دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

Department of
Computer Engineering

به نام خداوند جان و خرد

پروژه تحویلی دوم

درس مبانی امنیت اطلاعات

امیرفاضل کوزه گر کالجی

9931099

بخش اول

1-1 سوالات

1.1.1 Scanning، فازی است که در آن از تکنیک هایی برای جمع آوری اطلاعات درباره یک سیستم هدف یا یک شبکه است. هدف اصلی، شناسایی آسیب پذیری های محتمل، نقاط ضعف و گلوگاه های سیستمی می‌باشد.

Scan کردن می‌تواند انواع متفاوتی داشته باشد: اسکن پورت، اسکن شبکه، استن آسیب پذیری ها.

1.1.2 تفاوت کلیدی میان footprinting و scanning آن است که در footprining از تمام سرویس های سیستم که به طور عمومی در اختیارمان قرار داده شده استفاده می‌کنیم اما در scanning به طور فعال به دنبال نفوذ و کشف آسیب پذیری در سیستم هستیم مثل موردی که به دنبال پورت های فعال سیستم بگردیم.

1.1.3

- قرار دادن دیواره آتش
- توسعه یک سیستم detection/prevention
- تقسیم شبکه به زیرشبکه های مختلف و ایجاد کنترل های دسترسی
- به روز رسانی های مداوم شبکه
- غیرفعال کردن پورت های غیر فعال و بلا استفاده

1-2 پیاده سازی

در سمت پیاده سازی، یک برنامه با دو کاربرد داریم:

- بررسی یک بازه از آی پی ها و تشخیص ماشین های فعال درون آنها:

```
PS E:\University\Semester-7\Information S
scan -m 24 -ip 192.168.1.1 192.168.1.254
Scanning IPs...
IP 192.168.1.1/24 is active
IP 192.168.1.2/24 is not active
IP 192.168.1.3/24 is not active
IP 192.168.1.4/24 is not active
IP 192.168.1.5/24 is not active
IP 192.168.1.6/24 is not active
IP 192.168.1.7/24 is not active
IP 192.168.1.8/24 is not active
IP 192.168.1.9/24 is not active
IP 192.168.1.10/24 is not active
IP 192.168.1.11/24 is not active
```

```
IP 192.168.1.31/24 is not active
IP 192.168.1.32/24 is not active
IP 192.168.1.33/24 is not active
IP 192.168.1.34/24 is active
IP 192.168.1.35/24 is active
IP 192.168.1.36/24 is not active
IP 192.168.1.37/24 is not active
IP 192.168.1.38/24 is not active
IP 192.168.1.39/24 is not active
IP 192.168.1.40/24 is not active
IP 192.168.1.41/24 is not active
IP 192.168.1.42/24 is not active
```

- در مورد دوم یک بازه از پورت های یک ماشین طبق پروتوکلشان بررسی می شوند و اگر فعال بودند، سرویس مورد استفاده آنها ذکر می شود:

اجرای برنامه با محوریت پروتوکل TCP

```
TCP Port 74 is closed
TCP Port 75 is closed
TCP Port 76 is closed
TCP Port 77 is closed
TCP Port 78 is closed
TCP Port 79 is closed
TCP Port 80 is open      ------------->   http
TCP Port 81 is closed
TCP Port 82 is closed
TCP Port 83 is closed
TCP Port 84 is closed
TCP Port 85 is closed
```

اجرای برنامه با محوریت پروتوکل UDP:

```
UDP Port 79 is open      ------------>   Unable to retrieve service information
UDP Port 80 is open      ------------>   Unable to retrieve service information
UDP Port 81 is open      ------------>   hosts2-ns
UDP Port 82 is open      ------------>   Unable to retrieve service information
UDP Port 83 is open      ------------>   Unable to retrieve service information
UDP Port 84 is open      ------------>   Unable to retrieve service information
UDP Port 85 is open      ------------>   Unable to retrieve service information
UDP Port 86 is open      ------------>   Unable to retrieve service information
UDP Port 87 is open      ------------>   Unable to retrieve service information
UDP Port 88 is open      ------------>   kerberos
UDP Port 89 is open      ------------>   Unable to retrieve service information
UDP Port 90 is open      ------------>   Unable to retrieve service information
UDP Port 91 is open      ------------>   Unable to retrieve service information
```

2-1 سوالات

2-1-1

- -sS

TCP SYN port scan

- -sV

Attempts to determine the version of the service running on port

- -sT

TCP connect port scan (Default without root privilege)

2-1-2

- -F

این مود، عملیات اسکن را به صورت سریع انجام می دهد.

- -O

به ما اجازه تشخیص سیستم عامل ماشین هدف را می دهد.

- -A

این پرچم مخفف Aggressive detection mode می باشد و چندین عملیات را پشت سر هم انجام می دهد. عملیاتی مانند O- و sV-.

3-1-2

- -sn

به nmap می‌گوید که هیچ پورت اسکنی انجام ندهد.

- -pn

به nmap می گوید که هیچ پینگ اسکنی انجام ندهد.

پیاده سازی

در این بخش تمامی موارد پیاده سازی در بخش قبل را با ابزاری به نام nmap انجام می دهیم.

مورد اول:

با استفاده از دستور nmap ماشین های یک بازه داده شده را بررسی کرده و در میان آنها به دنبال ماشین های فعال می‌گردیم.

```
fazel@vawzen:~$ nmap -sn 192.168.1.1-200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-28 21:46 +0330
Nmap scan report for 192.168.1.1
Host is up (0.0019s latency).
Nmap scan report for 192.168.1.34
Host is up (0.0018s latency).
Nmap scan report for 192.168.1.35
Host is up (0.0016s latency).
Nmap done: 200 IP addresses (3 hosts up) scanned in 5.05 seconds
fazel@vawzen:~$
```

در قسمت دوم همانند قبل به دنبال پورت های فعال یک ماشین (در اینجا ماشین خودمان)، به همراه سرویس مورد استفاده و پروتوکل آن می‌گردیم:

```
fazel@vawzen:~$ nmap -p 20-100 192.168.1.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-28 22:05 +0330
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
Not shown: 78 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 7.13 seconds
```