Introdução à Cibersegurança
Recursos e atividades adicionais

Capítulo 1 Recursos

Conhecer os problemas do setor bancário

O site Tapestry Network declara que os membros da Rede de Serviços Financeiros desenvolvem estes relatórios para dar resposta aos problemas que se colocam às instituições financeiras. Visite a seguinte ligação e explore os tópicos nos problemas dos Serviços Financeiros:

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

Gestão do risco na cadeia de fornecimento

A seguinte ligação aponta para um documento que explica como é que um fornecedor pode comprometer a segurança da rede e fornece outros recursos relativos à gestão do risco na cadeia de fornecimento:

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

Cibercrime ou ciberguerra?

O cibercrime é o ato de cometer um crime em ambiente cibernético; contudo, um cibercrime não constitui necessariamente um ato de ciberguerra. A ciberguerra pode incluir diversas formas de sabotagem e espionagem com a intenção de explorar um país ou um governo. O seguinte artigo descreve a diferença entre cibercrime e ciberguerra:

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

Capítulo 2 Recursos

How to Rob a Bank: A social engineering walkthrough (Como roubar um banco: Uma apresentação da engenharia social)

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

XSS com uma aplicação Web vulnerável

Neste tutorial, Dan Alberghetti demonstra a cross-site scripting (XSS) ou a introdução de um código numa aplicação de um Web site que contém uma vulnerabilidade conhecida.

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

Pioneiro do Google Hacking

Johnny Long foi pioneiro do conceito Google Hacking. Reconhecido perito em segurança, é autor e contribuiu para diversos livros sobre segurança informática. O seu livro *Google Hacking for Penetration Testers* é de leitura obrigatória para qualquer pessoa realmente empenhada no domínio do Google Hacking. Ele mantém, também, um Web site dedicado a fornecer assistência a organizações sem fins lucrativos e de formação aos cidadãos mais pobres do mundo.

http://www.hackersforcharity.org

Centro de Proteção contra Software Maligno da Microsoft

Este site da Microsoft fornece uma ferramenta de pesquisa para encontrar informações sobre um tipo particular de software maligno.

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

Software maligno Flame

O Stuxnet é um dos mais publicitados softwares malignos desenvolvido para fins de ciberguerra. Todavia, existem diversas outras ameaças menos conhecidas. Este artigo fala sobre o software maligno conhecido como Flame e que foi desenvolvido como uma ferramenta de espionagem destinada principalmente a máquinas no Irão e noutros países do Médio Oriente. Para mais informações sobre este software maligno, visite a seguinte ligação:

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

Software maligno Duqu

Outro software maligno, que se pensa estar relacionado com o Stuxnet, é o Duqu. O Duqu é um software maligno de reconhecimento destinado a recolher informações sobre um sistema de controlo industrial desconhecido com vista a um possível ataque futuro. Para mais informações sobre o Duqu e a potencial ameaça que este representa, visite a seguinte ligação:

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

Catálogo de Exploits da NSA

A Agência Nacional de Segurança (NSA) dos Estados Unidos desenvolveu e mantém um catálogo de exploits para quase todo o principal software, hardware e firmware. Utilizando estas ferramentas e outros exploits, a NSA é capaz de monitorizar praticamente todos os níveis da nossa vida digital. Para mais informações sobre o catálogo de exploits da NSA, visite a seguinte ligação:

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

Computer Emergency Readiness Team dos Estados Unidos (US-CERT)

Parte do Departamento de Segurança Interna dos Estados Unidos, a Computer Emergency Readiness Team (US-CERT – Equipa de Resposta de Emergência a Incidentes Informáticos) esforça-se por melhorar a postura do país em termos de cibersegurança, partilhar informações cibernéticas e gerir riscos cibernéticos ao mesmo tempo que protege os direitos dos norte-americanos. Para mais informações sobre a US-CERT, visite a seguinte ligação:

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

Caso procure informações semelhantes para um país específico, visite a seguinte ligação e pesquise o país.

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

Capítulo 3 Recursos

Todos os seus dispositivos podem ser atacados

A utilização de aparelhos eletrónicos no corpo humano converte o corpo da pessoa num alvo cibernético, tal como qualquer computador ou telemóvel. Na conferência TEDx MidAtlantic, em 2011, Avi Rubin explicou como é que os piratas informáticos estão a comprometer os automóveis, os smartphones e os dispositivos médicos. Ele avisou-nos sobre os perigos de um mundo cada vez mais suscetível a ataques de piratas informáticos. Para mais informações, veja a apresentação de Avi Rubin na seguinte ligação:

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

OnGuard Online

Este Web site fornece uma diversidade de informações sobre como nos mantermos seguros online, como por exemplo: garantir a segurança do computador, evitar fraudes, ser inteligente online e proteger as crianças online.

http://www.onguardonline.gov/

Instituto Nacional de Normas e Tecnologia (NIST – National Institute of Standards and Technology)

O presidente Barack Obama emitiu o Decreto 13636, “Melhorar a cibersegurança de infraestruturas críticas”. No âmbito deste Decreto, o NIST foi instruído a trabalhar com partes interessadas no desenvolvimento de um quadro não vinculativo que incluísse normas, diretrizes e melhores práticas com a finalidade de reduzir os riscos cibernéticos para infraestruturas críticas. Para mais informações sobre este Decreto e o quadro em desenvolvimento pelo NIST, visite a seguinte ligação:

http://www.nist.gov/cyberframework

Capítulo 4 Recursos

Equipa de Resposta a Incidentes de Segurança Informática

Para mais informações sobre a CSIRT e como é composta, visite a seguinte ligação:

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

Monitorização da CSIRT para a Casa Cisco nos Jogos Olímpicos de 2012, em Londres

Veja o seguinte vídeo no YouTube que apresenta os membros da CSIRT em ação durante os Jogos Olímpicos de 2012:

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

Aplicação de Segurança da Web Cisco Ironport

A Aplicação de Segurança da Web Cisco (WSA) é uma solução completa que combina proteção avançada contra software maligno, visibilidade e controlo de aplicação, políticas de utilização aceitável, registos detalhados e mobilidade segura numa única plataforma. Para mais informações sobre a WSA, visite a seguinte ligação:

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

Aplicação de Segurança de E-mail com Filtros de Reputação Cisco IronPort

Os filtros de proteção Cisco IronPort fornecem proteção contra spam na infraestrutura do seu e-mail. Atuando como uma primeira linha de defesa, estes filtros eliminam até 80 por cento do spam recebido a nível da ligação. Para mais informações sobre a Aplicação de Segurança de E-mail (ESA) com filtros de reputação, visite a seguinte ligação:

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

Defesa Cisco contra ameaças cibernéticas

A Defesa Cisco contra ameaças cibernéticas foca-se nas mais complexas e perigosas ameaças à segurança da informação que se escondem nas redes durante meses ou anos, roubando informação vital e perturbando operações. Este instrumento expõe as ameaças através da identificação de padrões suspeitos de tráfego de rede no interior da rede. De seguida, fornece informação contextual sobre o ataque, utilizadores, identidade e mais – tudo visível a partir de um único painel de vidro. Para mais informações, visite a seguinte ligação:

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

Caso de estudo na prevenção contra intrusões baseadas na rede

Os Sistemas de prevenção contra intrusões (IPS) são uma parte importante da estratégia de defesa aprofundada da Cisco. Existem duas implementações primárias de IPS: implementação de IPS com base no perímetro e implementação de IPS com base na rede. Para mais informações sobre a necessidade de implementação de ambos os modelos de segurança do tráfego de rede, aceda ao caso de estudo na seguinte ligação:

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

Capítulo 4 Atividades

Utilização de um livro de atividades modelo

Numa rede complexa, os dados recolhidos a partir de diferentes ferramentas de monitorização podem, facilmente, tornar-se esmagadores. Nesta atividade, irá criar o seu próprio livro de atividades para organizar e documentar esta monitorização de dados.

Visite a seguinte ligação para compreender melhor um livro de atividades:

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

Crie o seu próprio livro de atividades delineando as suas três principais secções:

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

Hacking On a Dime

A ligação “Hacking On a Dime” explica como utilizar o nmap (cartógrafo da rede) para recolher informações sobre uma rede alvo.

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

Nota: o **nmap** é um analisador de portas extremamente popular e robusto que foi lançado pela primeira vez em 1997. Originalmente, destinava-se apenas ao Linux; contudo, foi posteriormente transferido para diversas plataformas, incluindo Windows e Mac OS X. Continua a ser fornecido como um software gratuito; para mais informações consulte http://nmap.org/.

Outras ferramentas de reconhecimento

A seguinte ligação para “danscources.com” fornece prática adicional na utilização de ferramentas de reconhecimento.

Do ponto de vista da segurança ou do reconhecimento, o Sistema de nomes de domínio (DNS) pode ser explorado e oferece um meio de descobrir os servidores públicos – e possivelmente os privados – de uma organização, bem como os respetivos serviços e localizações dos endereços IP correspondentes.

http://www.danscourses.com/Network-Penetration-Testing/dns-reconnaissance.html

Outro protocolo, conhecido como Whois, pode ser utilizado como uma ferramenta de reconhecimento para recolher dados de contactos, como nomes de domínio, blocos de endereços IP e números de sistemas autónomos.

http://www.danscourses.com/Network-Penetration-Testing/whois-reconnaisance.html

Capítulo 5 Recursos

Cisco Learning Network

Na Cisco Learning Network, pode explorar potenciais oportunidades de carreira, obter materiais de estudo para exames de certificação e construir redes de relacionamentos com outros estudantes e profissionais. Para mais informações, visite a seguinte ligação:

https://learningnetwork.cisco.com

Formação e certificações

Pode encontrar informações sobre formação e as mais recentes certificações Cisco na secção Formação e certificações do Web site da Cisco:

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

Informações sobre carreiras e salários

Agora que concluiu todos os módulos, é o momento de explorar o potencial de carreira e salário no domínio da rede. A seguir encontra duas ligações que fornecem listagens de oportunidades de emprego e informação sobre o potencial salário. Existem diversos sites como este na Internet.

https://www.cisco.apply2jobs.com

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

Certificações CompTIA

A Computing Technology Industry Association (http://www.comptia.org Associação da Indústria da Tecnologia Informática) oferece diversas certificações populares, incluindo a Security+. Este vídeo da CompTIA foca-se na cibersegurança.

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