

Task 1. Анализ дампа памяти с помощью утилиты Volatility

1. Смотрим историю bash

```
Администратор: Windows Pow + - X
vagrant@kali:~$ volatility --profile=LinuxUbuntu_4_15_0-72-generic_profilex64 --filename=/vagrant/task1/memory.vmem linux_bash
Volatility Foundation Volatility Framework 2.6
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo apt upgrade
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo apt upgrade
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo apt update
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo apt update
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo reboot
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo reboot
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo apt upgrade
1733 bash 2020-01-16 14:00:36 UTC+0000 rub
1733 bash 2020-01-16 14:00:36 UTC+0000 uname -a
1733 bash 2020-01-16 14:00:36 UTC+0000 AWAVH?#?
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo apt update
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo apt autoclean
1733 bash 2020-01-16 14:00:36 UTC+0000 uname -a
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo apt upgrade
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo reboot
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo apt upgrade
1733 bash 2020-01-16 14:00:36 UTC+0000 sudo reboot
1733 bash 2020-01-16 14:00:41 UTC+0000 chmod +x meterpreter
1733 bash 2020-01-16 14:00:42 UTC+0000 sudo ./meterpreter
vagrant@kali:~$
```

из истории видно, что был запущен **meterpreter** из-под суперпользователя.

2. Ищем pid и адрес памяти meterpreter с помощью команды linux_pslist

```
0xffff8a9db6dc0000 bash 1733 1724 1000 1000 0x0000000014662000 2020-01-16 14:00:57 UTC+0000
0xffff8a9dcf5ec5c0 sudo 1750 1733 0 0 0x000000005388a000 2020-01-16 14:01:22 UTC+0000
0xffff8a9dcf5ec5c0 meterpreter 1751 1750 0 0 0x0000000014540000 2020-01-16 14:01:22 UTC+0000
0xffff8a9d9e4c8000 update-notifier 1824 1266 1000 1000 0x00000000764ae000 2020-01-16 14:01:42 UTC+0000
0xffff8a9d9e4cdd00 gnome-software 1826 1266 1000 1000 0x0000000013850000 2020-01-16 14:01:43 UTC+0000
0xffff8a9dae358000 fwupd 1905 1 0 0 0x00000000791e4000 2020-01-16 14:01:47 UTC+0000
0xffff8a9dac645c0 xfsalloc 2526 2 0 0 ----- 2020-01-16 14:01:53 UTC+0000
0xffff8a9dcf69c5c0 xfs_mru_cache 2527 2 0 ----- 2020-01-16 14:01:53 UTC+0000
0xffff8a9db1abc5c0 jfsIO 2531 2 0 ----- 2020-01-16 14:01:53 UTC+0000
0xffff8a9dcdf9c5c0 jfsCommit 2532 2 0 ----- 2020-01-16 14:01:53 UTC+0000
0xffff8a9df7bddd00 jfsSync 2533 2 0 ----- 2020-01-16 14:01:53 UTC+0000
0xffff8a9dbc0e0000 deja-dup-monito 2950 1266 1000 1000 0x0000000013992000 2020-01-16 14:02:42 UTC+0000
0xffff8a9dc3c40000 sh 2964 1751 0 0 0x0000000076aec000 2020-01-16 14:02:57 UTC+0000
vagrant@kali:~$
```

3. Командой linux_netstat просматриваем сетевые соединения.

```
vagrant@kali:~$ volatility --profile=LinuxUbuntu_4_15_0-72-generic_profilex64 --filename=/vagrant/task1/memory.vmem linux_netstat -U
Volatility Foundation Volatility Framework 2.6
UDP 127.0.0.1 :41717 127.0.0.53 : 53 systemd-timesyn/465
UDP 127.0.0.53 : 53 0.0.0.0 : 0 systemd-resolve/466
TCP 127.0.0.53 : 53 0.0.0.0 : 0 LISTEN systemd-resolve/466
UDP 192.168.180.132 :57655 192.168.180.1 : 53 systemd-resolve/466
UDP 192.168.180.132 :47592 192.168.180.1 : 53 systemd-resolve/466
UDP 192.168.180.132 :54615 192.168.180.1 : 53 systemd-resolve/466
UDP 192.168.180.132 :45549 192.168.180.1 : 53 systemd-resolve/466
UDP 192.168.180.132 :50894 192.168.180.1 : 53 systemd-resolve/466
TCP 192.168.180.132 :59268 192.168.180.1 : 53 SYN_SENT systemd-resolve/466
UDP 192.168.180.132 :46139 192.168.180.1 : 53 systemd-resolve/466
UDP 192.168.180.132 :52945 192.168.180.1 : 53 systemd-resolve/466
TCP ::1 : 631 :: : 0 LISTEN cupsd/509
TCP 127.0.0.1 : 631 0.0.0.0 : 0 LISTEN cupsd/509
UDP 0.0.0.0 : 5353 0.0.0.0 : 0 avahi-daemon/526
UDP : : 5353 : : 0 avahi-daemon/526
UDP 0.0.0.0 :37604 0.0.0.0 : 0 avahi-daemon/526
UDP : : 36776 : : 0 avahi-daemon/526
UDP 0.0.0.0 : 631 0.0.0.0 : 0 cups-browsed/637
UDP 0.0.0.0 : 68 0.0.0.0 : 0 dhclient/697
TCP 192.168.180.132 :51934 192.168.180.131 : 1337 ESTABLISHED meterpreter/1751
UDP 127.0.0.1 :50803 127.0.0.53 : 53 gnome-software/1826
TCP 192.168.180.132 :51934 192.168.180.131 : 1337 ESTABLISHED sh/2964
```

использовал флаг -U чтобы игнорировать unix сокеты. Отфильтровав соединения по pid выясняем meterpreter установил соединение с другим хостом

```
vagrant@kali:~$ volatility --profile=LinuxUbuntu_4_15_0-72-generic_profilex64 --filename=/vagrant/task1/memory.vmem
Volatility Foundation Volatility Framework 2.6
TCP 192.168.180.132 :51934 192.168.180.131 : 1337 ESTABLISHED meterpreter/1751
```

4. Получим отчет с помощью команды `linux_malfind`

```
vagrant@kali:~$ volatility --profile=LinuxUbuntu_4_15_0-72-generic_profilex64 --filename=/vagrant/task1/memory.vmem linux_malfind > /vagrant/task1-report.txt
Volatility Foundation Volatility Framework 2.6
vagrant@kali:~$ cat /vagrant/task1-report.txt | grep Pid | awk '{print $4}' | uniq
573
657
835
1034
1389
1751
```

сохранив отчет в txt вытаскиваем все уникальные pid-ы

5. Запустим `linux_yarascan` по найденным pid-ам

```
vagrant@kali:~$ wget https://raw.githubusercontent.com/cuckoosandbox/community/master/data/yara/shellcode/metasploit.yar
--2020-05-23 22:19:30-- https://raw.githubusercontent.com/cuckoosandbox/community/master/data/yara/shellcode/metasploit.yar
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.76.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.76.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4286 (4.2K) [text/plain]
Saving to: 'metasploit.yar'

metasploit.yar          100%[=====] 4.19K  --.-KB/s   in 0s

2020-05-23 22:19:31 (44.1 MB/s) - 'metasploit.yar' saved [4286/4286]

vagrant@kali:~$ volatility --profile=LinuxUbuntu_4_15_0-72-generic_profilex64 --filename=/vagrant/task1/memory.vmem linux_yarascan -y metasploit.yar -p 573,657,835,1034,1389,1751
Volatility Foundation Volatility Framework 2.6
```

увы яраскан ничего не нашел.