Introduction to Cybersecurity
Additional Resources and Activities

Chapter 1 Resources

Supply Chain Risk Management

The following link points to a document that explains how a supplier can compromise network security and provides other resources regarding supply chain risk management:

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

Cybercrime or Cyberwarfare?

Cybercrime is the act of committing a crime in a cyber environment; however, a cybercrime does not necessarily constitute an act of cyberwarfare. Cyberwarfare can include various forms of sabotage and espionage with the intent to exploit a nation or government. The following article describes the difference between cybercrime and cyberwarfare:

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

Chapter 2 Resources

How to Rob a Bank: A social engineering walkthrough

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

XSS with a Vulnerable WebApp

In this tutorial, Dan Alberghetti demonstrates cross-site scripting (XSS) or injecting code into a website's web application that contains a known web app vulnerability.

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

Google Hacking Pioneer

Johnny Long pioneered the concept of Google Hacking. A renowned security expert, he has authored and contributed to many books on computer security. His book *Google Hacking for Penetration Testers* is a must read for anyone serious about the field of Google Hacking. He also maintains a website devoted to providing assistance to non-profits and training for the world's poorest citizens.

http://www.hackersforcharity.org

Microsoft Malware Protection Center

This Microsoft site provides a search tool to find information about a particular type of malware.

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

Flame Malware

Stuxnet is one of the most highly publicized pieces of malware developed for the purpose of cyberwarfare. However, many other lesser-known threats exist. This article discusses malware known as Flame, which was

developed as an espionage tool for targeting machines primarily in Iran and other parts of the Middle East. To learn more about this malware, visit the following link:

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

Duqu Malware

Another malware, thought to be related to Stuxnet, is Duqu. Duqu is a reconnaissance malware intended to gather information on an unknown industrial control system for the purpose of a possible future attack. To learn more about Duqu and the possible threat it imposed, visit the following link:

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

NSA's Catalog of Exploits

The United States National Security Agency (NSA) has developed and maintained a catalog of exploits for nearly every major software, hardware, and firmware. Using these tools and other exploits, the NSA is able to keep track of practically every level of our digital lives. To learn more about the NSA's catalog of exploits, visit the following link:

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)

As part of the Department of Homeland Security, the United States Computer Emergency Readiness Team (US-CERT) strives to improve the Nation's cybersecurity posture, share cyber information, and manage cyber risks while protecting the rights of Americans. To learn more about US-CERT, visit the following link:

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

If you want similar information for a specific country, visit the following link and search for the country.

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

Chapter 3 Resources

All Your Devices Can Be Hacked

The use of electronics within the human body turns that person's body into a cyber target, just like any computer or cell phone. At the TEDx MidAtlantic conference in 2011, Avi Rubin explained how hackers are compromising cars, smart phones, and medical devices. He warned us about the dangers of an increasingly "hackable" world. For more information, watch Mr. Rubin's presentation in the following link:

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

OnGuard Online

This website provides a wealth of information regarding how to stay safe online, such as securing your computers, avoiding scams, being smart online, and protecting kids online.
http://www.onguardonline.gov/

National Institute of Standards and Technology (NIST)

President Obama issued Executive Order 13636 (EO), "Improving Critical Infrastructure Cybersecurity." As part of this Executive Order, NIST was directed to work with stakeholders to develop a voluntary framework, to include standards, guidelines, and best practices, for the purpose of reducing cyber risks to critical infrastructure. To learn more about this Executive Order and the NIST framework in development, visit the following link:

http://www.nist.gov/cyberframework

Chapter 4 Resources

Computer Security Incident Response Team

To learn more about CSIRT, and how it is composed, visit the following link:

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

CSIRT Monitoring for the Cisco House at the London 2012 Olympics Games

View the following YouTube video, which depicts CSIRT members in action at the 2012 Olympic Games:

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

Cisco Web Security Appliance

The Cisco Web Security Appliance (WSA) is an all-in-one solution that combines advanced malware protection, application visibility and control, acceptable use policies, insightful reporting, and secure mobility on a single platform. For more information on WSA, visit the following link:

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

Cisco IronPort Email Security Appliance Reputation Filtering

Cisco IronPort Reputation Filters provide spam protection for your email infrastructure. Acting as a first line of defense, these filters remove up to 80 percent of incoming spam at the connection level. For more information about Email Security Appliance (ESA) reputation filtering, visit the following link:

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

Cisco Cyber Threat Defense

Cisco Cyber Threat Defense focuses on the most complex, dangerous information security threats, which lurk in networks for months or years, stealing vital information and disrupting operations. It exposes these threats by identifying suspicious network traffic patterns within the network interior. Then, it provides contextual information about the attack, users, identity, and more — all visible from a single pane of glass. For more information, visit the following link:

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

Network-Based Intrusion Prevention Case Study

Intrusion prevention systems (IPS) are an important part of the defense-in-depth strategy at Cisco. There are two primary IPS implementations: Perimeter-based IPS deployments and Network-based IPS deployments. To learn more about the need for both deployment models to secure network traffic, access the case study at the following link:

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

Chapter 4 Activities

Using a Playbook Model

In a complex network, the data gathered from different monitoring tools can easily become overwhelming. In this activity, you will create your own playbook to organize and document this monitoring data.

Visit the following link to have a better understanding of a playbook:

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

Create your own playbook by drafting its three main sections:

- Report ID and Report Type with Name
- Objective Statement
- Result Analysis

Hacking On a Dime

The “Hacking On a Dime” link explains how to use nmap (network mapper) to gather information about a target network.

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

Note: **nmap** is an extremely popular and powerful port scanner that was first released in 1997. Originally it was Linux only; however, it was later ported to numerous platforms, including Windows and Mac OS X. It is still provided as free software; for more information, see http://nmap.org/.

Chapter 5 Resources

Cisco Learning Network

At the Cisco Learning Network, you can explore your potential career possibilities, obtain study materials for certification exams, and build networking relationships with other networking students and professionals. For more information, visit the following link:

https://learningnetwork.cisco.com

Training and Certifications

Information regarding training and the latest Cisco certifications can be found in the Training & Certifications section on Cisco’s website:

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

Career and Salary Information

Now that you have completed all the modules, it is time to explore the career and salary potential in the networking field. Below are two links to sites that give job listings and potential salary information. There are many sites like this on the Internet.

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

CompTIA Certifications

The Computing Technology Industry Association (http://www.comptia.org) offers several popular certifications including the Security+. This video from CompTIA focuses on cybersecurity.

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