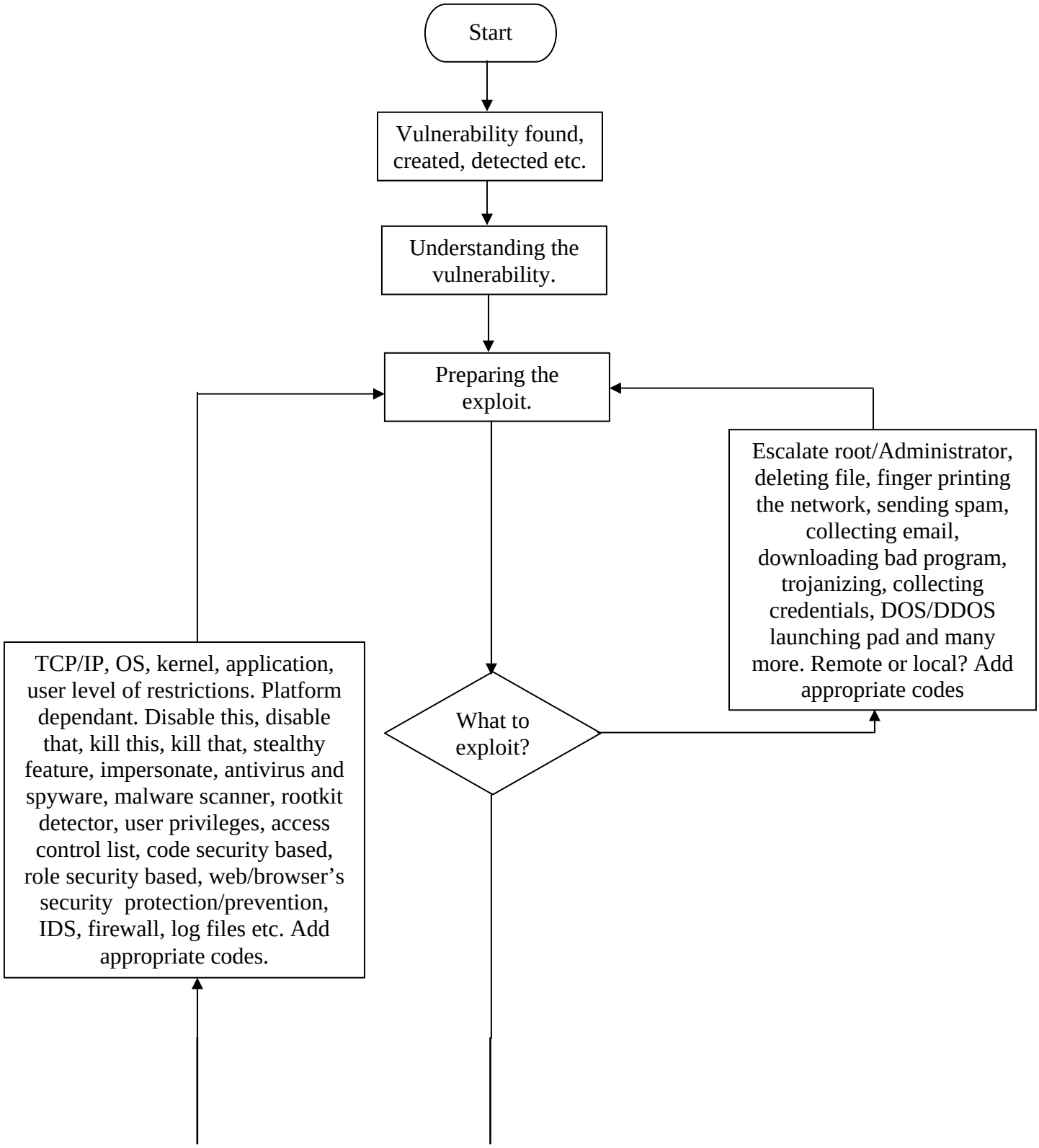
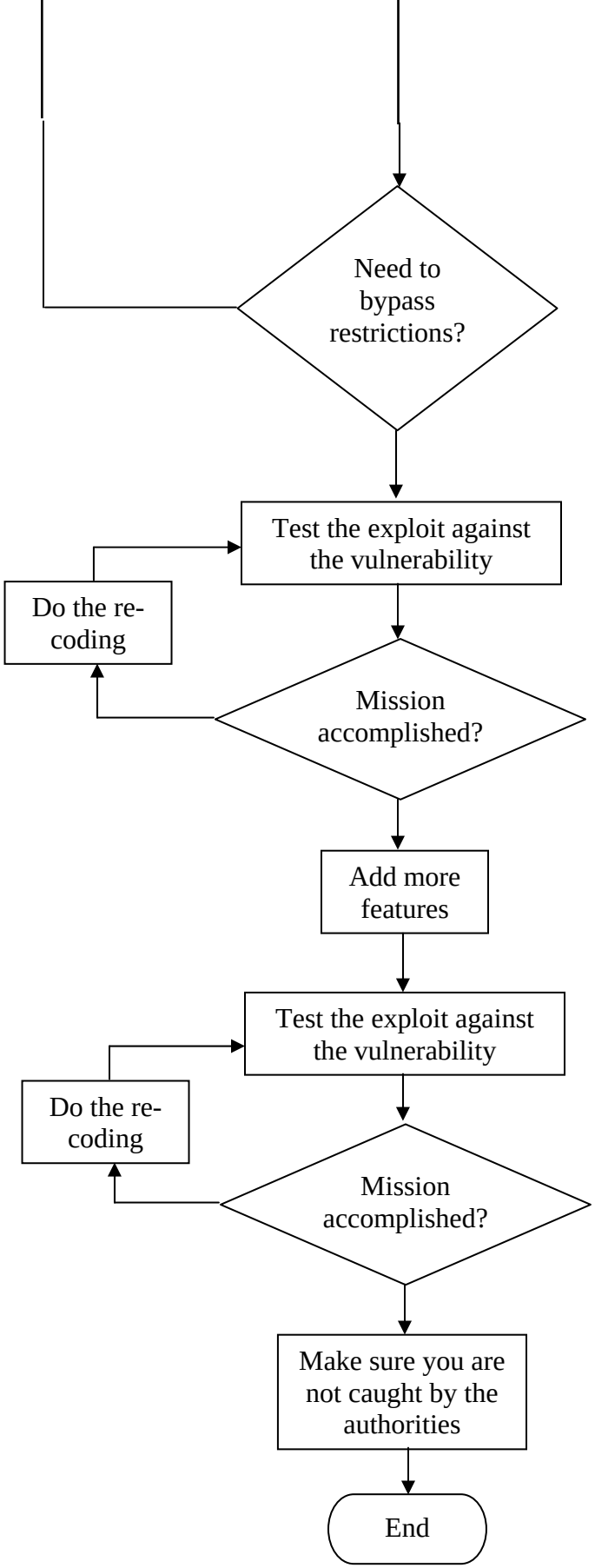
Well, this is for educational purpose only. Please read the disclaimer first. During the experimental demonstration we have controlled the flow of event which include the vulnerability and exploit environment. In order to describe a complete process for the real exploit, the following flow chart provides some idea. The theory and principle part of this thing can be applied to other exploit as well.




Need to bypass restrictions?
Test the exploit against the vulnerability
Do the re-coding
Mission accomplished?
Add more features
Test the exploit against the vulnerability
Do the re-coding
Mission accomplished?
Make sure you are not caught by the authorities
End