Übung #8 – Der Bootvorgang

In dieser Übung werden Sie lernen, wie Sie Ëmergency Passwort Recovery"betreiben können. Alternativ könnte die Übung auch als "Knacken von Linux-Systemen mit physischen Zugang"betitelt werden.

1 Anleitung

1. Sie haben Ihr root Passwort vergessen und verzweifeln. Sie können sich aber erinnern, einmal gehört zu haben, wie man das Passwort in solchen Notfällen neu setzen kann. Starten Sie dazu den Computer neu. Im Bootmanager drücken sie [ESC] und tippen folgende Zeile ein: *linux init=/bin/bash*. Dadurch wird anstatt des üblichen Startvorgangs eine Shell mit root-Rechten geöffnet und der Startvorgang unterbrochen. Sie haben jetzt die nötigen Rechte um das Passwort von root neu zu setzen. Allerdings müssen Sie vorher noch einige Schritte durchführen, die Ihnen aber nach einigem Nachdenken sofort logisch erscheinen werden.

2. Vergeben Sie im zweiten Schritt der Übung ein Passwort für Ihren Bootmanager. Finden Sie heraus wie das funktioniert (Ihr Bootmanager sollte Lilo sein). Damit ist es nur mehr mit Kenntnis des Passwortes möglich den Bootvorgang zu ändern.

3. Denken Sie darüber nach, wie Sie in ein Linuxsystem einbrechen können zu dem Sie physischen Zugang haben, dessen Bootmanager aber passwortgeschützt ist. Es gibt mindestens noch einen Weg.

4. In /etc/inittab alle bis auf drei virtuelle Konsolen entfernen. Auf tty8 soll ebenfalls ein Loginprompt laufen, der allerdings nach einem Logout nicht mehr neu gestartet werden soll. Teilen Sie dem Initprozess mit, dass er seine Konfiguration neu lesen soll ohne Neustart des Rechners.