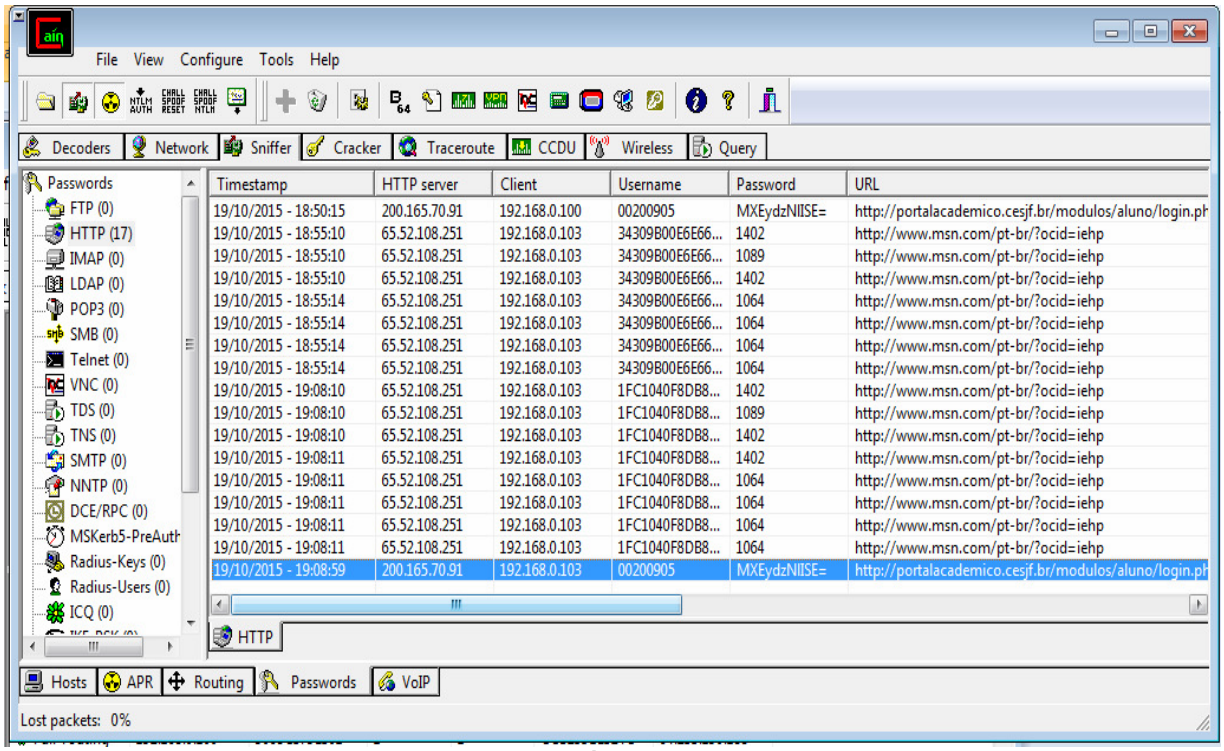

Figura 13. Trafego HTTP capturado da vítima com o Cain&Abel. Fonte: Autor.

6 Resultados Obtidos

Como critérios de comparação entre as duas ferramentas de ataque MITM, foi adotado três atributos de comparação: tempo, usabilidade e funcionalidade.

6.1 Tempo

Nesse critério de comparação, vai ser avaliado o tempo total de cada uma das duas ferramentas para executar o ataque MITM. Os tipos de ataques MITM que serão comparados nas duas ferramentas são: Envenenamento do cache ARP, Falsificação de DNS e sequestro de sessão.

Como as duas maquinas virtuais possuem as mesmas configurações de hardware, o tempo total para execução dos ataques é diretamente relacionado com a ferramenta analisada.

Tabela 1. Tempo gasto para realizar os ataques MITM.

Tipo de ataque MITM	Kalilinux	Cain&Abel
Envenenamento do cache ARP	3 minutos e 34	1 minuto e 45 segundos

	segundos	
Falsificação de DNS	4 minutos e 28 segundos	3 minutos e 05 segundos
sequestro de sessão	6 minutos e 40 segundos	5 minutos e 18 segundos

Fonte: Autor

Após obter o tempo gasto de cada ataque, foi tirada a média de tempo de cada ferramenta e o resultado obtido pode ser visto na tabela 2.

Tabela 2. Média de tempo obtida após os ataques com cada ferramenta.

Kalilinux	Cain&Abel
Média 4 minutos e 06 segundos	Média 3 minutos 23 segundos

Fonte: Autor

No critério de comparação tempo, a ferramenta Cain&Abel apresentou um resultado mais satisfatório demonstrando ser mais rápida para se executar os tipos de ataque MITM.

6.2 Usabilidade

Segundo Pagani (2011) Usabilidade aborda a forma como o usuário se comunica com a máquina e como a tecnologia responde a interação do usuário, considerando algumas habilidades como: facilidade de aprendizagem, maximizar a satisfação do usuário, fácil de memorizar e Interface amigável.

Partindo desse critério que o Cain&abel por apresentar uma interface gráfica mais amigável, facilidade na aprendizagem e fácil interação de um usuário comum com a ferramenta a torna melhor que o Kali Linux que exige um certo grau de conhecimento do usuário.

6.3 Funcionalidade

Nesse critério de comparação vai ser analisados quais tipos de ataque MITM cada ferramenta pode executar. Os ataques que cada ferramenta pode executar pode ser visto na tabela 3.

Tabela 3. Tipos de ataque MITM que cada ferramenta pode realizar.

Tipo de ataque	Cain&Abel	Kali linux
Envenenamento do ARP cache	X	X
DNS spoofing (falsificação de DNS)	X	X

Session Hijacking (sequestro de sessão)	X	X
SSL Hijacking		X

Como resultado dessa comparação, foi observado que o Kali Linux é capaz de realizar os quatro principais tipos de ataque MITM, e o Cain&abel só não é capaz executar o sequestro de SSL.

7 Conclusão

O artigo foi desenvolvido para apresentar a técnica de ataque man in the middle em redes locais, demonstrar o ataque com duas ferramentas distintas além de como se proteger das principais técnicas de ataque MITM existentes.

Foi visto que uma simples vulnerabilidade no protocolo ARP é possível realizar as principais técnicas de ataque MITM: Envenenamento do ARP cache, DNS Spoofing, Roubo de Sessão e Roubo de SSL.

O ataque MITM é muito efetivo tanto pela sua passividade quanto pela sua atividade. Sua passividade é um ponto forte pois a vítima não sabe que está sendo atacada, já que ele está em uma rede fechada, com isso ela utilizará normalmente como se nada tivesse acontecendo, já que sistemas de segurança como antivírus e firewalls não detectam esse tipo de ataque.

Algumas ações podem ser tomadas para evitar esse tipo de ataque, como os principais modos de ataque MITM, utilizam o envenenamento do ARP para conseguir capturar o trafego da rede é aconselhável que adicione os endereços de forma estática. Esses endereços são inseridos na tabela do cache ARP não dependendo mais do ARP *request* e ARP *response*. Para prover mais segurança no servidor de DNS pode-se utilizar um par de chaves público/privada, assim todas as informações trocadas serão autenticadas com a chave privada e assim o receptor verifica a autenticidade garantindo a integridade das informações. O acesso a sites é uma forma em que o atacante pode roubar informações da vítima, abusando da falta de conhecimento da vítima, o atacante cria páginas Web falsas, fazendo com que a ela insira suas informações sigilosas achando que está no site correto, o ataque de SSL hijacking por meio do protocolo HTTPS é de fácil detecção, pois o ataque redireciona o trafego para HTTP, e é possível ver no navegador o protocolo que está sendo utilizado. Sempre que precisar acessar algum site seguro como banco ou *e-comemerce* é aconselhável não estar conectado a uma rede em que não se sabe a procedência.

Ao comparar as duas ferramentas de ataque foi concluído que o Cain&Abel é mais indicado para realizar os diversos tipos de ataque MITM, pois além de rodar no sistema operacional Windows a instalação é muito simples, sua interface gráfica é de fácil entendimento tornando a interação com usuário mais fácil. Para realizar o ataque com o Kali Linux o usuário tem que ter um mínimo de conhecimento de sistemas Linux já que algumas ferramentas de ataque não vêm instaladas com o sistema, sendo necessário fazer o download e instalar os pacotes no terminal, via linha de comando. De acordo com os critérios de comparação escolhidos o Cain&abel teve um resultado significativo e é o mais indicado para esse tipo de ataque.

Para trabalhos futuros, poderá ser desenvolvido ferramentas e scripts para plataforma Windows e Linux que gerencie as atualizações da tabela ARP e os

servidores DNS fazendo que, caso ocorra uma atualização na tabela ARP ou alteração no DNS seja enviado uma mensagem do sistema para o Administrador informando que está sendo realizado o ataque Man in the middle na rede.

Referências

AUGUSTO, Eugênio. Segurança: Como funciona o protocolo SSL/TLS.Disponível em <https://www.ecommercebrasil.com.br/artigos/seguranca-como-funciona-o-protocolo-ssltls/> .2014. Acessado em 18 de Novembro de 2015.

CAIN & ABEL. Disponível em: <http://www.oxid.it/cain.html>. Acessado em 21 de agosto de 2015.

CUNHA, André, et al. Man In The Middle. Segurança de Sistemas e Redes. 2006.

ETTERCAP. Disponível em: <http://Ettercap.github.com/Ettercap/>. Acessado em:

12 de Setembro de 2015.

KALILINUX. Disponível em:< https://www.kali.org/about-us//>. Acessado em: 12 de Setembro de 2015.

ORACLE VirtualBox. Disponível em: <https://www.virtualbox.org/>. Acessado em 21 de agosto de 2015.

PAGANI, Talita. O que é usabilidade?. Disponível em:< http://tableless.com.br/o-que-e-usabilidade/ > 2011.

SANDERS, Chris.Unterstanding Man-In-The-Middle Attacks. Disponível em: <http://www.windowsecurity.com/articles/Understanding-*Man-In-The-Middle*-Attacks-ARP-Part1.html>. 2010.

SOUZA, André Luis Wagner de. Introdução a Redes de Computadores. Disponível em: <http://www.m8.com.br/andre/> 2010.

SILVA, Cadu.Servidor DNS: Veja como escolher o melhor para acelerar sua navegação.Disponivel em: <http://canaltech.com.br/dica/internet/veja-como-escolher-o-melhor-servidor-dns-para-acelerar-sua-navegacao/>.2014.

SSLSTRIP. Disponível em: < http://www.thoughtcrime.org/software/sslstrip/ >. Acessado em: 12 de Setembro de2015.

SZYMANSKI,Thiago.Os 4 ataques hackers mais comuns na web. Disponivel em: <http://www.tecmundo.com.br/ataque-hacker/19600-os-4-ataques-hackers-mais-comuns-da-web.htm>. Acessado em 13 de setembro de 2015.

VIEIRA, Luiz.Cain & Abel –Segurança e monitoramento de tráfego. Disponivel em:

<http://imasters.com.br/artigo/10363/seguranca/cain-e-abel-seguranca-e-monitoramento-de-trafego/ > . Acessado em 12 de Agosto de 2015.