Introducción a la ciberseguridad
Actividades y recursos adicionales

Capítulo 1: Recursos

Comprensión de problemas para el sector bancario

El sitio Tapestry Network afirma que los miembros de la Red de servicios financieros desarrollaron estos reportes para abordar los problemas que enfrentan las instituciones financieras. Visite el siguiente enlace y explore los temas relacionados a los problemas de los servicios financieros:

http://www.tapestrynetworks.com/issues/financial-services/

Administración de riesgos para cadenas de abastecimiento

El siguiente enlace hace referencia a un documento que explica cómo puede un proveedor comprometer la seguridad de la red y proporcionar otros recursos relacionados con la administración de riesgos de la cadena de abastecimiento:

http://measurablesecurity.mitre.org/directory/areas/supplychainrisk.html

¿Delitos cibernéticos o guerra cibernética?

Los delitos cibernéticos son el acto de cometer un delito en un entorno cibernético; sin embargo, un delito cibernético no constituye necesariamente un acto de guerra cibernética. La guerra cibernética puede incluir varias formas de sabotaje y espionaje con la intención de atacar una nación o un gobierno. El siguiente artículo describe la diferencia entre la ciberdelincuencia y la guerra cibernética:

http://www.pcworld.com/article/250308/when_is_a_cybercrime_an_act_of_cyberwar_.html

Capítulo 2: Recursos

Cómo robar un banco: un recorrido por la ingeniería social

http://www.csoonline.com/article/692551/how-to-rob-a-bank-a-social-engineering-walkthrough

XSS con aplicación web vulnerable

En este tutorial, Dan Alberghetti demuestra scripts (XSS) o inyección de código en una aplicación web que contiene una vulnerabilidad de aplicación web conocida.

http://www.danscourses.com/Network-Penetration-Testing/xss-with-a-vulnerable-webapp.html

Pionero en Google Hacking

Johnny Long fue pionero del concepto Google Hacking. Un reconocido experto en seguridad, ha escrito y contribuido en muchos libros sobre la seguridad informática. Su libro *Google Hacking for Penetration Testers* es una lectura obligatoria para cualquier persona interesada en el campo de Google Hacking. También tiene un sitio web dedicado a brindar asistencia a las organizaciones no lucrativas y de capacitación para los ciudadanos más pobres del mundo.

http://www.hackersforcharity.org

© Cisco y/o sus filiales. Todos los derechos reservados. Información confidencial de Cisco

Centro de protección contra malware de Microsoft

Este sitio de Microsoft proporciona una herramienta de búsqueda de información sobre un determinado tipo de malware

http://www.microsoft.com/security/portal/threat/threats.aspx

Malware Flame

Stuxnet es uno de los malware más publicados y desarrollado con el fin de la guerra cibernética. Sin embargo, existen muchas otras amenazas menos conocidas. Este artículo analiza el malware conocido como Flame, que se desarrolló como herramienta de espionaje para atacar máquinas principalmente en Irán y otras partes de Oriente Medio. Para conocer más sobre este malware, visite el siguiente enlace:

http://www.wired.com/threatlevel/2012/09/flame-coders-left-fingerprints

Malware Duqu

Otro malware, probablemente relacionado con Stuxnet, es Duqu. Duqu es un malware de reconocimiento pensado para obtener información sobre un sistema de control industrial desconocido, con el fin de un ataque futuro posible. Para conocer más sobre Duqu y la posible amenaza que impone, visite el siguiente enlace:

http://www.wired.com/threatlevel/2011/10/son-of-stuxnet-in-the-wild

Catálogo de ataques de la NSA

La Agencia de Seguridad Nacional (NSA, Agencia de Seguridad Nacional) de los Estados Unidos desarrolló y mantiene un catálogo de ataques para prácticamente cualquier software, hardware y firmware importante. Mediante estas herramientas y otros ataques, la NSA puede llevar un registro de prácticamente cada nivel de nuestra vida digital. Para conocer más sobre el catálogo de ataques de la NSA, visite el siguiente enlace:

http://leaksource.wordpress.com/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/

Equipo de Preparación de Emergencia Informática de los Estados Unidos (US-CERT)

Como parte del Departamento de Seguridad Nacional, el Equipo de Preparación de Emergencia Informática de los Estados Unidos (US-CERT) se esfuerza por mejorar la postura de ciberseguridad del país, compartir información cibernética y administrar los riesgos cibernéticos mientras protege los derechos de los estadounidenses. Para conocer más sobre el US-CERT, visite el siguiente enlace:

https://www.us-cert.gov/

Si desea información similar para un país en específico, visite el siguiente enlace y busque por país.

http://www.cert.org/incident-management/national-csirts/national-csirts.cfm

Capítulo 3: Recursos

Todos los dispositivos pueden hackearse

El uso de la electrónica dentro del cuerpo humano lo convierte en un objetivo cibernético, al igual que cualquier computadora o teléfono celular. En la conferencia TEDx MidAtlantic de 2011, Avi Rubin explicó cómo los hackers están comprometiendo automóviles, teléfonos inteligentes y dispositivos médicos. Advirtió sobre los peligros de un mundo cada vez más “hackeable”. Para obtener más información, vea la presentación del Sr. Rubin en el siguiente enlace:

http://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked.htm

© Cisco y/o sus filiales. Todos los derechos reservados. Información confidencial de Cisco

OnGuard Online

Este sitio web proporciona bastante información sobre cómo mantenerse protegido en línea, por ejemplo, protegiendo las computadoras, evitando engaños, siendo inteligente en línea y protegiendo a los niños en línea. http://www.onguardonline.gov/

Instituto Nacional de Normas y Tecnología (NIST)

El presidente Obama publicó el Decreto Ejecutivo (EO) 13636: “Mejora de la infraestructura crítica de ciberseguridad”. Como parte de este Decreto Ejecutivo, el NIST trabajó con las partes interesadas para desarrollar un esquema voluntario a fin de incluir los estándares, pautas y mejores prácticas con objeto de reducir los riesgos cibernéticos para la infraestructura crítica. Para conocer más sobre este Decreto Ejecutivo y el esquema en desarrollo del NIST, visite el siguiente enlace:

http://www.nist.gov/cyberframework

Capítulo 4: Recursos

Equipo de respuesta ante incidentes de seguridad informática

Para conocer más sobre el Equipo de respuesta ante incidentes de seguridad informática (CSIRT) y cómo se compone, visite el siguiente enlace:

https://tools.cisco.com/security/center/emergency.x?i=56#3

Monitoreo del CSIRT para el Cisco House en los juegos olímpicos de Londres en 2012

Vea el siguiente video de YouTube, que presenta a los miembros del CSIRT en acción en los Juegos Olímpicos de 2012:

http://www.youtube.com/watch?v=Hx8iGQIJ-aQ

Cisco Web Security Appliance

Cisco Web Security Appliance (WSA) es una solución integral que combina protección contra malware avanzado, control y visibilidad de la aplicación, políticas de uso aceptable, informes detallados y movilidad segura en una única plataforma. Para conocer más sobre WSA, visite el enlace siguiente:

http://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html

Cisco IronPort Email Security Appliance – Filtrado basado en reputación

Los filtros basados en reputación de la solución Cisco IronPort proporcionan protección contra correo electrónico no deseado para la infraestructura de su correo electrónico. Al actuar como primera línea de defensa, estos filtros eliminan hasta el 80% del correo electrónico no deseado entrante a nivel de la conexión. Para conocer más sobre el filtrado basado en la reputación de la solución Cisco Email Security Appliance (ESA), visite el siguiente enlace:

http://www.cisco.com/en/US/prod/vpndevc/ps10128/ps10154/rep_filters_index.html

Cisco Cyber Threat Defense

Cisco Cyber Threat Defense se concentra en las amenazas de seguridad informática más complejas y peligrosas que merodean en la red durante meses o años, robando información vital e interrumpiendo las operaciones. Expone estas amenazas mediante la identificación de patrones de tráfico sospechosos en el interior de la red. Proporciona información contextual acerca del ataque, los usuarios, la identidad y más, todo con visibilidad y claridad absoluta. Para obtener más información, visite el enlace siguiente:

http://www.cisco.com/en/US/netsol/ns1238/index.html

© Cisco y/o sus filiales. Todos los derechos reservados. Información confidencial de Cisco

Caso de estudio de prevención de intrusiones basadas en la red

Los sistemas de prevención de intrusiones (IPS, por sus siglas en inglés) son una parte importante de la estrategia de defensa de Cisco. Hay dos implementaciones principales de los IPS: implementaciones perimetrales del IPS e implementaciones con base en la red del IPS. Para obtener más información sobre la necesidad de estos dos modelos de implementación para proteger el tráfico en la red, acceda al caso de estudio en el siguiente enlace:

http://www.cisco.com/web/about/ciscoitatwork/security/csirt_network-based_intrusion_prevention_system_web.html

Capítulo 5: Actividades

Uso de un modelo del libro de estrategias

En una red compleja, los datos recopilados de diferentes herramientas de monitoreo pueden convertirse fácilmente en algo abrumador. En esta actividad, creará su propio libro de estrategias para organizar y documentar estos datos.

Visite el siguiente enlace para comprender mejor el concepto de un libro de estrategias:

https://blogs.cisco.com/security/using-a-playbook-model-to-organize-your-information-security-monitoring-strategy/

Cree su propio libro de estrategias considerando sus tres secciones principales:

- ID del informe y tipo de informe con nombre
- Establecimiento del objetivo
- Análisis del resultado

Hacking On a Dime

El enlace “Hacking On a Dime” explica cómo utilizar nmap (network mapper) para recopilar información relacionada con una red objetivo.

http://hackonadime.blogspot.com/2011/05/information-gathering-using-nmap-and.html

Nota: **nmap** es un escáner de puertos muy popular y potente lanzado por primera vez en 1997. Originalmente era solo para Linux; sin embargo, se transfirió a numerosas plataformas, como Windows y Mac OS X. Aún se ofrece como software gratuito. Para más información, consulte http://nmap.org/.

Capítulo 6: Recursos

Cisco Learning Network

En Cisco Learning Network, puede explorar las potenciales oportunidades profesionales, obtener los materiales de estudio para los exámenes de certificación y relacionarse en la red con otros estudiantes y profesionales de redes. Para conocer más, visite el enlace siguiente:

https://learningnetwork.cisco.com

Capacitación y certificaciones

En la sección "Capacitación y certificaciones" en el sitio web de Cisco encontrará información relacionada con capacitación y las últimas certificaciones de Cisco:

http://www.cisco.com/web/learning/training-index.html

© Cisco y/o sus filiales. Todos los derechos reservados. Información confidencial de Cisco

Información sobre desarrollo profesional y salarios

Ahora que ha cumplido con todos los módulos, es momento de explorar el ámbito profesional y posibles salarios en el campo de las redes. A continuación hay dos enlaces a sitios que brindan listas de trabajo e información sobre salarios. Hay muchos sitios como este en Internet.

http://www.indeed.com/salary?q1=Network+Security&l1

Certificaciones CompTIA

La Asociación de la Industria de la Tecnología Informática (http://www.comptia.org) ofrece varias certificaciones populares, incluida Security+. Este video de CompTIA se centra en la ciberseguridad.

https://www.youtube.com/watch?v=up9O44vEsDI

© Cisco y/o sus filiales. Todos los derechos reservados. Información confidencial de Cisco