TCP/IP

Camada de aplicação

Rogério Fontes

Definição

- É a camada número quatro do modelo TCP/IP que engloba também as camadas de apresentação e sessão no modelo OSI.

Definição

- É nessa camada que ocorre a interação micro-usuário. A camada de aplicação é responsável por identificar e estabelecer a disponibilidade da aplicação na máquina destinatária e disponibilizar os recursos para que tal comunicação aconteça.

Função da camada

- Composta por 3 camadas:
  - Sessão.
  - Apresentação e aplicação.
  - Que são distintas no modelo OSI.

Função da camada

- Tem por função servir como terminal para as operações que ocorrem em uma rede.

Função da camada

- Quando é preciso requisitar algo que está em uma rede, seja ela LAN, WAN, ou qualquer outra, é na camada de aplicação que irá ser feita a requisição ou recebimento de informações.

Responsabilidade

- A camada de aplicação é responsável por gerenciar e deixar disponível ao usuário, todos os sistemas e ferramentas a ele destinados, por ex: ERP, SSH, TELNET, FTP, SGDB, SNMP, e outros aplicativos e recursos disponíveis em uma rede, seja de pequeno ou grande porte.

Principais protocolos

- HTTP: Hypertext Transfer Protocol usa a porta 80 como padrão e é responsável pela ligação de recursos da World Wide Web. Quando acionado esse protocolo sabe que irá trafegar mensagens web com html.

Principais protocolos

- Telnet/SSH: usados para emular terminal, através deles podemos controlar remotamente qualquer sistema operacional de acordo com o privilégio determinado ao usuário logado. Telnet server (porta 23 TCP) usado em Windows e *nix, SSH server (porta 22 TCP) usado em *nix, SSH é criptografado enquanto Telnet não possui criptografia, podendo assim ser alvo fácil para sniffers. Incluindo equipamentos como routeadores.

Principais protocolos

- FTP: File Transfer Protocol, usado para transferência de arquivos entre servidores, seja por linha de comando ou por algum programa ex: Filezilla. Suportados em todos os sistemas operacionais. Utiliza a porta 21 TCP para troca de mensagens e comandos e a porta 20 para a transferência de arquivos propriamente dita.

Principais protocolos

- POP3/IMAP: usados para o recebimento de e-mails. Post Office Protocol (POP3) geralmente utiliza a porta 110 TCP. Internet Message Access Protocol (IMAP) alternativo ao POP3, pode-se gerir vários acessos simultâneos.

Principais protocolos

- SMTP: Simple Mail Transport Protocol, usado para o envio de emails. Utiliza a porta 25 TCP.

Principais protocolos

- DNS: Domain Name Server, usado para identificar nome de domínios ex: www.dominio.com, facilitando a memorização para consultas por parte do usuário. Utiliza a porta 53 TCP e UDP.

Principais protocolos

- SNMP: Simple Network Management Protocol, usado para gerenciar redes. Com ele é possível coletar ou receber dados referentes a CPU da máquina por exemplo. Vários programas de monitoramento de redes utilizam esse protocolo para coletar informações como o Nagios. Utiliza UDP para comunicação, porta 161 utilizada para comandos e 162 para alarmes, com ele é possível monitorar switches, routers.

Utilitários TCP/IP

- Telnet: para estabelecer uma conexão com o servir é necessário informar os parâmetros “telnet ip_do_servidor” por padrão se a porta for a 23 não é necessário informar, caso contrário deverá ser especificado exemplo: “telnet ip_do_servidor porta”.
- Após conectado é possível executar qualquer função administrativa desde que o usuário possua privilégios suficientes. Com ele podemos editar registro do windows, criar e remover pastas e arquivos(mkdir, rm, cp, edit), instalar programas, listar e eliminar tarefas(tasklist, taskkill), reiniciar ou desligar o equipamento (shutdown –s, shutdown –h, shutdown -r), mais uma infinita lista de programas via linha de comando.

Utilitários TCP/IP

- SSH: segue a mesma função do Telnet, porém com criptografia e para conectar a Linux. Com ssh podemos criar túneis que são muito úteis quando o firewall nos bloqueia.

Utilitários TCP/IP

- SSH: segue a mesma função do Telnet, porém com criptografia e para conectar a Linux. Com ssh podemos criar túneis que são muito úteis quando o firewall nos bloqueia.
- Para estabelecer uma conexão com SSH é necessário informar os parâmetros “ssh user@maquina” e após senha conforme solicitado, por padrão se a porta for a 22 não é necessário informar, caso contrário deverá ser especificado exemplo: “ssh user@maquina –P porta”. Para listar tarefas em linux o camando é o “top”, para desligar “halt”, reinicializar “reboot” e mais uma infinita lista de programas via linha de comando.

Utilitários TCP/IP

- PING: utilizado para testar se á comunicação entre servidores “ping ip_do_servidor”, envia pacotes icmp.

- $ ping -i 5 IP

Utilitários TCP/IP

- TRACEROUTE: utilizado para mostrar a rota feita entre o ponto de origem e o ponto de destino “tracert ip_de_destino”.

- $ traceroute <server-name> (google.com)

Utilitários TCP/IP

- ROUTE ADD: utilizado para definir rotas “route add ip mask gw”.

- $ route
- $ route –n
- $ route add default gw 192.168.1.10

Utilitários TCP/IP

- WMIC: útil para colectar informações do computador “wmic baseboard” ou “wmic service”.

Utilitários TCP/IP

- GETMAC: utilizado para capturar o endereço físico de um componente de rede “getmac” remotamente “getmac –S ip_destino -U usuario –P senha”.

Utilitários TCP/IP

- nmap: utilizado para capturar o endereço físico de um componente de rede no linux.

- **$nmap -v scanme.nmap.org**

Utilitários TCP/IP

- IPCONFIG ou IFCONFIG (Linux) : utilizado para descobrir informações sobre o componente de rede como, mascaramento, endereço ip, gatway padrão.

- $ ifconfig eth0

Utilitários TCP/IP

- NETSH: muito útil para executar comandos de configuração de rede

Utilitários TCP/IP

- NETSH: muito útil para executar comandos de configuração de rede, abaixo alguns exemplos:

Utilitários TCP/IP - Exemplos

- # pathping -n 192.168.1.102

Utilitários TCP/IP - Exemplos

- “nbtstat -a” para listar as máquinas por nome.
- “nbtstat -A” para listar as máquinas por IP.
- “nbtstat -c” para listar o nome do cache remoto incluindo os endereços IP.
- “nbtstat -n” para listar os nomes de NETBIOS Local.
- “nbtstat -r” para listar nomes resolvidos por Broadcast e por WINS.
- “nbtstat -R” para recarregar a tabela de cache remoto.
- “nbtstat -S” para listar a tabela de sessões com os IPs de destino.
- “nbtstat -s” para listar tabela de sessões convertendo IP de destino para nomes de

Utilitários TCP/IP - Exemplos

- NETSTAT: Mostra conexões de rede, tabela de roteamento, estatísticas de interfaces, conexões masquerade, e mensagens.
- netstat [opções]
- Onde:
  opções
  -i [interface]

- Mostra estatísticas da interface [interface].
- -M, –masquerade
- Se especificado, também lista conexões masquerade.
- -n, –numeric
- Usa endereços numéricos ao invés de tentar resolver nomes de hosts, usuários e portas.
- -c, –continuos

Referencias

- http://petterlopes.wordpress.com/2011/07/18/camada-de-aplicacao-modelo-tcpip/
- http://nmap.org/book/man-examples.html
- http://www.thegeekstuff.com/2009/03/ifconfig-7-examples-to-configure-network-interface/