به نام خدا

دانشکده مهندسی کامپیوتر

تمرین عملی دومِ 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: Prj2_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، اسکن سامانه و آشنایی با آسیب‌پذیری‌ها

✓ تعریف تمرین

این تمرین شامل سه بخش است:

۱. ابزارنویسی
۲. بررسی ابزارهای آماده
۳. بررسی OWASP TOP 10

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 و بخش سوم آشنایی با آسیب‌پذیری‌های رایج در وب اپلیکیشن‌ها 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 در تمرین اول را در نظر بگیرید؛ در تمرین دوم نیاز است تا قابلیت شناسایی سرویس‌های اجرا شده بر روی پورت‌های باز را به ابزار خود اضافه کنید.

۳. برای تست ابزار خود می‌توانید از رنج‌های آی‌پی زیر استفاده نمایید:

لازم به ذکر است از هر رنج آی‌پی زیر دو الی چهار عدد هاست فعال با پورت های باز بررسی شود کافیست.

- 89.43.3.0 – 89.43.3.255
- 89.43.4.0 – 89.43.4.255

۴. ترجیحا خروجی موارد گفته شده در بند ۲ را در یک فایل با نام result_[ActionName].txt ذخیره نمایید.

۵. **امتیازی:** اگر دانشجویان بتوانند علاوه بر بدست آوردن سرویس‌های اجرا شده بر روی پورت‌های باز، نسخه سرویس استفاده شده را نیز با استفاده از ابزار خود بدست آورند، نمره بیشتری کسب خواهند کرد.

✓ **قوانین تمرین – بخش دوم**

۱. پس از انجام بخش اولِ تمرین، می‌بایست، با استفاده از ابزار nmap یا سایت‌های آنلاین، سرویس‌هایی را که بر روی پورت‌های باز هاست‌های فعال که در بخش اول همین تمرین با استفاده از ابزار خود بدست آورده‌اید را مورد تطابق قرار داده و صحت کار خود را بسنجید.

۲. نسخه SSL / TLS آدرس زیر را بدست آورده، Grade آن را مورد بررسی قرارداده و علت آسیب‌پذیر بودن این نسخه را تحقیق کنید.

راهنمایی: برای اینکار می‌توانید از ابزار nmap و یا سایت‌های آنلاین استفاده کنید.

اسکرین‌شات از خروجی ابزار و یا سایت آنلاین برای بدست آوردن نسخه و جزئیات SSL / TLS می‌بایست در گزارش آورده شود.

آدرس سایت: https://www.washingtonpost.com

۳. با استفاده از ابزار whois در کالی لینوکس و یا سایت آنلاین https://ipinfo.info/html/ip_checker.php دامنه sazkala.com و shahreketabonline.com را مورد بررسی قرار داده و اسکرین‌شات از نتایج بدست آمده را در گزارش خود قرار دهید و تحقیق کنید کدام از اطلاعات بدست آمده موجب آسیب‌پذیر شدن وبسایت های گفته شده می‌شود.

*دقت کنید، در دامنه‌های گفته شده لزوما اطلاعات مهمی وجود ندارد که موجب آسیب‌پذیر بودن وبسایت شود و هدف از انجام این قسمت از تمرین این است که دانشجویان علاوه بر آشنایی با ابزار گفته شده، تحقیق نمایند، کدام اطلاعات باید و کدام اطلاعات نباید موقع ثبت دامنه به صورت عمومی منتشر شوند و چرا؟

- ✓ **قوانین تمرین – بخش سوم**

وارد سایت owasp.org/top10 شده و درباره هر یک از ۱۰ آسیب‌پذیری مطرح در وب، تحقیق کنید و برای هر کدام توضیح، نحوه شناسایی و نحوه اکسپلویت را در گزارش خود شرح دهید.

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

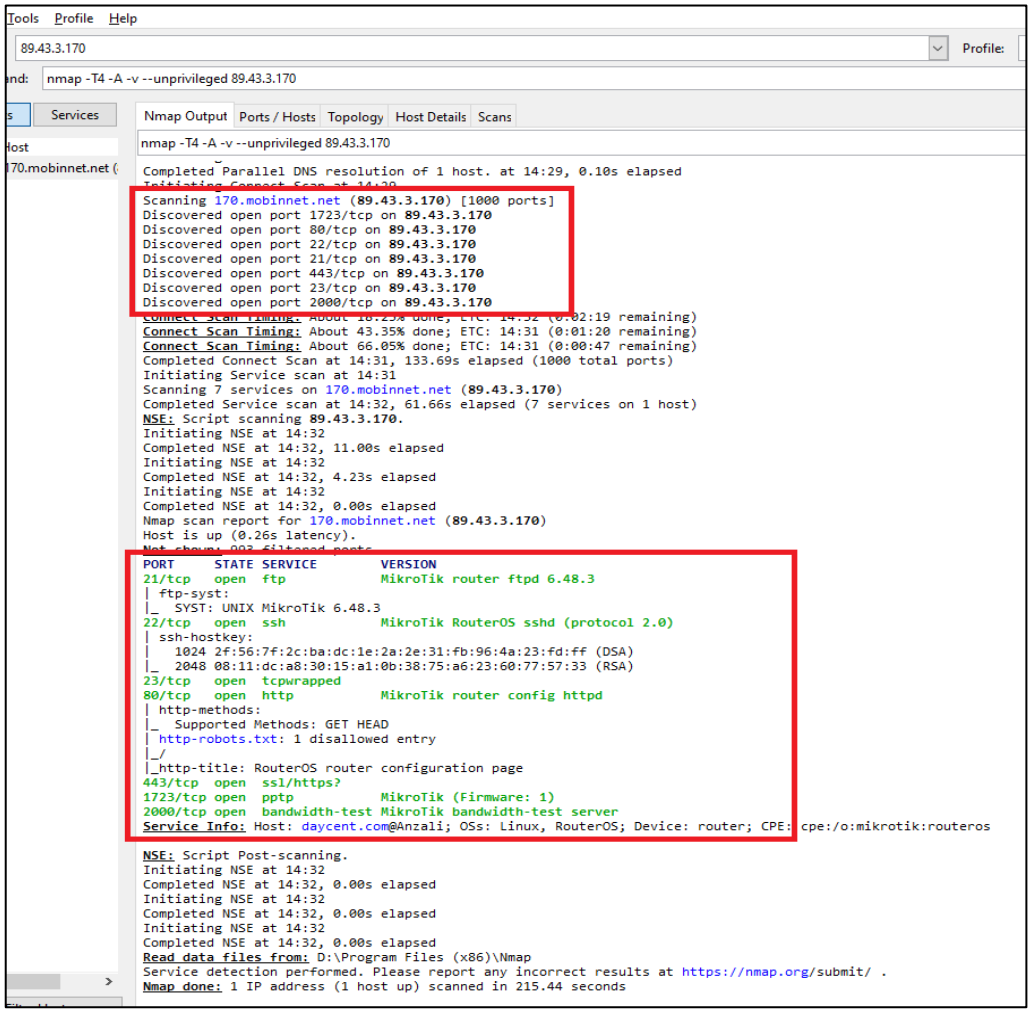
نکته۲: از تمامی مراحل انجام کار خود در بخش اول و دوم و سوم اسکرین‌شات گرفته و همراه با توضیحات، به فرمت گفته شده در بند **"ارسال"** قسمت نکات مهم در ابتدای این سند، در سامانه courses بارگذاری نمایید.

نمونه‌ای از موارد خواسته شده:

- **خروجی مورد نظر برای ابزار طراحی شده:**

```
Port Open:----> 23 -- Telnet
Port Open:----> 53 -- DNS
Port Open:----> 80 -- HTTP
Port Open:----> 1780 -- Not in Database
Port Open:----> 5000 -- Not in Database
Exiting Main Thread
scanning complete in  0:02:54.283984
```

- **خروجی مورد نظر بند ۱ بخش دوم:**



موفق باشید.