

Wprowadzenie do cyberbezpieczeństwa

Dodatkowe materiały i ćwiczenia

Rozdział. 1 Materiały

Próba zrozumienia problemów sektora bankowego

Na stronie internetowej Tapestry Network stwierdzono, że członkowie Financial Services Network opracowali raporty odnoszące się do problemów instytucji finansowych. Kliknij w poniższy odnośnik, aby zapoznać się z tematami dotyczącymi usług finansowych:

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

Zarządzanie ryzykiem związanym z łańcuchem dostaw

Poniższy odnośnik prowadzi do artykułu wyjaśniającego, w jaki sposób dostawca może zagrozić bezpieczeństwu sieci. Artykuł wyjaśnia także inne kwestie związane z zarządzaniem ryzykiem w łańcuchu dostaw:

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

Cyberprzestępstwo czy cyberwojna?

O cyberprzestępstwie mówimy wówczas, gdy jakaś osoba popełnia przestępstwo w cyberprzestrzeni. Cyberprzestępstwo nie zawsze stanowi akt cyberwojny. Cyberwojna może obejmować różne formy sabotażu i szpiegostwa. Celem jest zaatakowanie wybranego kraju lub rządu. Poniższy artykuł opisuje różnicę między cyberprzestępstwem a cyberwojną:

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

Rozdział. 2 Materiały

"Jak obrabować bank" – poradnik socjotechniczny

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

Wykorzystanie XSS w niezabezpieczonej aplikacji internetowej

W tym samouczku Dan Alberghetti demonstruje podatność o nazwie XSS (ang. cross-site scripting) nazywaną też wstrzykiwaniem kodu do aplikacji internetowej, która zawiera znaną lukę bezpieczeństwa.

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

Prekursor włamań przy użyciu Google

Johnny Long był pionierem koncepcji dokonywania włamań przy użyciu wyszukiwarki Google. Znany ekspert ds. bezpieczeństwa, autor wielu książek na temat bezpieczeństwa komputerowego. Jego książka „*Google Hacking for Penetration Testers*” jest obowiązkową pozycją na liście lektur dla każdego, kto poważnie myśli o kwestiach dotyczących włamań przy użyciu wyszukiwarki Google. Prowadzi także stronę internetową poświęconą udzielaniu pomocy organizacjom non-profit oraz edukuje najbiedniejszych.

<http://www.hackersforcharity.org>

Microsoftowe centrum ochrony przed złośliwym oprogramowaniem (ang. MMPC)

Ta witryna firmy Microsoft udostępnia narzędzie do wyszukiwania informacji o określonym typie złośliwego oprogramowania.

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

Flame (złośliwe oprogramowanie)

Stuxnet jest jednym z najbardziej znanych przykładów złośliwego oprogramowania opracowanego na potrzeby cyberwojny. Istnieje jednak wiele innych, mniej znanych zagrożeń. W tym artykule omówiono złośliwe oprogramowanie znane jako Flame. Narzędzie to zostało opracowane głównie w celu szpiegowania komputerów w Iranie oraz w innych krajach na Bliskim Wschodzie. Aby dowiedzieć się więcej o tym złośliwym oprogramowaniu, kliknij poniższy odnośnik:

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

Duqu (złośliwe oprogramowanie)

Kolejnym złośliwym oprogramowaniem, spokrewnionym z robakiem Stuxnet, jest Duqu. Duqu jest szkodliwym oprogramowaniem przeznaczonym do rozpoznawania i zbierania informacji o nieznanym systemach przemysłowych. Celem jego działania jest ewentualne przeprowadzenie ataku w przyszłości. Aby uzyskać więcej informacji na temat Duqu i zagrożeń, które ze sobą niesie, odwiedź poniższą stronę:

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

Katalog exploitów amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA)

Amerykańska Agencja Bezpieczeństwa Narodowego (ang. The United States National Security Agency, NSA) opracowała katalog exploitów dla większości oprogramowania, sprzętu oraz oprogramowania wbudowanego (firmware). Korzystając z tych oraz innych narzędzi, NSA jest w stanie śledzić praktycznie każdy aspekt naszego życia w sieci. Aby dowiedzieć się więcej o katalogu exploitów NSA, kliknij poniższy odnośnik:

<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)

W ramach Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (ang. Department of Homeland Security), zespół US-CERT dąży do poprawy krajowego cyberbezpieczeństwa, udostępnia wiedzę na tematy cybernetyczne oraz monitoruje cybernetyczne zagrożenia przy jednoczesnej ochronie praw obywateli. Aby dowiedzieć się więcej o US-CERT, kliknij poniższy odnośnik:

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

Jeśli chcesz uzyskać podobne informacje na temat innego kraju, przejdź do poniższej strony i wyszukaj kraj, który Cię interesuje.

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

Rozdział. 3 Materiały

Wszystkie Twoje urządzenia mogą stać się celem hakerów

Wszczepienie elektroniki do ludzkiego ciała zamienia je w potencjalny cel cyberataku. Cel podobny do komputera czy telefonu komórkowego. Na konferencji TEDx MidAtlantic w 2011 roku Avi Rubin wyjaśnił, w jaki sposób hakerzy przejmują kontrolę nad samochodami, smartfonami i urządzeniami medycznymi. Ostrzegł nas przed niebezpieczeństwami coraz bardziej „hakowalnego świata” (ang. hackable world). Aby uzyskać więcej informacji, obejrzyj prezentację Aviego Rubina dostępną pod następującym odnośnikiem:

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

OnGuard Online

Witryna OnGuard zawiera całe bogactwo informacji na temat internetowego bezpieczeństwa (kwestiach zabezpieczania komputerów, unikania oszustw, rozsądku w korzystaniu z zasobów Internetu, ochrony dzieci).
<http://www.onguardonline.gov/>

Amerykański Państwowy Instytut Standardów i Technologii (ang. National Institute of Standards and Technology, NIST)

Prezydent Obama wydał rozporządzenie wykonawcze o tytule „Poprawa cyberbezpieczeństwa kluczowej infrastruktury” (ang. Executive Order 13636 (EO): Improving Critical Infrastructure Cybersecurity) W ramach tego zarządzenia NIST rozpoczął współpracę z zainteresowanymi stronami w celu opracowania nowej koncepcji ramowej, obejmującej najlepsze standardy, wytyczne i praktyki w cyberbezpieczeństwie. Powodem tego działania jest chęć zredukowania ryzyka związanego z kluczową infrastrukturą. Aby dowiedzieć się więcej na temat tego rozporządzenia i struktury opracowywanej przez NIST, odwiedź poniższą stronę:

<http://www.nist.gov/cyberframework>

Rozdział. 4 Materiały

Zespół reagowania na incydenty bezpieczeństwa komputerowego (ang. Computer Security Incident Response Team, CSIRT)

Aby uzyskać więcej informacji na temat zespołu CSIRT oraz jego składu, kliknij poniższy odnośnik:

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

Nadzór zespołu CSIRT nad Cisco House podczas Igrzysk Olimpijskich w Londynie (2012)

Obejrzyj poniższy film w serwisie YouTube, który przedstawia działania członków CSIRT podczas Igrzysk Olimpijskich 2012:

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

Środki zabezpieczania sieci firmy Cisco

Środki zabezpieczania sieci firmy Cisco (z ang. WSA) to kompleksowe rozwiązanie łączące zaawansowaną ochronę przed złośliwym oprogramowaniem, dbałość o przejrzystość sieci i kontrolę, właściwe zasady użytkowania, skrupulatne raporty oraz bezpieczną mobilność w ramach jednego systemu operacyjnego. Aby uzyskać więcej informacji na temat WSA, odwiedź poniższy link:

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

Narzędzia zapewniające ochronę przed spamem – Cisco IronPort Email Security Appliance Reputation Filtering

Rozwiązanie IronPort Reputation Filters firmy Cisco zapewnia ochronę przed spamem dla Twojej poczty e-mail. Działając jako pierwsza linia obrony, filtry te usuwają do 80% przychodzącego spamu. Aby uzyskać więcej informacji o narzędziu zapewniającym ochronę przed spamem (ang. Email Security Appliance, ESA), kliknij poniższy odnośnik:

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

Obrona przed cyberzagrożeniami – Cisco Cyber Threat Defense

Cisco Cyber Threat Defense koncentruje się na najbardziej złożonych i niebezpiecznych zagrożeniach, które potrafią cziąć się w sieci przez długie miesiące lub nawet lata. Zagrożenia te dokonują kradzieży ważnych

informacji i zakłócają prawidłowe działanie. Cisco Cyber Threat Defense odkrywa te zagrożenia oraz identyfikuje podejrzane wzorce ruchu sieciowego wewnątrz danej sieci. Następnie dostarcza we właściwym kontekście informacje o ataku, użytkownikach, tożsamości i innych – wszystkie te informacje widoczne są z poziomu jednego panelu kontrolnego. Aby uzyskać więcej informacji, kliknij poniższy odnośnik:

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

Zapobieganie włamaniom w sieci – studium przypadku

Systemy zapobiegania włamaniom (ang. Intrusion prevention systems, IPS) są ważną częścią strategii tzw. obrony w głąb (ang. defense-in-depth) w firmie Cisco. Istnieją dwie podstawowe implementacje IPS: obwodowe wdrożenia IPS oraz sieciowe wdrożenia IPS. Jeżeli chcesz wiedzieć więcej o potrzebie wdrożenia obydwu modeli IPS dla gwarancji bezpieczeństwa ruchu sieciowego, zapoznaj się ze studium przypadku dostępnym pod następującym odnośnikiem:

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

Rozdział. 4 Ćwiczenia

Korzystanie z własnego zestawu procedur działania (ang. playbook)

W złożonych sieciach ilość danych zebrana przez narzędzia monitorujące może szybko stać się przytłaczająca. W tym ćwiczeniu utworzysz własny zestaw procedur działania, które pomogą Ci uporządkować zebrane dane.

Aby lepiej zrozumieć znaczenie posiadania takich procedur, kliknij poniższy odnośnik:

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

Stwórz własny zestaw procedur poprzez określenie trzech głównych wymiarów każdej procedury:

- Danych identyfikacyjnych (identyfikatora, kategorii oraz nazwy)
- Części opisowej (subiektywnego opisu „co” i „dlaczego” jest wykonywane)
- Analizy wyników

Blog „Hacking On a Dime”

Strona „Hacking On a Dime” wyjaśnia, jak używać narzędzia Nmap do zbierania informacji o sieci docelowej.

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

Uwaga: Narzędzie Nmap to niezwykle popularny i posiadający duże możliwości skaner portów, którego pierwsza wersja została opublikowana w 1997 roku. Pierwotnie Nmap był przeznaczony tylko dla systemu operacyjnego Linux. Jednak później został zaadoptowany dla wielu innych systemów, takich jak Windows i Mac OS X. Jest dostępny bez opłat. Więcej informacji na jego temat znajdziesz na stronie <http://nmap.org/>.

Rozdział. 5 Materiały

Cisco Learning Network

W Cisco Learning Network dowiesz się więcej na temat możliwych ścieżek kariery zawodowej, zdobędziesz materiały do egzaminów certyfikacyjnych oraz nawiądziesz kontakty ze studentami i specjalistami branży sieciowej. Aby uzyskać więcej informacji, kliknij w poniższy odnośnik:

<https://learningnetwork.cisco.com>

Szkolenia i certyfikaty

Informacje dotyczące szkoleń i najnowszych certyfikatów Cisco można znaleźć w dziale Training & Certifications na stronie internetowej Cisco:

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

Informacje na temat kariery zawodowej i wynagrodzeń

Po ukończeniu wszystkich modułów nadszedł czas poznania możliwości pracy w sektorze IT oraz oferowanych wynagrodzeń w branży sieciowej. Oto dwa odnośniki, które zawierają oferty pracy wraz z informacjami o potencjalnych zarobkach. W Internecie znajdziesz wiele podobnych stron.

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

Certyfikaty CompTIA

Stowarzyszenie CompTIA (<http://www.comptia.org>) oferuje kilka systemów certyfikacji, w tym certyfikat „Security +”. Oto materiał wideo stowarzyszenia CompTIA dotyczący cyberbezpieczeństwa:

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