Team10 - Moritz Rupp, Viktor Brandl

4 Kontrollfrage

Bearbeitet von Moritz Rupp und Victor Brandl

Frage 4.1

> Welcher Modus wird durch openVPN in der Aufgabe verwendet und was bedeu- tet dies für Pakete, die als Broadcast im Subnet des Servers (192.168.X.0/24) gesendet werden?

Mit statischem Schlüssel, mit X.509 Zertifikat und X.509 Zertifikat mit Benutzerkennung.
Bei erstem werden Pakete mit einem symmetrischen Schlüssel verschlüsselt, bei letzterem mit asymmetrischen.

Frage 4.2

> Betrachten Sie die Ausgabe von ifconfig und schauen Sie sich das Device tun0 an. Wo kommt dieses her und warum hat es eine solch seltsame Ausgabe?

tun devices sind Geräte auf der dritten Netzwerkschicht und werden zur Verbindung von Client zum Netzwerkstack verwendet.
Somit werden Daten verschlüsselt, bevor sie durch den VPN-Tunnel geschickt werden.

Frage 4.3

> In Ihrem Browser mussten Sie in einer der vorigen Aufgaben das Zertifikat ihrer CA (myroot.cer) importieren, damit die gesicherte Verbindung über X.509 Zertifikate möglich war. Wie wurde dies für openVPN gelöst?

Das Zertifikat ist sowohl auf dem Server als auch dem Client vorhanden und wird in der Konfigurationsdatei angegeben.

Frage 4.4

> Weshalb verwendet openVPN ein neues virtuelles Netzwerk? Könnte der Client nicht direkt die Netzwerkadressen des Servers (192.168.X.Y) auf dem tun Interface (anstatt des 10er Netzwerks) verwenden?

Da das Tun-Interface auf der dritten Netzwerkschicht mit seiner eigenen IP angesprochen wird und nicht der des Server.

Frage 4.5

> Was bewirken die Schlüsselwörter CA, CERT und KEY in der openVPN Konfiguration?

- **CA** gibt das Rootzertifikat an.
- **CERT** beinhaltet das Zertifikat samt Public Key.
- **Key** beinhaltet den Private Key

Frage 4.6

> Was ist PAM und was bewirkt /usr/lib/openvpn/openvpnauthpam.so?

PAM steht für Plugable Authentication Modules und beschreibt Module die zur Authentifizierung von Nutzern verwendet werden können.
Mit den .so Dateien werden die verwendeten Module spezifiziert.

Frage 4.7

> Frage 4.7 Beschreiben Sie den Zweck und die Funktionsweise der Software rkhunter.

rkhunter ist ein Shellskript das das lokalte System auf Rootkits, Mallware und Exploits überprüft. Es überprüft Systemdateien, Befehle und Netzwerkschnittstellen.

Frage 4.8

> Welche Funktion haben die Werkzeuge strace, ltrace und ldd?

- **strace** ist ein Tool um Prozesse, während ihres Ablaufs zu beobachten.
- **ltrace** kann Systemcalls, Funktionsaufrufe und Signale welche an den Prozess und von ihm ausgehen, überwachen und abfangen.
- **ldd** gibt die geteilten Dependencies für die angegeben Objekte aus.

Frage 4.9

> Was tut das Werkzeug ssldump? Wie wird es eingesetzt?

Zeigt und analysiert SSL/TLS-Traffic.

Frage 4.10

> Welche Informationen landen in den in /var/log gespeicherten Log Dateien.
> • syslog
> • auth.log
> • dmesg

Syslog enthält Meldungen von Prozessen des Betriebssystems, Services und vielen weiteren Komponenten. Darunter Kernel Nachrichten und System daemons, sicherheits/autorisierungs Meldungen, Netzwerk benachrichtigungen etc. Eine Log ist dabei aus folgenden Teile aufgebaut.

- Priorität
- Version
- Zeitstempel
- Hostname
- Anwendung
- Process id
- Message id

Auth.log enthält Events in Bezug auf Authentifizierung.
Konkret stehen hier also Anmeldungen bzw. Anmeldeversuche auf Benutzerkonten!

Dmesg enthält Logs bzw. Meldungen des Kernel-Ringpuffers. Hier finden sich speziell Logdateien │ bezogen auf den Boot Vorgangs!

Frage 4.11

> Was findet sich in den Dateien .bash_history und .viminfo? Weshalb ist der Inhalt auch aus Sicherheitssicht interessant?

In der .bash_history findet man alle eingebenen Bash-Befehle und in .viminfo die Konfigurationen von Vim, sowie die dazugehörige Command-Line-History und Search-String-History.

Frage 4.12

> Wie und warum würden Sie sudo und die Datei /etc/sudoers in einem System mit mehreren Benutzern verwenden? Wie stehen die Dateien im Bezug zur Systemsicher- heit?

Sudo lässt einen User als ein anderer agieren. Dies ist besonders praktisch, wenn ein User vorübergehend Root-Rechte braucht.
In /etc/sudoers sind die entsprechenden Rechte und Einstellungen abgespeichert. Ebenso lässt sich hier ein log der erfolgreichen und misslungenen Authentisierungsversuche ansehen.
Alle Möglichkeiten der Datei hier aufzulisten sprengt den Rahmen. Rechtevergabe ist allerdings sicherheitsrelevant, sowie das loggen.