Exploiting BigAnt using EggHunter

Exploiting the Vulnerable Server Application

In this Lab we want to write an exploit to achieve arbitrary code execution using a vulnerability in the application named "Big Ant Server" but using an EggHunter.

THE EASY WAY (*just get it done*):

In this lab, you can use a Windows 7 system which could be downloaded either from MS VM repository (or archive.org), or use our online environment (*highly recommended*). After downloading the Windows 7 system and before doing anything related to exploitation, make sure both your Kali Linux and Windows machine can communicate with each other. We can make sure of that by sending a ping request from Windows to Kali Linux, or the opposite (requires an update to the Windows firewall).

THE FUN WAY (*learn something cool*):

Please use all the previous skills, our discussions, videos, and the Corelan Team's blog post to exploit the same application but on Windows 10. Show me your skills, you can do this!

Note: You can start by using the template found here exploit-template, or use the exploit you did to exploit BigAnt Server using SEH and go from there.

NOTE: May the force be with you :)