Threat Intelligence & IOC

Come da richiesta abbiamo esaminato lo scambio di pacchetti che ci sono state tra le due macchine e possiamo trovare:

Richiesta ARP

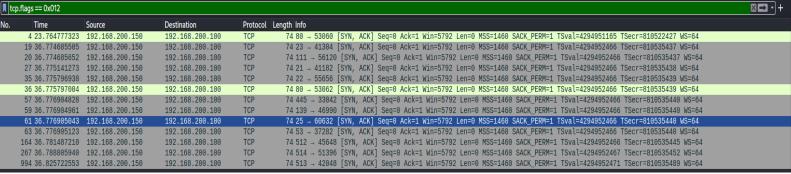
```
8 28.761629461
                PcsCompu_fd:87:1e
                                      PcsCompu_39:7d:fe
                                                           ARP
                                                                       60 Who has 192.168.200.100? Tell 192.168.200.150
9 28.761644619
                                                           ARP
                                                                       42 192.168.200.100 is at 08:00:27:39:7d:fe
                PcsCompu_39:7d:fe
                                      PcsCompu fd:87:1e
                                      PcsCompu_fd:87:1e
                PcsCompu_39:7d:fe
                                                                       42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230099
                PcsCompu_fd:87:1e
                                      PcsCompu_39:7d:fe
                                                                       60 192.168.200.150 is at 08:00:27:fd:87:1e
```

Dove viene inviata la richiesta per conoscere il MacAndress della macchina.

Possiamo notare alla prima richiesta le prime informazioni riguardante anche l'ip di provenienza:

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286 Host Announcement METASPLOITABLE, Workstation, S
-	00 704044005	400 400 000 400	400 400 000 450	TAD	74 50000 00 50001 00 1604040 10 400-4400

Come possiamo notare dalla scansione di Wireshark è stata fatta una scansione **Nmap -sT -sV** più nello specifico possiamo filtrare le richieste, cosi da avere una quadro generale più pulito, di ciò ch'è accaduto utilizzando il filtro



Tcp.flags == 0x012

In questo modo potremmo vedere le porte scansionate e dov'è stato effettuato lo scambio SYN\ACK

```
Transmission Control Protocol, Src Port: 445, Dst Port: 33042, Seq: 0, Ack: 1, Len: 0
  Source Port: 445
  Destination Port: 33042
  [Stream index: 15]
  [Conversation completeness: Complete, NO DATA (39)]
  [TCP Segment Len: 0]
  Sequence Number: 0
                         (relative sequence number)
  Sequence Number (raw): 1470223621
  [Next Sequence Number: 1
                               (relative sequence number)]
  Acknowledgment Number: 1
                               (relative ack number)
  Acknowledgment number (raw): 1246201613
  1010 .... = Header Length: 40 bytes (10)
    ags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
          .... = Nonce: Not set
         0... = Congestion Window Reduced (CWR): Not set
```

I Rimedi è scappare in messico e unirsi ad una banda di Chihuahua