Kinshu Technologies

emqu

Certificación en Ciberseguridad y Cómputo Forense

Aprende de la mano de expertos, con los estándares nacionales e internacionales.

Certificación Avalada por:

STPS
SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL

ESTADOS UNIDOS MEXICANOS

INICIAMOS EL 15 DE ABRIL

55 7323 8922 lms.emqu.net

I.O Conceptos de Redes

II Propósito y uso de puertos y protocolos de red.

• Protocols and ports
·SSH 22
·DNS 53
·SMTP 25
·SFTP 22
·FTP 20,21
·TFTP 69
·TELNET 23
·DHCP 67,68
·HTIP8o
·HTIPS 443
·SNMP161
·RDP 3389
·NTP 123
.51p 5060,5061
·SMB445
·POP 110
·IMAP143
·LDAP 389
·LDAPS 636
·H.3231720
• Protocol types
· ICMP
· UDP
·TCP
· IP
• Connection-oriented vs. connectionless

III Conceptos como, aplicaciones, protocolos, y servicios entendiendo las capas del modelo OSI.

• Layer 1- Physical
·Layer 2- Data link
• Layer 3- Network
• Layer 4- Transport
• Layer 5 - Session
• Layer 6- Presentation
• Layer 7- Application

II Conceptos y Características de Routing y Switching.

• Properties of network traffic
·Broadcast domains
·CSMNCD
·CSMNCA
·Collision domains
·Protocol data units
·MTU
·Broadcast
·Multicast
·Unicast
• Segmentation and interface properties
·VLANs
·Trunking {8o2.1q)
·Tagging and untagging ports
·Port mirroring
·Switching loops/spanning tree
·PoE and PoE+ {8o2.3af,802.3at)
·DMZ
·MAC address table
·ARP table
·Routing
·Routing protocols (IPV4 and 1Pv6)
· Distance-vector routing protocols
· RIP
· EIGRP
· Link-state routing protocols
· OSPF
· Hybrid
· BGP
·Routing types
· Static
· Dynamic
· Default
• 1Pv6 concepts
· Addressing
· Tunneling
·Dual stack
·Router advertisement
·Neighbor discovery
• Performance concepts
·Traffic shaping
·QoS
Diffserv
·CoS
• NAT/PAT
·Port forwarding
• Access control list
• Distributed switching
• Packet-switched vs.circuit·switched network
·Software-defined networking

II Escenario apropiado, componentes y configuración de IP.

Private vs. public
• Loopback and reserved
• Default gateway
• VirtuaiiP
• Subnet mask
• Subnetting
- Classful
- Classes A, B,C, D,and E
- Classless
- VLSM
- CIDR notation (1Pv4 vs. 1Pv6)
• Address assignments
-DHCP
- DHCPv6
-Static
- APIPA
- EU164
- IP reservations

Características de los tipos y tecnologías topológicos de red.

·Wired topologies
- Logical vs. physical
- Star
- Ring
- Mesh
- Bus

· Wireless topologies
- Mesh
- Ad hoc
- Infrastructure

·Types
- LAN
- WLA
- MAN
- WAN
- CAN
- SAN

·Technologies that facilitate the Internet of Things (loT}
-Z-Wave
- Ant+
- IR
-RFID
- 802.1

Implementación y configuración correcta de redes inalámbricas (WiFi).

· 802.11standards
- a
- b
-g
- n
-ac

• Cellular
- GSM
- TDMA
- CDMA

• Frequencies
- 2.4GHz
-s.oGHz

·Speed and distance requirements
• Channel bandwidth
• Channel bonding
• MIMO/MU-MIMO
• Unidirectional/omnidirectional
·Site surveys

Conceptos básicos y propósito de servicio en la nube.

• Types of services
- SaaS
- PaaS
- laaS

·Cloud delivery models
- Private
- Public
- Hybrid

• Connectivity methods
• Security implications/considerations
• Relationship between local and cloud resources

Funciones de los servicios de redes.

• DNS service
- Record types
- A, AAA
- TXT (SPF,DKIM}
- SRV
- MX
- CNAME
- NS
- PTR
- Internal vs. external DNS
- Third-party/cloud-hosted DNS
- Hierarchy
- Forward vs. reverse zone

• DHCP service
- MAC reservations
- Pools
- IP exclusions
- Scope options
- Lease time
-TIL
- DHCP relay/IP helper
•NTP
•IPAM

2.O Infraestructura

II Tipos de cable, configuración y uso.

·Media types
- Copper
- UTP
- STP
- Coaxial
- Fiber
- Single-mode
- Multimode
·Plenum vs. PVC
• Connector types
- Copper
- R]-45
- Rj-11
- BNC
- DB-g
·DB·2S
- F-type
- Fiber
- LC
- ST
- sc
- APC
- UPC
- MTRJ
·Transceivers
- SFP
- GBIC
- SFP+
- QSFP
- Characteristics of fiber transceivers
- Bidirectional
- Duplex
·Termination points
- 66 block
-110 block
- Patch panel
- Fiber distribution panel
·Copper cable standards
-Cat3
- cats
- cat se
- Cat6
- Cat 6a
- Cat?
- RG-6
- RG-59
·Copper termination standards
- TINEIA S68a
- TINEIA 568b
- Crossover
- Straight-through
• Ethernet deployment standards
- lOOBaseT
- lOOOBaseT
- lOOOBaseLX
- lOOOBaseSX
- lOGBaseT

II Implementación de equipo dentro de una red, instalación y configuración.

• Firewall
·Router
• Switch
·Hub
• Bridge
•Modems
·Wireless access point
• Media converter
·Wireless range extender
• VoiP endpoint

II Propósitos y los casos de uso de dispositivos de red avanzados.

· Multilayer switch
• Wireless controller
• Load balancer
•IDS/IPS
·Proxy server
• VPN concentrator
• AAA/RADIUS server
• UTM appliance
• NGFW/Layer 7 firewall
•VoiPPBX
• VoiP gateway
• Content filter

II Propósito de virtualización y tecnologías de almacenamiento.

• Virtualnetworking components
-Virtual switch
-Virtual firewall
- Virtual NIC
-Virtual router
- Hypervisor
• Network storage types
-NAS
- SAN
·Connection type
- FCoE
- Fibre Channel
- iSCSI
-InfiniBand
•)umbo frame

II Tecnologías WAN.

·Service type
-ISDN
- T1/T3
-El./E3
- OC-3- OC-192
-DSL
-Metropolitan Ethernet
-Cable broadband
-Dial-up
- PRI
·Transmission mediums
- Satellite
-Copper
-Fiber
-Wireless
·Characteristics of service
-MPLS
-ATM
-Frame relay
- PPPoE
-PPP
-DMVPN
-SIP trunk
• Termination
-Demarcation point
-CSU/DSU
-Smart jack

3.O Materia Legal en Informática.

· Normativas Internacionales para el manejo de evidencia.
· Planeación y Planimetría
· Manejo de cadena de custodia
· Diferencia entre reporte pericial y Dictamen
· Metodología de trabajo
· Juicio Oral.
· BYOD

4.O Métodos de extracción de evidencia en equipos de cómputo.

· Uso de Herramientas gratuitas
· Uso de Herramientas con licencia
· Extracción de evidencia
· Análisis de Tráfico en equipos de cómputo
· Análisis de información
· Principales Ataques
· Investigación de correos electrónicos.

5.O Archivos eliminados y métodos para su recuperación

· Herramientas de software libre
· Herramientas de licencia de paga
· Hardware para copia de imagen forense
· Recuperación de archivos en equipos de cómputo.
· Medios de almacenamiento

6.O Fallas en discos duros

· Herramientas de software libre
· Herramientas de licencia de paga
· Hardware para copia de imagen forense
· Recuperación de archivos en equipos de cómputo.
· Medios de almacenamiento

7.O Sistemas de Archivos

. Organización de los datos
· Particiones de disco
· Datos alojados o datos sin alojar
· Capas de Metadatos
· Sistemas de archivos ext2/3/4, NTFS y FAT 32/16
· Esteganografía

8.O Informática Forense dentro de la empresa

· Análisis de infraestructura
· Recolección de evidencia volátil y no volátil
· Generación de imágenes bit a bit
· Montaje y análisis de herramientas.

9.O Informática Forense en Linux

· Comandos en búsqueda de sistema sospechoso
· Volcado de memoria
· Historial y procesos
· Redes activas
· Interface de red
· Comparación de hash
· Archivos sospechosos
· Copia Forense en Linux

10.O Pruebas de Penetración con Kali Linux

· Obtener información de forma pasiva
· Manejo de información
· Maltego
· Google Hacking
· NMAP
· Zenmap
· Ataques a Passwords
· Ataques de Red
· Ingeniería Social

11.O Informática Forense en equipos móviles.

· Herramientas Forenses Software
· Obtener una imagen de un equipo móvil
· Análisis de información
· Recopilación y autenticación de logs
· Análisis de aplicaciones

Duración
El curso tiene una duración de 40hrs
Dividido en 2 Módulos.

Módulo 1: Redes y Seguridad.

Módulo 2: Cómputo Forense.

Inversión:

Iniciamos	*Inversión*	*Enero 20%* de descuento hasta marzo 30
15 de marzo	***$18,000.00 MXN***	***$14,400.00 MXN***

Febrero 10% de descuento hasta 14 de abril	*30% de Descuento*
$16,200.00 MXN	***Para Servidores Públicos***

Certificación Avalada por:

STPS
SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL

¿A quién va dirigido?

El curso va dirigido a personal dedicado al área de Tecnología de la información, cuerpos del orden que desean conocer las medidas de seguridad en delitos cometidos con tecnología de la información y comunicaciones, utilizar estos hallazgos como evidencia y poder manipular y almacenar esta información para su correcta exposición. Es importante tener conocimientos de Redes y computación, pero no es necesario que estos conocimientos sean muy extensos, se explicarán todos los puntos de este temario, y se deja una peque- ña brecha de tiempo para poder exponerlos en caso de que algunos conceptos hayan sido olvidados o poco usados, todo el temario se relaciona con el hecho de obtener información que pueda servir para el objetivo que es Obtener, Preservar, Analizar y Almacenar evidencia.

Objetivo

Al finalizar la certificación los alumnos serán capaces de entender y crear una red LAN utilizando herramienta real tanto conexión por cable como inalámbrica, analizar dichos datos y poder entender que es lo que se realiza. La Certificación está basada en Ciberseguridad y Cómputo Forense en la cual analizaremos dicha red y temas que son de interés para que se pueda comprender los términos como correos electrónicos, dispositivos móviles (tabletas y Teléfonos Celulares), equipo de cómputo, su recuperación y análisis de dichos dispositivos entre otros.

Certificaciones Internacionales

Las herramientas que utilizamos son las mismas herramientas que actualmente utilizan el FBI, Agencia de Seguridad Nacional en Estados Unidos, Centro de Inteligencia de Estados Unidos, Agencias de Seguridad de muchos países. Es importante que la metodología que enseñamos se entienda que cumple con los estándares tanto nacionales como internacionales, esto debido a que muchos temas pueden ser apelados en juzgados de índole internacional, por lo que los hallazgos que se obtengan de dichos aná lisis a equipo de cómputo puede ser utilizada en juicios internacionales.

Certificación con validez oficial por parte de STPS
KTE-170306-HW4-0013

STPS
SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL

Temario

Duración
El curso tiene una duración de 40hrs
Dividido en 2 Módulos.

Módulo 1: Redes y Seguridad.
Módulo 2: Cómputo Forense.

Expertise del Personal Certificador

Módulo Redes y Seguridad.
Ingeniero en informática Juan Carlos Velasco

- CCNA SP - Cisco Network Associate for Service Provider
- CCNP SP - Cisco Network Professional for Service Provider
- Cisco Advanced Services Expert
- PMP -Project Management Professional Certification
- ITIL V3 Fundations
- AWS - Certified Salutions Arquitect Associate
- ATT Security Advisor

Módulo Cómputo Forense.
M.S.I Daniel Esquivel

- Maestría en Seguridad Informática
- Certificado en Gestión de la Seguridad y Marco Legal
- Certificado en Seguridad en Redes, Sistemas y Aplicaciones
- CEH - Certified Ethical Hacking
- CHFI - Certified Hacking Forensics Investigator
- SANS Institute
- CCNA - Cisco Certificated Network Associate
- Mobiledit Training Partners

Valor Curricular

Actualmente Kinshu Technology es partner de Mobiledit empresa que apoya en la recopilación de evidencia a Agencias de Seguridad de todo el mundo, Asesor de empresas de seguridad, Perito en Informática Forense para el Tribunal de Justicia de la CDMX y otras instancias de Gobierno, así como perito oficial de empresas privadas como SOFTTEK y algunas que no pueden ser mencionadas debido a cláusulas de confidencialidad.

“Estamos junto a nuestros clientes y los capacitamos para construir casos más sólidos utilizando tecnología avanzada para descubrir la evidencia digital”

Requerimientos mínimos recomendados en el equipo de cómputo.
160 GB en espacio del disco duro (recuerden que utilizaremos espacio para virtualizaciones)
4 GB en RAM
Procesador Intel i3 - Rayzen 3 o superior

Al finalizar los módulos, todos los participantes recibirán un diploma con valor curricular por parte de Kinshu Technologies con el permiso de la STPS y de Mobiledit empresa de software Forense con certificados y pruebas de competencia en software de extracción de equipos móviles realizadas por el departamento de Homeland Security (Seguridad Nacional) en Estados Unidos