

## فهرست مطالب

|         |            |
|---------|------------|
| ۱۱..... | مقدمه ناشر |
| ۱۲..... | پیشگفتار   |
| ۱۶..... | سخن مترجم  |

### فصل ۱

|         |                                 |
|---------|---------------------------------|
| ۱۷..... | مبانی ارتباطات داده و شبکه سازی |
|---------|---------------------------------|

|         |                                       |
|---------|---------------------------------------|
| ۱۷..... | مقدمه                                 |
| ۱۸..... | ساختار فصل                            |
| ۱۸..... | اهداف                                 |
| ۱۸..... | مدل های مرجع شبکه                     |
| ۱۹..... | مدل اتصال متقابل سامانه های باز (OSI) |
| ۲۶..... | مدل OSI و مدل TCP/IP                  |
| ۲۷..... | انواع فلگ های TCP                     |
| ۲۸..... | هندشیک سه مرحله ای                    |
| ۲۹..... | ترجمه آدرس شبکه (NAT)                 |
| ۳۰..... | رسانه انتقال شبکه                     |
| ۳۲..... | دستگاه های شبکه                       |
| ۳۴..... | پروتکل ها: HTTP، HTTPS و DNS          |
| ۳۴..... | پروتکل انتقال ابرمتن (HTTP)           |
| ۳۶..... | پروتکل امن انتقال ابرمتن (HTTPS)      |
| ۳۷..... | سامانه نام دامنه (DNS)                |
| ۳۹..... | مقدمه ای بر پراکسی و زنجیره پراکسی    |
| ۳۹..... | زنجیره پراکسی                         |
| ۴۰..... | اهداف امنیت اطلاعات                   |
| ۴۱..... | محرمانگی، یکپارچگی و دسترس پذیری      |
| ۴۲..... | اهداف کلیدی در تأمین امنیت شبکه       |
| ۴۳..... | مفاهیم پایه ای رمزنگاری و نهان نگاری  |
| ۴۴..... | نهان نگاری                            |
| ۴۵..... | نتیجه گیری                            |
| ۴۵..... | نکات مهم این فصل                      |

|         |                   |
|---------|-------------------|
| ۴۴..... | سؤالات چندگزینهای |
| ۴۸..... | پاسخها            |
| ۴۸..... | سؤالات            |

## فصل ۲

|         |                              |
|---------|------------------------------|
| ۴۹..... | رمز گشایی از هک              |
| ۴۹..... | مقدمه                        |
| ۴۹..... | ساختار فصل                   |
| ۵۰..... | اهداف                        |
| ۵۰..... | مقدمه‌ای بر هک               |
| ۵۱..... | مفهوم هک اخلاقی              |
| ۵۲..... | تفاوت بین هک و هک اخلاقی     |
| ۵۳..... | مراحل هک اخلاقی              |
| ۵۵..... | هکتویسم                      |
| ۵۶..... | اهداف هکتویسم                |
| ۵۷..... | شکل‌های مختلف حملات هکتویستی |
| ۵۸..... | تخریب وبسایت                 |
| ۵۸..... | نرم‌افزار RECAP              |
| ۵۹..... | تکنیر وبسایت                 |
| ۵۹..... | انواع هکینگ                  |
| ۵۹..... | انواع رایج هکینگ             |
| ۶۱..... | انواع هکرها                  |
| ۶۳..... | تعریف و انواع جرائم سایبری   |
| ۶۶..... | حملات و طبقه‌بندی آن‌ها      |
| ۶۶..... | حملات فعال                   |
| ۶۸..... | حملات غیرفعال                |
| ۶۹..... | اصطلاحات ضروری               |
| ۶۹..... | هدف ارزیابی                  |
| ۷۰..... | اکسپلویت                     |
| ۷۱..... | آسیب‌پذیری                   |
| ۷۳..... | تهدید سایبری                 |
| ۷۷..... | نتیجه‌گیری                   |
| ۷۷..... | نکات مهم این فصل             |
| ۷۷..... | سؤالات چندگزینهای            |
| ۸۱..... | پاسخها                       |

پرسش‌ها ..... ۸۱

### فصل ۳

حقوق سایبری ..... ۸۳

مقدمه ..... ۸۳

ساختار فصل ..... ۸۳

اهداف ..... ۸۴

تروریسم سایبری ..... ۸۴

اقدامات حفاظتی در برابر تروریسم سایبری ..... ۸۹

حقوق سایبری ..... ۸۹

جرایم مشمول قوانین سایبری ..... ۹۲

کلاهبرداری ..... ۹۲

کپی‌رایت ..... ۹۲

اسرار تجاری ..... ۹۲

قانون کار و قرارداد ..... ۹۳

افترا ..... ۹۳

آزادی بیان ..... ۹۳

آزار و تعقیب ..... ۹۳

جعل ایمیل ..... ۹۴

جرایم سایبری علیه زنان ..... ۹۸

تعقیب سایبری ..... ۹۹

تماشاگری جنسی ..... ۹۹

داکسینگ ..... ۱۰۰

اغفال سایبری ..... ۱۰۱

قوانین هند در زمینه جرایم سایبری علیه زنان ..... ۱۰۲

ادله در فضای سایبری، نظارت و پایش ..... ۱۰۳

نتیجه‌گیری ..... ۱۰۵

نکات مهم این فصل ..... ۱۰۶

سؤالات چندگزینه‌ای ..... ۱۰۶

پاسخ‌ها ..... ۱۰۹

سؤالات ..... ۱۱۰

### فصل ۴

بدافزارها ..... ۱۱۱

مقدمه ..... ۱۱۱

|     |                                                  |
|-----|--------------------------------------------------|
| ۱۱۲ | ..... ساختار فصل                                 |
| ۱۱۲ | ..... اهداف                                      |
| ۱۱۲ | ..... مقدمه‌ای بر بدافزار                        |
| ۱۱۳ | ..... نشانه‌های آلودگی سیستم به بدافزار          |
| ۱۱۴ | ..... کرم رایانه‌ای                              |
| ۱۱۵ | ..... اسب تروا                                   |
| ۱۱۷ | ..... جاسوس افزار                                |
| ۱۱۸ | ..... تبلیغ افزار                                |
| ۱۱۹ | ..... باج افزار                                  |
| ۱۲۲ | ..... ویروس رایانه‌ای                            |
| ۱۲۲ | ..... انواع ویروس‌های رایانه‌ای                  |
| ۱۲۴ | ..... نشانه‌های حملات بدافزار                    |
| ۱۲۶ | ..... آنتی‌ویروس‌های محبوب و روش‌های تشخیص آنها  |
| ۱۲۶ | ..... روش شناسایی مبتنی بر امضا                  |
| ۱۲۸ | ..... روش مبتنی بر اکتشاف                        |
| ۱۳۰ | ..... روش مبتنی بر فضای ابری                     |
| ۱۳۱ | ..... حملات انکار سرویس و انکار سرویس توزیع شده  |
| ۱۳۴ | ..... سیستم شناسایی نفوذ و سیستم جلوگیری از نفوذ |
| ۱۳۸ | ..... Eavesdropping و snooping مفاهیم            |
| ۱۴۲ | ..... بات‌ها / زامبی‌های بات‌نت‌ها               |
| ۱۴۳ | ..... بات‌ها                                     |
| ۱۴۳ | ..... بات‌نت‌ها                                  |
| ۱۴۵ | ..... تهدیدات مبتنی بر برنامه‌های وب             |
| ۱۴۵ | ..... اسکریپت‌نویسی میان‌سایتی                   |
| ۱۴۶ | ..... تزریق به پایگاه داده                       |
| ۱۴۸ | ..... تزریق فرمان                                |
| ۱۴۹ | ..... سرریز بافر                                 |
| ۱۵۱ | ..... حمله پیمایش دایرکتوری                      |
| ۱۵۲ | ..... دانلودهای خودکار                           |
| ۱۵۴ | ..... اقدامات پیشگیرانه                          |
| ۱۵۴ | ..... کی‌لاکرها                                  |
| ۱۵۵ | ..... فایروال‌ها                                 |
| ۱۵۷ | ..... نتیجه‌گیری                                 |
| ۱۵۷ | ..... نکات مهم این فصل                           |
| ۱۵۸ | ..... سؤالات چندگزینده‌ای                        |

|     |         |
|-----|---------|
| ۱۶۱ | پاسخ‌ها |
| ۱۶۲ | پرسش‌ها |

## فصل ۵

|     |                |
|-----|----------------|
| ۱۶۳ | دنیای رمزنگاری |
|-----|----------------|

|     |                                        |
|-----|----------------------------------------|
| ۱۶۳ | مقدمه                                  |
| ۱۶۳ | ساختار فصل                             |
| ۱۶۴ | اهداف                                  |
| ۱۶۴ | اصول بنیادی رمزنگاری                   |
| ۱۶۷ | رمزگذاری با کلید متقارن                |
| ۱۶۹ | استاندارد رمزنگاری پیشرفته (AES)       |
| ۱۷۰ | استاندارد رمزنگاری داده‌ها (DES)       |
| ۱۷۲ | الگوریتم بین‌المللی رمزنگاری داده‌ها   |
| ۱۷۲ | بلوفیش                                 |
| ۱۷۳ | رمز ری‌وست ۴                           |
| ۱۷۳ | رمز ری‌وست ۵                           |
| ۱۷۴ | رمز ری‌وست ۶                           |
| ۱۷۵ | رمزنگاری کلید نامتقارن                 |
| ۱۷۷ | الگوریتم ری‌ویست-شامیر-ادل‌مان         |
| ۱۷۷ | الگوریتم امضای دیجیتال                 |
| ۱۷۸ | تبادل کلید دیفی-هلمن                   |
| ۱۸۰ | نقش توابع درهم‌ساز                     |
| ۱۸۲ | پروتکل‌های رمزنگاری                    |
| ۱۸۵ | اهمیت امضاها و دیجیتال                 |
| ۱۸۶ | فرآیند ایجاد امضای دیجیتال در رمزنگاری |
| ۱۸۸ | تکنیک‌های تحلیل رمز                    |
| ۱۹۱ | نتیجه‌گیری                             |
| ۱۹۱ | نکات مهم این فصل                       |
| ۱۹۱ | سؤالات چندگزینه‌ای                     |
| ۱۹۴ | پاسخ‌ها                                |
| ۱۹۵ | پرسش‌های تشریحی                        |

## فصل ۶

|     |                                         |
|-----|-----------------------------------------|
| ۱۹۶ | شبکه‌های بی‌سیم و چالش‌های امنیتی آن‌ها |
|-----|-----------------------------------------|

|     |       |
|-----|-------|
| ۱۹۶ | مقدمه |
|-----|-------|

|     |                                                                |
|-----|----------------------------------------------------------------|
| ۱۹۶ | ..... ساختار فصل                                               |
| ۱۹۷ | ..... اهداف فصل                                                |
| ۱۹۷ | ..... مقدمه‌ای بر امنیت شبکه‌های بی‌سیم                        |
| ۲۰۰ | ..... پروتکل‌های رمزگذاری Wi-Fi                                |
| ۲۰۱ | ..... WEP                                                      |
| ۲۰۱ | ..... WPA                                                      |
| ۲۰۱ | ..... WPA2                                                     |
| ۲۰۲ | ..... WPA3                                                     |
| ۲۰۳ | ..... آسیب‌پذیری‌های رایج در شبکه‌های بی‌سیم                   |
| ۲۰۷ | ..... مکانیسم‌های احراز هویت و کنترل دسترسی                    |
| ۲۰۹ | ..... سامانه تشخیص و پیشگیری از نفوذ در شبکه‌های بی‌سیم (IDPS) |
| ۲۱۷ | ..... نظارت و مدیریت امنیت شبکه‌های بی‌سیم                     |
| ۲۲۳ | ..... نتیجه‌گیری                                               |
| ۲۲۴ | ..... نکات مهم این فصل                                         |
| ۲۲۴ | ..... سوالات چندگزینه‌ای                                       |
| ۲۲۷ | ..... پاسخ‌ها                                                  |
| ۲۲۸ | ..... سوالات                                                   |

## فصل ۷

### ۲۲۹..... امنیت ابری

|     |                                                    |
|-----|----------------------------------------------------|
| ۲۲۹ | ..... مقدمه                                        |
| ۲۲۹ | ..... ساختار فصل                                   |
| ۲۳۰ | ..... اهداف                                        |
| ۲۳۰ | ..... مدل‌های استقرار ابر                          |
| ۲۳۱ | ..... ابر عمومی                                    |
| ۲۳۲ | ..... ابر خصوصی                                    |
| ۲۳۴ | ..... ابر جامعه‌ای                                 |
| ۲۳۶ | ..... ابر ترکیبی                                   |
| ۲۴۰ | ..... مدل‌های خدمات ابری                           |
| ۲۴۰ | ..... زیرساخت به عنوان خدمت (IaaS)                 |
| ۲۴۲ | ..... پلتفرم به عنوان خدمت (PaaS)                  |
| ۲۴۴ | ..... نرم‌افزار به عنوان خدمت (SaaS)               |
| ۲۴۷ | ..... امنیت و تهدیدات در محیط‌های ابری             |
| ۲۵۱ | ..... مراحل پیشگیری از ریسک‌های امنیتی رایانش ابری |
| ۲۵۲ | ..... امنیت داده و حفظ حریم خصوصی در فضای ابری     |

|     |                                          |
|-----|------------------------------------------|
| ۲۵۴ | مدیریت هویت و دسترسی در محیط‌های ابری    |
| ۲۵۶ | بهترین شیوه‌ها و استانداردهای امنیت ابری |
| ۲۶۱ | تطبیق‌پذیری و حاکمیت در رایانش ابری      |
| ۲۶۴ | ابزارها و فناوری‌های امنیت ابری          |
| ۲۶۷ | نتیجه‌گیری                               |
| ۲۶۷ | نکات مهم این فصل                         |
| ۲۶۷ | سؤالات چندگزینه‌ای                       |
| ۲۷۰ | پاسخ‌ها                                  |
| ۲۷۱ | سؤالات تشریحی                            |

## فصل ۸

### ۲۷۲..... امنیت در دنیای دیجیتال

|     |                                             |
|-----|---------------------------------------------|
| ۲۷۲ | مقدمه                                       |
| ۲۷۲ | ساختار فصل                                  |
| ۲۷۳ | اهداف                                       |
| ۲۷۳ | امنیت مبتنی بر رمز عبور                     |
| ۲۷۴ | مزایای احراز هویت مبتنی بر رمز عبور         |
| ۲۷۴ | معایب احراز هویت مبتنی بر رمز عبور          |
| ۲۷۴ | کاربرد رمز عبور                             |
| ۲۷۵ | انواع مختلف رمز عبور                        |
| ۲۷۶ | انواع حملات به رمز عبور و اقدامات پیشگیرانه |
| ۲۸۰ | امنیت اینترنت اشیا                          |
| ۲۸۵ | امنیت شبکه‌های اجتماعی                      |
| ۲۹۰ | امنیت و رمز ارزها                           |
| ۲۹۳ | نرم‌افزارهای مجموعه امنیتی                  |
| ۲۹۵ | فایروال                                     |
| ۲۹۶ | انواع فایروال‌ها                            |
| ۳۰۲ | نتیجه‌گیری                                  |
| ۳۰۲ | نکات مهم این فصل                            |
| ۳۰۳ | سؤالات چندگزینه‌ای                          |
| ۳۰۶ | پاسخ‌ها                                     |
| ۳۰۶ | سؤالات تشریحی                               |

## روندهای نوظهور و مباحث پیشرفته در امنیت سایبری..... ۳۰۸

|     |                                                            |
|-----|------------------------------------------------------------|
| ۳۰۸ | ..... مقدمه                                                |
| ۳۰۸ | ..... ساختار فصل                                           |
| ۳۰۹ | ..... اهداف                                                |
| ۳۰۹ | ..... امنیت ابری و مجازی سازی                              |
| ۳۱۶ | ..... هوش مصنوعی (AI) و یادگیری ماشین (ML) در امنیت سایبری |
| ۳۱۹ | ..... جرم‌شناسی دیجیتال                                    |
| ۳۲۴ | ..... پیامدهای فناوری بلاک چین بر امنیت سایبری             |
| ۳۲۶ | ..... پیامدهای محاسبات کوانتومی بر امنیت سایبری            |
| ۳۲۷ | ..... چالش‌های امنیتی در اینترنت اشیاء                     |
| ۳۲۹ | ..... نتیجه‌گیری                                           |
| ۳۲۹ | ..... نکات مهم این فصل                                     |
| ۳۳۰ | ..... سوالات چندگزینه‌ای                                   |
| ۳۳۳ | ..... کلید پاسخ‌ها                                         |
| ۳۳۴ | ..... سوالات                                               |