Вступ до кібербезпеки

Додаткові ресурси та завдання

Ресурси до Розділу 1

Розуміння проблем банківської сфери

Сайт Tapestry Network повідомляє, що члени мережі фінансових послуг розробили ці звіти для вирішення питань, з якими стикаються фінансові установи. Перейдіть за наступним посиланням і вивчіть теми в розділі «Фінансові послуги»:

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

Управління ризиками ланцюга поставок

Наступне посилання вказує на документ, який пояснює, як постачальник може поставити під загрозу безпеку мережі і надає інші ресурси щодо управління ризиками ланцюга поставок:

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

Кіберзлочинність або кібервійна?

Кіберзлочинність - це скоєння злочину в кібер-середовищі; проте кіберзлочинність не обов'язково є кібервійною. Кібервійна може містити різні форми саботажу і шпигунства з наміром використати націю чи уряд. У наступній статті описується різниця між кіберзлочинністю і кібервійною:

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

Ресурси до Розділу 2

Як пограбувати банк: Соціальна інженерія – крок за кроком

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

XSS з вразливим веб-додатком

У цьому прикладі Ден Альбергетті демонструє міжсайтовий скриптинг (XSS) або введення коду в додаток веб-сайту, який містить відому уразливість в веб-додатку.

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

Піонер Google Hacking

Джонні Лонг вперше розробив концепцію Google Hacking. Відомий експерт з безпеки, він є автором і співавтором багатьох книг з комп'ютерної безпеки. Його книга *Google Hacking проникнення для тестувальників* обов'язкова для вивчення усіма, хто зацікавлений сферою Google Hacking. Він також підтримує веб-сайт для надання допомоги некомерційним організаціям, який також містить тренінги для найбідніших громадян світу.

http://www.hackersforcharity.org

Центр захисту від зловмисних програм Microsoft

Цей сайт Microsoft надає інструмент для пошуку інформації про конкретний тип зловмисних програм.

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

Зловмисне ПЗ Flame

Stuxnet є однією з найбільш широко поширених зловмисних програм, розроблених для кібервійни. Однак існує багато інших менш відомих загроз. У цій статті розглядається зловмисне ПЗ, відоме як Flame, яке було розроблено як інструмент шпигунства, орієнтований основному на Іран та інші частини Близького сходу. Щоб дізнатися більше про цю зловмисну програму, перейдіть за наступним посиланням:

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

Зловмисне ПЗ Duqu

Іншою зловмисною програмою, яка, як вважають, пов'язана з Stuxnet, є Duqu. Duqu - це зловмисне ПЗ для розвідки, призначене для збору інформації про невідому промислову систему управління з метою можливої майбутньої атаки. Щоб дізнатися більше про Duqu і можливу загрозу, яку вона представляє, перейдіть за наступним посиланням:

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

Каталог експлойтів АНБ

Агентство національної безпеки США (National Security Agency - NSA) розробило і підтримує каталог експлойтів практично для всіх основних програмних, апаратних засобів і прошивок. Використовуючи ці інструменти та інші експлойти, NSA може відстежувати практично кожен рівень нашого цифрового життя. Щоб дізнатися більше про каталог експлойтів NSA, перейдіть за наступним посиланням:

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

Група комп'ютерної безпеки США з реагування на інциденти (US-CERT)

В рамках Департаменту внутрішньої безпеки Група комп'ютерної безпеки США з реагування на інциденти (US-CERT) прагне покращити кібербезпеку нації, ділитися кібер-інформацією та керувати кібер-ризиками при захисті прав американців. Щоб дізнатися більше про US-CERT, перейдіть за наступним посиланням:

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

Якщо ви хочете отримати подібну інформацію для конкретної країни, перейдіть за наступним посиланням і знайдіть країну.

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

Ресурси до Розділу 3

Всі ваші пристрої можуть бути зламані

Використання електроніки в людському тілі перетворює тіло людини в кібер-мішень, як і будь-який комп'ютер або мобільний телефон. На конференції TEDx MidAtlantic в 2011 році Аві Рубін пояснив, як хакери компрометують автомобілі, смартфони і медичні пристрої. Він попередив нас про небезпеку все більш «зламаного» світу. Для отримання додаткової інформації дивіться презентацію пана Рубіна за наступним посиланням:

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

OnGuard Online

На цьому веб-сайті представлена велика кількість інформації про те, як залишатися в безпеці в Інтернеті, наприклад, захищати комп'ютери, уникати шахрайства, бути мудрим і захищати дітей в Інтернеті.
http://www.onguardonline.gov/

Національний інститут стандартів і технологій (NIST)

Президент Обама видав Наказ 13636 (EO) «Покращення критичної інфраструктури кібербезпеки». В рамках цього наказу NIST було спрямовано на роботу з зацікавленими сторонами для розробки добровільних рамок, включно зі стандартами, керівними принципами і передовими методами з метою зниження кібер-ризиків для критичної інфраструктури. Щоб дізнатися більше про цей наказ і фреймворк NIST, який розробляється, перейдіть за наступним посиланням:

http://www.nist.gov/cyberframework

Ресурси до Розділу 4

Команда комп'ютерної безпеки та реагування на інциденти

Щоб дізнатися більше про CSIRT і про те, як вона створена, перейдіть за наступним посиланням:

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

Моніторинг CSIRT для Cisco House на Олімпійських іграх в Лондоні в 2012 році

Перегляньте наступне відео на YouTube, в якому представлені члени CSIRT в дії на Олімпійських іграх 2012 року:

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

Cisco Web Security Appliance

Cisco Web Security Appliance (WSA) - це рішення «все-в-одному», яке поєднує в собі розширений захист від зловмисних програм, видимість і контроль додатків, прийнятні політики використання, прозорі звіти і безпечну мобільність в єдиній платформі. Для отримання додаткової інформації про WSA перейдіть за наступним посиланням:

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

Фільтри репутації Cisco IronPort Email Security Appliance

Фільтри репутації Cisco IronPort забезпечують захист від спаму для вашої електронної пошти. Діючи як перша лінія захисту, ці фільтри видаляють до 80 відсотків вхідного спаму на рівні з'єднання. Для отримання додаткової інформації про фільтри репутації Email Security Appliance (ESA) перейдіть за наступним посиланням:

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

Cisco Cyber Threat Defense

Cisco Cyber Threat Defense фокусується на найскладніших, небезпечних загрозах інформаційної безпеки, які ховаються в мережах протягом декількох місяців або років, викрадаючи важливу інформацію і порушуючи роботу. Ці загрози розкриваються завдяки ідентифікації підозрілого мережного трафіку. Далі рішення надає контекстуальну інформацію про атаку, користувачів, ідентифікаційні дані та інше - усе стає видно як на долоні. Для отримання додаткової інформації перейдіть за наступним посиланням:

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

Дослідження системи запобігання вторгнень, яка розгорнута на основі мережі

Системи запобігання вторгнень (IPS) є важливою частиною стратегії поглибленого захисту Cisco. Існують дві основні реалізації IPS: розгортання IPS на основі периметра і розгортання IPS на основі мережі. Щоб дізнатися більше про необхідність використання обох моделей розгортання для захисту мережного трафіку, зверніться до тематичного дослідження за наступним посиланням:

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

Вправи до Розділу 4

Використання моделі Playbook

У складній мережі дані, зібрані з різних інструментів моніторингу, можуть легко стати незліченими. У цій вправі ви створите свій власний playbook для організації та документування даних моніторингу.

Перейдіть за наступним посиланням, щоб краще зрозуміти як виглядає playbook:

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

Створіть свій власний playbook, склавши три основні розділи:

- Ідентифікатор звіту і тип звіту з назвою
- Постановка задачі
- Аналіз результатів.

Hacking On a Dime

Посилання на «Hacking on Dime» пояснює, як використовувати nmap для збору інформації про цільову мережу.

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

Примітка: **nmap** - надзвичайно популярний і потужний сканер портів, вперше випущений в 1997 році. Спочатку він був реалізований тільки на Linux; проте пізніше був перенесений на численні платформи, включно з Windows і Mac OS X. Як і раніше розповсюджується у вигляді безкоштовного програмного забезпечення; для отримання додаткової інформації, див. http://nmap.org/.

Інші інструменти розвідки

Наступні посилання на «danscources.com» надають додаткову практику використання інструментів розвідки. З точки зору безпеки або розвідки система доменних імен (DNS) може бути використана для виявлення загальнодоступних і, можливо, приватних серверів, служб та відповідних IP-адрес.

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

Інший протокол, відомий як Whois, може використовуватися як інструмент розвідки для збору контактної інформації, такої як імена доменів, блоки IP-адрес і номери автономних систем.

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

Ресурси до Розділу 5

Cisco Learning Network

В Cisco Learning Network ви можете дослідити свої потенційні можливості кар'єрного росту, отримати навчальні матеріали для сертифікаційних іспитів і налагодити зв'язки з іншими студентами і професіоналами в області мереж. Для отримання додаткової інформації перейдіть за наступним посиланням:

https://learningnetwork.cisco.com

Навчання і сертифікація

Інформацію щодо навчання та останніх версій сертифікатів Cisco можна знайти в розділі «Навчання і сертифікація» на веб-сайті Cisco:

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

Інформація про кар'єру і зарплату

Тепер, коли ви завершили всі модулі, прийшов час дослідити кар’єрний потенціал і зарплати в сфері комп’ютерних мереж. Нижче наведені два посилання на сайти, що містять переліки вакансій і потенційну інформацію про зарплату. В Інтернеті є багато таких сайтів.

https://www.cisco.apply2jobs.com

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

Сертифікати CompTIA

Галузева асоціація виробників комп'ютерної техніки (http://www.comptia.org) пропонує кілька популярних сертифікатів, включаючи Security +. Це відео від CompTIA фокусується на кібербезпеці.

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