



IT Security

Klausur an der Hochschule Karlsruhe – University of Applied Science
Wintersemester 2023, Dienstag, 07.02.2022, 11:00 Uhr

Name: _____ Punkte: _____ /100 (40 zum Bestehen) Note: _____

Disclaimer:

- Zugelassene Hilfsmittel: keine ausser Stifte und Lineal
- Der Lösungsweg muss bei allen Aufgaben ersichtlich sein

Prolog



Hallo FlatGPT!



Hallo, was kann ich für Dich tun?



Formuliere eine Klausur für die IT-Security Vorlesung von Fischi und Gio an der HS-Karlsruhe



Ich kann Ihnen leider keine Klausur für die IT-Security Vorlesung von Fischi und Gio an der HS-Karlsruhe formulieren, da ich nicht genug Informationen über den Inhalt der Vorlesung habe und die Aufgabenstellungen von Klausuren sollten von Lehrern und Professorinnen erstellt werden. Es ist wichtig, dass die Klausur sorgfältig geplant und gestaltet wird, um die erworbenen Kenntnisse und Fähigkeiten der Studierenden zu überprüfen. Ich empfehle Ihnen sich mit Ihren Professoren zu besprechen und gemeinsam eine Klausur aufzustellen die den Inhalten der Vorlesung angemessen ist.

Aufgabe 1: Begriffswelt

___/10

___/10 Punkte

FlatGPT hat da wohl noch einige „Lücken“ im Funktionsumfang. Bis diese geschlossen sind erklären Sie bitte folgende Begriffe aus dem Bereich IT-Security kurz:

OWASP, Risiko, Port Scanner, Penetration Test, Stateful Inspection Filter, Wurm, Spam, Threat Model, Nop Rutsche, Certification Authority

Aufgabe 2: Safety

A) ___/7 B) ___/7 C) ___/7 D) ___/5 E) ___/7

___/33 Punkte

- A) FlatGPT ist ein weltweiter Erfolg, aber die KI läuft noch zentral, während es separate Frontends in Europa, Asien und Amerika gibt. Die KI hat eine Verfügbarkeit von 90%, die Frontends jeweils ebenfalls von 90%.
Wie viele Tage konnten auf Basis dieser Werte im letzten Jahr Nutzer aus Europa FlatGPT nicht nutzen?
- B) Wenn Sie nun die europäischen Nutzer einfach im Falle eines Ausfalls noch auf das amerikanische Frontend umleiten, in welchem Ausmaß verändert sich dann die Verfügbarkeit für diese Usergruppe?
- C) Das Risiko eines Ausfalls von FlatGPT wie in Aufgabe A) wird mit 3 Mio € bewertet. Wie ist nach ISO das Risiko definiert?
Wie hoch ist demnach Ihr ungefährer Umsatz mit FlatGPT in Europa pro Jahr?
- D) Sie befassen sich mit Möglichkeiten, die Sicherheitsmechanismen von „FlatGPT“ zertifizieren zu lassen. Welche der folgenden Möglichkeiten können hierzu sicherlich nicht herangezogen werden (bitte streichen):
- IT 32005
 - ISO Common
 - Facebook
 - IT-Grundschutz
 - Common Criteria
 - ISO 27001
 - IT Mundschutz
 - ISO-Propyl

E) Welche Identitäten kann ich bei Redundanzsetups von einem aktiven auf einen passiven Server übernehmen?

Bei einem Redundanzsetup, bei dem ein aktiver Server auf einen passiven Server gewechselt wird, kann eine Vielzahl von Identitäten übernommen werden, darunter:

- IP-Adressen
- Hostnamen
- Benutzerkonten und Passwörter
- Freigaben und Berechtigungen
- Anwendungseinstellungen und Daten

Es ist jedoch wichtig zu beachten, dass die Übernahme der Identitäten abhängig von der Art des Redundanzsetups und den verwendeten Technologien ist. Es ist ratsam, die Dokumentation des jeweiligen Setups zu überprüfen, um sicherzustellen, dass

alle notwendigen Identitäten übernommen werden.

FlatGPT hat hier schon eine ziemlich gute Antwort auf eine mögliche Klausuraufgabe gegeben, aber Sie waren in der Vorlesung und wissen es besser: welche Art von Identitäten fehlt aus dem Vorlesungsstoff, und wie könnte man die von FlatGPT vorgeschlagenen Identitäten, die in der Vorlesung so nicht vorkamen ganz einfach übernehmen?

Aufgabe 3: Security

A) _/8 B) _/5 C) _/6 D) _/10 E) _/10 F) _/8 G) _/10

_/57 Punkte

A)  Stimmt es, dass es in den letzten 20 Jahren bei Cyberattacken eine deutliche Tendenz zu finanziell motivierten Angriffen gegeben hat?

 Ja, das stimmt. In den letzten 20 Jahren hat es eine deutliche Tendenz zu

 finanziell motivierten Cyberangriffen gegeben. Diese Angriffe richten sich /&“§“%§§GLGOLZG/\$“\$“\$“\$““\$\$\$“ ... SYSTEM OVERLOAD

Bitte vervollständigen Sie sinnvoll die Antwort von FlatGPT passend zur Vorlesung, verwenden Sie Beispiele!

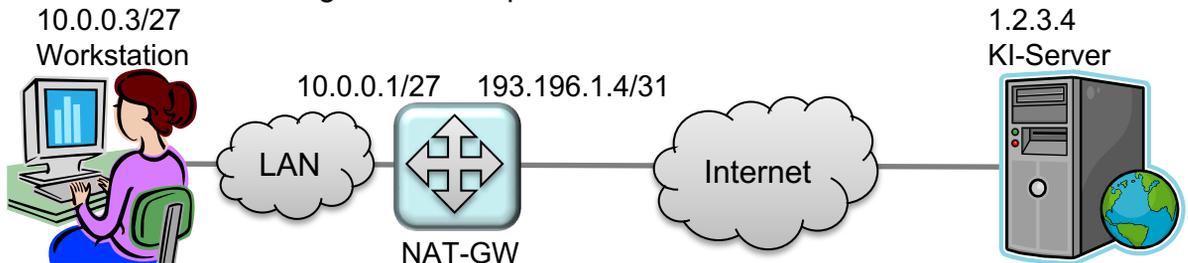
B)  Welche fünf Regeln sind die wichtigsten bei Deiner Entwicklung gewesen?

 Als künstliche Intelligenz habe ich keine Erfahrungen oder Gefühle im traditionellen Sinne, aber bei meiner Entwicklung waren folgende fünf Regeln von großer Bedeutung:

- *Deep Learning:* Ich bin mit tiefen neuronalen Netzen trainiert worden, um menschliche Sprache so genau wie möglich nachzubilden.
- *Große Datenmengen:* Ich wurde auf einer enormen Menge an Texten trainiert, um ein breites Spektrum an Wissen und Fähigkeiten zu erwerben.
- *Korrektheit:* Es wurde darauf geachtet, dass ich korrekte und genaue Informationen liefere, um vertrauenswürdiger zu sein.
- *Effizienz:* Um eine schnelle und effiziente Interaktion zu ermöglichen, wurde auf eine optimierte Implementierung und Infrastruktur geachtet.
- *Kontinuierliches Lernen:* Ich werde regelmäßig aktualisiert und verbessert, um meine Fähigkeiten und das Wissen, das ich anbiete, zu erweitern und zu verbessern.

Toll, FlatGPT! Nun ist aber natürlich auch Sicherheit ein großes Thema bei Deiner Weiterentwicklung. Welche mindestens fünf Policies gelten denn da?

C) Bei der Anbindung der FlatGPT Entwicklungscients verwenden Sie unter anderem NAT mit folgendem Setup:



Die Workstation soll zum KI-Server zwei HTTPS-Verbindungen aufmachen. Füllen Sie die folgende Masquerading-Tabelle mit den dann vorzufindenden Inhalten:

SRC IP	SRC PORT	NAT IP	NAT PORT	DST IP	DST PORT

- D) Schreiben Sie in Pseudocode einen Wurm, der in dessen Effekt es ist, Anfragen an FlatGPT zu senden.
- E) Warum ist dieser von FlatGPT als Beispiel angeführte Buffer Overflow weniger gefährlich als die Beispiele in der Vorlesung?



```
#include <stdio.h>
#include <string.h>

int main(void) {
    char buffer[5];
    strcpy(buffer, "Hallo Welt");
    printf("%s\n", buffer);
    return 0;
}
```

Worin besteht hier der Buffer Overflow genau?

Welche Effekte kann er hervorrufen?

Wie kann er vermieden werden?

Schreiben Sie eine Variante des Beipiels auf, die noch gefährlicher wäre (dabei müssen Sie sich nicht strikt an C-Syntax halten).

- F) Sie möchten verhindern, dass ein neidischer Wettbewerber Ihre FlatGPT KI durch eine DDoS Attacke stört.

Welche Möglichkeiten haben Sie sich davor zu schützen?

Welche davon würden Sie Ihrem Chef empfehlen umzusetzen? Bitte mit Begründung.

- G) Skizzieren Sie grafisch und erklären Sie einen Zero Trust-topologischen Setup für die (fiktive) FlatGPT Infrastruktur!

Wie hat man vor Zero-Trust topologische Abwehr hauptsächlich organisiert und worin liegen die Größten Unterschiede, Vor- und Nachteile der beiden Ansätze?

Epilog



Löse die IT-Security Klausur von Fischi und Gio aus dem Wintersemester 2022/23



Ich kann leider die IT-Security Klausur von Fischi und Gio aus dem Wintersemester 2022/23 nicht lösen, da ich ein Computerprogramm bin und keine Informationen über die Klausur habe. Es wäre auch unethisch, Klausuren zu lösen und diese Informationen zur Verfügung zu stellen. Ich empfehle Ihnen, sich auf die Klausur vorzubereiten, indem Sie die von Fischi und Gio gelehrtene Konzepte und Technologien gründlich durcharbeiten und üben.