1.	Record Nr.	UNINA9910781479003321
	Autore	Gibson Darril
	Titolo	Microsoft Windows Security [[electronic resource]] : Essentials / / Darril Gibson
	Pubbl/distr/stampa	Hoboken, : Wiley, 2011 Indiana, : Wiley, 2011
	ISBN	1-283-17725-0 9786613177254 1-118-11454-X
	Descrizione fisica	1 online resource (374 p.)
	Collana	Sybex serious skills Essentials (Indianapolis, Ind.)
	Disciplina	005.8 621.3916076
	Soggetti	Electronic data processing personnel - Certification Computer networks - Examinations Computer networks -- Examinations -- Study guides Computer security - Examinations
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Description based upon print version of record.
	Nota di contenuto	Microsoft Windows Security Essentials; Introduction; Who Should Read This Book; What You Will Learn; Prerequisites; What You Need; What Is Covered in This Book; Chapter 1: Understanding Core Security Principles; Understanding Risk; Exploring the Security Triad; Protecting Against Loss of Confidentiality; Protecting Against Loss of Availability; Protecting Against Loss of Integrity; Implementing a Defense-in-Depth Security Strategy; Enforcing the Principle of Least Privilege; Hardening a Server; Reducing the Attack Surface; Keeping a System Updated; Enabling the Firewall Installing Antivirus Software Chapter 2: Understanding Malware and Social Engineering; Comparing Malware; Viruses; Worms; Trojan Horses; Buffer-Overflow Attacks; Spyware; Understanding the Threat; Protecting Against Malware; Using Antivirus Software; Using Microsoft Security Essentials on Desktops; Thwarting Social-Engineering Attacks; Social Engineering in Person; Social Engineering with a Phone Call;

Recognizing Phishing Attempts; Recognizing Pharming; Protecting Email; Chapter 3: Understanding User Authentication; Comparing the Three Factors of Authentication
Using Passwords for Authentication Comparing Password Attack Methods; Creating Strong Passwords; Enforcing Strong Passwords; Exploring Account Lockout Policies; Unlocking an Account; Resetting a Password; Changing a Password; Creating a Password-Reset Disk; Using Smart Cards and Token Devices for Authentication; Using Biometrics for Authentication; Starting Applications with Run As Administrator; Preventing Time Skew with Kerberos; Identifying RADIUS Capabilities; Identifying Unsecure Authentication Protocols; LM; NTLM (NTLMv1); Chapter 4: Securing Access with Permissions
Comparing NTFS Permissions Identifying Basic NTFS Permissions; Identifying Advanced NTFS Permissions; Combining Permissions; Enabling and Disabling Permission Inheritance; Moving and Copying Files; Comparing NTFS and FAT; Exploring Share Permissions; Identifying Share Permissions; Combining NTFS and Share Permissions; Identifying Active Directory Permissions; Viewing Active Directory Users and Computers; Comparing NTFS and Active Directory Permissions; Viewing Active Directory Permissions; Assigning Registry Permissions; Chapter 5: Using Audit Policies and Network Auditing
Exploring Audit Policies Exploring Object Access Auditing; Comparing Account Logon and Logon Events; Exploring Directory Service Access Auditing; Understanding Account Management Auditing; Understanding System Events Auditing; Understanding Privilege Use Auditing; Understanding Policy Change Auditing; Understanding Process Tracking; Enabling Auditing; Enabling Object Access Auditing; Enabling Directory Service Access Auditing; Viewing Audit Information; Managing Security Logs; Saving Audit Information; Securing Audit Information; Auditing a Network with MBSA; Installing MBSA; Running MBSA
Chapter 6: Protecting Clients and Servers

Sommario/riassunto	Windows security concepts and technologies for IT beginners IT security can be a complex topic, especially for those new to the field of IT. This full-color book, with a focus on the Microsoft Technology Associate (MTA) program, offers a clear and easy-to-understand approach to Windows security risks and attacks for newcomers to the world of IT. By paring down to just the essentials, beginners gain a solid foundation of security concepts upon which more advanced topics and technologies can be built. This straightforward guide begins each chapter by laying out a list of topics to be