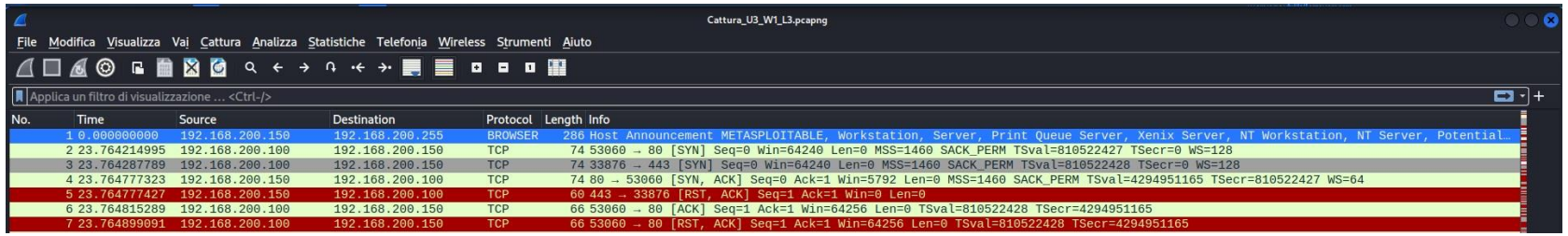
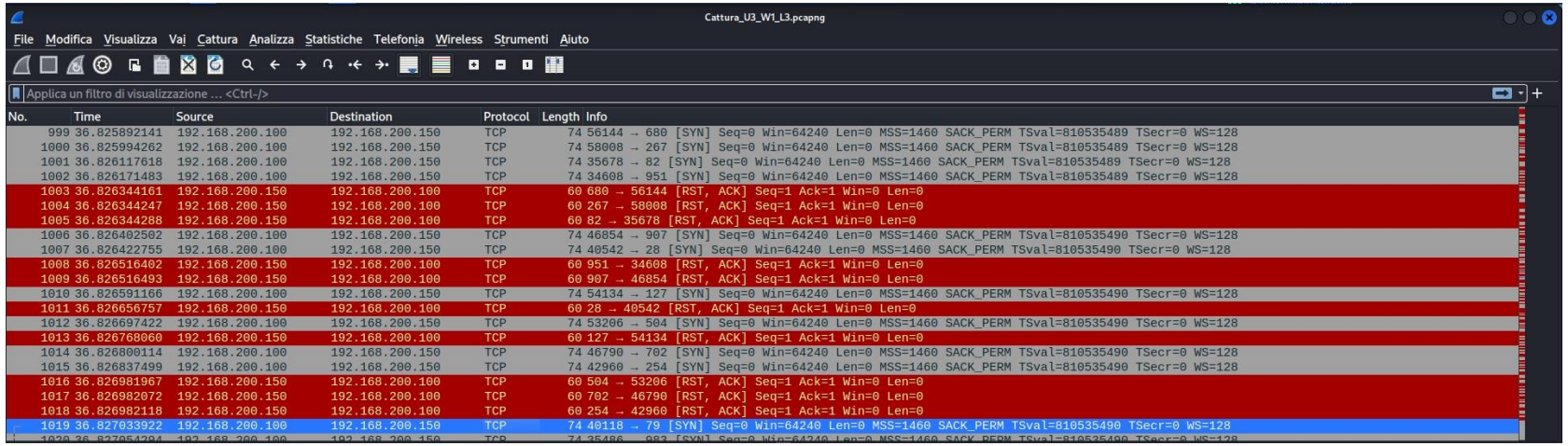
Threat Intelligence
&
Indicator of Compromise

Analisi di una cattura di rete effettuata con Whireshark

Orlando Tangari





Identificazioni eventuali IOC

Già dai primi pacchetti si nota che l'host vittima è una Macchina Metasploitable con IP: 192.168.200.150 ed è stato effettuato un Three Way Handshake da una macchina con IP: 192.168.200.100 .

Dagli oltre mille pacchetti analizzati si può dedurre che stato usato il port scanning Nmap per vedere se Metasploitable avesse porte aperte e, quindi, vulnerabilità da sfruttare.

Sulla macchina vittima come prima cosa, si consiglia di attivare il firewall con regole che limitano il traffico in ingresso ai soli utenti autorizzati, di disabilitare i servizi non in uso, per non lasciare porte aperte inutilizzate, di configurare i servizi usati in modo che solo gli utenti autorizzati possano accedervi ed, infine, conoscendo già un IP di una macchina che ha attaccato il sistema, lo si può inserire in una black list.