Tracking the route

`ping exampl e.com -c 1`	Envia apenas 1 pacote ICMP para testar a conectividade com o destino.
`ping exampl e.com -c 1 -t 1`	Envia 1 pacote ICMP com TTL (Time to Live) definido como 1.
`traceroute exampl e.com`	Exibe o caminho completo (hops) até o destino.
`traceroute exampl e.com -w 1`	Define o tempo de espera em 1 segundo por resposta de cada hop.
`traceroute exampl e.com -m 1`	Limita o número máximo de hops (TTL) a 1.
`traceroute exampl e.com -m 5`	Limita o número máximo de hops (TTL) a 5.
`traceroute exampl e.com -m 25 -f 15`	Define o TTL inicial como 15 e o TTL máximo como 25.
`traceroute exampl e.com -A`	Mostra as informações do sistema autônomo (AS) dos hops.
`traceroute exampl e.com -n`	Exibe os endereços IP dos hops sem resolver os nomes DNS.
`traceroute exampl e.com -n -I`	Usa pacotes ICMP em vez de UDP para a rota.
`traceroute exampl e.com -n -U`	Usa pacotes UDP em vez de ICMP para a rota.
`traceroute exampl e.com -n -T`	Usa pacotes TCP em vez de UDP para a rota.
`traceroute exampl e.com -n -T -p 80`	Usa pacotes TCP com a porta de destino 80.
`traceroute exampl e.com -n -m 1`	Limita o número máximo de hops (TTL) a 1 e exibe o resultado em formato numérico.
`traceroute exampl e.com -n -m 1 -U`	Limita o número máximo de hops (TTL) a 1 e usa pacotes UDP.

firewall

`iptables -nL`	Lista todas as regras de firewall ativas, sem resolver nomes de host ou serviços.
`iptables -P INPUT DROP`	Define a política padrão para INPUT como DROP (bloquear todo o tráfego de entrada).
`iptables -P INPUT ACCEPT`	Define a política padrão para INPUT como ACCEPT (permitir todo o tráfego de entrada).
`iptables -A INPUT -p tcp --dport 80 -j ACCEPT`	Permite conexões TCP na porta 80 (HTTP).
`iptables -A INPUT -p tcp --dport 80 -j DROP`	Bloqueia conexões TCP na porta 80 (HTTP).
`iptables -A INPUT -p icmp -j ACCEPT`	Permite pacotes ICMP (como os usados pelo comando ping).
`iptables -F`	Remove todas as regras de firewall ativas.
`iptables -A INPUT -p tcp --dport 80 -s 192.16 8.0.11 -j ACCEPT`	Permite conexões TCP na porta 80 (HTTP) somente do IP 192.168.0.11.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

firewall (cont)

`iptables -A INPUT -p tcp --dport 80 -s 192.16 8.0.11 -d 192.16 8.0.12 -j ACCEP T`	Permite conexões TCP na porta 80 (HTTP) do IP 192.168.0.11 para o IP 192.168.0.12.
`iptables -A INPUT -p icmp --icmp -type 8 -j ACCEPT`	Permite pacotes ICMP de tipo 8 (echo request, usados pelo ping).
`iptables -A INPUT -p udp -j ACCEPT`	Permite todo o tráfego UDP de entrada.
`iptables -A INPUT -p tcp -dport 3306 -s <IP> -j ACCEPT`	Permite conexões TCP na porta 3306 (MySQL) vindas de um IP específico.
`iptables -A INPUT -p tcp -dport 3306 -d <IP> -j ACCEPT`	Permite conexões TCP na porta 3306 (MySQL) destinadas a um IP específico.
`iptables -A INPUT -p tcp -sport 3306 PORT -j ACCEPT`	Permite conexões TCP com porta de origem 3306 (MySQL).

ping sweep

`for ip in $(seq 1 254); do ping -c 1 172.16.1.$ ip ;done | grep "64 bytes"`	Realiza um ping em todos os IPs do intervalo 172.16.1.1 a 172.16.1.254 e exibe apenas os IPs que responderem com "64 bytes".
`for ip in $(seq 1 254); do ping -c 1 172.16.1.$ip -w 1;done | grep "64 bytes"`	Faz o mesmo que o comando anterior, mas define um tempo limite de 1 segundo para cada ping.
`for ip in $(seq 224 239); do ping -c 1 37.59.1 74.$ip -w 1;done | grep "64 bytes"`	Realiza um ping nos IPs do intervalo 37.59.174.224 a 37.59.174.239, com um tempo limite de 1 segundo, exibindo somente os IPs que responderem.
`fping -a -g 172.16.1.0/24`	Verifica todos os IPs no intervalo 172.16.1.0/24 e exibe apenas os que estão ativos (respondendo ao ping).

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com