بسمه تعالی

آزمایشگاه امنیت شبکه

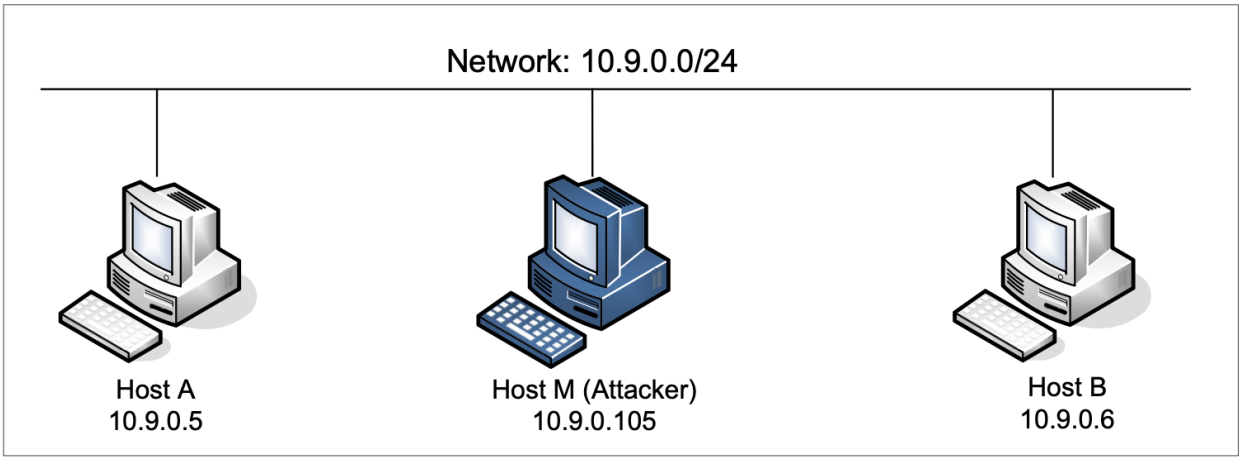
دانشکده برق و کامپیوتر

دانشگاه صنعتی اصفهان

دکتر فانیان

دستورکار جلسه دوم

آماده‌سازی اولیه:



فایل این آزمایشگاه را Extract و در مسیر باز شده Terminal خود را باز کنید و دستور زیر را اجرا کنید:

```
sudo docker compose up -d
```

در صورتی که از نسخه‌های قدیمی‌تر Docker Compose استفاده می‌کنید بجای docker compose از عبارت docker-compose استفاده کنید. اگر نیاز به ساخت مجدد کانتینرها و imageها دارید دستور زیر داکر را مجبور به ساخت مجدد می‌کند:

```
sudo docker compose up --force-recreate --build -d
```

دستور بالا تا حدی این اطمینان را می‌دهد که داکر از لایه‌های Cache شده قبلی استفاده نمی‌کند.

همانطور که از توپولوژی این آزمایشگاه مشخص است ما سه دستگاه داریم که هر کدام دارای کانتینری مجزا هستند و هر سه دستگاه از شبکه داخلی داکر استفاده می‌کنند کار اصلی ما با کانتینر Attacker است برای دسترسی به محیط Shell این کانتینر ابتدا دستور زیر را اجرا کنید:

```
sudo docker compose ps --format "table {{.ID}}\t{{.Name}}"
```

دستور بالا اسم هر کانتینر و ID مختص بهش را نمایش می‌دهد، با کمک این IDها می‌توان به Shell هر کدام دسترسی داشت.

برای دسترسی به محیط Shell هر یک از کانتینرها دستور زیر را اجرا کنید:

```
sudo docker exec -it <container-id> bash
```

این دستور Shell کانتینر مدنظر با دسترسی root به ما می‌دهد. توصیه می‌شود که به تعداد کانتینرهای موجود تب Terminal باز کنید و در هر تب دستور بالا را اجرا کنید.

درمورد کانتینرها:

ساختار کانتینرها شامل یک فولدر به اسم volume است که بین سیستم و کانتینر Attacker مشترک است از این فولدر برای انتقال کدها به کانتینر Attacker استفاده کنید.
در این آزمایشگاه کانتینر Attacker نیاز دارد که پارامترهای سیستمی را تغییر دهد، بصورت عادی داکر امکان اینگونه عملیات‌ها را به کانتینرها نمی‌دهد برای دسترسی به این موارد پارامتر privileged ست شده که امکان استفاده از sysctl را داخل کانتینر Attacker به ما می‌دهد.

مشاهده و عیب‌یابی بسته‌ها:

در این آزمایشگاه بسیار مهم است که بسته‌هایی را که ارسال می‌کنیم مشاهده کنیم و در صورت وجود ایراد، عیب‌یابی کنیم برای این کار می‌توانیم از Wireshark و یا tcpdump استفاده کنیم برای استفاده از tcpdump در هر یک از کانتینرها دستور زیر را وارد کنید:

```
tcpdump -i <interface-name> -n
```

با اجرای دستور بالا امکان دیدن بسته‌ها وجود دارد.

تمرین‌ها:

تمرین 1:

تمامی بخش‌های زیر را در دو سناریو انجام دهید:

1. آدرس IP کانتینر B داخل ARP Cache کانتینر HostA وجود دارد.
2. آدرس IP کانتینر B داخل ARP Cache کانتینر HostA وجود ندارد.(برای حذف رکورد از جدول ARP دستور arp -d <ip-address> را اجرا کنید یا اینکه با دستور ip -s -s neigh flush all کل Cache را پاک کنید.

الف) با کمک Scapy برنامه‌ای بنویسید که آدرس IP کانتینر HostB به آدرس MAC کانتینر HostM یا همان Attacker ترجمه شود، دقت کنید که نوع بسته ARP ای که ارسال می‌کنید باید از نوع Request باشد.(برای صحت درستی حمله در کانتینر HostA دستور arp -n را اجرا کنید)

ب) دقیقا همان کار بخش **الف** را انجام دهید اما بسته ARP از نوع Reply باشد.(تفاوت را بیان کنید و بگویید که نوع Reply در چه صورتی تاثیر گذار بود)

ج) دقیقا کاری مشابه بخش‌های **الف و ب** را انجام دهید ولی بسته ARP gratuitous message ارسال کنید.(این بسته از نوع Request است ولی برای آپدیت کردن همه نودهای شبکه است)

تمرین 2:

گام اول) حمله ARP Cache Poisoning را روی دو کانتینر HostA و HostB اجرا کنید.

```
sysctl net.ipv4.ip_forwarding=0
```

گام دوم) دستور زیر را در کانتینر HostM یا همان Attacker اجرا کنید:

از یکی از HostA یا HostB دیگری را پینگ بگیرید و نتایج را با Wireshark یا tcpdump بررسی کنید.

گام سوم) دستور زیر را در کانتینر HostM یا همان Attacker اجرا کنید:

```
sysctl net.ipv4.ip_forwarding=1
```

از یکی از HostA یا HostB دیگری را پینگ بگیرید و نتایج را با Wireshark یا tcpdump بررسی کنید.

گام چهارم) در این گام باید که با استفاده از ARP Cache Poisoning حمله MiTM روی ارتباط Telnet دو کانتینر HostA و HostB انجام دهید و کاری کنید که ارتباط Telnet از کانتینر HostM عبور کند. رفتار Telnet به این گونه است که با تایپ هر کاراکتر یک بسته TCP ساخته می‌شود و ارسال می‌شود، بعد از موفقیت آمیز بودن حمله هر کاراکتری که تایپ می‌شود باید با **کاراکتر 'Z' جایگزین شود.**

راهنمایی‌ها:

1. کانتینر HostA را Client و کانتینر HostB را Server ارتباط Telnet در نظر بگیرید همچنین اینکه نام کاربری "seed" و رمزعبور "dees" است. دقت کنید که بسته‌هایی که از سمت HostA به HostB می‌روند را باید تغییر دهید و برعکس آن را نیاز به تغییر آن نیست.
2. برای موفقیت‌آمیز بودن حمله ابتدا در کانتینر HostM ویژگی ip_forwarding را روشن کنید و ارتباط اولیه Telnet را برقرار کنید بعد از برقراری ارتباط ip_forwarding را خاموش کنید.
3. ARP Cache مدت زمان محدودی اعتبار دارد برای بالا بردن شانس موفقیت برنامه‌ای که کار ARP Cache Poisoning را انجام می‌دهد را داخل یک حلقه بی‌نهایت قرار دهید و کنار برنامه حمله MiTM اجرا کنید.(می‌توانید دو Shell مجزا به کانتینر HostM متصل کنید و کد هر حمله را در هر Shell بصورت مجزا اجرا کنید، در صورت استفاده از Thread در پایتون نمره امتیازی خواهید گرفت)
4. برای ساخت بسته جدید از تکه کد زیر می‌توانید استفاده کنید:

```
...
newpkt = IP(bytes(pkt[IP]))
del(newpkt.chksum)
del(newpkt[TCP].chksum)
del(newpkt[TCP].payload)
...
```

برای ساخته بسته جدید نیاز است که Checksum های بسته قبلی را پاک کنیم نیاز به تولید Checksum جدید نیست.

5. برای بررسی کد حمله هنگام تایپ کاراکترها سعی کنید که به آرامی تایپ کنید در غیر اینصورت ممکن است ارتباط Telnet کاملا Freeze کند.

تمرین 3:

این تمرین مشابه تمرین 2 است ولی باید حمله MiTM را برای ارتباط Netcat اجرا کنید عملکرد Netcat کمی متفاوت است و بعد از وارد کردن هر خط کاراکتر بسته جدید می‌سازد، بعد موفقیت آمیز بودن حمله شما باید حرف اول خط داده شده را بردارید و به تعداد حروف داخل خط آن را تکرار کنید، دقت کنید که طول رشته جایگذاری شده باید برابر با طول رشته قبلی باشد.