زمستان ۱۳۹۷

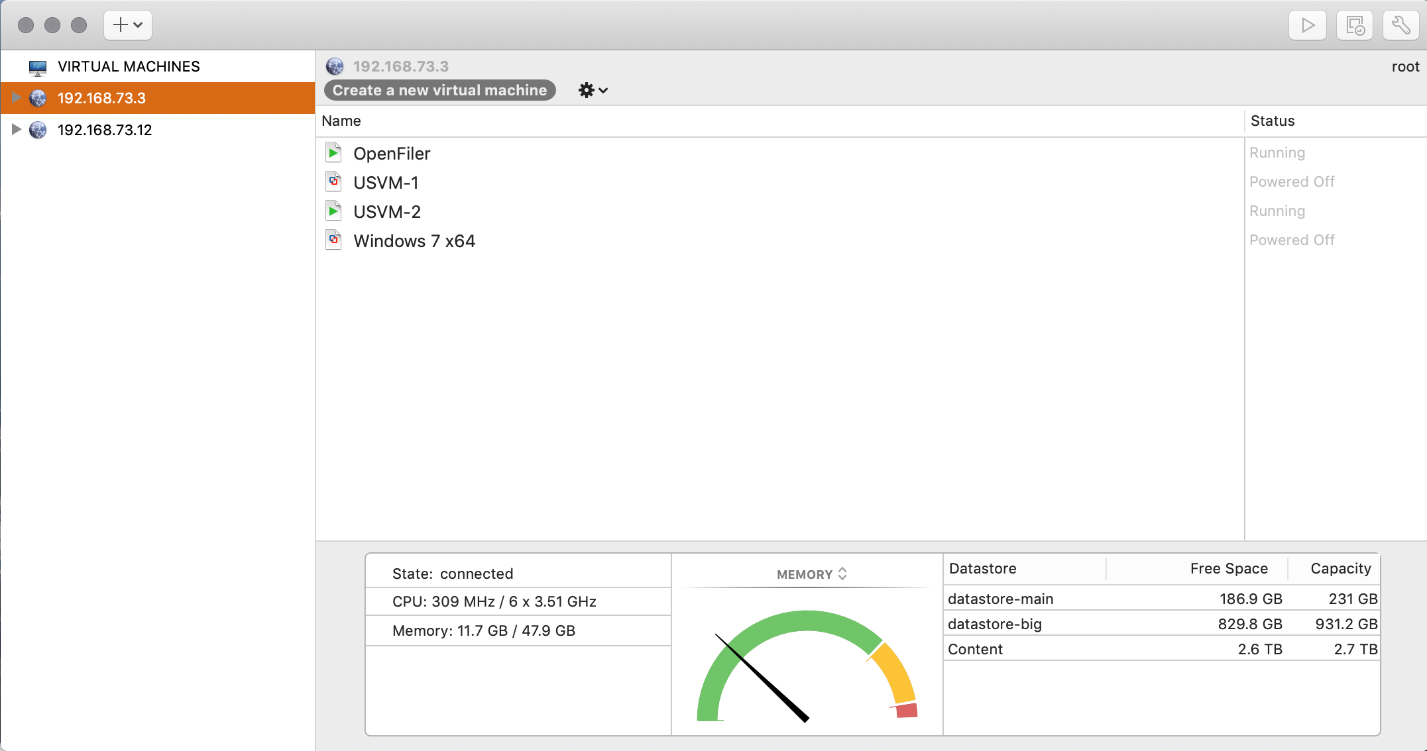
پرهام الوانی

۹۶۱۳۱۱۱۲

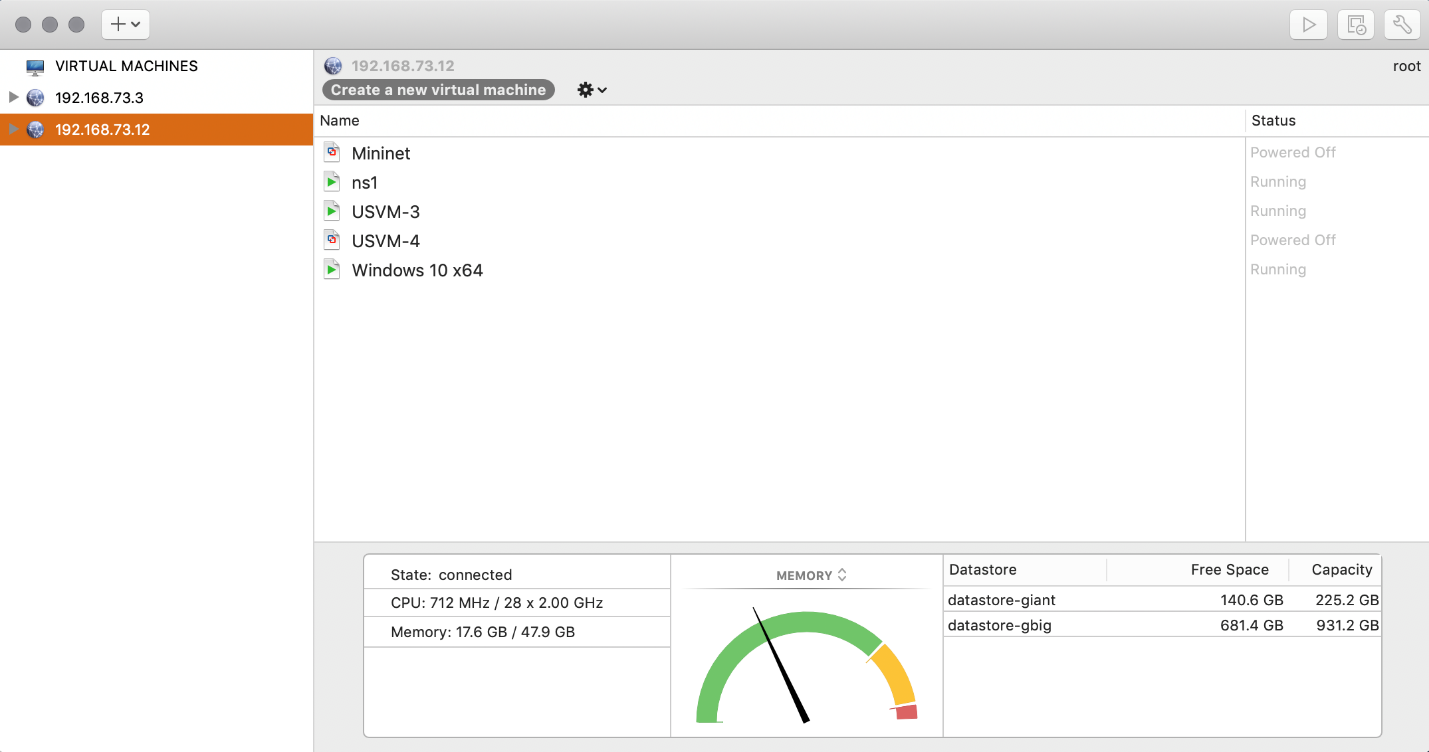
تمرین اول

امنیت شبکه

همبندی شبکه شامل دو سرور سخت‌افزاری است که بر روی هر یک VMWare EXSi 6.7 نصب شده است و یک ماشین Ubuntu 18.04 نیز بر روی آن‌ها وجود دارد.



شکل 1 سرور فیزیکی اول



شکل 2 سرور فیزیکی دوم

بر روی یکی از این ماشین‌ها با استفاده از دستور زیر یک سرور TCP روی پورت 3000 بالا آورده شده است:

nc -l -p 3000

ابزار nc یا netcat یکی از ابزارهایی است که می‌توان از آن برای عیب‌یابی شبکه استفاده کرد. در دستور فوق پرچم l مفهوم listening را نشان داده و پرچم p مفهوم پورت را نشان می‌دهد.

در ادامه با استفاده از telent یک کلاینت tcp می‌باشد از روی ماشین دیگر به پورت 3000 ماشین اول متصل می‌شویم:

telnet 192.168.73.5 3000

برای capture کردن بسته‌ها از دستور tshark که cli برنامه محبوب wireshark می‌باشد استفاده می‌کنیم.

tshark -f “not port 22” -i ens192 -F pcap -P -w file.pcap

در دستور فوق بسته‌های کارت شبکه ens192 را بدون در نظر گرفتن بسته‌هایی که با پورت 22 (پورت ssh) ارسال می‌شوند capture می‌کنیم و آن‌ها را با فرمت pcap در فایل file.pcap ذخیره می‌کنیم.

اگر از روی ماشین 192.168.73.6 به یک پورت بسته ماشین 192.168.73.5 متصل شویم پیام‌های زیر رد و بدل می‌شوند:

57 23.910132 192.168.73.6 → 192.168.73.5 TCP 74 39404 → 23 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK\_PERM=1 TSval=2561801316 TSecr=0 WS=128

58 23.910186 192.168.73.5 → 192.168.73.6 TCP 54 23 → 39404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

یک پیام SYN برای ایجاد ارتباط با پورت 23 ماشین 192.168.73.5 از یک پورت تصادفی (39404) ماشین 192.168.73.6 ارسال می‌گردد. از آنجایی که پورت 23 روی ماشین 192.168.73.5 باز نمی‌باشد سیستم عامل با یک پیام TCP Reset پاسخ می‌دهد.

اگر از روی ماشین 192.168.73.6 به پورت 3000 که نرم افزار nc روی آن در حال گوش دادن بود از ماشین 192.168.73.5 متصل شویم و متنی را تایپ کنیم پیام‌های زیر رد و بدل می‌شوند.

78 28.719289 192.168.73.6 → 192.168.73.5 TCP 74 47244 → 3000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK\_PERM=1 TSval=2561806125 Tsecr=0 WS=128

79 28.719357 192.168.73.5 → 192.168.73.6 TCP 74 3000 → 47244 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK\_PERM=1 Tsval=2184098846 Tsecr=2561806125 WS=128

80 28.719716 192.168.73.6 → 192.168.73.5 TCP 66 47244 → 3000 [ACK] Seq=1 Ack=1 Win=29312 Len=0 Tsval=2561806125 Tsecr=2184098846

92 34.493881 192.168.73.6 → 192.168.73.5 TCP 92 47244 → 3000 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=26 Tsval=2561811900 Tsecr=2184098846

93 34.493920 192.168.73.5 → 192.168.73.6 TCP 66 3000 → 47244 [ACK] Seq=1 Ack=27 Win=29056 Len=0 Tsval=2184104621 Tsecr=2561811900

133 49.087432 192.168.73.6 → 192.168.73.5 TCP 121 47244 → 3000 [PSH, ACK] Seq=27 Ack=1 Win=29312 Len=55 Tsval=2561826493 Tsecr=2184104621

134 49.087464 192.168.73.5 → 192.168.73.6 TCP 66 3000 → 47244 [ACK] Seq=1 Ack=82 Win=29056 Len=0 Tsval=2184119215 Tsecr=2561826493

147 53.855036 192.168.73.6 → 192.168.73.5 TCP 66 47244 → 3000 [FIN, ACK] Seq=82 Ack=1 Win=29312 Len=0 Tsval=2561831261 Tsecr=2184119215

148 53.855144 192.168.73.5 → 192.168.73.6 TCP 66 3000 → 47244 [FIN, ACK] Seq=1 Ack=83 Win=29056 Len=0 Tsval=2184123983 Tsecr=2561831261

149 53.855353 192.168.73.6 → 192.168.73.5 TCP 66 47244 → 3000 [ACK] Seq=83 Ack=2 Win=29312 Len=0 Tsval=2561831261 Tsecr=2184123983

یک پیام SYN برای ایجاد ارتباط از یک پورت تصادفی (47244) ماشین 192.168.73.5 به پورت 3000 ماشین 192.168.73.6 ارسال می‌گردد که در پاسخ یک SYNACK دریافت می‌کند. در ادامه ماشین 192.168.73.5 یک ACK را به عنوان پاسخ ارسال کرده و با روش دست دادن سه‌گانه ارتباط شکل می‌گیرد. در ادامه ارتباط پیام‌ها منتقل می‌شوند که نکته‌ی اصلی در آن‌ها پرچم PSH یا Push است. این پرچم باعث می‌گردد که داده‌ها مستقیما به لایه کاربرد تحویل داده شوند.

در نهایت با پیام FIN ارتباط بسته می‌شود.