Simulação ARP Spoofing

1. Executando arquivos python do ryu e do mininet

Instalando a ferramenta de ataque ettercap

sudo apt-get install ettercap-grafical

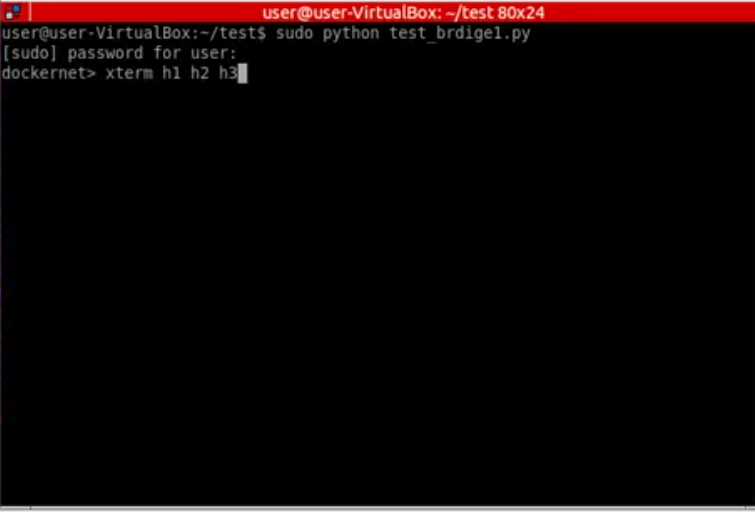
Executando primeiramente o controlador Ryu

ryu-manager ryu/ryu/app/simple\_switch\_13.py

Executando o arquivo python do mininet para criar topografia

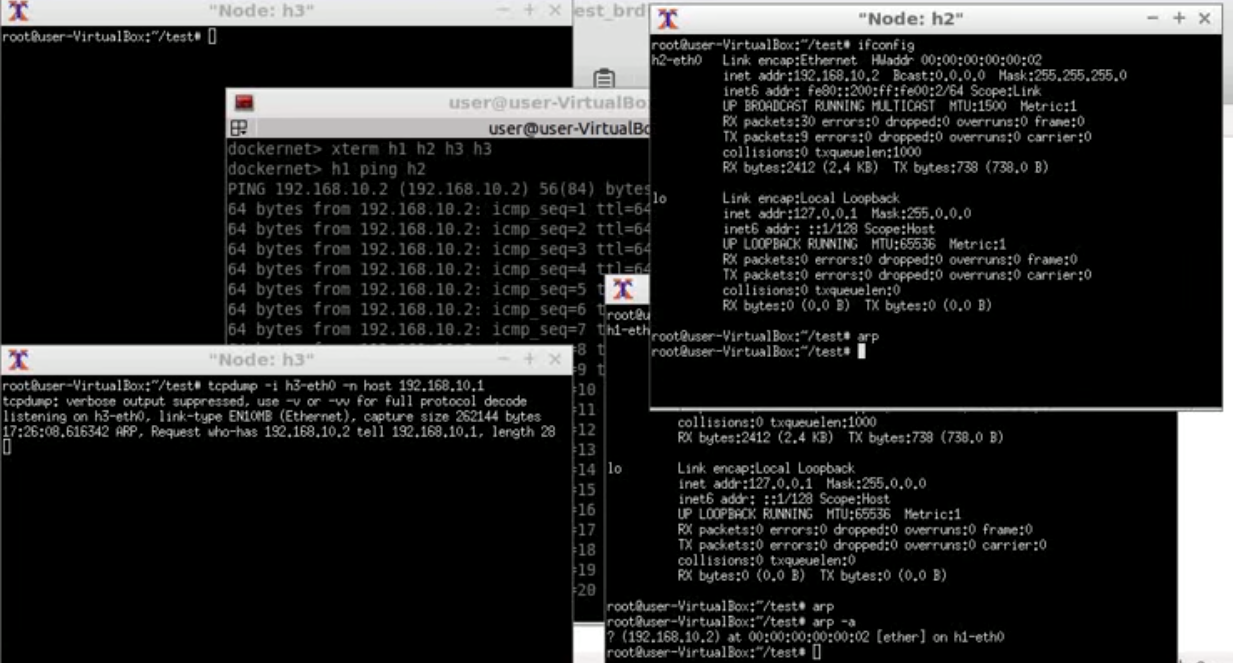
sudo python ./arp\_spoofing.py

1. Abra os hosts virtualmente da topologia criada na mininet



1. executando comando de escuta pelo invasor

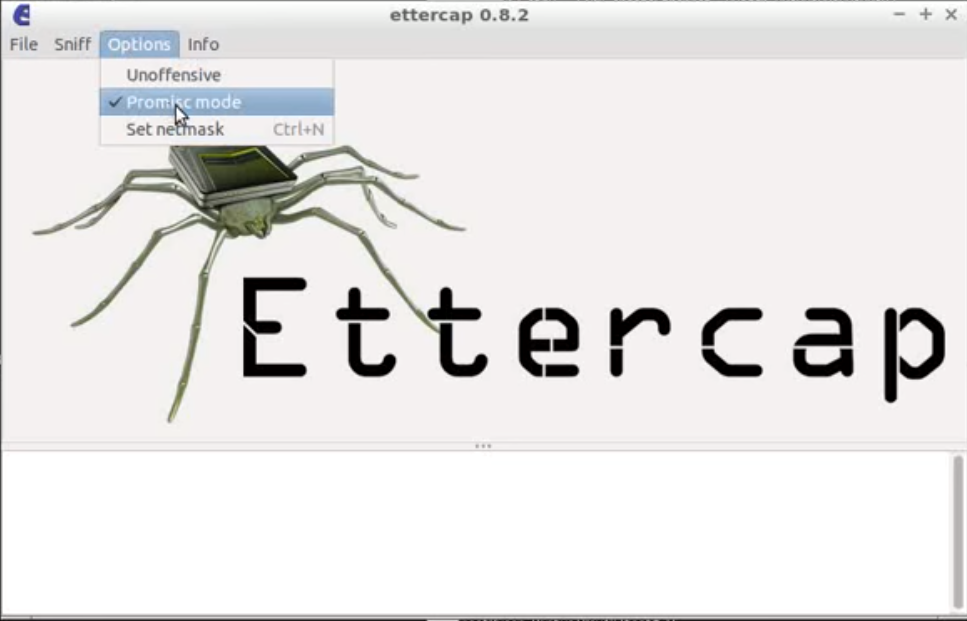
tcpdump -i h3-eth0 -n host 192.168.0.1



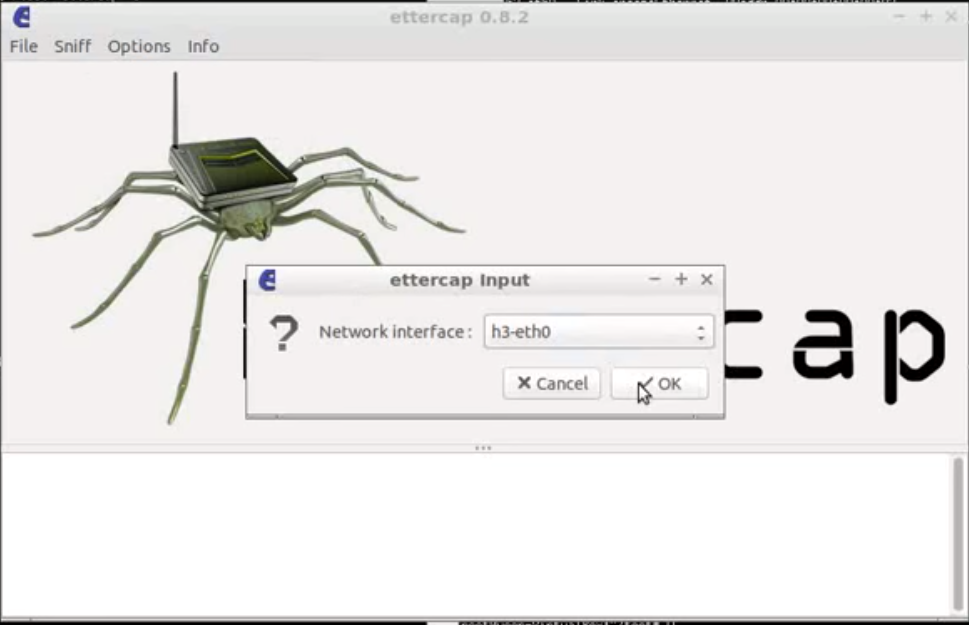
1. executando o Ettercap no invasor

ettercap -G

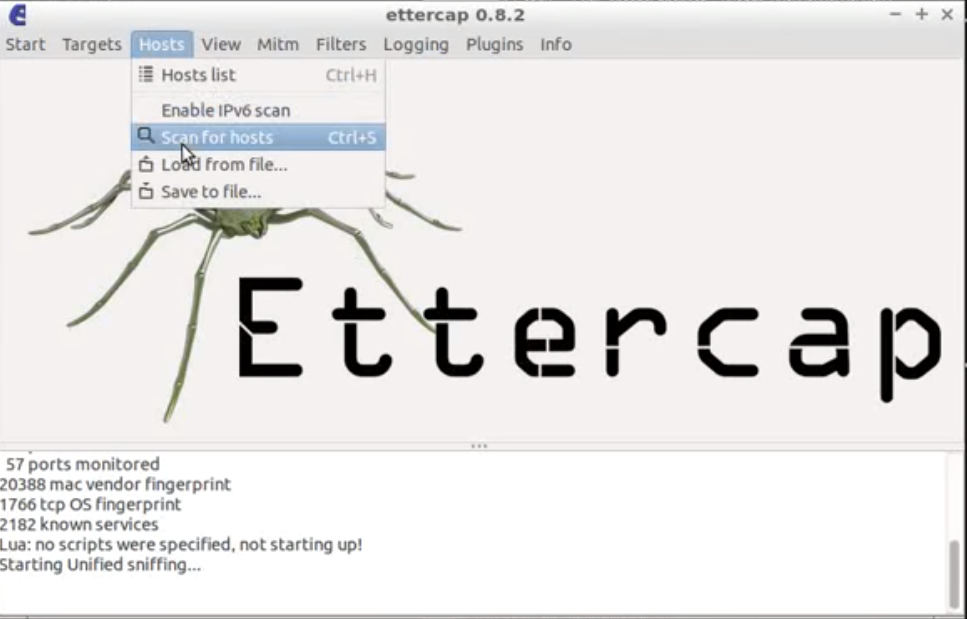
1. configurando a interface modo promiscuo



1. Selecionando a opção unified sniffing em sniff



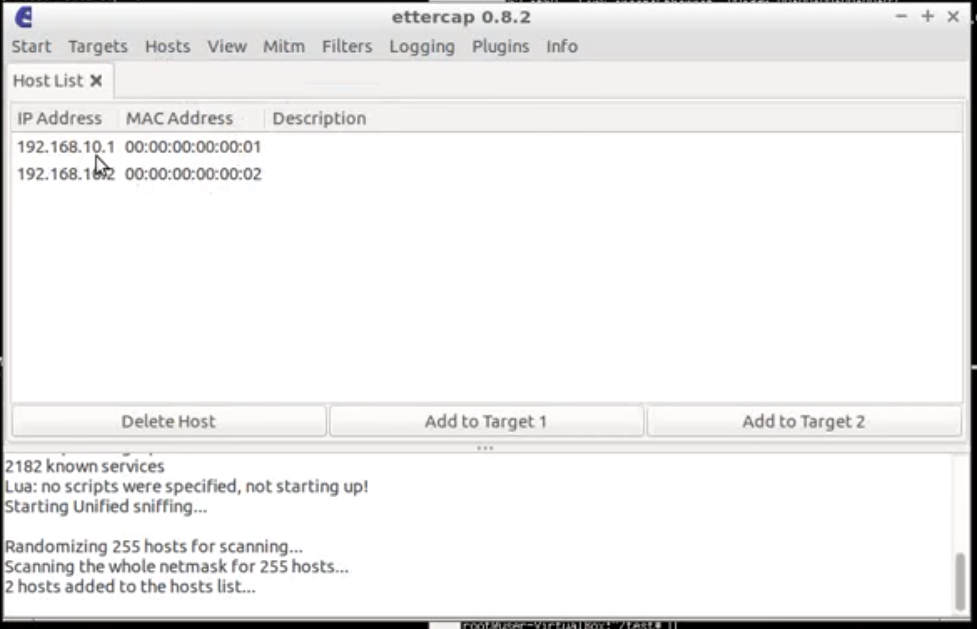
1. Escaneando os alvos



1. SELECIONANDO OS ALVOS

Targe1 – 192.168.10.1 00:00:00:00:00:01

Targe2 – 192.168.10.2 00:00:00:00:00:02



1. Selecionando a opção sniff remote connections
2. Visualizando a MODIFICAÇÃO DA tabela arp do host H2

arp -a

REFERÊNCIAS

KE, C.-H. **youtube**, 2016. Disponivel em: <https://www.youtube.com/watch?v=WUslbs2B-kU&feature=youtu.be>. Acesso em: out. 2017.