Ataques (básicos) a uma rede local

João Fiuza de Alencastro 15/0131933

***Abstract*—Este relatório não tem um ataque principal em questão, aqui é onde comecamos a falar sobre ataques simples em geral, ataques conhecidos, como, por exemplo, *Gathering, DoS, Flood,* entre outros.**

***Index Terms*—Ataques, redes, LAN, ARP, DDoS, Gathering, Flood, BruteForce, HTTP, IP, NMap, Python3.**

I. Introduction

OS ataques mencionados a cima são somente o primeiro passo para ataques maiores. Por esse motivo, ataques simples podem acabar se tornando extremamente perigosos.

Uma das principais solucões para ataques externos é a implementação de uma IDS (Invasion Detection System), uma aplicação, normalmente local, que monitora a rede ou os sistemas à procura de invasores ou softwares maliciosos.

Abaixo são apresentados alguns dos principais ataques que já foram muito bem sucedidos no passado e continuam sendo efetivos em sistemas mais vulneráveis.

A. NMap

Tema já abordado no relatório NMap[1], porém de extrema importância para o processo de *'information Gathering'*. Também conhecido como Port Scanner, o NMap pode almejar de sistemas a redes inteiras e é já é utilizado por diversos frameworks conhecidos.

B. Flood

A proposta do *Flood*, como o nome já indica, é encher/"entupir" algo ou alguém com algo. Imaginemos uma analogia básica para fins didáticos, um atendente de bar, por exemplo, está trabalhando em uma noite especial e 100 pessoas tentam fazer pedidos simultaneamente para ele, sem dúvida alguma, ele não conseguirá lidar com toda essa demanda e talvez até desista da tarefa. Pois, esse é o princípio do *Flood*, enviar pedidos em larga escala em um curto período de tempo.

C. DoS (Denial of Service)

O ataque de negação de serviço utiliza-se do princípio do *Flood*, entupindo os recursos de um serviço com requisições, indisponibilizando aos usuários daquele serviço acesso e comunicação.

No experimento realizado, um simples script em python foi o suficiente para simular um pequeno ataque DoS ao serviço criado pelo colega próximo do laboratório, conectado à mesma LAN. O serviço era uma pequena aplicação HTTP na porta 8000 e o script cria 300 conexões HTTP.

Na imagem abaixo, pode ser visto que o IP da máquina localhost é 172.16.5.93 e foi feito um ataque DoS no endereço IP 172.16.5.91. Pode-se confirmar que o ataque foi bem sucedido, pois a resposta HTTP é um código 200, indicando sucesso. O número na linha logo abaixo do código 200 há um número que se repete, 715, este número representa o número de bytes no diretório no qual a aplicação está diretamente associado.

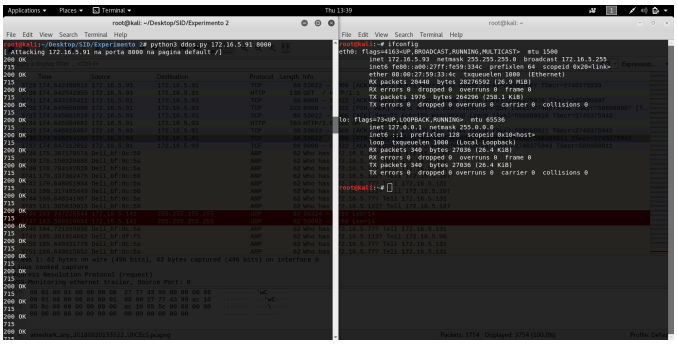

Fig. 1. Ataque DoS ao colega em mesma LAN

Na figura seguinte, podemos ver um mesmo ataque acontecendo, porém agora no próprio localhost, ou seja, em um serviço criado na mesma máquina atacante. Nessa imagem, é possível ver as requisições do lado do servidor, onde há informações do endereço IP do cliente, timestamp da requisição e o tipo da requisição, nesse caso o log do serviço é esse, porém pode ser muito diferente dependendo da aplicação. Perceba também, que o intervalo entre uma requisição e outra é tão pequena que todas na tela do terminal apresentam mesmo timestamp.

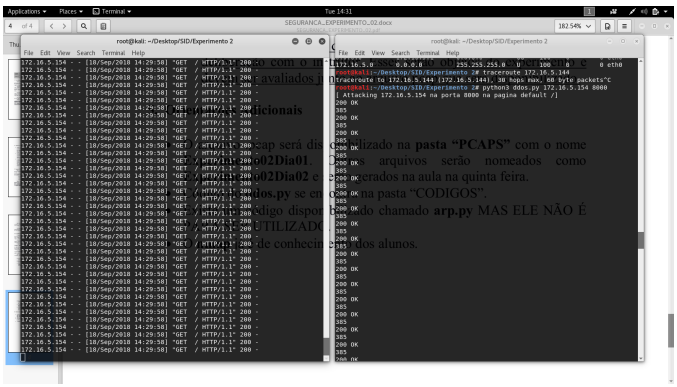

Fig. 2. Ataque DoS ao próprio endereço local

Ao analisar o tráfego da rede, fica claro como um ataque de negação de serviço acaba sendo muito custoso para conexões TCP, já que para requisição HTTP, até mesmo um simples 'GET', requer um 'three-way-handshake' da conexão segura fornecida pelo TCP. Na figura abaixo podemos ver um pequeno pedaço da análise do tráfego em modo promíscuo no WireShark no exato momento do ataque.

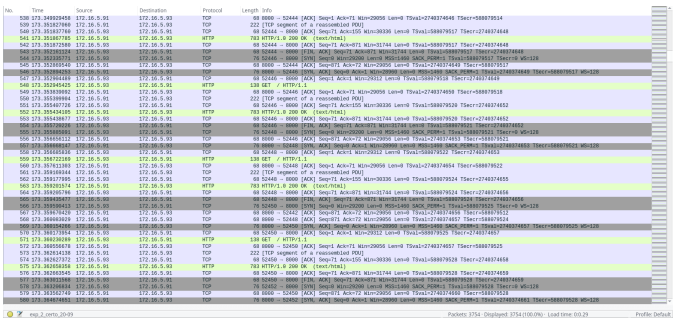

Fig. 3. Pacotes ataque DoS

O DDoS continua sendo um ataque de negação de serviço da mesma forma, porém mais ”inteligente”, já que ele distribui a origem do ataque, fazendo com que várias máquinas diferentes façam algumas poucas requisições, totalizando em um ataque generalizado e bem organizado. A maior vantagem do ataque ser distribuído dessa forma, é que o atacante gera uma dificuldade de localização grande, já que as requisições não são de um único endereço IP. Além disso, um ataque com várias máquinas dispõem de muito mais recursos do que somente uma máquina gerando requisições.

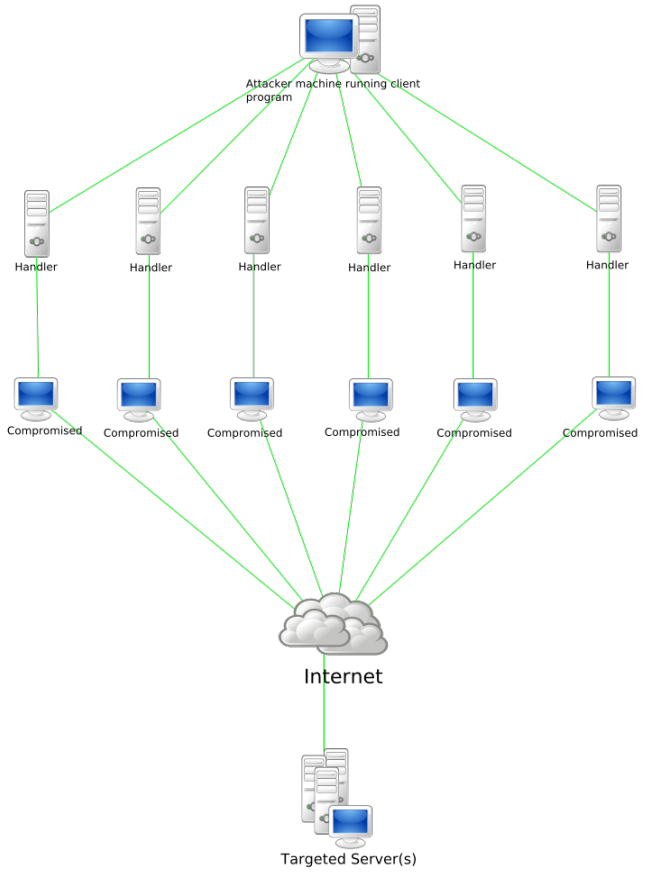

Fig. 4. Topologia clássica de um DDoS distribuído

II. Conclusion

Excluindo as descobertas de vulnerabilidades, ataques de *Flood* são, usualmente, custosos para o atacante também. Eles comprometem as conexões de um certo serviço, porém seus recursos ficam inutilizáveis. Por este motivo, hoje, atacantes utilizam-se de máquina alheias espalhadas pelo globo para realizar ataques distribuídos. E esse processo acontece, na maioria das vezes, sem o consentimento do dono da máquina, às vezes por ele baixar uma aplicação de fontes não confiáveis.

Ataques de negação de serviço podem ser prevenidos por utilização de IDS (Invasion Detection System) em sua rede ou sistema. É necessário que haja algum processo específico para a detecção de intrusos ou atividades suspeitas, o caso do DoS. Ele pode ser o responsável por ”perceber” múltiplas requisições, enviadas em um tempo realizável somente por máquinas, e deve ser capaz de ”negar” o serviço demandado, e assim surge o nome do ataque.

References

[1] https://en.wikipedia.org/wiki/Intrusion-detection-system
[2] https://pt.wikipedia.org/wiki/Ataque-de-negacao-de-servico