



به نام خدا



مبانی امنیت اطلاعات و شبکه

SECURITY +

مؤلف

احسان امجدی بیگوند

فهرست مطالب

۱۶.....	فصل اول: INTRODUCTION TO SECURITY
۱۸.....	FOUNDATION TOPICS
۱۸.....	THE CIA OF COMPUTER SECURITY
۲۱.....	THE BASICS OF INFORMATION SECURITY
۲۴.....	THINK LIKE A HACKER!
۲۶.....	THREAT ACTOR TYPES AND ATTRIBUTES
۲۸.....	فصل دوم: COMPUTER SYSTEMS SECURITY PART I
۳۰.....	MALICIOUS SOFTWARE TYPES
۳۰.....	VIRUSES
۳۲.....	WORMS
۳۲.....	TROJAN HORSES
۳۳.....	RANSOMWARE
۳۴.....	SPYWARE
۳۴.....	ROOTKITS
۳۵.....	FILELESS MALWARE
۳۵.....	SPAM
۳۷.....	DELIVERY OF MALWARE
۳۷.....	VIA SOFTWARE, MESSAGING, AND MEDIA
۳۹.....	BOTNETS AND ZOMBIES
۴۰.....	ACTIVE INTERCEPTION
۴۰.....	PRIVILEGE ESCALATION

٤١	BACKDOORS
٤١	LOGIC BOMBS
٤٢	PREVENTING AND TROUBLESHOOTING MALWARE
٤٣	PREVENTING AND TROUBLESHOOTING VIRUSES
٤٧	PREVENTING AND TROUBLESHOOTING WORMS AND TROJANS
٤٨	PREVENTING AND TROUBLESHOOTING SPYWARE
٥٠	BADWARE
٥٠	PREVENTING AND TROUBLESHOOTING ROOTKITS
٥١	PREVENTING AND TROUBLESHOOTING SPAM
٥٣	YOU CANT'T SAVE EVERY COMPUTER FROM MALWARE!
٥٤	SUMMARY OF MALWARE PREVENTION TECHNIQUES
٥٥	فصل سوم: COMPUTER SYSTEMS SECURITY PART II
٥٦	IMPLEMENTING SECURITY APPLICATIONS
٥٧	PERSONAL SOFTWARE FIREWALLS
٥٩	HOST-BASED INTRUSION DETECTION SYSTEMS
٦١	POP-UP BLOCKERS
٦٢	DATA LOSS PREVENTION SYSTEMS
٦٣	SECURING COMPUTER HARDWARE AND PERIPHERALS
٦٤	SECURING THE BIOS
٦٦	SECURING STORAGE DEVICES
٦٧	NETWORK ATTACHED STORAGE
٦٧	WHOLE DISK ENCRYPTION
٦٩	HARDWARE SECURITY MODULES
٦٩	SECURING WIRELESS PERIPHERALS
٧٠	SECURING MOBILE DEVICE
٧١	MALWARE
٧١	BOTNET ACTIVITY
٧٢	SIM CLONING AND CARRIER UNLOCKING
٧٣	WIRELESS ATTACKS
٧٤	THEFT

۷۴	APPLICATION SECURITY
۷۷	BYOD CONCERNS
۸۱	فصل چهارم: OS HARDENING AND VIRTUALIZATION
۸۳	HARDENING OPERATIONG SYSTEMS
۸۳	REMOVING UNNECESSARY APPLICATIONS AND SERVICES
۹۲	WINDOWS UPDATE, PATCHES, AND HOTFIXES
۹۴	PATCHES AND HOTFIXES
۹۸	GROUP POLICIES, SECURITY TEMPLATES, AND CONFIGURATION BASELINES
۱۰۰	HARDENING FILE SYTEMS AND HARD DRIVES
۱۰۳	KEEPING A WELL-MAINTAINED COMPUTER
۱۰۴	VIRTUALIZATION TECHNOLOGY
۱۰۴	TYPE OF VIRTUALIZATION AND THEIR PURPOSES
۱۰۵	HYPERVERSOR
۱۰۵	SECURING VIRTUAL MACHINES
۱۰۸	فصل پنجم: APPLICATION SECURITY
۱۰۹	SECURING THE BROWSER
۱۱۱	GENERAL BROWSER SECURITY PROCEDURES
۱۱۱	IMPLEMENT POLICIES
۱۱۳	TRAIN YOUR USERS
۱۱۳	USE A PROXY AND CONTENT FILTER
۱۱۵	WEB BROWSER CONCERNS AND SECURITY METHODS
۱۱۵	BASIC BROWSER SECURITY
۱۱۵	COOCKIES
۱۱۷	LSOS
۱۱۷	ADD-ONS
۱۱۸	ADVANCED BROWSER SECURITY
۱۱۹	SECURING OTHER APPLICATIONS
۱۲۲	SECURE PROGRAMMING
۱۲۳	SOFTWARE DEVELOPMENT LIFE CYCLE
۱۲۴	CORE SDLC PRINCIPLES

١٢٦	PROGRAMMING TESTING METHODS
١٢٧	INPUT VALIDATION
١٢٨	STATIC AND DYNAMIC CODE ANALYSIS
١٢٨	FUZZ TESTING
١٢٩	PROGRAMMING VULNERABILITIES AND ATTACKS
١٢٩	BACKDOORS
١٢٩	MEMORY/BUFFER VULNERABILITIES
١٣١	ARBITRARY CODE EXECUTION/ REMOVE CODE EXECUTION
١٣١	XSS AND XSRF
١٣٢	MORE CODE INJECTION EXAMPLES
١٣٤	DIRECTORY TRAVERSAL
١٣٥	ZERO DAY ATTACK

١٣٦NETWORK DESIGN ELEMENTS: فصل ششم:

١٣٧	OSI MODEL
١٣٩	NETWORK DEVICES
١٣٩	SWITCH
١٤١	BRIDGE
١٤١	ROUTER
١٤٢	NETWORK ADDRESS TRASLATION, AND PRIVATE VERSUS PUBLIC IP
١٤٣	NETWORK ZONES AND INTERCONNECTIONS
١٤٤	LAN VERSUS WAN
١٤٤	INTERNET
١٤٤	DEMILITARIZED ZONE (DMZ)
١٤٦	INTRANET AND EXTRANET
١٤٧	NETWORK ACCESS CONTROL (NAC)
١٤٧	SUBNETTING
١٤٨	VIRTUAL LOCAL AREA NETWORK (VLAN)
١٥١	CLOUD COMPUTING
١٥٢	CLOUD SECURITY
١٥٤	OTHER "CLOUD"-BASED CONCERNS

١٥٤	SERVER DEFENCE
١٥٤	FILE SERVERS
١٥٤	NETWORK CONTROLLERS
١٥٥	EMAIL SERVERS
١٥٥	WEB SERVERS
١٥٦	FTP SERVER

١٥٨ NETWORKING PROTOCOLS AND THREATS: فصل هفتم:

١٥٩	PORT RANGES, INBOUND VERSUS OUTBOUND, AND COMMON PORTS
١٦٧	PORT ZERO SECURITY
١٦٨	MALICIOUS ATTACKS
١٧٠	DDoS
١٧١	SINKHOLES AND BLACKHOLES
١٧٢	SPOOFING
١٧٣	SESSION HIJACKING
١٧٥	REPLAY
١٧٥	NULL SESSIONS
١٧٦	TRANSITIVE ACCESS AND CLIENT-SIDE ATTACKS
١٧٦	DNS POISONING AND OTHER DNS ATTACKS
١٧٨	ARP POISONING

١٧٩ NETWORK PERIMETER SECURITY: فصل هشتم:

١٨٠	FIREWALLS AND NETWORK SECURITY
١٨١	FIREWALLS
١٨٥	PROXY SERVERS
١٨٨	HONEYPOTS AND HONEYNETS
١٨٩	DATA LOSS PREVENTION (DLP)
١٩٠	NIDS VERSUS NIPS
١٩٠	NIDS
١٩١	NIPS
١٩٣	UNIFIED THREAT MANAGEMENT

١٩٤SECURING NETWORK DEVICES: فصل نهم:

١٩٥	NETWORK DEVICE VULNERABILITIES
١٩٥	DEFAULT ACCOUNTS
١٩٦	WEAK PASSWORDS
١٩٧	PRIVILEGE ESCALATION
١٩٨	BACK DOORS
١٩٨	NETWORK ATTACKS
١٩٨	OTHER NETWORK DEVICE CONSIDERATIONS
١٩٩	CABLE MEDIA VULNERABILITIES
١٩٩	INTERFERENCE
٢٠٠	CROSSTALK
٢٠٠	TAPPING INTO DATA AND CONVERSATION
٢٠١	SECURING WIRELESS NETWORKS
٢٠١	WIRELESS ACCESS POINT VULNERABILITIES
٢٠٢	THE ADMINISTRATION INTERFACE
٢٠٢	SSID BROADCAST
٢٠٢	ROGUE ACCESS POINTS
٢٠٢	EVIL TWIN
٢٠٣	WEAK ENCRYPTION
٢٠٥	WI-FI PROTECTED SETUP
٢٠٥	AD HOC NETWORKS
٢٠٥	VPN OVER OPEN WIRELESS
٢٠٦	WIRELESS ACCESS POINT SECURITY STRATEGIES
٢٠٧	WIRELESS TRANSMISSION VULNERABILITIES
٢٠٩	FINAL NETWORK DOCUMENTATION

٢١٠AUTHENTICATION MODELS: فصل دهم:

٢١٢	AUTHENTICATION MODELS AND COMPONENTS
٢١٢	AUTHENTICATION MODELS
٢١٤	LOCALIZED AUTHENTICATION TECHNOLOGIES
٢١٤	802.1X AND EAP

۲۱۷	LDAP
۲۱۷	KERBEROS AND MUTUAL AUTHENTICATION
۲۱۹	REMOTE DESKTOP SERVICES
۲۲۰	REMOTE AUTHENTICATION TECHNOLOGIES
۲۲۰	REMOTE ACCESS SERVICE
۲۲۱	VIRTUAL PRIVATE NETWORKS
۲۲۳	RADIUS VERSUS TACACS

۲۲۵.....ACCESS CONTROL METHODS AND MODELS: فصل یازدهم:

۲۲۶	ACCESS CONTROL MODELS DEFINED
۲۲۶	DISCRETIONARY ACCESS CONTROL
۲۲۸	MANDATORY ACCESS CONTROL
۲۲۸	ROLE-BASED ACCESS CONTROL (RBAC)
۲۲۹	ATTRIBUTE-BASED ACCESS CONTROL (ABAC)
۲۳۲	RIGHTS, PERMISSIONS AND POLICIES
۲۳۲	USERS, GROUPS, AND PERMISSIONS
۲۳۶	PERMISSION INHERITANCE AND PROPAGATION
۲۳۷	MOVING AND COPYING FOLDERS AND FILES
۲۳۸	USERNAMES AND PASSWORDS
۲۴۰	POLICIES
۲۴۱	COMPLEXITY AND LENGTH OF A PASSWORD
۲۴۳	USER ACCOUNT CONTROL (UAC)

۲۴۴.....VULNERABILITY AND RISK ASSESSMENT: فصل دوازدهم:

۲۴۵	CONDUCTING RISK ASSESSMENTS
۲۴۷	QUALITATIVE RISK ASSESSMENT
۲۴۸	QUANTITATIVE RISK ASSESSMENT
۲۵۰	SECURITY ANALYSIS METHODOLOGIES
۲۵۱	SECURITY CONTROLS
۲۵۲	VULNERABILITY MANAGEMENT
۲۵۳	PENETRATION TESTING
۲۵۵	OVAL

۲۵۶	ASSESSING VULNERABILITY WITH SECURITY TOOLS
۲۵۶	NETWORK MAPPING
۲۵۷	VULNERABILITY SCANNING
۲۵۹	NETWORK SNIFFING
۲۶۰	PASSWORD ANALYSIS

۲۶۳ فصل سیزدهم: MONITORING AND AUDITING

۲۶۴	MONITORING METHODOLOGIES
۲۶۴	SIGNATURE-BASED MONITORING
۲۶۵	ANOMALY-BASED MONITORING
۲۶۵	BEHAVIOR-BASED MONITORING
۲۶۵	USING TOOLS TO MONITOR SYSTEMS AND NETWORKS
۲۶۵	PERFORMANCE BASELINING
۲۶۷	PROTOCOL ANALYZER
۲۶۸	WIRESHARK
۲۶۹	SNMP
۲۷۰	ANALYTICAL TOOLS
۲۷۲	CONDUCTING AUDITS
۲۷۳	AUDITING FILES
۲۷۵	LOGGING
۲۷۸	LOG FILE MAINTENANCE AND SECURITY
۲۸۰	AUDITING SYSTEM SECURITY SETTINGS
۲۸۳	SIEM

۲۸۴ فصل چهاردهم: ENCRYPTION AND HASHING CONCEPTS

۲۸۵	CRYPTOGRAPHY CONCEPTS
۲۸۷	SYMMETRIC VERSUS ASYMMETRIC KEY ALGORITHMS
۲۸۷	SYMMETRIC KEY ALGORITHMS
۲۸۸	ASYMMETRIC KEY ALGORITHMS
۲۸۹	PUBLIC KEY CRYPTOGRAPHY
۲۹۰	KEY MANAGEMENT
۲۹۰	STEGANOGRAPHY

٢٩١		ENCRYPTION ALGORITHMS
٢٩٢		DES AND 3DES
٢٩٢		AES
٢٩٣		RC
٢٩٤		BLOWFISH AND TWOFISH
٢٩٤		RSA
٢٩٦		DIFFIE-HELLMAN
٢٩٦		ELLIPTIC CURVE
٢٩٧		HASHING BASICS
٢٩٨		CRYPTOGRAPHIC HASH FUNCTIONS
٢٩٨		MD5
٢٩٨		SHA
٢٩٩		LANMAN, NTLM, AND NTLMv2
٢٩٩		LANMAN
٣٠٠		NTLM AND NTLMv2
٣٠١		HASHING ATTACKS
٣٠١		PATH THE HASH
٣٠٢		HAPPY BIRTHDAY
٣٠٣		ADDITIONAL PASSWORD HASHING CONCEPTS
٣٠٥		PKI AND ENCRYPTION PROTOCOLS: فصل پانزدهم:
٣٠٦		PUBLIC KEY INFRASTRUCTURE
٣٠٦		CERTIFICATE
٣٠٧		SSL CERTIFICATE TYPES
٣٠٨		SINGLE-SIDED AND DUAL-SIDED CERTIFICATES
٣٠٨		CERTIFICATE CHAIN OF TRUST
٣٠٩		CERTIFICATE FORMATS
٣١٠		CERTIFICATE AUTHORITIES
٣١٤		WEB OF TRUST
٣١٤		SECURITY PROTOCOLS
٣١٥		S/MIME

٣١٦	SSL/TLS
٣١٨	SSH
٣١٩	PPTP, L2TP, AND IPSEC
٣١٩	PPTP
٣١٩	L2TP
٣٢٠	IPSEC

فصل شانزدهم: SOCIAL ENGINEERING, USER EDUCATION, AND

٣٢٢	FACILITIES SECURITY
-----	--------------------------

٣٢٣	SOCIAL ENGINEERING
٣٢٤	PRETEXTING
٣٢٤	MALICIOUS INSIDER
٣٢٥	DIVERSION THEFT
٣٢٥	PHISHING
٣٢٧	HOAXES
٣٢٧	SHOULDER SURFING
٣٢٨	EAVESDROPPING
٣٢٨	DUMPSTER DIVING
٣٢٨	BAITING
٣٢٨	PIGGYBACKING/ TAILGATING
٣٢٩	WATERING HOLE ATTACK
٣٢٩	USER EDUCATION

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی است که بتواند
خواسته‌های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.
هر کتاب دیباگران تهران، یک فرصت جدید شغلی

حمد و سپاس ایزد منان را که با الطاف بی‌کران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "جناب آقای احسان امجدی بیگونند" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
bookmarket@mft.info

با سپاس از پدر و مادر عزیزم بخاطر زحمات و مهر بی دریغشان...
این کتاب را به همسر عزیزم و دخترم، نیکی، که در زمان نگارش این
متن، بی صبرانه برای ورودش به کانون گرم خانواده لحظه شماری
میکنیم، تقدیم می کنم.

❖ مقدمه مولف

از سال ۱۹۷۰ به بعد که به تدریج هکرها در معنای امروزی، متولد شدند، تا به الان، دنیای دیجیتال، فناوری‌های مختلفی را به خود تجربه کرده است که هرکدام از آن‌ها در طول این دوران یا جایگزین تکنولوژی‌های بهینه‌تر شدند و یا در مسیر تکامل خود گام برداشته‌اند. اما در این مسیر همواره رشد و خدمت به بشر مد نظر نبوده است و به موازات آن اهداف و اقداماتی در جهت سوءاستفاده از این تکنولوژی‌ها برای مقاصد شخصی، سیاسی، اقتصادی، فرهنگی و... نیز متولد شده و رشد کرده‌اند. در چنین شرایطی باید نه فقط صرفاً به فکر توسعه تکنولوژی‌ها و محصولات جدیدتر بود بلکه محافظت از آن‌ها نیز به مراتب در جایگاهی بالاتر از آن‌ها می‌تواند قرار داشته باشد؛ چراکه در صورت دسترسی‌ها غیرمجاز و سوءاستفاده‌های احتمالی از پیشرفت‌های حاصله در دنیای شبکه و تکنولوژی نه تنها زندگی بهتر را رقم نخواهد زد بلکه تأثیرات ناشی از سوءاستفاده‌های انجام شده، شرایط فعلی را نیز در مخاطره قرار خواهد داد. مطالعه این کتاب برای علاقه‌مندان به امنیت اطلاعات و همچنین کارشناسانی که تصمیم به فعالیت در حوزه امنیت شبکه و اطلاعات را دارند، توصیه می‌شود.

در این کتاب سعی شده است تا به هر دو وجه شبکه و امنیت پرداخته شود؛ به این معنا که ضمن آشنایی با مولفه‌هایی که نقش اساسی در شبکه را دارند، به نحوه ایمن کردن آن‌ها نیز به عنوان اصل موضوع، اشاره شده است. این مولفه‌ها شامل بخش‌های مختلفی مانند فایروال‌ها، آنتی‌ویروس‌ها، فایل‌های حساس، منابع عملیاتی، تهدیدها، حملات، رمزنگاری، مهندسی اجتماعی و... که می‌توانند در یک شبکه سازمانی وجود داشته باشند و یا اثرات خود را نشان دهند، است. علاوه بر این بیان مفاهیم پایه‌ای و اصلی در دنیای امنیت اطلاعات و تبیین آن‌ها نیز یکی از اهداف این کتاب بوده است که در متن کتاب به خوبی به آن پرداخته شده است.

پایه اصلی مطالب این کتاب مفاهیم ارائه شده در نسخه اصلی کتاب security+ از موسسه EC-Council بوده که به زبان فارسی بیان شده است. هدف از ترجمه آن، انتقال مفاهیم موجود به زبان گویاتر برای فارسی‌زبانان بوده است. ضمن آن که هدف از ارائه این کتاب، ترجمه آن بوده است اما سعی شده است تا اثرات هر دو وجه زبانی تحت تأثیر یکدیگر قرار نگیرند.

با توجه به آن که بسیاری از مفاهیم و عبارت به صورت تخصصی و در فرمت اصلی‌شان در دنیای شبکه بیان می‌شوند، سعی شده در مواجهه با آن‌ها ترجمه لغوی و یا قرابتی تا حد امکان صورت نگیرد و یا در صورت ترجمه، معادل استاندارد آن‌ها در باورقی بیان شود. علاوه بر این، از آنجایی که ترجمه برخی تیتراها ممکن بود مفهوم اصلی را نرساند و یا از زیبایی بیان آن بکاهد، تصمیم بر آن شد تا عبارت تیتراها در این کتاب با همان فرمت زبان اصلی باشد و معنا و توضیح آن‌ها در ادامه متن بیاید.