WIRESHARK

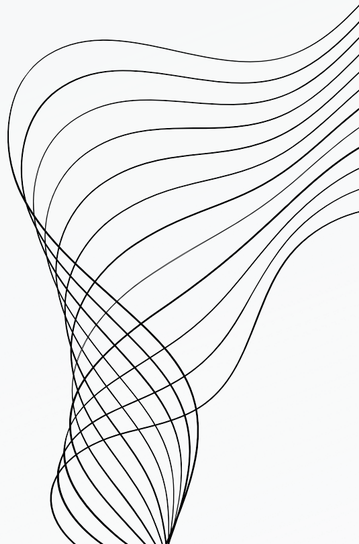
01 IDENTIFICARE EVENTUALI IOC, OVVERO EVIDENZE DI ATTACCHI IN CORSO

02 IN BASE AGLI IOC TROVATI, FATE DELLE IPOTESI SUI POTENZIALI VETTORI DI ATTACCO UTILIZZATI

03 CONSIGLIATE UN’AZIONE PER RIDURRE GLI IMPATTI DELL’ATTACCO

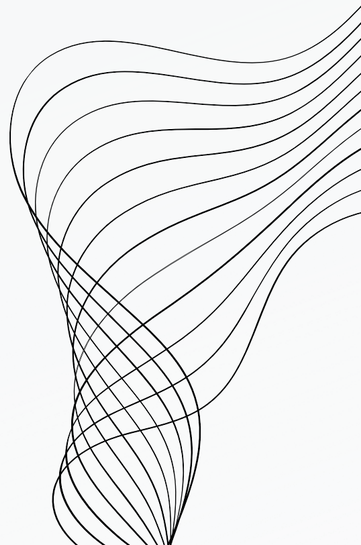
IDENTIFICARE EVENTUALI IOC, OVVERO EVIDENZE DI ATTACCHI IN CORSO

NELLA SCANSIONE FATTA CON WIRESHARK NOTIAMO CHE CI SONO MOLTISSIME RICHIESTE TCP RIPETUTE DALLO STESSO IP



IN BASE AGLI IOC TROVATI, FATE DELLE IPOTESI SUI POTENZIALI VETTORI DI ATTACCO UTILIZZATI

COME DETTO PRIMA ESSENDOCI MOLTE RICHIESTE EFFETTUATE DALLO STESSO INDIRIZZO IP, POTREMMO IPOTIZZARE CHE “L’ATTACCANTE” STIA EFFETUANDO UNA SCANSIONE SULLE PORTE DEL NOSTRO SERVER



CONSIGLIATE UN'AZIONE PER RIDURRE GLI IMPATTI DELL'ATTACCO

PER RIDURRE HO ELIMINARE QUESTO PROBLEMA, POTREMMO METTERE DELLE REGOLE AL NOSTRO FIREWALL CHE ANDRA A BLOCCARE LE RICHIESTE PING O BLOCCARE QUESTO INDIRIZZO IP