

فهرست

۱	فصل ۱: تست نفوذ هدفمند
۲	۱-۱ انواع مختلف بازیگران تهدید
۲	۱-۲ نمای کلی مفهومی تست امنیت
۳	۱-۳ مشکلات رایج ارزیابی آسیب پذیری، تست نفوذ، و تمرین های رد تیم
۵	۱-۴ تست نفوذ هدفمند
۵	۱-۵ روش شناسی تست
۸	۱-۶ آشنایی با ویژگی های کالی لینوکس
۱۰	۱-۷ نقش کالی در تاکتیک رد تیم
۱۱	۱-۸ نصب و به روز رسانی کالی لینوکس
۱۳	۱-۸-۱ نصب کالی روی Raspberry Pi 4
۱۳	۱-۸-۲ نصب کالی در VM
۱۴	۱-۸-۳ VMware Workstation Player
۱۵	۱-۸-۴ VirtualBox
۱۷	۱-۸-۳ نصب بر روی دستگاه داکر
۱۸	۱-۸-۴ کالی در AWS Cloud
۲۱	۱-۸-۵ کالی در Google Cloud Platform (GCP)
۲۷	۱-۸-۶ کالی در اندروید (تلفن های روت نشده)
۲۹	۱-۹ سازماندهی کالی لینوکس
۲۹	۱-۱۰ پیکربندی و سفارشی سازی کالی لینوکس
۳۰	۱-۱۰-۱ بازنشانی رمز عبور پیش فرض
۳۰	۱-۱۰-۲ کانفیگ تنظیمات پروکسی شبکه
۳۰	۱-۱۰-۳ دسترسی به شل امن از راه دور

۳۱.....	۱-۱۰-۴ تسریع عملیات کالی.....
۳۲.....	۱-۱۰-۵ به اشتراک گذاری پوشه‌ها با سیستم عامل میزبان.....
۳۳.....	۱-۱۱ استفاده از اسکریپت‌های Bash برای سفارشی کردن کالی.....
۳۳.....	ساخت آزمایشگاه تأیید.....
۳۳.....	نصب اهداف تعریف شده.....
۳۴.....	شبکه آزمایشگاهی.....
۳۴.....	۱-۱۲ Domain Controller و Active Directory.....
۳۷.....	۱-۱۳ نصب Microsoft Exchange Server 2016.....
۴۰.....	۱-۱۴ Metasploitable3.....
۴۳.....	۱-۱۵ Mutillidae.....
۴۵.....	۱-۱۶ CloudGoat.....
۴۹.....	۱-۱۷ مدیریت تست نفوذ مشارکتی با استفاده از Faraday.....
۵۱.....	خلاصه.....
۵۳.....	فصل ۲: راه‌اندازی کالی لینوکس برای تکنیک‌های هک پیشرفته
۵۴.....	۲-۱ ساخت آزمایشگاه رد تیم AD.....
۵۶.....	۲-۱-۱ نصب ویندوز سرور ۲۰۱۹.....
۶۱.....	۲-۱-۲ نصب ویندوز ۱۰ اینترپرایز.....
۶۳.....	۲-۱-۳ راه‌اندازی خدمات AD.....
۶۴.....	۲-۱-۴ ارتقاء به DC.....
۶۶.....	۲-۱-۵ ایجاد کاربران دامنه و حساب‌های سرپرست.....
۶۷.....	۲-۱-۶ غیرفعال کردن محافظت از ضد بدافزار و فایروال دامنه.....
۶۹.....	۲-۱-۷ راه‌اندازی برای به اشتراک‌گذاری فایل و حملات احراز هویت سرویس.....
۷۱.....	۲-۱-۸ پیوستن کلاینت‌ها به دامنه AD.....

۷۱.....	۲-۱-۹ راه‌اندازی برای حملات local account takeover and SMB
۷۲.....	۲-۱-۱۰ راه‌اندازی آزمایشگاه تست نفوذ بی‌سیم
۷۴.....	۲-۲ پیاده‌سازی سرور RADIUS
۷۴.....	۲-۲-۱ نصب سرور اوبونتو
۷۸.....	۲-۲-۲ نصب و پیکربندی FreeRadius
۸۲.....	۲-۳ پیکربندی روتر بی‌سیم با RADIUS
۸۴.....	خلاصه
۸۵	فصل ۳: کاوش در جمع‌آوری اطلاعات فعال
۸۶.....	۳-۱ الزامات فنی
۸۶.....	۳-۲ آشنایی با شناسایی فعال
۸۷.....	۳-۳ بررسی استراتژی‌های هک با گوگل (google hacking)
۹۲.....	۳-۴ کاوش در شناسایی DNS
۹۵.....	۳-۵ انجام کاوش DNS
۹۷.....	بررسی پیکربندی نادرست انتقال منطقه DNS
۱۰۰.....	۳-۶ خودکارسازی OSINT
۱۰۴.....	۳-۷ کاوش زیردامنه‌ها (sub domain)
۱۰۵.....	۳-۷-۱ کار با DNSmap
۱۰۶.....	۳-۷-۲ کاوش Sublist3r
۱۰۷.....	۳-۸ پروفایل ساختن از وبسایت‌ها با استفاده از EyeWitness
۱۰۹.....	۳-۹ بررسی تکنیک‌های اسکن فعال
۱۱۰.....	۳-۱۰ جعل آدرس‌های مک
۱۱۲.....	۳-۱۱ کشف سیستم‌های لایو در یک شبکه
۱۱۵.....	۳-۱۲ بررسی پورت‌ها، سرویس‌ها و سیستم‌عامل‌های سرویس باز

۱۱۸.....	۳-۱۳ کار با تکنیک دور زدن.....
۱۱۹.....	اجتناب از تشخیص با استفاده از Decoys.....
۱۲۰.....	جعل (Spoofing) آدرس‌های MAC و IP در حین اسکن.....
۱۲۱.....	انجام اسکن مخفیانه.....
۱۲۳.....	۳-۱۴ برشمردن خدمات مشترک شبکه.....
۱۲۳.....	۳-۱۴-۱ اسکن با استفاده از Metasploit.....
۱۲۵.....	۳-۱۴-۲ کاوش SMB.....
۱۲۸.....	۳-۱۵ کاوش SSH.....
۱۲۹.....	۳-۱۶ انجام کاوش کاربران از طریق کنترل‌های احراز هویت پر سروصدا.....
۱۳۲.....	۳-۱۷ یافتن نشئت داده‌ها در فضای ابری.....
۱۳۷.....	خلاصه.....
۱۳۷.....	مطالعه بیشتر.....
۱۳۹.....	فصل ۴: انجام ارزیابی‌های آسیب‌پذیری
۱۴۰.....	۴-۱ Nessus و سیاست‌های آن.....
۱۴۰.....	راه‌اندازی Nessus.....
۱۴۴.....	۴-۲ اسکن با Nessus.....
۱۴۶.....	۴-۳ تجزیه و تحلیل نتایج Nessus.....
۱۵۰.....	۴-۴ خروجی گرفتن از نتایج Nessus.....
۱۵۲.....	۴-۵ کشف آسیب‌پذیری با استفاده از Nmap.....
۱۵۷.....	۴-۶ کار با Greenbone Vulnerability Manager.....
۱۶۱.....	۴-۷ استفاده از اسکنرهای وب اپلیکیشن.....
۱۶۲.....	۴-۷-۱ WhatWeb.....
۱۶۳.....	۴-۸ Nmap.....

۱۶۴	۴-۸-۱ متاسپلویت
۱۶۷	۴-۸-۲ Nikto-نیکتو
۱۶۸	۴-۸-۳ WPScan
۱۷۰	خلاصه
۱۷۱	فصل ۵: آشنایی با تست نفوذ شبکه
۱۷۱	الزامات فنی
۱۷۲	۵-۱ مقدمه‌ای بر تست نفوذ شبکه
۱۷۶	۵-۲ کار با شل‌های bind و reverse
۱۷۸	ریموت شل‌ها با استفاده از Netcat
۱۸۰	۵-۳ ایجاد یک شل bind
۱۸۱	ایجاد شل معکوس (Reverse Shell)
۱۸۲	۵-۴ تکنیک‌های دور زدن ضد بدافزار
۱۸۴	۵-۴-۱ استفاده از MSFvenom برای رمزگذاری پیلودها
۱۸۷	۵-۴-۲ ایجاد پیلود با استفاده از Shellter
۱۹۳	۵-۵ کار با آداپتورهای بی سیم
۱۹۴	۵-۵-۱ اتصال آداپتور بی سیم به کالی لینوکس
۱۹۷	۵-۶ اتصال آداپتور بی سیم با چیپست RTL8812AU
۲۰۰	مدیریت و نظارت بر حالت‌های بی سیم
۲۰۱	۵-۶-۱ پیکربندی حالت مانیتور به صورت دستی
۲۰۳	۵-۶-۲ استفاده از Aircrack-ng برای فعال کردن حالت مانیتور
۲۰۶	خلاصه
۲۰۷	فصل ۶: حملات بی سیم و بلوتوث
۲۰۷	۶-۱ مقدمه‌ای بر فناوری‌های بی سیم و بلوتوث

۲۰۸	۶-۲ پیکربندی کالی برای حملات بی‌سیم
۲۰۹	۶-۳ شناسایی بی‌سیم
۲۱۳	۶-۴ دور زدن SSID مخفی
۲۱۶	۶-۵ دور زدن احراز هویت آدرس MAC و احراز هویت باز
۲۱۸	۶-۵-۱ حمله به WPA و WPA2
۲۱۸	۶-۵-۲ حملات Brute-Force
۲۲۲	۶-۵-۳ حمله به روترهای بی‌سیم با Reaver
۲۲۴	۶-۵-۴ حملات انکار سرویس (DoS) علیه ارتباطات بی‌سیم
۲۲۶	۶-۵-۵ رخنه در پیاده‌سازی سازمانی WPA2
۲۲۸	۶-۵-۶ کار با bettercap
۲۳۰	۶-۵-۷ حمله Evil Twin با استفاده از Wifiphisher
۲۳۳	۶-۵-۸ WPA3
۲۳۳	۶-۵-۹ حملات بلوتوث
۲۳۶	خلاصه
۲۳۷	فصل ۷: دور زدن کنترل‌های امنیتی
۲۳۸	۷-۱ دور زدن کنترل دسترسی شبکه (NAC)
۲۳۸	۷-۱-۱ NAC پیش از پذیرش
۲۴۱	۷-۱-۲ NAC پس از پذیرش
۲۴۱	۷-۲ دور زدن کنترل‌های سطح برنامه
۲۴۱	۷-۲-۱ تونل زدن از فایروال سمت کلاینت با استفاده از SSH
۲۴۲	۷-۲-۲ دور زدن مکانیسم‌های فیلتر URL
۲۴۵	۷-۲-۳ خروجی به ورودی (Outbound to inbound)
۲۴۶	۷-۳ دور زدن آنتی‌ویروس با فایل‌ها

۲۴۸	۷-۳-۱ استفاده از فریم‌ورک Veil.....
۲۵۳	۷-۳-۲ استفاده از Shellter.....
۲۵۷	۷-۳-۳ بدون فایل و فرار از آنتی ویروس.....
۲۵۷	۷-۴ دور زدن کنترل‌های سیستم عامل ویندوز.....
۲۵۷	۷-۴-۱ کنترل حساب کاربری (UAC).....
۲۶۰	۷-۴-۲ استفاده از fodhelper برای دور زدن UAC در ویندوز ۱۰.....
۲۶۲	۷-۴-۳ استفاده از Disk Cleanup برای دور زدن UAC در ویندوز ۱۰.....
۲۶۲	۷-۴-۴ مبهم‌سازی PowerShell و استفاده از تکنیک‌های بدون فایل.....
۲۶۵	۷-۵ سایر کنترل‌های سیستم عامل مخصوص ویندوز.....
۲۶۶	۷-۵-۱ دسترسی و مجوز.....
۲۶۷	۷-۵-۲ رمزگذاری.....
۲۶۸	۷-۵-۳ امنیت ارتباطات.....
۲۶۸	۷-۵-۴ حسابرسی و ثبت.....
۲۶۹	خلاصه.....
۲۷۱	فصل ۸: آشنایی با امنیت وب اپلیکیشن
۲۷۲	۸-۱ الزامات فنی.....
۲۷۲	۸-۲ آشنایی با وب اپلیکیشن‌ها.....
۲۷۳	۸-۲-۱ مبانی HTTP.....
۲۷۷	۸-۳ کاوش در OWASP 10: 2021.....
۲۷۹	۸-۳-۱ شروع کار با FoxyProxy و Burp Suite.....
۲۸۹	۸-۴ آشنایی با حملات مبتنی بر تزریق.....
۲۹۰	۸-۵ انجام یک حمله تزریق SQL.....

۶-۸ بررسی حملات کنترل دسترسی شکسته (Exploring broken access control attacks)	۲۹۷
۷-۸ کاوش کنترل دسترسی شکسته	۲۹۸
۸-۸ کشف خرابی‌های رمزنگاری	۳۰۱
۸-۹ بهره‌برداری از شکست‌های رمزنگاری	۳۰۱
۸-۱۰ آشنایی با طراحی ناامن	۳۰۷
۸-۱۱ کاوش در پیکربندی نادرست امنیتی	۳۰۷
بهره‌برداری از تنظیمات نادرست امنیتی	۳۰۸
خلاصه	۳۱۲
فصل ۹: Exploit (بهره‌برداری)	۳۱۳
۹-۱ فریم‌ورک Metasploit	۳۱۳
۹-۱-۱ کتابخانه‌ها	۳۱۴
REX	۳۱۵
هسته فریم‌ورک	۳۱۵
پایه فریم‌ورک	۳۱۵
رابط‌ها	۳۱۵
ماژول‌ها	۳۱۶
راه‌اندازی و پیکربندی پایگاه داده	۳۱۷
۹-۲ بهره‌برداری از اهداف با استفاده از MSF	۳۲۳
۹-۲-۱ اهداف منفرد با استفاده از یک شل معکوس ساده	۳۲۳
۹-۲-۲ بهره‌برداری از چندین هدف با استفاده از فایل‌های منبع MSF	۳۲۷
۹-۳ استفاده از اکسپلویت‌های عمومی	۳۲۸
۹-۳-۱ مکان‌یابی و تأیید اکسپلویت‌های در دسترس عموم	۳۲۸

۲۲۹	۹-۳-۲ کامپایل و استفاده از اکسپلویت‌ها
۲۳۱	۹-۴ توسعه یک اکسپلویت ویندوز
۲۳۳	۹-۴-۱ شناسایی آسیب‌پذیری با فایزینگ
۲۳۶	دییابگینگ و تکرار خرابی
۲۳۹	۹-۴-۳ کنترل اجرای برنامه
۲۴۱	۹-۴-۴ شناسایی کاراکترهای بد مناسب و ایجاد شل‌کد
۲۴۲	۹-۴-۵ بدست آوردن شل
۲۴۴	۹-۴-۶ فریم‌ورک PowerShell Empire
۲۴۸	خلاصه
۳۴۹	فصل ۱۰: اقدام برای حرکت جانبی
۳۴۹	۱۰-۱ فعالیت در سیستم محلی رخنه شده
۳۵۰	۱۰-۲ انجام شناسایی سریع یک سیستم رخنه شده
۳۵۲	۱۰-۳ یافتن و گرفتن داده‌های حساس - غارت هدف
۳۵۵	ایجاد حساب‌های اضافی
۳۵۶	ابزارهای پس از بهره‌برداری
۳۵۶	فریم‌ورک Meterpreter - Metasploit
۳۶۰	۱۰-۳-۱ پروژه PowerShell Empire
۳۶۱	۱۰-۳-۲ CrackMapExec
۳۶۵	۱۰-۴ ارتقاء افقی و حرکت جانبی
۳۶۶	رنخه کردن در تراست‌ها و اشتراک‌گذاری‌های دامنه
۳۶۹	۱۰-۴-۱ WMIC, PsExec، و ابزارهای دیگر
۳۷۰	WMIC
۳۷۴	۱۰-۴-۲ ابزار Windows Credentials Editor

۳۷۵	حرکت جانبی با استفاده از سرویس‌ها
۳۷۵	Port Forwarding و Pivoting
۳۷۷	استفاده از ProxyChains
۳۷۹	فصل ۱۱: افزایش سطح دسترسی
۳۷۹	۱۱-۱ مروری بر روش‌های متداول افزایش سطح دسترسی
۳۸۱	۱۱-۲ افزایش سطح دسترسی از کاربر دامنه به مدیر سیستم
۳۸۲	۱۱-۳ ارتقاء سطح دسترسی Local System
۳۸۴	۱۱-۳-۱ افزایش دسترسی از ادمین به سیستم
۳۸۵	۱۱-۳-۲ تزریق DLL
۳۸۸	۱۱-۴ برداشت اطلاعات کاربری و حملات ارتقاء دسترسی
۳۸۸	۱۱-۴-۱ انسیفرهای رمز عبور
۳۹۰	Responder
۳۹۴	۱۱-۴-۲ انجام حمله MiTM به LDAP از طریق TLS
۳۹۹	۱۱-۴-۳ افزایش سطح دسترسی در اکتیو دایرکتوری
۴۰۳	دستور قبلی چه کاری انجام می‌دهد؟
۴۰۴	۱۱-۴-۴ Kerberos - یک حمله با گلدن تیکت (Golden Ticket) ...
۴۱۱	فصل ۱۲: تاکتیک‌های فرماندهی و کنترل
۴۱۲	۱۲-۱ درک C2
۴۱۳	۱۲-۲ راه‌اندازی عملیات C2
۴۲۰	۱۲-۳ پس از اکسپلویت با استفاده از Empire
۴۳۲	کار با Starkiller
۴۴۵	منابع و مآخذ