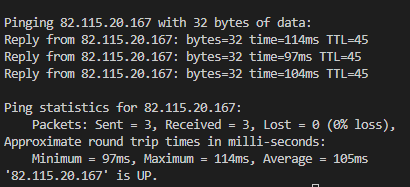
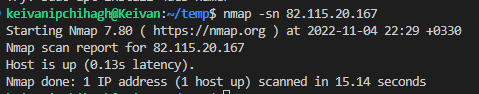
# بخش اول و دوم

* فایل README.md برای اجرای صحیح کد های Python و bash اسکریپت ها قرار داده شده است. (نوع ورودی گرفتن اسکریپت ها تغییر کرده!)
* خروجی های کد در فایل های با پسوند .txt قرار داده شده اند.
* اسکرین شات ها رو فایل های با پسوند .png قرار داده شده اند.

## Ping

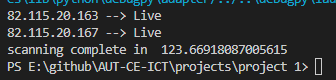


خروجی هر دو اسکریپت نوشته شده با Python و Bash مطابقت داشت که دستور nmap را اجرا میکرد. خروجی nmap:



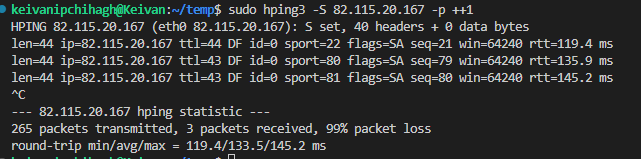
## IP Range

تصویر بالا مربوط به این [سایت](http://ports.my-addr.com/ip-range-port-scanner-tool.php) است که برای IP های داده شده ۲ IP باز پیدا کرده که سرور با IP 82.115.20.167 برا من است.

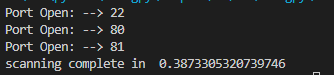


تصویر بالا مربوط به اجرای کد Python است که با اتصال socket به پورت 80 آدرس های داده شده، آن ها را چک میکند. همانطور که مشاهده می شود خروجی این دو با یکدیگر مطابقت دارد.

## Port Scanner

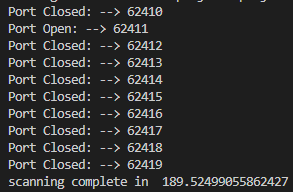


تصویر بالا مربوط به خروجی hping3 است که برای 82.115.20.167 سه پورت 22، 80 و 81 را باز یافته است.



تصویر بالا مربوط به خروجی کد Python که بوسیله باز کردن socket کار میکند است، همانطور که مشاهده میشود سه پورت 22، 80 و 81 را باز یافته است. (برای سرعت یافتن فرایند لیست ۵ پورت را تست کردیم)

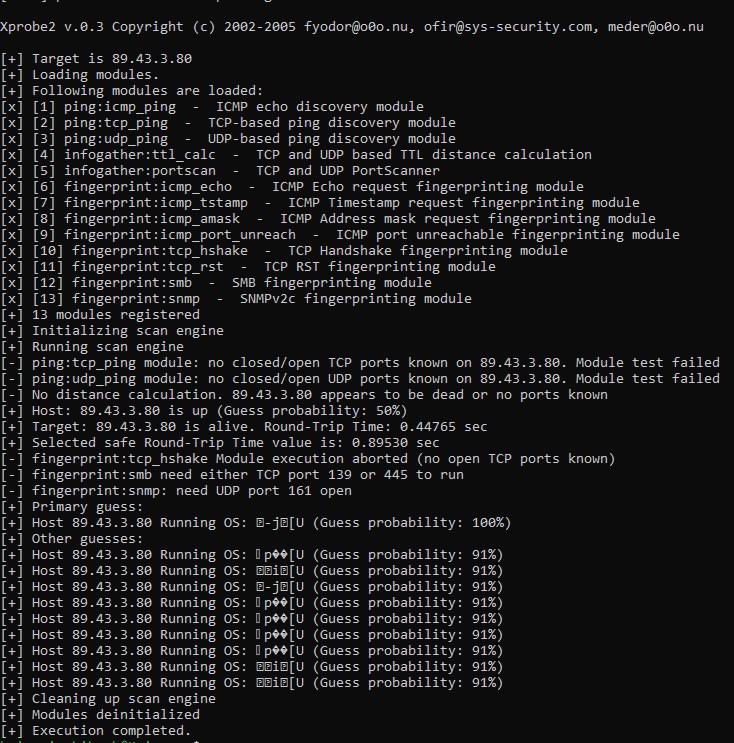
خروجی هر دو اسکریپت نوشته شده با Python و Bash مطابقت داشت. در Bash از hping3 و در Python از socket استفاده شده است.



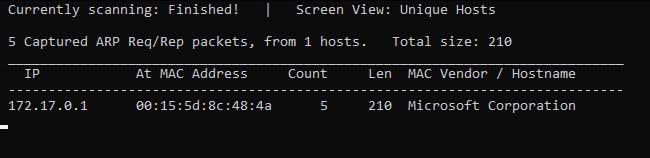
برای اطمینان از کارکرد صحیح کد، پورت 62411 توسط من برای IP به عنوان 82.115.20.167 باز شد. تصویر بالا مربوط به اجرای کد Python برای این IP است. ابزار hping3 نیز این پورت را تایید کرد.

توضیح حالت های nmap برای اتصال:

* TCP full scan: زمانی است که TCP three-way handshake به کاملی اجرا شود تا باز یا بسته بودن پورت برسی شود.
* Stealth scan: در این حالت از آنجایی که اتصال TCP هیچگاه به شکل کامل برقرار نمیشود (نیازی به این امر نیست) پس میتوان تعداد زیادی پورت را در هر ثانیه چک کد. این حالت معروف ترین حالت اسکن است.
* UDP scan: در این حالت بسته UDP به جای TCP ارسال می شود که معمولا payload ندارد.
* Fingerprint scan: این حالت برای فهمیدن سیستم عامل IP مورد نظر است که با ارسال درخواست به برخی پورت های باز انجام میشود.
* Idle scan: در این حالت درخواست مستقیم از ماشین حمله کننده ارسال نمیشود، بلکه از دستگاه دیگری که معمولا zombie فراخوانده میشود ارسال میشود تا هویت حمله کننده محفوظ بماند.



خروجی دستور xprobe2 89.43.3.80



خروجی دستور sudo netdiscover -i eth0 -r 89.43.3.80/16

لینک های استفاده شده:

http://ports.my-addr.com/check-all-open-ports-online.php