دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

به نام خدا

تمرین عملی دوم درس امنیت کامپیوتر

آشنایی با تست نفوذ و scanning

دکتر حمیدرضا شهریاری

پاییز ۱۴۰۲

نکات مهم:

کد: به جز کتابخانه‌های socket و os استفاده از کتابخانه‌های دیگر در زبان پایتون مجاز نیست. برای راحتی و درگیر نبودن با رابط کاربری گرافیکی، از کتابخانه argparse و رابط کاربری کامند لاینی (CLI) استفاده کنید.

گزارش: بخش اصلی ارزشیابی شما گزارش است؛ لذا ارسال کدها بدون گزارش شامل نمره نخواهد بود. گزارش باید شامل اسکرین‌شات از کد و خروجی و نحوه کار ابزارها باشد. همچنین سعی کنید توضیحی کوتاه درباره نحوه پیاده‌سازی و کارکرد توابع و کدها ارائه دهید.

تذکر: هر نوع کپی‌برداری غیرقابل‌قبول بوده و باعث درج نمره‌منفی برای هر دو طرف خواهد بود.

ارسال: فایل گزارش به همراه فایل کدها را به‌صورت یک فایل فشرده درآورده و آن را با فرمت prj2_studentfamilyname_studentnumber.zip در سامانه بارگذاری نمایید.

تأخیر: درمجموع ۱۰ روز تاخیر قابل قبول خواهد بود که هر روز تاخیر منجر به کسر ۵ درصد از نمره تمرین خواهد بود.

** در صورت نیاز می‌توانید سؤالات خود را در خصوص انجام تمرین، از طریق راه‌های ارتباطی زیر از تدریس یار بپرسید.

ایمیل: erf.mohammadi@aut.ac.ir

تعریف تمرین:

تمرین شامل دو بخش است.

بخش اول شامل مطالعه درباره فاز scanning در بحث تست نفوذ و پیاده‌سازی یک ابزار اسکن شبکه با استفاده از زبان پایتون است.

بخش دوم شامل تست و بررسی صحت عملکرد ابزار نوشته شده و همچنین آشنایی با ابزارهای Scanning است.

بخش ۱:

۱-۱-لطفا در ابتدا به بررسی فاز scanning در بحث تست نفوذ بپردازید و به سوالات زیر پاسخ دهید

۱-۱-۱- scanning چیست و در این فاز چه اطلاعاتی حاصل می‌گردد.

۱-۱-۲-تفاوت scanning با footprintingچیست ؟

۱-۱-۳-راه های مقابله با scanning (کاهش اطالاعاتی که هکر با اسکن شبکه هدف میتواند بدست بیاورد) چیست؟

۱-۲-در این بخش از شما خواسته شده است تا با استفاده از زبان برنامه نویسی پایتون یک ابزار اسکن شبکه را پیاده سازی کنید. ابزار مورد نظر باشد شامل قابلیت های زیر باشد.

۱-اسکن یک محدوده ip و یافتن ماشین‌های فعال

۲-اسکن پورت های باز tcp و udpیک ماشین فعال

۳-شناسایی سرویس اجرا شده بر روی پورت‌های باز یک ماشین فعال

۴-نمایش گزارش به کاربر و ذخیره آن در یک فایل با فرمت txt

**** نکات مهم پیاده‌سازی:**

۱-حتما از قالب دستوری زیر برای پیاده سازی بخش CLI ابزار استفاده کنید.

1-Scanner.py --ipscan –m 24 –ip 192.168.1.1 192.168.1.254

آدرس اول برای شروع رنج دامنه و آدرس دوم برای پایان و سوئیچ m– برای مشخص‌کردن subnet mask

2-scanner.py –portscan –tcp 1 1000

2-scanner.py –portscan –udp 1 1000

عدد اول برای شروع رنج پورت‌ها و عدد دوم برای پایان رنج شماره پورت‌ها

۲-فایل متنی گزارش تولید شده توسط ابزار باید در آدرس روت درایو c ذخیره گردد.

۳-برای تست ابزار میتوانید از شبکه لوکال خود (lAN) در صورت وجود ماشین کافی در شبکه (حداقل ۴ تا) و یا استفاده از ماشین های مجازی بر روی یک سیستم استفاده کنید.در غیر این صورت میتوانید از رنج ip زیر بعد از اتصال به VPN استفاده کنید.

89.43.3.0 – 89.43.3.255

بخش ۲:

در این بخش از شما خواسته شده است تا با استفاده از ابزارهای nmap و یا netscan pro صحت عملکرد و اطلاعات به‌دست‌آمده توسط ابزار پیاده‌سازی شده در قسمت اول را بررسی کنید.

۲-۱-لطفا در ابتدا به سوالات زیر در مورد nmap پاسخ دهید

۲-۱-۱-تحقیق کنید هریک از سوییچ های زیر چه کاربردی دارند.

-sS

-sV

-sT

-sV

۲-۱-۲- تحقیق کنید که هریک از سوییچ های زیر مربوط به چه مودی از Scan هستند و تفاوت آن ها در چیست؟

-F

-O

-A

۲-۱-۳-تحقیق کنید که سوییچ های sn– و pn– چه تفاوتی دارند

۲-۲- در این قسمت با استفاده از ابزار nmap و یا netscan tools pro تمامی اسکن هایی که با استفاده از ابزار پیاده سازی شده خود انجام دادید را دوباره انجام داده و خروجی ها را باهم مقایسه کنید.

در صورت استفاده از netscan tools pro از ابزارهای ping scan و portscan استفاده کنید.

لطفاً از تمامی بخش‌های خروجی ابزار و تست‌ها اسکرین‌شات گرفته و در گزارش خود بیاورید.

برای کسب اطلاعات بیشتر درمورد ابزار nmap می‌توانید از کتابی که همراه با فایل تمرین بارگذاری شده است استفاده کنید.

موفق باشید