Szenario:

Der befreundete Nachrichtendienst von Musterland hat den Bundesnachrichtendienst um Hilfe bei der Aufklärung eines Sicherheitsvorfalls gebeten. Ein Webserver der staatlichen Versicherungsgesellschaft wurde gehackt. Die Angreifer haben anschließend das root-Passwort des Servers verändert und Daten anderer Hacks in einem geschützten Verzeichnis abgelegt. Ein Administrator hat zunächst versucht, das neue root-Passwort zu ermitteln, ist daran aber leider gescheitert. Daher hat er ein Image des Servers erstellt und an den BND übergeben, das Sie nun analysieren sollen.

Das Ziel ist es nicht nur zu ermitteln, welche Daten die Angreifer auf dem System gespeichert haben, sondern zusätzlich möchten Sie wissen, wie die Angreifer ursprünglich auf das System gelangen konnten und wie sie in der Lage waren, root-Zugriff zu bekommen.

Diesbezüglich wurden Sie darüber unterrichtet, dass die verantwortlichen Administratoren des Öfteren Passwörter in geschützten Bereichen unverschlüsselt ablegen. Sie wissen, dass Schwachstellen häufig in Webanwendungen zu finden sind und vermuten daher, dass dort der Einfallsvektor liegen könnte. Ihnen wurde außerdem mitgeteilt, dass die Hacker zusätzlich einen niedrig privilegierten Benutzer angelegt haben, dessen Zugangsdaten glücklicherweise aufgrund eines schwachen Passworts schnell ermittelt werden konnten (hacker:abcd1234).

Die beigefügte OVA Datei können Sie mit einer entsprechenden Virtualisierungssoftware verwenden.

Ziele im Überblick:

1. Wie konnten die Angreifer ursprünglich auf das System gelangen (bedenken Sie, dass die Angreifer zunächst keinen Konsolenzugriff auf das System hatten)?
2. Wie waren die Angreifer in der Lage, root-Rechte zu bekommen?
3. Was für Daten (Inhalt) haben die Hacker auf dem System abgelegt?

Beachten Sie, dass für die Beantwortung jeder Frage eine technische Erläuterung (Begründung) erwartet wird.

Tragen Sie Ihre Antworten bitte in die folgenden Felder ein:

Beschreiben Sie die Schwachstelle, die die Hacker ausnutzen konnten, um das System zu infiltrieren. Welche Art von Schwachstelle wurde genutzt? Geben Sie einen konkreten Proof-of-Concept (PoC) dafür an.

Wie waren die Angreifer nach erfolgter Infiltration in der Lage, root-Rechte zu bekommen? Beschreiben Sie die Sicherheitslücke und ermitteln Sie das von den Hackern neu gesetzte root-Passwort.

Welche Daten wurden auf dem System abgelegt? Wie wurden die Daten versteckt? Benennen Sie die Flag.