CCNA Security 2.0 Study Material – Chapter 11: Managing a Secure Network

itexamanswers.net/ccna-security-2-0-study-material-chapter-11-managing-secure-network.html

October 9, 2017

Chapter Outline:

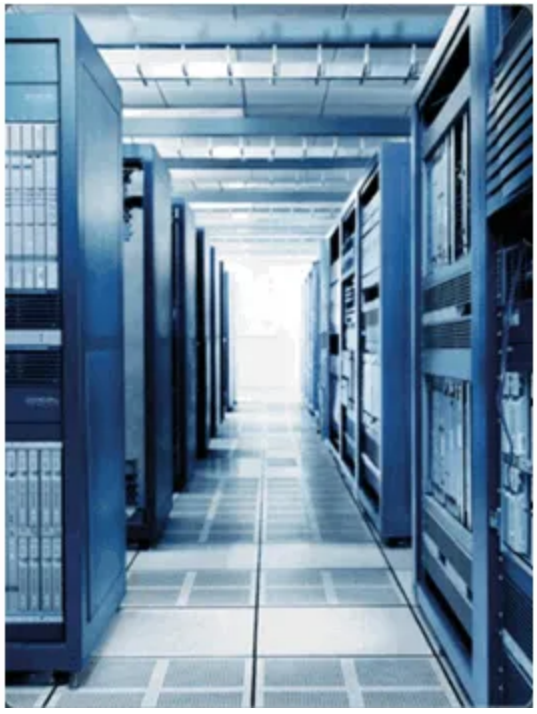
Section 11.1: Network Security Testing

Upon completion of this section, you should be able to:

- Describe the techniques used in network security testing.
- Describe the tools used in network security testing.

Topic 11.1.1: Network Security Testing Techniques

Operations Security



Testing and Evaluating Network Security

Objectives of ST&E:

- Uncover design, implementation, and operational flaws that could lead to the violation of the security policy.
- Determine the adequacy of security mechanisms, assurances, and device properties to enforce the security policy.
- Assess the degree of consistency between the system documentation and its implementation.

Types of Network Tests

Operational Status of the Network:

- Penetration testing
- Network scanning
- Vulnerability scanning
- Password cracking
- Log review
- Integrity checks
- Virus detection

Applying Network Test Results

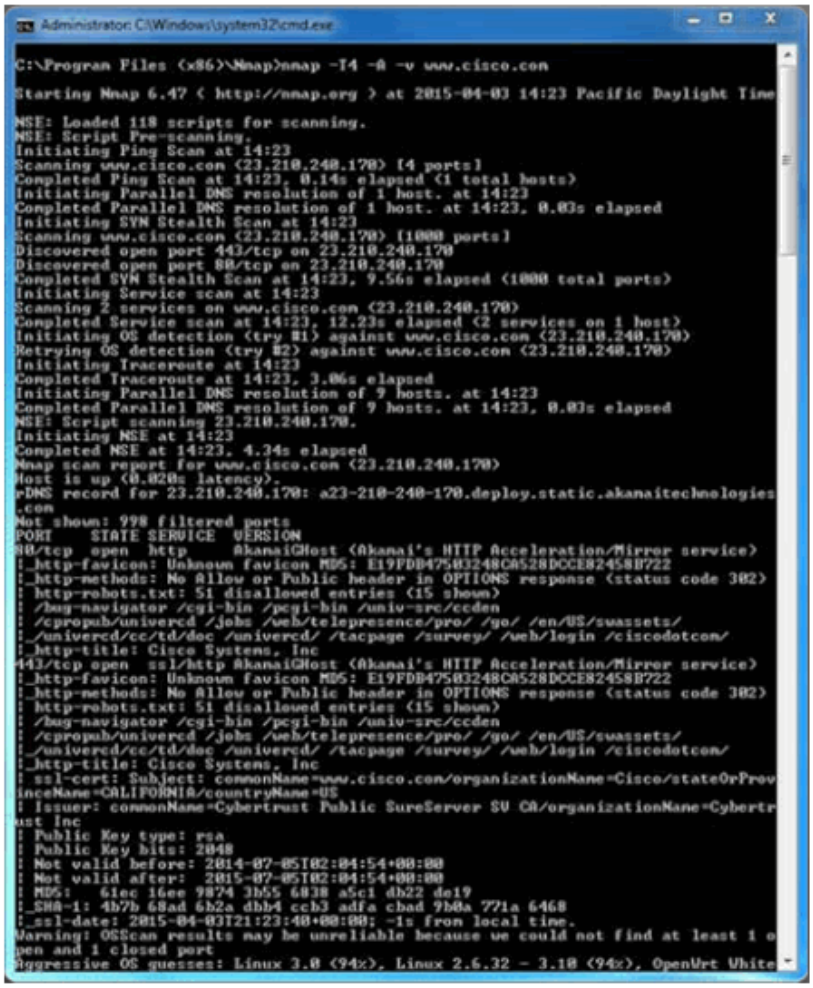
Topic 11.1.2: Network Security Testing Tools

Network Testing Tools

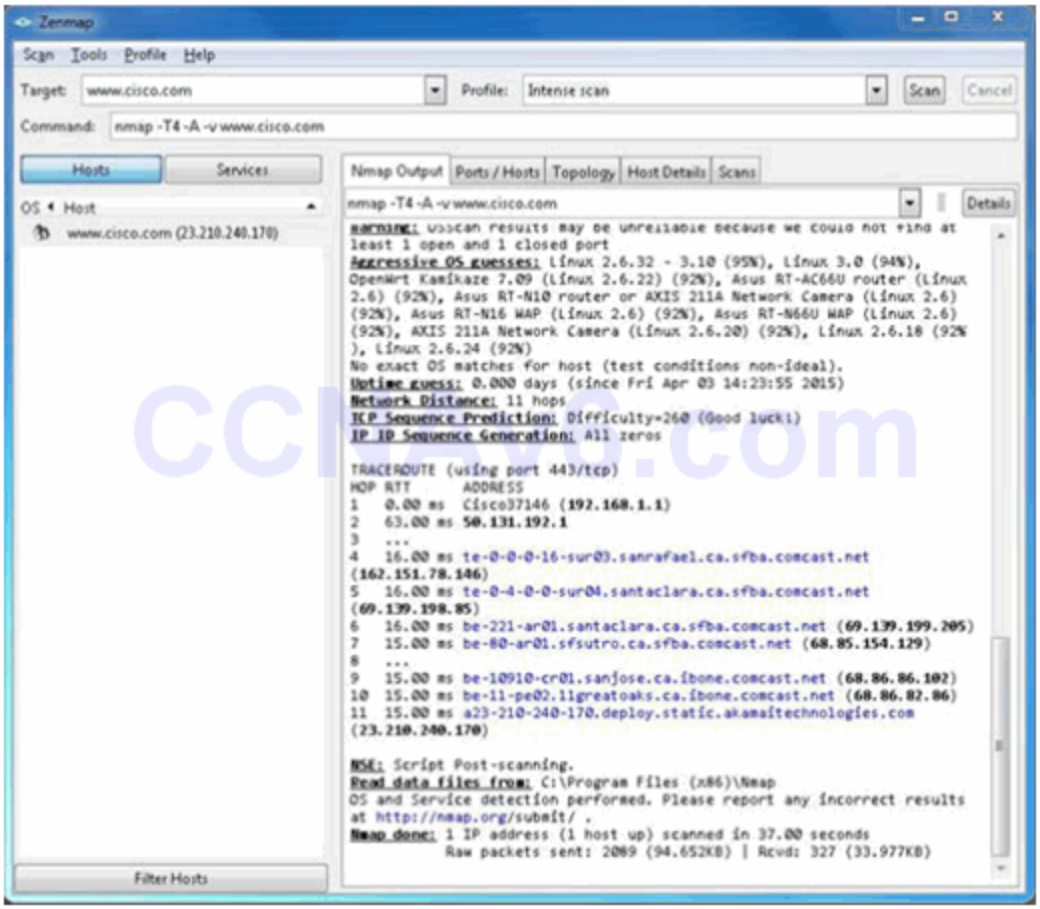
- Nmap/Zenmap
- SuperScan
- SIEM
- GFI LANguard
- Tripwire
- Nessus
- LOphtCrack
- Metasploit

Nmap and Zenmap

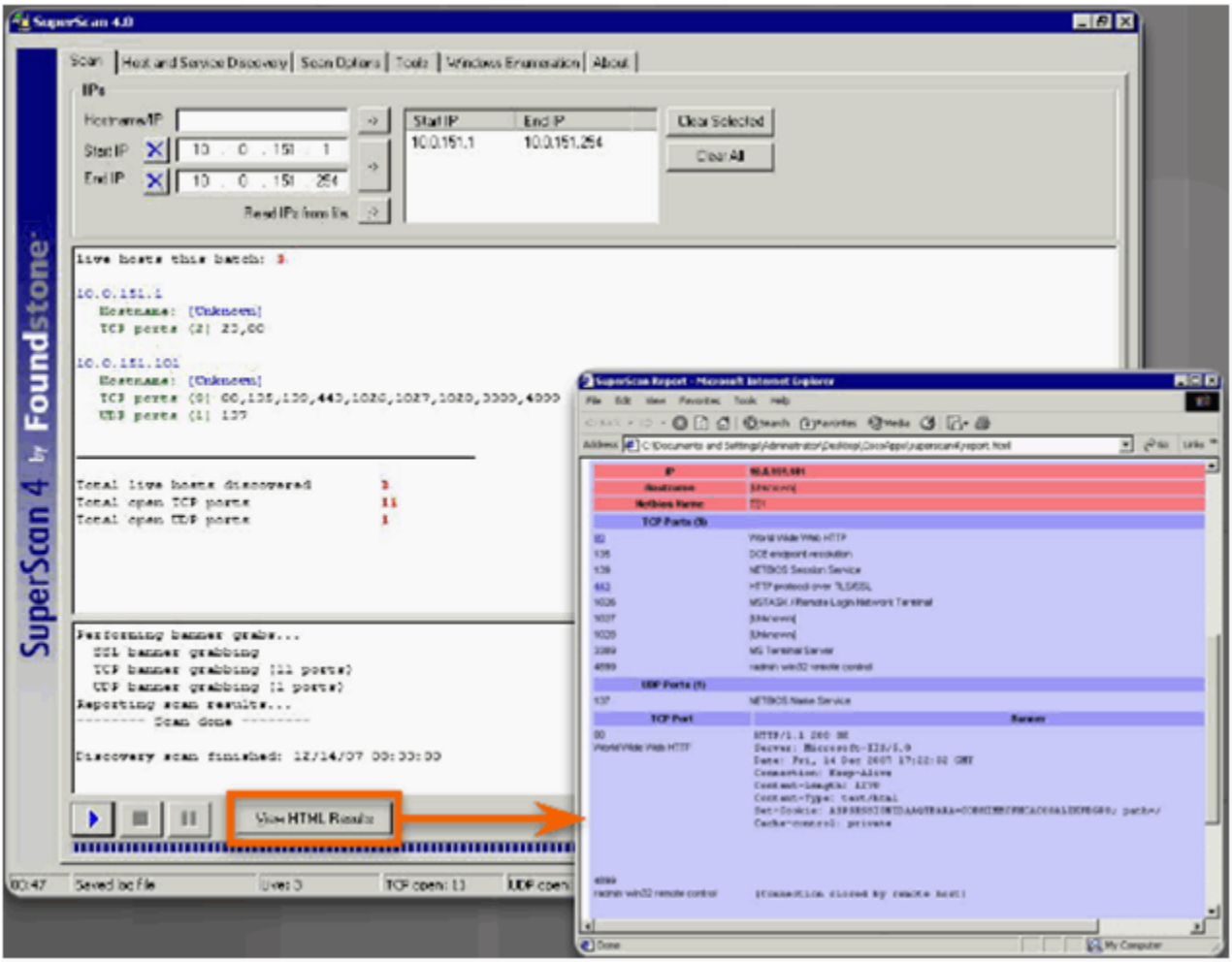
Sample Nmap Screenshot



Sample Zenmap Screenshot


Zenmap
Scan Tools Profile Help
Target: www.cisco.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v www.cisco.com
Hosts
Services
OS Host
www.cisco.com (23.210.240.170)
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v www.cisco.com
Details
WARNING: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 - 3.10 (95%), Linux 3.0 (94%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (92%), Asus RT-AC66U router (Linux 2.6) (92%), Asus RT-N10 router or AXIS 211A Network Camera (Linux 2.6) (92%), Asus RT-N16 WAP (Linux 2.6) (92%), Asus RT-N66U WAP (Linux 2.6) (92%), AXIS 211A Network Camera (Linux 2.6.20) (92%), Linux 2.6.18 (92%), Linux 2.6.24 (92%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.000 days (since Fri Apr 03 14:23:55 2015)
Network Distance: 11 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 0.00 ms Cisco37146 (192.168.1.1)
2 63.00 ms 50.131.192.1
3 ...
4 16.00 ms te-0-0-0-16-sur03.sanrafael.ca.sfba.comcast.net (162.151.78.146)
5 16.00 ms te-0-4-0-0-sur04.santaclara.ca.sfba.comcast.net (69.139.198.85)
6 16.00 ms be-221-ar01.santaclara.ca.sfba.comcast.net (69.139.199.205)
7 15.00 ms be-80-ar01.sfsutro.ca.sfba.comcast.net (68.85.154.129)
8 ...
9 15.00 ms be-10910-cr01.sanjose.ca.ibone.comcast.net (68.86.86.102)
10 15.00 ms be-11-pe02.11greatoaks.ca.ibone.comcast.net (68.86.82.86)
11 15.00 ms a23-210-240-170.deploy.static.akamaitechnologies.com (23.210.240.170)
NSE: Script Post-scanning.
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.00 seconds
Raw packets sent: 2089 (94.652KB) | Rcvd: 327 (33.977KB)

SuperScan



SIEM

Essential functions:

- Forensic Analysis
- Correlation
- Aggregation
- Retention

Section 11.2: Developing a Comprehensive Security Policy

Upon completion of this section, you should be able to:

- Explain the purpose of a comprehensive security policy.
- Describe the structure of a comprehensive security policy.
- Describe the standards, guidelines, and procedures of a security policy.
- Explain the roles and responsibilities entailed by a security policy.
- Explain security awareness and how to achieve through education and training.
- Explain how to respond to a security breach.

Topic 11.2.1: Security Policy Overview

Secure Network Life Cycle

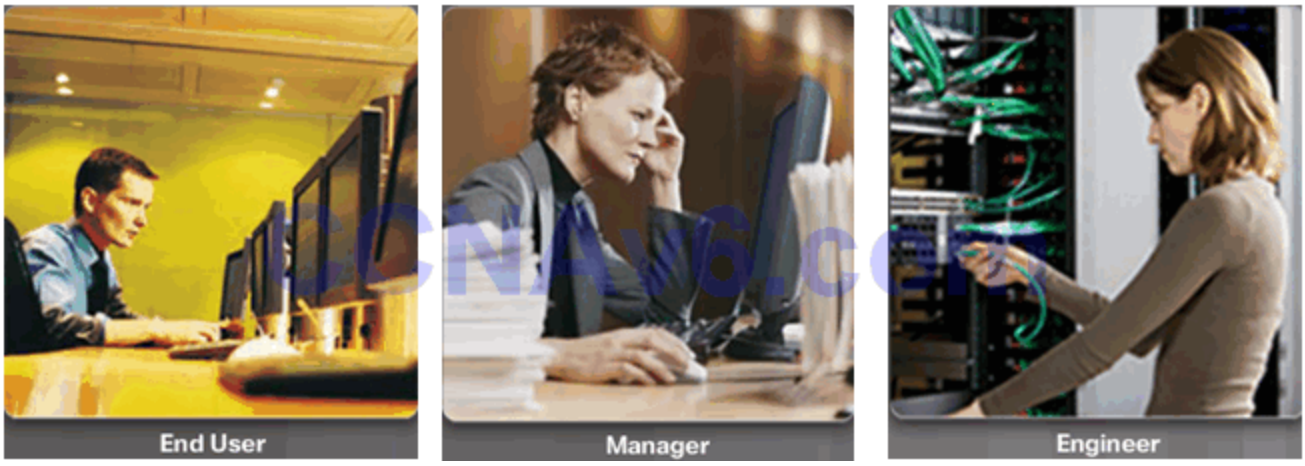
Determine what the assets of an organization are by asking:

- What does the organization have that others want?
- What processes, data, or information systems are critical to the organization?
- What would stop the organization from doing business or fulfilling its mission?

Security Policy

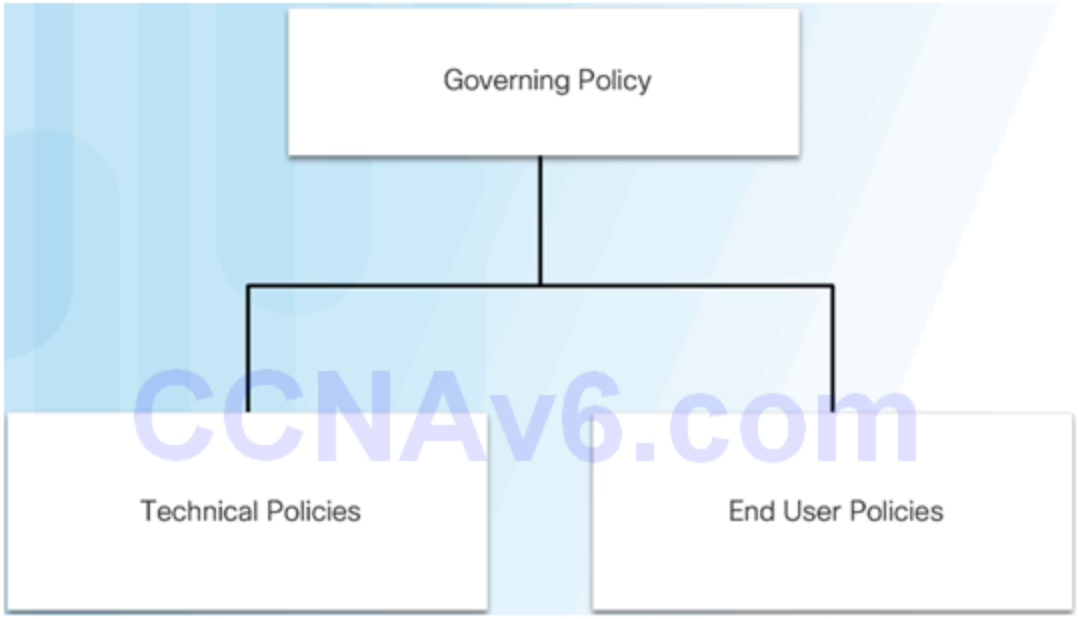
Security Policy Audience

Audience Determines Security Policy Content



Topic 11.2.2: Structure of a Security Policy

Security Policy Hierarchy



Governing Policy

A governing policy includes:

- Statement of the issue that the policy addresses
- How the policy applies in the environment
- Roles and responsibilities of those affected by the policy
- Actions, activities, and processes that are allowed (and not allowed)
- Consequences of noncompliance

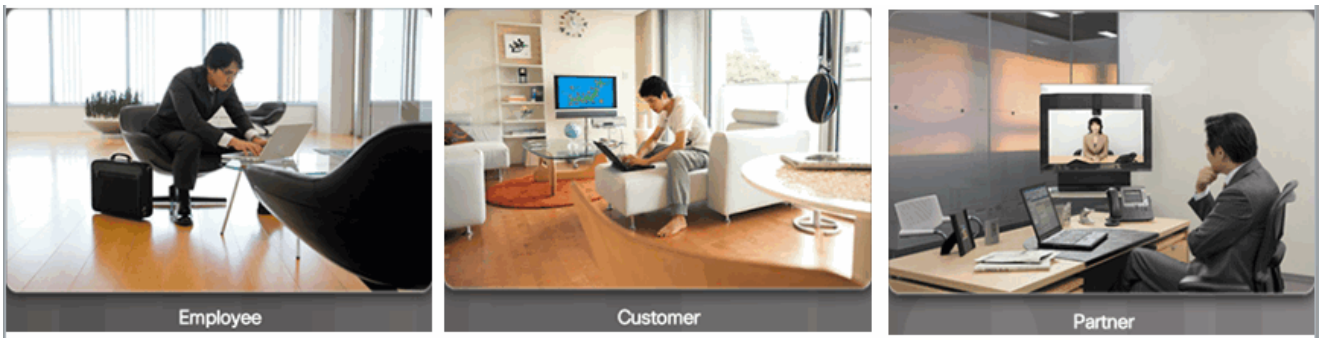
Technical Policies

Technical components:

- General policies
- Telephony policy
- Email and communication policy
- Remote access policy
- Network policy
- Application policy

End User Polices

Customize End-User Policies for Groups



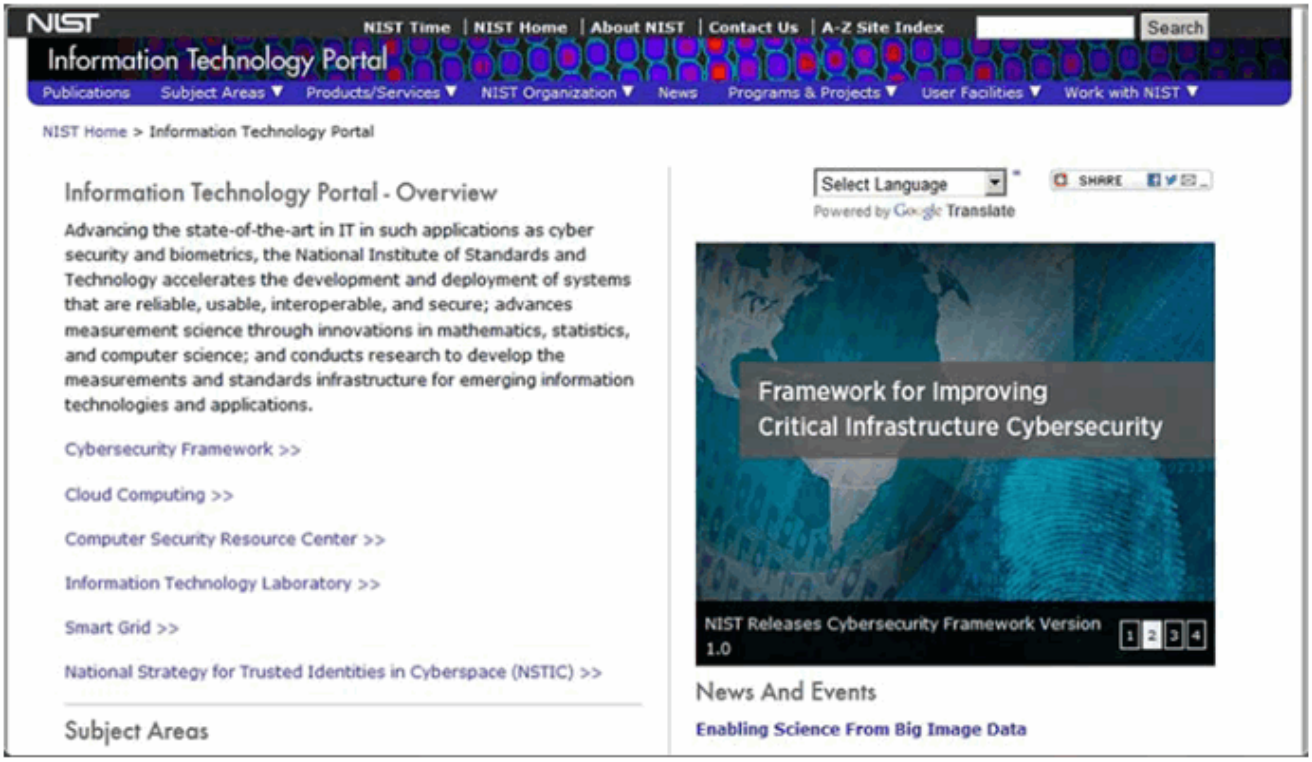
Topic 11.2.3: Standards, Guidelines, and Procedures

Security Policy Documents

Standards Documents

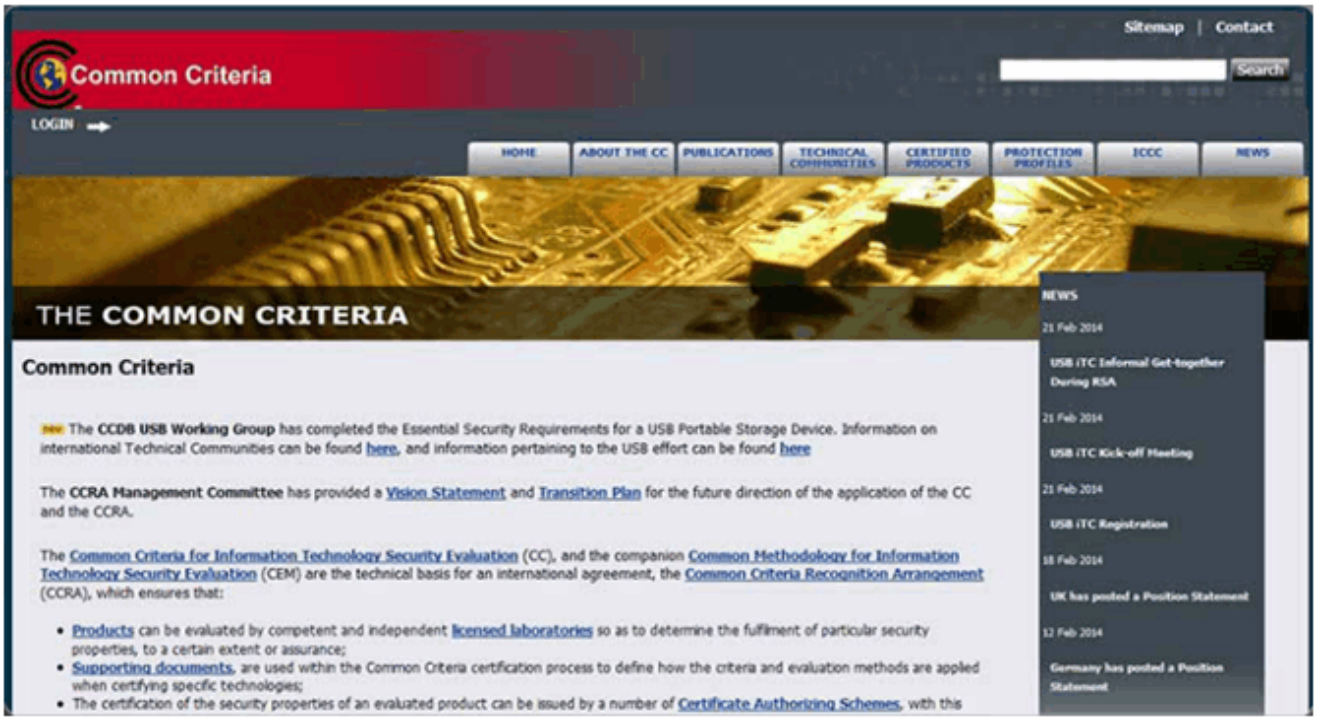
Guideline Documents

NIST Information Technology Portal



NSA Website

Common Criteria Website



Procedure Documents

Topic 11.2.4: Roles and Responsibilities

Organizational Reporting Structure

Common Executive Titles

- Chief Executive Officer (CEO)
- Chief Technology Officer (CTO)
- Chief Information Officer (CIO)

- Chief Security Officer (CSO)
- Chief Information Security Officer (CISO)

Topic 11.2.5: Security Awareness and Training

Security Awareness Program

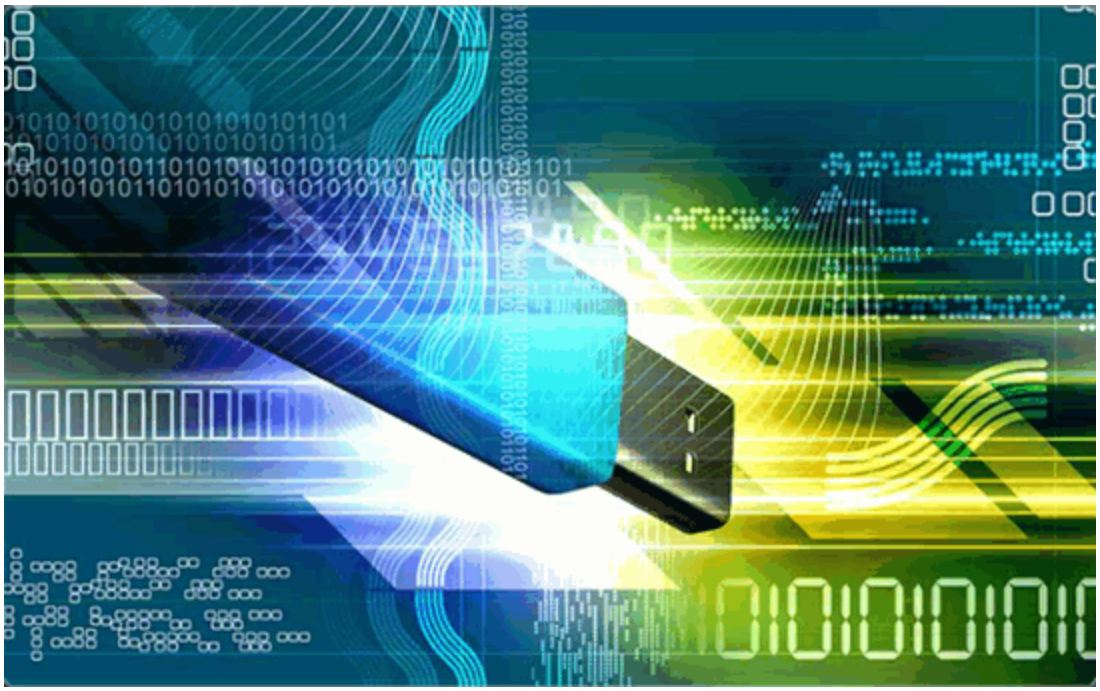
Primary components:

- Awareness campaigns
- Training and education

Topic 11.2.6: Responding to a Security Breach

Motive, Opportunity, and Means

Collecting Data



Section 11.3: Summary

Chapter Objectives:

- Explain the various techniques and tools used for network security testing.

- Explain how to develop a comprehensive security policy.

Download Slide PowerPoint (pptx):

[sociallocker id=”54558″]

CCNASv2_InstructorPPT_CH11.pptx **6.30 MB** **2185 downloads**

...

Download

[/sociallocker]