Hacking com Python

Scapy

Poderoso “Packet tool” para forjar e manipular pacotes.

Instalação:

sudo pip3 install scapy-python3

```
from scapy.all import *
```

Hacking com Python

Funções de baixo nível

sr() - Enviar e receber pacotes na camada 3(rede);
sr1() - Enviar pacotes na camada de rede e receber apenas a primeira resposta;
srp() - Enviar e receber pacotes na camada de enlace;
srp1() - Enviar e receber pacotes na camada de enlace e receber apenas a primeira resposta;
srloop() - Enviar pacotes na camada 3 em um loop e imprimir as saídas;
srploop() - Enviar pacotes na camada 2 em um loop e imprimi as saídas;
sniff() - Capturar pacotes;
send() - Enviar pacotes na camada 3;
sendp() - Enviar pacotes na camada 2;
ls() - Mostra a lista de camadas suportadas pelo Scapy;
ls(x) - Mostra as características de uma determinada camada x;
lsc() - Mostra todas as funções presentes no Scapy;
lsc(x) - Mostra os parâmetros da função x;
conf - Mostra todos os parâmetros iniciais predefinidos.

Hacking com Python

Funções de alto nível

p0f() - Função passiva de recebimento de pacotes do SO;
arpcachepoison() - Capturar e desviar pacotes de um determinado host para outro desejado;
traceroute() - Traça a rota de IP's até um determinado nó da rede.
arping() - Envia um ARP para determinar quais hosts estão funcionando;
nmap_fp() - Função que implementa a ferramenta nmap;
report_ports() - Scanner de portas que gera uma tabela em Latex como relatório;
dyndns_add() - Envia uma mensagem de adição ao DNS para um novo nó;
dyndns_del() - Envia uma mensagem para apagar do DNS o nome desejado.

Hacking com Python

Funções para criação de pacotes

IP()

ICMP()

TCP()

Ether()

NET()

Hacking com Python

Criando primeiro pacote

```
ip = IP(dst='192.168.0.1')   #define o destino no protocolo ip

tcp = TCP(dport=80)          #define a porta de destino no protocolo tcp

pkt = ip/tcp                 #monta o pacote unindo os protocolos formando o TCP/IP

sr(pkt)                      #envia o pacote criado
```

Hacking com Python

Pacote TCP básico

Opção:	Padrão:	Significado:
sport	20	Porta de origem (source)
dport	80	Porta de destino
flags	2 (S)	Flags do pacote
Raw (payload)	null	Payload do pacote

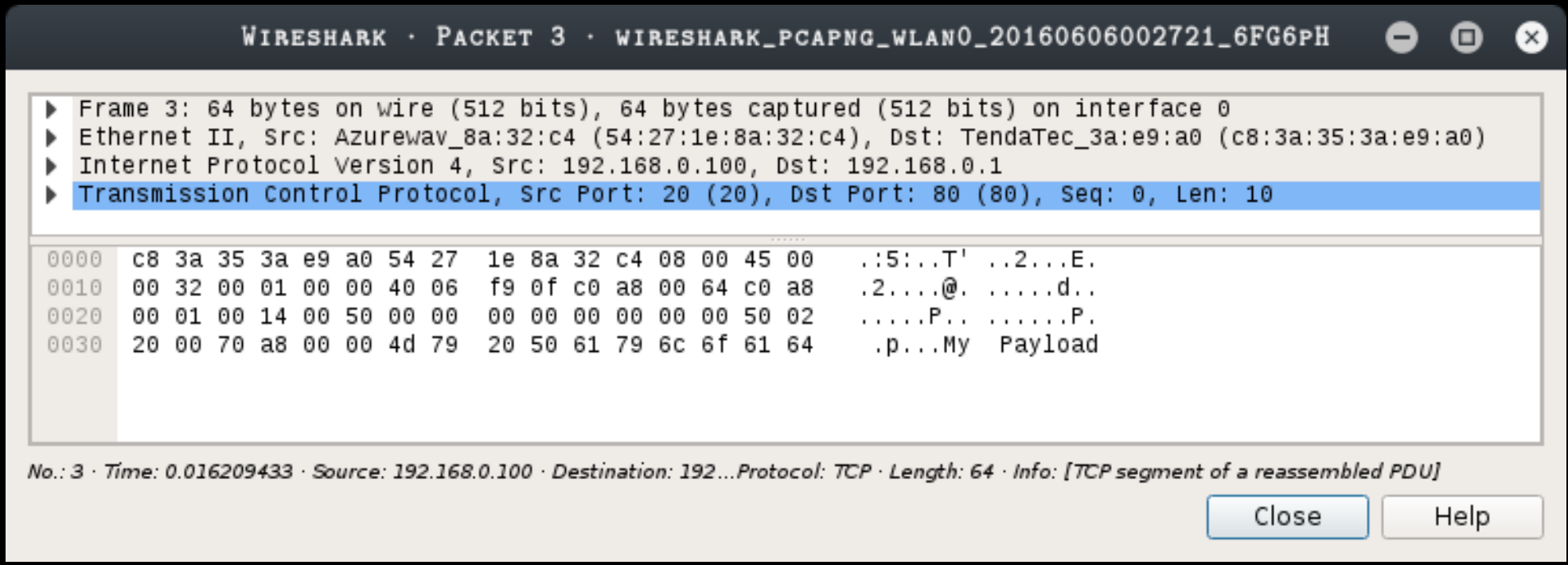
Hacking com Python

Payload TCP

O envio de um payload vai ser bastante eficiente no teste de web app's e/ou servidor

ip = IP(dst="192.168.0.1")

tcp = TCP(dport=80)/"My Payload"



Hacking com Python

Lendo pcap files

```
a = rdpcap("pcapfile.pcap")

a[n] ex: a[33]

a.summary()
a[n].summary

a.show()
a[n].show()

a.hexdump()
```

Hacking com Python

Criando pcap files

```
pkts = sniff(iface="wlan0")

wrpcap(“my.pcap”, pkts)
```

Hacking com Python

Traceroute

Traçar a rota dos pacotes é uma arte!

traceroute("www.gmail.com")

O traceroute é muito usado para “Master Invasion” isso quando o servidor alvo é “blindado” então é necessário “pivoting”

Hacking com Python

Sockets

Sockets são usados para conexões tais como envio de dados, bind...

socket é a interface entre a camada de aplicação e a de transporte

```
socket.socket(socket.AF_INET, socket.SOCK_STREAM)

connect((HOST, PORT))

send()
```