Universidade Estadual de Londrina

KAUEE ROCHA PUERTAS

COMANDOS/FUNÇÕES BÁSICAS DE REDE

LONDRINA - PR
2023

Trabalho de Laboratório – 04/04/2023

Questão 01) Descreva as funções de cada um destes comandos

- Ping:

O comando "ping" (Packet Internet Groper) é usado para testar a conectividade de rede entre dois dispositivos, enviando pacotes de dados para um endereço IP específico e, em seguida, esperando por uma resposta. Ele pode ser usado para testar a conexão com um site ou servidor específico, ou para diagnosticar problemas de rede, como perda de pacotes ou latência excessiva.

- Netstat:

O comando "netstat" (Network Statistics) é usado para exibir informações sobre as conexões de rede ativas em um sistema. Ele pode mostrar os endereços IP e portas que estão sendo usados, o estado da conexão (estabelecido, aguardando, fechado, etc.), o número de pacotes enviados e recebidos, entre outras informações úteis para o diagnóstico de problemas de rede.

- Nslookup:

O comando "nslookup" (Name Server Lookup) é usado para consultar servidores DNS (Domain Name System) para obter informações sobre um nome de domínio ou endereço IP. Ele pode ser usado para verificar a resolução de nomes de domínio, bem como para encontrar o endereço IP de um site específico.

- Tracert:

O comando "tracert" (Trace Route) é usado para rastrear a rota que os pacotes de dados tomam de um dispositivo para outro através da rede. Ele exibe uma lista de todos os roteadores e dispositivos intermediários pelos quais os pacotes passam, juntamente com o tempo que leva para cada salto. Isso pode ser útil para diagnosticar problemas de latência ou determinar onde ocorrem falhas de rede.

- Ipconfig/Ifconfig:

Os comandos "ipconfig" (Windows) e "ifconfig" (Linux/Unix) são usados para exibir informações sobre as interfaces de rede de um dispositivo. Eles podem mostrar o endereço IP, máscara de sub-rede, gateway padrão e outras informações relevantes para a configuração da rede. Eles também podem ser usados para redefinir a interface de rede, liberar ou renovar um endereço IP DHCP, ou configurar opções avançadas de rede.

Questão 02) Exemplos de cada um deles

- Ping:

1. ping uol.com.br
2. ping 200.147.3.157
3. ping -t www.facebook.com (ping contínuo para um endereço específico)

- Netstat:

1. netstat -a (exibe todas as conexões de rede ativas)
2. netstat -n (exibe endereços IP em vez de nomes de host)
3. netstat -o (exibe o número do processo associado a cada conexão)

- Nslookup:

1. nslookup www.globo.com
2. nslookup -type=mx gmail.com (exibe registros MX de um domínio específico)
3. nslookup -debug www.youtube.com (exibe informações detalhadas sobre a consulta DNS)

- Tracert:

1. tracert www.facebook.com
2. tracert 8.8.8.8 (rastreia a rota para um endereço IP específico, no exemplo, dns.google)
3. tracert -d www.google.com (desativa a resolução DNS para acelerar o rastreamento)

- Ipconfig/Ifconfig:

1. ipconfig (exibe informações sobre as interfaces de rede em um computador Windows)
2. ipconfig /all (exibe informações detalhadas sobre a configuração de rede)
3. ifconfig eth0 (exibe informações sobre a interface de rede eth0 em um sistema Linux/Unix)

Questão 03) Qual destes comandos podem ser utilizados como forma de ataque a um computador e explique como?

Os comandos “netstat”, “nslookup” e “ipconfig/ifconfig” podem ser utilizados por invasores para explorar vulnerabilidades de segurança ou obter informações sobre o sistema do alvo. Aqui estão alguns exemplos de como eles podem ser usados para ataque:

1. Netstat: um invasor pode usar para identificar conexões ativas em um sistema alvo e identificar portas de redes abertas. Isso pode ser usado para encontrar vulnerabilidades conhecidas em serviços de redes ou para identificar potenciais alvos para ataques posteriores
2. Nslookup: um invasor pode usar o comando para obter informações sobre a configuração de DNS de um sistema alvo, incluindo endereços IP e registros de recursos. Isso pode ser

usado para identificar vulnerabilidades em serviços DNS ou para obter informações sobre outros servidores de rede.
3. Ipconfig/ifconfig: um invasor pode usar para identificar informações de rede, como endereços IP, máscaras de sub-rede e gateways padrão. Essas informações podem ser usadas para identificar sistemas em uma rede e potencialmente explorar vulnerabilidades de segurança conhecidas.

Questão 04) Qual a função do serviço Whois?

O serviço Whois é um protocolo de pesquisa e consulta utilizado para obter informações sobre registro de domínios, como o nome do registrante, informações de contato, data de registro, data de expiração, informações do servidor de nomes e outras informações relacionadas aos registros de domínios. Essas informações são mantidas por registradores de domínios e são públicas, pois o registro de domínios é um processo transparente.

Pode ser útil para diversas finalidades, como pesquisa de domínios, identificação de proprietários de sites, verificação da disponibilidade de um nome de domínio e resolução de problemas de rede relacionados ao domínio. Além disso, o serviço Whois é utilizado por órgãos reguladores e agências de aplicação da lei para investigação de atividades ilegais, como fraudes, spam, violações de direitos autorais e outras violações de leis relacionadas à internet.

No entanto, é importante lembrar que algumas informações sensíveis, como endereços de e-mail e números de telefone, podem ser exibidas nos resultados da pesquisa Whois e podem ser usadas por spammers e outros invasores para enviar e-mails não solicitados ou realizar outras atividades mal-intencionadas. Por esse motivo, muitos registradores de domínios oferecem serviços de privacidade de domínio para proteger as informações pessoais do proprietário do domínio.

Questão 05) Qual a função do serviço DHCP (Dynamic Host Configuration Protocol)?

O DHCP (Dynamic Host Configuration Protocol) é um protocolo de rede que permite que os dispositivos conectados a uma rede obtenham automaticamente um endereço IP (Internet Protocol), além de outras informações de configuração de rede, como máscara de sub-rede, gateway padrão e servidores DNS.

O DHCP facilita a atribuição dinâmica de endereços IP aos dispositivos de uma rede, evitando conflitos de endereço e simplificando a administração da rede. Sem o DHCP, os administradores de rede teriam que configurar manualmente cada dispositivo com um endereço IP exclusivo, o que seria impraticável em redes grandes ou em constante mudança.

Quando um dispositivo é conectado a uma rede que usa DHCP, ele envia uma solicitação de endereço IP ao servidor DHCP da rede. O servidor DHCP responde com um endereço IP disponível na rede e outras informações de configuração de rede necessárias para o dispositivo se comunicar com outros dispositivos na rede. O dispositivo então configura automaticamente sua interface de rede com as informações fornecidas pelo servidor DHCP e começa a se comunicar com outros dispositivos na rede.

Questão 06) Qual o endereço MAC e seu endereço IP do seu computador e smartphone? Qual a diferença entre eles e para que eles servem?

Computador:

- [redacted]
- [redacted]

Smartphone:

- [redacted]
- [redacted]