Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Ethical Hacking and Countermeasures Ethical Hacking Essential Concepts - II	Exam 312-50 Certified Ethical Hacker
Information Security Controls	CEH
Administrative Security Controls Physical Secontrols	
Technical Security Controls	Capyright © by 85-GREEGE. All Rights Reserved. Reproduction is Strictly Prohibited.
A set of security measures taken to protect data and syst Examples of Technical Access Controls Authorization	
1 2 3	4 5 6 uditing Network Security Devices
Notes:	Capyright © by ED-Countil, All Rights Reserved. Reproduction is Strictly Prohibited.
Appendix B Page 3699	Ethical Hacking and Countermeasures Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Access Control Access control is the selective restriction of access to a place or other system or network resource Protects information assets by determining who can and cannot access them Involves user identification, authentication, authorization, and accountability **Access Control Principles** Access Control Terminology Refers to a particular user or process which wants to access the resource Refers to a specific resource that the Object user wants to access such as a file or any hardware device Checks the access control rule for Reference specific restrictions Monitor Represents the action taken by the Operation subject on the object

Types of Access Control



Discretionary Access Control (DAC)

- Permits the user who is granted access to information to decide how to protect the information and determine the desired level of sharing
- Access to files is restricted to users and groups based upon their identity and the groups to which the users belong



Mandatory Access Control (MAC)

- Does not permit the end user to decide who can access the information
- Does not permit the user to pass privileges on to other users, as system access could then be circumvented

Role-based Access

- Users can be assigned access to systems, files, and fields on a one-by-one basis, whereby access is granted to the user for a particular file or system
- Can simplify the assignment of privileges and ensure that individuals have all the privileges necessary to perform their duties



Copyright © by ES-Coppell, All Rights Reserved, Reproduction is Strictly Prohibited

Notes:				