Exploración, Monitoreo y Seguridad en Redes bajo el Sistema Operativo Linux

Prof. Wilmer Pereira
UCAB/USB
http://www.ldc.usb.ve/~wpereira
wpereira@ucab.edu.ve, wpereira@usb.ve

1. Resumen

Este tutorial es una introducción teórico práctica para mostrar los fundamentos de los servicios de redes y protocolos que, a través de Linux, permite la búsqueda de información en Internet y monitoreo de tráfico respetando principios básicos de seguridad. Estas funcionalidades constituyen para Linux sus fortalezas lo que hace que sea muy utilizado, como sistema operativo, en los servidores corporativos.

2. Contenido

Teoría

1. Direccionamiento por capas:
   1.1. Puerto Físico
   1.2. MacAddress
   1.3. IP
   1.4. Puerto lógico
   1.5. Dominio
2. Filosofía Cliente/Servidor
3. IPv4 e IPv6
4. Dispositivos:
   4.1. Concentradores
   4.2. Switches
   4.3. Enrrutadores
5. Servicios de red:
   5.1. `ICMP`
   5.2. `ARP`
   5.3. `DHCP`
   5.4. `NAT`
   5.5. `DNS`
6. Principios de protocolos
7. *Sniffing* y monitoreo de red (`SNMP`)
8. Seguridad en linux

Práctica

1. Conexión remota y transferencia de archivos:
   1.1. /etc/services
   1.2. ssh
   1.3. telnet
   1.4. sftp
   1.5. scp
   1.6. write y talk
2. Exploración y consulta en red
   2.1. traceroute
   2.2. nmap
   2.3. nslookup
   2.4. whois
3. *Sniffing*
   3.1. wireshark
   3.2. tcpdump
4. Seguridad en Linux
   4.1. sudo
   4.2. umask
   4.3. /etc/passwd
   4.4. /etc/shadow

3. Duración y público

El tutorial será dictado con sesiones de teoría intercaladas con la práctica. Está previsto para ocho (8) horas con 2 sesiones prácticas en la mañana y 2 en la tarde dirigido a todo público con conocimientos básicos de linux y redes. La cantidad de personas máxima para que el curso se dicte en las mejores condiciones el tutorial no debería exceder las 20 personas de preferencia una persona por máquina.

4. Requerimientos del laboratorio

Cada máquina debe tener conexión a Internet y se deben crear cuentas para cada participante con privilegios de administrador (`root`) mínimo para los siguientes comandos:

- Ejecutar *wireshark*
- Visualizar algunos archivos del sistema operativo: shadow y sudoers
- Cada máquina debe tener instalados los servidores de ssh, telnet y sftp
- Montado los programas: wireshark y traceroute y whois habilitados

Prof. Wílmer Efrén Pereira González PhD

Nacimiento: 13/02/61, Caracas

Dirección Trabajo: Universidad Católica Andrés Bello, Urb. Montalbán
Escuela de Ingeniería Informática, Caracas.
Universidad Simón Bolívar, Valle de Sartenejas
Dpto. de Computación, Baruta, Caracas.

Teléfono Trabajo: UCAB – 4074407, USB – 9063241

Educación

- **Post-doctorado** en la Universidad de Pierre et Marie Curie, Francia. En el seno del equipo de investigación "Sistemas Multiagentes" del Laboratorio de Informática de Paris VI (LIP6), Sep/09 - Jul/10.
- **Doctorado en Informática** (Mención de Honor) en la Universidad de Rennes I, Francia. En el área de Inteligencia Artificial: "Una Lógica Modal para el Tratamiento de la Incertidumbre", Sep/88 - Jul/92.
- **Post-Diploma en Redes de Computadoras** en la Escuela Superior de Electricidad de Rennes, Oct/87 - Jul/88.
- **Diploma de Ingeniero en Computación** de la Universidad Simón Bolívar, Caracas, Sep/79 - Jul/85.

Experiencia Laboral

- **Universidad Católica Andrés Bello**, profesor a dedicación en Ingeniería Informática y Maestría en Sistemas de Información desde Abr/00.
- **Universidad Simón Bolívar**, profesor convencional en pregrado de Ingeniería en Computación, Especialización en Telemática y Maestría en Ciencias de la Computación desde Abr/00.
- **Universidad Central de Venezuela** (Caracas). Profesor de la Maestría en Ciencias de la Computación desde Sept/05.
- **Université de Dauphine** (Paris, France), Profesor por contrato para el *Diplôme Universitaire de Gestion et d'Economie Appliquée* (DUGEAD), segundo año, tercer semestre, de Ene/10 a Jul/10.
- **Universidad Centro Occidental Lisandro Alvarado** (Barquisimeto). Profesor invitado, Ene/96 - Jul/96, Dic/01-Abr/02 y Ene/05-Abr/05.
- **Universidad de Rennes I** (Francia). Profesor-investigador. Feb/92 - Ago/93.
- **Escuela de Organización Industrial** (España). Profesor Internacional. Oct/00 – actual.
- **Oficina Central de Estadísticas e Informática**, responsable de la unidad de lectoras ópticas. May/88-Jul/88

Publicaciones y Seminarios

Expositor de 20 artículos arbitrados en conferencias internacionales, 26 artículos en conferencias nacionales y ponente invitado en seminarios y jornadas estudiantiles en la USB, UCV y UCAB en informática y telecomunicaciones.

Méritos y Afiliaciones

- Presidente y fundador de la Sociedad Venezolana de Computación desde Sep/2011.
- Investigador acreditado por el Programa de Estímulo al Investigador (PEI) desde Jul/2011
- Miembro del Comité Editorial de la Revista Venezolana de Computación (ReVeCom) desde Jul/2013.
- Responsable de Grupo de Investigación de Inteligencia Artificial y Robótica de la UCAB.
- Director de la Revista de la Facultad de Ingeniería de la UCAB (Tekhné) desde Sept/2008.
- Miembro del comité de programa de 15 conferencias internacionales.
- Participante del proyecto iberoamericano IDEAS (Ingeniería en Ambientes de Software) Patrocinado por el CYTED (Agencia de Cooperación Española) y coordinador de un proyecto MAPFRE sobre seguridad y 3 proyectos CDCHT (Consejo de Desarrollo Científico, Tecnológico y Humanístico) en robótica
- Primer lugar en el Premio al trabajo de Investigación UCAB edición 2006-2007, con el trabajo titulado "*Evaluación de Arquitecturas de Software Locales y Distribuidas en Robótica Autónoma y Teledirigida*". También en la edición 2004-2005 con el trabajo: *Elementos Difusos para un Modelo Orientado a Objetos*.
- Presidente del Comité Organizador Conferencia Nacional en Computación, Informática y Sistemas (CoNCISa2014), UCAB, Oct/2014.
- Miembro del Comité de Asesores de la Revista Técnica de la Facultad de Ingeniería de la Universidad del Zulia desde Ene/12 -- actual.