

2. Übungszettel

Abgabe: Bis Dienstag, 4. Mai 2021 – 16:00 Uhr

Besprechung: Dienstag, 4. Mai 2021

Abgabe in Gruppen von 2-3 Personen (Name + Matrikelnummer angeben)

Abgabe per Mail an: wueb+Uebung02@cs.uni-bonn.de

Aufgabe 1 (5 Punkte)

Betrachten Sie die Schutzobjekte „Dateien“ und „Prozesse“ als passive und aktive Objekte. Worin unterscheiden sich die beiden und wo erkennen Sie Gemeinsamkeiten?

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 Ordnern und Dateien.
- c) Warum gibt es Berechtigungen für „Owner“, „Group“ und „World“?
- d) Welche zusätzlichen Berechtigungen gibt es in aktuellen Windows-Systemen?

Aufgabe 3 (3 + 3 Punkte)

- a) Beschreiben Sie die Elemente des STRIDE-Bedrohungsmodells von Microsoft.
- b) Erläutern Sie die 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) Welche Schutzziele können durch den Einsatz von Wireshark verletzt werden?
- b) Wireshark bietet die Möglichkeit Filter zu setzen, so dass nur bestimmter Traffic angezeigt wird. Wie müssen sie vorgehen, 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.