

# فهرست مطالب

۱۶	فصل ۱. مقدمه ای بر هک
۱۸	۱-۱. شناسایی عوامل تهدید و هدف آنها.....
۲۲	درک آنچه برای بازیگران تهدید مهم است.....
۲۲	۱-۱-۱. زمان.....
۲۳	۱-۲. منابع.....
۲۳	۱-۲-۱. عوامل مالی.....
۲۴	۱-۳. ارزش هک.....
۲۴	۱-۴. کاوش اصطلاحات امنیت سایبری.....
۲۸	بررسی نیاز به تست نفوذ و مراحل آن.....
۲۹	۱-۵. ایجاد یک طرح نبرد تست نفوذ.....
۳۲	مدل سازی تهدید.....
۳۳	۱-۶. تجزیه و تحلیل آسیب پذیری.....
۳۳	بهره برداری.....
۳۵	۱-۷. درک رویکردهای تست نفوذ.....
۳۶	انواع تست نفوذ.....
۳۹	۱-۸. بررسی مراحل هک.....
۴۳	درک چارچوب زنجیره کشتار سایبری.....
۵۰	۱-۹. خلاصه.....
۵۱	فصل ۲. راه اندازی برای تکنیک های هک پیشرفته
۵۲	۲-۱. ساخت آزمایشگاه تیم قرمز AD.....

۵۴.....	قسمت ۱ - نصب ویندوز سرور ۲۰۱۹.....	۲-۲
۶۵.....	قسمت ۳ - ارتقاء به DC.....	۲-۳
۶۷.....	بخش ۴ - ایجاد کاربران دامنه و حساب های سرپرست.....	۲-۴
۶۹.....	قسمت ۵ - غیرفعال کردن محافظت از ضد بدافزار و فایروال دامنه.....	۲-۵
۷۵.....	راه اندازی آزمایشگاه تست نفوذ بی سیم.....	۲-۶
۷۷.....	پیاده سازی سرور RADIUS.....	۲-۷
۸۷.....	قسمت ۳ - پیکربندی روتر بی سیم با RADIUS.....	۲-۸
۸۹.....	خلاصه.....	۲-۹

### فصل ۳. شناسایی فعال شبکه های خارجی و داخلی

۹۱		۹۱
۹۳.....	تکنیک های اسکن مخفی.....	۳-۱
۹۳.....	تنظیم پشته IP منبع و تنظیمات شناسایی ابزار.....	۳-۱-۱
۹۵.....	اصلاح پارامترهای بسته.....	۳-۱-۲
۹۸.....	استفاده از پروکسی با شبکه های ناشناس.....	۳-۱-۳
۱۰۳.....	شناسایی DNS و route mapping.....	۳-۲
۱۰۳.....	فرمان whois (پس از GDPR).....	۳-۲-۱
۱۰۴.....	بکارگیری برنامه های شناسایی جامع.....	۳-۳
۱۰۵.....	فریم ورک recon-ng.....	۳-۴
۱۱۸.....	شناسایی زیرساخت شبکه خارجی.....	۳-۵
۱۲۰.....	نقشه برداری فراتر از فایروال.....	۳-۶
۱۲۱.....	شناسایی IDS/IPS.....	۳-۶-۱
۱۲۲.....	کاوش هاست ها.....	۳-۷
۱۲۴.....	کشف پورت، سیستم عامل و سرویس.....	۳-۸
۱۲۵.....	نوشتن پورت اسکنر خود با استفاده از netcat.....	۳-۹
۱۲۶.....	فوت پریتینگ سیستم عامل.....	۳-۹-۱
۱۲۷.....	تعیین سرویس های فعال.....	۳-۹-۲
۱۲۹.....	اسکن در مقیاس بزرگ.....	۳-۱۰

## فصل ۱. مقدمه ای بر هک ■ ۹

اطلاعات DHCP	۳-۱۰-۱	۱۳۰
شناسایی و کاوش میزبان های شبکه داخلی	۳-۱۰-۲	۱۳۱
دستورات نیتو MS Windows	۳-۱۰-۳	۱۳۳
پخش ARP	۳-۱۰-۴	۱۳۶
پینگ سوئیپ	۳-۱۰-۵	۱۳۷
استفاده از اسکریپت ها برای ترکیب اسکن nmap و masscan	۳-۱۰-۶	۱۳۸
استفاده از SNMP	۳-۱۰-۷	۱۴۰
اطلاعات اکانت ویندوز با نشست های SMB	۳-۱۰-۸	۱۴۳
مکان یابی اشتراک های شبکه	۳-۱۰-۹	۱۴۴
شناسایی سرورهای دامنه اکتیو دایرکتوری	۳-۱۰-۱۰	۱۴۶
کاوش محیط Microsoft Azure	۳-۱۰-۱۱	۱۴۷
استفاده از ابزار جامع (Legion)	۳-۱۰-۱۲	۱۵۰
استفاده از یادگیری ماشینی برای شناسایی	۳-۱۰-۱۳	۱۵۱
خلاصه	۳-۱۱	۱۵۴

## فصل ۴. ارزیابی آسیب پذیری ۱۵۵

دیتابیس های آسیب پذیری محلی و آنلاین	۴-۱	۱۵۷
اسکن آسیب پذیری با Nmap	۴-۱-۱	۱۶۲
مقدمه ای بر اسکریپت نویسی Lua	۴-۱-۲	۱۶۴
سفارشی کردن اسکریپت های NSE	۴-۱-۳	۱۶۶
اسکنرهای آسیب پذیری وب اپلیکیشن ها	۴-۱-۴	۱۶۸
نیکتو	۴-۱-۵	۱۶۹
OWASP ZAP	4-1-6	۱۷۳
اسکنر آسیب پذیری برای برنامه های موبایل	۴-۲	۱۷۷
اسکنر آسیب پذیری شبکه OpenVAS	۴-۲-۱	۱۷۹
سفارشی کردن OpenVAS	۴-۲-۲	۱۸۲



۱۸۲.....	اسکرهای آسیب پذیری تجاری	۴-۳
۱۸۳.....	نسوس	۴-۳-۱
۱۸۵.....	Qualys	۴-۳-۲
۱۸۶.....	اسکرهای تخصصی	۴-۴
۱۸۷.....	مدل سازی تهدید	۴-۵
۱۹۲.....	خلاصه	۴-۶

## ۱۹۳ فصل ۵. مهندسی اجتماعی پیشرفته و امنیت فیزیکی

۱۹۵.....	متدولوژی فرمان و TTP	۵-۱
۱۹۶.....	فن آوری	۵-۱-۱
۲۰۰.....	حملات فیزیکی به کنسول	۵-۱-۲
۲۰۶.....	Sticky Keys	۵-۱-۳
۲۰۸.....	ایجاد یک دستگاه فیزیکی Rogue	۵-۱-۴
۲۰۹.....	عوامل حمله میکرو کامپیوتر یا USB	۵-۱-۵
۲۱۰.....	Raspberry Pi	۵-۱-۶
۲۱۲.....	Malduino : BadUSB	5-1-7.
۲۱۶.....	مجموعه ابزار مهندسی اجتماعی (SET)	۵-۲
۲۲۰.....	حملات مهندسی اجتماعی	۵-۲-۱
۲۲۱.....	روش حمله وب Credential harvester	۵-۲-۲
۲۲۶.....	روش وب اتک چند حمله ای (Multi-attack web attack)	۵-۲-۳
۲۲۷.....	روش حمله به وب HTA	۵-۲-۴
۲۳۰.....	استفاده از حمله تزریق شل کد الفبایی PowerShell	۵-۲-۵
۲۳۱.....	مخفی کردن فایل های اجرایی و مبهم کردن URL مهاجم	۵-۲-۶
۲۳۳.....	تشدید حمله با استفاده از تغییر مسیر DNS	۵-۲-۷
۲۳۵.....	حمله Spear phishing	۵-۲-۸
۲۴۰.....	فیشینگ ایمیل با استفاده از Gophish	۵-۲-۹
۲۴۳.....	راه اندازی یک حمله فیشینگ با استفاده از Gophish	۵-۲-۱۰

۱۱-۲-۵. استفاده از انتقال انبوه به عنوان فیشینگ برای تحویل پیلود.....۲۴۸

۵-۳. خلاصه .....۲۴۹

## فصل ۶. انجام تست نفوذ شبکه

۲۵۰

۶-۱. کشف سیستم های زنده .....۲۵۱

۶-۲. ایجاد پروفایل برای یک سیستم هدف.....۲۵۵

۶-۳. بررسی حملات مبتنی بر رمز عبور.....۲۵۸

۶-۳-۱. بهره برداری از پروتکل ریموت دسکتاپ ویندوز.....۲۶۱

۶-۳-۲. ایجاد لیست کلمات با استفاده از کلمات کلیدی.....۲۶۵

۶-۳-۳. استفاده از Crunch برای آن لیست کلمات.....۲۶۶

۶-۴. شناسایی و بهره برداری از خدمات آسیب پذیر .....۲۶۷

۶-۴-۱. بهره برداری از یک سرویس آسیب پذیر در یک سیستم لینوکس.....۲۶۷

۶-۴-۲. بهره برداری از SMB در مایکروسافت ویندوز.....۲۷۲

6-4-3. تکنیک Pass the Hash.....۲۸۸

۶-۴-۴. دستیابی به دسترسی با بهره برداری از SSH.....۲۹۳

۶-۴-۵. بهره برداری از مدیریت از راه دور ویندوز.....۲۹۷

۶-۴-۶. بهره برداری از ElasticSearch.....۳۰۳

۶-۴-۷. بهره برداری از پروتکل مدیریت شبکه ساده.....۳۰۵

۶-۵. درک حملات گودال آب (watering hole).....۳۰۷

۶-۶. خلاصه .....۳۰۹

## فصل ۷. بهره برداری از وب اپلیکیشن ها

۳۱۰

۷-۱. روش هک وب اپلیکیشن ها .....۳۱۱

۷-۲. نقشه ذهنی هکرها .....۳۱۴

۷-۳. شناسایی وب اپلیکیشن ها .....۳۱۶

۷-۳-۱. تشخیص فایروال برنامه وب و Load Balancers.....۳۱۹

۷-۳-۲. فوت پریتینگ وب سرویس و CMS.....۳۲۲

۷-۳-۳. مرور یک وب سایت از خط فرمان.....۳۲۶

۳۲۷.....	۷-۴. پروکسی های سمت کلاینت.....
۳۲۸.....	۷-۴-۱. برپ پروکسی (Burp Proxy).....
۳۳۷.....	۷-۴-۲. خزیدن وب و حملات brute-force دایرکتوری.....
۳۳۷.....	۷-۴-۳. اسکنرهای آسیب پذیری خاص سرویس وب.....
۳۳۹.....	۷-۵. حملات ویژه برنامه.....
۳۳۹.....	۷-۵-۱. بروت فورس کردن اطلاعات کاربری.....
۳۴۰.....	۷-۵-۲. تزریق فرمان سیستم عامل با استفاده از commix.....
۳۴۲.....	7-5-3. sqlmap.....
۳۴۶.....	۷-۵-۴. تزریق XML.....
۳۴۹.....	۷-۵-۵. حمله Bit-flipping.....
۳۵۳.....	۷-۵-۶. حفظ دسترسی با وب شل ها.....
۳۵۸.....	۷-۵-۷. فریم ورک بهره برداری مرورگر ( BeEF ).....
۳۶۴.....	۷-۵-۸. آشنایی با مرورگر BeEF.....
۳۷۰.....	۷-۵-۹. استفاده از BeEF به عنوان یک پروکسی تونل سازی.....
۳۷۳.....	۷-۶. خلاصه.....

## ۳۷۵ فصل ۸ مرحله پس از اکسپلویت

۳۷۶.....	۸-۱. پس از اکسپلویت با استفاده از Meterpreter.....
۳۷۸.....	۸-۱-۱. عملیات اصلی.....
۳۸۲.....	۸-۱-۲. عملیات رابط کاربری.....
۳۸۳.....	۸-۱-۳. انتقال فایل.....
۳۸۵.....	۸-۱-۴. افزایش سطح دسترسی.....
۳۸۷.....	۸-۱-۵. دزدی توکن و جعل هویت.....
	۸-۱-۶. حرکت جانبی و چرخش ( Pivoting و Lateral movement )
	۳۹۵
۴۰۱.....	۸-۱-۷. پاکسازی ردها.....
۴۰۲.....	۸-۲. رمزگذاری و استخراج داده ها.....



۴۰۲.....	کدگذاری فایل های اجرایی با استفاده از exe2hex	۸-۲-۱
۴۰۵.....	استخراج داده ها با استفاده از PacketWhisper	۸-۲-۲
۴۱۴.....	آشنایی با حملات MITM و packet sniffing	۸-۳
۴۱۸.....	انجام حملات MITM با استفاده از Ettercap	۸-۴
۴۲۱.....	خلاصه	۸-۵

## فصل ۹. تست نفوذ وای فای پیشرفته

۴۲۲.....		
۴۲۳.....	الزامات فنی	۹-۱
۴۲۴.....	مقدمه ای بر شبکه های بی سیم	۹-۲
۴۲۶.....	MIMO و SISO	۹-۲-۱
۴۳۰.....	استانداردهای امنیتی وای فای	۹-۲-۲
۴۳۲.....	انجام شناسایی بی سیم	۹-۳
۴۳۸.....	تعیین کلاینت های مرتبط برای یک شبکه خاص	۹-۳-۱
۴۴۰.....	رخنه کردن در شبکه های WPA و WPA2	۹-۴
۴۴۷.....	انجام حملات بدون AP	۹-۵
۴۵۳.....	بهره برداری از شبکه های بی سیم سازمانی	۹-۶
۴۶۵.....	ساخت هانی پات وای فای	۹-۷
۴۷۱.....	بررسی حملات WPA3	۹-۸
۴۷۳.....	انجام یک Downgrade و حمله دیکشنری	۹-۸-۱
۴۷۷.....	ایمن سازی شبکه بی سیم	۹-۹
۴۷۷.....	مدیریت SSID	۹-۹-۱
۴۷۹.....	سطوح قدرت برای آنتن ها	۹-۹-۲
۴۸۰.....	رمزهای عبور قوی	۹-۹-۳
۴۸۱.....	ایمن سازی شبکه های بی سیم سازمانی	۹-۹-۴
۴۸۲.....	خلاصه	۹-۱۰

## فصل ۱۰. فرماندهی و کنترل

۴۸۴.....	پایدارسازی	۱۰-۱
----------	------------	------

- ۴۸۵..... استفاده از عوامل پایدارسازی ۱۰-۲
- ۴۸۶..... استفاده از Netcat به عنوان یک عامل دائمی ۱۰-۲-۱
- ۴۹۱..... استفاده از schtasks برای پیکربندی یک کار مداوم ۱۰-۳
- ۴۹۳..... پایدارسازی با فریم ورک Metasploit ۱۰-۳-۱
- ۴۹۳..... استفاده از مازول پس از اکسپلویت persistence ۱۰-۳-۲
- ۴۹۴..... ایجاد یک عامل پایدار مستقل با Metasploit ۱۰-۴
- ۴۹۷..... پایدارسازی استفاده از سرویس های ابری ذخیره سازی فایل آنلاین ۱۰-۵
- ۴۹۷..... دراپ باکس ۱۰-۵-۱
- ۵۰۰..... مایکروسافت وان درایو ۱۰-۵-۲
- ۵۰۵..... Covenant ۱۰-۵-۳
- ۵۰۸..... PoshC2 10-5-4
- ۵۱۱..... فرانتینگ دامنه (Domain fronting) ۱۰-۶
- ۵۱۱..... استفاده از Amazon CloudFront برای C2 ۱۰-۶-۱
- ۵۱۷..... استخراج داده ها ۱۰-۷
- ۱۰-۷-۱..... استفاده از سرویس های سیستم موجود (VNC و RDP، Telnet)
- ۵۱۸
- ۵۲۰..... استفاده از پروتکل ICMP ۱۰-۷-۲
- ۵۲۲..... پنهان کردن شواهد حمله ۱۰-۷-۳
- ۵۲۵..... خلاصه ۱۰-۸

## فصل ۱۱. انجام حملات کلاینت ساید - مهندسی اجتماعی ۵۲۶

- ۵۲۷..... مبانی مهندسی اجتماعی ۱۱-۱
- ۵۲۹..... عناصر مهندسی اجتماعی ۱۱-۱-۱
- ۵۳۱..... انواع مهندسی اجتماعی ۱۱-۲
- ۵۳۱..... مبتنی بر انسان ۱۱-۲-۱
- ۵۳۳..... مبتنی بر کامپیوتر ۱۱-۲-۲
- ۵۳۵..... مبتنی بر موبایل ۱۱-۲-۳



۵۳۶.....	شبکه اجتماعی	۱۱-۲-۴
۵۳۸.....	برنامه ریزی برای هر نوع حمله مهندسی اجتماعی	۱۱-۳
۵۳۹.....	بررسی ابزارها و تکنیک های مهندسی اجتماعی	۱۱-۴
۵۳۹.....	ایجاد یک وب سایت فیشینگ	۱۱-۴-۱
۵۴۴.....	ایجاد رسانه های آلوده (infectious)	۱۱-۴-۲
۵۴۷.....	خلاصه	۱۱-۵

## تست نفوذ پیشرفته وب سایت

## فصل ۱۲

۵۴۸

۵۴۹.....	الزامات فنی	۱۲-۱
۵۵۰.....	شناسایی اجزای آسیب پذیر و قدیمی	۱۲-۲
۵۵۵.....	بهره برداری از نقص های شناسایی و احراز هویت	۱۲-۲-۱
۵۵۵.....	کشف خرابی های احراز هویت	۱۲-۲-۲
۵۶۳.....	آشنایی با نقص نرم افزار و یکپارچگی داده ها	۱۲-۳
۵۶۴.....	آشنایی با گزارش های امنیتی و نظارت بر خرابی ها	۱۲-۴
۵۶۵.....	انجام جعل درخواست سمت سرور	۱۲-۵
۵۷۰.....	خودکارسازی حملات تزریق SQL	۱۲-۶
۵۸۲.....	آشنایی با تزریق کد در وب سایت	۱۲-۷
۵۹۲.....	انجام حملات سمت کلاینت	۱۲-۸
۶۰۰.....	خلاصه	۱۲-۹

## فصل ۱۳. نکات حرفه ای برای تست نفوذ به عنوان یک شغل

۶۰۲.....	الزامات فنی	۱۳-۱
۶۰۳.....	دستورالعمل برای آزمونگرهای نفوذ	۱۳-۲
۶۰۳.....	کسب مجوز کتبی	۱۳-۳
۶۰۴.....	اخلاق مدار بودن	۱۳-۴
۶۰۴.....	قرارداد تست نفوذ	۱۳-۵
۶۰۵.....	قوانین اقدام	۱۳-۶

۶۰۶.....	چک لیست تست نفوذ	۱۳-۷.
۶۱۰.....	ساخت کیف ابزار هکر	۱۳-۸.
۶۱۶.....	راه اندازی دسترسی از راه دور	۱۳-۹.
۶۲۲.....	گام های بعدی در پیش	۱۳-۱۰.
۶۲۴.....	خلاصه	۱۳-۱۱.

۶۲۷

کپی رایت