هوالحق

تمرین کامپیوتری شماره ۳

مبانی امنیت شبکه، پاییز ۹۹

هدف از این تمرین، استثمار مرورگر[1] در بستر یک شبکه محلی است. ابزار مورد استفاده، فریم‌ورک BeEF که در توزیع Kali الحاق شده است می‌باشد. این ابزار تحت زبان Ruby توسعه داده شده است، فلذا برپاسازی آن بر روی سیستم عامل‌های غیر از لینوکس به راحتی امکان پذیر نبوده و یا غیر ممکن می‌باشد.

برای انجام این تمرین پیشنهاد می‌گردد که **دو ماشین مجازی**[2]، یکی سیستم‌عامل حمله‌کننده (**Kali**) و دیگری سیستم‌عامل قربانی (**Windows 7**)، بر روی یک بستر مجازی‌سازی مانند Virtual Box معماری گردد. این دو ماشین می‌بایست از طریق یک شبکه محلی مجازی با هم در ارتباط باشند. برای این مقصود، پیشنهاد می‌گردد که از ساده‌ترین معماری شبکه مجازی با نام **NAT Network** بر روی Virtual Box استفاده گردد. در این حالت، ماشین‌های مجازی درون یک شبکه‌ی محلی مجازی NAT قرار گرفته و هر دو در یک رنج قابل مشاهده طرفین IP می‌پذیرند. دقت داشته باشید که این مُد ارتباطی با NAT عادی در Virtual Box متفاوت است.

در ادامه، با مطالعه مطالب، مقالات و آموزش‌های متنوع موجود در سطح اینترنت، به استثمار مرورگر IE پیش‌فرض موجود در سیستم‌عامل Windows 7 قربانی از طریق سیستم عامل Kali حمله کننده اقدام نمایید. هدف ازین تمرین، کارکرد با واسط وب فریم‌ورک BeEF مد نظر است و نیازی به کارکرد با واسط کنسول آن نمی‌باشد. پس از طی پروسه‌ی مربوطه و برپاسازی سناریو به صورت کامل، در قالب یک گزارش به سؤالات زیر پاسخ داده و مواد مورد نظر را تأمین کنید:

۱) **یک روش مؤثر برای به دام‌اندازی مرورگر قربانی را ارائه کنید.** این راهکار می‌تواند در قالب یک سناریوی مهندسی اجتماعی (با فرض هوشمند بودن نسبی قربانی) و یا یک روش نفوذپذیری باشد. دقت کنید که روش پیشنهادی باید به صورت واضح نحوه‌ی تزریق فایل hook.js مشخص را به مرورگر قربانی مشخص کند و کاملاً عملیاتی و قابل اجرا باشد.

۲) آخرین نسخه‌ی مرورگر Google Chrome را بر روی سیستم عامل قربانی نصب کنید. علاوه بر مرورگر IE سیستم قربانی، این مرورگر را نیز به دام بیندازید. **۳ نمونه از امکانات بخش Commands از واسط BeEF را ذکر کنید که در مرورگر Chrome نصب شده اجرایی نیست**، ولی در مرورگر IE پیشفرض این سیستم عامل اجرا می‌گردند. این ۳ نمونه را با ذکر نام دسته، نام و عملکرد مربوطه مشخص کنید.

---

[1] Browser Exploitation
[2] Virtual Machine

هوالحق

تمرین کامپیوتری شماره ۳

مبانی امنیت شبکه، پاییز ۹۹

۳) **۳ نمونه از جذاب‌ترین حملات ممکن تحت BeEF در نظر شخصی خود را از لیست Commands که بر مرورگر IE سیستم قربانی کارگر هستند را ذکر کنید.** این ۳ نمونه می‌بایست با ذکر دسته، نام، توضیح عملکرد مربوطه و همچنین تصاویر (اسکرین‌شات) مربوط به عملکرد هر یک (شامل نتایج برگشتی و یا عملکرد روی مرورگر قربانی) باشد. تصاویر مربوطه می‌بایست به صورت واضح بیان کننده موفقیت‌آمیز بودن حملات توسط شما، چه در سیستم حمله کننده و چه سیستم قربانی، باشد.

۴) **یک سناریوی حمله Google Phishing را به صورت کامل بر روی سیستم قربانی اعمال نمایید.** نتایج را در قالب توضیحات مختصر و تصاویر ذکر نمایید. دقت کنید که به عنوان نام کاربری، «**نام خود**» را در فیلد صفحه جعلی باز شده در سیستم قربانی وارد کنید. بدیهیست که در قالب تصاویر تهیه شده، این نام می‌بایست در نتایج برگشتی به واسط وب BeEF مشخص باشد.

۵) **یک تصویر از بخش Logs که در آن «ستون تاریخ و زمان» حملات اخیر به صورت واضح مشخص باشد را ارائه کنید.** تنها زمان حملات مد نظر است، نیازی به نمایش تمامی حملات انجام شده در این تصویر نمی‌باشد.

۶) **در صورتی که بخواهیم این سناریو را بر روی بستر وب (نه شبکه محلی) پیاده‌سازی کنیم، چه راه حلی را ارائه می‌کنید؟** پاسخ خود را با فرض امکانات در دسترس (یک کامپیوتر متصل به اینترنت با آدرس IP داینامیک و بدون دامنه و تنها با شناخت آدرس IP فرد قربانی) شرح دهید.

نکات:

- پیشنهادات ارائه شده برای برپاسازی محیط اجرای تمرین، راحت‌ترین و سریع‌ترین روش ممکن برای اجرای سناریوهای مورد نظر است.
- پاسخ‌های خود را در قالب یک فایل PDF یکتا (فقط) با نام شماره دانشجویی خود ارائه کنید. داخل این فایل، به صورت کاملاً مجزا می‌بایست هر یک از پاسخ‌های مربوط به ۶ سؤال مطرح شده قابل تشخیص باشد. خارج از پاسخ این ۶ سؤال نیازی به ارائه توضیحات بیشتر نیست.
- هدف نهایی از گزارش، تشخیص پیاده‌سازی کامل و درست سناریوها توسط **خود** شماست. فلذا حجم توضیحات و تعداد عکس‌های خود را با این هدف تنظیم نمایید.
- گزارش شما باید لازم و در عین حال کافی باشد. تعداد صفحات یک گزارش کیفیت آن را تعیین نخواهد کرد.