



Ferramentas para Redes

Everson Santos Araujo
everson@por.com.br

Ping

- Função do protocolo ICMP para testar conectividade
- Funcionamento:
 - Envia uma requisição a um equipamento
 - Aguarda resposta

Ping

- Função do protocolo ICMP para testar conectividade
- Funcionamento:

- Envia uma requisição a um equipamento

- Aguarda

```
everson ~ $ ping -c 4 everson.por.com.br
PING everson.por.com.br (208.97.184.170): 56 data bytes
64 bytes from 208.97.184.170: icmp_seq=0 ttl=49 time=281.858 ms
64 bytes from 208.97.184.170: icmp_seq=1 ttl=48 time=297.736 ms
64 bytes from 208.97.184.170: icmp_seq=2 ttl=51 time=247.100 ms
64 bytes from 208.97.184.170: icmp_seq=3 ttl=50 time=253.866 ms

--- everson.por.com.br ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 247.100/270.140/297.736/20.582 ms
```

Traceroute

- Função do protocolo ICMP para determinar caminho
- Permite conhecer o caminho que um pacote percorre para trafegar até um destino utilizando o parâmetro TTL
- Funcionamento:
 - Cada roteador verifica o TTL e subtrai 1 unidade do mesmo
 - Ao se enviar um pacote com TTL 1 o primeiro roteador irá retornar erro, pois o TTL chegou a 0

Netstat

- Apresenta informações sobre conexões realizadas ou sistemas aguardando conexão na máquina local
- Função:
 - Verificar quais serviços estão ativos e aguardando conexão
 - Verificar se existem serviços não autorizados executando na máquina

Netstat

- Apresenta informações sobre conexões realizadas ou sistemas aguardando conexão na máquina local

- Função

- Verificar se estão estabelecidas conexões

estã
con

- Verificar se não há conexões na máquina

nã
na m

```
everson ~ $ netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4    0      0 *.mysql                 *.*                     LISTEN
tcp4    0      0 *.*                     *.*                     CLOSED
tcp46   0      0 *.http                  *.*                     LISTEN
tcp4    0      0 *.kerberos              *.*                     LISTEN
tcp6    0      0 *.kerberos              *.*                     LISTEN
tcp4    0      0 *.ssh                   *.*                     LISTEN
tcp6    0      0 *.ssh                   *.*                     LISTEN
tcp4    0      0 *.microsoft-ds         *.*                     LISTEN
tcp4    0      0 *.netbios-ssn          *.*                     LISTEN
tcp4    0      0 *.afpovertcp           *.*                     LISTEN
tcp6    0      0 *.afpovert              *.*                     LISTEN
tcp4    0      0 localhost.ipp           *.*                     LISTEN
tcp6    0      0 localhost.ipp           *.*                     LISTEN
udp4    0      0 *.*                     *.*                     LISTEN
udp6    0      0 localhost.ntp           *.*                     LISTEN
udp4    0      0 localhost.ntp           *.*                     LISTEN
udp6    0      0 localhost.ntp           *.*                     LISTEN
```

```
ngbe    0      0 localhost.*             *.*                     LISTEN
ngbe    0      0 localhost.*             *.*                     LISTEN
ngbe    0      0 localhost.*             *.*                     LISTEN
```



Análise de tráfego: Wireshark

Filter: + Expression... Limpar Aplicar

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	63.245.209.21	10.0.2.15	HTTP	HTTP/1.1 302 Found (tex
2	0.000028	10.0.2.15	63.245.209.21	TCP	41128 > http [ACK] Seq=1
3	0.000051	10.0.2.15	10.0.2.3	DNS	Standard query A newsrss
4	1.139820	10.0.2.3	10.0.2.15	DNS	Standard query response
5	1.141577	10.0.2.15	212.58.226.29	TCP	57905 > http [SYN] Seq=0
6	1.474581	212.58.226.29	10.0.2.15	TCP	http > 57905 [SYN, ACK] :
7	1.475043	10.0.2.15	212.58.226.29	TCP	57905 > http [ACK] Seq=1
8	1.479351	10.0.2.15	212.58.226.29	HTTP	GET /rss/newsonline worl

Frame 5 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: CadmusCo_bc:27:3e (08:00:27:bc:27:3e), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol, Src: 10.0.2.15 (10.0.2.15), Dst: 212.58.226.29 (212.58.226.29)
Transmission Control Protocol, Src Port: 57905 (57905), Dst Port: http (80), Seq: 0, Len: 0

```
0000  52 54 00 12 35 02 08 00 27 bc 27 3e 08 00 45 00  RT..5... '.'>..E.
0010  00 3c 1c 4b 40 00 40 06 5c 0a 0a 00 02 0f d4 3a  .<.K@.@. \.....:
0020  e2 1d e2 31 00 50 d3 d7 5c 8a 00 00 00 00 a0 02  ...1.P.. \.....
0030  16 d0 1b 23 00 00 02 04 05 b4 04 02 08 0a 00 03  ...#.... .....
```

File: "/tmp/etherXXXXWBWgNH" 211 ... Packets: 518 Displayed: 518 Marked: 0 Dro... Profile: Default