CCNA Security 640-554 Quick Reference

Anthony Sequeira

Cisco Press

CCNA Security 640-554 Quick Reference

Anthony Sequeira
CCIE, CCSI, VCP, Data Center Specialist

ciscopress.com

About the Author

Anthony Sequeira, CCIE No. 15626, is a Cisco Certified Systems Instructor and auth
tracks of Cisco Certification. Anthony formally began his career in the information te
IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer
his true passion—teaching and writing about Microsoft and Cisco technologies. Anth
Computers in 1996 and lectured to massive audiences around the world about the late
Mastering Computers became the revolutionary online training company KnowledgeN
for many years. Anthony is currently pursuing his second CCIE in the area of Security
for the next generation of KnowledgeNet, StormWind Live.

About the Technical Editor

Sean Wilkinsis an accomplished networking consultant for SR-W Consulting (http:/
and has been in the field of IT since the mid 1990s working with companies such as C
AT&T. Sean currently holds certifications with Cisco (CCNP/CCDP), Microsoft (MC
and Network+). He also has a master's of science degree in Information Technology w
Architecture and Design, a master's of science degree in Organizational Management
Network Security, a bachelor's of science degree in Computer Networking, and an ass
Science in Computer Information Systems. In addition to working as a consultant, Se
technical writer and editor for various companies.

Chapter 1
Network Security Principles

Network Security Fundamentals

This section covers the need for network security and the security objectives found within most or examines the different types of attacks that modern networks can experience.

Why Do We Need Network Security?

Network threats include internal and external threats. Internal threats are the most serious. These t practices are not followed. For example, blank or default passwords are used, or in-house develop practices.

External threats typically rely on technical methods to attack the network. The CCNA in Security using technical means. Firewalls, routers with access control lists (ACL), intrusion prevention sys the focus.

Network Security Objectives

Network security should provide the following:

- Data confidentiality
- Data integrity
- Data and system availability

Confidentiality ensures that only authorized individuals can view sensitive data. Powerful method
encryption and access controls.

Integrity ensures that data has not been changed by an unauthorized individual.

Availability ensures that access to the data is uninterrupted. Denial-of-service (DoS) attacks attem
These attacks typically try to fail a system using an unexpected condition or input, or fail an entire
information.

Assets, Vulnerabilities, and Threats

Assets are anything of value to the organization. Not all assets have the same value. An organizati

A *vulnerability* is a weakness in a system or a design that might be exploited. Common categories
weaknesses, and software vulnerabilities. There is a National Vulnerability Database and also a C
Exposures document.

A *threat* is a potential danger to information or systems.

A *countermeasure* is a safeguard that mitigates against potential risks. Countermeasures are typica
physical controls.

Information security risk is the measure of the impact of threat vectors exploiting the vulnerabilitie

Data Classification

Public-sector classification levels include the following:

- Unclassified
- Sensitive but unclassified (SBU)

- Confidential
- Secret
- Top-secret

Private-sector classification levels include the following:

- Public
- Sensitive
- Private
- Confidential

Classification criteria include the following:

- **Value:** This is the most important factor.
- **Age:** With time, the sensitivity of data typically decreases.
- **Useful life:** Information can be made obsolete with newer information.
- **Personal association:** The data is associated with sensitive issues or individuals.

Classification roles include the following:

- Owner
- Custodian (responsible for the day-to-day management of the data)
- User

Security Controls

Administrative controls involve policies and procedures.

Technical controls involve electronics, hardware, and software.

Physical controls are mostly mechanical.

Controls are categorized as preventative, deterrent, or detective.

Responses

Investigators must prove motive, opportunity, and means.

The system should not be shut down or rebooted before the investigation begins.

Laws and Ethics

Security policy must attempt to follow criminal, civil, and administrative law.

Ethics refer to values that are even higher than the law.

Network Attack Methodologies

You must understand the command types of attacks that a network can experience. Studying these
against them.

Motivations and Classes of Attack

A *vulnerability* is a weakness in a system that can be exploited by a threat.

A *risk* is the likelihood that a specific attack will exploit a particular vulnerability of a system.

An *exploit* happens when computer code is developed to take advantage of a vulnerability.

The main vulnerabilities of systems are categorized as follows:

- Design errors
- Protocol weaknesses
- Software vulnerabilities
- Misconfiguration
- Hostile code
- Human factor

Potential adversaries can include the following:

- Nations or states
- Terrorists
- Criminals
- Hackers
- Corporate competitors
- Disgruntled employees
- Government agencies

Many different classifications are assigned to hackers, including the following:

- **Hackers:** Individuals who break into computer networks and systems to learn more about
- **Crackers (criminal hackers):** Hackers with a criminal intent to harm information system
- **Phreakers (phone breakers):** Individuals who compromise telephone systems.
- **Script kiddies:** Individuals with low skill level. They do not write their own code. Instead more skilled attackers.
- **Hacktivists:** Individuals who have a political agenda in doing their work.
- **Academic hackers:** People who enjoy designing software and building programs with a s cleverness.
- **Hobby hacker:** Focuses mainly on computer and video games, software cracking, and the hardware and other electronic devices.

How Does a Hacker Usually Think?

1. Perform footprint analysis (reconnaissance).
2. Enumerate applications and operating systems.
3. Manipulate users to gain access.
4. Escalate privileges.
5. Gather additional passwords and secrets.
6. Install back doors.
7. Leverage the compromised system.

Defense in Depth

The defense-in-depth strategy recommends several principles:

- Defend in multiple places.
- Defend the enclave boundaries.
- Defend the computing environment.
- Build layered defenses.
- Use robust components.
- Use robust key management.
- Deploy IDS or IPS.

Enumeration and Fingerprinting

Ping sweeps and *port scans* are common practices to identify all devices and services on the netwo
typically the first steps in a much larger more damaging attack.

IP Spoofing

IP spoofing refers to forging the source address information of a packet so that the packet appears
network. IP spoofing is often the first step in the abuse of a network service, or a DoS type of atta

In IP spoofing, the attacker sends messages to a computer with an IP address that indicates the me

The basis of IP spoofing lies in an inherent security weakness in TCP known as *sequence predictio*
TCP sequence numbers that are used to construct a TCP packet without receiving any responses fi
allows them to spoof a trusted host on a local network.

IP spoofing attacks are categorized in one of two ways:

- **Nonblind spoofing:** The attacker sniffs the sequence and acknowledgment numbers and c
- **Blind spoofing:** The attacker sends several packets to the target machine to sample sequer for the attack.

Spoof attacks are often combined with IP source-routing options set in packets. *Source routing* is t within the IP header a full routing path between endpoints. Cisco IOS routers drop all source-route `route global` command is configured. Security devices, such as Cisco PIX 500 Series Security 5500 Series Adaptive Security Appliances, drop such packets by default.

Man-in-the-middle attacks are often the result of TCP/IP spoofing. Figure 1-1 shows a man-in-the identify the client and server IP addresses and relative port numbers. The attacker then modifies h packets from the client. The attacker waits to receive an ACK packet from the client communicati contains the sequence number of the next packet that the client expects. The attacker replies to the the source address of the server and the destination address of the client. This packet results in a re client. The attacker takes over communications with the server by spoofing the expected sequence sent from the legitimate client to the server.

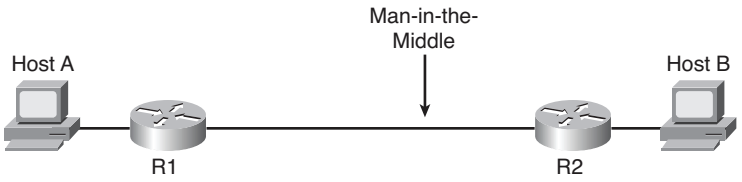

Figure 1-1 Man-in-the-Middle Attack

Confidentiality Attacks

Attackers can use many methods to compromise confidentiality. Following are some of the comm

- **Packet sniffing:** Eavesdropping and logging traffic that passes over a digital network or p
- **Port scanning:** Searching a network host for open ports.
- **Dumpster diving:** Searching through company dumpsters, looking for information that c information for hackers.
- **Emanations capturing:** Capturing electrical transmissions from the equipment of an orga about the organization.
- **Wiretapping:** Monitoring the telephone or Internet conversations of a third party.
- **Social engineering:** Using social skills to manipulate people inside the network to provid the network.
- **Overt channels:** The ability to hide information within a transmission channel based on t another. *Steganography* is an example of an overt channel: hiding messages in digital pictu
- **Covert channels:** The ability to hide information within a transmission channel based on events.
- **Phishing, pharming, and identity theft:** *Phishing* is an attempt to criminally acquire sen usernames, passwords, and credit card details, by masquerading as a trustworthy entity. *P* redirecting the traffic of one website to another website.

Integrity Attacks

Hackers can use many types of attacks to compromise integrity:

- **Salami attacks:** A series of minor data security attacks that together result in a larger atta
- **Data diddling:** Changing data before or as it is input into a computer.

- **Trust exploits:** An individual taking advantage of a trust relationship within a network. P between a system in the DMZ and a system in the inside network.
- **Password attacks:** Any attack that attempts to identify a user account, password, or both.
- **Session hijacking:** The exploitation of a valid computer session to gain unauthorized acc computer system.

Availability Attacks

Hackers can use many types of attacks to compromise availability:

- **Botnets:** A collection of software robots that run autonomously and automatically.
- **DoS (denial-of-service):** An attack seeks to make a system or service unavailable after th traffic.
- **DDoS (Distributed DoS):** Hackers use a terminal to scan for systems to hack. The hacker them.
- **SYN floods:** The system is sent many different false SYN requests for TCP communicatio
- **ICMP floods:** The system is sent many false ICMP packets.
- **Electrical power:** Attacks involve power loss, reduction, or spikes.
- **Computer environment:** Temperature, airflow, humidity, water, and gas.

Blended Threats

A growing trend is for attacks to combine techniques. For example, malware that combines the ch Trojan horses, spyware, and others.

Best Practices for Mitigation

These include the following:

- Keep patches up-to-date.
- Shut down unnecessary services and ports.
- Use strong passwords, and change them often.
- Control physical access to systems.
- Avoid unnecessary web page inputs.
- Perform backups and test the backed-up files on a regular basis.
- Educate employees about the risks of social engineering.
- Encrypt and password-protect sensitive data.
- Implement security hardware and software.
- Develop a written security policy for the company.

Security Architecture Design Guidelines

- Defense in depth
- Compartmentalization
- Least privilege
- Weakest link
- Separation and rotation of duties
- Hierarchically trusted components and protection

- Mediated access
- Accountability and traceability
- Regulatory compliance
- Strengthened enforcement
- Global spread of data breach notification laws
- More prescriptive regulations
- Growing requirements regarding third parties (business partners)
- Risk-based compliance on the rise
- Compliance process streamlined and automated
- Examples: HIPAA, FISMA, and GLB

Operation Security

Secure Network Life Cycle Management

A general system development life cycle (SDLC) includes five phases:

- **Initiation:** Consists of a security categorization and a preliminary risk assessment.
- **Acquisition and development:** Includes a risk assessment, security functional requireme requirements analysis, cost considerations and reporting, security planning, security contr security test and evaluation, and other planning components.
- **Implementation:** Includes inspection and acceptance, system integration, security certific
- **Operations and maintenance:** Includes configuration management and control, and cont
- **Disposition:** Includes information preservation, media sanitization, and hardware and sof

Security Testing

Many types of testing techniques are available:

- Network scanning
- Vulnerability scanning
- Password cracking
- Log review
- Integrity checkers
- Virus detection
- War dialing
- War driving (802.11 or wireless LAN testing)
- Penetration testing

The following list is a collection of popular tools:

- Nmap
- GFI LANguard
- Tripwire
- Nessus
- Metasploit
- SuperScan by Foundstone, a division of McAfee

Incident Management

- Preparation
- Detection and analysis
- Containment, eradication, recovery
- Post-incident activities

Computer Crime Investigations

- **Motive:** Why did they do it?
- **Opportunity:** Were they able to do it?
- **Means:** Were they capable of doing it?

Disaster Recovery

Possible disruptions can be categorized as follows:

- **Nondisaster:** A situation in which business operations are interrupted for a relatively shor
- **Disasters:** These cause interruptions of at least a day.
- **Catastrophe:** The facilities are destroyed, and all operations must be moved.
- **Business Continuity Concepts**
- **Maximum Tolerable Downtime (MTD):** The maximum length of time a business functi causing irreparable harm to the business

- **Recovery Time Objective (RTO):** The duration of time that a service level within a busi
  disaster (or disruption) in order to avoid unacceptable consequences associated with a bre
- **Recovery Point Objective (RPO):** The maximum tolerable period in which data might b
  major incident

Backups

- **Hot site:** A completely redundant site with similar equipment to the original site.
- **Warm site:** A facility with similar equipment to the original site but is unlikely to have cu
  frequent replication with the original site.
- **Cold site:** Does not typically contain redundant computing equipment (for example, serve

Borderless Networking

Mobility is dissolving the borders of networks. The borderless end zone consists of intelligent end
broad coverage, persistent connectivity, and advanced security. A secure virtualized data center is

Borderless security products include the following:

- Secure-X and context-aware security
- Threat control and containment
- Cloud security and data loss prevention
- Secure connectivity through VPNs
- Security management

- Cisco SecureX: SecureX is an access control strategy that enables effective, high-level po
  mobile users. The components of SecureX include the following:
  - Context awareness
  - Cisco AnyConnect Client
  - TrustSec: End-to-end security using security group tags on traffic
  - Cisco Security Intelligence Operations: Cloud-based security service
- Threats in cloud services
  - Abuse of cloud computing
  - Insecure interfaces and APIs
  - Malicious insiders
  - Shared technology issues
  - Data loss or leakage
  - Account or service hijacking
  - Unknown risk profile

Network Foundation Protection

Understanding the device planes:

- Control plane, such as routing protocols
- Data plane, forwarding of data packets
- Management plane, used by management sessions

Cisco NFP Toolkit

- **Control Plane:** Control Plane Policing (CoPP), Control Plane Protection (CPPr), Routing AutoSecure
- **Management Plane:** Authentication, Authorization, and Accounting (AAA), Network Ti Network Management Protocol (SNMP), Secure Shell (SSH), Transport Layer Security (T (CLI) views
- **Data Plane:** Access control lists (ACLs), Layer 2 controls, Zone-Based Firewall, and IOS

Developing a Network Security Policy

This section details the creation of a network security policy—an important document that details procedures for the organization.

Why Do You Need One?

Aside from protecting organization assets, a security policy serves other purposes, such as the foll

- Making employees aware of their security-practice obligations
- Identifying specific security solutions required to meet the goals of the security policy
- Acting as a baseline for ongoing security monitoring

Components of the Security Policy

What are the components found in the network security policy? This section covers these details.

Governing Policy

At a high level, a governing policy addresses security concepts deemed important to an organizati
of this section:

- Identification of the issue addressed by the policy
- Discussion of the organization's view of the issue
- Examination of the relevance of the policy to the work environment
- Explanation of how employees must comply with the policy
- Enumeration of appropriate activities, actions, and processes
- Explanation of the consequences of noncompliance

Technical Policies

Technical policies provide a more detailed treatment of an organization's security policy, rather th
of this section include the following:

- E-mail
- Wireless networks
- Remote access

End-User Policies

End-user policies address security issues and procedures relevant to end users.

More Detailed Documents

More detailed documents are often contained in a security policy:

- **Standards:** Support consistency within a network
- **Guidelines:** Tend to be suggestions
- **Procedures:** Detailed documents providing step-by-step instructions for completing speci

Roles and Responsibilities

The ultimate responsibility for an organization's security policy rests on the shoulders of senior m
typically oversees the development of a security policy. Senior security or IT personnel are usuall
of the security policy. Examples of senior security or IT personnel include the following:

- Chief security officer (CSO)
- Chief information officer (CIO)
- Chief information security officer (CISO)

Risk Analysis, Management, and Avoidance

Network designers identify threats to the network using threat identification practices. Also, analy
probability that a threat will occur and the severity of that threat. This is *risk analysis*. When perfo
of two approaches:

- **Quantitative analysis:** Mathematically models the probability and severity of a risk. A sa
is ALE = AV * EF * ARO; this formula calculates the annualized loss expectancy (ALE).
that you can use to help justify the expense of security solutions. AV is an asset value, EF
the annualized rate of occurrence.
- **Qualitative analysis:** Uses a scenario model, where scenarios of risk occurrence are iden

Creating the Cisco Self-Defending Network

This type of network is built in three phases:

- **Integrated:** Every element is a point of defense.
- **Collaborative:** Collaboration occurs among the service and devices throughout the netwo
- **Adaptive:** The network can intelligently evolve and adapt the threats.

Benefits

- Reduced integration costs
- Proactive, planned upgrades
- Improves efficiency of security management

Key Tools

Note
MARS is currently End of Sale/End of Life.

- **Cisco Security Manager:** Powerful but easy-to-use solution that enables you to centrally configurations and security policies for the Cisco family of security products
- **MARS (Cisco Security Monitoring, Analysis, and Response System):** Provides securit devices and host applications made by Cisco and other providers

Chapter 2
Perimeter Security

Securing Administrative Access to Routers

It is critical to secure administrative access to the routers that help power your network infrastruct
you must do this.

Router Security Principles

Following are three areas of router security:

- Physical security
- Operating system
- Router hardening

Cisco Integrated Services Router Family

Cisco Integrated Services Routers feature comprehensive security services, embedding data, secur
platform portfolio for fast, scalable delivery of mission-critical business applications. Models incl
2800 Series, and 3800 Series.