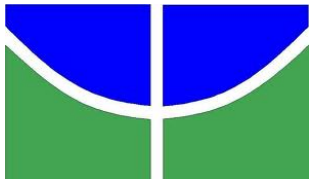


Universidade de Brasília
Engenharia de Redes de Comunicação
Análise de Desempenho de Redes

Emulação via NS-3 para detecção de ataque a rede

André Araújo

Lucas Coelho

OBJETIVOS

Utilizar a ferramenta NS-3 para realizar uma simulação que se comunique com o mundo real a fim de rastrear ataques DoS na rede.

- Emulação NS-3

- Simulador projetado para integração em ambientes de teste e de máquina virtual.

- Possibilidade de comunicação de uma simulação com o mundo real.

- Fornece um ambiente controlado e permite o uso de protocolos e aplicativos reais.

- NS-3 disponibiliza dois tipos de dispositivo de rede para emulação: *Tap NetDevice* e *Emu NetDevice*.

- *NetDevice* é a interface que define a API que as camadas IP e ARP acessar.

- *Emu NetDevice:* Permite que um nó simulado utilize a rede real para enviar e receber pacotes. Abre um soquete e se liga a essa interface

- *Tap NetDevice*: usado para permitir que um host real ou máquinas virtuais interajam com uma simulação.

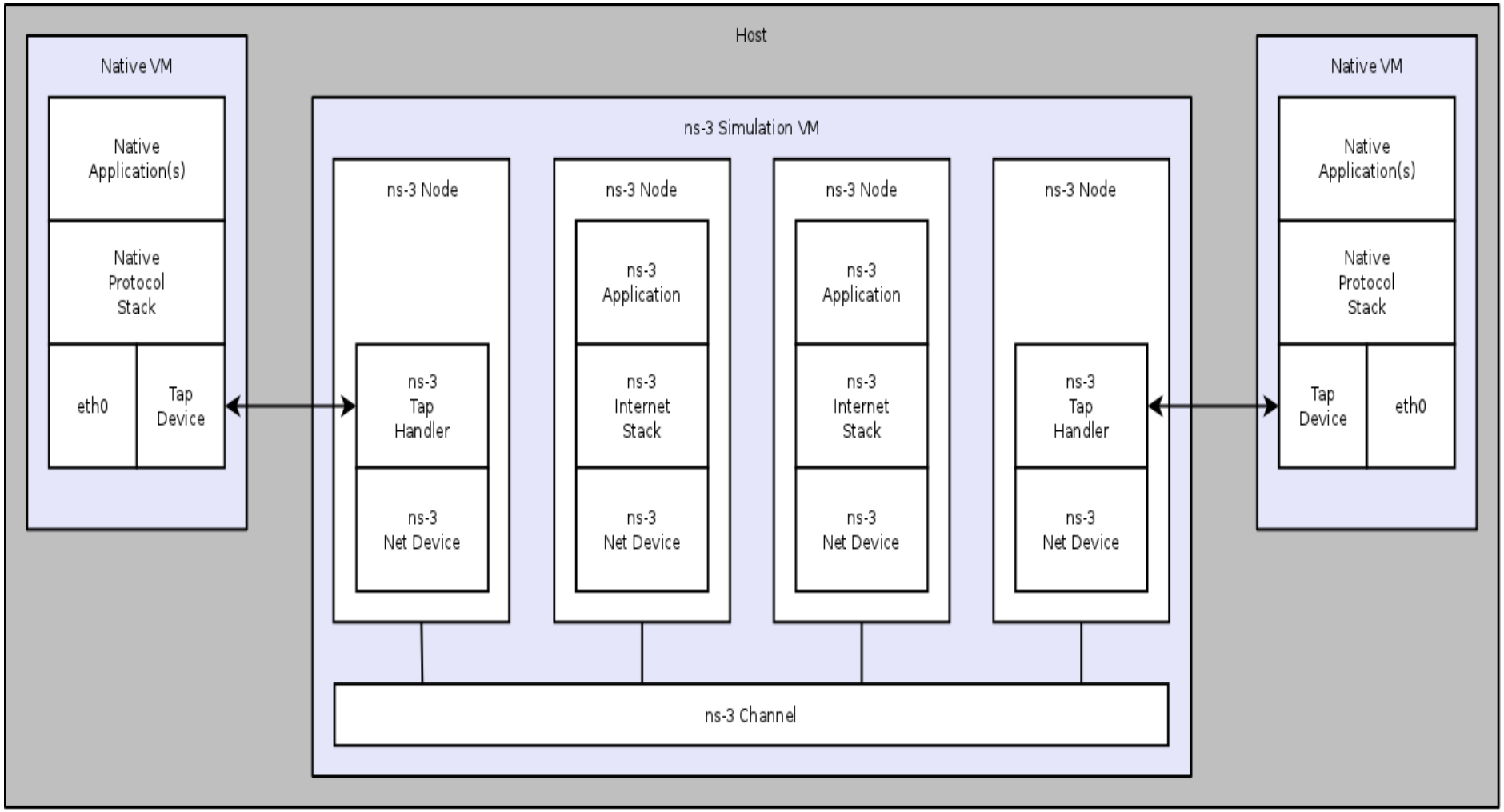
-*TapBridge Model:* Conectar entradas e saídas de um dispositivo de rede do NS-3 em entradas e saídas de um dispositivo de rede Linux.

-3 Modos:

-*Configure Local: TapBridge* cria e configura os dispositivos. (*Default*)

-*UseLocal:* Usuário cria e configura os dispositivos.

-*UseBridge: TapBridge* usa uma configuração já existente estendendo uma lógica de bridge Linux


Host
Native VM
Native Application(s)
Native Protocol Stack
eth0
Tap Device
ns-3 Simulation VM
ns-3 Node
ns-3 Tap Handler
ns-3 Net Device
ns-3 Node
ns-3 Application
ns-3 Internet Stack
ns-3 Net Device
ns-3 Node
ns-3 Application
ns-3 Internet Stack
ns-3 Net Device
ns-3 Node
ns-3 Tap Handler
ns-3 Net Device
ns-3 Channel
Native VM
Native Application(s)
Native Protocol Stack
Tap Device
eth0

- Ataque DoS

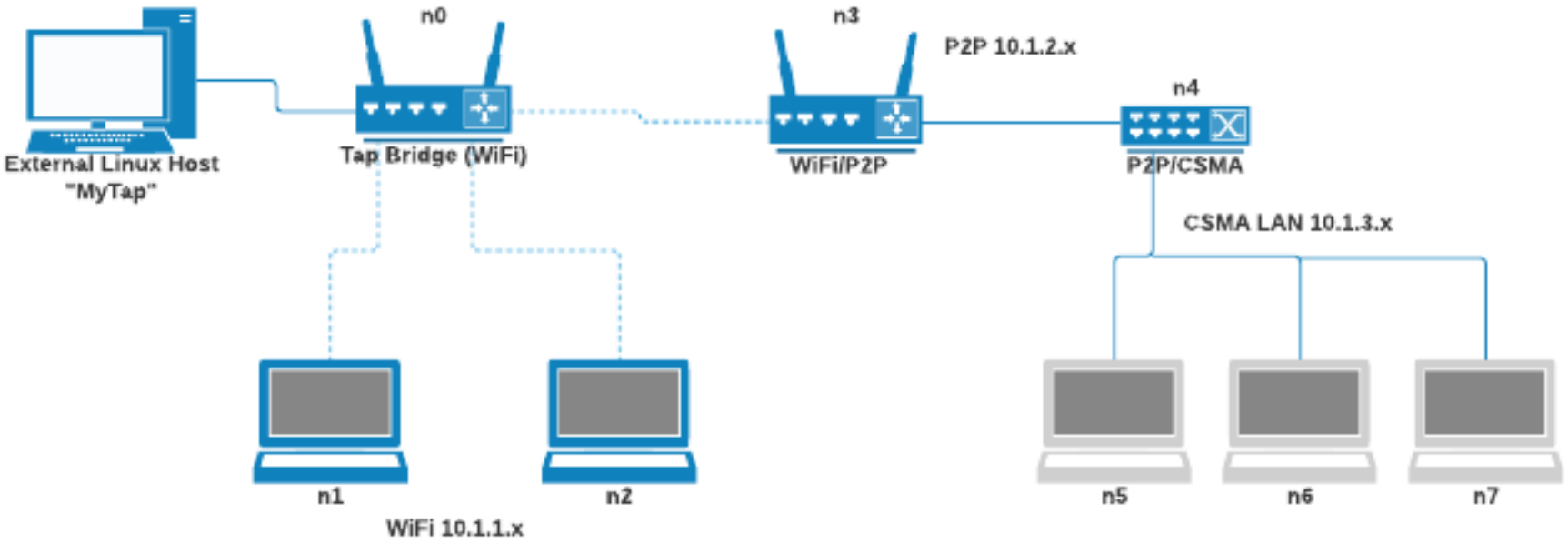
- Ataque à rede: Método, processo ou meio usado para tentar comprometer a segurança e utilização de uma rede.

- DoS = Denial of Service (Negação de Serviço0

- Procura tornar os recursos de um sistema indisponíveis para os usuários (Servidores web).

- Sobrecarregam o sistema forçando a reinicializar, consomem os recursos ou obstrui a comunicação do sistema com o usuário.

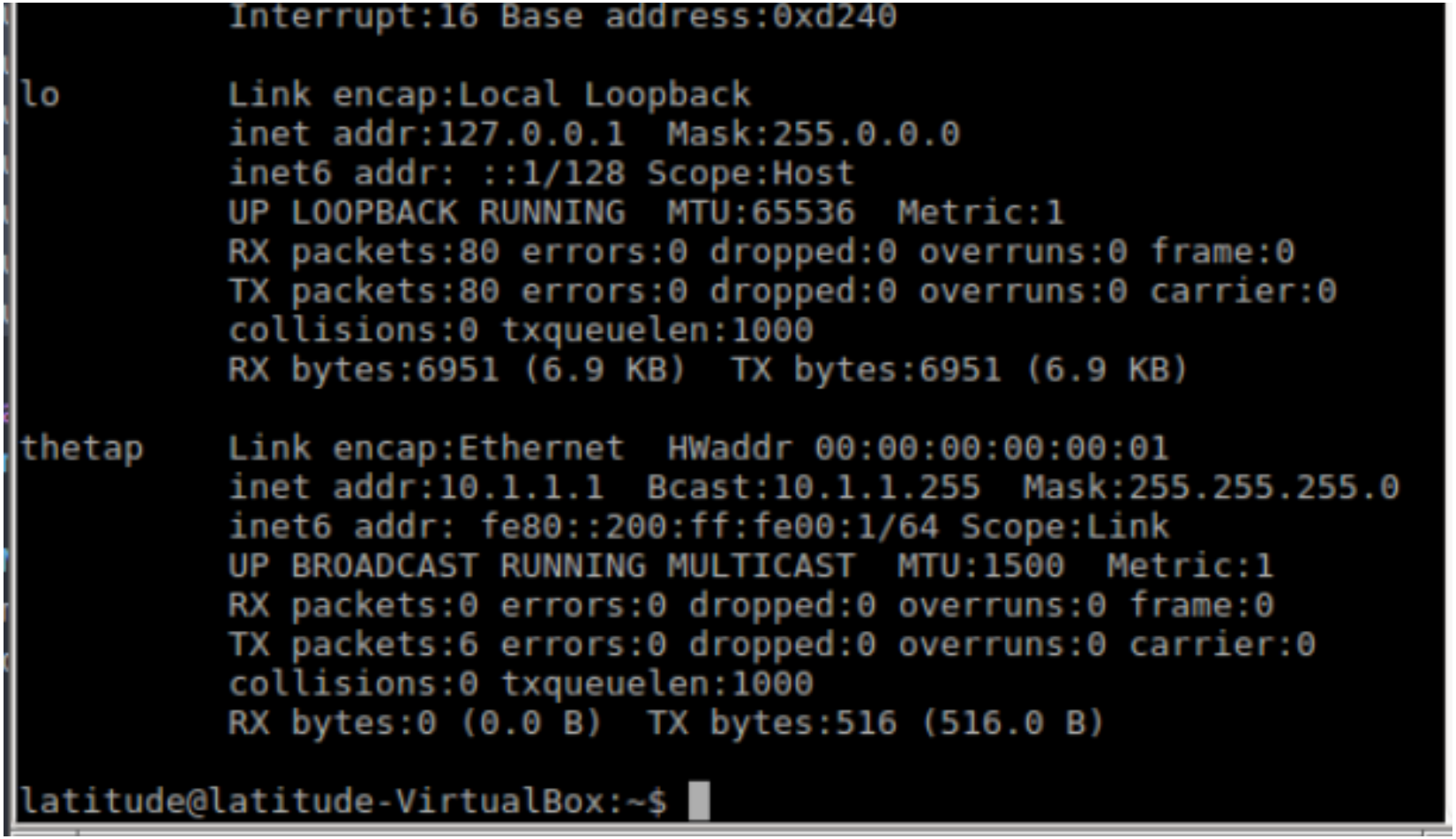
- Topologia


n0
n3
P2P 10.1.2.x
n4
External Linux Host
"MyTap"
Tap Bridge (WiFi)
WiFi/P2P
P2P/CSMA
CSMA LAN 10.1.3.x
n1
n2
n5
n6
n7
WiFi 10.1.1.x

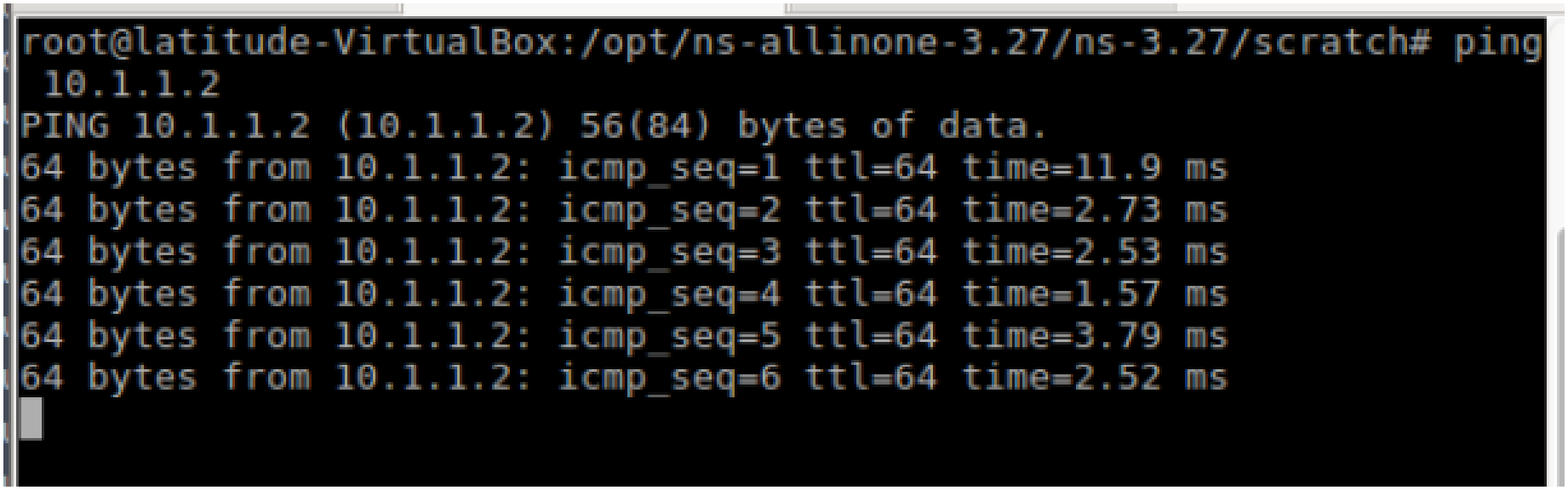
Simulação e Resultados

```
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27# ./waf --run
trabalho-adr-lucas-andre
Waf: Entering directory `/opt/ns-allinone-3.27/ns-3.27/build'
[ 955/2702] Compiling scratch/trabalho-adr-lucas-andre.cc
[2670/2702] Linking build/scratch/trabalho-adr-lucas-andre
Waf: Leaving directory `/opt/ns-allinone-3.27/ns-3.27/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (20.604s)
Versão do TCP utilizada : ns3::TcpSocketFactory
```

Script de emulação em execução, após ser compilado.



TapDevice criado pelo programa, após ser compilado.



O host real já é capaz de usar o programa "Ping" com nós da rede '10.1.1.0'.

```
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch# route add -net 10.1.2.0 netmask 255.255.255.0 dev thetap gw 10.1.1.2
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch#
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch#
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch#
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch# route add -net 10.1.3.0 netmask 255.255.255.0 dev thetap gw 10.1.1.2
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch#
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch#
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch#
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch#
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch#
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch#
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch# ping 10.1.2.1
PING 10.1.2.1 (10.1.2.1) 56(84) bytes of data.
64 bytes from 10.1.2.1: icmp_seq=1 ttl=64 time=16.9 ms
64 bytes from 10.1.2.1: icmp_seq=2 ttl=64 time=4.97 ms
^C
--- 10.1.2.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 4.978/10.977/16.976/5.999 ms
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch# ping 10.1.3.1
PING 10.1.3.1 (10.1.3.1) 56(84) bytes of data.
64 bytes from 10.1.3.1: icmp_seq=1 ttl=63 time=24.6 ms
64 bytes from 10.1.3.1: icmp_seq=2 ttl=63 time=24.7 ms
64 bytes from 10.1.3.1: icmp_seq=3 ttl=63 time=25.2 ms
^C
```

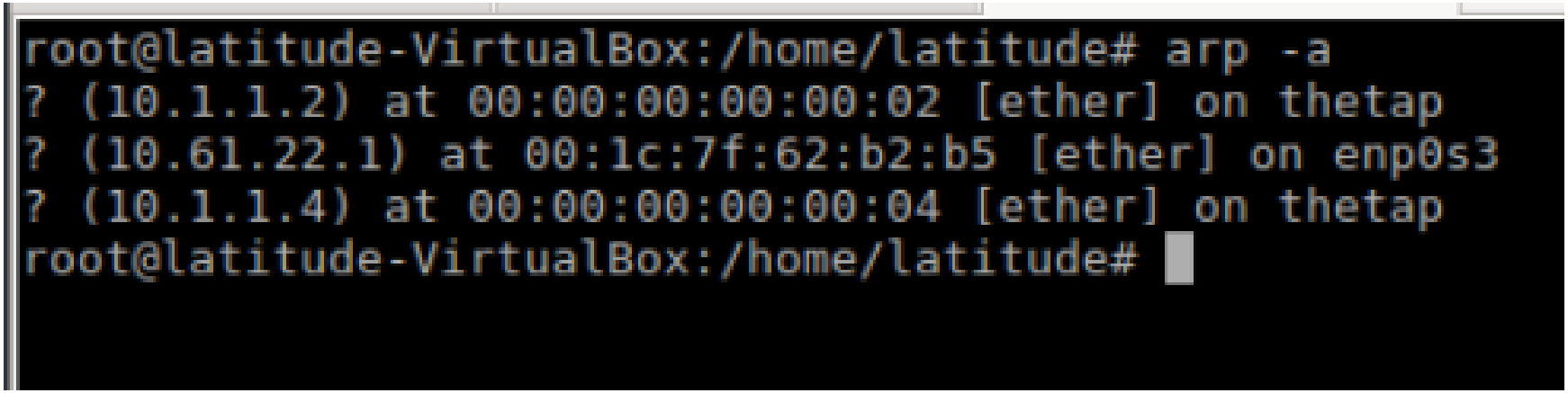
Após a configuração de duas novas rotas, o host real também é capaz de usar o programa "Ping" com nós da rede '10.1.2.0' e '10.1.3.0'.

```
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch# nmap -F 10.1.1.3

Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-28 21:27 -02
Nmap scan report for 10.1.1.3
Host is up (0.0040s latency).
Not shown: 99 closed ports
PORT     STATE SERVICE
8080/tcp open  http-proxy
MAC Address: 00:00:00:00:00:03 (Xerox)

Nmap done: 1 IP address (1 host up) scanned in 3.15 seconds
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch#
```

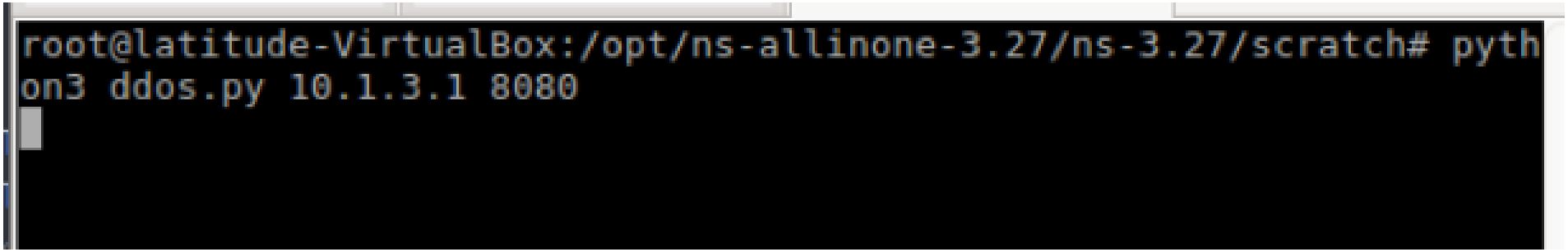
O programa NMAP consegue perceber que existe uma aplicação TCP no nó 10.1.1.3 utilizando a porta 8080.

```
root@latitude-VirtualBox:/home/latitude# traceroute 10.1.3.1
traceroute to 10.1.3.1 (10.1.3.1), 30 hops max, 60 byte packets
 1  10.1.1.2 (10.1.1.2)  15.373 ms  15.788 ms  16.743 ms
 2  10.1.1.4 (10.1.1.4)  17.404 ms  17.669 ms  17.934 ms
 3  * * *
 4  * * *
 5  * * *
 6  * 10.1.2.2 (10.1.2.2)  23.496 ms  27.269 ms
root@latitude-VirtualBox:/home/latitude#
```

O programa TraceRoute consegue rastrear a rota para chegar até a rede '10.1.3.0'.



O programa ARP consegue perceber a presença de outros nós da rede '10.1.1.0'.



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.

```
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27/scratch# python3 ddos.py
10.1.1.3 8080
deu certo

deu certo

deu certo

deu certo

deu certo

deu certo

deu certo

deu certo

deu certo

deu certo

deu certo
```

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

```
  Throughput(bps): -nan bps
  Delay médio(s): -nan
  Jitter médio(s): 0
Flow 298 (10.1.1.3 -> 10.1.1.1)
  Taxa Aplicação(bps): 395.325 bps
  Throughput(bps): -nan bps
  Delay médio(s): -nan
  Jitter médio(s): 0
Flow 299 (10.1.1.3 -> 10.1.1.1)
  Taxa Aplicação(bps): 394.847 bps
  Throughput(bps): -nan bps
  Delay médio(s): -nan
  Jitter médio(s): 0
Flow 300 (10.1.1.3 -> 10.1.1.1)
  Taxa Aplicação(bps): 394.378 bps
  Throughput(bps): -nan bps
  Delay médio(s): -nan
  Jitter médio(s): 0
Flow 301 (10.1.1.3 -> 10.1.1.1)
  Taxa Aplicação(bps): 393.899 bps
  Throughput(bps): -nan bps
  Delay médio(s): -nan
  Jitter médio(s): 0
root@latitude-VirtualBox:/opt/ns-allinone-3.27/ns-3.27#
```

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, tamanho o consumo de recursos que um ataque desses causa.

Conclusões

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 construir uma aplicação real e útil usando o programa.