Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica. A tal proposito, con riferimento al malware chiamato «Malware_U3_W3_L2» presente all'interno della cartella «Esercizio_Pratico_U3_W3_L2» sul Desktop della macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti, utilizzando IDA Pro.

- 1. Individuare l'indirizzo della funzione DLLMain(così com'è, in esadecimale)
- 2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione?
- 3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?
- 4. Quanti sono, invece, i parametri della funzione sopra?



La funzione gethostbyname è una funzione utilizzata per ottenere informazioni associate a un nome host. È una funzione di sistema che restituisce una struttura di tipo 'hostent' contenente informazioni come l'indirizzo IP associato al nome host, l'elenco degli alias del nome host e altri dettagli.

```
stdcall sub_10001656(LPV010)
 sub_10001656 proc mear
var_675= byte ptr -675h
var 674- dword ptr -674h
hLibHodule= dword ptr -670h
timeout- timeval ptr -66Ch
name= sockaddr ptr -664h
var_654= word ptr -654h
Ost- dword ptr -650h
Parameter- byte ptr -644h
 var_640- byte ptr -640h
CommandLine- byte ptr -63Fh
 Saurce= byte ptr -630h
Data- byte ptr -638h
 var_637- byte ptr -637h
var_544= dword ptr -544h
var_500= dword ptr -500h
var_500= dword ptr -500h
Buf2= byte ptr
                  -AFCh
 readfds- fd_set ptr -48Ch
phkResult- byte ptr -388h
var_380= dword ptr -380h
var_184= dword ptr -184h
var_194= dword ptr -194h
WSAData- WSAData ptr -198h
```

Capiamo che sono variabili perchè hanno un risultato negativo mentre con risultato positivo sono i parametri.

```
WSAData= WSAData ptr -190h
arg_0= dword ptr 4
```

Il parametro è solo uno ed è quello con il risultato positivo.

5. Il malware in teoria è un trojan che tramite backdoor può instaurare connessioni o eseguire comandi in background