Security+

Essentials

Security+ Essentials

Security+ Essentials – First Edition

The content of this book is provided for informational purposes only. Neither the publisher nor the author offers any warranties or representation, express or implied, with regard to the accuracy of information contained in this book, nor do they accept any liability for any loss or damage arising from any errors or omissions.

Find more eBooks online at http://www.eBookFrenzy.com.

Table of Contents

Chapter 1. About Security+ Essentials 10

Chapter 2. Mandatory, Discretionary, Role and Rule Based Access Control 11

2.1 An Overview of Access Control 11

2.2 Mandatory Access Control 11

2.3 Discretionary Access Control 12

2.4 Role Based Access Control 13

2.5 Rule Based Access Control 13

Chapter 3. Authentication and Identity Verification 14

3.1 What is Authentication? 14

3.2 Username and Password 14

3.3 Challenge Handshake Authentication Protocol (CHAP) 15

3.4 Kerberos Authentication 15

3.4.1 Logon at Client 16

3.4.2 Client Authentication 16

3.4.3 Client Service Authorization 16

3.4.4 Client Service Request 17

3.5 Mutual Authentication 17

3.6 Certificates 18

3.7 Authentication using Tokens 18

3.8 Biometrics 18

Chapter 4. An Overview of IT Security Threats and Attacks 20

4.1 TCP and UDP Based Denial of Service (DoS) Attacks 20

4.2 Distributed Denial of Service (DDoS) Attacks 21

4.3 Back Door Attacks 22

4.4 IP and DNS Spoofing Attacks 22

4.5 Man in the Middle Attacks 23

4.6 Replay Attacks 23

4.7 TCP/IP Hijacking 24
4.8 Mathematical Attacks 24
4.9 Password Guessing 24
4.10 Brute Force Password Attacks 24
4.11 Dictionary Password Attacks 25
4.12 Password Cracking 25
Chapter 5. Software Exploitation, Malicious Code and Social Engineering 26
5.1 Software Exploitation 26
5.2 Malicious Code 26
5.3 Viruses 26
5.4 Trojan Horses 27
5.5 Logic Bombs 27
5.6 Worms 28
5.7 Social Engineering 28
Chapter 6. Identifying Common and Nonessential Services 29
6.1 Understanding Ports and Services 29
6.2 Securing Ports and Services 30
6.3 Port Scanning 30
6.4 Primary TCP/IP Ports and Assignments 30
Chapter 7. An Overview of Communications Security 35
7.1 Remote Access 35
7.2 Virtual Private Network (VPN) Communications 35
7.3 Point-to-Point-Tunneling Protocol (PPTP) 35
7.4 Layer 2 Tunneling Protocol (L2TP) 35
7.5 Internet Protocol Security (IPSec) 36
7.6 802.11x Wireless Connections 36
7.7 Dial-Up Access 37
7.8 Terminal Access Controller Access Control System (TACACS) 37

7.9 Remote Authentication Dial-In User Service (RADIUS) 38
7.10 Terminal Access Controller Access Control System Plus (TACACS+) 38
7.11 Secure Shell (SSH) 38
Chapter 8. The Basics of Email and Web Security 39
8.1 Email Security 39
8.1.1 Pretty Good Privacy (PGP) 39
8.1.2 Secure Multipurpose Internet Mail Extension (S/MIME) 39
8.2 Dealing with Spam Email 40
8.3 Web Based Security (SSL and TLS) 40
8.4 IT Infrastructure Security 42
8.5 Understanding Firewalls 42
8.5.1 Packet-Filtering Firewalls 42
8.5.2 Proxy Service Firewalls 43
8.5.3 Stateful Inspection Firewalls 43
8.6 Routers 43
8.7 Switches 44
8.8 Wireless 44
8.9 DSL and Cable Modems 45
8.10 Remote Access Service (RAS) 46
8.11 Telecom/PBX 46
8.12 Virtual Private Networks (VPN) 46
8.13 Intrusion Detection Systems (IDSs) 47
8.14 Network Monitoring and Diagnostics 47
8.15 Simple Network Management Protocol (SNMP) 47
Chapter 9. IT Media Security Basics 49
9.1 Cable Media 49
9.1.1 Coax Cable 49
9.1.2 Shielded and Unshielded Twisted Pair Cable (UTP/STP) 49

9.2 Fiber Optic Cable 50
9.3 Removable Storage Media 50
9.3.1 Hard Drives 50
9.4 Diskettes 50
9.5 Tape Storage 51
9.6 CD-R/DVD 51
9.7 Electronic Media 51
Chapter 10. Network Security Topologies 52
10.1 DMZ 52
10.2 Internet 52
10.3 Intranet 53
10.4 Extranet 53
10.5 Virtual Local Area Network (VLAN) 53
10.6 Network Address Translation (NAT) 53
10.7 Tunneling 54
Chapter 11. Intrusion Detection Systems 55
11.1 An Overview of Intrusion Detection Systems 55
11.2 IDS Architecture 55
11.3 Host-based Intrusion Detections Systems (HIDS) 56
11.3.1 Strengths of Host-based Intrusion Detection Systems 56
11.3.2 Weaknesses of Host-based Intrusion Detection Systems 57
11.4 Network-based Intrusion Detection Systems (NIDS) 57
11.4.1 Strengths of Network-based Intrusion Detection Systems 58
11.4.2 Weaknesses of Network-based Intrusion Detection Systems 58
11.5 Responding to Incidents 59
Chapter 12. Security Baselines and Operating System, Network and Application Hardening .. 60
12.1 Security Baselines 60
12.2 Operating System Hardening 60

12.3 Network Hardening 61
12.4 Application Hardening 62
12.4.1 Web Servers 62
12.5 Email Servers 62
12.6 FTP Servers 62
12.7 DNS Servers 63
Chapter 13. Cryptography Basics 64
13.1 What is Cryptography? 64
13.2 Algorithms 64
13.3 Hashing Algorithms 64
13.4 Symmetric Encryption Algorithms 65
13.4.1 Data Encryption Standard (DES) 65
13.4.2 Triple DES (3DES) 65
13.4.3 Advanced Encryption Standard (AES) 65
13.4.4 Blowfish 66
13.4.5 International Data Encryption Algorithm (IDEA) 66
13.4.6 CAST 66
13.4.7 Rivest Cipher (RC2, RC3, RC4, RC5, RC6) 66
13.5 Asymmetric Algorithms 66
13.5.1 RSA 67
13.5.2 Diffie-Hellman 67
13.5.3 ElGamal 67
13.5.4 Elliptic Curve Cryptography (ECC) 67
13.6 Cryptography Usage 67
13.6.1 Confidentiality 68
13.6.2 Integrity 68
13.6.3 Nonrepudiation 68
13.6.4 Authentication 68

13.7 Digital Signatures........ 68

Chapter 14. An Overview of Public Key Infrastructures (PKI)........ 70

14.1 What is a Public Key Infrastructure?........ 70

14.2 Certificate Authorities (CA)........ 71

14.3 Registration Authorities (RA)........ 71

14.4 Certificate Repositories........ 71

14.5 Digital Certificate Structure........ 72

14.6 Certificate Lifecycles and Key Management........ 72

14.7 Centralized and Decentralized Infrastructures........ 73

Chapter 1. About Security+ Essentials

Ever since people started to connect computer systems together (be it via local area networks, wide area networks or the internet) the issue of IT Security has become a matter of concern for everyone, including the home user all the way up to the global enterprise. Without a comprehensive information security strategy individuals and organization are at risk of compromised confidential data and loss of business as a result of malicious damage to operating systems and data.

Security+ Essentials is designed to provide the knowledge needed by IT professionals to pass the CompTIA Security+ exam. That said, the book is also of considerable use to anyone with a need to understand the concepts involved in creating and maintaining a secure IT environment.

Security+ Essentials is largely a platform agnostic book and as such many of the concepts described apply equally to a range of popular operating systems including Windows, Linux, Mac OS X and UNIX.

On completion of this book it is intended that the reader will have a clear understanding of both the threats faced by IT infrastructures together with a basic understanding of the steps involved in planning and implementing a comprehensive multi-layered IT security strategy.

Chapter 2. Mandatory, Discretionary, Role and Rule Based Access Control

One of the key foundations of a comprehensive IT security strategy involves implementing an appropriate level of access control to all computer systems in an organization or enterprise. This chapter of *Security+ Essentials* will provide an overview of four types of access control for which an understanding is required to achieve CompTIA Security+ certification:

- Mandatory Access Control
- Discretionary Access Control
- Rule-Based Access Control
- Role-Based Access Control

2.1 An Overview of Access Control

The term *Access Control* is something of an ambiguous term. To some it could be interpreted as controlling the access to a system from an external source (for example controlling the login process via which users gain access to a server or desktop system). In fact, such access control is actually referred to as *Authentication* or *Identity Verification* and is not what is meant by *Access Control* in this context (authentication is covered in detail in *Chapter 3 - Authentication and Identity Verification*).

The term *Access Control* actually refers to the control over access to system resources *after* a user's account credentials and identity have been authenticated and access to the system granted. For example, a particular user, or group of users, might only be permitted access to certain files after logging into a system, while simultaneously being denied access to all other resources.

2.2 Mandatory Access Control

Mandatory Access Control (MAC) is the strictest of all levels of control. The design of MAC was defined, and is primarily used by the government.

MAC takes a hierarchical approach to controlling access to resources. Under a MAC enforced environment access to all resource objects (such as data files) is controlled by settings defined by the system administrator. As such, all access to resource objects is strictly controlled by the operating system based on system administrator configured settings. It is not possible under MAC enforcement for users to change the access control of a resource.

Mandatory Access Control begins with *security labels* assigned to all resource objects on the system. These security labels contain two pieces of information - a classification (top secret, confidential etc) and a category (which is essentially an indication of the management level, department or project to which the object is available).

Similarly, each user account on the system also has classification and category properties from the same set of properties applied to the resource objects. When a user attempts to access a resource under Mandatory Access Control the operating system checks the user's classification and categories and compares them to the properties of the object's security label. If the user's credentials match the MAC security label properties of the object access is allowed. It is important to note that *both* the classification and categories must match. A user with top secret classification, for example, cannot access a resource if they are not also a member of one of the required categories for that object.

Mandatory Access Control is by far the most secure access control environment but does not come without a price. Firstly, MAC requires a considerable amount of planning before it can be effectively implemented. Once implemented it also imposes a high system management overhead due to the need to constantly update object and account labels to accommodate new data, new users and changes in the categorization and classification of existing users.

2.3 Discretionary Access Control

Unlike Mandatory Access Control (MAC) where access to system resources is controlled by the operating system (under the control of a system administrator), Discretionary Access Control (DAC) allows each user to control access to their own data. DAC is typically the default access control mechanism for most desktop operating systems.

Instead of a *security label* in the case of MAC, each resource object on a DAC based system has an *Access Control List* (ACL) associated with it. An ACL contains a list of users and groups to which the user has permitted access together with the level of access for each user or group. For example, *User A* may provide read-only access on one of her files to *User B*, read and write access on the same file to *User C* and full control to any user belonging to *Group 1*.

It is important to note that under DAC a user can only set access permissions for resources which they already own. A hypothetical *User A* cannot, therefore, change the access control for a file that is owned by *User B*. *User A* can, however, set access permissions on a file that she owns. Under some operating systems it is also possible for the system or network administrator to dictate which permissions users are allowed to set in the ACLs of their resources.

Discretionary Access Control provides a much more flexible environment than Mandatory Access Control but also increases the risk that data will be made accessible to users that should not necessarily be given access.

2.4 Role Based Access Control

Role Based Access Control (RBAC), also known as *Non discretionary Access Control*, takes more of a real world approach to structuring access control. Access under RBAC is based on a user's job function within the organization to which the computer system belongs.

Essentially, RBAC assigns permissions to particular roles in an organization. Users are then assigned to that particular role. For example, an accountant in a company will be assigned to the *Accountant* role, gaining access to all the resources permitted for all accountants on the system. Similarly, a software engineer might be assigned to the *developer* role.

Roles differ from *groups* in that while users may belong to multiple groups, a user under RBAC may only be assigned a single role in an organization. Additionally, there is no way to provide individual users additional permissions over and above those available for their role. The accountant described above gets the same permissions as all other accountants, nothing more and nothing less.

2.5 Rule Based Access Control

Rule Based Access Control (RBAC) introduces acronym ambiguity by using the same four letter abbreviation (RBAC) as Role Based Access Control.

Under Rules Based Access Control, access is allowed or denied to resource objects based on a set of rules defined by a system administrator. As with *Discretionary Access Control*, access properties are stored in Access Control Lists (ACL) associated with each resource object. When a particular account or group attempts to access a resource, the operating system checks the rules contained in the ACL for that object.

Examples of Rules Based Access Control include situations such as permitting access for an account or group to a network connection at certain hours of the day or days of the week.

As with MAC, access control cannot be changed by users. All access permissions are controlled solely by the system administrator.