

---

## Get Root

**By rac**

Published: 11.01.2008 - 01:58



**!!! This is a Draft and not yet finished document !!!**

## Aufgabenstellung

Die Aufgabenstellung war, dass man auf einem gegebenen System, eingeloggt mit einem niedrig privilegierten user, root Rechte erlangen musste.

Das System war von den [Wargame initianten](#) mit einer Fehlkonfiguration aus Praxiserfahrungen bei Kunden präpariert worden.

## Lösungsweg

Um root rechte auf einem System zu erlangen ist der einfachste Weg, wenn man sich mal Gedanken macht welche accounts die Berechtigung haben um sachen mit höherprivilegierten rechten auf dem System auszuführen.

Darunter fallen häufig systemservices wie cron jobs, die zu unserem glück regelmässig ausgeführt werden.

Wir durchsuchten die cron jobs danach, ob irgend ein script ausgeführt wird, auf das wir schreib zugriff hatten.

---

Ein bash script, das durch ein anderes script ausgeführt wird das im cron.minutely ausgeführt wird ist World Writable.

Wir kopierten /bin/bash in unser home Verzeichniss, liessen durch das beschreibbare script den Befehl

1.  
chown root.root /home/hacker/bash

2.  
chmod 4755 /home/hacker/bash

ausführen und warteten eine Minute.

Die Befehle wurden zwar ausgeführt, jedoch ist es anscheinend auf einem Ubuntu system nicht möglich das binary nun unter root laufen zu lassen obwohl das SUID Bit gesetzt ist und das File root gehört.

Wir entschieden uns dann für die billige Variante (fliegt sehr schnell auf) und führten im script nun den Befehl

1.  
adduser hacker admin

aus und konnten danach einen sudo bash machen um die root privilegien zu erhalten.

---

## Lesson learned

Ein script, das von cron ausgeführt wird, sollte nie World Writable sein.

## Related Links

- [Compass Security](#)