به نام خدا

دانشکده مهندسی کامپیوتر

تمرین عملی اولِ پروژه تست نفوذ، درس مبانی امنیت اطلاعات

دکتر حمیدرضا شهریاری

آبان ۱۴۰۰

نکات مهم

- **کد:** استفاده از کتابخانه‌های رایج در محدوده هک و امنیت در زبان پایتون مجاز است.
- **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.
- **تذکر:** مطابق قوانین دانشگاه، هر نوع کپی برداری و اشتراک کار دانشجویان غیرمجاز بوده و **نمره هر دو نفر منفی** لحاظ خواهد شد.
- **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.
- **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.
- **ارسال:** فایل گزارش به همراه کدهای نوشته شده را در قالب یک فایل فشرده (zip) همانند فرمت زیر در سامانه بارگذاری نمایید: Prj1_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.

جمع‌آوری اطلاعات و اسکن سامانه

✓ تعریف تمرین

فاز اول شامل دوبخش است:

۱. ابزارنویسی
۲. بررسی ابزارهای آماده

بخش اول، طراحی یک ابزاری برای جمع‌آوری اطلاعات و اسکن‌کردن برخی اطلاعات پیدا شده، بخش دوم شامل استفاده از ابزارهای آماده و آشنایی با نحوه کار آن‌ها می‌باشد.

لازم به ذکر است سامانه‌های یافت شده در محدوده آی‌پی گفته شده، قبلا مورد بررسی برای جمع‌آوری اطلاعات قرارگرفته‌اند و نتایج حاصل از فعالیت دانشجویان با آن‌ها مطابقت داده خواهد شد.

✓ قوانین تمرین – بخش اول

۱. طراحی و توسعه ابزار در بخش اول این تمرین، می‌بایست به زبان پایتون باشد و دانشجویان مجاز به استفاده از هر محیط برنامه‌نویسی پایتون همانند vscode، pycharm و ... و کتابخانه‌هایی نظیر nmap، scapy و ... هستند.

۲. ابزار طراحی شده می‌بایست شامل موارد زیر باشد:
   - گرفتن ping از آی پی خاص
   - اسکن یک محدوده آی‌پی و یافتن هاست‌های فعال
   - اسکن پورت‌های باز یک هاست فعال

۳. برای تست ابزار خود می‌توانید از رنج آی‌پی 89.43.0.0 الی 89.43.7.255 بعد از اتصال به VPN استفاده نمایید. استفاده از این آی‌پی صرفا جهت آموزش و حل تمرین مجاز است.

۴. ترجیحا خروجی موارد گفته شده در بند ۲ را در یک فایل با نام result_[ActionName].txt ذخیره نمایید. به عنوان مثال فایل کدپایتون مربوط به قسمت ping تمرین با نام ping.py و خروجی آن به فرمت result_ping.txt در فایل فشرده قرار گیرد.

۵. **نکته مهم:** هر کدام از سه قابلیت مطرح شده در بند ۲، می‌بایست با استفاده از کدنویسی انجام شود. به عنوان مثال گرفتن ping با استفاده از command prompt سیستم عامل، قابل قبول نیست و نمره‌ای به آن تعلق نخواهد گرفت.

✓ قوانین تمرین – بخش دوم

پس از انجام بخش اول تمرین، می‌بایست، با ابزارهای namp، netdiscover، hping3 صحت انجام کار خود را بررسی نمایید و پس از آن با استفاده از ابزارهای whatweb، httprint، xprube2 و یا سایت‌های آنلاین، اطلاعات بیشتری درباره هاست‌های فعالی که در محدوده آی‌پی گفته شده یافته‌اید، بدست آورید.

نکته۱: لازم به ذکر است اگر از سایت‌های آنلاین برای بدست آوردن اطلاعات اضافی استفاده می‌کنید، آدرس آن را در گزارش خود قید نمایید.

نکته۲: لازم است هنگام کار با ابزار nmap موارد زیر را در وارد کردن دستورات لحاظ فرمایید:

- TCP full scan
- Stealth scan
- UDP scan
- Fingerprint scan
- Idle scan

نکته۳: از تمامی مراحل انجام کار خود در بخش اول و دوم 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.

به عنوان نمونه یک تصویر از آنچه که مورد نظر است در بخش ابزارنویسی، در ادامه شرح داده می‌شود:

- قسمت ping می‌بایست هم با آی‌پی کار کند هم با نام دامنه و خروجی آن به صورت زیر می‌باشد:

```
Please Enter Your IP/Domain: www.google.com


Pinging www.google.com [216.58.212.228] with 32 bytes of data:

Reply from 216.58.212.228: bytes=32 time=128ms TTL=115



Ping statistics for 216.58.212.228:

    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 128ms, Maximum = 128ms, Average = 128ms
```

- خروجی اسکن محدوده آی‌پی و یافتن هاست های فعال:

```
Enter the Network Address: 89.43.3.0
Enter the Starting Number: 60
Enter the Last Number: 70
Scanning in Progress...
89.43.3.66 --> Live
89.43.3.67 --> Live
89.43.3.68 --> Live
89.43.3.69 --> Live
89.43.3.70 --> Live
scanning complete in  0:00:25.525210
```

- خروجی اسکن پورت های باز هاست های فعال:

```
        Enter the remote host IP to scan: 89.43.3.170
        Enter the start port number:   1
        Enter the last port number:    500
*************************************


 Mohit's Scanner is working on  89.43.3.170
*************************************
Port Open:-->    21
Port Open:-->    22
Port Open:-->    23
Port Open:-->    80
```

موفق باشید.