

بسته: رهگیری جرم





۲.....	فصل اول
۳.....	فصل دوم
۴.....	فصل سوم
۵.....	فصل چهارم
۶.....	فصل پنجم
۷.....	فصل ششم
۸.....	فصل هفتم
۱۰.....	فصل هشتم
۱۱.....	فصل نهم

فصل اول

- معرفی ۷ لایه مدل OSI
- تفاوت UDP و TCP چیست؟
- مفهوم حمله Denial of service چیست؟
- مفهوم حمله Packet sniffing چیست؟
- مفهوم MAC Flooding چیست؟
- Network Device Security
- معرفی فانکشن های تجهیزات شبکه
- تفاوت MAC Address و IP Address چیست؟
- کاربرد ابزار Wireshark چیست؟
- چگونه می توان سورس یک فیلم در اینستاگرام را پیدا کرده و آن را دانلود کرد؟
- کاربرد دیوایس Data Diode چیست؟
- تفاوت fault، fail و error چیست؟
- Security Wireless Networks
- چرا شبکه Wireless امنیت خوبی ندارد؟
- چگونه می توان امنیت شبکه وایرلس را افزایش داد؟
- تشریح مفهوم ریسک و ارتباط آن با آسیب پذیری و تهدید

فصل دوم

- در انتخاب پسورد مناسب به چه نکاتی می بایست دقت کنیم؟
- اصل Single Sign-in به چه نکته ای اشاره دارد؟
- مفهوم Hash دیتابیس چیست؟
- ضرورت انتخاب پسوردهای پیچیده چیست؟
- کاربرد نرم افزار John the ripper چیست؟
- تشریح مفهوم CIS Controls
- Wanna cry چیست و چگونه از بین رفت؟
- مفهوم Deep Web و Dark Web چیست؟
- Securing Web Communications
- معرفی ابزار mimikatz و کاربرد آن
- کاربرد SSL یا TLS چیست؟
- چگونه می توانیم از بارگذاری کوکی ها در مرورگر جلوگیری کنیم؟

فصل سوم

- Threat Management
- vulnerability scanning and penetration testing
- کاربرد نرم افزار Nessus چیست؟
- کاربرد دیتا دیود چیست؟
- Endpoint Security
- معرفی Splunk و قابلیت های آن

فصل چهارم

- cryptography & Risk management
- مفهوم cryptography و cryptanalysis چیست؟
- تشریح مفاهیم اساسی مبحث cryptography
- تشریح مفهوم رمزگذاری متقارن (Symmetric) و نامتقارن (Asymmetric)
- ارائه یک نمونه از تهیه کلید رمزنگاری به روش ریاضی
- ارائه چند نمونه از رمزگذاری متن
- تشریح مفاهیم PKI و Digital Sign
- تشریح steganography و کاربرد آن
- معرفی الگوریتم های رمزنگاری
- windows Security
- امنیت لینوکس (Linux security Essentials)

فصل پنجم

- در رابطه با سرعت اطلاعات، چه سوال هایی مطرح می شود که دانستن آنها اهمیت دارد؟
- هنگام مواجهه با یک مورد نفوذ به سیستم چه کارهایی را می بایست انجام دهیم؟
- ضرورت تهیه image از رم قربانی (سیستم هک شده) چیست؟
- معرفی یکی از ابزارهای تهیه image از رم
- ضرورت بررسی Encryption دیسک چیست؟
- ضرورت تریاژ دیتای سیستم قربانی شده چیست؟
- معرفی نرم افزار FTK imager
- معرفی ابزار CYLR

فصل ششم

- آنالیز رجیستری ویندوز
- چه مواردی در SUM نگهداری می شوند؟
- فایل های NTUSER.DAT و USRCLASS.DAT در چه مسیری نگهداری می شوند؟
- کاربرد ابزار Registry Explorer چیست؟
- ارائه یک نمونه پروژه ساده از آنالیز فایل پاک شده
- معرفی دو کتاب انگلیسی در زمینه رجیستری
- استخراج اطلاعات یوزر چگونه انجام می گیرد؟
- نمایش Microsoft OS Version در رج ادیت
- مفهوم Control Set چیست؟
- ضرورت دانستن Computer Name کامپیوتر قربانی شده چیست؟
- دانستن چه نکاتی در استخراج Time Zone اهمیت دارد؟
- ضرورت دانستن Network Interfaces چیست؟
- دانلود و معرفی نرم افزار Decode
- تشریح روش کانورت کد به تایم با نرم افزار Decode
- چگونه می توانیم از آخرین سرچ هکر آگاه شویم؟

فصل هفتم

- shell item ها شامل چه مواردی می شوند؟
- Short Files (LNK)
- چگونه می توان اطلاعات یک فایل پاک شده را مشاهده کرد؟
- آدرس LNK فایل ویندوز کجاست؟
- ارائه خروجی گرافیکی از LNK فایل
- معرفی ابزار lp64.exe
- مفهوم Jump Lists و کاربرد آن چیست؟
- معرفی AppID چند اپلیکیشن معروف
- معرفی ابزار JLECmd
- تشریح روش استخراج AppID نرم افزارها
- مفهوم Shellbags و کاربرد آن چیست؟
- معرفی ابزار Shellbags Explorer
- USB Device Analysis
- چه اطلاعاتی را می توان در مورد سخت افزاری که از طریق درگاه USB به رایانه وصل شده استخراج کرد؟
- یو اس پی ها در چه تایپ هایی توسط ویندوز شناخته می شوند؟
- انواع Malware را چگونه می توان شناخت؟
- مفهوم پروتکل های PTP، MTP و MSC چیست؟
- کدام پروتکل مربوط به استاندارد ISO 15740 می شود؟
- LNK فایل هر پروتکل در چه مسیری ذخیره می شود؟
- چگونه می توانیم مدل USB و سریال نامبر آن را استخراج کنیم؟
- چگونه می توانیم کاربری که از USB Device استفاده نموده را پیدا کنیم؟

- تشریح روش استخراج زمان های اتصال و جداسازی USB
- معرفی ابزار USB Detective و تشریح روش استفاده از آن

فصل هشتم

- فارنزیک ایمیل
- از هر ایمیل چند نسخه وجود دارد و در چه سرورهایی ذخیره می شود؟
- در بحث فارنزیک ایمیل به چه اطلاعاتی می توان دسترسی یافت؟
- Mail Header شامل چه اطلاعاتی می شود؟
- Message Body شامل چه اطلاعاتی می شود؟
- Attachment شامل چه اطلاعاتی می شود؟
- با استفاده از ابزارهای مرورگر، چه اطلاعاتی از ایمیل می توان استخراج کرد؟
- آشنایی با Artifacts
- دیتابیس سرچ های ویندوز در چه آدرسی ذخیره می شود؟
- کاربرد ابزار esentutl.exe چیست؟
- معرفی ابزار refiuti.exe
- در مسیر windows Prefetch چه اطلاعاتی ذخیره می شود؟
- کاربرد ابزار SRUM در علم فارنزیک چیست؟
- event log analysis
- کاربرد windows Events چیست؟
- event log های هر ویندوز، در چه مسیری ذخیره می شوند؟
- چگونه می توانیم Alert های ویندوز را مشاهده کنیم؟
- در security log چه اطلاعاتی موجود است؟
- معرفی انواع Event Type
- کد Logon type به چه معناست؟
- معرفی ابزار Event Log Explorer
- کاربرد ابزار Sysmon چیست؟

فصل نهم

- Browser Forensics
- تاریخچه یا History مرورگر IE در چه مسیری ذخیره می شود؟
- Cache و Cookie های مرورگر IE در چه مسیری ذخیره می شوند؟
- معرفی و استفاده از ابزار faview
- در History Database مرورگر کروم چه مواردی موجود است؟
- Cache و Cookie های مرورگر فایرفاکس در چه مسیری ذخیره می شوند؟