## Frage 6.1

> Woher hat der Benutzer mit den „vielen“ Rechten diese? Welchem anderen Benutzer entspricht dieser Benutzer?

Der Nutzer entspricht dem Root-User und kann daher alles.

## Frage 6.2

> Weshalb war das Finden des Passworts mit john so schnell möglich? Wie könnte man diese Zeit deutlich verlängern?

Die Informationsgehalt war zu gering bzw. folgte einem einfachen Muster.
Man könnte Maßnahmen zur Passwortsicherheit anwenden.
- keinem Muster Folgend - lange Passwörter - Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen verwenden
etc.

## Frage 6.3

> Was befindet sich in /proc und wofür werden die Inhalte benötigt?

/proc ist ein Pseudo-Dateisystem und stellt ein Interface für Kernel-Daten-Strukturen.

## Frage 6.4

> Warum sehen Sie nach der Einrichtung der chroot Umgebung die Meldung I have no Name!? Wie konnte man diese Meldung beseitigen?

Weil das System der UID keinen Nutzernamen zuordnen kann.
Um die Meldung zu beseitigen reicht es eine passwd Datei, mit Eintrag für sysbar, anzulegen.

## Frage 6.5

> Wie kann es sein, dass der Neue Prozess aus Aufgabe 5.6.3 mit einer hohen (nicht privilegierten) UID läuft und trotzdem Port 21 verwendet? Wie kann man so etwas bewerkstelligen?

Es gibt mehrere Möglichkeiten dies zu realisieren! Durch setuid, einem Port Redirect, setcap oder einem lokalem ssh Tunnel.
Setuid setzt bzw. ändert die userkennung bei Ausführung eines Dienstes/Datei.
Ein port redirect der in etwa folgende Syntax hat: iptables -A PREROUTING -t nat -i eth0 -p tcp –dport [port] -j REDIRECT –to-port [port]
Setcap setzt mit Parametern -n [rootuid] root Datei Rechte.

## Frage 6.6

> Wäre eine Aktivierung von rkhunter gleich nach der Installation hilfreich gewesen? Wie hätte Ihnen dies das Leben erleichtert?

Es hätte im Rahmen von einigen Aufgaben dabei geholfen die neuen User, Veränderungen im Dateisystem und den neuen TCP-Dienst zu finden.

## Frage 6.7

> rkhunter findet Veränderungen und zeigt sie an. Wie könnte ein Benutzer mit entsprechenden Rechten rkhunter austricksen?

Auch hier gibt es mehrere Möglichkeiten dies zu realisieren.
Man könnte anhand von 'touch' die timestamps von Dateien auf ein jeweiliges Datum zurücksetzen.
Mit Rootrechten kann rkhunter.conf entsprechend manipuliert werden.