Emulação via NS-3 para detecção de um ataque à rede

André de Medeiros Araújo
Departamento de Engenharia Elétrica
Engenharia de Redes de Comunicação
Universidade de Brasília
Matrícula: 09/0003187
andredemedeirosaraujo@gmail.com

Lucas Coelho de Almeida
Departamento de Engenharia Elétrica
Engenharia de Redes de Comunicação
Universidade de Brasília
Matrícula: 14/0045279
luccoelhoo@gmail.com

I. Resumo

Este trabalho tem por objetivo de aprofundar os conhecimentos sobre o NS-3, realizando uma simulação que se comunique com o mundo real. A rede simulada será utilizada como "isca" para potenciais atacantes que, ao tentar atacar a rede real, encontrarão endereços desprotegidos (usando protocolo ARP) e rodarão aplicações de scan (NMAP), para então identificar as portas das aplicações TCP simuladas e tentar realizar ataques de DDoS. Idealmente, ao se detectar esse ataque, a rede emulada mandaria uma mensagem avisando sobre o endereço do atacante, servindo, por fim, como uma verdadeira rede honeypot. Essa detecção se daria através da análise constante de parâmetros de rede, como throughput e delay das interações da rede emulada com os atacantes. Todavia, percebeu-se que a implementação dessa tarefa fugiria fugiria bastante do escopo deste estudo, visto que não é tão simples programar o NS-3 para reagir em tempo real a variáveis que geralmente só são medidas ao fim da simulação, o que inviabiliza o projeto de automação de detecção de ataques. Contudo, por fim, descobriu-se que, com o suporte já existente hoje do simulador, é possível criar redes honeypot emuladas que se mostrem verdadeiros desafios para os atacantes, e isso sem que esses consigam sequer atacar ou tirar vantagem de um único nó, pois não existe informação útil nessa rede. Nesse caso, apesar de não ser possível realizar a automação como desejado, é possível criar labirintos, os quais podem ter vantagens enormes em casos de ataques.

II. Introdução

O NS-3 é um simulador de rede de eventos discretos para sistemas da internet, voltado principalmente para pesquisa e uso educacional. Esse simulador se trata de um software livre, disponível publicamente para pesquisa, desenvolvimento e uso. O NS-3 foi projetado para integração em ambientes de teste e de máquina virtual. Dessa forma é possível fazer uma emulação com esse software, ou seja, integrar o mundo virtual do NS-3 com o mundo real. Para esse tipo de emulação, o NS-3 disponibiliza dois tipos de dispositivos de rede, o primeiro sendo o "*Emu NetDevice*", que permite que o NS-3 envie dados para uma rede "real", e o segundo dispositivo é o "*Tap NetDevice*", que permite que um host real participe de uma simulação como se fosse um dos nós simulados. Uma simulação pode ser feita de várias formas combinando estes dispositivos. O *NetDevice* é a interface que define a API que as camadas IP e ARP precisam acessar para gerenciar uma instância de cada dispositivo de rede. Especificamente, esta classe encapsula o formato específico dos endereços MAC usados por um dispositivo.

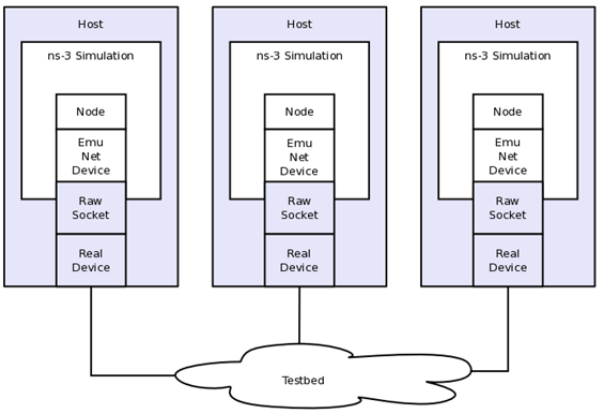

Fig. 1. Exemplo de uma emulação com o NS-3.

Usar o método de emulação de rede fornece um ambiente controlável e permite a avaliação de comportamentos de placas adaptadoras e protocolos reais. Na emulação, os hosts reais que executam protocolos e aplicações do mundo real são capazes de interagir através de um ambiente que simule condições de rede especificadas. Dessa forma o NS-3 pode ser usado como uma ferramenta de análise de um ataque de rede, como por exemplo um DDoS, ou outros scans que fazem parte das fases preliminares. Um ataque à rede pode ser definido como qualquer método, processo ou meio usado para tentar comprometer a segurança da rede. Os indivíduos que realizam ataques de rede são comumente chamados de invasores de rede, hackers ou crackers. Esses ataques servem para roubar dados, roubar softwares, usar os dados para ganho financeiro ou espionagem, modificar dados guardados, tornar algum host indisponível, entre outros tipos de crime. O ataque DDoS (Distributed Denial of Service), ou ataque distribuído de negação de serviço, é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Servidores web são os alvos típicos desse ataque, que procuram tornar as páginas hospedadas indisponíveis. Os ataques DDoS sobrecarregam esses servi-

dores web, tornando-os indisponíveis. Esse ataque pode forçar o sistema reinicializar ou consumir todos os recursos da rede, ou então ocupar o canal de comunicação entre os utilizadores e o sistema. Dessa forma, utilizando o NS-3 para a simulação de uma rede que emula troca de dados com o mundo real, seria possível identificar um ataque desses olhando apenas o throughput e delay da rede.

III. Experimentos realizados

Para este trabalho foi montada uma rede com 3 roteadores, onde o primeiro se comunica via WiFi com o segundo, e o segundo é ligado ponto a ponto com o terceiro. O host emulado está conectado diretamente ao primeiro roteador, que se trata do TapBridge, fazendo a conexão do real com a simulação. Esse roteador consegue se comunicar com os outros nós da simulação via rede interna do NS-3. O terceiro roteador está ligado a uma LAN via CSMA, onde os usuários podem se comunicar entre si e também com o host emulado.

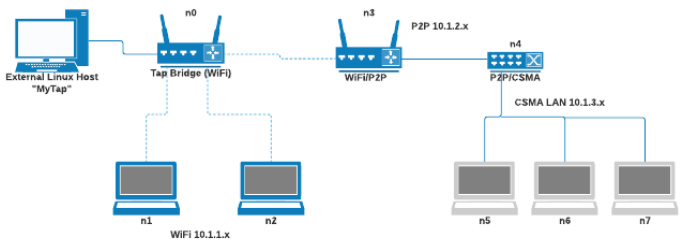

Fig. 2. Topologia utilizada para emular um host Linux via NS-3.

O módulo do NS-3 utilizado para esse trabalho foi o *TapBridge*, que nos permitiu integrar um host do mundo real nas simulações realizadas. Essa interface tem esse nome pois conecta as entradas e saídas de um dispositivo de rede do NS-3 às entradas e saídas de um dispositivo de rede do Linux (ou seja, através de softwares, cria-se um dispositivo de rede que atua tal qual um do mundo físico, mas é capaz de repassar dados para um mundo virtualizado, é exatamente isso que os tão conhecidos "TUN/TAP devices" do Linux fazem). Existem três modos operacionais básicos deste módulo disponíveis para os usuários, que são *ConfigureLocal*, *UseLocal* e *UseBridge*. No modo *ConfigureLocal*, o *TapBridge* tem a responsabilidade de criar e configurar os dispositivos *TAP*. Nos modos *UseBridge* ou *UseLocal*, o usuário fornece uma configuração e o *TapBridge* se adapta a essa configuração. Esses dois últimos casos, no entanto, ainda não estão completamente bem documentados, e suas implementações são limitadas, além de terem como requisito configurações de adaptadores que não refletem o funcionamento normal das interfaces de redes dos dias atuais. Sabendo disso, o conceito a ser apresentado foi baseado no modo *ConfigureLocal*.

IV. Resultados

O objetivo inicial do experimento era criar uma aplicação que ficasse, continuamente, emulando uma rede no NS-3 que servisse de alvo fácil para atacantes. Quando estes realizassem quaisquer tentativas de ataque/intrusão a essa rede, a simulação acionaria scripts externos e avisaria sobre a tentativa. Entretanto, descobriu-se que a emulação suportada pelo NS-3 ainda é muito limitada pelas próprias capacidades do NS-3 de processar e responder a aplicações reais. Com o simulador, é possível copiar e simular quaisquer comportamentos possíveis, mas este ainda não tem suporte adequado para incluir programas externos em seus projetos (como um servidor HTTP que realmente recebe requisições e responde com código HTML, por exemplo). Para que isso fosse possível, seria necessário grande esforço em conjunto com IDE's externas e escrita manual do processamento e comportamento de aplicações reais. Portanto, apesar de ser possível fazer redes que podem interagir e serem exploradas com o mundo real usando emulações, ainda não é possível embutir aplicações verdadeiras nas simulações.

Mesmo sabendo que não seria possível atingir o objetivo inicial, os estudos sobre o tema forneceram um outro viés talvez até mais interessante que o anterior: o NS-3 é, provavelmente, a forma mais segura de "enganar" qualquer possível atacante. As redes emuladas podem conter topologias extremamente complexas, e com o devido conhecimento dos programas que exploram os informações de camadas mais baixas (como PING, ARP, NMAP e TraceRoute), além de conhecimento sobre rotas e protocolos de roteamento, um atacante poderia passar horas investigando a rede sem nem ao menos desconfiar de se tratar de uma emulação. Adicionalmente, o fato mais curioso é que, devido o NS-3 ter sido projetado para análise de desempenho de redes, especificamente, e não conter traços de aplicações reais que respondem a requisições, um atacante jamais consegue sequer realizar um ataque bem sucedido a um nó da rede emulada, pelo simples fato de que não existe serviço a ser derrubado, apenas os recursos que o NS-3 estiver usando para o socket alvo do ataque naquele momento. E mais curioso ainda: as principais ferramentas dos atacantes não são capazes de fornecer nenhuma pista sobre a emulação. Tudo pelo fato de que é possível "pingar" esses nós, escaneá-los, descobrir rotas, etc, mas não é possível interagir a nível de aplicação, que é onde esses softwares têm inteligência para reconhecer padrões. Portanto, num caso mais concreto, um script de ataque DDoS tenta conectar a um desses hosts emulados milhares de vezes, de forma que em algum momento conseguirá consumir todos os recursos daquele sistema, porém, de nada valerá, pois ele ainda estará dentro de um "labirinto".

V. Conclusão

Foi possível concluir que a ferramenta de simulação NS-3 tem muito mais abordagens possíveis de estudo e uso do que simplesmente avaliar capacidades de enlaces e modelos teóricos de fluxos de dados. Na verdade, foi possível contruir uma aplicação real e útil usando o programa.

VI. Imagens dos Procedimentos Experimentais

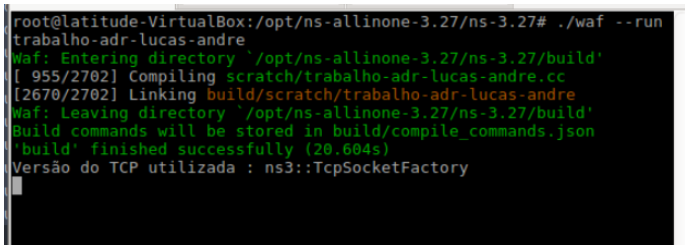

Fig. 3. Script de emulação em execução, após ser compilado.

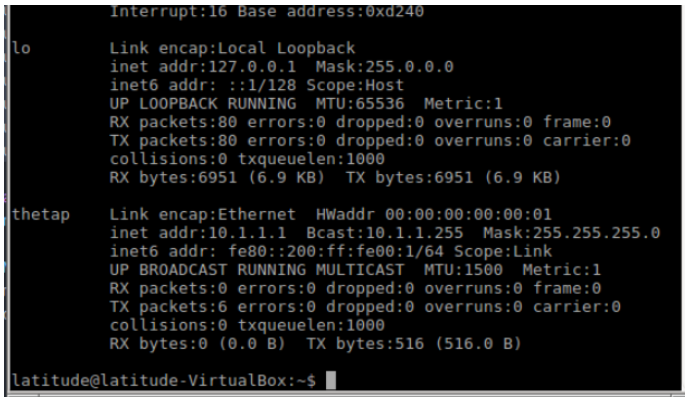

Fig. 4. TapDevice criado pelo programa, após ser compilado.

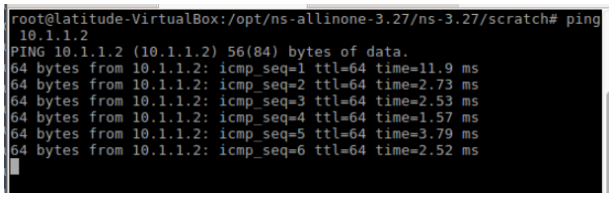

Fig. 5. O host real já é capaz de usar o programa ”Ping” com nós da rede ’10.1.1.0’.

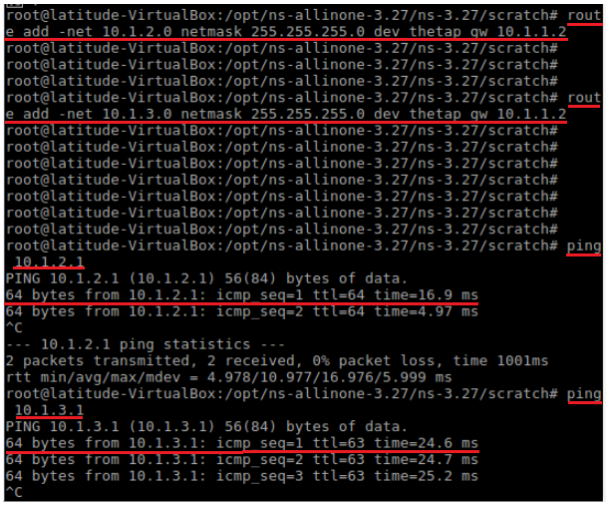

Fig. 6. Após a configuração de duas novas rotas, o host real também é capaz de usar o programa ”Ping” com nós da rede ’10.1.2.0’ e ’10.1.3.0’.

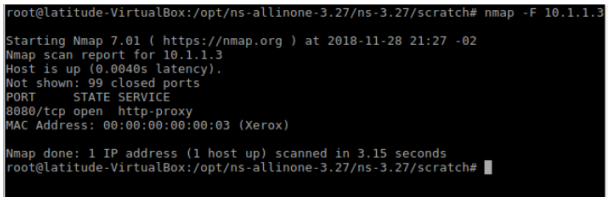

Fig. 7. O programa NMAP consegue perceber que existe uma aplicação TCP no nó 10.1.1.3 utilizando a porta 8080.

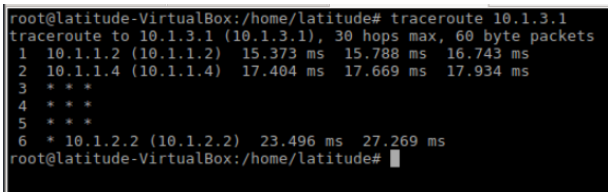

Fig. 8. O programa TraceRoute consegue rastrear a rota para chegar até a rede ’10.1.3.0’.

VII. Referências

1) ”NS3” - Jacy, Cláudia, professor.”
2) ”Tap NetDevice” - https://www.nsnam.org/docs/models/html/
3) ”Emu NetDevice” - https://www.nsnam.org/docs/release/3.11/models/html/emu.h
4) ”Emulation Overview” - https://www.nsnam.org/docs/release/3.11/models/html/emulation-overview.html
5) https://www.nsnam.org/docs/release/3.9/doxygen/group___tap_bridge_model.html
6) https://www.nsnam.org/doxygen/tap-wifi-dumbbell_8cc.html
7) https://www.nsnam.org/doxygen/tap-wifi-dumbbell_8cc_source.html
8) https://www.nsnam.org/doxygen/tap-csma-virtual-machine_8cc_source.html
9) https://www.nsnam.org/doxygen/tap-bridge-helper_8cc_source.html

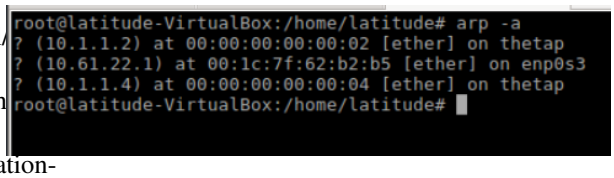

Fig. 9. O programa ARP consegue perceber a presença de outros nós da rede ’10.1.1.0’.

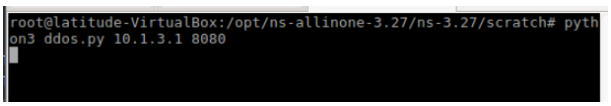

Fig. 10. Um script de ataque DDoS escrito em Python é acionado tendo como alvo o endereço IP 10.1.1.3, que tem a porta 8080 vulnerável.

Fig. 11. O ataque é um sucesso, e não existe nenhum indício de se tratar de uma falsa aplicação.

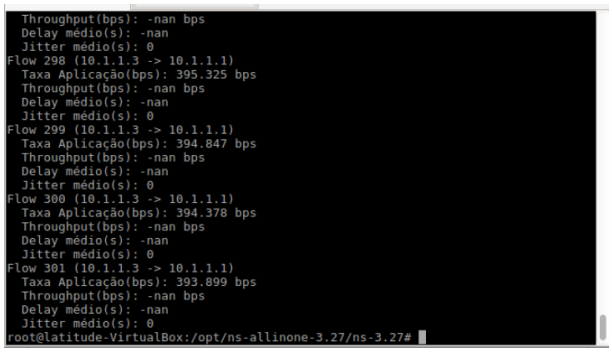

Fig. 12. O FlowMonitor do NS-3 rastreia todas as conexões e fluxos de dados, logo, após um ataque DDoS, os registros da aplicação se tornam completamente inúteis, tamanha o consumo de recursos que um ataque desses causa.

10) https://www.nsnam.org/wiki/HOWTO_make_ns-3_interact_with_the_real_world