**TRACCIA 4**

REPORT - EXTRACT EXE from PCAP

Virtual Machine: Cyber-Ops Workstation

File: nimda.download.pcap

Oggetto: Analisi del file “File” e successiva estrazione di un eseguibile

Software: Wireshark

Parte 1 - Analisi

Il “File” è una cattura di pacchetti eseguita durante un precedente download del Malware Nimda. Si trova nella “VM” nella directory “/home/analyst/lab.support.files/pcaps”.

Tramite terminale è possibile trovare il “File”.

Con Wireshark si procede all’analisi:

Il “File” contiene pacchetti di protocolli TCP e HTTP.

Al seguito dei pacchetti di Handshake si trova il primo pacchetto di interesse, ovvero una richiesta “GET /W32.Nimida.Amm.exe HTTP/1.1”, viene fatta dalla sorgente “209.165.200.235” al destinatario “209.165.202.133”

Poichè il protocollo HTTP funziona su TCP, è possibile seguire lo Stream TCP per poter ricostruire la transazione. Quindi clic destro sul primo pacchetto e poi su “Follow TCP Stream”, si ottiene una finestra con una pseudo-traduzione del codice binario in testo.

Parte 2 - Estrazione