بسمه تعالی

تمرین عملی دوم

۱. **شنود با وایرشارک:**

یک نسخه پایدار از نرم افزار وایر شارک را از آدرس wireshark.org دانلود کنید .پس از دانلود و نصب نرم افزار را باز کنید و از بخش Capture بر روی List Interface کلیک کنید و کانکشن مربوطه را انتخاب کنید سپس بر روی دکمه استارت کلیک کنید تا شنود بسته ها آغاز شود Capture start/stop . اگر خارج از محل کار این فعالیت را آزمون میکنید میتوانید کامپیوترتان را در حالت spot hot قرار دهید و از روی موبایل نرم افزار تلگرام را اجرا کنید .می توانید بر روی بسته ها کلیک کنید تا جزئیات آن را مشاهده کنید و آن را آنالیز کنید. آنچه لازم است در پاسخ به این تمرین آماده کنید عبارت است از:

- شرح پروتکل های مورد استفاده و تحلیل ترافیک بطور کلی (به همراه تصاویر مربوطه)
- کامپیوتر خود را در حالت access point یا hotspot قرار دهید و از موبایلتان نرم افزار مربوط به یک پیام رسان مثال سروش را اجرا کنید . برای مدت زمانی ترافیک را کپچر کنید و خروجی را تحلیل کنید.
- کاربری ابزارهای مانیتورینگ و لزوم استفاده از آن برای ادمین های شبکه را در یک سازمان با کسب و کار خاص تشریح کنید و اهمیت تحلیل ترافیک شبکه و مسئولیت ادمین شبکه در آن سازمان را تحلیل کنید.(برای این کار سعی کنید تحلیل شخصی خودتان را در استفاده از این راهبرد برای مدیران فناوری اطلاعات بنویسید و از آوردن تعاریف کلیشه‌ای موجود در صفحات وب بهتر است خودداری کنید.)
- به آدرس زیر بروید و فایل ftpv6-1 را دانلود کنید. بسته های FTP را به وسیله قابلیت های وایر شارک جدا کرده (فیلتر کنید) در یکی از این بسته ها USERNAME و PASSWORDقربانی حمله مشخص شده است،آن را ثبت کنید .نام کاربری و رمز عبور را در قالب یک تصویر نمایش دهید. https://wiki.wireshark.org/SampleCaptures

۲. **فیشینگ:**

- با استفاده از ابزار fsociety اقدام به طراحی یک صفحه برای حمله فیشینگ بر روی محیط لوکال خود کنید. سپس توسط یک سیستم‌عامل دیگر (در محیط مجازی) اقدام به باز کردن این صفحه و وارد کردن اطلاعات کنید. اطلاعات دریافتی توسط نفوذگر را در یک عکس نمایش دهید. صفحه انتخابی برای حمله فیشینگ میتواند صفحات معروفی همچون صفحات مربوط به بانک‌ها، اینستاگرام و... باشد، مراحل انجام این کار عبارتند از ساخت یک صفحه جعلی دلخواه، راه اندازی وب سرور، و وارد شدن به صفحه جعلی توسط مرورگر موجود در سیستم عامل قربانی، وارد کردن اطلاعات، و نهایتا شنود اطلاعات توسط نفوذگر. (از تمام مراحل ذکر شده عکس بگیرید و گزارش کاملی از آنچه انجام داده‌اید تهیه کنید.) (از انجام این تمرین به جز در محیط لوکال خودداری کنید.)

- به نظر شما از چه راهکارهایی میتوان برای جلوگیری از انجام حملات فیشینگ برای حساب‌های بانکی استفاده کرد؟