
Bypassing Security Tips

By rac

Published: 15.01.2008 - 14:35

Get root

- Schaut euch die cron jobs an und haltet ausschau nach beschreibbaren dateien ;-)
- [Wargame sample](#)

Restricted Shell breakout

- Hab ich Befehle zur verfügung, mit denen ich andere Befehle überschreiben kann...???

z.B. tee, cat oder notfals auch nur ein simpler echo...

Encrypted files (EFS) in Windows Offline Folders

Überlegt mal, welcher account (man muss sich mit diesem nicht einloggen können) automatisiert auf diese Files zugreifen muss bzw. diese Ent- und Verschlüsseln kann...
Welche tasks werden unter diesem account ausgeführt???

By the way: cmd, [xcopy](#) (Backup tool) und [cipher](#) (Ver-/Entschlüsseln, zum aufspüren der Speicherorte von verschlüsselten Dateien) sind nützliche tools in verbindung mit einem USB stick (FAT32 - dateien werden bei xcopy entschlüsselt da kein NTFS) ;-)

Related Links

- [Diverse Security related distros \(LiveCD's\)](#)
- [Hacking Illustrated Videos](#)