Information Technology Security (ITS)
Competency Requirements

This competency listing serves to identify the major knowledge, skills, and standards areas which the Information Technology Security (ITS) specialist needs in order to perform the professional tasks associated with the development of security plans and processes for information technology and cybersecurity. An ITS should have prior networking experience; certification in networking practices is highly suggested.

Information Technology Security specialists must be knowledgeable in the following technical areas:

1.0 Hardware Network Security Fundamentals

- 1.1 Define and explain both hardware and software firewalls including:
  - 1.1.1 Stateful firewalls
    - 1.1.1.1 Deep Packet Inspection (DPI)
  - 1.1.2 Application level firewalls
- 1.2 Explain the use of servers, gateway servers, Virtual Private Networks (VPNs) and proxy servers
  - 1.2.1 Identify the differences between the following proxies:
    - 1.2.1.1 Reverse proxies
    - 1.2.1.2 Transparent proxies
    - 1.2.1.3 Anonymous proxies
    - 1.2.1.4 Highly anonymous proxies
    - 1.2.1.5 Socks 4 and 5 proxies
    - 1.2.1.6 Domain Name System (DNS) proxies
- 1.3 Explain a perimeter network or “Demilitarized Zone” (DMZ) and why it is used
- 1.4 Explain data redundancy and RAID (Redundant Array of Independent Disks)
  - 1.4.1 Identify how data redundancy can be implemented
  - 1.4.2 List types of RAID arrays
- 1.5 Explain how to set up physical security procedures for IT systems
- 1.6 Identify how to use embedded system security
  - 1.6.1 Describe security level access terminology

2.0 Software Network Security

- 2.1 Identify and explain network protocols
- 2.2 Define the “OSI Model” and its relation to network security
- 2.3 Identify basic port numbers in regards to network security
- 2.4 Describe how patch management relates to software security
- 2.5 Identify antivirus, and anti-malware software suites
  - 2.5.1 Describe how security software should be deployed
- 2.6 Identify methods to manage access control
- 2.7 Describe “Domain Name System” (DNS) attack mitigations to include:
  - 2.7.1 Denial of Service (DoS)
  - 2.7.2 Distributed Denial of Service (DDoS)
  - 2.7.3 Cache Poisoning
  - 2.7.4 DNS Amplification
  - 2.7.5 Fast-flux DNS
  - 2.7.6 Zero Day Attack
- 2.8 Explain how TCP/IP Hijacking is accomplished the accompanying attacks including:
  - 2.8.1 Man-in-the-Middle
    - 2.8.1.1 Replay attack
  - 2.8.2 Evil Twin
- 2.9 Explain Structured Query language (SQL) access security procedures
  - 2.9.1 Identify the configuration of Internet Information Services (IIS) to access SQL Server
  - 2.9.2 Explain an SQL Injection attack

3.0 Wireless Security

- 3.1 Describe the IEEE wireless security standards
  - 3.1.1 Explain the purpose for wireless encryption keys
  - 3.1.2 “Temporal Key Integrity Protocol” (TKIP)

- 3.1.3 "Advanced Encryption Standard" (AES)
- 3.1.4 "Counter Mode with Cipher Block Chaining Message Authentication Code Protocol" (CCMP) (IEEE 802.11i)

3.2 Identify security best practices for wireless networks
3.3 Identify and explain wireless network attack vectors
3.4 Explain "Wireless Access Point" (WAP) technology
- 3.4.1 Explain Wireless Transport Layer Security (WTLS)
- 3.4.2 Describe these different types of IEEE wireless protocols:
  - 3.4.2.1 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac
- 3.4.3 Describe IEEE 802.1x and the "Extensible Authentication Protocol" (EAP)
- 3.4.4 Define "Remote Authentication Dial In User Service" (RADIUS) protocol
- 3.4.5 Describe wireless network security protocols (WEP, WPA, WPA2)

4.0 Device Security

4.1 Identify security concepts that are needed with the development of Internet of Things (IoT)
4.2 Describe the vulnerabilities associated with Bluetooth technology
4.3 Explain the vulnerabilities of mobile devices and how to mitigate them
4.4 Identify possible attack vectors for device security

5.0 Software Exploitations and Vulnerabilities

5.1 Explain what computer malware is and how it can disrupt a computer's operation
- 5.1.1 Identify how different malware (malicious software) affects computers including:
  - 5.1.1.1 Spyware
  - 5.1.1.2 Keyloggers
  - 5.1.1.3 Viruses
  - 5.1.1.4 Logic bombs
  - 5.1.1.5 Worms
  - 5.1.1.6 Trojans
  - 5.1.1.7 other malicious code that infiltrates a computer
- 5.1.2 Explain how a "botnet" works across a network
- 5.1.3 Explain Ransomware and how it used
- 5.1.4 Identify how a Back Door is used
- 5.1.5 Explain the concept of "Reverse Shells" within a network
- 5.1.6 Explain "Weak Keys" and "Password Guessing"

5.2 Explain and describe different attack vectors on a network

6.0 Operational Standards, Policies and Risk Assessments

6.1 Identify forms of risk in security management
6.2 Explain different forms of operational standards and policies to mitigate risk
6.3 Identify network exposure factors and how to calculate potential loss
6.4 Explain operational security controls and how they work
6.5 Identify Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) including:
- 6.5.1 Explain how IDS and IPS work
- 6.5.2 Explain methods of intrusion such as honeynets and honeypots

6.6 Identify key points required for a typical network enterprise disaster plan
6.7 Describe network security tools and procedures to:
- 6.7.1 Identify safeguards against virus attacks
- 6.7.2 Explain incident handling
- 6.7.3 Identify software used to monitor activities

6.8 Identify backup tools used in safeguarding critical resources to include:
- 6.8.1 software
- 6.8.2 hardware

6.9 Explain Transport Layer and Secure Socket Layer (SSL) in network cybersecurity including the Hyper Text Transport Protocol over Secure Socket layer (HTTPS)

7.0 Physical Security: Disaster Recovery and Computer Forensics

7.1 Identify and describe the different forms of data classification
7.2 Explain "clean desk policy"
7.3 Identify key points required for an enterprise disaster recovery plan and how it is developed

- 7.3.1 Continuity of Operations Planning (COOP)
- 7.3.2 secure recovery

7.4 Explain succession planning
7.5 Explain computer forensics and how it is used
7.6 Identify the responsibilities of a “Computer Incident Response Team” (CIRT)
7.7 Identify physical security procedures and policies, including access control
- 7.7.1 Explain methods of network equipment security to include:
  - 7.7.1.1 enclosure security
  - 7.7.1.2 “Defense in Depth” strategy
  - 7.7.1.3 layered security

8.0 Cryptography

8.1 Identify the three types of authentication:
- 8.1.1 password
- 8.1.2 blocker tag (RSA®)/smartcard
- 8.1.3 biometrics

8.2 Explain asymmetric and symmetric style key encryption including:
- 8.2.1 Cryptography
- 8.2.2 Hashing

8.3 Explain Public Key Infrastructure (PKI) including:
- 8.3.1 trust models
- 8.3.2 certificates and revocation

8.4 Explain PGP (Pretty Good Privacy)(Source of Certificate Authorities)
8.5 Explain in depth knowledge of multi-factor authentication
8.6 Explain in depth encryption technologies and block ciphers such as Twofish, Blowfish AES
8.7 Explain stream ciphers in depth
8.8 Describe Secure Hash Algorithm (SHA) and define MD5 collisions

9.0 Social Engineering

9.1 Explain the different types of social engineering attacks
- 9.1.1 Identify processes involved in:
  - 9.1.1.1 phishing attacks
  - 9.1.1.2 pretexting
  - 9.1.1.3 baiting
  - 9.1.1.4 Scareware attacks
  - 9.1.1.5 email spoofing
- 9.1.2 Explain “quid pro quo”
- 9.1.3 Explain how tailgating works

9.2 Identify methods and tools for countering social engineering attacks
9.3 Explain internet social engineering principles used in psychological manipulation
9.4 Explain how advanced persistent threats are orchestrated

End of Information Technology Security Competency

Find An ETA Test Site: http://www.eta-i.org/testing.html

Suggested Additional Resource and Study Material:

As with most networking systems, you will find details and information on Websites: dhs.gov; nist.gov; ieee.org; sans.org, (sans.edu); sae.org; rsa.com (blogs.rsa.com); schneier.com, networkcomputing.com; cisco.com; pcworld.com; cnet.com; computerworld.com; pcmag.com; consumerreports.org; maximumpc.com; infoworld.com; microsoft.com; itunes.apple.com; rmroberts.com; professormesser.com; youtube.com; and many, many other websites.

ITS By The Numbers; T. Houser, Michael Goshen; Self Publishing; 2017; ebook & softcover;

Cyber Reconnaissance, Surveillance and Defense; Robert Shimonski; ISBN 978-0128013083; Syngress; 2014; softcover; 258 pgs

Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information; Michael Bazzell; ISBN 978- 1530508907; Create Space Publishing; 2016; softcover; 422 pgs.

Cybersecurity and Cyberwar: What Everyone Needs to Know; P.W. Singer, Allan Friedman; ISBN 978-0199918119; Oxford Univ. Press; 2014; softcover; 320 pgs.

Thinking Security: Stopping Next Year's Hackers; Steven Bellovin; ISBN 978-0134277547; Addison-Wesley Professional Computing Series; Nov.2015; hardcover; 400 pgs.

Information Technology Security Specialist Committee Advisory Board:

Capano, Daniel, CWSP	dcapano@sbcglobal.net
Carr, Frederick,	fwcarr@gmail.com
Gonzales, Brandon CETsr	bsgonzales@bsu.edu
Goshen, Michael, CST, ITS	
Houser, T., RESIma, CST, NST, ITS	tcat.houser@gmail.com
Kirkpatrick, Ed, PVI, CSS	ekirkpatrick@eta-i.org
Kirschbaum, Tim, NST, CST, FOT	kirschbaumt@hotmail.com
Klier, Brian	brian.klier@gmail.com
Moran, Bruce	bruce@totalrecallpress.com

ETA certification programs are accredited through the ICAC, complying with the ISO/IEC 17024 standard.

