IT-Sicherheit - Projektarbeit SS 2025

Jürgen Quade, Martin Grothe, Hochschule Niederrhein

1.7.2025

Allgemeines

Die Lehrinhalte des Fachs *IT-Sicherheit* (Bachelor Informatik, Bachelor Elektrotechnik, Bachelor Mechatronik) werden in Form einer digital als auch handschriftlich signierten Projektarbeit abgeprüft. Für die Projektarbeit finden Sie untenstehend drei Aufgaben, die Sie bearbeiten und dokumentieren. Beachten Sie, dass die Aufgabenstellung in einigen Teilen individualisiert ist. Um keinen Verdacht des Kopierens von anderen Lösungen aufkommen zu lassen, achten Sie bitte daher auch auf Details.

Über den Moodle-Exam-Raum https://moodle-exam.hsnr.de/course/view.php?id=6370 reichen Sie die Lösung ein. Die Dokumentation ist in **Markdown** zu verfassen und muss Ihre eidesstattliche, eigenhändig **unterschriebene** Erklärung der Eigenständigkeit enthalten. Zusätzlich wird die Dokumentation von Ihnen digital unterschrieben.

Formale Randbedingungen

- Abgaben:
  1. Dokumentation als Markdown- und PDF-Datei
  2. Digitale Signatur der PDF-Datei
  3. Zur Signatur gehörender Public Key (Unterschriftenprobe)
  4. Tar-Archiv mit den erstellten Dateien (Firewall-Skript)
- Ausgabe der Aufgabenstellung: 14.7.2025
- Letzer Abgabetermin: 30.8.2025 - 23.59 Uhr
- Arbeitsumfang: ca. 40h

Vorlage für die Eigenständigkeitserklärung

```
Eidesstattliche Erklärung zur Projektarbeit IT-Sicherheit im SS 2025

Name:
Matrikelnummer:

Ich versichere durch meine Unterschrift, dass die vorgelegte Arbeit
ausschließlich von mir erstellt und verfasst wurde. Es wurden keine
anderen als die von mir angegebenen Quellen und Hilfsmittel benutzt.

---------------             ------------------
Ort, Datum                  Unterschrift
```

Bewertung

Die Arbeit gilt als **nicht bestanden**, wenn einer der nachfolgenden Punkte zutrifft:

- Die Ausarbeitung ist nicht **fristgerecht** eingereicht worden.
- Die Einreichung ist **unvollständig**.
- Die Eigenständigkeitserklärung liegt nicht vor.
- Die Eigenständigkeitserklärung ist nicht handschriftlich **unterschrieben**.
- Die Abgabe ist nicht korrekt per GPG digital signiert.
- Der Public-Key zur digitalen Unterschrift fehlt.
- Die Projektarbeit ist mit **weniger als 50 Punkten** bewertet worden.
- Die Projektarbeit weist nicht die geforderte **Individualisierung** auf.

Notenskala

```
00-49 = 5,0
50-54 = 4,0
55-59 = 3,7 | 60-64 = 3,3 | 65-69 = 3,0
70-74 = 2,7 | 75-79 = 2,3 | 80-84 = 2,0
85-90 = 1,7 | 90-94 = 1,3 | 95-100 = 1,0
```

Falls die Arbeit bestanden ist, werden zur Notenbildung die in der Übung des aktuellen Semesters gesammelten **Bonuspunkte** hinzuaddiert.

Dokumentation

Die Dokumentation ist im Format *Markdown* zu erstellen und im PDF-Format zu rendern. Dazu setzen Sie das freie Programm `pandoc` ein. Als Basis für die Dokumentation finden Sie im Moodle-Lernraum ein Template, das Ihnen Hinweise zum Aufbau und zur Formatierung des Dokuments gibt.

Achten Sie darauf, dass sich in der Dokumentation unter anderem die nachfolgenden Dinge befinden:

- Aufgabe Passwörter
  - Defintion Algorithmus
  - Auswahl Testdomains plus Begründung
  - Passwörter für die ausgewählten Domains
- Aufgabe angewandte Kryptografie
  - Entschlüsselung der Geheimnachricht
  - Antwortmail von *Mira de la Mar*
  - OpenVPN-Client-Konfiguration
  - Antworten bezüglich der Zugriffsrechte
  - Inhalt der im Homeverzeichnis abgelegten Datei
- Aufgabe Firewall
  - ICMP-Pakettypen
  - Testplan
  - `izpriv_fw.sh`
  - Screenshots
- Aufgabe Sichere Netzplanung
  - Netzwerktopologie
  - `izfirewall.sh`

Die Dokumentation muss lesbar und strukturiert sein.

Digitale Signatur

- Die Dokumentation (PDF) muss digital auf Basis von **GPG** respektive **PGP** signiert sein.
- Die digitale Unterschrift wird über eine separate Datei gewährleistet.
- Der **Public-Key** zur digitalen Signatur muss mit eingereicht werden.

---

1. Passwörter

1. Definieren Sie analog zu den in der Vorlesung vermittelten Prinzipien einen Algorithmus zur Generierung von Passwörtern, die für das Login auf Webseiten oder Geräten genutzt werden können. Die Definition muss auch den Fall abdecken, dass der Hashwert Ihres Passworts auf einer Webseite (z.B. durch Einbruch) bekannt geworden ist (Stichwort Passwort-Versionierung).
2. Wählen Sie **acht** unterschiedliche Domains/Fälle aus, anhand denen Sie die Tauglichkeit des von Ihnen definierten Algorithmus testen können. Sinnvolle Auswahlkriterien könnten beispielsweise *kurze Domain* oder *Zahlen in der Domain* sein. Begründen Sie Ihre Auswahl!
3. Wenden Sie Ihren Algorithmus auf die acht Domains an.

---

2. Angewandte Kryptografie

Die Aufgabe baut auf einer komplexen Infrastruktur, bestehend aus diversen Systemkomponenten, auf, die unter Umständen nicht zu jeder Zeit störungsfrei zur Verfügung stehen. Melden Sie sich, wenn Sie den Eindruck haben, dass beispielsweise der Mailbot, der OpenVPN-Server oder der Rechner im OpenVPN nicht ordnungsgemäß arbeiten.

1. Gegeben ist die per XOR-Verfahren per Cipher Block Chaining (xor(cbc)) verschlüsselte Geheimnachricht in hexadezimaler Form:

   14 20 16 72 16 73 15 2b 17 36 43 21 41 20 4c 2a 4a

   Entschlüsseln Sie die Nachricht, wenn der Schlüssel "0x55" und der Initialisierungsvektor "0x29" lautet. Dokumentieren Sie die Entschlüsselung.

   Hinweis: Die entschlüsselte Geheimnachricht besteht aus zwei Worten, wobei das erste Wort mit "hac" beginnt und das zweite Wort nur aus Ziffern besteht. Die dezimale Quersumme aus den zehn Ziffern beider Wörter beträgt 38.

2. Schicken Sie die entschlüsselte Nachricht (die beiden Worte) in einer verschlüsselten und signierten EMail an *Mira de la mar* (mira@quku.de). Verwenden Sie als *Subject* "Geheimnachricht von Zimmermann".

   Falls die Mail korrekt verschlüsselt und signiert ist und die korrekte Nachricht enthält, schickt Ihnen Mira das Passwort zu einem Veracrypt-Container zu. Ignorieren Sie den in der Mail befindlichen Tipp.

3. Übernehmen Sie Miras Antwort (per copy-paste) als Klartext in die Dokumentation.

4. Laden Sie sich unter https://hs-niederrhein.sciebo.de/s/gHihaYox0KBskcE den Veracrypt-Container `facd7317fe885cab5b8d009b62387a64.vc` herunter. Das Passwort zum Sciebo-Ordner bilden Sie über ROT+1 des (kompletten) Wortes "3tryittoday1".

5. Mounten Sie den Veracrypt-Container mit Hilfe des Passwortes, das Ihnen Mira gesendet hat. Im Container finden Sie Ihre persönlichen Credentials, die Ihnen Zugang zu einem OpenVPN geben.

6. Erstellen Sie mit Hilfe der folgenden Eckdaten eine OpenVPN-Client-Konfiguration, die Sie in die Dokumentation mit aufnehmen.

   - Server-IP: 194.94.121.241
   - Portnummer: 11194
   - Protokoll: tcp

7. Verbinden Sie sich mit dem OpenVPN. Loggen Sie sich per *ssh* auf dem Rechner mit der IP `172.18.1.99` mit dem Loginnamen `kr-zimmermannben` ein. Als Passwort nehmen Sie das in Teilaufgabe 1 entschlüsselte, **zweite, nur aus Ziffern bestehende** Wort.

   Im Verzeichnis finden Sie eine Datei, deren Name identisch mit dem in Teilaufgabe 1 entschlüsselten Wort ist.

   Beantworten Sie in der Dokumentation die folgenden Fragen:

   - Welche Zugriffsrechte hat Ihr **Homeverzeichnis** auf dem Rechner `172.18.1.99`?
   - Dokumentieren Sie die Zugriffsrechte der Datei, die mit "hac" beginnt.
   - Ändern Sie die Zugriffsrechte auf die Datei, so dass nur der Besitzer auf die Datei **lesend** zugreifen kann. Ein schreibender oder ausführender Zugriff soll für niemanden möglich sein. Dokumentieren Sie das Kommando.

8. Lesen Sie die Datei aus und geben Sie den Inhalt in der Dokumentation an.

9. Legen Sie in Ihrem Homeverzeichnis eine neue Datei an. Der Name der Datei soll Ihrer User-ID (Kommando `id -u`, zum Beispiel 1142) entsprechen. In der Datei selbst soll die aktuelle Zeit abgespeichert sein, also die Ausgabe des Kommandos `date`. Dokumentieren Sie, mit welchen Kommandos Sie die Datei angelegt haben.

---

3. Firewall

Ihre lokale Linux-Instanz soll über eine Firewall abgesichert werden. Die Firewall soll die folgende Kommunikation erlauben:

- OpenVPN-Client über Port 11194 mit Rechner 194.94.121.241
- ICMP (Echo Request und Echo Reply) mit 194.94.121.241
- SSH Client mit Rechner 172.18.1.99
- ankommende Echo Request Pakete
- ausgehende Echo Reply Pakete

Andere Kommunikationsbeziehungen sind **nicht** erlaubt.

1. Informieren Sie sich im Internet über die verschiedenen Pakettypen von ICMP. Listen Sie 10 Pakettypen in der Dokumentation auf.
2. Entwerfen und dokumentieren Sie einen Plan, mit dem die Firewall getestet werden kann. Der Plan besteht aus den auszuführenden **Kommandos** (zum Beispiel `ping -c 4 x.x.x.x`), dem **erwarteten Ergebnis** (zum Beispiel `100% Paketverlust`) und eine **Beschreibung**, was genau mit den Befehlen getestet werden soll.
3. Entwerfen Sie ein Firewallskript `izpriv_fw.sh` für Ihren Rechner gemäß der oben stehenden Kommunikationsbeziehungen und dokumentieren Sie dieses.
4. Aktivieren Sie auf Ihrer lokalen Linux-Instanz die Firewall und verbinden Sie sich mit dem OpenVPN (siehe vorherige Aufgabe).
5. Öffnen Sie ein Terminalfenster und führen Sie die nachfolgenden Kommandos (auf Ihrem lokalen System) aus. Fertigen Sie einen Screenshot vom Terminalfenster (**nicht vom gesamten Bildschirm**) über die Ausführung der Kommandos an, den Sie in die Dokumentation mit aufnehmen:

```
echo "zimmermannben: CHECK PARAMS"
date
id
ip -br a
ping -c 3 194.94.121.241
ping -c 3 172.18.1.99
echo "END"
```

---

6. Öffnen Sie auf Ihrem lokalen Linux Rechner ein Terminal, bauen Sie gemäß nachfolgendem Kommando eine SSH-Verbindung zum Rechner 172.18.1.99 auf.

   ```
   ssh kr-zimmermannben@172.18.1.99
   ```

   Führen Sie auf dem Rechner 172.18.1.99 die nachfolgenden Kommandos aus und fertigen Sie als Beleg einen Screenshot vom Terminalfenster (**nicht vom gesamten Bildschirm**) über die Ausführung der Kommandos an, den Sie in die Dokumentation mit aufnehmen:

```
echo "START REMOTE CHECK (zimmermannben)"
# Sie sind jetzt auf dem entfernten Rechner
id
who
ip -br a
ping -c 4 194.94.121.241
ping -c 4 <Ihre IP im VPN>
echo "END"
```

---

4. Planung sicherer Netze

Eine Werbeagentur ist über eine Linux-Firewall mit der IP-Adresse 94.97.121.154 mit dem Internet verbunden. Die Agentur selbst ist in einen Kreativ-Bereich und einer Verwaltung gegliedert. Neben einem Webauftritt, der von der Agentur vor Ort (on premise) gehostet wird, gibt es einen Server mit einer Bilddatenbank. Auf der Linux-Firewall ist ein OpenVPN-Server installiert, über die der Zugang auf die Bilddatenbank auch von außerhalb (Home-Office) möglich wird.

Die Firewall der Agentur greift auf die in der nachfolgenden Tabelle unter *Clientdienste* gelisteten Services im Internet zu. Unter *Serverdienste* befinden sich die Dienste, die die Firewall selbst zur Verfügung stellt. Ob der Dienst nur von intern oder auch über das Internet genutzt werden kann, ist in Klammern vermerkt.

Die Rechner der Mitarbeiterinnen und Mitarbeiter nutzen die als intern gekennzeichneten Serverdienste (SSH, NTP, DNS, HTTPS, Datenbank). Für den Zugriff auf das Internet soll die Firewall nur die Dienste HTTP und HTTPS freigeben.

Komponente	Serverdienste	Clientdienste
Firewall: 94.97.121.154	• SSH (intern, extern) • NTP (intern) • DNS (intern) • OpenVPN (intern, extern)	• SSH Internet • NTP Internet • DNS Internet
Web-Server: 172.24.84.119	• SSH (intern, extern) • https (intern, extern)	• DNS (intern) • NTP (intern)
Bilddatenbank: 172.24.84.110	• SSH (intern, vpn) • Datenbank (intern, vpn)	• DNS (intern) • NTP (intern) • OpenVPN

1. Planen Sie das Netzwerk im Hinblick auf IT-Sicherheit und vergeben Sie Netz- und IP-Adressen. Erstellen Sie ein Bild der **gesamten**, auf Sicherheit ausgerichteten Netzwerktopologie. Kennzeichnen Sie Netz- und IP-Adressen und auf den Servern angebotene Dienste.
2. Erstellen Sie ein Shell-Skript `izfirewall.sh` mit den Regeln für die Linux-Firewall. **Kommentieren** Sie die Regeln!

Bewertungskriterien

Bei der Benotung der Arbeit werden unter anderem die folgenden Aspekte berücksichtigt:

- Digitale Signatur
- Passwortgenerierung
  - Korrektheit (liefert unter allen Umständen “sichere” Passwörter)
  - Ausgewogene Komplexität des Algorithmus (muss ohne Hilfsmittel anwendbar sein)
  - Sonderfälle (Versionsmanagement)
  - Sinnhaftigkeit und Begründung für die Beispiel-URLs
- Angewandte Kryptografie
  - Entschlüsselung der Geheimnachricht
  - Mailverkehr mit Mira de la Mar
  - Umgang mit VeraCrypt
  - OpenVPN-Client-Konfiguration
  - SSH
  - Umgang mit Zugriffsrechten
  - Zugriff auf die abgelegte Datei
- Firewall
  - Dienste sind gemäß Anforderung nur von außen und *NICHT* von innen erreichbar
  - Filterung über IP-Adressen *und* Interface
  - Kommentierter Testplan und Test
- Sichere Netzplanung
  - Vollständigkeit
  - Korrektheit
  - Struktur
  - Aussagekräftige Kommentierung
- Dokumentation
  - Aufbau der Arbeit
  - Vollständigkeit
  - Aufgelockertes Schriftbild (z.B. für Grafiken)
  - Lesbarkeit
  - Zusammenfassung
  - Rechtschreibung und Kommasetzung
  - Quellenangaben