Vorlesung Netzwerksicherheit – Sommersemester 2022

2. Übungszettel

Abgabe bis Dienstag, 26. April 2022 – 16:00 Uhr
Besprechung: Dienstag, 26. April 2022

Abgabe in festen Gruppen (Namen + Matrikelnummern angeben)

Abgabe via Artemis: https://alpro.besec.uni-bonn.de

Aufgabe 1 (5 Punkte)

Beschreiben Sie die Gemeinsamkeiten und Unterschiede der beiden Schutzobjekte „Dateien“ und „Prozesse“ als passive und aktive Objekte.

Aufgabe 2 (1 + 2 + 1 + 1 Punkte)

Im klassischen *nix-Berechtigungssystem unterscheiden sich die Zugriffsrechte von Dateien und Ordnern.

a) Nennen Sie die möglichen Berechtigungen. Bedenken Sie dabei auch die erweiterten Rechte.
b) Erklären Sie die Unterschiede in der Bedeutung zwischen Dateien und Ordnern.
c) Erläutern Sie, warum es Berechtigungen für „Owner“, „Group“ und „World“ gibt.
d) Nennen Sie die zusätzlichen Berechtigungen in aktuellen Windows-Systemen.

Aufgabe 3 (3 + 3 Punkte)

a) Beschreiben Sie die Elemente des STRIDE-Bedrohungsmodells von Microsoft.
b) Erläutern Sie die dem STRIDE-Modell in der Vorlesung zugeordneten Schutzziele mit jeweils einem Satz.

Aufgabe 4 (1 + 1 + 2 Punkte)

Wireshark ist ein Programm, das genutzt wird, um Netzwerk-Traffic abzuhören. Installieren Sie Wireshark (unter Ubuntu etwa mit „sudo apt install wireshark“) auf ihrem System und machen Sie sich mit dem Programm vertraut. Bearbeiten Sie dann folgende Aufgaben.

a) Beschreiben Sie, welche Schutzziele durch den Einsatz von Wireshark verletzt werden können.
b) Wireshark bietet die Möglichkeit Filter zu setzen, so dass nur bestimmter Traffic angezeigt wird. Erläutern Sie, wie Sie vorgehen müssen, damit nur Nachrichtenpakete angezeigt werden, die über die IP-Adresse 127.0.0.1 und Port 8080 verschickt werden.
c) Laden Sie das auf der Vorlesungs-Website verlinkte ZIP-Archiv auf Ihren Computer. Kompilieren Sie die beiden darin liegenden Objektdateien (z.B. mit „gcc -o alice alice.o“ und „gcc -o bob bob.o“). Die entstehenden Programme stellen eine klassische Client-Server Struktur dar, wobei Alice als Server und Bob als Client fungiert. Einmal ausgeführt werden sich Alice und Bob automatisch gegenseitig Nachrichten schicken. Diese werden jedoch nicht auf der Konsole ausgegeben. In unserem fiktiven Szenario sind Alice und Bob zwei Personen, die mit einem unverschlüsselten Chatprotokoll kommunizieren. Dabei ist Bob leider sehr unvorsichtig und teilt Alice sein neu erstelltes Bank-Passwort mit. Aufgrund eines Systemfehlers in der Chat-Software wird der Chat-Verlauf von Alice und Bob alle 10 Sekunden erneut gesendet. Ermitteln Sie mithilfe von Wireshark Bobs neu gewähltes Passwort. Schildern Sie im Nachhinein ausführlich, wie Sie vorgegangen sind.

   Hinweise:
   – Alice und Bob kommunizieren mit der IP-Adresse 127.0.0.1 über den Port 8080.
   – Um Traffic zu berücksichtigen, der innerhalb desselben Computers verschickt wird, muss in Wireshark das Loopback-Interface verwendet werden.