2017

SEMINARIO

Análisis de Tráfico en Red con Wireshark

ACTIVIDAD DE FORMACION PRACTICA

1. Formación experimental (laboratorio).

OBJETIVOS

1. Conocer las principales funcionalidades del software **Wireshark, última versión**.
2. Comprender las técnicas básicas de análisis de tráfico en red, con particular interés en capas 2, 3 y 4.

CONOCIMIENTOS PREVIOS

1. Redes LAN Ethernet/IEEE 802.3 y 802.1Q. Arquitectura y funcionamiento.
2. Formato de tramas, paquetes y segmentos.
3. Funcionamiento del proceso de encapsulamiento.
4. Protocolos IP, ICMP, ARP, DHCP.
5. Formatos de las PDUs y funcionamiento.
6. PDU, funcionamiento y direccionamiento IP.
7. Proceso de enrutamientos básicos.
8. Formatos de las PDUs y funcionamiento de los protocolos TCP y UDP
9. PDU y funcionamiento del protocolo DNS, HTTP y HTTPS.

MATERIAL NECESARIO

1. Para las **ACTIVIDADES PREVIAS**:
   a. Software **Wireshark, última versión** (https://www.wireshark.org/).
   b. Archivos de apoyo a la autopreparación:
      https://www.wireshark.org/download/docs/user-guide-a4.pdf
   c. VIDEO ON LINE https://www.youtube.com/watch?v=Y5rZlmmqVQk
   d. Otros materiales sobre modos de captura y análisis de seguridad con Wireshark:
      https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf
2. Para el desarrollo de los ***Casos de Estudio***:
   a. Una PC de escritorio con el software **Wireshark, última versión**, instalado.
   b. Proyector para PC.

ACTIVIDADES PREVIAS

1. Puede utilizar el apoyo el manual del archivo ***user-guide-a4.pdf***.
2. También, puede ser muy útil apoyar el estudio en los recursos en línea de Wireshark: https://wiki.wireshark.org/
3. Instale el software de trabajo.
4. Haga un estudio comprensivo de las siguientes funciones del software:
   a. Descripción de la Interfaz de Usuario
      - Menúes: “File”, “Edit”, “View, “Go”, “Capture”, “Analyze”, “Statistics”, “Telephony”, ”Wireless”, “Tools”
      - Barra de herramientas: “Main”, “Filter”
      - Paneles “Packet List” , “Packet Details”, “Packet Bytes”
      - Barra de estado

   b. Funciones básicas de Capturar, Desplegar y Filtrar tramas (en detalle).

   c. Funcionalidades en detalle de “Capture” (Options, Capture Filters), “Analyze” (Display, Apply, Prepare y Conversation Filter – ver detalles en https://wiki.wireshark.org/DisplayFilters ; Enabled Protocols; Follow), “Statistics” (Conversations, Endpoints, Flowgraphs, HTTP, IPv4/IPv6 Statistics y ”Wireless (WLAN Traffic)”. Cuando sea posible, deberán disponerse de capturas “ejemplo”
5. Profundice el estudio para preparar una demo de cada función, con capturas que haya realizado en la autopreparación, con la finalidad de demostrar su conocimiento en clase (**se deben traer archivos para realizar “demos” y explicar las habilidades alcanzadas en el uso del software**).

DESARROLLO

Este trabajo será desarrollado en tres etapas:

1. **EXPOSICIÓN de “Conocimientos básicos del software”**: a desarrollar por aquellos alumnos que sean designados por el docente, mediante una PC, proyector y ejemplos de uso del software.

   Todos deberán preparar los temas indicados en **ACTIVIDADES PREVIAS**.

   Requerimientos para el alumno (Objetivos Técnicos)

   a. Realizar las operaciones del software con habilidad.

   b. Demostrar la comprensión de las funciones más útiles, en base a ejemplos demostrativos preparados con antelación.

2. **EXPLICACIÓN de DÓNDE REALIZAR LA CAPTURA DE DATOS**: el docente explicará las diferentes opciones de localización del host de captura, indicando brevemente las particularidades de cada caso:
   a. UTILIZANDO UN HUB
   b. PORT MIRRORING O VACL (VLAN-BASED ACLS)

c. MODO BRIDGE

d. ARP SPOOF

e. REMOTE PACKET CAPTURE

3. **DEMOSTRACIÓN de "Análisis de tramas"**: Los docentes demostrarán ejemplos de análisis de tráfico para diferentes protocolos de capas, con la finalidad de explicar las diferentes técnicas de análisis de PDU, "bytes" más importantes a analizar en cada caso, aspectos destacados en el transmisor / receptor. Además, se ampliará el conocimiento de las facilidades del software.

   Se tendrán en cuenta los siguientes casos:

   a. Capa de Enlace: alguno de los siguientes protocolos,
      - Ethernet: IEEE 802.3 Ethernet
      - IEEE 802.11: IEEE 802.11 wireless LANs
      - STP: IEEE 802.1D Spanning Tree Protocol
      - VLAN: IEEE 802.1Q Virtual Bridged Local Area Networks

   b. Capa de Red: alguno de los siguientes protocolos,
      - IP: Internet Protocol (version 4)
      - IPv6: Internet Protocol (version 6)
      - ICMP: Internet Control Message Protocol (version 4)

   c. Capa de Transporte: alguno de los siguientes protocolos,
      - UDP: User Datagram Protocol
      - TCP: Transmission Control Protocol

   d. Capa de Sesión:
      - NetBIOS

   e. Capa de Presentación:
      - MIME

   f. Capa de Aplicación: alguno de los siguientes protocolos,
      - HTTP: Hyper Text Transfer Protocol
      - DHCP: Dynamic Host Configuration Protocol
      - DNS: Domain Name System
      - FTP: File Transfer Protocol
      - IMAP
      - POP: Post Office Protocol
      - SSH: Secure Shell

- SNMP: Simple Network Management Protocol
- Telnet: remote shell Access

TIEMPO ASIGNADO: 180 minutos

CRITERIO DE EVALUACION

Esta actividad no tendrá evaluación.

ACTIVIDAD DE REPASO

Para integrar de manera práctica el conocimiento particular adquirido sobre el software Wireshark, el alumno preparará filtros adecuados para los Trabajos de Laboratorio 5 y 6:

- Tramas Ethernet/IEEE 802.3, 802.1Q, 802.11.
- Paquetes ARP, IP, ICMP.
- Segmentos TCP, UDP.
- Protocolos NetBIOS, HTTP, HTTPS, FTP, DNS, TELNET y DHCP.