ETS de la asignatura de Administración de Servicios en Red

REQUISITO:
Llevar en un CD o DVD (el cual se entregará al finalizar el examen) y en una USB (adicional al CD para facilidad, en caso de que se ocupe la unidad de CD con el examen), los archivos necesarios para poder importar en virtualbox un servidor (o dos en caso de que lo considere necesario) con los siguientes servicios, tanto como servidor (o agente) y cliente (o gestor):

http, ftp, tftp, snmp, dns, y la aplicación wget

Adicionalmente se pueden considerar los archivos para importar maquinas virtuales con el software necesario para realizar algunas de las funciones que se listan adelante.

NOTA: por cuestiones de espacio en el CD/DVD y de licenciamiento, el software a utilizar será de licencia libre o de creación propia.

SOBRE LA EVALUACIÓN:

Los profesores de la asignatura, en busca de un enfoque práctico de la asignatura y de uniformizar más los contenidos, hemos decidido incluir dentro de la evaluación los rubros que se pueden encontrar al final del documento:

http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-453503.html

Los cuales se listan a continuación:

Auto-evaluación de la gestión de fallos

¿Tiene la organización un ping poller que considere una falla cuando un dispositivo no responde a un ping?
¿Se monitorizan los traps SNMP, y traps específicos son considerados como fallas?
¿Se monitorizan los registros del sistema (syslog) y mensajes específicos dan lugar a una falla?
¿Se supervisa el estado del hardware del dispositivo y se consideran fallas por eventos como falla en el suministro de energía, falla del sistema redundante, temperaturas del dispositivo, etc.?
¿Se envían los fallos al sistema de servicio de atención y se administran mediante un proceso de gestión de incidentes?

Autoevaluación de la gestión de la configuración

¿La información de inventario se recopila de la red incluyendo todos los chasis, módulos y números seriales?
¿Se recopilan las configuraciones de los dispositivos regularmente?
¿Se detectan, informan e investigan los cambios en la configuración de los dispositivos?
¿Existe una plantilla de configuración básica bien documentada?
¿Pueden las configuraciones en ejecución ser auditadas contra las plantillas de configuración?

Autoevaluación de la gestión contable

¿Está habilitada la exportación de NetFlow o equivalente en todos los dispositivos?
¿Se recogen y almacenan datos NetFlow o equivalentes?
¿Se clasifican los datos almacenados según el tipo de servicio o la aplicación?
¿Pueden los datos recopilados ser atribuidos a usuarios o grupos de usuarios específicos?
¿Se hacen ajustes contables por violaciones de SLA?

Autoevaluación de la gestión del rendimiento

¿Se consultan los dispositivos para las estadísticas de las interfaces y los resultados se almacenan para el análisis histórico?
¿Son los dispositivos consultados para saber la utilización del CPU y las estadísticas del uso de memoria; y los resultados se almacenan para su análisis histórico?
¿Se puede producir un informe de los 10 enlaces WAN con más carga?
¿Se comprueban los umbrales de los datos de rendimiento recopilados y cuando se exceden dichos umbrales se considera una falla?
¿Se presentan informes empresariales para la planificación de la capacidad, apoyados por el análisis de los enlaces WAN y las métricas de rendimiento de los dispositivos?

Autoevaluación de la gestión de la seguridad

¿Se utiliza TACACS o RADIUS para la administración de dispositivos, autorización, acceso, y contabilidad?
¿Existen diferentes niveles de acceso y autorización para la mesa de servicio, los operativos y el personal de apoyo de tercer nivel?
¿Los syslog de los dispositivos se alimentan en un servidor syslog común?
¿Se monitorizan y / o revisan los registros de servidores, enrutadores, conmutadores, cortafuegos (firewalls) y aplicaciones? Ya sea manualmente o empleando algún software para este fin.
¿Se puede implementar un cambio de configuración global en todos los dispositivos en menos de 24 horas? (Como la solución de configuración de CERT o PSIRT)

Por lo que algunos de estos elementos se evaluarán de manera conjunta a los elementos que se han venido evaluando como la configuración de equipos de comunicaciones, interacción con agentes y gestores SNMP, etc.

SOBRE EL PROYECTO A ENTREGAR COMO REQUISITO:

Dado que la escuela no cuenta con licencia para software con la funcionalidad indicada (y que el objetivo de un ingeniero no es manejar paquetería) se ha optado por la búsqueda de software de licencia libre o de creación propia que cubra dicha funcionalidad. Por tal motivo el examen se desarrollara con el live cd RAIZO que es un sistema operativo configurado para hacer emulaciones con la herramienta GNS3, al cual se le han agregado herramientas como RCPLive, Observium, NetEm, Zeroshell, etc. Por lo que, para la realización del examen, se tienen dos opciones:

- Que la (o las) maquinas virtuales que entregue como requisito ya cuenten con las herramientas que le permitan realizar las funciones que se listaron con anterioridad.

- Que se empleen las herramientas que encontrara en RAIZO durante el examen para implementar dicha funcionalidad (NetSnmp, rrdtool, pmacct, entre otras).

SOBRE UN POSIBLE TALLER DE PREPARACIÓN PARA EL ETS.
Considerando que a lo largo de la impartición de la asignatura la visión sobre la misma ha venido evolucionando, que lo importante de la asignatura es poder desarrollar las practicas de gestión, más resulta complicado desligar estas de alguna herramienta particular, y que ha habido varios alumnos que lo han solicitado, se ha pensado en realizar un taller de preparación para el ETS.

Cabe aclarar que no se trata de hacer un curso para pasar en una semana lo que no se pudo pasar en un semestre y que los conocimientos de la unidad de aprendizaje (al menos desde el punto de vista de su servidor) no se transmiten eficientemente mediante un plumón y un pizarrón, sino que hay que poner manos a la obra para desarrollar las habilidades y actitudes adecuadas sobre los contenidos de la unidad de aprendizaje.

Por lo que, de realizarse, el taller pretendería dar la oportunidad de familiarizarse con RAIZO y las demás herramientas de las que se dispondría durante el examen, y podría emplearse para terminar el proyecto a entregar en el ETS; sin embargo, para esto, se requiere que los interesados se documenten (Lean y comprendan sobre lo que se necesita realizar y como se puede realizar) y asistan al taller para aterrizar lo aprendido.

En caso de realizarse seguramente se tendra un cupo limitado, por lo que se les pide que envíen un correo a eduardogutierrezaldana@gmail.com con sus datos y asunto: “curso ets asr” para crear una lista de interesados a los cuales de dará prioridad en función del orden de llegada de su correo.

SOBRE EL ETS.

Dado que se trata de un examen de índole práctico es posible que se altere la hora o fecha del mismo en función de la disponibilidad de un laboratorio para su realización. Por lo que los invito a revisar los avisos que se pudieran generar al respecto, en el departamento de Ingeniería en Sistemas de la Escuela, la ponderación de las características del proyecto aun esta por definirse entre los profesores de la asignatura, pero es seguro que no sera necesario cumplir con todos los rubros para pasar, así como que la ponderación de configuración de software de otras personas sera menor a la que se tendrá si la funcionalidad se obtiene por softtware de desarrollo propio.

ALGUNAS REFERENCIAS QUE PODRÍAN RESULTARLES DE INTERÉS:

http://blog.hermione.de/?p=67
http://developers-club.com/posts/135086/
http://hints.jeb.be/2009/12/04/trend-prediction-with-rrdtool/
https://www.terena.org/activities/tf-noc/meeting4/slides/111012-virt-ipv6-wp.pdf
http://www.pmacct.net/

RECOMENDACIONES:

Por motivos de licencia se usará el software RCP100 para emular los enrutadores (en una versión en live CD denominada rcplive), el cual presenta una interfaz de consola muy similar a la de algunos enrutadores comerciales, por lo que se recomienda familiarizarse con la configuración de los mismos.

Es probable que se emplee el software GNS3 para la integración de los servicios y los equipos utilizados para la administración mediante el livecd raizo (https://sourceforge.net/projects/live-raizo/) por lo que es recomendable practicar en cada uno de los ambientes mencionados la configuración de los elementos en red.

De igual manera se recomienda practicar con los comandos para consultar y modificar una MIB, por ejemplo con el software net-snmp (snmpget, snmpset, snmpwalk y snmptrapd); y la inclusión de estos comandos en scripts.

Se puede solicitar obtener conclusiones a partir de datos obtenidos mediante snmp, ya sea en un archivo de texto o en un archivo rrd (de la herramienta rrdtool).

Así mismo es recomendable saber localizar los datos a administrar por lo que se sugiere revisar los siguientes documentos:
• SNMP – SMI: Definida en el RFC 1155, es la estructura de información de gestión (SMI).
• MIB-I: Definida en el RFC 1156, históricamente usada con CMOT pero no vale para SNMP.
• SNMPv2-SMI: Definida en el RFC 2578, es la estructura de información de gestión versión 2 (SMIv2)
• MIB-II: Definida en el RFC 1213, es la MIB para gestión de redes internet (basadas en TCP/IP).
•SNMPv2-MIB: Definida en el RFC 3418 es una MIB para la versión 2 de SNMP (SNMPv2).
•TCP-MIB: Definida en el RFC 4022, es una MIB para TCP.
•UDP-MIB: Definida en el RFC 4113, es la MIB para UDP.
•IP-MIB: Definida en el RFC 4293, es la MIB para IP.
•IF-MIB: Definida en el RFC 2863 es la MIB del grupo de interfaces.
•ENTITY-MIB: Definida en el RFC 4133, es la MIB de entidades versión 3.
• ENTITY-STATE-MIB: Definida en el RFC 4268, es la MIB de los estados de las entidades.
•ALARM-MIB: Definida en el RFC 3877, es una MIB que define alarmas.
(https://www.rfc-editor.org/info/rfc1156 por ejemplo)

Informes: Profr. Eduardo Gutiérrez Aldana