IT-Sicherheit

Praktikumsaufgabe 3: Mandatory Access Control

Aufgabenstellung: Einrichten der Umgebung

1. Importieren Sie die bereitgestellte, virtuelle Maschine in VirtualBox
   WICHTIG:
   Ändern Sie die Netzwerkkonfiguration dieser VM nicht. Sie enthält eine Backdoor!
   - Melden Sie sich mit dem Nutzernamen `user` und dem Passwort `user` an dem virtuellen System an.
   - Optional:
     Klonen Sie die virtuelle Maschine (linked-clone), so dass Sie zwei Kopien in einem NAT-Netzwerk zur Verfügung haben.
2. Prüfen Sie mit einem Browser, dass ein lokaler Webserver läuft.

Das root-Passwort lautet `t00r`. Mit dem Kommando `su -` können Sie eine root-Shell öffnen.

Aufgabenstellung: Test der Web-Shell

Im Verzeichnis attackclient finden Sie die Client-Tools der WebShell „weevely3“. (vgl. https://github.com/epinna/weevely3)

Dem laufenden Webserver wurde die WebShell untergeschoben. Das vom Angreifer gesetzte Passwort ist „`hacked`“.

3. Sehen Sie sich die Dokumentation von weevely3 an. Um welche Art Software handelt es sich?
4. Benutzen Sie die WebShell mit dem Kommando
   `./weevely.py http://localhost/funny.php hacked`
   Was können Sie über diesen Zugriffsweg machen?

Aufgabenstellung: Härtung

Sie möchten einen Weg entwickeln, die Auswirkungen von WebShells auf Ihrem System zu minimieren.

5. Nutzen Sie AppArmor für Mandatory Access Control und **machen Sie damit die (meisten) Funktionen der WebShell für den Angreifer unbrauchbar**.
6. Testen Sie Ihre Einstellungen durch Wiederholung von Schritt (4) mit eingeschalteter Mandatory Access Control.

Hinweise

- Die AppArmor-Tools sind noch nicht installiert, AppArmor ist jedoch bereits aktiviert.
  Gute Anleitungen zur Installation und Einrichtung finden Sie unter
  - https://wiki.debian.org/AppArmor/HowToUse
  - https://linuxhint.com/debian_apparmor_tutorial/
  - https://gitlab.com/apparmor/apparmor/-/wikis/QuickProfileLanguage
- AppArmor kann im „complaint“- oder „enforce“-Mode laufen. Testen Sie erst die Einstellungen im complaint-Modus!