به نام خدا

دانشکده مهندسی کامپیوتر

تمرین عملی چهارمِ پروژه تست نفوذ، درس مبانی امنیت اطلاعات

دکتر حمیدرضا شهریاری

دی ۱۴۰۰

نکات مهم

۱. **کد:** استفاده از کتابخانه‌های رایج در محدوده هک و امنیت در زبان پایتون مجاز است.

۲. **گزارش:** ملاک اصلی انجام پروژه و گزارش آن است و ارسال کد بدون گزارش فاقد ارزش است. لذا می‌بایست یک فایل گزارش با فرمت pdf تهیه کنید و در آن برای هر قسمت از فعالیت صورت گرفته درباره تمرین، تصاویر اسکرین شات، تصاویر خروجی مربوطه و همچنین توضیحات مربوط به آن‌ها را ذکر کنید. سعی کنید تا حدامکان توضیحات کامل و جامعی تدوین کنید.

۳. **تذکر:** مطابق قوانین دانشگاه، هر نوع کپی برداری و اشتراک کار دانشجویان غیرمجاز بوده و **نمره هر دو نفر منفی** لحاظ خواهد شد.

۴. **راهنمایی ۱:** می‌توانید برای سهولت و راه‌اندازی آزمایشگاه خود، از vmware و نصب ویندوز و یا نسخه مناسب لینوکس بر روی ماشین مجازی استفاده کنید.

۵. **راهنمایی ۲:** در صورت نیاز می‌توانید سوالات خود را در خصوص انجام پروژه، از طریق راه‌های ارتباطی زیر از تدریس‌یار بپرسید:

آدرس ایمیل: mahmood.faraji133@gmail.com

شناسه تلگرام: @mr_faraji1997

لطفا در صورت ارسال ایمیل عنوان آن را Information_Sec قراردهید.

۶. **ارسال:** فایل گزارش به همراه کدهای نوشته شده را در قالب یک فایل فشرده (zip) همانند فرمت زیر در سامانه بارگذاری نمایید: Prj4_StudentNumber.zip

۳ روز تاخیر در ارسال گزارش و فایل نهایی، موجب کسر ۳۰ درصد از نمره به ازای هر روز می‌شود و پس از ۳ روز، امکان بارگذاری وجود نخواهد داشت.

سیستم هکینگ

✓ تعریف تمرین

این تمرین در سه بخش قابل انجام است.

در این تمرین می‌خواهیم با استفاده از یک malware یکسری اطلاعات را از سیستم قربانی دریافت کنیم. برای اینکار نیاز است تا یک سرور لوکال راه‌اندازی کرده و با نوشتن یک reverse malware، اطلاعات مورد نیاز مهاجم را برایش ارسال کنیم.

*malware : بدافزار، هر نوع نرم‌افزاری است که از روی عمد برای آسیب‌زدن به رایانه، سرور و یا شبکه رایانه‌ای طراحی شده است.

✓ قوانین تمرین – بخش اول

۱. ابتدا سعی کنید با استفاده از کتابخانه socket در زبان برنامه‌نویسی پایتون، یک سرور لوکال با نام server.py راه‌اندازی کنید.
۲. سپس یک بدافزار با نام malware.py ایجاد کرده و سعی کنید با کتابخانه socket آن را طوری برنامه‌نویسی کنید که به محض اجرا بتواند به سرور لوکالی که در مرحله اول ساخته‌اید متصل شود.
۳. با استفاده از پیغامی نشان دهید که دو مرحله فوق به درستی انجام شده است.

✓ قوانین تمرین – بخش دوم

۱. پس از انجام بخش اول، فایل malware.py را به گونه‌ای تغییر دهید تا به محض متصل شدن به سرور، اطلاعات مربوط به سیستم قربانی نظیر موارد زیر را به سمت سرور برگرداند:

```
Host Name:
OS Name:
OS Version:
OS Manufacturer:
OS Configuration:
OS Build Type:
Registered Owner:
Registered Organization:
Product ID:
Original Install Date:
System Boot Time:
System Manufacturer:
System Model:
System Type:
Processor(s):
```

```
BIOS Version:
Windows Directory:
System Directory:
Boot Device:
System Locale:
Input Locale:
Time Zone:
Total Physical Memory:
Available Physical Memory
Virtual Memory: Max Size:
Virtual Memory: Available
Virtual Memory: In Use:
Page File Location(s):
Domain:
Logon Server:
Hotfix(s):
```

✓ **قوانین تمرین – بخش سوم**

۱. در بخش آخر می‌بایست، فایل server.py و malware.py را به گونه‌ای تغییر دهید تا زمانی که اتصال بین سیستم قربانی و سرور مهاجم، به درستی برقرار شد، دو مورد زیر در آن‌ها امکان پذیر باشد:

- مهاجم بتواند با استفاده از وارد کردن دستور sysinfo اطلاعات سیستم قربانی را دریافت کند (دقیقا بر خلاف بخش دوم که فایل malware به محض اجرا شدن این اطلاعات را بصورت خودکار برای سرور می‌فرستاد)
- کانکشن ایجاد شده بین سرور و سیستم قربانی با وارد دستور فوق قطع نشود و این ارتباط تا زمانی که مهاجم می‌خواهد برقرار باشد.

نکته ۱: نیازی به طراحی یک User friendly interface نیست و اجرای هر دو فایل در محیط ترمینال کافیست اما اگر دانشجویی تمایل به طراحی UI مناسب داشت، نمره‌ی امتیازی برای او در نظر گرفته می‌شود.

نکته ۲: از تمامی مراحل انجام کار خود اسکرین‌شات گرفته و همراه با توضیحات، به فرمت گفته شده در بند "ارسال" قسمت نکات مهم در ابتدای این سند، در سامانه courses بارگذاری نمایید.

موفق باشید.