Ferramenta de manipulação de pacotes Scapy

Gabriel Mazzardo

Sobre

- Disponível para a linguagem Python.
- Por que utilizar Python?
  - Muita coisa com **poucas linhas de código**;
  - Linguagem **FÁCIL** de utilizar/aprender.

- Ferramenta de manipulação de pacotes.
  - **AMPLAMENTE UTILIZADA**. Possui **INÚMEROS RECURSOS**, utilizados em **diversas aplicações**.
    - Criar pacotes;
    - Enviar/receber pacotes;
    - Sniffar a rede;
    - ...

Instalação

- Apenas a ferramenta: **pip install scapy**
- Ferramenta + Dependências: **pip install --pre scapy[complete]**

Lista dos comandos da ferramenta

Em um terminal:

```
>> scapy
>> lsc()
```

Lista dos protocolos suportados

Em um terminal:

```
>> scapy
>> ls()
```

Campos de um protocolo específico:

```
>> scapy
>> ls(PROTOCOLO)
```

onde PROTOCOLO = protocolo desejado. Ex.: IP, TCP.

Enviando e recebendo pacotes

sr() : envia pacotes L3, e fica aguardando por respostas (até que um número X de pacotes sejam respondidos, por exemplo);

sr1() : envia pacotes L3 e aguarda apenas a PRIMEIRA resposta, fechando a conexão;

srp() : envia pacotes L2 e fica aguardando por respostas;

srp1() : envia pacotes L2 e aguarda apenas a PRIMEIRA resposta, fechando a conexão.

Exemplo 1: Enviando ping para o DNS no Google

- Montar pacote IP/ICMP echo request;
- Enviar o “echo request” para o servidor DNS do Google e aguardar a resposta.

ping_dns_google.py

Exemplo 2: Sniffer de rede

- Observar todo o tráfego que está passando pela rede
  - Útil para tomar decisões com base na análise dos pacotes que compõem o tráfego

sniffer.py

Exemplo 3: **PortScan TCP**

- Descobrir quais portas estão acessíveis (abertas)
  - Portas indesejadas e que estejam abertas podem representar vulnerabilidades que eventualmente podem ser exploradas por atacantes para efetuar acessos não autorizados.

sniffer.py

Links úteis

- Funções de rede PRONTAS utilizando Scapy (créditos: Vinicius Garcia)
  - https://github.com/ViniGarcia/ViNeFuR

- Documentação Scapy:
  - https://scapy.readthedocs.io/en/latest/

- StackOverflow/YouTube/... -> MUITA INFORMAÇÃO DISPONÍVEL!