SICIT
Semana de Iniciação Científica e Tecnológica
25 a 29 de setembro de 2017
Engenharias e Computação
Universidade de Itaúna

Técnica MITM para análise de segurança em redes públicas

Isadora de Oliveira[1]

Dalmy Freitas de Carvalho Júnior[2]

Resumo: Sabe-se da importância de uma rede de comunicação segura, na qual as pessoas tenham privacidade em seus dados. O objetivo deste trabalho é usar um método de ataque, analisar o nível de segurança e conscientizar as pessoas o quão vulnerável seus dados podem ficar ao conectar-se em uma rede pública. Visando verificar isto, realizou-se o MITM (*man in the middle)* uma técnica na qual o invasor conecta-se a uma rede de computadores e passa a interceptar todos os tipos de dados sem que os demais usuários saibam. Foi usado o SSLSTRIP para interceptar o tráfego dos alvos usando MITM, assim o invasor engana o alvo passando-se pelo servidor e engana o servidor, passando-se pelo cliente. A partir do momento que os dados foram interceptados, utilizou-se o Ettercap para capturá-los. Os experimentos mostram que, em um rede com 6 pessoas conectadas foram capturados mais de 546 KB de informações em 15 minutos. Os resultados computados mostram como é grande a quantidade de dados em um curto período de tempo. As pessoas já tendo conhecimento, de que é possível capturar os seus dados, o próximo passo é informar como proceder para protegê-los de forma que todos possam ter uma conexão segura.

Palavras-chave: MITM, segurança, redes públicas, vulnerabilidade, captura de dados.

1. Ciência da Computação, Universidade de Itaúna, contato@isadoraoliveira.com.
2. Doutor em Engenharia Elétrica, Universidade de Itaúna, dalmyjr@gmail.com.

1. Introdução

Os testes de invasão consistem em procedimentos e processos usados pelos pentesters que estão empenhados em melhorar a segurança do seu sistema ou da rede de computadores. Normalmente os usuários da rede-alvo não sabem quando um teste está sendo conduzido.

Uma das técnicas de ataque na rede de computadores mais prevalentes usados contra pessoas e grandes organizações é a técnica homem-em-meio (MITM), funciona quando o invasor consegue acessar a rede e passa a estabelecer uma conexão com a vítima.

Nesse caso a vítima acredita que está tendo comunicação direta com o seu servidor da rede (*gateway*) como é feito frequentemente, quando na realidade todo o tráfego da rede flui pelo host do invasor, onde está sendo executado o teste.

O resultado final é que o host do invasor não apenas pode interceptar dados confidenciais, mas também pode injetar e manipular um fluxo de dados para poder ter mais controle sobre a vítima.

O objetivo é usar a técnica apenas para interceptar dados e alertar as pessoas sobre os tipos de riscos que eles podem correr quando se estão conectados em uma rede de computadores, principalmente se for uma rede pública onde não sabemos quem são os hosts que fazem parte da rede e a intenção dos mesmos.

Para realizar o ataque foi usado o Kali Linux versão 2.0. Ele é um sistema operacional Linux baseado no debian e contém mais de 300 ferramentas nativas para testes de invasão e é muito usado por hackers, pentesters, analistas e profissionais de segurança.

2. Metodologia

Primeiramente vamos compreender como funciona a comunicação ARP e o envenenamento do cache desta tabela conhecido como *ARP Poison Routing,* permite que o invasor intercepte todo o tráfego da rede onde está a vítima.

O protocolo ARP (*Address Resolution Protocol)* foi projetado por necessidade para facilitar a tradução de endereços entre a segunda e terceira camadas do modelo OSI. A segunda camada ou a camada de ligação de dados, usa endereços físicos MAC para que os dispositivos de hardware possam se comunicar diretamente em uma pequena escala. A terceira camada ou camada de rede, usa endereços lógicos IP para criar grandes redes escaláveis que podem se comunicar em todo o mundo. A partir do momento que a tabela ARP tem o endereço MAC associado ao IP do host, um host na rede pode facilmente encontrar o outro e passar a estabelecer uma comunicação. Na figura abaixo é mostrado o fluxo de informações de uma comunicação normal na rede. O computador requisita uma informação, essa solicitação chega ao roteador (*gateway*) e em seguida o roteador responde a solicitação enviando a informação para o computador.

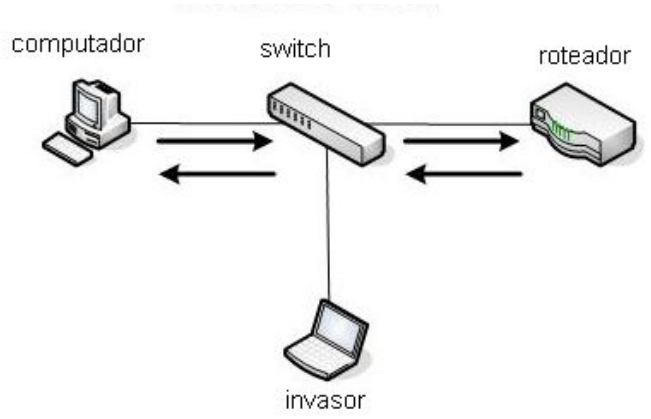

FIGURA 1 - Comunicação normal em uma rede de computadores.

Já na figura abaixo mostra o fluxo de informações depois do envenenamento do cache ARP, tirando proveito da insegurança do protocolo ARP. Desta forma qualquer host na rede pode enviar um pacote de resposta ARP para outro host e forçar esse host a atualizar o cache ARP com o novo valor. Assim da próxima vez que o host da vítima for se comunicar na rede, as informações passarão primeiro pelo host do invasor que estará interceptando os dados.

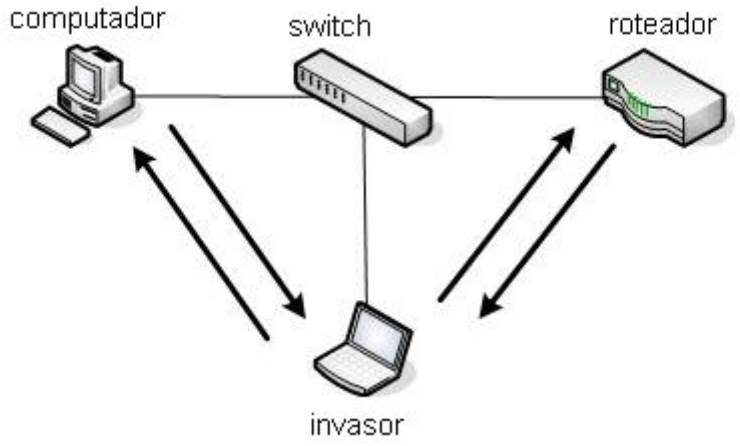

FIGURA 2 - Interceptando a comunicação com o envenenamento da tabela ARP.

Agora que já compreendemos como funciona o processo de interceptação de dados, vamos mostrar como utilizar as ferramentas para fazer a captura.

Para realizar o ataque foi utilizado um roteador configurado sem senha, para que qualquer tipo de pessoa pudesse se conectar à rede pública. O sistema operacional usado foi Kali Linux versão 2.0, que contém as ferramentas que serão utilizadas para os testes.

Primeiro é necessário habilitar o modo promíscuo, para que o computador invasor passe a ser o servidor da rede (gateway). Após habilitar o encaminhamento de pacotes, é criado uma regra para que todo o tráfego com destino a porta 80 seja redirecionada para uma nova escuta e depois é usado a ferramenta SSLStrip para que faça a escuta nesta nova porta.

```
root@kali:~# echo 1 proc/sys/net/ipv4/ip_forward
1 proc/sys/net/ipv4/ip_forward
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIR
ECT --to-port 10000
root@kali:~# sslstrip -l 10000

sslstrip 0.9 by Moxie Marlinspike running...
```

FIGURA 3 - Ativando modo promíscuo e iniciando a ferramenta SSLStrip.

Em seguida é utilizado o Ettercap uma ferramenta utilizada para capturar todas as informações na rede em texto puro. O Ettercap vai interceptar o tráfego da rede pública, primeiramente é preciso envenenar o cache do ARP como mostra a figura abaixo:

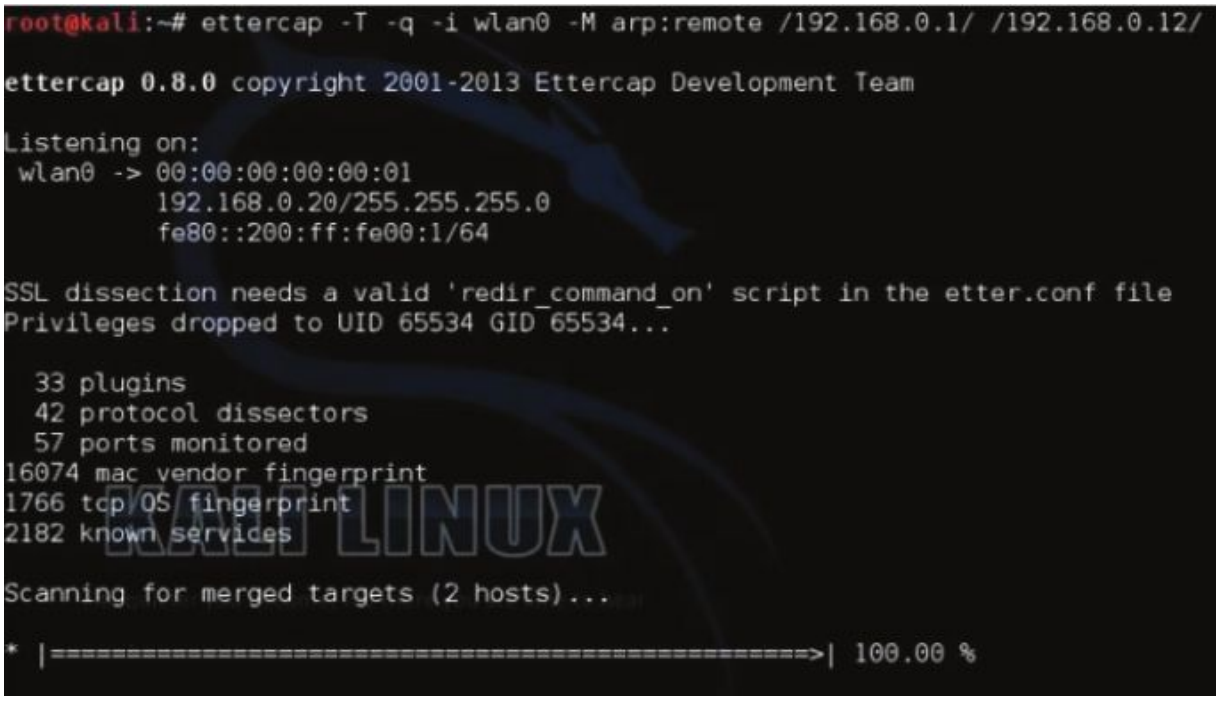

FIGURA 4 - Usando Ettercap para envenenar o cache do ARP.

Agora já é possível realizar a coleta de todos os dados.

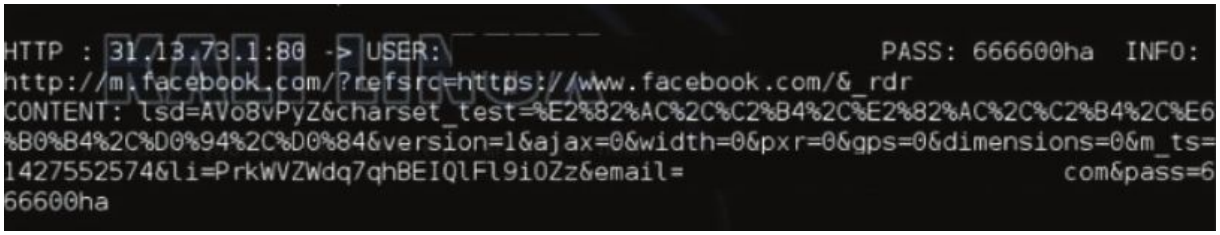

FIGURA 5 - Capturando os dados com a ferramenta Ettercap.

3. Resultados

Com base nos resultados computados, foi elaborado um gráfico que apresenta a quantidade de pessoas que estavam conectadas em um rede pública e a quantidade de dados em KB que foram coletados em um tempo de 15 minutos.

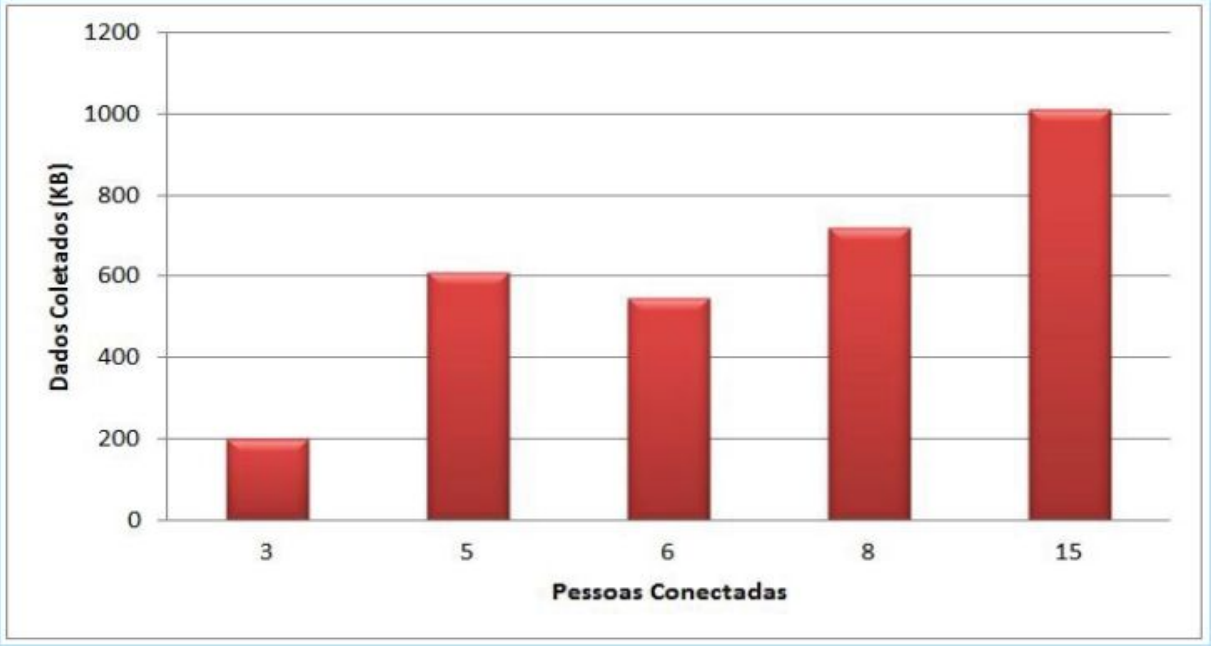

TABELA 1 - Gráfico resultante do número de pessoas conectadas e dados coletados.

4. Discussão

Quando o assunto é utilizar a internet, nem sempre as pessoas se preocupam com segurança. Esse trabalho levanta o questionamento e mostra para as pessoas o quão vulneráveis elas podem estar ao se conectar em uma rede pública. Mesmo que a pessoa pense que só está conectado para enviar/receber uma simples mensagem, a quantidade de informação que precisa ser enviada e validada é grande. Além disso, ao estabelecer uma conexão com um servidor o host da pessoa precisa estar aberto a comunicação e temos um grande risco de um outro host na rede poder agir de forma maliciosa e capturar informações para usufruir da forma que quiser. Atualmente existem casos em que invasores criptografam os dados roubados e pedem dinheiro para devolvê-los. Se as pessoas tiverem mais consciência sobre os riscos de se conectarem a um rede pública, elas estarão mais preparadas para se prevenirem e protegerem de uma ameaça futura.

5. Conclusão

Os resultados computados mostram como é grande a quantidade de dados que são acessados em um curto período de tempo, e como as pessoas que tem a necessidade de se manterem *on-line* acabam conectando em um rede pública sem saber que seus dados podem estar sendo capturados. As pessoas já tendo o conhecimento, de que é possível capturar os seus dados em uma rede, o próximo passo é informar como proceder para poder estar protegendo esses dados de forma que todos possam ter uma conexão segura na rede.

Referências

MUNIZ, J.; LAKHANI, A.; *Web Penetration Testing with Kali Linux*. 1a Edição Livery Lugar 35 Brimingham, Reino Unido. Packt Publishing Ltd, 2013.

ENGEBRETSON, P.; *Introdução ao Hacking e aos Testes de Invasão: Facilitando o hacking ético e os testes de invasão*. 1a Edição São Paulo: Novatec Editora Ltda, 2014.

BROAD, J.; BINDNER, A.; *Hacking com Kali Linux: Técnicas práticas para teste de invasão.* 1a Edição São Paulo: Novatec Editora Ltda, 2014.

TANENBAUM, A.S.; WETHERALL, D.; Rede de Computadores. 5a Edição São Paulo: Pearson Prentice Hall, 2011.