دانشکده مهندسی کامپیوتر

پروژه درس شبکه‌های کامپیوتری

نیم‌سال اول سال تحصیلی ۱۴۰۳-۱۴۰۴

دستیاران آموزشی:

محمد حسین رنگ‌رز

محمد حسین دهقانی اشکذری

محمد حسین چهکندی

زهرا سعیدی

کیمیا میرمقتدایی

علی کثیری

۱.۰ فاز اول :پیاده‌سازی قابلیت‌های نرم‌افزار nmap

nmap یک ابزار بسیار قدرتمند است که توسط مدیران شبکه [۱]، متخصصان امنیت [۲] و حتی هکرها [۳] برای کاوش، بررسی و درک بهتر شبکه‌های کامپیوتری مورد استفاده قرار می‌گیرد. نام این ابزار مخفف شده عبارت نگاشت کننده اینترنت [۴] است. این ابزار به کاربر کمک می‌کند تا دستگاه‌هایی [۵] که در یک شبکه کامپیوتری فعال هستند را پیدا کند، سرویس‌ها و برنامه‌هایی که روی آن دستگاه‌ها در حال اجرا هستند را شناسایی کند و حتی مواردی را که از لحاظ امنیتی، آسیب‌پذیر [۶] هستند را مشخص کند.

برای کسب اطلاعات بیشتر در مورد این ابزار می‌توانید به این لینک مراجعه کنید.

۱ Network Administrator ۲ Security Expert ۳ Hacker ۴ Network Mapper ۵ Device ۶ Vulnerable

۱.۱.۰ تعاریف مورد نیاز

ممکن است در حین خواندن این نوشتار به بعضی تعاریف نیاز پیدا کنید. برای سادگی کار شما برخی از آن تعاریف آورده شده‌اند:

- میزبان[۷]: در مفهوم شبکه‌های کامپیوتری، میزبان به دستگاه یا سیستمی اشاره دارد که قادر است به شبکه متصل شود و در شبکه‌ای حضور دارد. میزبان می‌تواند یک کامپیوتر، سرور[۸]، روتر[۹]، گیتوی[۱۰] یا ... باشد. برای شناسایی هر میزبان در شبکه یک آدرس IP منحصر به فرد به آن داده می‌شود.
- سرویس[۱۱]: در تعریف شبکه، سرویس به خدمت ارائه شده توسط یک نرم‌افزار یا پروتکل خاص اشاره دارد که بر روی یک میزبان در شبکه اجرا می‌شود و به دیگر دستگاه‌های حاضر در شبکه خدماتی را ارائه می‌دهند.
- پورت[۱۲]: در شبکه‌های کامپیوتری، پورت به یک عدد از ۰ تا ۶۵۵۳۵ اشاره دارد که برای تعیین و شناسایی خدمات و برنامه‌ها مورد استفاده قرار می‌گیرد. معمولا هر پورت متناظر با یک خدمت یا برنامه خاص در یک میزبان است و به آن امکان ارتباط و تبادل داده با سایر میزبان‌های موجود در شبکه را می‌دهد.

  - پورت باز[۱۳] : اگر در یک میزبان پورتی در وضعیت باز قرار داشته باشد یعنی آن دستگاه به درخواست‌های ورودی به این پورت پاسخ می‌دهد و ارتباط با آن دستگاه از طریق آن پورت امکان پذیر است.
  - پورت بسته [۱۴]: در نقطه مقابل پورت باز قرار دارد و اگر در دستگاهی، پورتی در این حالت قرار داشته باشد به آن معناست که میزبان موردنظر به درخواست‌های ورودی به این پورت پاسخ نخواهد داد و ارتباط با آن دستگاه از طریق پورت ذکرشده امکان‌پذیر نخواهد بود.

---

۷ Host ۸ Server ۹ Router ۱۰ Gateway ۱۱ Service ۱۲ Port ۱۳ Open Port ۱۴ Closed Port

۲.۱.۰ آموزش کار با نرم‌افزار

توصیه می‌شود برای آشنایی بیشتر با این نرم‌افزار، برنامه را دانلود کرده و پس از نصب، تعدادی از قابلیت‌های ساده آن را امتحان کنید. همچنین برای مشاهده نحوه کار این ابزار می‌توانید از این لینک به صورت آنلاین، برخی از قابلیت‌های آن را امتحان کرده و نتیجه را مشاهده کنید.

در ادامه تصاویری از محیط ابزار و همچنین وبسایت معرفی شده قرار داده شده است.

گزارش پورت ها

```
pentester@TryHackMe$ sudo nmap -sV 10.10.76.34

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:03 BST
Nmap scan report for 10.10.76.34
Host is up (0.0040s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
25/tcp  open  smtp    Postfix smtpd
80/tcp  open  http    nginx 1.6.2
110/tcp open  pop3    Dovecot pop3d
111/tcp open  rpcbind 2-4 (RPC #100000)
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
Service Info: Host:  debra2.thm.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

شکل ۱: در تصویر بالا، کاربر پس از دادن آدرس IP هدف خود به ابزار nmap و استفاده از دستور `-sV` نتایج اسکن را که شامل شماره پورت، وضعیت هر پورت، سرویسی که روی آن پورت در حال اجراست و همچنین نسخه آن سرویس را به عنوان گزارش دریافت کرده است.

گزارش کامل

```
root@kali:/home/geek
File  Actions  Edit  View  Help

┌──(root💀kali)-[/home/geek]
└─# nmap -A 192.168.2.107
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-09 15:20 EST
Nmap scan report for 192.168.2.107
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.2.104
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
```

شکل ۲: در این تصویر کاربر با استفاده از عبارت `-A` به ابزار گزارش کاملی از اسکن هدف را درخواست میکند.

۳.۱.۰ هدف پروژه

در این پروژه قصد داریم تا دانشجویان پس از آشنایی با تعدادی از قابلیت‌های نرم‌افزار ،nmap به پیاده‌سازی برخی از قابلیت‌های ساده این ابزار بپردازند.

قابلیت‌های مدنظر جهت پیاده‌سازی

برنامه پیاده‌سازی شده توسط شما باید بتواند پس از دریافت آدرس آیپی هدف و یک بازه از پورت‌هایی که قصد بررسی آن‌ها را داریم عملیات‌های زیر را انجام دهد:

- بررسی وضعیت آنلاین بودن یا نبودن یک میزبان
- بررسی محدوده‌ای از پورت‌های یک میزبان و گزارش پورت‌هایی که در حالت باز قرار دارند
- بررسی مدت زمان تاخیر در پاسخگویی پورت‌ها
- شبیه‌سازی متدهای GET و POST پروتکل HTTP

تمامی قابلیت‌های خواسته شده به وسیله برنامه نویسی سوکت [۱۵] قابل پیاده سازی هستند. در ادامه به بررسی هرکدام از موارد گفته شده می‌پردازیم.

بررسی وضعیت آنلاین بودن یا نبودن یک میزبان

برای پیاده‌سازی این قابلیت، برنامه باید تلاش کند یک ارتباط با میزبان خواسته شده برقرار کند. در صورتی که این ارتباط با موفقیت برقرار شد، میزبان آنلاین است و در غیر این صورت میزبان آفلاین شناخته خواهد شد.

بررسی پورت‌ها

برنامه باید پس از دریافت آدرس IP یک میزبان و یک بازه از پورت‌های مدنظر جهت اسکن شدن، تک‌تک پورت‌ها را مورد بررسی قرار دهد و در صورتی که پورت در وضعیت باز قرار داشت، شماره آن پورت و سرویسی که روی آن پورت در حال اجراست را برگرداند.

```
PS C:\Users\mhda1\Desktop> python nmap.py 1.1.1.1 80 81
1.1.1.1 is online
open port detected: 1.1.1.1     -- Port: 80     -- Service: http        -- Hostname: one.one.one.one
```

شکل ۳: نمونه ای از ورودی و خروجی مدنظر برای قابلیت‌های شماره ۱ و ۲.

[۱۵] Socket Programming

بررسی مدت زمان تاخیر در پاسخگویی پورت‌ها

برنامه شما باید قادر باشد تا میانگین زمان تاخیر در پاسخگویی [۱۶] برای یک پورت مشخص را محاسبه کند. میانگین ذکر شده باید برای مقادیر مختلف تعداد درخواست، قابل محاسبه و اندازه‌گیری باشد. برای مثال میانگین تاخیر پاسخگویی برای n درخواست ارسالی.

شبیه‌سازی متدهای GET و POST

POST و GET از متدهای درخواست پروتکل HTTP [۱۷] هستند. GET برای فراخوانی داده مورد استفاده قرار می‌گیرد و متد پست برای ثبت کردن یک مقدار جدید. برای پیاده سازی این قابلیت، یک فایل server.py در اختیار شما قرار خواهد گرفت. این فایل یک سرور را شبیه‌سازی می‌کند که اطلاعات تعدادی از کاربران را نگهداری می‌کند. این اطلاعات در تصویر زیر قابل مشاهده هستند.

```
users = {
    'user1': {'name': 'Alice', 'age': 30},
    'user2': {'name': 'Bob', 'age': 25},
    'user3': {'name': 'Charlie', 'age': 35},
}
```

شکل ۴: اطلاعات کاربران نگهداری شده در سرور شبیه‌سازی شده.

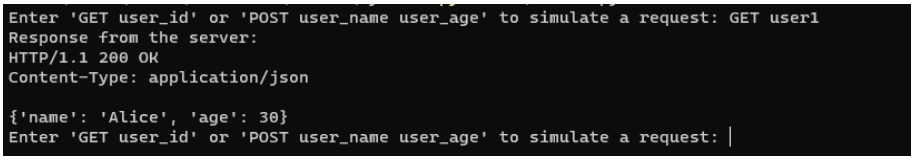
شما باید در برنامه پیاده‌سازی شده خودتان قابلیتی را به وجود بیاورید که ابزار بتواند با متد GET اطلاعات کاربر خواسته شده را که با ID آن کاربر (ستون اول که شامل مقادیر user۱، user۲ user۳ می‌باشد ID کاربران را مشخص می‌کند) داده می‌شود پیدا کرده و مقادیر آن را گزارش دهد. فرمت قابل قبول برای برنامه سرور به شرح زیر است:

```
GET user_id
```

[۱۶] latency

[۱۷] HTTP Request Methods

که شما با وارد کردن ID کاربر مدنظر می‌توانید اطلاعات آن را مشاهده کنید. به عنوان مثال به تصویر زیر دقت کنید.



همچنین ابزار باید این قابلیت را داشته باشد که بتواند با استفاده از متد POST و دریافت نام و سن کاربر، اطلاعات آن کاربر را به مجموعه اطلاعات کاربرها اضافه کند. فرمت قابل قبول برای برنامه سرور به شرح زیر است:

```
POST user_name user_age
```

دستور POST پس از ساخت هر کاربر جدید یک ID منحصربه فرد برای او می‌سازد که به فرمت `user + {شماره آخرین یوزر ساخته شده + ۱}` است

نکته: لازم به ذکر است که در هر دو دستور مقادیر باید با کاراکتر space از هم جدا شده باشند.