Insper

Tecnologias Hackers

Aula análise de logs e conexões

Professor Dr. Rodolfo Avelino

Objetivo da aula

Analisar conexões TCP;

Explorar as características de uma comunicação TCP;

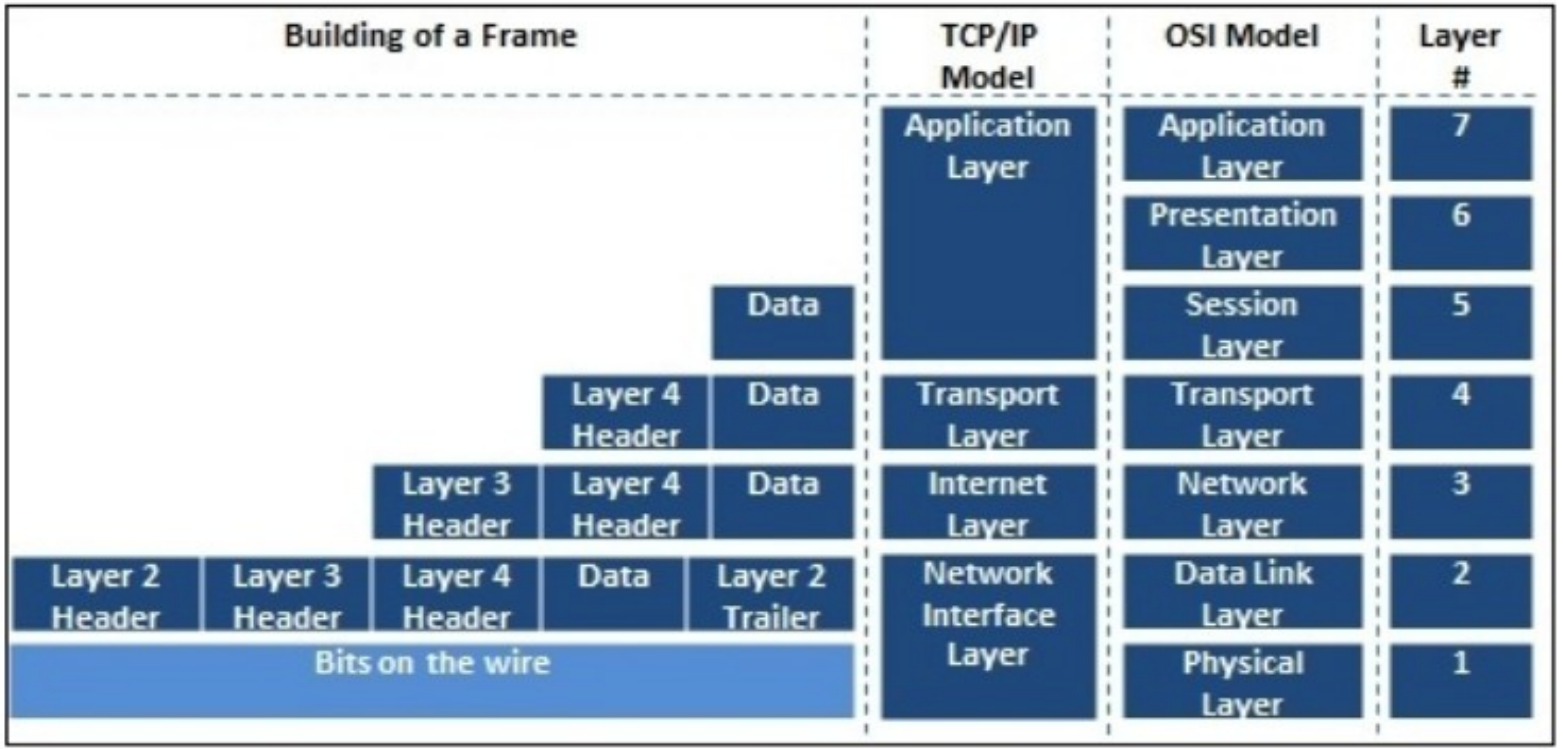
Utilizar ferramentas para análise;

Entender a importância da análise de logs e conexões de rede;

Aprender a interpretar os diferentes tipos de logs;

Identificar padrões e anomalias em conexões de rede.

Encapsulamento



Fonte: Aprendendo Pentest com Python, Christopher Duffy. Pág. 96

Protocolo ARP (fundamental em redes locais

O protocolo ARP, permite encontrar o endereço físico a partir do endereço IP da máquina alvo. Para tal, o protocolo usa um mecanismo de difusão (broadcast) na rede local, enviando uma solicitação a todas as máquinas da rede, sendo que a máquina alvo responde indicando o par endereço IP/endereço físico.

Mac address

O endereço físico também é conhecido como endereço de MAC e corresponde ao endereço Ethernet de 48 bits, representado na forma de seis bytes hexadecimais, por exemplo:

54:8c:a0:df:c7:4f

Para melhorar a performance do protocolo no mapeamento dos endereços IP em endereços físicos, cada máquina possui uma memória (cache) com as últimas consultas realizadas, evitando múltiplos broadcasts. Ainda como refinamento, junto com o broadcast, a estação solicitante envia seu par endereço IP/endereço físico, permitindo que todas as máquinas da rede incluam este par em suas caches locais.

Visualizando o cache ARP

Comando arp -a

```
C:\Users\rodolfosa1>arp -a

Interface: 10.100.0.212 --- 0x12
  Endereço IP           Endereço físico       Tipo
  10.100.0.1            00-00-0c-9f-f4-5e     dinâmico
  10.100.0.3            d0-94-66-ab-93-10     dinâmico
  10.100.0.4            fc-4d-d4-4d-ad-3b     dinâmico
  10.100.0.5            64-1c-67-70-7b-79     dinâmico
  10.100.0.6            fc-4d-d4-4d-a1-c3     dinâmico
  10.100.0.7            64-1c-67-a2-93-da     dinâmico
  10.100.0.10           64-1c-67-a0-ef-4f     dinâmico
  10.100.0.11           64-1c-67-74-0e-6d     dinâmico
  10.100.0.15           64-1c-67-85-5c-6a     dinâmico
  10.100.0.16           64-1c-67-6d-99-c7     dinâmico
```

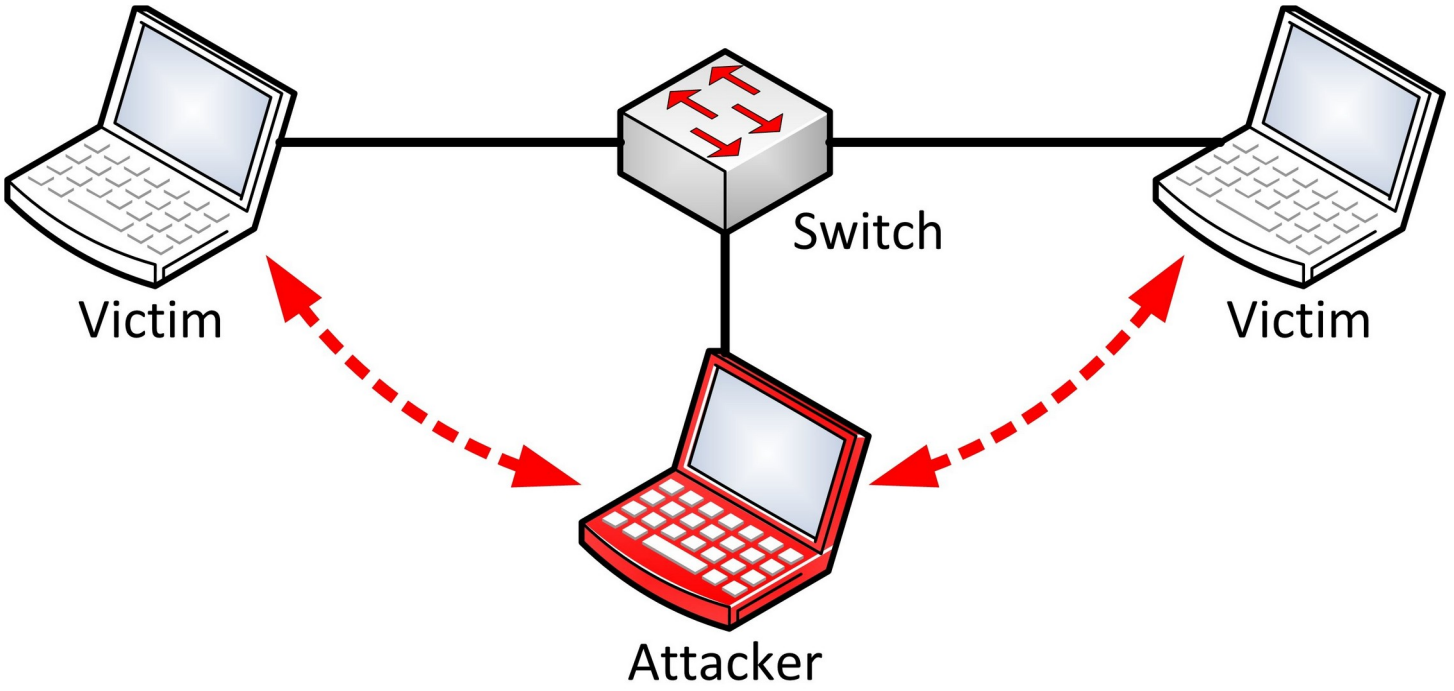
Descobrindo máquinas na rede

- arp-scan --interface=wlp58s0 --localnet

```
root@avelino-XPS-13-9350:/home/avelino# arp-scan --interface=wlp58s0 --localnet
Interface: wlp58s0, type: EN10MB, MAC: 54:8c:a0:df:c7:4f, IPv4: 10.100.31.100
Starting arp-scan 1.9.7 with 4096 hosts (https://github.com/royhills/arp-scan)
10.100.16.1     00:00:0c:9f:f4:5f       Cisco Systems, Inc
10.100.16.7     08:8c:2c:4c:57:b6       Samsung Electronics Co.,Ltd
10.100.16.19    04:ea:56:e8:c5:92       Intel Corporate
10.100.16.25    bc:ff:eb:5e:13:8a       Motorola Mobility LLC, a Lenovo Company
10.100.16.26    52:ae:af:bd:7b:47       (Unknown: locally administered)
10.100.16.29    0c:3e:9f:e9:8e:ed       Apple, Inc.
10.100.16.33    42:32:29:bf:17:a1       (Unknown: locally administered)
10.100.16.34    c0:8c:71:b5:4f:72       Motorola Mobility LLC, a Lenovo Company
10.100.16.40    70:fd:46:88:91:8a       Samsung Electronics Co.,Ltd
10.100.16.41    2e:dd:91:86:d0:68       (Unknown: locally administered)
10.100.16.43    24:77:03:4c:d8:90       Intel Corporate
```

Por meio da infecção do cache ARP é possível direcionar máquinas em uma LAN para máquinas ou servidores comprometidas

Arp Spoofing



Ataque Arp spoofing

Este ataque consistem em adicionar/substituir na tabela arp da maquina alvo uma entrada que aponte um IP do Alvo para o MAC Address do Atacante na tabela ARP da vítima.

É o método mais rápido de se estabelecer no meio da comunicação entre duas máquinas e interceptar as informações enviadas entre ambas

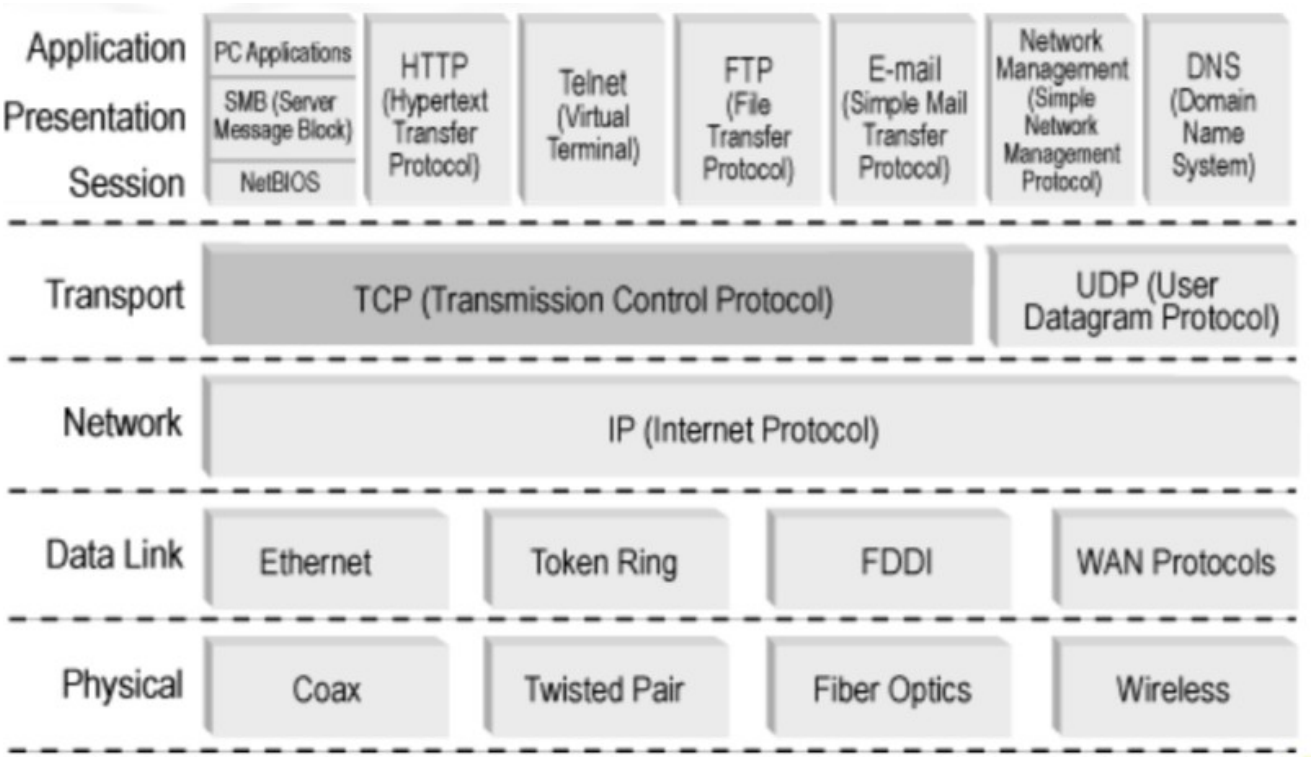
Executando com arpsoof

arpspoof -i <INTERFACE REDE> -t <IP_DO_ALVO> <IP_DO_GATEWAY >

-i → nome da interface de rede

-t → alvo

Considerações protocolo TCP

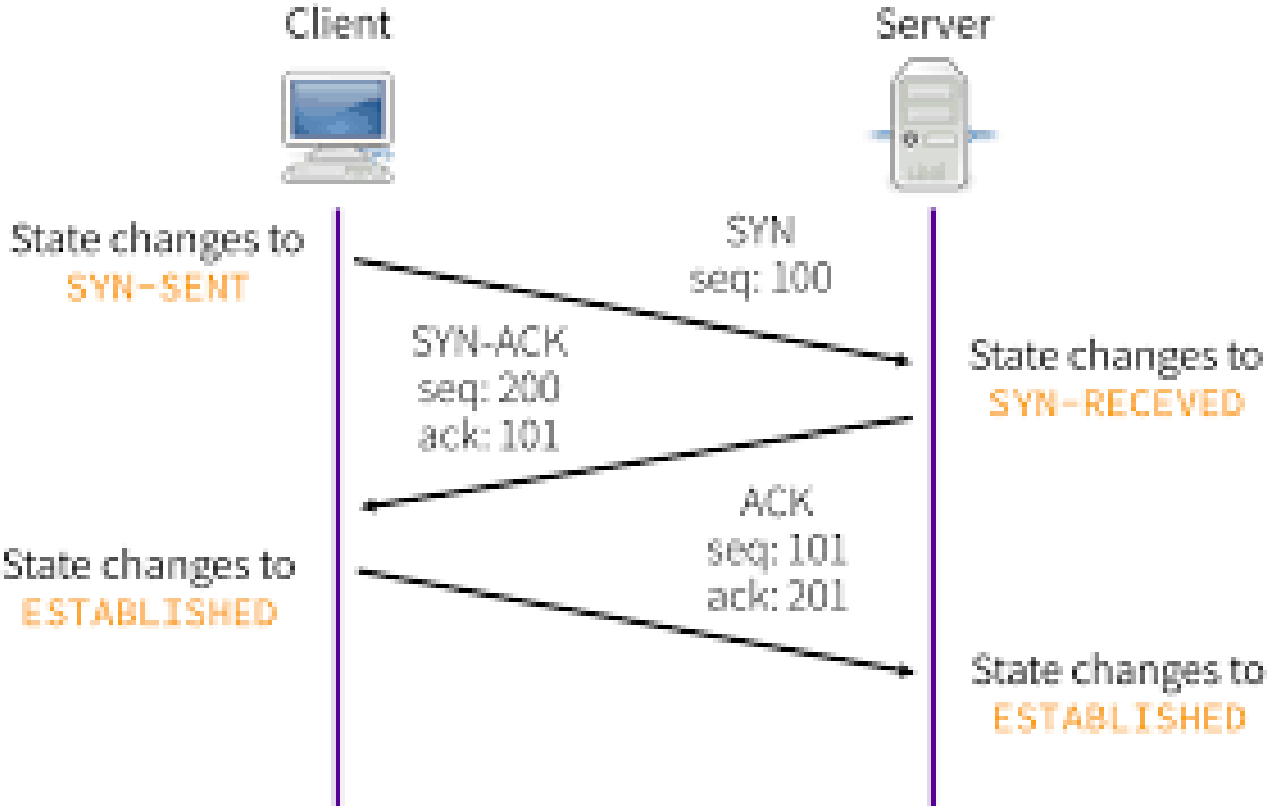


Características comunicação TCP

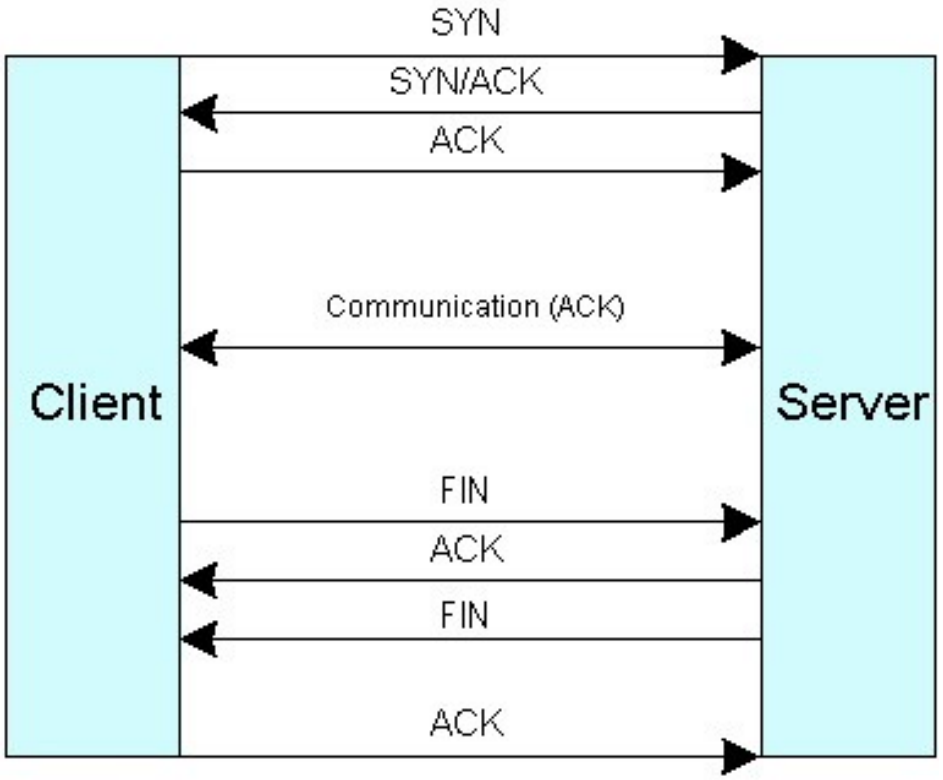
- Usa o conceito de sockets para caracterizar uma conexão.
- Permite estabelecer uma conexão entre um par de sockets de acordo com parâmetros de qualidade de serviço e segurança previamente especificados.
- O estabelecimento de conexões é negociado (uso do mecanismo de “three-way handshaking”).

“Handshaking” = troca de mensagens de controle.

Three- way Handshake



Three- way Handshake (finalizando conexão)



Características

- Admite o término negociado ou abrupto de conexões.
- Implementa temporização na entrega de dados.
- Realiza a entrega ordenada de dados.
- Permite a sinalização de dados urgentes.
- Permite o relato de falha de serviço.
- Permite a entrega obrigatória de dados (flagpush).

Características

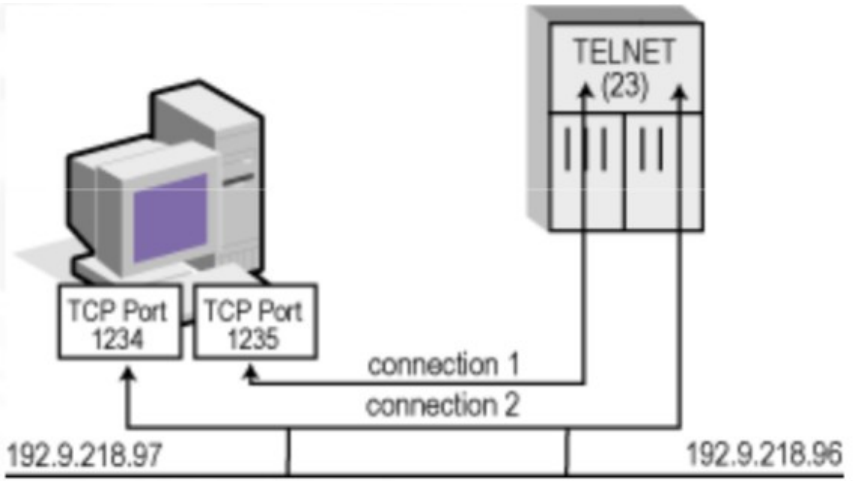
- A camada de transporte associa um identificador a cada processo de aplicação. Esse identificador é chamado de “Porta” (“port number).
- Os números das portas TCP variam de 0 a 65535.Portas de 0 a 1023 são reservadas para o acesso a serviços padrão, como FTP e Telnet (well-knownports).
- Um socket é definido pela combinação de um endereço IP e uma porta, sendo escrito sob a forma “número IP.número da porta”

Exemplo: 192.168.0.11.3389

Socket

- Um socket provê toda a informação de endereçamento que um cliente ou um servidor necessita para identificar seu parceiro na comunicação.
- Uma conexão TCP é caracterizada univocamente por dois sockets, um em cada lado da conexão.

Permitem diferenciar múltiplas conexões



TCP Connection of Two Hosts

Connection	Source IP Address	TCP Port	Destination IP Address	TCP Port
1	192.9.218.97	1234	192.9.218.96	23 Telnet
2	192.9.218.97	1235	192.9.218.96	23 Telnet

Visualizando conexões e sockets

Netstat

O netstat é uma ferramenta de linha de comando usada para exibir informações sobre conexões de rede, tabelas de roteamento, estatísticas de interface, entre outros detalhes.

Netstat

Algumas opções comuns:

-a: Mostra todas as conexões e portas em escuta.

- t: Mostra as conexões tcp.

- u: Mostra as conexões udp

-n: Exibe os endereços IP e portas em formato numérico.

-p: Mostra o PID e o nome do programa associado a cada conexão.

-r: Exibe a tabela de roteamento.

-s: Exibe estatísticas de protocolo.

TCPDUMP

É uma ferramenta utilizada para monitorar os pacotes trafegados numa rede de computadores. Ela mostra os cabeçalhos dos pacotes que passam pela interface de rede.

Instalação

apt install tcpdump

Introdução

O tcpdump é muito flexível as necessidades do administrador, permitindo a especificação desde a interface desejada para a execução do monitoramento até a especificação de portas de origem ou destino que serão monitoradas.

Argumentos

-i Escute na interface. Se não especificado o tcpdump irá procurar a lista de interfaces do sistema, interfaces ativas (excluindo a de loopback).

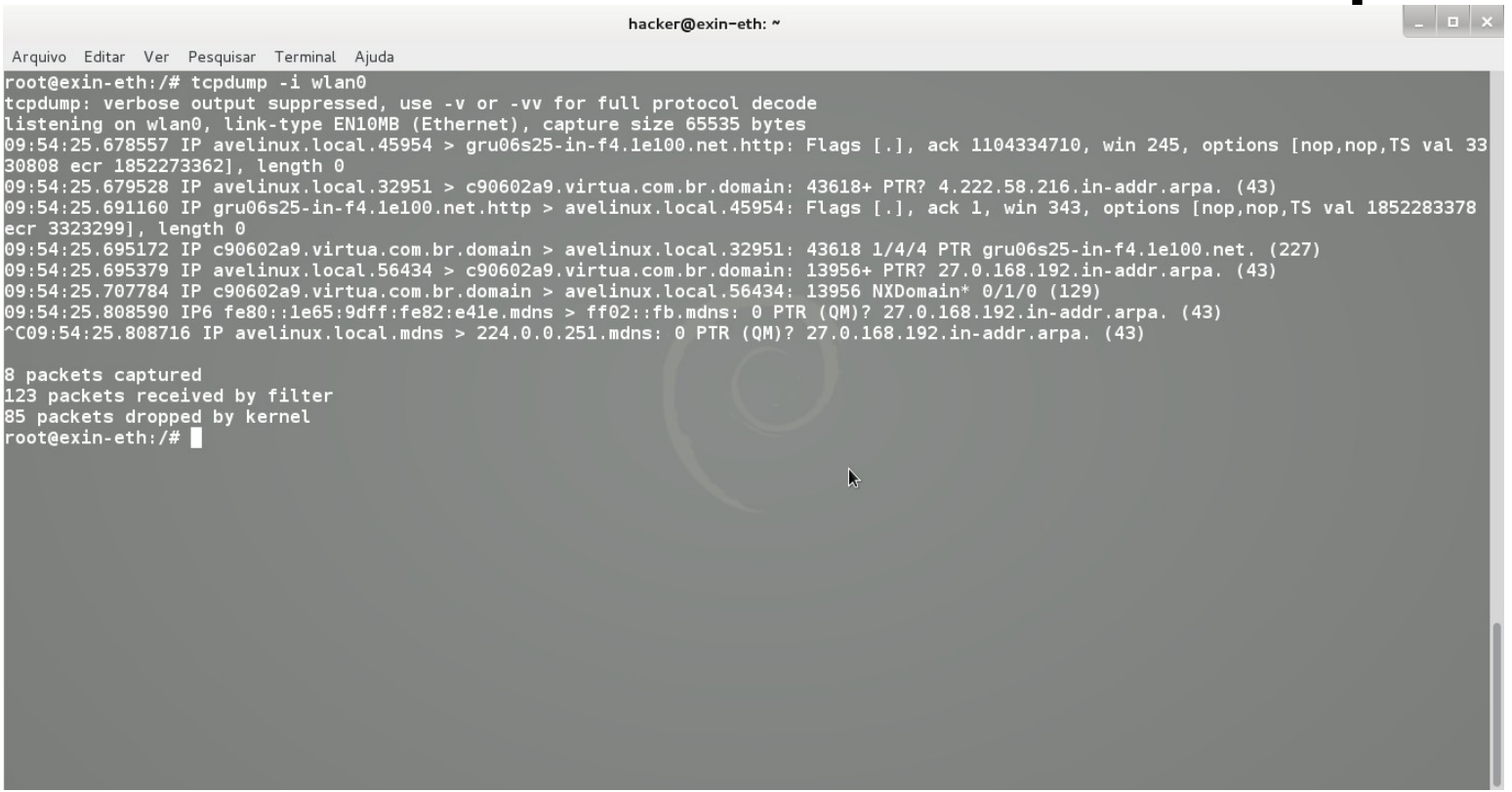
-n Não converter endereços (Ex: endereços de hosts e números de portas, etc) para nomes.

-p Não coloca a interface em modo promíscuo.

-v Detalhamento da saída.

-vv Saída mais detalhada. Por exemplo, campos adicionais serão impressos em pacotes NFS de resposta.

Exemplo



Capturando pacotes de uma interface específica (wlan0)

Saída do commando

22:01:07:710000 192.168.0.2.1173 > 192.168.0.30.21: S 32691180:32691180(0) win 512

22:01:07:710000 Carimbo do pacote (time stamp).

- 2 dígitos HH
- 2 dígitos MM
- 2 dígitos SS
- Últimos 6 dígitos para fração de segundos.

Adaptado : http://www.itnerante.com.br

Saída do comando

- 22:01:07:710000 192.168.0.2.1173 > 192.168.0.30.21: S 32691180:32691180(0) win 512

- 192.168.0.2 IP ou o nome de domínio origem do pacote.

Saída do comando

- 22:01:07:710000 192.168.0.2.1173 > 192.168.0.30.21: S 32691180:32691180(0) win 512

- 1173 Essa é a porta de origem.
- > Somente indica a direção do fluxo. (ORIGEM > DESTINO).
- 192.168.0.30 Esse é o IP de destino.
- 21 Esse indica a porta de destino
- S Esse indica que a flag SYN do TCP.

Saída do comando

- 22:01:07:710000 192.168.0.2.1173 > 192.168.0.30.21: S 32691180:32691180(0) win 512

- 32691180:32691180(0) Esse é o NUMERO DE SEQUENCIA INICIAL:NUMERO DE SEQUENCIA FINAL (QUANTIDADE DE BYTES).
- win 512 É o tamanho do buffer para receber dados que o IP 192.168.0.2 está aceitando em bytes. (Tamanho da Janela).

Outro exemplo de saída

avelinux.com.39006 > faculdade.edu.21: **S** 3774957990:3774957990(0) win 8760 <mss 1460> (DF)

faculdade.edu.21> avelinux.com.39006: **S** 2009600000:2009600000(0) **ack** 3774957991 win 1024 <mss 1460>

avelinux.com.39006 > faculdade.edu.21: .**ack** 1 win 8760 (DF)

avelinux.com.39006 > faculdade.edu.21: P 1:28(27) ack 1 win 8760 (DF)

avelinux.com.39006 > faculdade.edu.21: **S**
3774957990:3774957990(0) win 8760 <mss 1460> (DF)

3774957990:3774957990(0) Número de sequência. Nenhum dado sendo transmitido.

<mss 1460> Isso indica o Maximum Segmet Size ou tamanho máximo do segmento.

(DF) Flag que indica que este pacote não aceita fragmentação.

Adaptado :
http://www.itnerante.com.br

faculdade.edu.21> avelinux.com.39006: **S** 2009600000:2009600000(0) **ack** 3774957991 win 1024 <mss 1460>

ack 3774957991 Indica que confirmou os pacotes com sequence number 3774957990 e agora o próximo pacote que esperar receber é o que tem sequence number 3774957991

Adaptado : http://www.itnerante.com.br

avelinux.com.39006 > faculdade.edu.21: .**ack** 1 win 8760 (DF)

ack 1 Confirma o recebimento do ultimo pacote e espera receber o próximo pacote de sequence number relativo 1 do server.com

Adaptado : http://www.itnerante.com.br

avelinux.com.39006 > faculdade.edu.21: **P 1:28(27)** ack 1 win 8760 (DF)

P Indica que a flag PUSH está ligada, essa flag fala para enviar o pacote diretamente para a aplicação.

1:28(27) Sequence numbers que está enviando. Indica que tem uma carga (payload) de 27 bytes sendo enviado. Está enviando os sequence number de 1 a 28.

Adaptado : http://www.itnerante.com.br

Expressões

Seleciona quais pacotes serão capturados. Se nenhuma expressão for passada, todos os pacotes da rede serão capturados.
Se informada, apenas os pacotes que tiverem a expressão como sendo verdadeira (combinarem com a expressão) serão capturados.

Expressões

Existem 3 principais expressões do TCPDUMP: type, dir e proto

- As opções do type são: host, net e port
- As opções do dir (direção) são: src e dst (e suas combinações)
- proto , permite a seleção dos protocolos : tcp, udp, icmp, entre outras opções tratadas pelo tcpdump

Expressões

Identificadores

host - indicação do host a ser identificado na captura
net - indicação da rede a ser identificada na captura
port - indicação da porta de comunicação

Direções

src – host de origem
dst – host de destino
src or dst – origem ou destino
src and dst – origem e destino

Exemplos

- Captura de pacotes sem que o ip seja resolvido para nome

tcpdump –n –i eth0

- Capturando pacotes do host de origem 10.0.0.20 com o destino a porta 80.

tcpdump -i eth0 src host 10.0.0.20 and dst port 80

- Capturar somente o tráfego associado ao protocolo ICMP, na interface eth0:

tcpdump -i eth0 icmp

Exemplos

Para que o tcpdump grave um arquivo com os resultados da captura utilizamos a opção –w:

tcpdump -i eth0 -w resultadodacaptura.pcap

O arquivo resultadodacaptura.pcap que foi gerado pode ser acessado por meio da opção –r:

tcpdump -r resultadodacaptura.pcap

Um dos principais fundamentos em SI

A análise de logs e conexões de rede é fundamental para:

- Identificar atividades maliciosas: Os logs podem revelar tentativas de intrusão, malware, ataques de negação de serviço (DDoS) e outras ameaças cibernéticas.
- Solução de problemas: Através da análise de logs, é possível diagnosticar problemas de rede, identificar falhas em aplicativos e resolver questões de desempenho.
- Otimização de desempenho: Analisar padrões de tráfego e uso de recursos permite otimizar a infraestrutura de rede, melhorar a eficiência operacional e planejar upgrades futuros.

Exemplos de log

- Logs de firewall
- Logs de servidores web
- Logs de servidores de aplicativos
- Logs de sistemas operacionais
- Logs de IDS/IPS

Diretório de logs (/var/log)

```
root@Debian-107-buster-64-minimal /var/log # ls
alternatives.log       apt             daemon.log       debug.3.gz     dpkg.log.6.gz  kern.log.2.gz  messages.3.gz  syslog.3.gz
alternatives.log.1     auth.log        daemon.log.1     debug.4.gz     dpkg.log.7.gz  kern.log.3.gz  messages.4.gz  syslog.4.gz
alternatives.log.2.gz  auth.log.1      daemon.log.2.gz  dpkg.log       dpkg.log.8.gz  kern.log.4.gz  mysql          syslog.5.gz
alternatives.log.3.gz  auth.log.2.gz   daemon.log.3.gz  dpkg.log.1     faillog        lastlog        postgresql     syslog.6.gz
alternatives.log.4.gz  auth.log.3.gz   daemon.log.4.gz  dpkg.log.2.gz  installer      letsencrypt    private        syslog.7.gz
alternatives.log.5.gz  auth.log.4.gz   debug            dpkg.log.3.gz  journal        messages       syslog         sysstat
alternatives.log.6.gz  btmp            debug.1          dpkg.log.4.gz  kern.log       messages.1     syslog.1       user.log
apache2                btmp.1          debug.2.gz       dpkg.log.5.gz  kern.log.1     messages.2.gz  syslog.2.gz    user.log.1
```

Diretório de logs (/var/log)

```
Feb 14 10:09:01 Debian-107-buster-64-minimal systemd[1]: Starting Clean php session files...
Feb 14 10:09:02 Debian-107-buster-64-minimal systemd[1]: phpsessionclean.service: Succeeded.
Feb 14 10:09:02 Debian-107-buster-64-minimal systemd[1]: Started Clean php session files.
Feb 14 10:15:01 Debian-107-buster-64-minimal CRON[21163]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Feb 14 10:17:01 Debian-107-buster-64-minimal CRON[21580]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Feb 14 10:19:56 Debian-107-buster-64-minimal systemd[1]: Created slice User Slice of UID 0.
Feb 14 10:19:56 Debian-107-buster-64-minimal systemd[1]: Starting User Runtime Directory /run/user/0...
Feb 14 10:19:56 Debian-107-buster-64-minimal systemd[1]: Started User Runtime Directory /run/user/0.
Feb 14 10:19:56 Debian-107-buster-64-minimal systemd[1]: Starting User Manager for UID 0...
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Listening on GnuPG network certificate management daemon.
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Reached target Timers.
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Starting D-Bus User Message Bus Socket.
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Listening on GnuPG cryptographic agent and passphrase cache (
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Listening on GnuPG cryptographic agent and passphrase cache (
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Listening on GnuPG cryptographic agent and passphrase cache.
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Reached target Paths.
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Listening on D-Bus User Message Bus Socket.
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Reached target Sockets.
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Reached target Basic System.
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Reached target Default.
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[22170]: Startup finished in 1.390s.
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[1]: Started User Manager for UID 0.
Feb 14 10:19:57 Debian-107-buster-64-minimal systemd[1]: Started Session 243399 of user root.
```

Em uma análise o que interpretar?

- Identificação de padrões e tendências.
- Reconhecimento de eventos incomuns ou suspeitos.
- Identificação de tráfego suspeito.

Exemplo ataque brute force ssh

```
Oct  2 06:25:46 host-vps sshd[8463]: Failed password for root from 116.31.116.17 port 31142 ssh2
Oct  2 06:25:48 host-vps sshd[8463]: Failed password for root from 116.31.116.17 port 31142 ssh2
Oct  2 06:25:51 host-vps sshd[8463]: Failed password for root from 116.31.116.17 port 31142 ssh2
Oct  2 06:25:51 host-vps sshd[8463]: Received disconnect from 116.31.116.17: 11:  [preauth]
```

Em uma análise o que interpretar?

- Identificar atividades maliciosas: Os logs podem revelar tentativas de intrusão, malware, ataques de negação de serviço (DDoS) e outras ameaças cibernéticas.

Exemplo ataque web server

191.96.249.97 - - [20/Apr/2017:15:45:49 +0200] "GET /phpmyadmin/scripts/setup.php HTTP/1.0" 404 162 "-" "-" "-"
190.129.24.154 - - [14/Jul/2015:06:41:59 -0400] "GET /phpMyAdmin/index.php HTTP/1.1" 404 162 "-" "Python-urllib/2.6" "-"
190.129.24.154 - - [20/Apr/2017:09:04:47 +0200] "PROPFIND /webdav/ HTTP/1.1" 405 166 "-" "WEBDAV Client" "-"
180.97.106.37 - - [20/Apr/2017:04:31:02 +0200] "\x04\x01\x00P\xB4\xA3qR\x00" 400 166 "-" "-" "-"

Fique atento com os status http

1xx Informações

2xx Sucesso

3xx Redirecionamento

4xx Erro Do Cliente

5xx Erro De Servidor

Caixa de ferramentas

Ping e traceroute

São dois comandos básicos muito utilizados por administradores de rede. Permitem determinarmos qual Sistema Operacional do alvo por meio doTTL (Time-To-Live)

TTL:

Linux	64
Windows	128
Unix	255

fping

Ferramenta usada para envio de ICMP Echo Request para vários hosts ao mesmo tempo.

fping –g 192.168.0.0/24

fping 192.168.0.2 192.168.0.10

Arping

Utiliza o protocolo ARP Request como protocolo de requisição, sendo muito útil na análise em uma Rede Local.

arping 192.168.0.1

Netdiscover

Similar à ferramenta arping, porém é possível enviar pacotes ARP Request para um range de Ips.

netdiscover -r 10.0.0.0/24 –i eth0

-r - rande de Ips

-i - interface de rede

Exercício

Utilizando a ferramenta tcpdump:

1) Capture somente os pacotes gerados por sua máquina.
2) Capture somente pacotes destinados à sua máquina.
3) Capture pacotes para ou do gateway
4) Capture pacotes HTTPS.

Salve os pacotes capturados de cada exercício em arquivos chamado “exercicio_X_capturados_SEUNOME”.