

بسمه تعالی

تمرین ۱: آشنایی با ابزار Cain & Abel

این ابزار امکان کرک کردن پسوندها به دو شیوه جستجوی تمام فضای حالت (بروت فورس) و حمله پسوندهای رایج (دیکشنری) به شما میدهد. محیط آزمایشگاه را به نحوی طراحی کنید که بر روی یک سیستم اکانت‌های متعددی باشد، سپس هر دو نوع حمله را بر روی این دو اکانت اجرا کنید تا پسورد سایر حساب‌های کاربری به شما نمایش داده شود.

گزارش کاملی از نحوه‌ی عملکرد این ابزار برای کرک کردن پسوندها آماده کنید. (این ابزار کاربردهای دیگری نیز دارد، تمرکز این تمرین صرفاً بر روی کرک کردن پسوندهاست).

تمرین ۲: نفوذ از طریق متاسپلویت

مطابق آنچه در کلاس توضیح داده شد، آزمایشگاهی طراحی کنید که در آن نفوذگر از طریق سیستم عامل کالی لینوکس، قصد حمله به یک هدف با ویندوز XP را دارد. برای این حمله از اکسپلویت ms08_067 و پیلود windows/meterpreter استفاده کنید. دقت کنید وصله امنیتی این اکسپلویت بر روی ویندوز نصب نشده باشد و اگر شده است آن را پاک کنید.

پس از گرفتن دسترسی meterpreter بر روی سیستم هدف، اقدام به راه اندازی keylogger از طریق سیستم کالی لینوکس کنید. شماره دانشجویی خود را در سیستم XP وارد کرده و آن را در سمت کالی لینوکس شنود کنید. از تمام مراحل کار خود عکس گرفته و به همراه توضیحات در گزارش کار مربوط به این تمرین بیاورید.

قسمت امتیازی

تمرین ۳: نفوذ به گوشی‌های اندروید به وسیله ابزار Evil_Droid

برای طراحی محیط آزمایشگاه ابتدا ابزار Evil_Droid را بر روی کالی لینوکس خود نصب کنید. پس از آن سیستم خود را به نحوی طراحی کنید که یک دستگاه اندرویدی نیز در آن وجود داشته باشد؛ برای این کار میتوانید یک شبکه طراحی کنید که دستگاه اندرویدی حقیقی در آن وجود داشته باشد و یا یک ماشین مجازی

اندروید بر روی سیستم خود نصب کنید. پس آن به وسیله ابزار ذکر شده، یک فایل apk را آلوده به یک بدافزار کنید و آن را در پوشه var/html قرار داده و وب سرویس ماشین مجازی خود را راه اندازی کنید. سپس از طریق مرورگر و وارد کردن آی پی کالی لینوکس در سیستم اندروید نرم افزار آلوده شده را بر روی سیستم خود ذخیره کنید؛ دسترسی meterpreter را نشان دهید و بگویید هم اکنون نفوذگر میتواند چه اقداماتی را انجام دهد.