INSTITUTO TECNOLOGICO DE CANCÚN

INGENIERIA EN SISTEMAS COMPUTACIONALES

FUNDAMENTOS DE TELECOMUNICACIONES

EXAMEN UNIDAD 3

Peraza Soberanis Gabriel Alfredo

1.- Factors to consider when selecting a packet sniffer

R = Protocolos soportados: Que sean compatibles para poder utilizar

2) Diseño

3) Facilidad de instalación

4) El costo

5) El fujo general de las operaciones a realizar

2.- How Packet Sniffers Work? R= INTERCEPTANDO Y REGISTRANDO EL TRÁFICO DE RED QUE PUEDEN VER A TRAVÉS DE LA INTERFAZ DE RED CABLEADA O INALÁMBRICA A LA QUE EL SOFTWARE DE SNIFFING DE PAQUETES TIENE ACCESO EN SU COMPUTADORA HOST.

3.- Describe The Seven-Layer OSI Model. R=

7	Aplicación	Se compone de los servicios y aplicaciones de comunicación estándar que puede utilizar todo el mundo.
6	Presentación	Se asegura de que la información se transfiera al sistema receptor de un modo comprensible para el sistema.
5	Sesión	Administra las conexiones y terminaciones entre los sistemas que cooperan.
4	Transporte	Administra la transferencia de datos. Asimismo, garantiza que los datos recibidos sean idénticos a los transmitidos.
3	Red	Administra las direcciones de datos y la transferencia entre redes.
2	Vínculo de datos	Administra la transferencia de datos en el medio de red.
1	Física	Define las características del hardware de red.

4.- Describe Traffic Classifications

Trafico sensible: Es el tráfico que el operador espera entregar a tiempo.

Trafico de máximo esfuerzo: son todos los demás tipos de tráfico no perjudicial
Trafico no deseado: Esta categoría generalmente se limita a la entrega de Correo
no deseado y tráfico creado por gusanos y otros ataques maliciosos.
5.- Describe sniffing around hubs. R= SI EN UNA RED TIENE REALMENTE INSTALADO HUBS, COMO DETECTAR QUERER ENTRAR, YA QUE AL TRATAR DE CONECTARSE PODEMOS VER TODA LA COMUNICACIÓN QUE ESTÉN CONECTADOS A ESE HUB
6.- Describe sniffing in a switched environment R= LOGRA MEDIANTE LA CONFIGURACIÓN DE UN ATAQUE "HOMBRE EN EL MEDIO". EL ATACANTE UTILIZA UNA VARIEDAD DE TÉCNICAS PARA FORZAR EL TRÁFICO DE RED A / DESDE LA VÍCTIMA PARA IR A LA MÁQUINA DEL ATACANTE.
7.- How ARP Cache Poisoning Works?R = ES PARA INFILTRARSE EN UNA RED, Y MODIFICAR EL TRAFICO QUE SUCEDE EN ESA RED LOCAL, COMO ENVIANDO MENSAJES FALSOS AL YA ESTAR INTERCEPTADO.
8.- Describe sniffing in a routed environment R= TODO DEPENDE DE LA COLACIÓN DEL SNIFFER YA QUE SI SE QUIERE SOLUCIONAR UN PROBLEMA TIENE QUE APLICARSE A TODOS LOS SEGMENTOS DE RED
9.- Describe the Benefits of wireshark
R= ES EL ANALIZADOR DE TRÁFICO DE RED LÍDER EN EL MUNDO Y UNA HERRAMIENTA ESENCIAL PARA CUALQUIER PROFESIONAL DE LA SEGURIDAD O ADMINISTRADOR DE SISTEMAS
10.- Describe The three panes in the main window in Wireshark
R = PANEL DE CAPTURA: ES DONDE MUESTRA LOS DATOS DE LA CAPTURA COMO EL NÚMERO DE PAQUETE, TIEMPO, LONGITUD E INFORMACIÓN.
-PANEL DE DETALLE DEL PAQUETE MUESTRA DE FORMA MÁS DETALLA SOBRE LA INFORMACIÓN DE LOS PAQUETES EN ESPECIAL DE LOS PROTOCOLOS.
-PANEL DE BYTES DEL PAQUETE MOSTRARÍA LA INFORMACIÓN DE PAQUETE EN EL LENGUAJE HEXADECIMAL O ASCII.
11.- How would you setup wireshark to monitor packets passing through an internet router
R= Conectarse al un puerto LAn del router y selercionar el puerto y empezar la captura
12.- Can wireshark be setup on a Cisco router?R= Si es possible, pero con comandos
13.- Is it possible to start wireshark from command line on Windows?
R = SI ES POSIBLE

14.- A user is unable to ping a system on the network. How can wireshark be used to solve the problem.
15.- Which wireshark filter can be used to check all incoming requests to a HTTP Web server? R = http.response se refiere al filtrado por mensajes y códigos de respuesta. Estos son enviados por el servidor al navegador.
16.- Which wireshark filter can be used to monitor outgoing packets from a specific system on the network?
R = DST HOST HOST CAPTURA POR HOST DE DESTINO
17.- Wireshark offers two main types of filters:
R= Los filtros de captura (Capture Filter) son los que se establecen para mostrar solo los paquetes de cumplan los requisitos indicados en el filtro.

Los filtros de visualización (Display Filer) establecen un criterio de filtro sobre los paquetes capturados y que estamos visualizando en la pantalla principal de Wireshark. Estos filtros son mas flexibles y pontentes.
18.- Which wireshark filter can be used to monitor incoming packets to a specific system on the network? R = CON EL “HOST” POR SI HAY UNO QUE YA EXISTE O SE CREA UN FILTRO PARA BUSCARLO.
19.- Which wireshark filter can be used to Filter out RDP traffic?
R = RDP es un protocolo propietario desarrollado por Microsoft para sus servicios de Terminal Server. PUERTO 3389, tcp port 3389
20.- Which wireshark filter can be used to filter TCP packets with the SYN flag set R = TCP.FLAGS.SYN == 1
21.- Which wireshark filter can be used to filter TCP packets with the RST flag set
R = TCP.FLAGS.RESET == 1
22.- Which wireshark filter can be used to Clear ARP traffc R= NOT.ARP
23.- Which wireshark filter can be used to filter All HTTP trafficR= Http REQUEST

24.- Which wireshark filter can be used to filter Telnet or FTP traffic
USAR EN LA BARRA DEL FILTRO, AL MOMENTO DE BYSCAR TRAFICO EN LA RED, INDICAR EL USO DEL FILTRO PARA TELNET O FTP. FILTRO DE CAPTURA
25.- Which wireshark filter can be used to filter Email traffc (SMTP, POP, or IMAP)
26.- List 3 protocols for each layer in TCP/IP model
R=

Ref. OSI Nº de capa	Equivalente de capa OSI	Capa TCP/IP	Ejemplos de protocolos TCP/IP
5,6,7	Aplicación, sesión, presentación	Aplicación	NFS, NIS, DNS, LDAP, RIP, RDISC, SNMP
4	Transporte	Transporte	TCP, UDP, SCTP
3	Red	Internet	IPv4, IPv6, ARP, ICMP
2	Vínculo de datos	Vínculo de datos	PPP, IEEE 802.2
1	Física	Red física	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI y otros.

27.- What does means MX record type in DNS?

UN REGISTRO DNS DE "INTERCAMBIO DE CORREO"(MX)DIRIGE EL CORREO ELECTRÓNICO A UN SERVIDOR DE CORREO. EL REGISTRO MX INDICA CÓMO SE DEBEN ENRUTAR LOS MENSAJES DE CORREO ELECTRÓNICO DE ACUERDO CON EL PROTOCOLO SIMPLE DE TRANSFERENCIA DE CORREO (SMTP, EL PROTOCOLO ESTÁNDAR PARA TODO EL CORREO ELECTRÓNICO).

28.- Describe the TCP Three Way HandShake

TCP UTILIZA UN PROTOCOLO DE ENLACE DE TRESVÍAS PARA ESTABLECER UNA CONEXIÓN CONFIABLE. LA CONEXIÓN ES DÚPLEX COMPLETO, Y AMBOS LADOS SINCRONIZAN (SYN) Y RECONOCEN (ACK) ENTRE SÍ. EL INTERCAMBIO DE ESTOS CUATRO INDICADORES SE REALIZA EN TRES PASOS — SYN, SYN-ACK, Y ACK

29.- Mention the TCP Flags

SYN", "ACK" y "FIN, Restablecer (RST), Empuje (PSH), Urgente (URG), NC, ECE, CWR

30.- How ping command can help us to identify the operating system of a remote host?R = HACE UNA VERIFICACIÓN DEL ESTADO DE UNA DETERMINADA CONEXIÓN DE UN HOST LOCAL CON AL MENOS UN EQUIPO REMOTO CONTEMPLADO EN UNA RED DE TIPO TCP/IP. SIRVE PARA DETERMINAR SI UNA DIRECCIÓN IP ESPECÍFICA SI UN HOST ES ACCESIBLE DESDE LA RED O NO LO ES.