Introdução à segurança cibernética

Recursos e atividades adicionais

Capítulo 1 Recursos

Compreensão das questões para os setores de serviços bancários

O site da Tapestry Network afirma que membros da Financial Services Network desenvolveram estes relatórios para resolver problemas enfrentados pelas instituições financeiras. Acesse o link a seguir e explore os tópicos sobre questões de serviços financeiros:

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

Gerenciamento de riscos da cadeia de fornecimento

O link a seguir aponta para um documento que explica como um fornecedor pode comprometer a segurança da rede e fornece outros recursos relacionados ao gerenciamento de riscos da cadeia de fornecimento:

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

Crime digital ou guerra cibernética?

O crime digital é o ato de cometer um crime em um ambiente cibernético; no entanto, um crime digital não constitui necessariamente um ato de guerra cibernética. A guerra cibernética pode incluir várias formas de sabotagem e espionagem com a intenção de explorar uma nação ou governo. O artigo a seguir descreve a diferença entre o crime digital e a guerra cibernética:

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

Capítulo 2 Recursos

Como roubar um banco: um passo a passo da engenharia social

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

XSS com um WebApp vulnerável

Neste tutorial, Dan Alberghetti demonstra o cross-site scripting (XSS) ou a injeção de código em um aplicativo da Web de um site que contém uma vulnerabilidade de aplicativo da Web conhecida.

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

Pioneiro do Google Hacking

Johnny Long foi pioneiro no conceito de Google Hacking. Um renomado especialista em segurança, ele escreveu e colaborou com muitos livros sobre segurança de computadores. Seu livro *Google Hacking for Penetration Testers* é uma leitura fundamental para qualquer pessoa que leva a sério o campo de Google Hacking. Ele também mantém um site dedicado a fornecer assistência sem fins lucrativos e a treinar os cidadãos mais pobres do mundo.

http://www.hackersforcharity.org

Centro de proteção contra malware da Microsoft

Este site da Microsoft fornece uma ferramenta de busca para encontrar informações sobre um determinado tipo de malware.

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

Malware Flame

O Stuxnet é uma das partes de malware com mais repercussão desenvolvida para guerra cibernética. No entanto, existem muitas outras ameaças menos conhecidas. Este artigo discute o malware conhecido como Flame, desenvolvido como uma ferramenta de espionagem para mirar em máquinas, principalmente no Irã e em outras partes do Oriente Médio. Para saber mais sobre este malware, acesse o link a seguir:

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

Malware Duqu

Outro malware, considerado para estar relacionado ao Stuxnet, é o Duqu. Duqu é um malware de reconhecimento destinado a reunir informações sobre um sistema de controle industrial desconhecido, para um possível ataque futuro. Para saber mais sobre Duqu e a possível ameaça que ele representa, acesse o seguinte link:

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

Catálogo de exploits da NSA

A Agência de Segurança Nacional dos Estados Unidos (NSA) tem desenvolvido e mantido um catálogo de exploits para quase todos os softwares, hardwares e firmwares principais. Com estas ferramentas e outros exploits, a NSA é capaz de manter o controle de praticamente todos os níveis da nossa vida digital. Para saber mais sobre o catálogo de exploits da NSA, acesse o link a seguir:

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

United States Computer Emergency Readiness Team (US-CERT)

Como parte do departamento de segurança interna, o United States Computer Emergency Readiness Team (US-CERT) esforça-se para melhorar a postura de segurança cibernética do país, compartilhar informações cibernéticas e gerenciar os riscos cibernéticos, protegendo os direitos dos norte-americanos. Para saber mais sobre US-CERT, acesse o link a seguir:

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

Se você quiser informações semelhantes de um país específico, acesse o link a seguir e pesquise o país.

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

Capítulo 3 Recursos

Todos os seus dispositivos podem ser hackeados

O uso de equipamentos eletrônicos dentro do corpo humano transforma o corpo da pessoa em um alvo cibernético, assim como qualquer computador ou celular. Na conferência TEDx MidAtlantic de 2011, Avi Rubin explicou como os hackers estão prejudicando carros, smartphones e dispositivos médicos. Ele nos alertou sobre os perigos de um mundo com cada vez mais possibilidade de ser hackeado. Para obter mais informações, assista a apresentação do Sr. Rubin no link a seguir:

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

OnGuard Online

Este site oferece uma variedade de informações sobre como se manter seguro on-line, tais como proteger seus computadores, evitar fraudes, estar atento on-line e proteger crianças on-line.
http://www.onguardonline.gov/

Instituto Nacional de Padrões e Tecnologia (NIST)

O Presidente Obama emitiu o Decreto 13636 (EO), Improving Critical Infrastructure Cybersecurity" (Melhoria da segurança cibernética infraestrutura essencial) Como parte deste decreto, a NIST foi direcionada para o trabalho com as partes interessadas para desenvolver uma estrutura voluntária, incluir padrões, diretrizes e melhores práticas, com a finalidade de reduzir os riscos cibernéticos à infraestrutura essencial. Para saber mais sobre este Decreto e a estrutura da NIST em desenvolvimento, acesse o link a seguir:

http://www.nist.gov/cyberframework

Capítulo 4 Recursos

Equipe de resposta a incidentes de segurança do computador

Para saber mais sobre a CSIRT e como ela é formada, acesse o link a seguir:

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

O monitoramento da CSIRT para Cisco House nos jogos olímpicos de Londres de 2012

Assista ao vídeo do YouTube a seguir, que mostra os membros da CSIRT em ação nos jogos olímpicos de 2012:

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

Cisco Web Security Appliance

O Cisco WSA (Web Security Appliance) é uma solução completa que combina proteção avançada contra malware, visibilidade e controle de aplicativo, políticas de uso aceitável, relatórios criteriosos e mobilidade segura em uma única plataforma. Para obter mais informações sobre o WSA, acesse o seguinte link:

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

Filtragem de reputação do Cisco IronPort Email Security Appliance

Os filtros de reputação Cisco IronPort fornecem proteção antispam para sua infraestrutura de e-mail. Atuando como uma primeira linha de defesa, estes filtros removem até 80% do spam recebido na conexão. Para obter mais informações sobre filtragem de reputação do Email Security Appliance (ESA), acesse o link a seguir:

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

Cisco Cyber Threat Defense

O Cisco Cyber Threat Defense se concentra nas ameaças de segurança da informação mais complexas e perigosas, que ficam escondidas nas redes durante meses ou anos, roubando informações vitais e interrompendo as operações. Ele expõe estas ameaças, identificando os padrões de tráfego de rede suspeitos no interior da rede. Desse modo, essa solução fornece informações contextuais sobre o ataque, os usuários, a identidade e muito mais — tudo isso visível em um único painel. Para obter mais informações, acesse o seguinte link:

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

Estudo de caso de prevenção contra intrusões pela rede

Os sistemas de prevenção de intrusões (IPS) são uma parte importante da estratégia de defesa interna na Cisco. Existem duas implementações de IPS primárias: implantações de IPS baseadas em perímetro e implantações de IPS pela rede. Para saber mais sobre a necessidade de ambos os modelos de implantação para proteger o tráfego de rede, acesse o estudo de caso no link a seguir:

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

Capítulo 5 Atividades

Uso de um modelo de manual

Em uma rede complexa, os dados coletados de diferentes ferramentas de monitoração podem facilmente se tornar avassaladores. Nesta atividade, você criará seu própria manual para organizar e documentar esses dados de monitoramento.

Acesse o link a seguir para compreender melhor um manual:

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

Crie seu próprio manual ao elaborar essas três seções principais:

- ID e tipo de relatório com nome
- Declaração objetiva
- Análise de resultado

Hacking On a Dime

O link "Hacking On a Dime" explica como usar o nmap (mapeador de rede) para reunir informações sobre uma rede de destino.

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

Nota: **nmap** é um scanner de porta extremamente popular e eficiente, lançado em 1997. Originalmente era Linux apenas; no entanto, mais tarde foi transferido para diversas plataformas, incluindo Windows e Mac OS X. Ele ainda é fornecido como software gratuito; para obter mais informações, consulte http://nmap.org/.

Capítulo 6 Recursos

Cisco Learning Network

Na Cisco Learning Network, você pode explorar suas possibilidades de carreira potencial, obter materiais de estudo para os exames de certificação e ter contato com outros estudantes e profissionais de rede. Para obter mais informações, acesse o seguinte link:

https://learningnetwork.cisco.com

Treinamentos e certificações

As informações sobre o treinamento e as certificações da Cisco mais recentes podem ser encontradas na seção de treinamento e certificações no site da Cisco:

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

Informações sobre salário e carreira

Agora que você concluiu todos os módulos, é hora de explorar a carreira e o possível salário no campo de rede. A seguir, há dois links para sites com listagens de emprego e informações de salário possível. Existem muitos sites como este na Internet.

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

Certificações CompTIA

A Computing Technology Industry Association (http://www.comptia.org) oferece diversas certificações populares, incluindo a Security+. Este vídeo da CompTIA é voltado para a segurança cibernética.

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