Projekt Aufgabe SECMA

Inhaltsverzeichnis

Teil 1: Installation und Grundkonfiguration 2
Teil 2 :Sicherheit durch Konfiguration 2
SSH Zugang mit SSL-Zertifikat sichern 2
Portschutz 3
Berechtigungen mittels CHMOD konfigurieren 3
Teil 3: Netzwerküberwachung und Blacklisting 3

Teil 1: Installation und Grundkonfiguration

Installieren von OpenSSH, Wireshark und Iptables

```
peter05@secmabh:~$
peter05@secmabh:~$
peter05@secmabh:~$ sudo apt install openssh-server
```

Installation für OpennSSH

Installation für Wireshark: sudo apt install -y wireshark

Installation für Iptables: sudo apt install -y iptables

Teil 2 :Sicherheit durch Konfiguration

SSH Zugang mit SSL-Zertifikat sichern

Zuerst muss ich in die Datei **„etc/ssh/sshd_config“** gehen.

Dort schreibe ich **„PermitRootLogin no“** hinzu um den Root-Login zu deaktiviern.

Und ich schreibe noch **„PasswordAuthentication no“** hinzu um die Passwort Authentifizierung zu deaktivieren.

Dann installiere ich noch **openSSL** mit dem Befehl **„sudo apt install -y openssl“**.

“OpenSSL req -x509 -newkey rsa:4096 -keyout ssh-selfsigned.key -out ssh-selfsigned.crt -days 365 -nodes” mit diesem Befehl erstelle ich dann mein SSL Zertifikat.

„HostCertificate /etc/ssh/ssh-selfsigned.crt

HostKey /etc/ssh/ssh-selfsigned.key“

Die beiden geraden schlüssel schreibe ich dann in die Datei „/etc/ssh/sshd_config“ hinzu

Portschutz

Mit dem Befehl „sudo iptables -A INPUT -p tcp --dport 80 -j DROP“ kann ich den Port 80 schließen.

Das gleiche kann ich tun mit dem Port 21 für FTP und für den Port 23 für das Telnet

Warum diese Ports:

Port 80: Die Daten werden unverschlüsselt übertragen und können mit Man-in-the-Middle Angriffe abgefangen werden

Angreifer können die HTTP Verbindung für Malware nutzen.

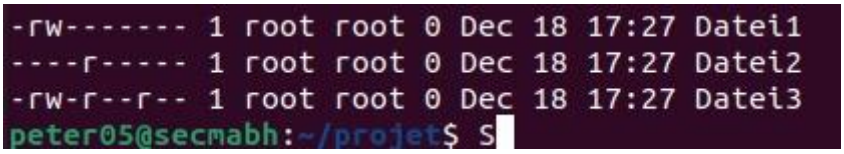
Port 21: FTP-Server sind Ziele für Brute Forcing

Keine Verschlüsselung für die übertragenen Dateien

Port 23: Telnet schickt Benutzernamen und Passwörter sichtbar

Die Kommunikation zwischen Client und Server ist offgelegt

Berechtigungen mittels CHMOD konfigurieren



1) Mit dem Befehl „**sudo chmod 600 Datei1**“ mache ich dass nur der Benutzer lesen und schreiben kann
2) Mit dem Befehl „**sudo chmod 040 Datei2**“ mache ich dass nur die Gruppe lesen kann
3) Mit dem Befehl „**sudo chmod 644 Datei3**“ mache ich dass der Besitzer lesen und schreiben kann und alle anderen nur lesen können

Teil 3: Netzwerküberwachung und Blacklisting