به نام خداوند جان و خرد

پروژه تحویلی دوم

درس مبانی امنیت اطلاعات

امیرفاضل کوزه گر کالجی

9931099

بخش اول

* 1. سوالات

Scanning 1.1.1، 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.

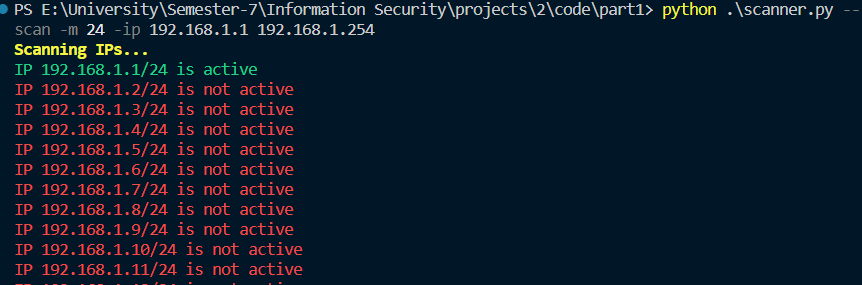
Scan کردن می‌تواند انواع متفاوتی داشته باشد: اسکن پورت، اسکن شبکه، استن آسیب پذیری ها.

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. پیاده سازی

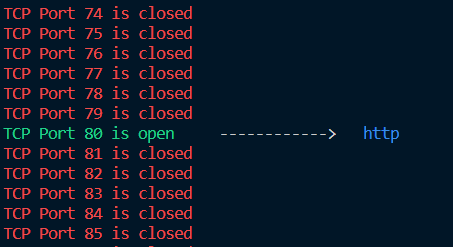
در سمت پیاده سازی، یک برنامه با دو کاربرد داریم:

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



* 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



اجرای برنامه با محوریت پروتوکل UDP:



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

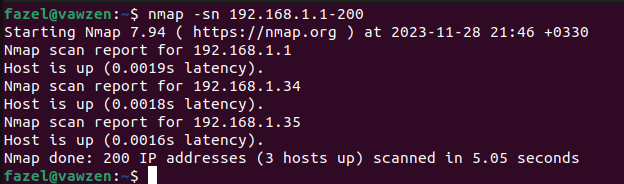
به nmap می گوید که هیچ پینگ اسکنی انجام ندهد.

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.



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:

