

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:

11.0 Introduction

11.1 Network Security Testing

11.2 Developing a Comprehensive Security Policy

11.3 Summary

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

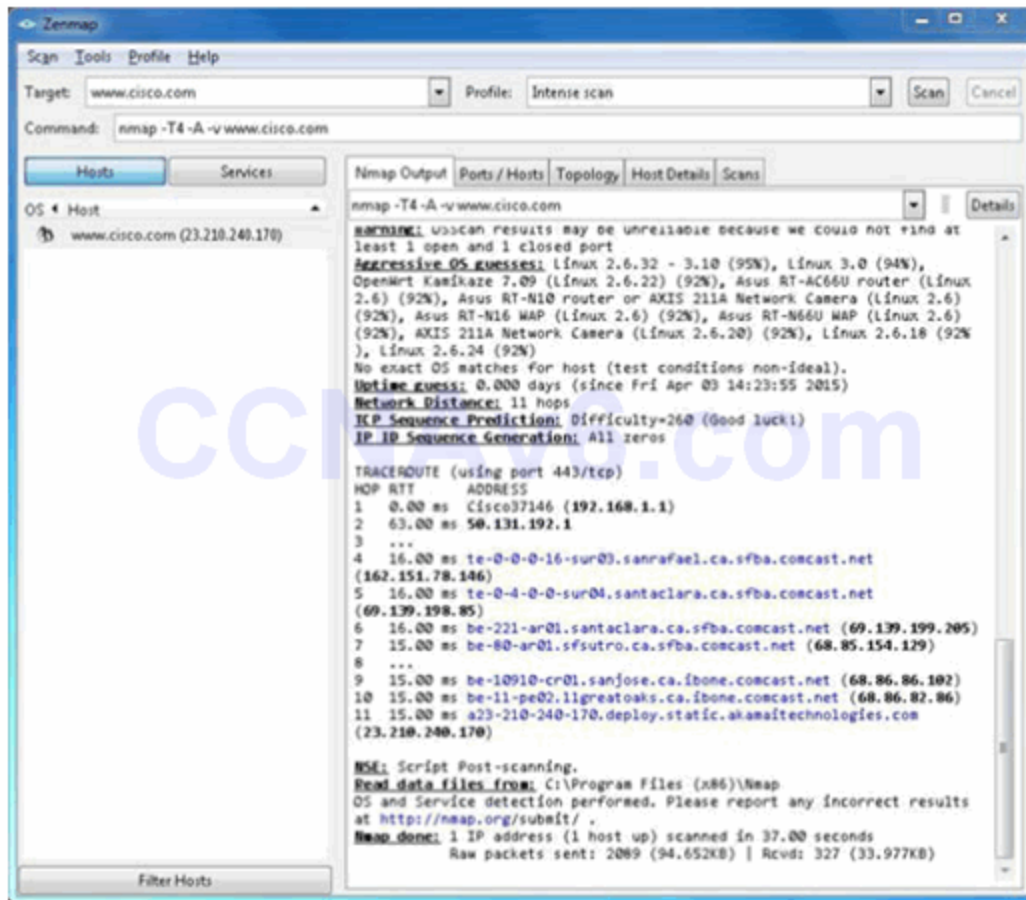
Sample Nmap Screenshot

```
Administrator: C:\Windows\system32\cmd.exe

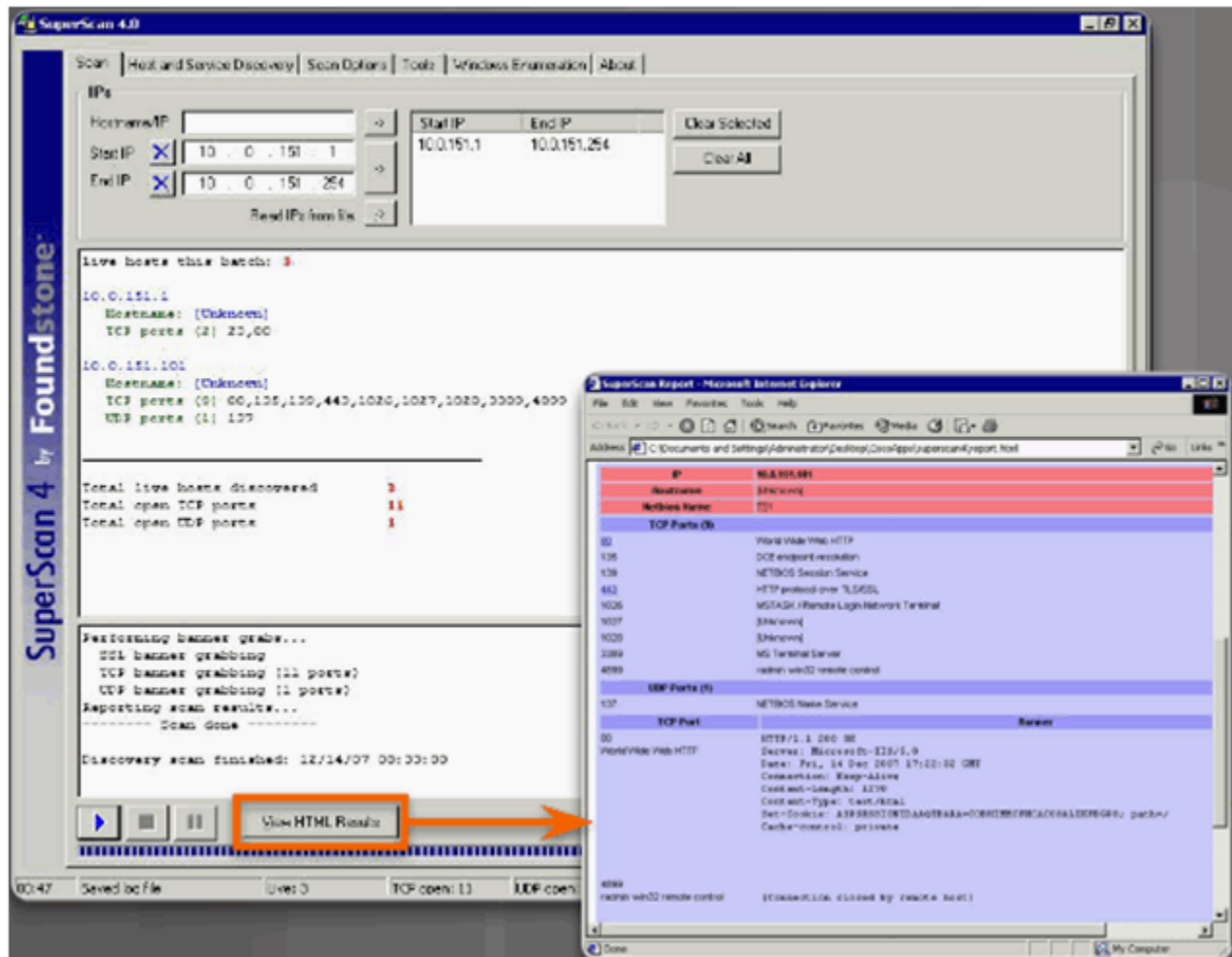
C:\Program Files (x86)\Nmap>nmap -I4 -A -v www.cisco.com

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-03 14:23 Pacific Daylight Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 14:23
Scanning www.cisco.com (23.210.240.170) [4 ports]
Completed Ping Scan at 14:23, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:23
Completed Parallel DNS resolution of 1 host. at 14:23, 0.03s elapsed
Initiating SYN Stealth Scan at 14:23
Scanning www.cisco.com (23.210.240.170) [1000 ports]
Discovered open port 443/tcp on 23.210.240.170
Discovered open port 80/tcp on 23.210.240.170
Completed SYN Stealth Scan at 14:23, 7.56s elapsed (1000 total ports)
Initiating Service scan at 14:23
Scanning 2 services on www.cisco.com (23.210.240.170)
Completed Service scan at 14:23, 12.23s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.cisco.com (23.210.240.170)
Retrying OS detection (try #2) against www.cisco.com (23.210.240.170)
Initiating Traceroute at 14:23
Completed Traceroute at 14:23, 3.06s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 14:23
Completed Parallel DNS resolution of 9 hosts. at 14:23, 0.03s elapsed
NSE: Script scanning 23.210.240.170.
Initiating NSE at 14:23
Completed NSE at 14:23, 4.34s elapsed
Nmap scan report for www.cisco.com (23.210.240.170)
Host is up (0.820s latency).
rDNS record for 23.210.240.170: a23-210-240-170.deploy.static.akanaitechnologies.com
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_ http-favicon: Unknown favicon MD5: E19FDB47583248C8528DCCE82458B722
|_ http-methods: No Allow or Public header in OPTIONS response (status code 302)
|_ http-robots.txt: 51 disallowed entries (15 shown)
|_ /bug-navigator/cgi-bin/cgi-bin/uniu-src/ccden
|_ /cpropub/univercd/jobs/web/telepresence/pro/go/en/US/swassets/
|_ /univercd/cc/td/doc/univercd/tacpage/survey/web/login/ciscodotcom/
|_ http-title: Cisco Systems, Inc
443/tcp    open  ssl/http  AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_ http-favicon: Unknown favicon MD5: E19FDB47583248C8528DCCE82458B722
|_ http-methods: No Allow or Public header in OPTIONS response (status code 302)
|_ http-robots.txt: 51 disallowed entries (15 shown)
|_ /bug-navigator/cgi-bin/cgi-bin/uniu-src/ccden
|_ /cpropub/univercd/jobs/web/telepresence/pro/go/en/US/swassets/
|_ /univercd/cc/td/doc/univercd/tacpage/survey/web/login/ciscodotcom/
|_ http-title: Cisco Systems, Inc
|_ ssl-cert: Subject: commonName=www.cisco.com/organizationName=Cisco/stateOrProv
inceName=CALIFORNIA/countryName=US
|_ issuer: commonName=Cybertrust Public SureServer SU CA/organizationName=Cybertr
ust Inc
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Not valid before: 2014-07-05T02:04:54+00:00
|_ Not valid after: 2015-07-05T02:04:54+00:00
|_ MD5: 61ec 16ee 7874 3b55 6838 a5c1 db22 de19
|_ SHA-1: 4b7b 68ad 6b2a dbb4 ccb3 adfa chad 7b8a 771a 6468
|_ ssl-date: 2015-04-03T21:23:40+00:00; -1s from local time.
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Aggressive OS guesses: Linux 3.0 (94%), Linux 2.6.32 - 3.10 (94%), OpenVrt White
```

Sample Zenmap Screenshot



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



End User



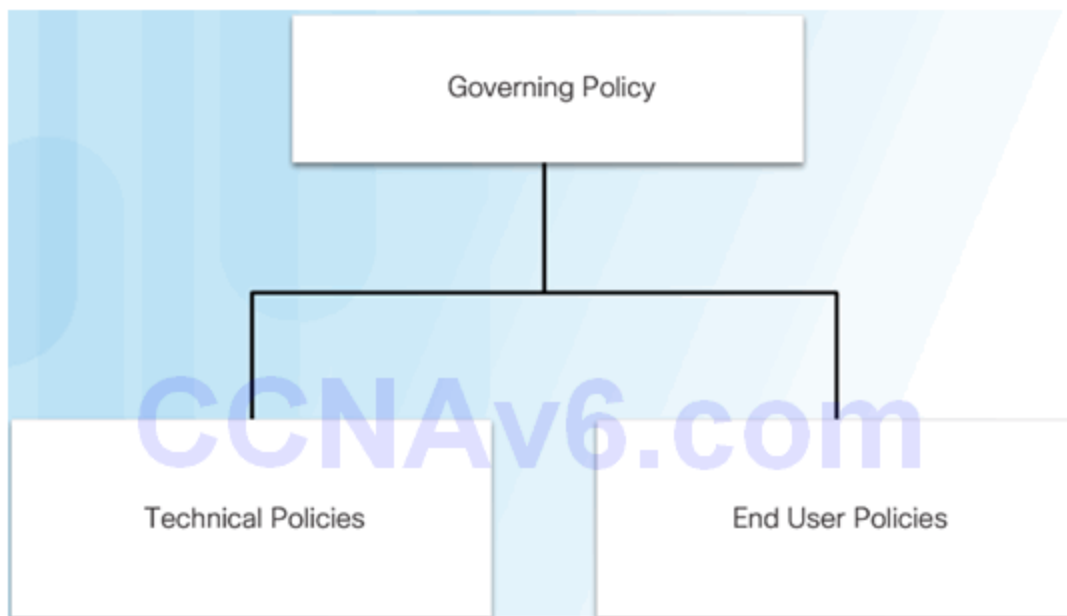
Manager



Engineer

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 Policies

Customize End-User Policies for Groups



Topic 11.2.3: Standards, Guidelines, and Procedures

Security Policy Documents



Standards Documents



Guideline Documents

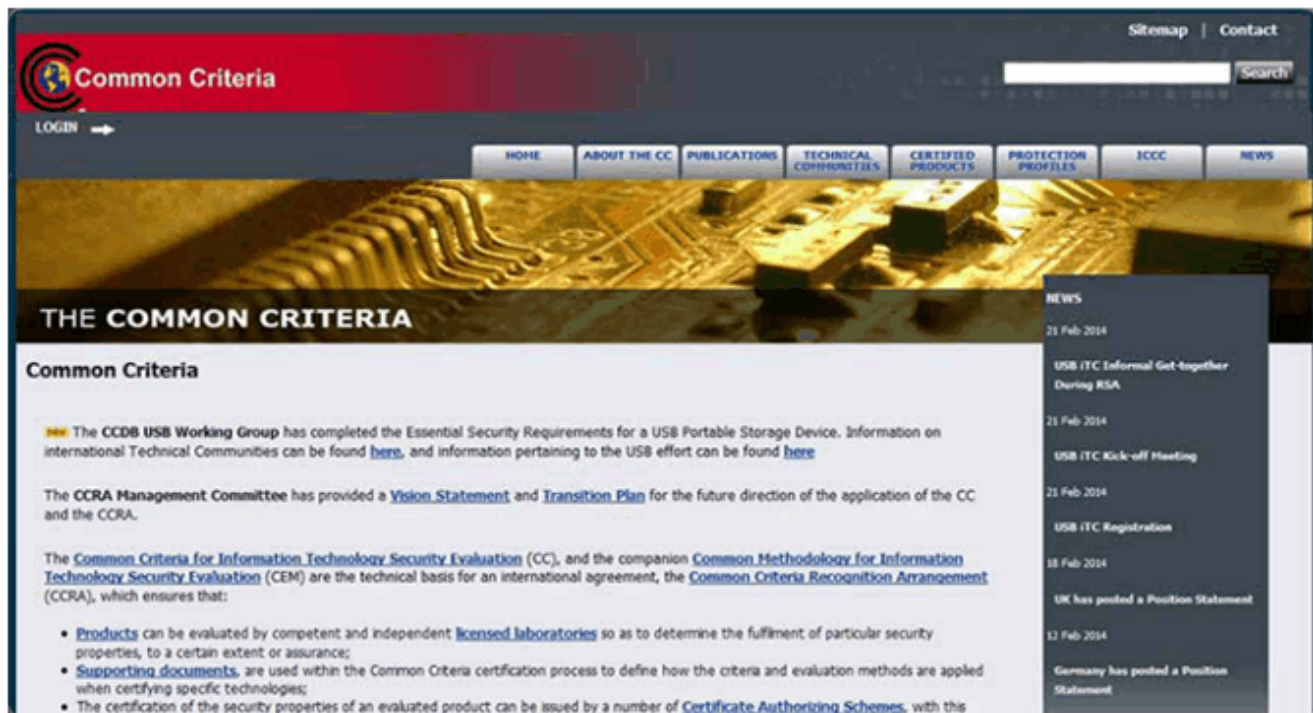
NIST Information Technology Portal

A screenshot of the NIST Information Technology Portal homepage. The header features the NIST logo and navigation links: NIST Time, NIST Home, About NIST, Contact Us, and A-Z Site Index. A search bar is on the right. Below the header is a blue navigation bar with links: Publications, Subject Areas, Products/Services, NIST Organization, News, Programs & Projects, User Facilities, and Work with NIST. The main content area is divided into two columns. The left column has a heading "Information Technology Portal - Overview" followed by a paragraph about advancing IT state-of-the-art. Below this are links to Cybersecurity Framework, Cloud Computing, Computer Security Resource Center, Information Technology Laboratory, Smart Grid, and National Strategy for Trusted Identities in Cyberspace (NSTIC). The right column has a "Select Language" dropdown, a "Powered by Google Translate" note, and a "SHARE" button. Below this is a large image of a world map with the text "Framework for Improving Critical Infrastructure Cybersecurity". At the bottom of the right column, there is a section titled "News And Events" with a link to "Enabling Science From Big Image Data".

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:

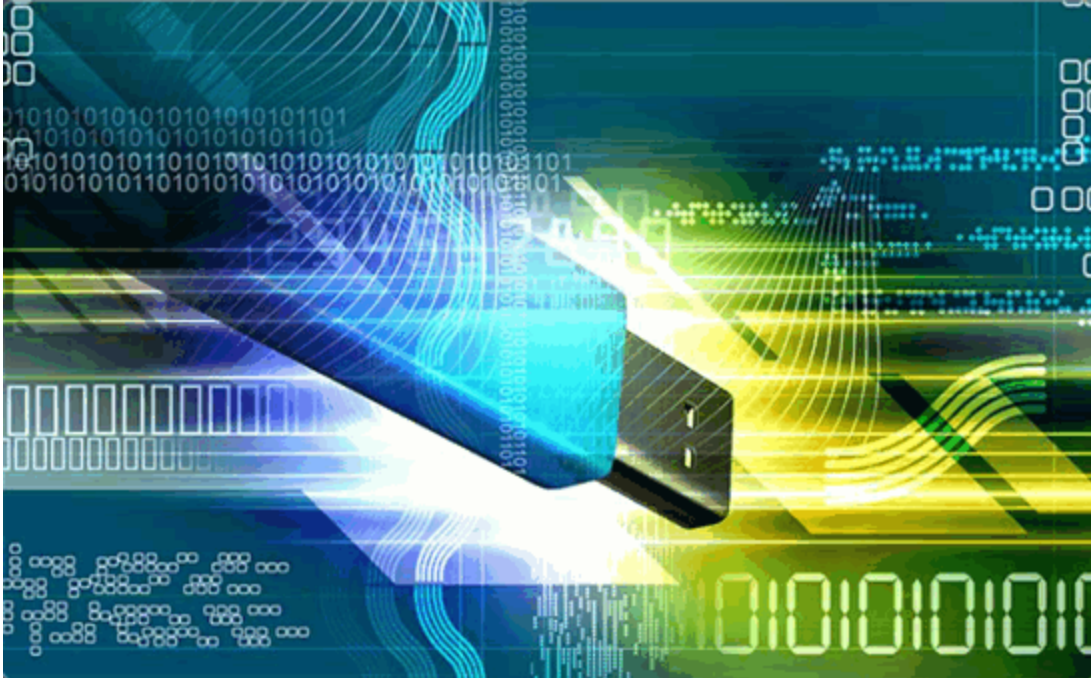
- Awareness campaigns
- Training and education



Topic 11.2.6: Responding to a Security Breach



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]