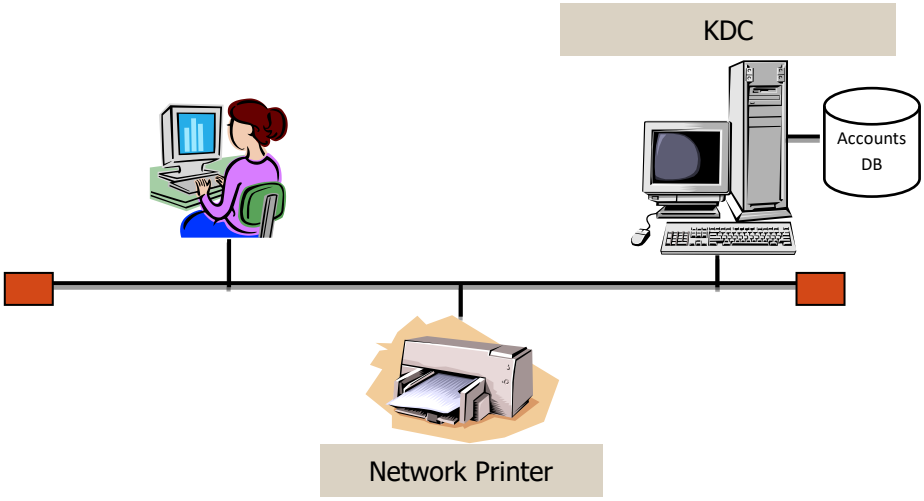
SVS | Exercise 8

Task 1

1. Alice möchte von ihrem Textverarbeitungsprogramm aus auf einen Netzwerkdrucker zugreifen. Sowohl das Textverarbeitungsprogramm als auch der Netzwerkdrucker sind an einen Key Distribution Center (KDC) angebunden. Beschreiben Sie, wie sowohl das Textverarbeitungsprogramm als auch der Netzwerkdrucker an ein gemeinsames Geheimnis rankommen, sodass der gegenseitige Datenaustausch vertraulich ablaufen kann. Welche Vorteile bringt der Einsatz von KDC?

1. Alice wants to use a network printer out of her text editor. Both the text editor and the network printer are connected to a Key Distribution Center (KDC). Describe how both the text editor and the network printer can obtain a session key, so that they can exchange data confidentially. What are the advantages of using KDC?



2. Eve gelingt es die Kommunikation während des Schlüsselaustauschs zwischen dem Textverarbeitungsprogramm, KDC und Netzwerkdrucker abzuhören. Kann sie die mitgeschnittenen Daten entschlüsseln?
3. Nach dem Abhören der Daten gelingt es Eve die Kommunikation zwischen dem Textverarbeitungsprogramm und dem Netzwerkdrucker zu unterbrechen. Sie zeigt dem Netzwerkdrucker die mitgeschnittenen Daten unverändert vor. Kann sie sich nun als Alice ausgeben?
4. Eve möchte den KDC umgehen und direkt auf den Netzwerkdrucker zugreifen. Gelingt ihr das?

2. Eve is able to sniff the traffic between the text editor, the KDC and the network printer during the key exchange. Is she able to decrypt the sniffed data key?
3. After sniffing the data Eve was successful in interrupting the communication between the text editor and the network printer. She forwards the unmodified sniffed data to the network printer. Is she now able to impersonate Alice?
4. Eve wants to bypass KDC and access the printer directly. Is it possible?

Task 2

Wiederholen Sie den Ablauf der Kerberos-Authentifizierung:

1. Das Betriebssystem von Alice ist an einen Kerberos Server angebunden. Alice möchte sich nun an ihrem Rechner anmelden. Beschreiben Sie, wie der Authentifizierungsvorgang abläuft.
2. Alice möchte nun auf einen Kerberos-fähigen Dienst, z.B. POP3, zugreifen. Muss Alice ihr Passwort erneut eingeben?
3. Wie überprüft der POP3-Dienst ob die Anfrage wirklich von Alice und von keinem anderen stammt? Wozu dienen die Zeitstempeln?

Repeat the process of Kerberos authentication:

1. The operation system of Alice has Kerberos integration. Alice wants to sign in into the system. Describe how the authentication process takes place.
2. Alice wants to access a Kerberos-enabled service, e.g. POP3. Does she have to re-enter her password?
3. How does POP3 service check if the request comes really from Alice? What are the timestamps used for?

Task 3

In einer Organisation wird ein LAN (IP-Bereich 192.168.0.0/24) mit einem Web/FTP-server (IP 83.160.17.4), und einer Firewall mit dynamischen Paketfilter (IP 220.20.117.6) betrieben (siehe Bild unten). Erstellen Sie Firewall-Regeln, die die unten aufgeführten Anforderungen erfüllen. Achten Sie dabei auf maximale Sicherheit.

- Der Zugriff auf den Webserver ist nur über HTTPS erlaubt (sowohl von außen als auch aus dem LAN)
- Der Zugriff auf den FTP-Dienst ist nur aus dem LAN erlaubt
- Die Administration vom Webserver soll per SSH erfolgen und nur von den Rechnern 192.168.0.6 sowie 192.168.0.7 möglich sein
- Der Zugriff aus dem LAN auf den Server eines Onlinespielebetreibers (IP 65.223.145.12) ist verboten.
- Der Zugriff auf TCP-basierte Internet-Dienste aus dem LAN ist erlaubt
- DNS-Anfragen aus dem LAN sind erlaubt

Füllen Sie die unten stehende Tabelle aus. Gehen Sie davon aus, dass die Regeln von oben nach unten verarbeitet werden. Die erste passende Regel bricht die Abarbeitung ab.

An organization operates a LAN (IP range 192.168.0.0/24) with a Web/FTP-server (IP 83.160.17.4), and a Firewall with dynamic packet filter (IP 220.20.117.6) (cf. illustration below). Create firewall rules, which fulfil the requirements below. Try to achieve maximum security.

- Access to the Web server should be allowed only using HTTPS (both from the internet and from the LAN).
- Access to the FTP service is allowed only from the LAN
- The administration of the Webserver should take place over SSH and only from the machines 192.168.0.6 and 192.168.0.7.
- Access from LAN to the server of an online game operator (IP 65.223.145.12) should be forbidden.
- Access to TCP-based internet services from the LAN is allowed.
- DNS requests from LAN are allowed.

Fill the table below. Assume, that the rules are executed from the top to the bottom until a matching rule is found. The first matching rule stops the further processing.

Action	Protocol	Interface	From	To	Port
Permit	TCP	any	any/any	83.160.17.4	443
…	…	…	…	…	…