Vorgehen für die Ausarbeitung noch folgende Tipps:

1. Sicherheitsmechanismus ASLR deaktivieren. Man muss es ja nicht gleich zu Beginn extra schwer machen. Das geht z.B. auch mit gdb-peda für die jew. Sitzung.
2. Lokalisieren der Schwachstelle
    a. Was kontrollieren wir?
    b. Bestimmung des Offset. (Hint: pattern_create gibt es auch für gdb-peda)
3. NX umgehen. Dafür haben wir – unter Windows – ROP kennengelernt. Wie war das nochmal unter Linux?
4. Nutzt die man page eines geeigneten Syscall um ein vorhandenes Binary (z.B. /bin/sh) auszuführen. Darin seht ihr welche Parameter der Syscall braucht.
5. Nun solltet ihr es schaffen, /bin/sh aufzurufen.

Erst wenn das geht empfehle ich euch, sich um ASRL zu kümmern.

6. Findet einen Adress-Leak.
7. Identifikation der Basisadresse zur Adresse des Leaks.
8. Identifikation des Offset der jew. geleakten Adresse.
9. Anpassen des Exploit, dass er den Leak übernimmt und daraus die neue Basisadresse von libc errechnet.
10. Stack präparieren und Exploit zünden.