UNIVERSIDAD SAN IGNACIO DE LOYOLA

La Universidad que forma emprendedores

CPEL CARRERAS UNIVERSITARIAS PARA PERSONAS CON EXPERIENCIA LABORAL

18

TOPICOS DE SEGURIDAD INFORMATICA - PRÁCTICA N° 1 2011 – II M1

Profesor: Jorge Reátegui **Duración:** 20 min

Apellido y Nombre: [redacted] **Fecha:** 19 May 2011

Indicaciones:

1. Sea cuidadoso con su ortografía y redacción. Este aspecto formará parte de su calificación.
2. Sea breve y objetivo en su respuesta utilice datos y cifras para respaldarlas. No se califica por extensión, si no por calidad de respuesta.

1. Marque cual de las afirmaciones es falsa: **(10 puntos)**

La conexión remota segura a nuestra red:
( ) Requiere solo una VPN
( ) Requiere una VPN y en adición Strong Authentication (tal como un token)
( ) Por ningún motivo debe permitirse que se conecten a nuestra red, de manera remota
(X) Ninguna de las anteriores

La Familia ISO 27001:
( ) Contiene la ISO 27001 que se puede Certificar
(X) Contiene la ISO 27002 que es igual a la Peruana NTP ISO 17799:2007
( ) Contiene las mejores prácticas para la administración integral de la Seguridad de Información
( ) Ninguna de las anteriores

El ISO 27002 se ha vuelto el estándar de seguridad de información defacto :
( ) Porque es el más completo en la actualidad
( ) Porque es aplicable a grandes y pequeñas Organizaciones
( ) Porque es internacional, ya que está respaldado por la ISO
(X) Ninguna de las anteriores

El Packet Sniffing:
( ) Es usado para capturar la información que circula en una red
( ) Requiere que se ponga la tarjeta de red en "modo promiscuo"
( ) Para burlar los switches usa la técnica de ARP Poisoning (envenanamiento de tabla ARP)
(X) Ninguna de las anteriores

Un Firewall:
( ) Protege principalmente nuestra red de la Internet
( ) Protege redes adicionales llamadas DMZ
(X) No es necesario si se tiene un IPS de última generación
( ) Ninguna de las anteriores

Para cada paquete que pasa por un FW, las reglas:
( ) Es indispensable ordenarlas como especificas primero y generales después
( ) Se verifican correlativamente desde la primera
( ) Se revisan hasta encontrar la que hace match y las siguientes reglas ya no se verifican
(X) Ninguna de las anteriores

Un Firewall en un equipo del tipo UTM (Unified Threat Management):

( ) Permite tener otros elementos de seguridad en un solo equipo
(X) Si el equipo del UTM deja de funcionar, los elementos pueden seguir brindando el servicio
( ) Permite ahorrar costos
( ) Ninguna de las anteriores

La Seguridad de Información:

( ) Busca que la información de la Organización se maneje, con un nivel de riesgo aceptable
( ) Tiene como pilares a la Confidencialidad, Integridad y Disponibilidad
(X) Para una empresa que se dedique a las TI, es la razón de ser del negocio
( ) Ninguna de las anteriores

La regla del FW "any any any drop":

(X) Debe ser la primera regla
( ) Hace match con cualquier paquete que pase por el FW
( ) Nos permite parar los paquetes que no lleguen a hacer match con ninguna de las regla existentes
( ) Ninguna de las anteriores

Un IDS:

( ) Se comporta como un packet sniffer
( ) Verifica el tráfico que el FW, dejo pasar
(X) Permite que el tráfico pase a través de él
( ) Ninguna de las anteriores

2. Haga el match, colocando las letras de las definiciones superiores correspondientes, entre los paréntesis de los términos que siguen luego. Existen términos en la parte inferior que quedaran sin match: **(7 puntos)**

A) Utiliza la misma semilla o llave para cifrar como para descifrar
B) Utiliza una llave para cifrar y la pareja de dicha llave para descifrar
C) Por defecto se usa para cifrar la conexión con http en un browser
D) Por defecto se usa para cifrar la conexión entre 2 redes, mediante VPN
E) Permite impedir que un hosts no autorizado se pueda conectar a una red
F) Requiere una separación geográfica que impida el efecto de una misma amenaza
G) Se le contrata para un Ethical Hacking

(A)	Cifrado simétrico	( )	Spoofing
( )	ARP Poisoning	(B)	Cifrado asimétrico
(C)	SSL	( )	IPS
(F)	Desaster Recovery	(E)	VLAN
( )	Port Scanning	(G)	White Hat
( )	NAC	(D)	IPsec

3. Marque con (V) Verdadero o (F) Falso para las siguientes frases **(3 puntos)**

(F) Un Honeypot permite que el trafico pase a través de él, para analizarlo
(F) En el FW no se ejecuta una regla "especifica" colocada luego de una "general", si ambas están relacionadas
(V) Indecopi es la entidad que representa al Perú ante la ISO
(F) Un ADS es un tipo de Firewall
(V) Los tipos de IDS son: Network based y Host based
(V) Un IPS captura el tráfico que el FW deja pasar