بسم الله الرحمن الرحیم

اقدامات عملی یک هکر

جهت حمله به پروتکل های شبکه

مترجمان:

علی اکبر رنجبر امامزاده هاشمی علیرضا پوربهرام

سرشناسه : فورشاو، جیمز
Forshaw, James
عنوان و نام پدیدآور : اقدامات عملی یک هکر جهت حمله به پروتکل‌های شبکه/نویسنده [جیمز فورشاو] ؛ مترجمان علی‌اکبر رنجبرامامزاده‌هاشمی،علیرضا پوربهرام.
مشخصات نشر : رشت: دلکام، ۱۳۹۸.
مشخصات ظاهری : ۳۸۲ص.
شابک : 978-622-6229-52-4
وضعیت فهرست نویسی : فیپا
یادداشت : عنوان اصلی: Attacking network protocols : a hacker's guide to capture, analysis, and exploitation,[2017] .
موضوع : پروتکل‌های شبکه کامپیوتری
موضوع : Computer network protocols
موضوع : شبکه‌های کامپیوتری — تدابیر ایمنی
موضوع : Computer networks -- Security measur
شناسه افزوده : رنجبر امامزاده هاشمی، علی‌اکبر، ۱۳۶۱، مترجم
شناسه افزوده : ربهر ، علیرضا، ۱۳۷۰، مترجم
رده بندی کنگره : Tk ۱۰۵/۵
رده بندی دیویی : ۰۰۴/۶۲
شماره کتابشناسی ملی : ۵۸۵۱۱۵۲

آدرس وب سایت انتشارات دلکام: www.delkampub.ir

آدرس الکترونیکی انتشارات دلکام: nikoo[illegible]5@gmail.com

کانال تلگرامی انتشارات دلکام :@pubdelkam تلفن انتشارات : ۰۹۱۱۳۳۱۰۵۸۰

قطع: وزیری شمارگان: ۱۰۰۰ جلد نوبت وسال چاپ: اول ،۱۳۹۸۰

پیشگفتار

به نام حضرت دوست که هرچه داریم از اوست.

زندگی صحنه‌ی یکتای هنرمندی ماست... هر کسی نغمه خود خواند و از صحنه رود...

صحنه پیوسته به جاست... خرم آن نغمه که مردم بسپارند به یاد...

پژوهش و تحقیق کردن یکی از نیازهای اساسی زندگی بشر است. بشر همیشه خواهان بهبود وضعیت خود در هر زمینه‌ها می‌باشد و این مُهم مگر با پژوهش کردن، امکان پذیرنمی‌باشد. برای حمله به پروتکل‌های شبکه، شما باید اصول شبکه کامپیوتری را درک کنید. هر چه بیشتر بدانید که شبکه‌های رایج چگونه ساخته شده و چه عملکردی داشته است، در نتیجه استفاده از آن دانش برای ثبت، تجزیه و تحلیل بهره‌مند از پروتکل‌های جدیدتر، آسان‌تر خواهد شد.

امیدواریم در این کتاب توانسته باشیم همه سوالات شما را پاسخ داده و توانسته باشیم که سوال و انگیزه‌ی تحقیق را در وجودتان شعله‌ور کنیم. این بدان علت است که به طور کلی ماهیت شکل‌گیری این کتاب، سوال و انگیزه تحقیق بوده است که هر اینک در دستان گرانقدر شما مخاطب گرامی قرار گرفته است. مطمئناً کاستی‌هایی در کتاب حاضر وجود دارد، از همه آنهایی که این کتاب را می‌خوانند و به خصوص مدیران؛ کارشناسان، مهندسین و دانشجویان عزیز می‌خواهیم که نقدها و پیشنهادات سازنده خود را از طریق راه‌های ارتباطی زیر، به ما اعلام برسانند. در پایان جا دارد از ناشر محترم و همکاران ایشان به پاس تلاش‌هایی که در فرآیند چاپ این اثر داشته‌اند، کمال تشکر را داشته باشیم.

- علی اکبر رنجبر امامزاده هاشمی کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار.
- علیرضا پوربهرام کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار.

a.ranjbar2013@gmail.com

alirezapourbahram@gmail.com

فهرست مطالب

عنوان — شماره صفحه

فصل اول: اساس و مبانی شبکه

۱-۱- مقدمه ۲۰

۱-۲- معماری شبکه و پروتکل‌ها ۲۰

۱-۳- سوئیت پروتکل اینترنت ۲۲

۱-۴- تجز[illegible] و تحلیل داده‌ها ۲۵

۱-۴-۱- [illegible]رصفحه ها، باورقی ها و آدرس ها ۲۵

۱-۴-۲- انتقال د[illegible]ه ۲۷

۱-۵- مسیریابی شبکه ۲۸

۱-۶- مدل برای تحلیل قرارداد[illegible]شبکه ۳۰

۱-۷- جمع بندی فصل ۳۳

فصل دوم: ثبت ترافیک برنامه

۲-۱- مقدمه ۳۵

۲-۲- ظبط ترافیک شبکه منفعل ۳۵

۲-۳- Quick Primer برای Wireshark ۳۶

۲-۴- تکنیک‌های ضبط منفعل جایگزین ۳۸

۲-۵- ردیابی تماس سیستم ۳۹

۲-۶- برنامه strace Utility در لینوکس ۴۰

۲-۷- نظارت بر اتصالات شبکه با DTrace ۴۱

۲-۸- پایش فرآیند بر روی ویندوز ۴۳

۲-۹- مزایا و معایب ضبط منفعل ۴۵

۲-۱۰- ثبت ترافیک شبکه فعال ۴۶
۲-۱۱- پروکسی های شبکه ۴۷
۲-۱۱-۱- پروکسی Port-Forwarding ۴۷
۲-۱۱-۱-۱- اجرای ساده ۴۷
۲-۱۱-۱-۲- هدایت ترافیک به پروکسی ۴۹
۲-۱۱-۱-۳- مزایای یک پروکسی پیشکار پورت ۵۰
۲-۱۱-۱-۴- معایب یک پروکسی پیشکار پورت ۵۱
۲-۱۱-۲- پروکسی [illegible] اکس ۵۲
۲-۱۱-۲-۱- [illegible] ای ساده ۵۴
۲-۱۱-۲-۲- ترافیک د [illegible] ایت شده پروکسی ۵۴
۲-۱۱-۲-۳- مزایای یک پروکسی SOCKS ۵۷
۲-۱۱-۲-۴- معایب یک پروکسی SOCKS ۵۷
۲-۱۱-۳- پروکسی های HTTP ۵۷
۲-۱۱-۳-۱- فوروارد یک پروکسی HTTP ۵۸
۲-۱۱-۳-۲- اجرای ساده ۶۰
۲-۱۱-۳-۳- ترافیک هدایت شده به پروکسی ۶۱
۲-۱۱-۳-۴- مزایای یک پروکسی HTTP فوروارد ۶۱
۲-۱۱-۳-۵- معایب یک پروکسی HTTP فوروارد ۶۱
۲-۱۱-۴- پروکسی HTTP معکوس ۶۲
۲-۱۱-۴-۱- اجرای ساده ۶۳
۲-۱۱-۴-۲- ترافیک هدایت شده به پروکسی شما ۶۴
۲-۱۱-۴-۳- مزایای یک پروکسی HTTP معکوس ۶۵

۲-۱۱-۴-۴- معایب یک پروکسی HTTP معکوس ۶۶
۲-۱۲- جمع بندی فصل ۶۶

فصل سوم: ساختارهای پروتکل شبکه

۳-۱- مقدمه ۶۸
۳-۲- ساختارهای پروتکل دودویی ۶۸
۳-۲-۱- داده‌های عددی ۶۹
۳-۲-۲- اعداد صحیح بدون علامت ۶۹
۳-۲-۳- اعداد صحیح امضا شده ۷۰
۳-۲-۴- طول متغیر اعداد صحیح ۷۱
۳-۲-۵- داده های آرایش شده ۷۲
۳-۲-۶- داده های بولین ۷۳
۳-۲-۷- پرچم بیتی ۷۴
۳-۲-۸- دودویی Endian ۷۴
۳-۲-۹- متن و داده های انسانی قابل خواندن ۷۵
۳-۲-۹-۱- صفحات کد ۷۷
۳-۲-۹-۲- کاراکترهای مولتی بایت Set شده ۷۷
۳-۲-۱۰- استاندارد یونی کُد ۷۷
۳-۲-۱۱- اطلاعات طول دودویی متغییر ۸۰
۳-۲-۱۲- داده های Padded ۸۳
۳-۲-۱۳- داده ها و زمان ها ۸۴
۳-۳- برچسب، طول و الگوی ارزش ۸۵
۳-۴- مولتی پلکسینگ و تقسیم بندی ۸۶

۳-۵- اطلاعات نشانی شبکه ۸۷
۳-۶- فرمت های زیرساخت باینری ۸۸
۳-۶-۱- ساختارهای پروتکل متن ۸۹
۳-۶-۲- داده‌های Numeric ۹۰
۳-۶-۳- مقادیر integer ۹۰
۳-۶-۴- مقادیر Decimal ۹۰
۳-۶-۵- متن Boolean ۹۱
۳-۶-۶- تاریخ و زمان ۹۱
۳-۷- داده‌های طولا متغیر ۹۱
۳-۷-۱- متن محدود شده ۹۱
۳-۷-۲- متن ترمینال ۹۲
۳-۷-۳- ساختاربندی فرمتهای متن ۹۲
۳-۷-۴- ضمیمه های Mail اینترنتی چند هدفه ۹۳
۳-۷-۵- نماد شی جاوا اسکریپت ۹۴
۳-۷-۶- زبان نشانه گذاری قابل گسترش ۹۵
۳-۸- کدگذاری داده‌های دودویی ۹۵
۳-۸-۱- کدگذاری Hex ۹۶
۳-۸-۲- کدگذاری Base64 ..... ۹۷
۳-۹- جمع بندی فصل ۹۹
فصل چهارم: برنامه کاربردی ضبط ترافیک پیشرفته
۴-۱- مقدمه ۱۰۱
۴-۲- ترافیک مسیریابی ۱۰۱

۴-۳- استفاده از traceroute ۱۰۲
۴-۴- جداول مسیریابی ۱۰۳
۴-۵- پیکربندی کردن یک روتر ۱۰۴
۴-۵-۱- فعالسازی مسیریابی در ویندوز ۱۰۵
۴-۵-۲- فعالسازی مسیریابی در *nix ۱۰۵
۴-۵-۳- ترجمه نشانی شبکه ۱۰۶
۴-۵-۳-۱- فعال سازی SNAT ۱۰۶
۴-۵-۳-۲- پیکربندی SNAT در لینوکس ۱۰۸
۴-۵-۳-۳- فعالسازی DNAT ۱۰۸
۴-۶- فوروارد ترافیک بین دو واره ۱۱۰
۴-۶-۱- اِسپوفینگ DHCP ۱۱۱
۴-۶-۲- اساس ARP ۱۱۴
۴-۷- جمع بندی فصل ۱۱۸

فصل پنجم: تحلیل از سیم WIRE

۵-۱- مقدمه ۱۲۱
۵-۲- برنامه تولید ترافیک(Super Funky Chat) ۱۲۱
۵-۳- شروع سرور Server ۱۲۲
۵-۴- شروع مشتری Client ۱۲۲
۵-۵- ارتباط بین مشتریان ۱۲۳
۵-۵-۱- یک دوره Crash در تحلیل با Wireshark ۱۲۴
۵-۵-۲- تولید ترافیک شبکه و کپچر بسته ها ۱۲۵
۵-۶- تحلیل پایه ۱۲۷

۵-۶-۱- خواندن محتویات یک نشست TCP ۱۲۷
۵-۶-۲- شناسایی ساختار بسته با Hex Dump ۱۲۹
۵-۶-۳- نمایش بسته های فردی ۱۳۰
۵-۶-۴- تعیین ساختار پروتکل ۱۳۱
۵-۶-۴-۱- آزمایش فرضیات ۱۳۳
۵-۶-۴-۲- رد کردن پروتکل با پایتون ۱۳۴
۵-۶-۴-۳- انجام تبدیل دودویی ۱۳۴
۵-۶-۴-۴- رسیدگی به داده های ورودی ۱۳۶
۵-۶-۴-۵- فاری ر بخش‌های ناشناخته پروتکل ۱۳۷
۵-۶-۵- محاسبات Checksu ۱۳۷
۵-۶-۵-۱- کشف یک مقدار برچسب ۱۳۸
۵-۷- توسعه Wireshark در Lua ۱۴۱
۵-۷-۱- ایجاد دیسکتور ۱۴۴
۵-۷-۲- تشریح LUA ۱۴۵
۵-۷-۳- تجزیه بسته بندی پیام ۱۴۶
۵-۷-۴- استفاده از یک پروکسی برای تجزیه و تحلیل ترافیک ۱۴۹
۵-۸- برپاسازی پروکسی ۱۵۰
۵-۸-۱- تحلیل پروتکل با استفاده از یک پروکسی ۱۵۳
۵-۸-۲- اضافه کردن تجزیه کننده پروتکل پایه ۱۵۴
۵-۸-۳- تغییر رفتار پروتکل ۱۵۶
۵-۹- جمع بندی فصل ۱۵۸

فصل ششم: برنامه کاربردی مهندسی معکوس

۶-۱- مقدمه ۱۶۰

۶-۲-کامپایلر، مترجمان و اِسمبلر ۱۶۱

۶-۲-۱-زبان های تفسیری ۱۶۱

۶-۲-۲-زبان های کامپایل شده ۱۶۲

۶-۲-۳-پیوند ایستا در مقابل پیوند پویا ۱۶۳

۶-۲-۴-معماری X86 ..... ۱۶۳

۶-۳- مجموعه دستورالعمل معماری ۱۶۴

۶-۳-۱- ریجستر CPU ۱۶۵

۶-۳-۱-۱- ثبت اهداف عمومی ۱۶۶

۶-۳-۱-۲- فهرست شاخص حافظه ۱۶۷

۶-۳-۱-۳- ریجستر انتخاب کننده ۱۶۸

۶-۴- جریان برنامه ۱۶۹

۶-۵- اصول سیستم‌عامل ۱۷۰

۶-۵-۱- فرمت فایل قابل اجرا ۱۷۰

۶-۵-۲- مقطع ۱۷۱

۶-۵-۳- فرآیندها و تهدیدات ۱۷۲

۶-۵-۴- واسط شبکه سیستم‌عامل ۱۷۳

۶-۵-۴-۱- ایجاد یک اتصال کارگیر ساده TCP به یک سرور ۱۷۳

۶-۵-۴-۲- ایجاد یک اتصال مشتری ساده به TCP یک سرور ۱۷۵

۶-۶- واسط دودویی برنامه کاربردی ۱۷۶

۶-۶-۱- مهندسی معکوس ایستاء ۱۷۷

۶-۶-۲- راهنمای سریع استفاده از نسخه رایگان ۱۷۸
۶-۶-۳- تحلیل متغیرهای پشته و استدلال‌ها ۱۸۳
۶-۶-۴- شناسایی کارکرد کلیدی ۱۸۴
۶-۶-۴-۱- استخراج اطلاعات نمادی ۱۸۴
۶-۶-۴-۲- مشاهده کتابخانه‌های وارد شده ۱۸۸
۶-۶-۴-۳- تحلیل رشته ها ۱۸۹
۶-۶-۴-۴- شناسایی کد خودکار ۱۸۹
۶-۶-۵- مهندسی معکوس پویا ۱۹۲
۶-۶-۶- تنظیمات Breakpoint ۱۹۲
۶-۷- اشکال زدایی ویندوز ۱۹۳
۶-۷-۱- پنجره EIP ۱۹۳
۶-۷-۲- پنجره ESP ۱۹۴
۶-۸- وضعیت ثبت اهداف عمومی ۱۹۴
۶-۸-۱- مکان مناسب برای Breakpoint ۱۹۵
۶-۸-۲- مهندسی معکوس مدیریت زبان ها ۱۹۵
۶-۸-۳- برنامه کاربردی دات NET ۱۹۶
۶-۸-۴- استفاده از ILSpy ۱۹۷
۶-۸-۵- برنامه های جاوا ۲۰۱
۶-۸-۶- برخورد با انسداد ۲۰۳
۶-۸-۷- منابع مهندسی معکوس ۲۰۵
۶-۹-جمع بندی فصل ۲۰۵

فصل هفتم: امنیت پروتکل شبکه

۷-۱- مقدمه ۲۰۸

۷-۲- الگوریتم‌های رمزنگاری ۲۰۹

۷-۲-۱- رمز های جانشین شده ۲۱۰

۷-۲-۲- رمزنگاری XOR ۲۱۱

۷-۲-۳- تولیدکننده اعداد تصادفی ۲۱۳

۷-۲-۴- رمزنگاری کلید متقارن ۲۱۴

۷-۲-۴-۱- مسدودسازی رمزها ۲۱۴

۷-۲-۴-۲- DES سه‌گانه ۲۱۶

۷-۲-۴-۳- مسدود کننده‌های دیگر بلوک ۲۱۸

۷-۳- مدل های مسدود سازی رمز ۲۱۸

۷-۳-۱- دفترچه کد الکترونیکی ۲۱۹

۷-۳-۲- زنجیره بلوکی رمز گذاری ۲۱۹

۷-۳-۳- حالت‌های جایگزین ۲۲۰

۷-۴- مسدود کردن شناسه رمز ۲۲۱

۷-۴-۱- حمله اوراکلِ پَد ۲۲۲

۷-۴-۲- رمزگذاری جریان ۲۲۶

۷-۴-۳- رمزنگاری کلید نامتقارن ۲۲۷

۷-۴-۳-۱- الگوریتمRSA ۲۲۸

۷-۴-۳-۲- پَد شدن RSA ۲۳۰

۷-۴-۳-۳- تبادل کلید با دیفی هلمن ۲۳۱

۷-۴-۴- الگوریتم های امضاء ۲۳۳

۷-۴-۴-۱- الگوریتم‌های هشینگ ۲۳۳
۷-۴-۴-۲- الگوریتم‌های امضای نامتقارن ۲۳۴
۷-۴-۵- کدهای تصدیق پیغام ۲۳۵
۷-۴-۵-۱- طول گسترش و حمله تصادم ۲۳۶
۷-۴-۵-۲- کدهای تأیید هویت پیام هَش ۲۳۸
۷-۴-۵-۳- زیرساخت کلید عمومی ۲۳۹
۷-۴-۶- گواهینامه X.509 ..... ۲۴۰
۷-۴-۶-۵- ایجاد یک زنجیره گواهی ۲۴۲
۷-۵- مطالعه موردی (امنیت لایه انتقال) ۲۴۳
۷-۵-۱- مفهوم TLS Handshake ۲۴۴
۷-۵-۲- مذاکره اولیه ۲۴۵
۷-۵-۳- تأیید هویت Endpoint ۲۴۶
۷-۵-۴- ایجاد رمزنگاری ۲۴۸
۷-۵-۵- الزامات امنیتی جلسه ۲۴۹
۷-۶- جمع بندی فصل ۲۵۱

فصل هشتم: پیاده‌سازی پروتکل شبکه

۸-۱- مقدمه ۲۵۴
۸-۲- پاسخ مجدد به ترافیک شبکه ضبط شده ۲۵۴
۸-۲-۱- دستیابی به ترافیک با Netcat ۲۵۴
۸-۲-۲- استفاده از پایتون برای Resend کردن ترافیک UDP ۲۵۷
۸-۲-۳- تکرار پروکسی تجزیه و تحلیل ما ۲۵۹
۸-۲-۴- دستیابی به مثال ترافیک ۲۵۹

۸-۳- پیاده سازی یک مشتری شبکه ساده ۲۶۰
۸-۳-۱- اجرای یک سرور ساده ۲۶۲
۸-۳-۲- بازپسگیری کد اجرایی موجود ۲۶۴
۸-۳-۳- کد بازپسگیری در برنامه کاربردی دات نِت ۲۶۶
۸-۴- استفاده از API های بازتاب ۲۶۷
۸-۴-۱- بارکردن اِسمبلی ۲۶۸
۸-۴-۲- تکرار کد در برنامه های Java ۲۷۲
۸-۴-۳- اجرای غیرقابل کنترل ۲۷۴
۸-۴-۴- تماس با کتابخانه ها بدا ۲۷۴
۸-۴-۵- بار کردن یک کتابخانه با پایت ۲۷۵
۸-۴-۶- تماس با وظایف پیچیده بیشتر ۲۷۶
۸-۵- فراخوانی تابع با یک پارامتر ساختار ۲۷۸
۸-۵-۱- خواندن توابع با پایتون در (مایکروسافت) ۲۷۸
۸-۵-۲- رمزنگاری و برخورد با TLS ۲۷۹
۸-۵-۳- یادگیری درباره رمزنگاری مورد استفاده ۲۷۹
۸-۶- باز کردن ترافیک TLS ۲۸۱
۸-۶-۱- اجبار TLS1.2 ..... ۲۸۲
۸-۶-۲- جایگزینی گواهی با خودتان ۲۸۳
۸-۷- جمع بندی فصل ۲۸۷
فصل نهم: علل ریشه‌ای آسیب‌پذیری
۹-۱- مقدمه ۲۸۹
۹-۲- کلاس های آسیب پذیری ۲۸۹

۹-۲-۱- اجرای کد راه دور ۲۹۰
۹-۲-۲- انکار سرویس ۲۹۰
۹-۲-۳- اِفشاگری اطلاعات ۲۹۱
۹-۲-۴- گذرگاه تأیید هویت ۲۹۱
۹-۲-۵- گذرگاه اجازه ۲۹۲
۹-۳- آسیب پذیری فساد در حافظه ۲۹۳
۹-۳-۱- زبان برنامه نویسی حافظه ایمن در برابر حافظه غیر ایمن ۲۹۳
۹-۳-۲- سرریز بافر حافظه ۲۹۴
۹-۳-۲-۱- سرریز بافر با طول ثابت ۲۹۵
۹-۳-۲-۲- سرریز بافر با طول متغیر ۲۹۸
۹-۴- سرریز صحیح ۲۹۹
۹-۴-۱- شاخص بافر خارج از باند ۳۰۰
۹-۴-۲- حمله گسترش داده ۳۰۲
۹-۴-۳- تخصیص حافظه خطای پویا ۳۰۳
۹-۴-۴- پیش فرض یا اعتبار هارد کُد گذاری شده ۳۰۳
۹-۴-۵- شمارش کاربر ۳۰۴
۹-۴-۶- دسترسی به منابع نادرست ۳۰۵
۹-۴-۷- کانونی سازی ۳۰۶
۹-۴-۸- خطای لفظ ۳۰۸
۹-۵- حملات خستگی حافظه ۳۰۹
۹-۵-۱- ذخیره حملات در حال حمله ۳۱۰
۹-۵-۲- حملات خستگی CPU ۳۱۱

۹-۵-۳- پیچیدگی الگوریتم ۳۱۱
۹-۵-۴- رمزنگاری قابل تنظیم ۳۱۳
۹-۵-۵- قالب بندی رشته آسیب پذیری ۳۱۵
۹-۶- تزریق فرمان ۳۱۶
۹-۶-۱- تزریق SQL ۳۱۷
۹-۶-۲- جایگزینی کدگذاری متن ۳۱۸
۹-۷- جمع بندی فصل ۳۲۰

فصل دهم: شناسایی و بهره‌برداری از آسیب‌پذیری‌های امنیتی

۱۰-۱- مقدمه ۳۲۳
۱۰-۲- آزمایش فازی ۳۲۳
۱۰-۳- آزمایش ساده فازی ۳۲۴
۱۰-۳-۱- جهش فازی ۳۲۵
۱۰-۳-۲- ایجاد موارد تست ۳۲۶
۱۰-۳-۳- پیگیری آسیب پذیری ۳۲۶
۱۰-۳-۴- برنامه های کاربردی اشکال زدایی ۳۲۷
۱۰-۳-۴-۱- آغاز اشکال زدایی ۳۲۷
۱۰-۳-۴-۲- تحلیل Crash ۳۲۹
۱۰-۳-۴-۳- مثال Crash ۳۳۲
۱۰-۳-۵- بهبود شانس خود برای پیدا کردن علت ریشه‌ای یک Crash ۳۳۵
۱۰-۳-۵-۱- بازسازی برنامه‌ها با نشانی اینترنتی ۳۳۶
۱۰-۳-۵-۲- پنجره‌های Debug ویندوز و صفحه Heap ۳۳۸
۱۰-۳-۵-۳- بهره‌برداری از منابع مشترک ۳۳۹

۱۰-۳-۵-۴- سو استفاده از آسیب پذیری فساد حافظه ۳۴۰
۱۰-۳-۵-۵-پشته سرریز بافر ۳۴۰
۱۰-۴- سرریز Heap بافر ۳۴۲
۱۰-۴-۱- آسیب پذیری Use-After-Free ۳۴۴
۱۰-۴-۲- تغییر چیدمان لایه بندی Heap ۳۴۵
۱۰-۴-۳- تخصیص مخزنِ حافظه تعریف شده ۳۴۸
۱۰-۴-۴- ذخیره حافظه Heap ۳۴۹
۱۰-۵- نوشتن آسیب پذیری حافظه دلخواه ۳۴۹
۱۰-۵- سو استفاده از نوشتن پرونده های ممتاز ۳۵۱
۱۰-۵-۱- سوء استفاده از نوشتن پرونده های دارای امتیاز کم ۳۵۲
۱۰-۵-۲- نوشتن کد پوسته ۳۵۳
۱۰-۵-۳- تکنیک ساده Debug ۳۵۶
۱۰-۵-۴- فراخوانی سیستم تماس‌ها ۳۵۷
۱۰-۵-۵- فراخوانی سیستم با کالینگ ۳۵۸
۱۰-۶- فراخوانی سیستم نوشتاری ۳۶۰
۱۰-۶-۱- دسترسی نشانی نسبی در سیستم های ۳۲ و ۶۴ بیتی ۳۶۲
۱۰-۶-۲- تنظیم برنامه‌های دیگر ۳۶۳
۱۰-۶-۳- ایجاد کد پوسته با Metasploit ۳۶۴
۱۰-۶-۴- دسترسی به مبلغ پرداختی Metasploit ۳۶۵
۱۰-۶-۵- ایجاد یک پوسته معکوس ۳۶۵
۱۰-۶-۶- اجرای payload ۳۶۶
۱۰-۷- به فراموشی سپردن فساد ۳۶۶

۱۰-۷-۱- پیشگیری از اجرای داده ۳۶۷
۱۰-۷-۲- شمارنده برنامه‌سازی بازگشتی ۳۶۹
۱۰-۷-۳- چیدمان فضای نشانیASLR ۳۷۲
۱۰-۷-۴- ذخیره اطلاعات حافظه ۳۷۲
۱۰-۷-۵- بهره‌برداری از منابع اجرایی ASLR ۳۷۴
۱۰-۷-۶- دور زدن ASLR با استفاده از سرریز نوشتار جزئی ۳۷۵
۱۰-۷-۷- تشخیص سرریزهای پشته با کناری حافظه ۳۷۶
۱۰-۸- دور زدن canary ها با فاسد کردن متغیرهای محلی ۳۷۷
۱۰-۸-۱- دور زدن canary ها با پشته بافر پاریز ۳۷۸
۱۰-۹- جمع بندی فصل ۳۸۰
منابع ۳۸۱