گزارش تمرین پروژه ایریدیوم

علیرضا اسلامی خواه 99521064

محمدرضا صاحب زاده 99521397

1. آشنایی با پروژه و خواسته های آن

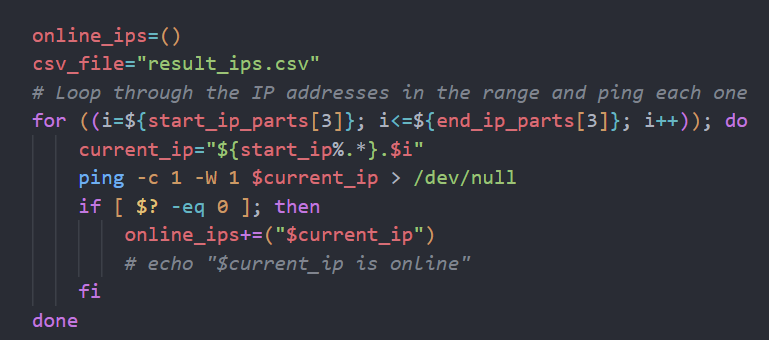
در کل هدف از این پروژه آشنایی با پرتکل ssh و همچنین درک بهتر از فضای امنیت شبکه و کاربرد های لینوکس میباشد.

در ابتدا باید تمام آی پی های بلوک داده شده در شبکه اسکن شوند سپس اطلاعات آنها درون یک فایل csv ریخته میشود در جایی دیگر فایل های مربوطه به آنها فرستاده میشود. در مرحله بعدی این فایل ها در سیستم هدف اجرا شده و اطلاعات شخص قربانی توسط یک API به یک سامانه فرستاده میشود.

در آخر هم باید اطلاعات در دامنه مربوطه نمایش داده شوند.

1. مرحله اول : شناسایی بلوک شبکه ای موجود و اسکن کردن آی پی های آنلاین

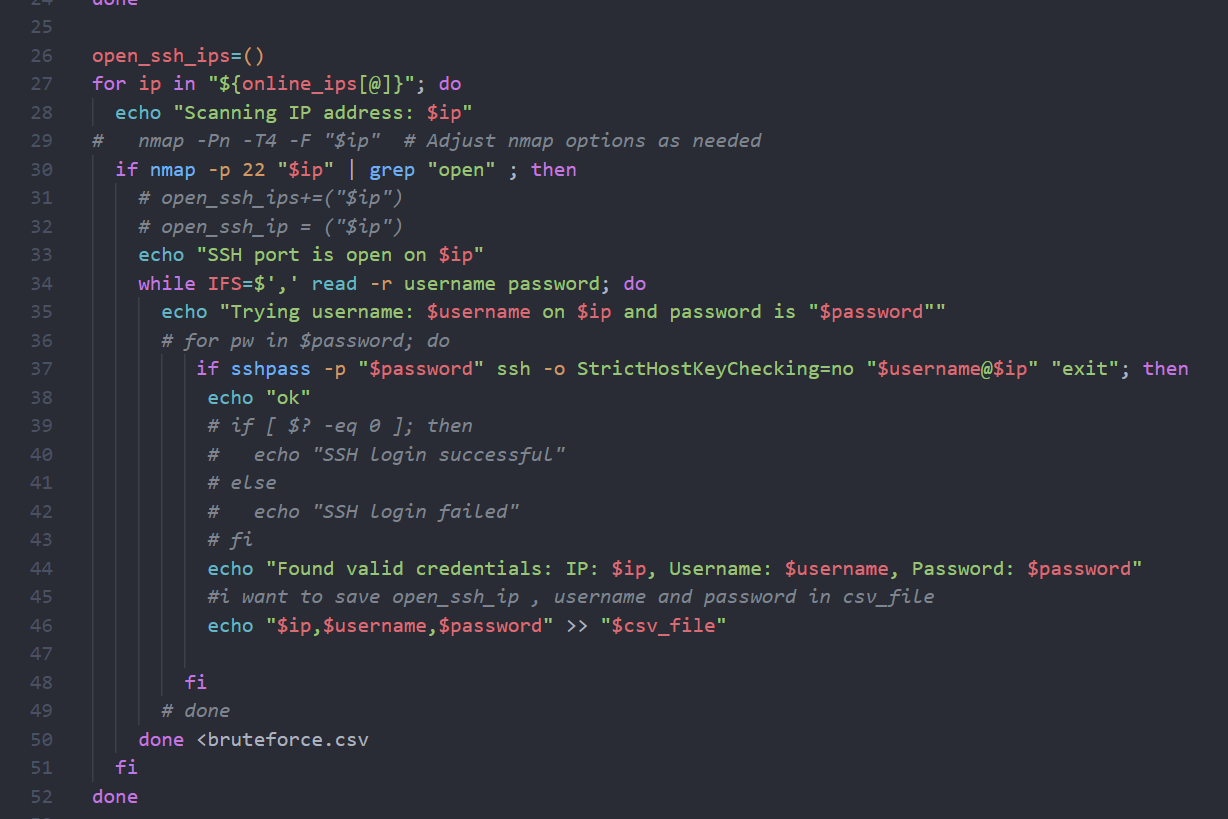
در اینجا ما از کاربر بازه آی پی های مدنظرش را گرفته و برای مشخص کردن ملاک درست برای آنلاین بودن آنها به تمامی آنها پینگ میزنیم.



سپس با استفاده از nmap مشخصا پورت 22 آنها را که مخصوص ssh میباشد را به منظور باز بودن یا نبودن تست میکنیم.

ما از قبل یک فایل csv به نام bruteforce.csv داشتیم که تعدادی یوزرنیم و پسورد رندوم در آنها قرار دارد.

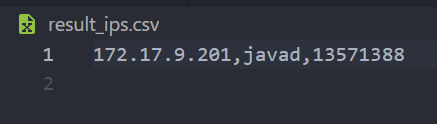
اینجا تمامی اینها را روی آی پی های مشخص شده و پورت ssh آنها تست کرده و متوجه میشویم که یوزنیم و پسورد کدام یکی از آنها را داریم.



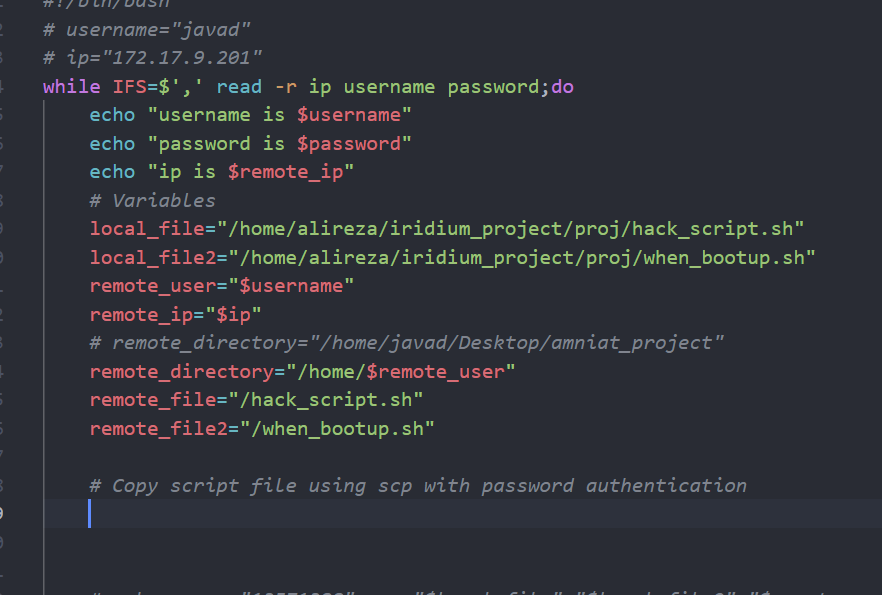
در خط 30 مشخصا پورت 22 را مورد هدف قرار میدهیم و پایین تر با دستور sshpass پورت را تست میکنیم.

1. مرحله اجرایی : فرستادن فایل و اجرای آن

نتایج بدست آمده در مرحله قبل را که در فایل result\_ip.csv ذخیره کرده بودیم را برای استفاده مجدد بکار میگیریم.

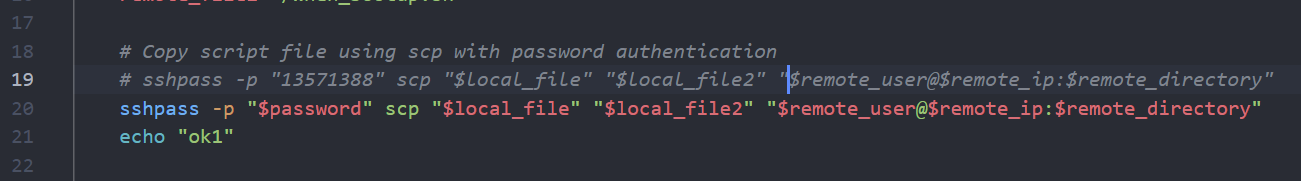


در فایل send bash file 2 دیتاها را از فایل خوانده و یک سری متغیرها تعریف میکنیم.

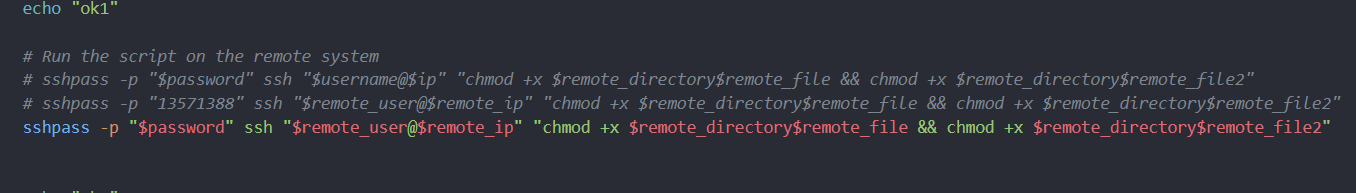


مثلا محل ذخیره سازی فایل های ما یا دیرکتوری ذخیره سازی فایل در سیستم هدف تعریف شده اند.

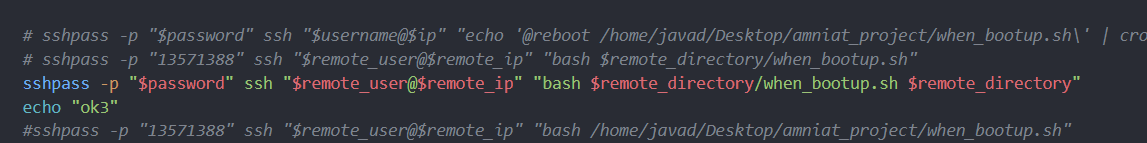
در مرحله بعد نوبت به فرستادن فایل ها میرسد که با دستور زیر تعریف شده است.



و سپس اجرای آنها :

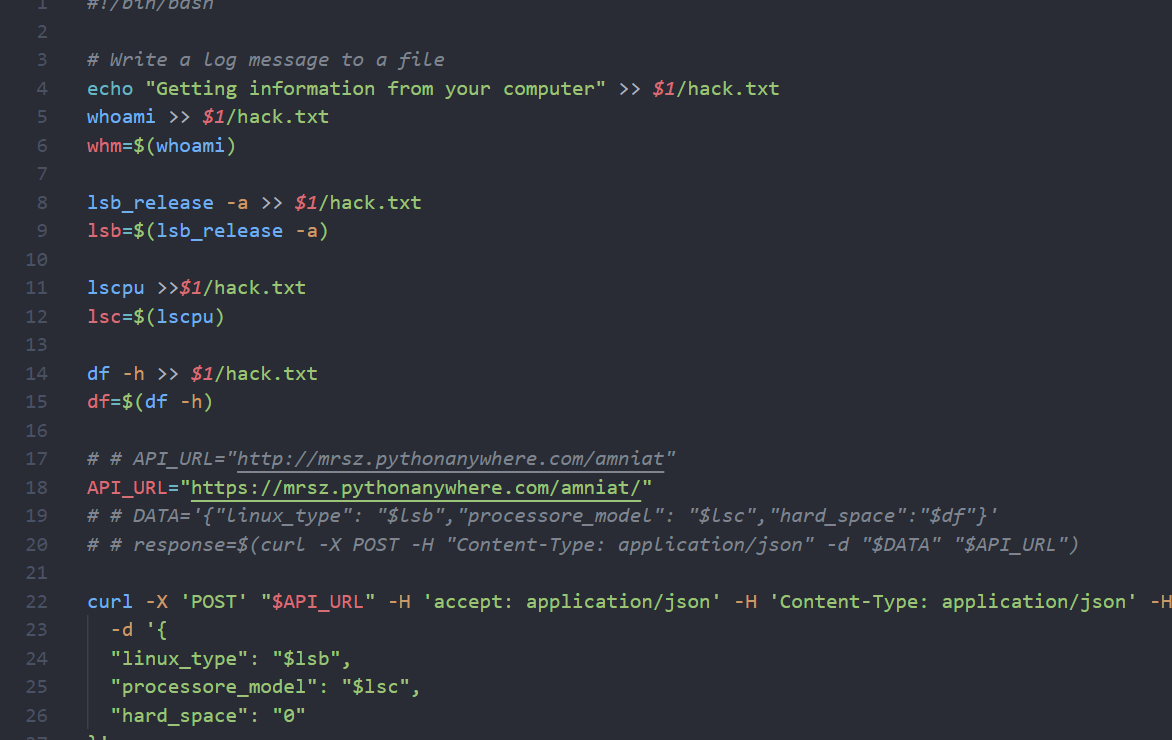


و در آخر when boot up رو در همان لحظه اجرا میکرد .



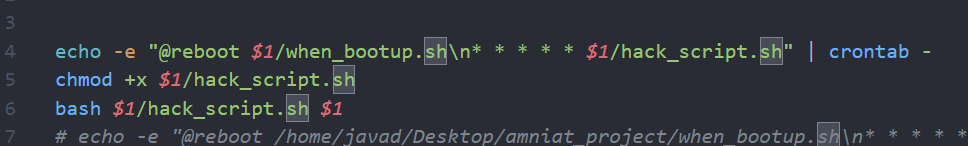
1. بررسی فایل های جانبی :
   1. فایل hack\_script.sh :

این فایل بعد از ذخیره شدن در سیستم هدف وظیفه تست کردن یکسری دستورات و ذخیره سازی آنها : ابتدا در یک فایل txt و سپس فرستادن آنها به یک api مشخص را دارد.



* 1. فایل when\_bootup :

در این فایل دو وظیفه وجود دارد ، اول اینکه با هر بار روشن شدن سیستم گزارشات مبنی بر آن را به سرور و فایل بفرستد. دوم اینکه در یک بازه مشخص همین کارها را تکرار کند.



1. ذخیره سازی و نمایش اطلاعات بدست آمده در یک سرور جداگانه :

با استفاده از api ای که قبلا شرح داده شد اطلاعاتی از قبیل ورژن سیستم عامل ، حافظه باقیمانده و مدل پردازنده پردازش میشود.

نمونه ای از فضای API مربوطه :

