دانشکده مهندسی کامپیوتر

پروژه ایریدیوم درس امنیت سیستم‌های کامپیوتری

گردآورندگان: مهدی قضاوی - ۹۹۵۲۲۰۱۴ احسان احمدپور - ۹۹۵۲۱۰۱۹

نیم‌سال دوم

سال تحصیلی ۱۴۰۲-۱۴۰۳

۱.۰ مقدمه

در این پروژه قصد داریم بدافزار میرای (Mirai) را شبیه‌سازی کنیم. میرای با دسترسی به تعداد کثیری از سیستم‌ها و ارسال درخواست DNS، Dyn سرورها را از کار می‌انداخت و باعث قطع دسترسی بسیاری از وبسایت‌های معروف دنیا می‌شد.

هدف این پروژه ساخت برنامه‌ای است که پورت‌های باز موجود در شبکه که ssh در آن‌ها اجرا می‌شود را پیدا کند و سپس با تست کردن رمز عبورهای معروف که در تعداد زیادی از دستگاه‌ها استفاده می‌شوند به این سیستم‌ها دسترسی پیداکرده و با پیاده‌سازی یک بدافزار روی آن‌ها اطلاعات امنیتی این سیستم‌ها را به یک سرور مشخص ارسال کند.

۲.۰ ساختار شبکه

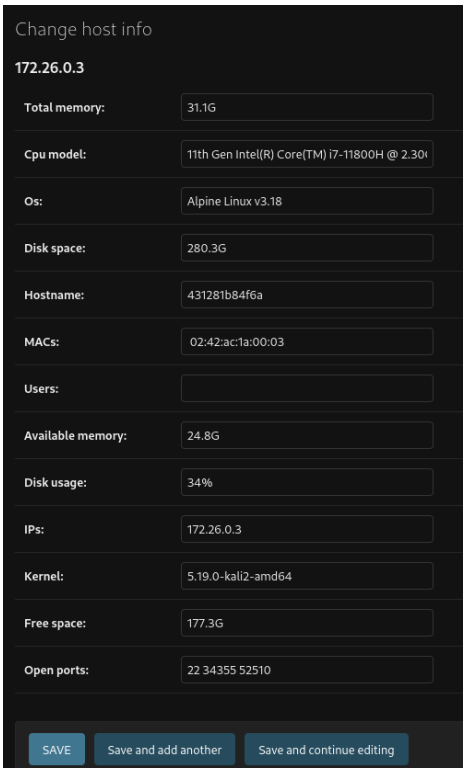
در این پروژه با استفاده از داکر یک شبکه ایجاد کرده و تعدادی کانتینر به آن اضافه کرده و درنهایت یک حمله را در این شبکه شبیه سازی کرده‌ایم.

این شبکه دارای سه نوع image است: وب‌سرور، حمله‌کننده و سرور هدف. برای هر image یک Dockerfile پیاده‌شده که از imageهای سرورهدف چند و از imageهای سیستم‌های وب‌سرور و حمله‌کننده تنها یک کانتینر ایجاد می‌شوند.

۳.۰ وب‌سرور

از این وب سرورکه با جنگو پیاده سازی‌شده برای اهداف مختلفی مانند ارسال اطلاعات امنیتی جمع آوری شده از سیستم‌های مورد حمله قرار گرفته و ارسال به این سرور و ذخیره اطلاعات در این دیتابیس و دانلود بدافزار توسط سیستم های قربانی از این سرور استفاده می‌شود.

اسکریپت infocrawler.sh در این وب سرور ذخیره‌شده‌است که روی سیستم مورد هدف دانلود شده و اطلاعات امنیتی سیستم هدف را به صورت json به وب‌سرور ارسال میکند.



شکل ۱: نمونه اطلاعات استخراج شده از سیستم هدف

۴.۰ Image Attacker

برای حمله به سیستم‌های قربانی یک attacker image ساخته‌شده است. سه فایل موجود در این ایمیج hack.sh، userpass.csv و scan.sh می‌باشند.

اسکریپت hack.sh با خواندن openports.csv به پورت های ssh پیدا شده حمله کرده و رمزعبورهای معروف با Brute-force تست کرده و در صورت اتصال، بدافزار را از وب سرور بر روی سرور قربانی دانلود و اجرا می‌کند.

فایل userpass.csv دارای usernameها و passwordهای معروف و پرتکرار می‌باشد و در حمله به ssh استفاده می‌شود.

اسکریپت scan.sh هاست‌های فعال در رنج ورودی را تست‌کرده و پورت‌های باز آن‌ها را پیدا می‌کند

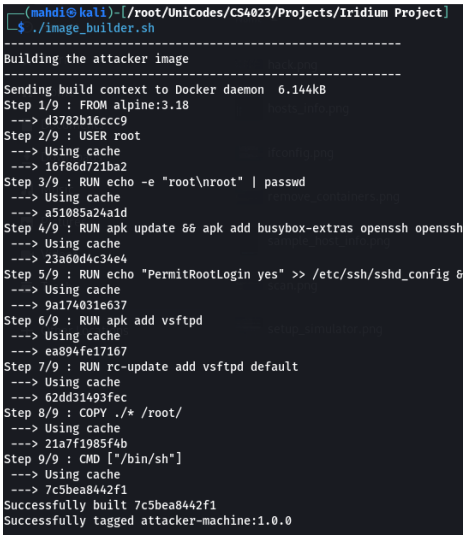
که درنهایت اطلاعات پیداشده را در فایل openports ذخیره می‌کند.

۵.۰ سرور هدف

imageهای سرورهای هدف که مورد حمله قرار می‌گیرند روی لینوکس alpine قرار گرفته اند تا سبک باشند.

۶.۰ اجرای حمله

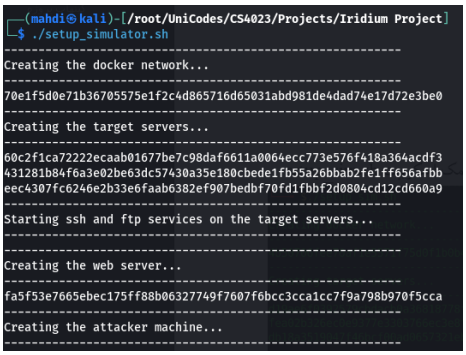
ابتدا با اسکریپت buildimages.sh شبکه را راه‌اندازی می‌کنیم و imageها را می‌سازیم و سپس اسکریپت setupsimulator.sh را برای اجرا کردن کانتینرها اجرا می‌کنیم. برای مشاهده دیتابیس، می‌توان به پورت 8000 و قسمت ادمین مراجعه کرد (127.0.0.1:8000/admin ، نام کاربری و پسورد : superuser:superuser)



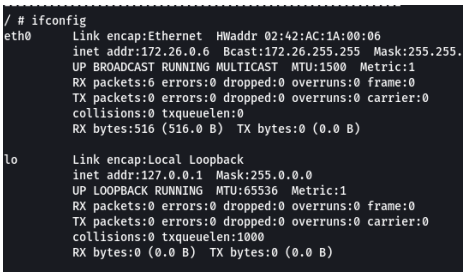
شکل ۲: راه‌اندازی imageها

۷.۰ حمله به سیستم‌های هدف

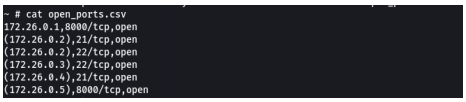
ابتدا ادرس network شبکه داکر که کانتینرها در آن در حال اجرا هستند را پیدا کرده و سپس با اجرای فایل scan.sh نتایج مورد نظر در فایل openports.csv ذخیره می‌شوند. سپس با اجرای hack.sh حمله آغاز می‌شود و در هر دقیقه یک بار اطلاعات امنیتی سیستم های هدف در دیتابیس ذخیره می‌شوند.



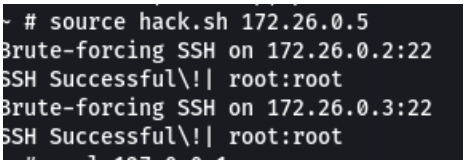
شکل ۳: اجرای کانتینرها



شکل ۴: اسکن‌کردن شبکه



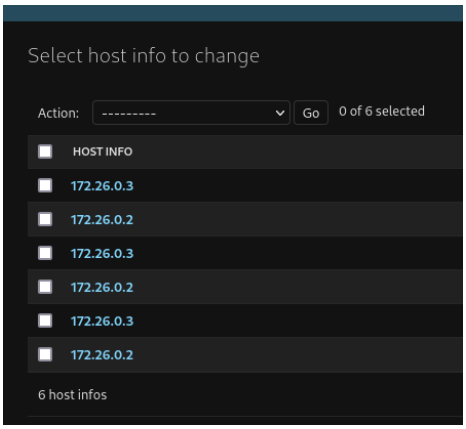
شکل ۵: پورت‌های باز پیداشده



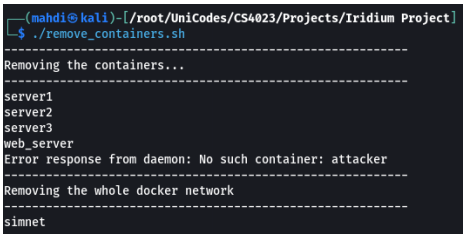
شکل ۶: اجرای اسکریپت hack

۸.۰ پایان حمله

در نهایت با استفاده از اسکریپت removecontainers.sh کانتینرهای در حال اجرا را متوقف کرده و شبکه داکر را حذف می‌کنیم.



شکل ۷: هاست‌های ذخیره‌شده در دیتابیس



شکل ۸: حذف کانتینرها و پایان حمله

۹.۰ داکرهاب و گیت‌هاب

Image هریک از بخش‌های پروژه در در این لینک و کد پروژه پیاده‌شده در این لینک گیت‌هاب قرار دارند.