060 Portscans

Aufgabe 1

Erklären Sie die Begriffe sowie die Bedeutung Authentisierung, Autorisierung und Accounting.

- **Authentisierung:**
  - **Identitätsnachweis**
- **Autorisierung:**
  - **Rechtevergabe**
- **Accounting:**
  - **audit trail über logging**

wikipedia: Authentication, authorization, and accounting

Aufgabe 2

Was ist ein Port?

Als Port versteht man einen Kommunikationsendpunkt. Auf der Softwareebene ist ein Port ein Konstrukt, mit dem man ein spezifischen Prozess oder ein network-service identifizieren kann.

wikipedia: Port_(computer_networking)

Aufgabe 2

Was ist ein Portscanner und wofür wird er verwendet?

Ein Portscanner ist eine Applikation, die dazu dient offene Ports bei bspw. Applikationen und Servern zu ermitteln. Dieser kann sowohl von Administratoren verwendet werden um Sicherheitslücken zu ermitteln, als auch von Angreifern um sich zugriff zu schaffen.

wikipedia: Port_scanner

Aufgabe 3

Ein Portscanner sendet eine Anfrage zur Verbindung mit einem Port eines Computers und zeichnet die Antwort auf. Es gibt drei mögliche Antworten, welche sind es?

1. **Open or Accepted**
2. **Closed or Denied**
3. **Filtered, Dropped or Blocked**

wikipedia: Port_scanner

Aufgabe 4

Welche Portscan-Techniken gibt es?

- **TCP**
- **SYN**
- **UDP**
- **ACK**
- **Window**
- **FIN**

wikipedia: Port_scanner

Aufgabe 5

Welche Möglichkeiten gibt es zur Erkennung von Portscannern?

Mehrere Requests durch einen oder mehrere IP-Adressen an unterschiedlichen Ports (abtasten).

Aufgabe 6

Welche Auswirkungen kann ein Portscan haben?

- **Entdeckung von offenen Ports**
- **Geldstrafe lulz**

Aufgabe 7

An welchem Angriffs-Muster könnte man einen Portscan identifizieren und wie lässt sich dies vermeiden?

1. **inkrementierende Portnummer-Anfragen durch eine Person**
2. **Auslastung und Testen aller Ports anhand eines Botnets**

Aufgabe 8 - Praxis

Welche Möglichkeiten gibt es auf einem Linux-System mit Kommandozeilenzugriff die offenen Ports herauszufinden ohne einen Portscan durchzuführen? (bspw. auf dem Kali-Container)

`#netstat -lntu`

```
┌──(root㉿Kali-Linux)-[~]
└─# netstat -lntu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:6789          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3000            0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
```

Aufgabe 9 - Praxis

Führen Sie mit Hilfe der folgenden Tools jeweils einen Port-Scan für Port 20 bis 80 durch: nmap, netcat bzw. nc, echo, bash

nmap

```
┌──(root㉿Kali-Linux)-[~]
└─# nmap localhost -p 1-80
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-23 14:24 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 79 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```