

به نام خدا



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر

تمرین عملی دوم 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 حد امکان 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 قرار دهید.
- **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 اسکن کردن 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، قبلاً مورد بررسی برای جمع‌آوری اطلاعات قرار گرفته‌اند 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 `pycharm`، `vscode` و ... و کتابخانه‌هایی نظیر `scapy`، `nmap` 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 پورت‌های باز بررسی شود کفایت.

- 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 اول 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 قرار داده 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 وبسایت‌های 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.

نکته ۱: لازم به ذکر است اگر از سایت‌های آنلاین برای بدست آوردن اطلاعات اضافی استفاده می‌کنید، آدرس آن را در گزارش خود قید نمایید.

نکته ۲: 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:

The screenshot shows the Nmap output for the IP address 89.43.3.170. The command used is `nmap -T4 -A -v --unprivileged 89.43.3.170`. The output is divided into several sections, with two specific areas highlighted by red boxes. The first box highlights the 'Scanning 170.mobinnet.net (89.43.3.170) [1000 ports]' section, which lists discovered open ports: 1723/tcp, 80/tcp, 22/tcp, 21/tcp, 443/tcp, 23/tcp, and 2000/tcp. The second box highlights the 'PORT STATE SERVICE VERSION' section, which provides details for each open port: 21/tcp (ftp, MikroTik router ftpd 6.48.3), 22/tcp (ssh, MikroTik RouterOS sshd (protocol 2.0)), 23/tcp (tcpwrapped), 80/tcp (http, MikroTik router config httpd), 443/tcp (ssl/https?), 1723/tcp (pptp, MikroTik (Firmware: 1)), and 2000/tcp (bandwidth-test, MikroTik bandwidth-test server). The output also includes a 'Service Info' section indicating the host is a MikroTik router running Linux.

```
Tools Profile Help
89.43.3.170
nd: nmap -T4 -A -v --unprivileged 89.43.3.170
s Services Nmap Output Ports / Hosts Topology Host Details Scans
Host 170.mobinnet.net (89.43.3.170)
Completed Parallel DNS resolution of 1 host, at 14:29, 0.10s elapsed
Initiating Connect Scan at 14:30
Scanning 170.mobinnet.net (89.43.3.170) [1000 ports]
Discovered open port 1723/tcp on 89.43.3.170
Discovered open port 80/tcp on 89.43.3.170
Discovered open port 22/tcp on 89.43.3.170
Discovered open port 21/tcp on 89.43.3.170
Discovered open port 443/tcp on 89.43.3.170
Discovered open port 23/tcp on 89.43.3.170
Discovered open port 2000/tcp on 89.43.3.170
Connect Scan Timing: About 10.22% done; ETC: 14:32 (0:02:19 remaining)
Connect Scan Timing: About 43.35% done; ETC: 14:31 (0:01:20 remaining)
Connect Scan Timing: About 66.05% done; ETC: 14:31 (0:00:47 remaining)
Completed Connect Scan at 14:31, 133.69s elapsed (1000 total ports)
Initiating Service scan at 14:31
Scanning 7 services on 170.mobinnet.net (89.43.3.170)
Completed Service scan at 14:32, 61.66s elapsed (7 services on 1 host)
NSE: Script scanning 89.43.3.170.
Initiating NSE at 14:32
Completed NSE at 14:32, 11.00s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 4.23s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.26s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          MikroTik router ftpd 6.48.3
|_ ftp-syst:
|_ SYST: UNIX MikroTik 6.48.3
22/tcp    open  ssh          MikroTik RouterOS sshd (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 2f:56:7f:2c:ba:dc:1e:2a:2e:31:fb:96:4a:23:fd:ff (DSA)
|_ 2048 08:11:dc:a8:30:15:a1:0b:38:75:a6:23:60:77:57:33 (RSA)
23/tcp    open  tcpwrapped
80/tcp    open  http         MikroTik router config httpd
|_ http-methods:
|_ Supported Methods: GET HEAD
|_ http-robots.txt: 1 disallowed entry
|_/
|_ http-title: RouterOS router configuration page
443/tcp    open  ssl/https?
1723/tcp  open  pptp         MikroTik (Firmware: 1)
2000/tcp  open  bandwidth-test MikroTik bandwidth-test server
Service Info: Host: daycent.com@Anzali; OS: Linux, RouterOS; Device: router; CPE: cpe:/o:mikrotik:routeros
NSE: Script Post-scanning.
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Initiating NSE at 14:32
Completed NSE at 14:32, 0.00s elapsed
Read data files from: D:\Program Files (x86)\Nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.44 seconds
```

موفق باشید.