**(( گزارش پروژه اول مبانی امنیت اطلاعات ))**

**گردآورنده : عرفان ماجدی 9831099**

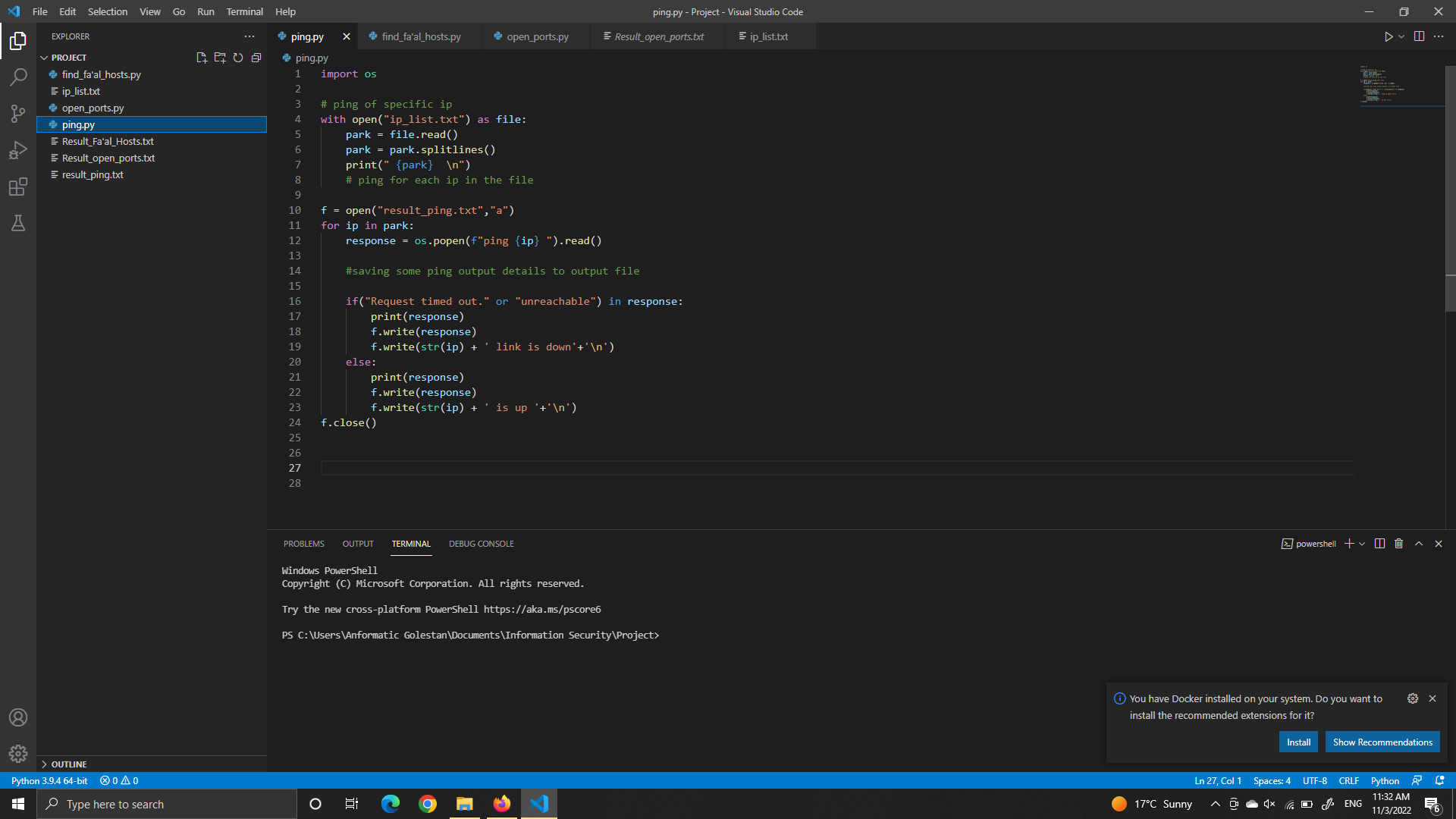
**مبانی امنیت اطلاعات**

**دکتر شهریاری**

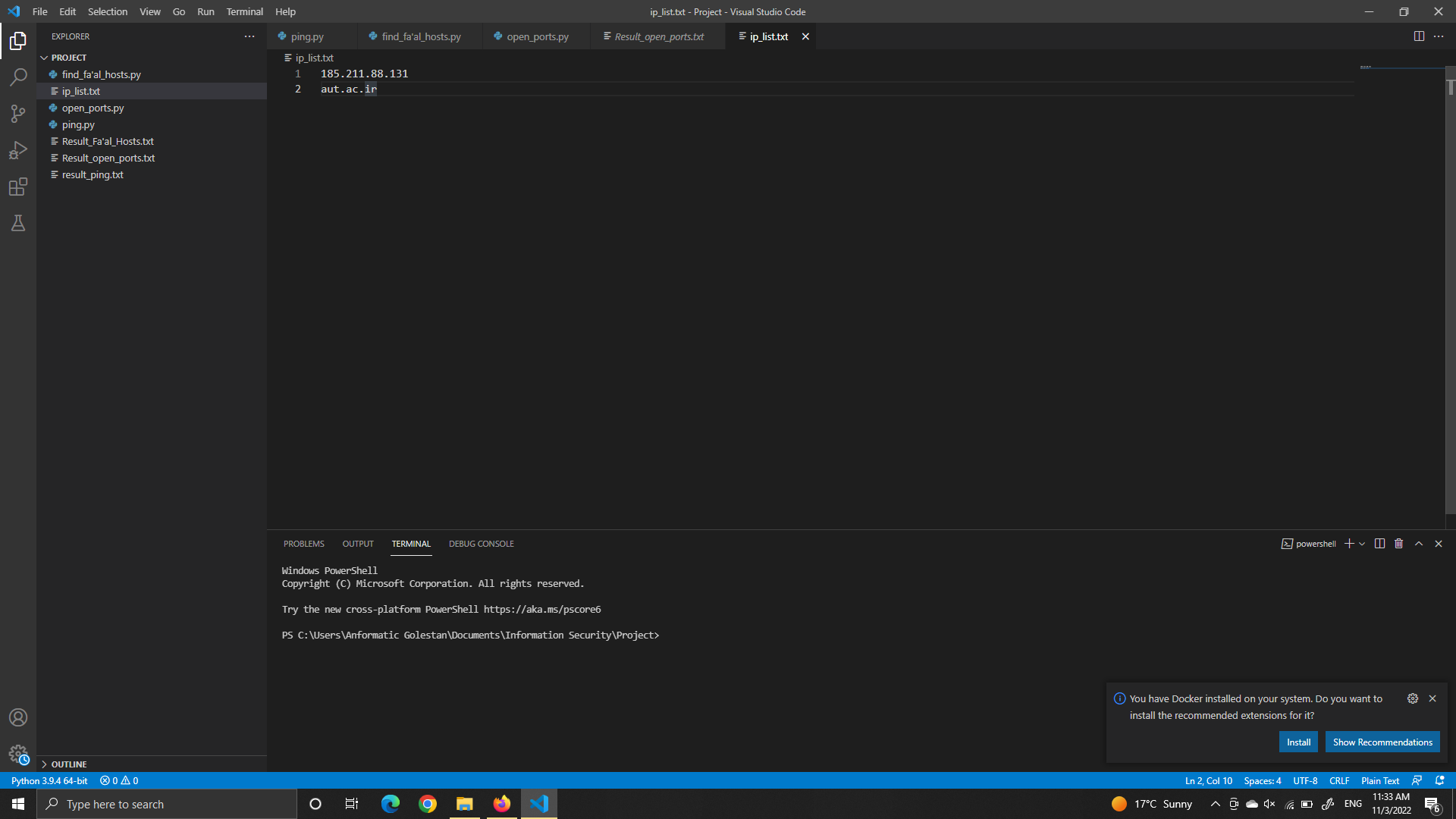
**گزارش بخش اول )**

**1) گرفتن ping از یک آی پی خاص :**

**کد این قسمت به شکل زیر است :**

****

**کد بخش 1**

****

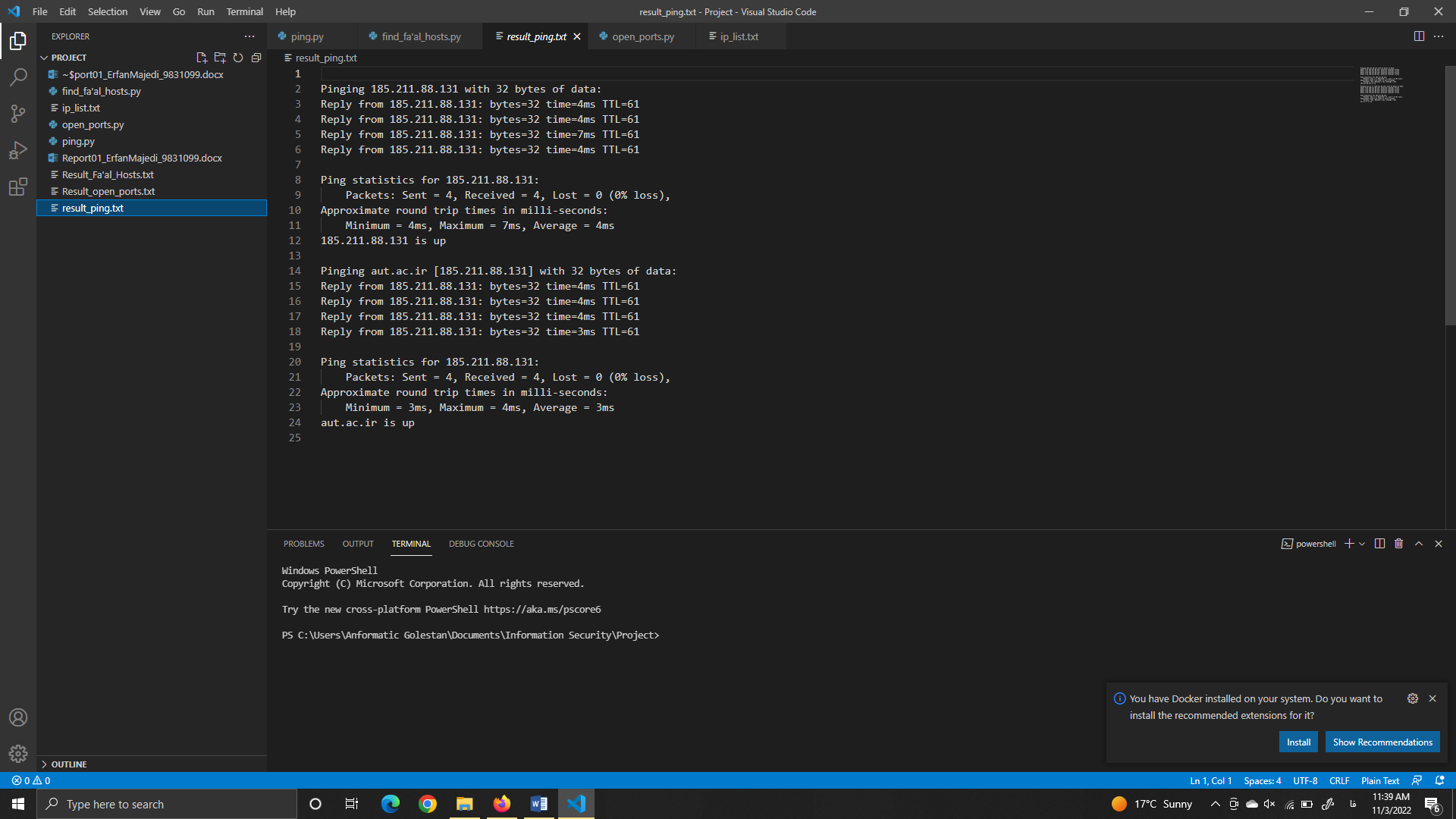
**محتوای فایل ip\_list**

**در این بخش ابتدا با استفاده از cmd، ip address سایت دانشگاه به نشانی aut.ac.ir را پیدا کرده و این ادرس و دامنه ی سایت را در یک فایل txt ذخیره کردیم. در پیاده سازی کد از کتابخانه ی os استفاده کردیم. در ابتدا فایل txt را باز کردیم و محتوای آن را خواندیم و در متغیر park ذخیره کردیم و سپس آن را print کردیم. سپس فایل result\_ping را در قالب یک فایل txt درست کردیم و در متغیر f قرار دادیم. حال متغیر park که شامل ip ها می باشد را در یک حلقه ی for گذاشتیم تا محتوای آن را گردش کنیم و به ازای هر ip از method ای استفاده کردیم به نام os.popen که در واقع کاری همان گرفتن ping را انجام می دهد و سپس در اخر خط یک method read() قرار دادیم تا محتوای object ساخته شده را بخواند. در اخرین مرحله دو حالت وجود دارد :**

**1) درخواست ما time out شود یا پیام unreachable دریافت کنیم -> ادرس ip ما down است.**

**2) پیام های بالا را دریافت نکنیم -> ادرس ip ما up است.**

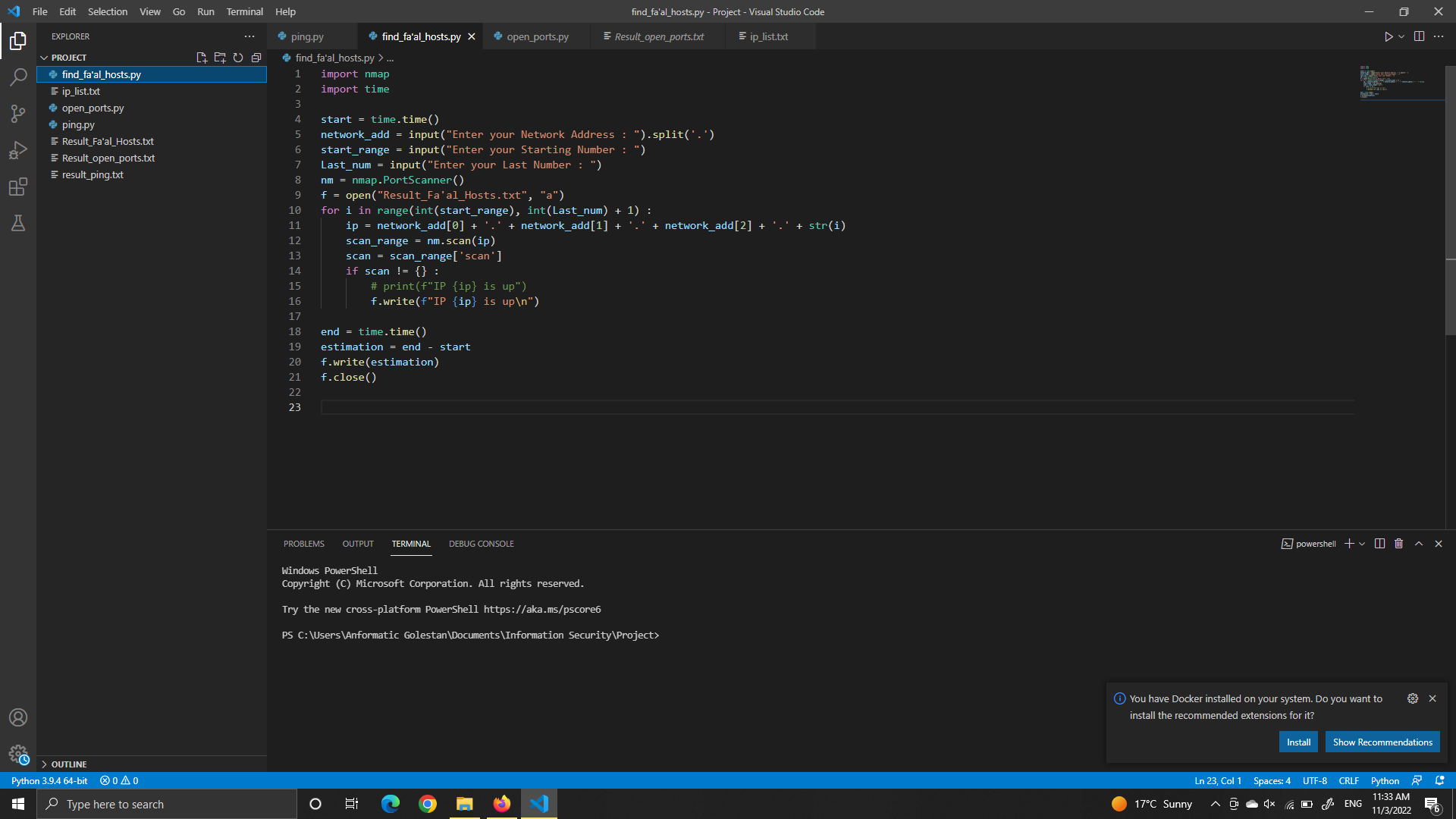
**دو حالت توضیح داده شده را در قالب یک if – else می نویسیم و سپس نتیجه را در فایلی که در f ریختیم ذخیره می کنیم. نتیجه به صورت زیر خواهد بود :**

****

**محتوای فایل result\_ping**

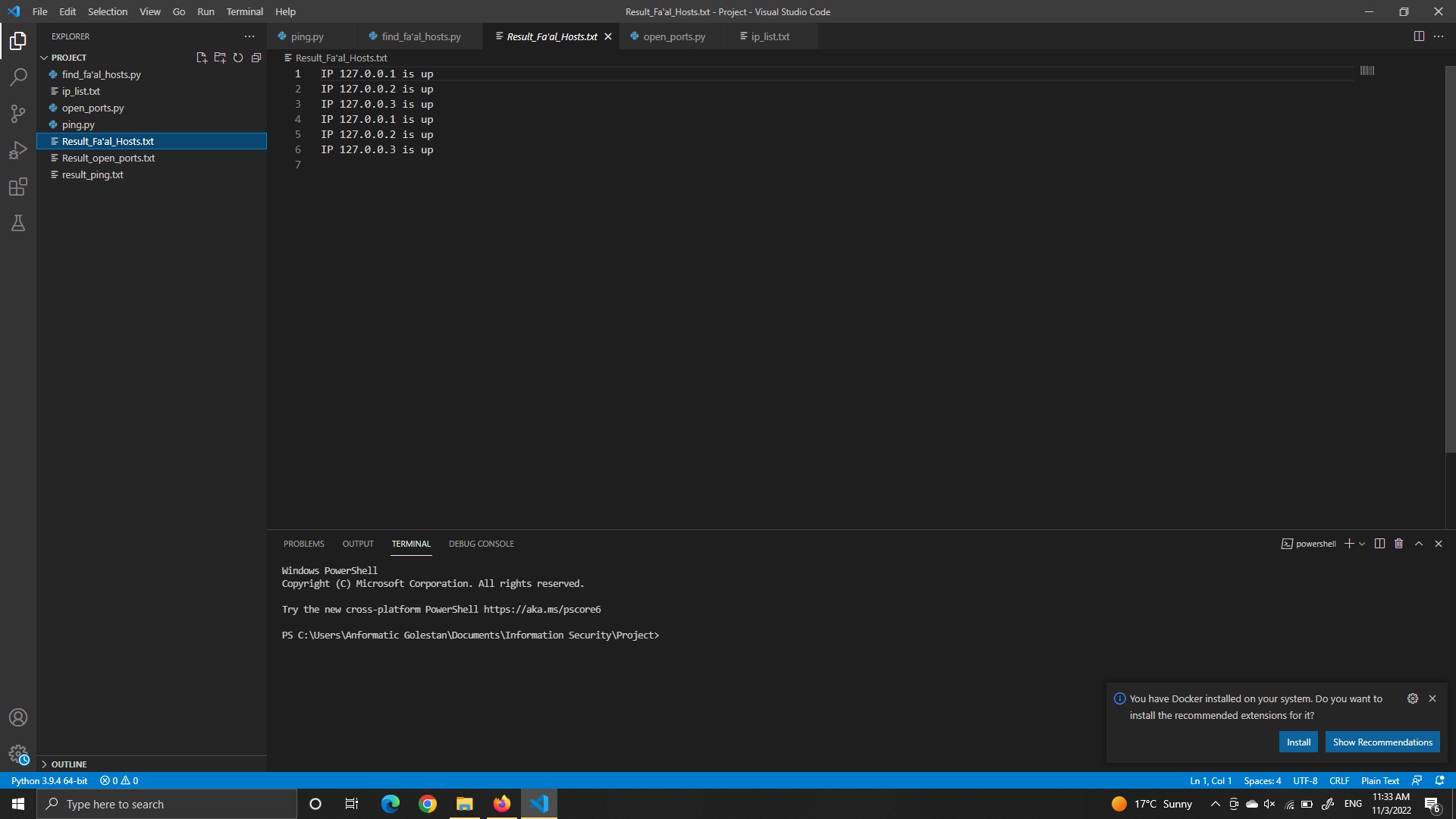
**2) اسکن یک محدوده آی پی خاص و یافتن هاست های فعال :**

**کد این بخش نیز به صورت زیر است :**

****

**کد بخش دوم**

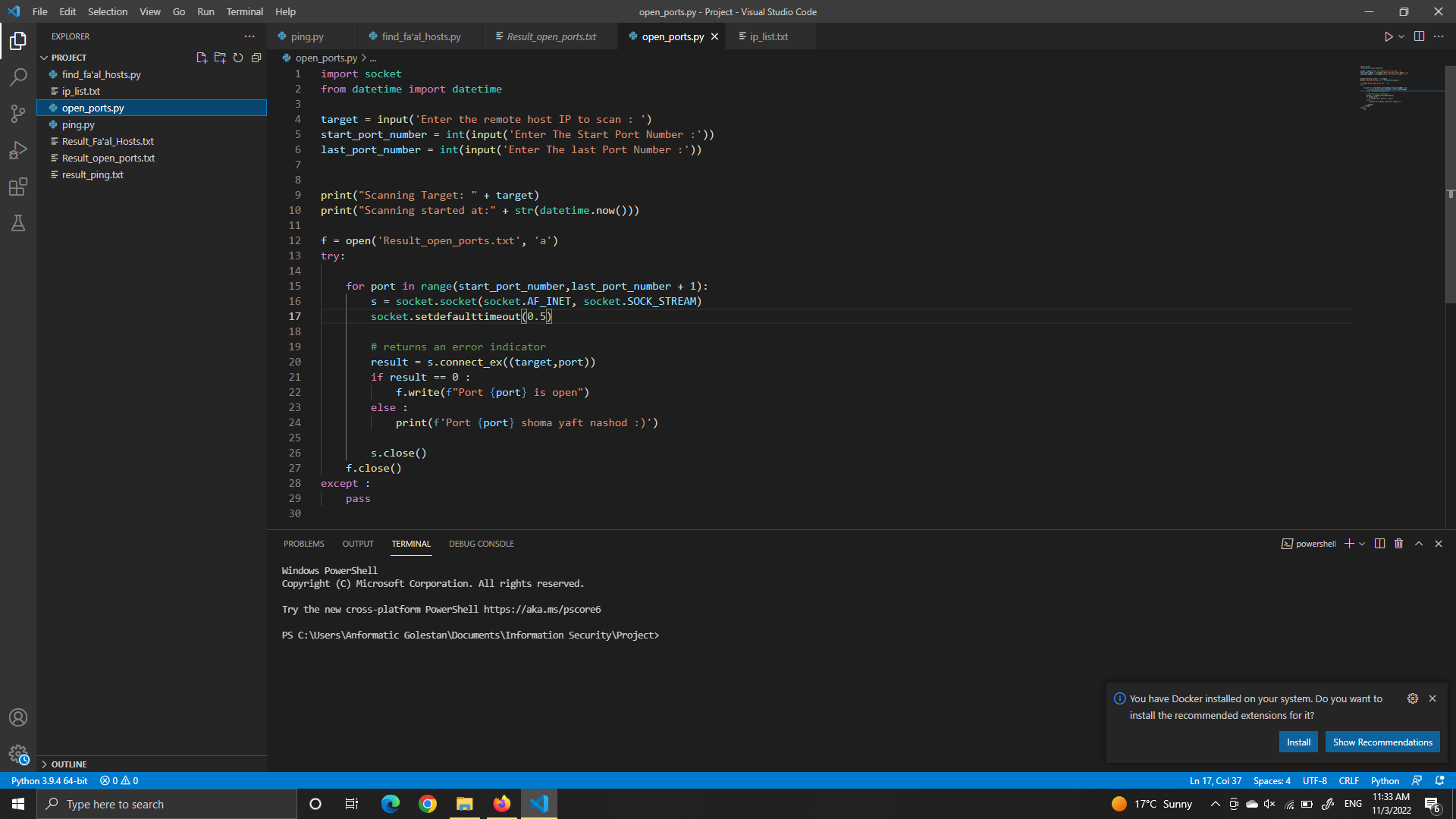
**در این بخش از کتابخانه های nmap و time استفاده کردیم. در اولین خط کد شروع زمان گیری را انجام میدهیم و آن را start نامیدیم. سپس سه تا ورودی از کاربر میگیریم که شامل ادرس ip است که با نقطه split کردیم ، عدد شروع و پایان ip را هم گرفتیم. سپس یک object از تابع nmap ساختیم با استفاده از nmap.PortScanner() و در nm ریختیم. برای ذخیره ی نتیجه ی این کد هم یک فایل txt به اسم Result\_Fa’al\_Hosts درست کردیم. حال یک حلقه ی for در range عدد شروع و (پایان + 1) زدیم و توجه کنید چون ورودی str است آن ها را به int تبدیل کردیم. حال ip ها را در این محدوده درست کردیم ( خط 11 ) و کار scan را با استفاده از method ای به نام nm.scan() انجام دادیم و چون به صورت یک dictionary است و ما با key = scan کار داریم ، value های آن را در متغیر scan ذخیره می کنیم. حال اگر این scan خالی نباشد می گوییم ip فعال است و سپس پایان زمان گیری را انجام داده و estimate می کنیم و نتایج را در فایل ایجاد شده می نویسیم که به صورت زیر است ( توجه کنید به عنوان ورودی ادرس ip 127.0.0.0 را دادیم ) :**

****

**محتوای فایل Report\_Fa’al\_Hosts**

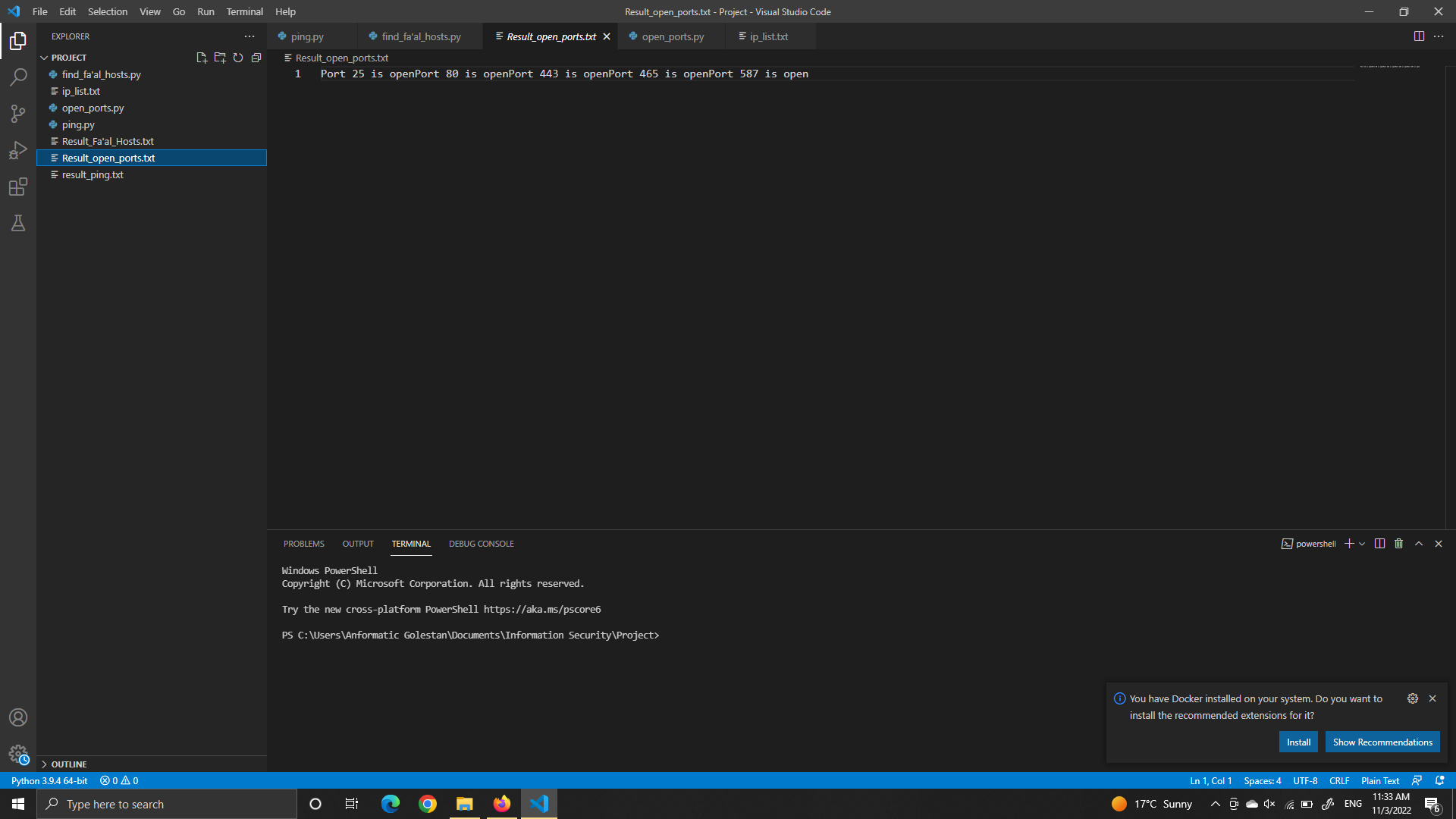
**3) اسکن پورت های باز یک هاست فعال :**

**کد این بخش به صورت زیر است :**

****

**کد بخش سوم**

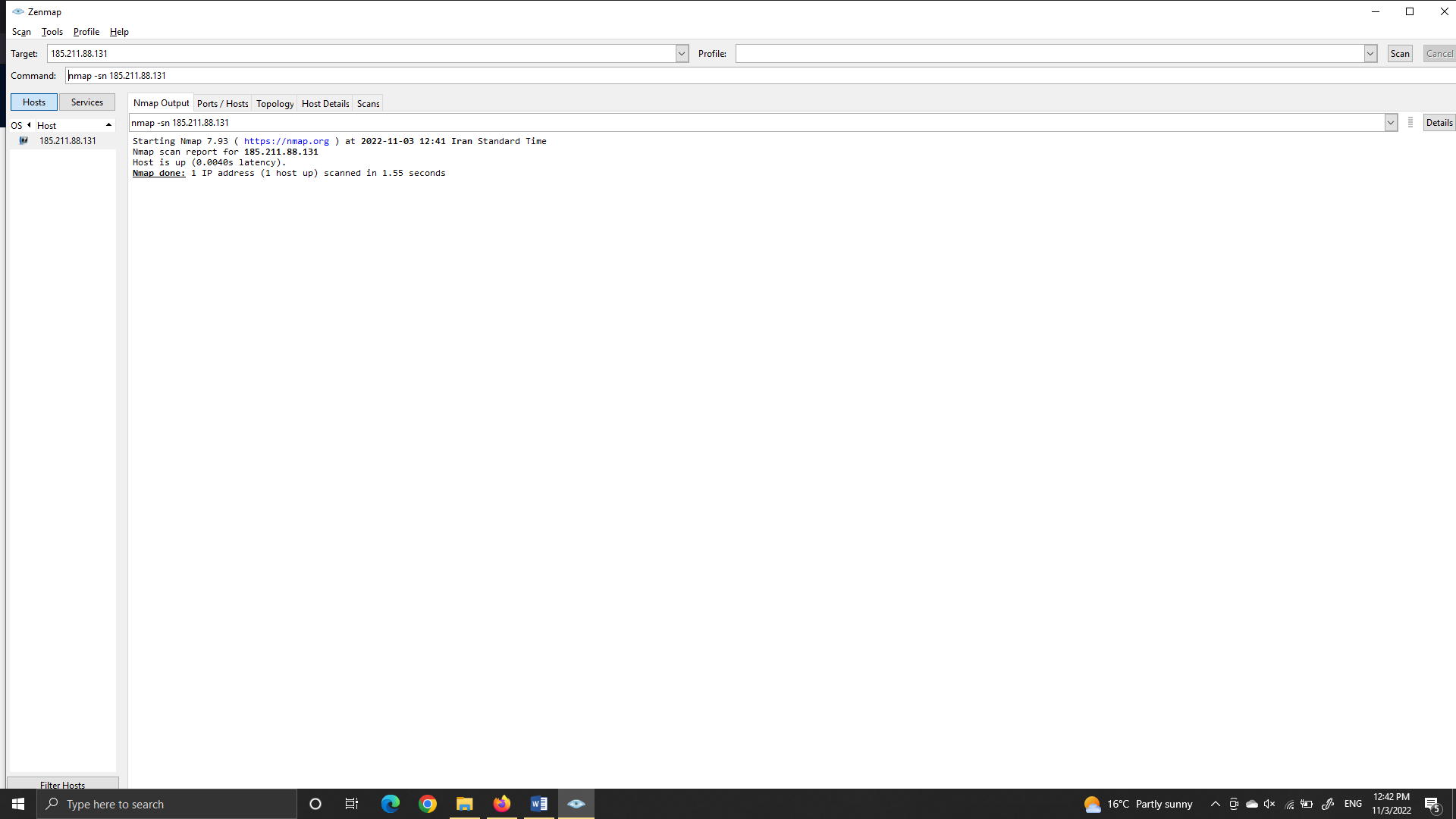
**در این بخش از کتابخانه ی socket و datetime استفاده کردیم . سه تا ورودی شامل host ip ، عدد شروع port و عدد پایان آن را گرفتیم. ( توجه کنید که اعداد شروع و پایان را به int تبدیل کردیم ) سپس host ip و زمان شروع اجرا را print کردیم و یک فایل txt برای ذخیره نتایج درست کردیم. در قسمت اصلی کد یک try – except ایجاد کردیم و در قسمت try آن یک حلقه روی port ها از اعداد شروع تا (پایان + 1 ) می زنیم. سپس یک socket روی پروتکل tcp درست می کنیم و آن را s می نامیم و default time out آن را روی 0.5 قرار میدهیم. از متد connect\_ex که یک tuple از (target, port) می گیرد استفاده میکنیم تا port های فعال را پیدا کنیم و در صورت فعال بودن این method مقدار صفر و در غیر این صورت مقدار یک را برمیگرداند و نتیجه ی آن را در result می ریزیم . result اگر برابر با صفر بود در فایل می نویسیم که port مورد نظر فعال است و در غیر این صورت یافت نشده است سپس سوکت را می بندیم و فایل را نیز می بندیم و در قسمت except چون کاری انجام نمیدهیم pass می گذاریم. نتیجه ی این کد را روی ip سایت اصلی دانشگاه aut.ac.ir در زیر مشاهده می کنید :**

****

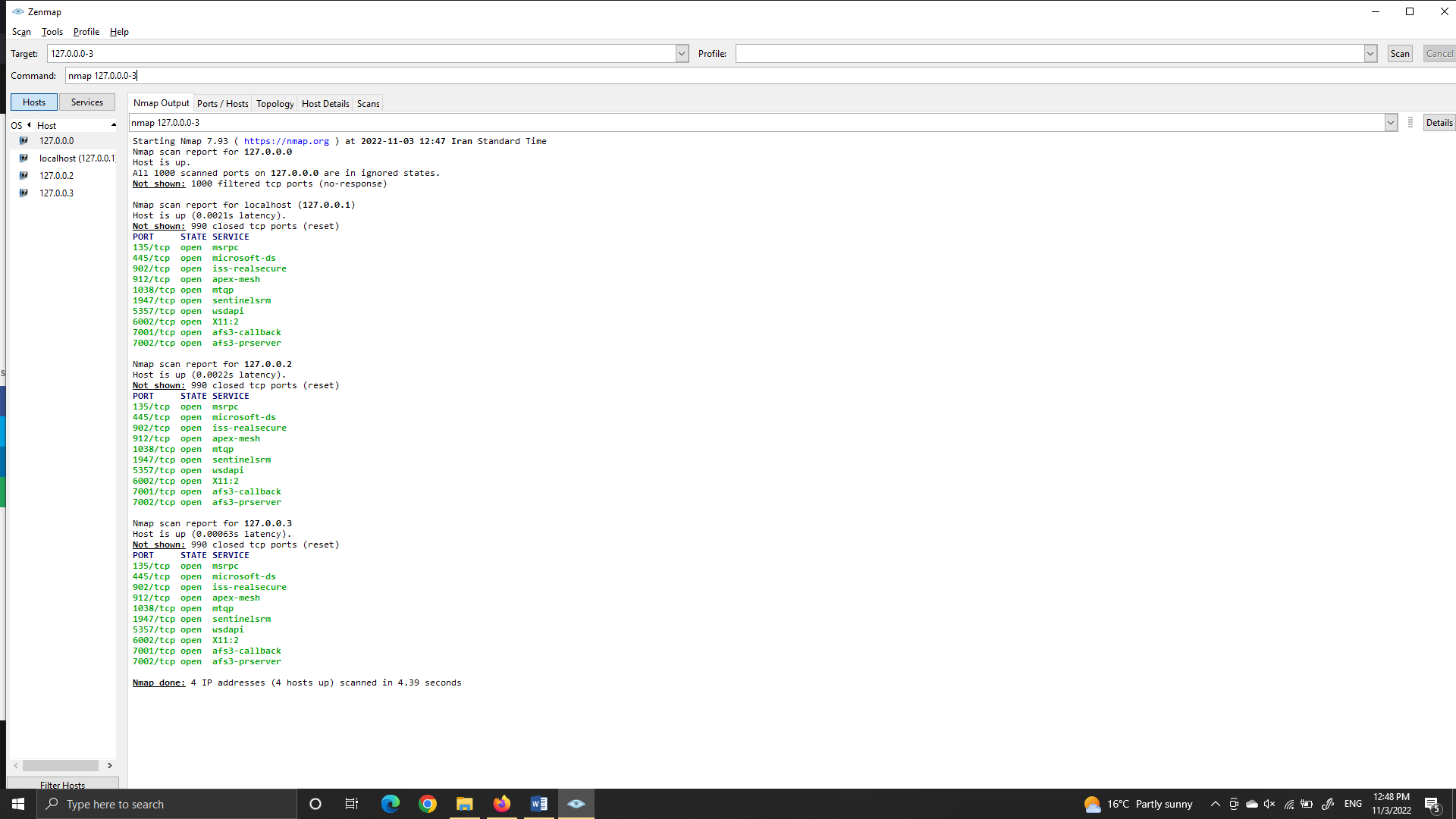
**محتوای فایل Result\_open\_ports**

**گزارش بخش دوم )**

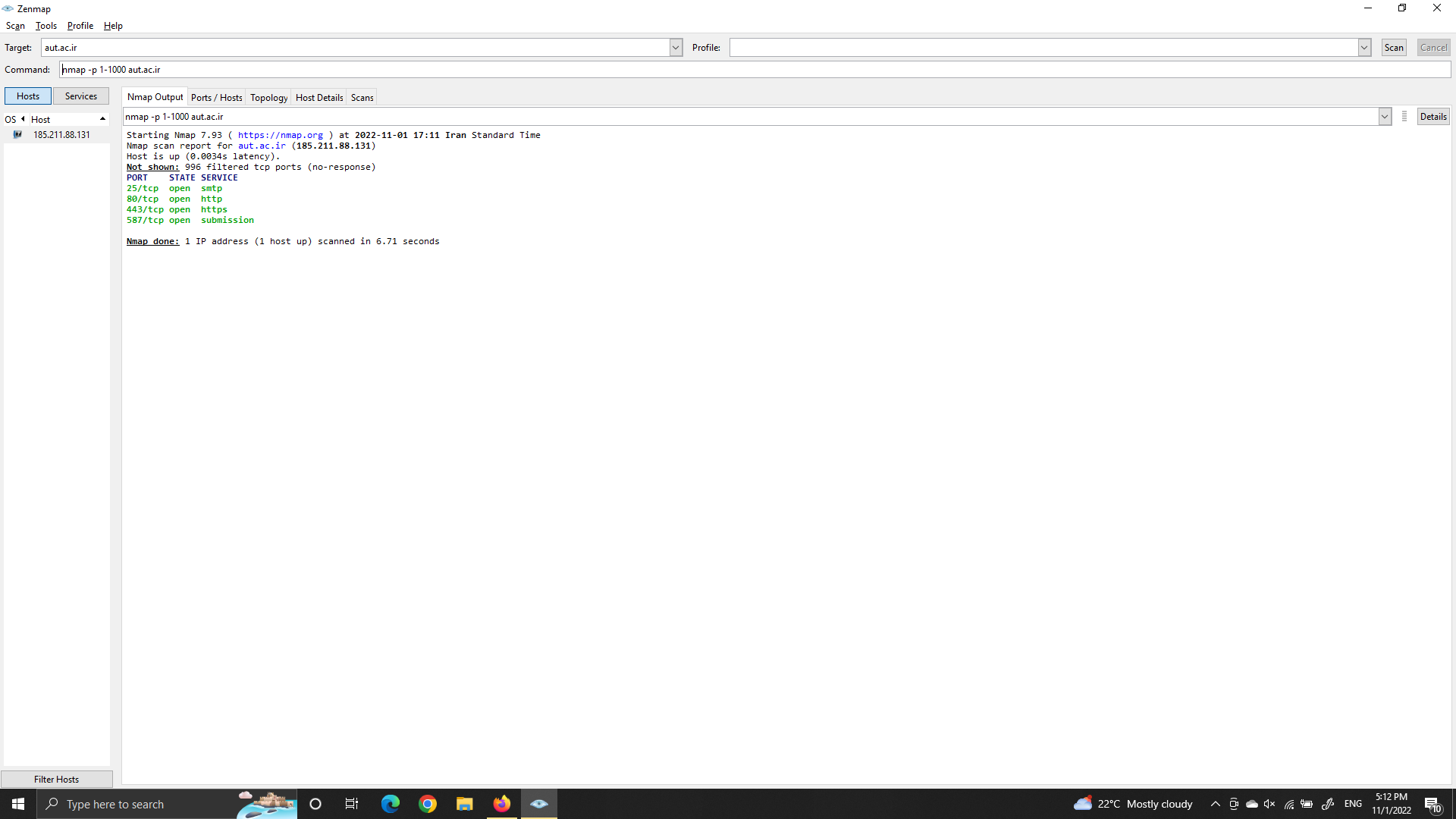
**در این قسمت با استفاده از نرم افزار nmap صحت کارهایی که در بخش اول انجام داده ایم را با استفاده از اسکرین شات های زیر بررسی می کنیم :**

****

**صحت گرفتن ping از یک آی پی خاص**

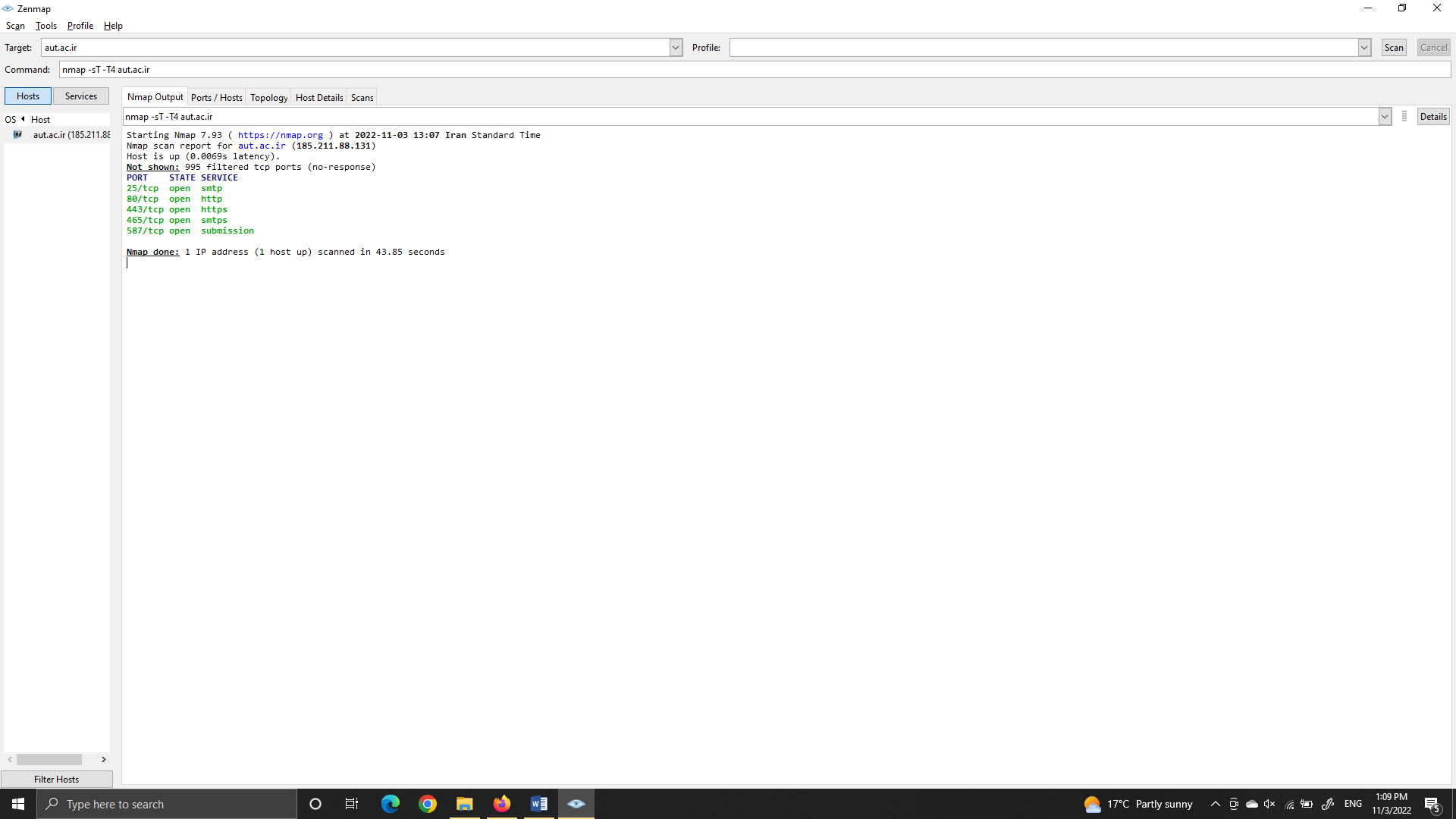
****

**صحت یافتن هاست های فعال یک ip range**

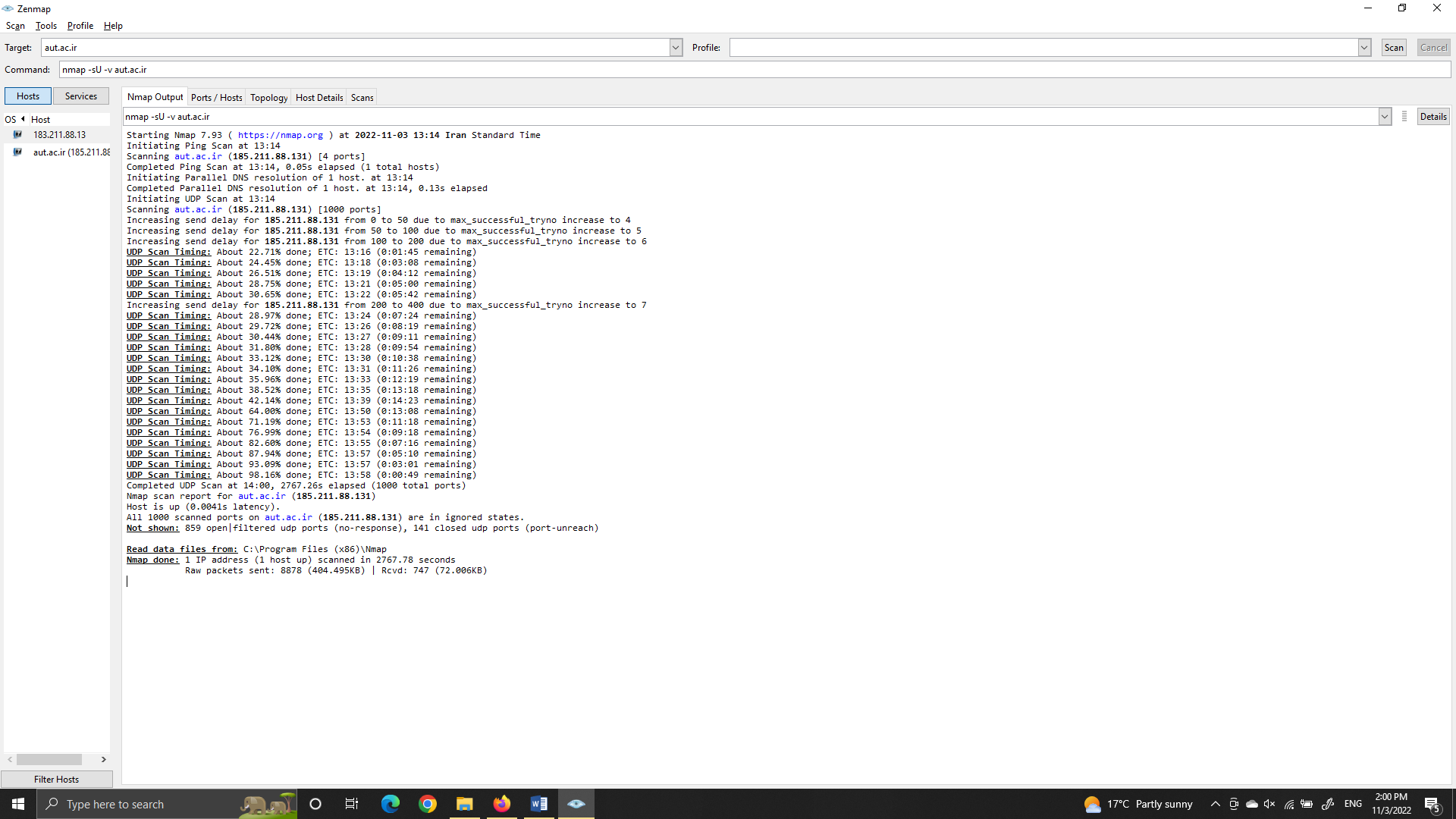
****

**یافتن پورت های باز یک هاست**

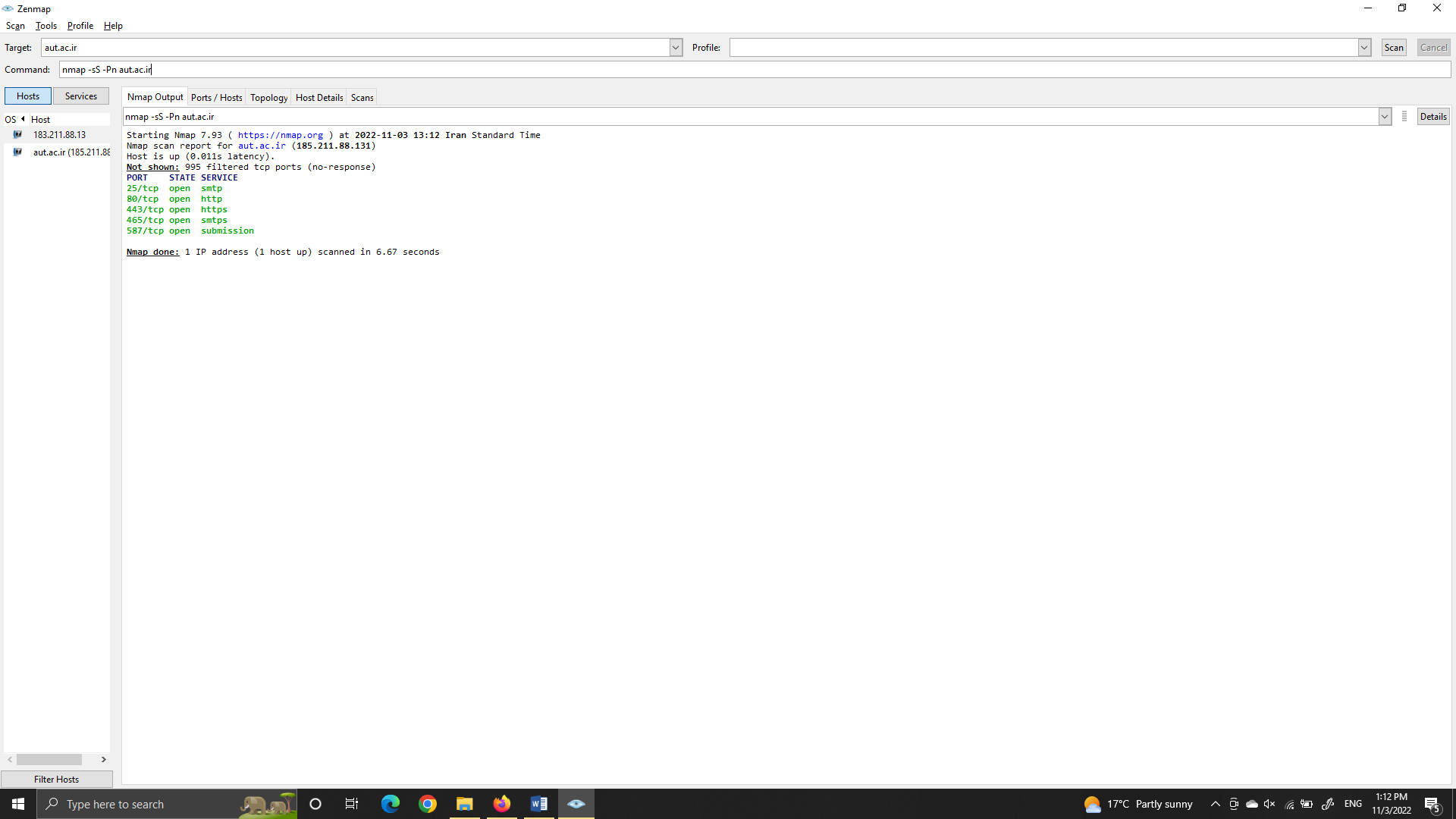
**دستورات خواسته شده برای اجرا در nmap :**

****

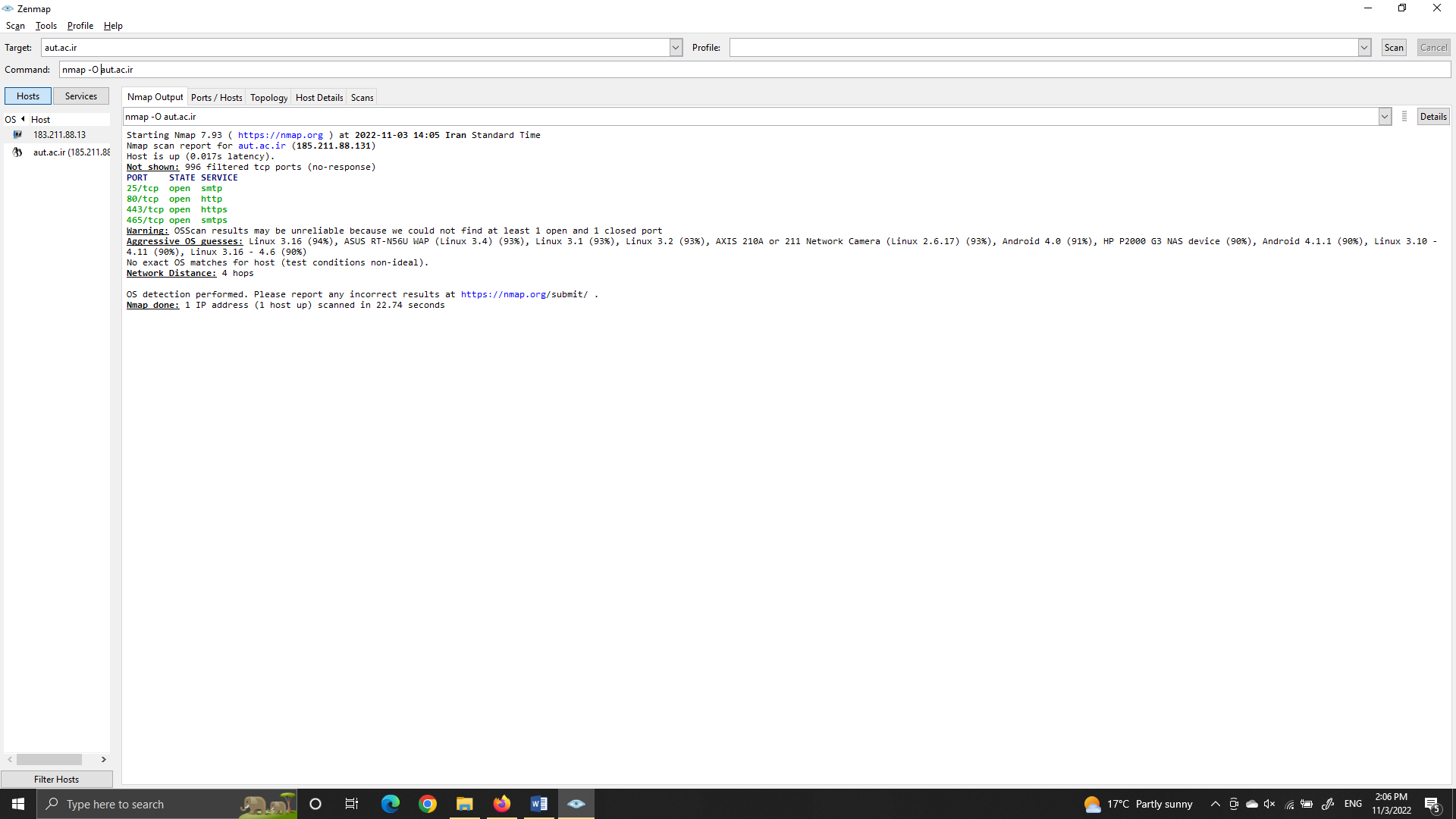
**TCP Full Scan**

****

**UDP Full Scan**

****

**Stealth Scan**

****

**Fingerprint (OS) scan**