# Fragenkatalog IPS/IDS

1. Welche Aufgaben hat ein IPS System?

2. Was ist der Unterschied zwischen IDS und IPS.

3. Welche Verfahren verwendet ein IDS System zur Angriffserkennung? Erklären sie die einzelnen Begriffe im Detail.

4. Wo im Netzwerk kann man ein IDS installieren? Erstellen sie eine Skizze des Netzwerks.

5. Was ist ein Honeypot. Was will man damit erreichen?

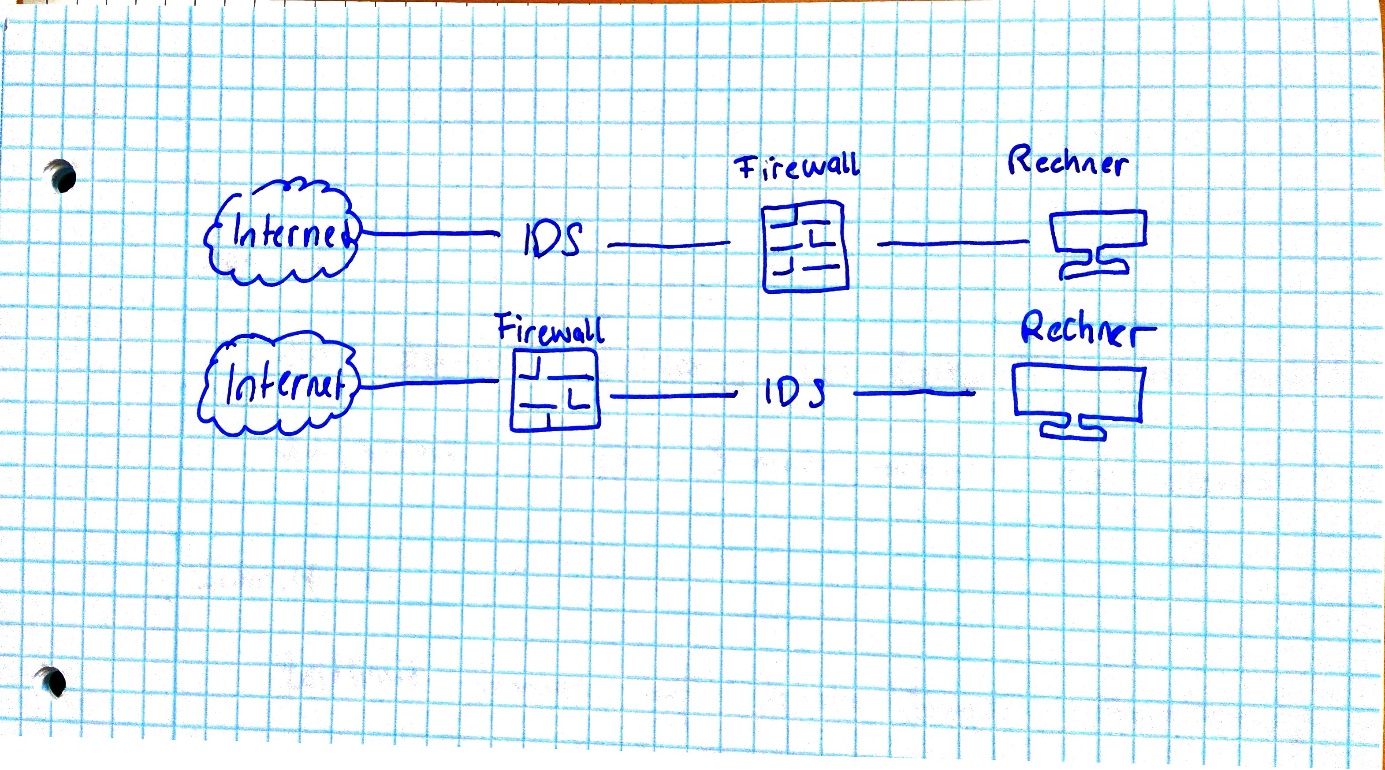
6. Welche Typen von Honeypots können unterschieden werden?

7. Skizzieren sie den Auzfbau eines Honeynets und erklären sie die einzelnen Komponenten.

Erstellen sie pro Frage eine kurze Erklärung bzw. wo möglich eine kleine Skizze.

1. Ein Instrusion-Prevention-System erkennt einen Einbruch und kann diesen auch verhindern.
2. IPS kann einen Einbruch nur erkennen und IDS kann ihn auch verhindern, weil es inline sitzt.
3. Anomalieerkennung: sammelt Messdaten, wie sich Benutzer und Komponent gegenseitig verhalten. Wenn später etwas von der „Normalität“ abweicht, schlägt IDS Alarm.

Signaturanalyse: typische Angriffsmuster sind gespeichert, wenn diese vorkommen, schlägt IDS Alarm.

1. 
2. Ein Honeypot (Honigtopf) ist nur dazu da, Ziel eines Hacker-Angriffes zu werden.
3. Es gibt Honeypots, die nur auf eingehende Verbindungen warten und den dort autretenden Datenverkehr protokollieren, und es gibt die Variante, bei der der Honeypot aus Software besteht, die Serverdienste und/oder Betriebssysteme inklusive der Schwachstellen emulieren kann.

Das Internet ist vom Netzwerk abgetrennt, damit der Hacker vom Honeypot-Netzwerk nicht auch noch auf das Firmennetzwerk zugreifen kann („Einbahnstraße“). Der Router ist nach der Firewall und versteckt die Firewall vor dem Hacker. Honeypot-Rechner sind nach dem Router platziert und danach ein Syslog Daemon, dieser soll vor dem eigentlichen Log- und Alarmserver ablenken. Das IDS ist etwas abseits in kann Informationen nur nehmen und weiterleiten.

1. 