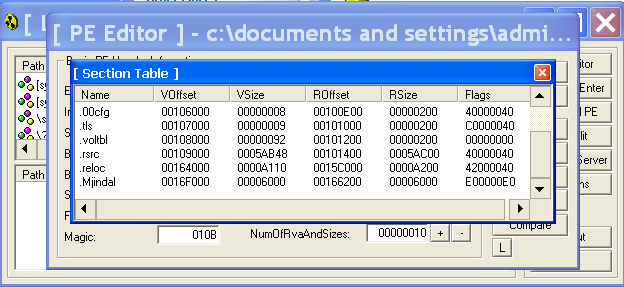
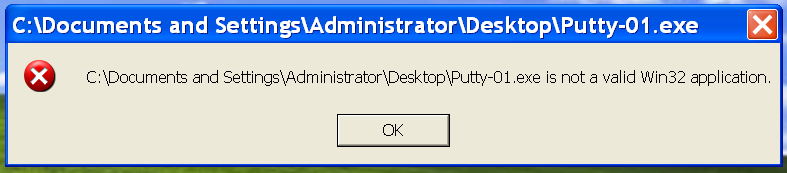
PE code Injection

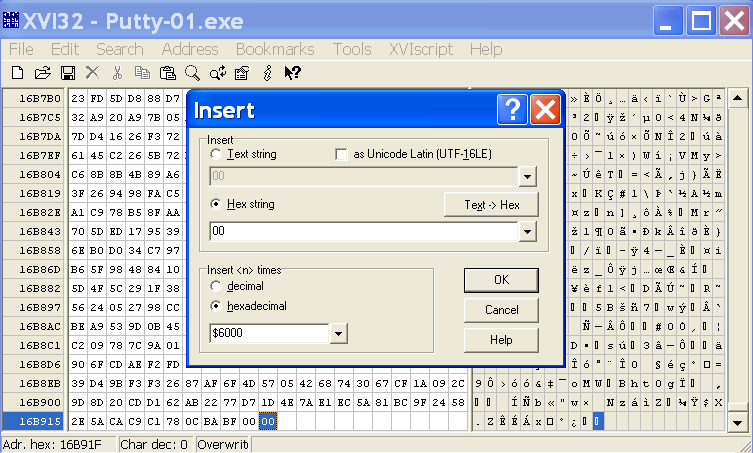
Adding of new section of 6000 bytes to putty



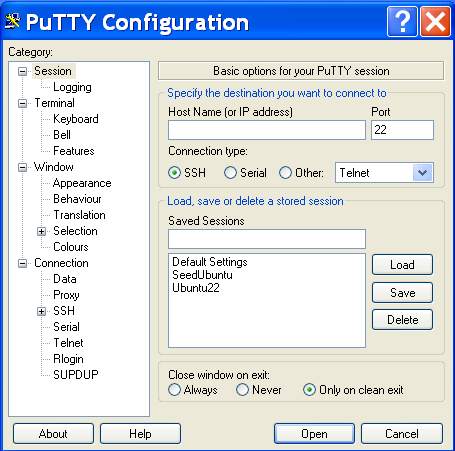
Program get crashed due to header mismatch



Filling extra 00 bytes equivalent to 6000 bytes to balance header and program size



Program runs successfully after that



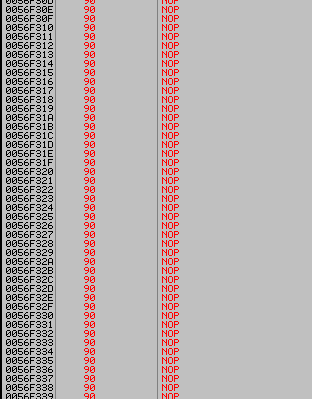
Modifying the entry point of the program



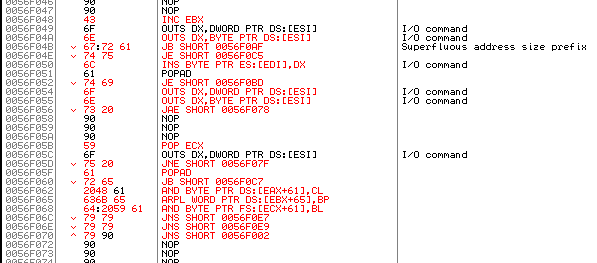
Program crashes



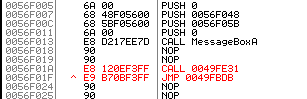
Filling section with NOPs

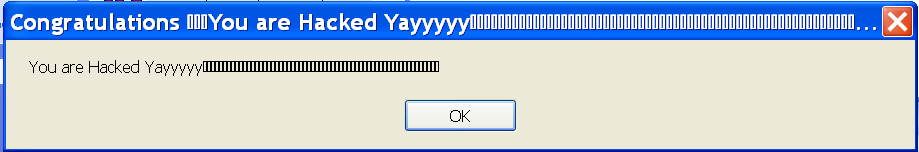


Writing strings for MessageBoxA

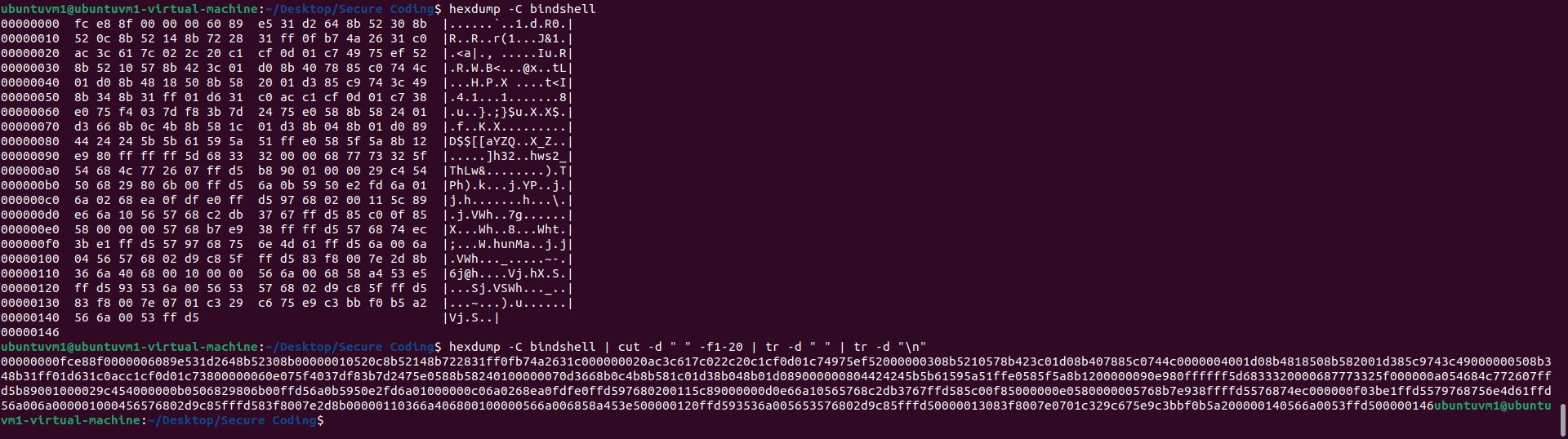


Calling MessageBoxA

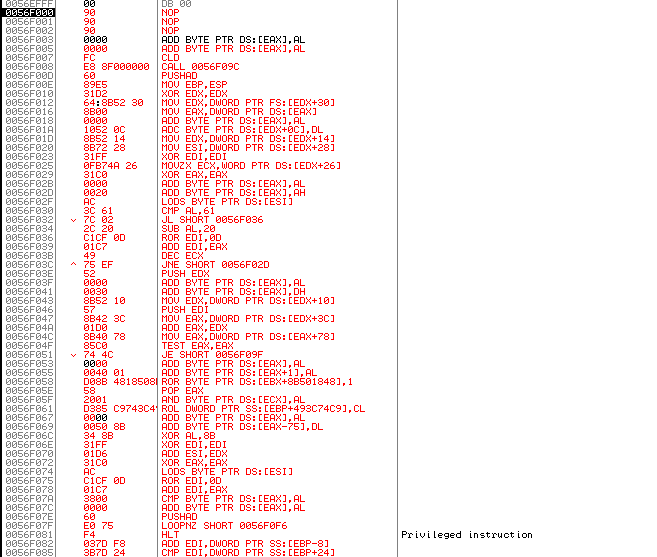




Payload Creation



Adding of payload in executable



Netstat Command (no 4444 port)

