



## Security Monitoring Tools and Techniques

Study online at [https://quizlet.com/\\_97zrd4](https://quizlet.com/_97zrd4)

- 
- |                                     |   |
|-------------------------------------|---|
| 1. <b>Neural net-work-based IDS</b> | Which IDS has the capacity to update its database and self-learn? |
|-------------------------------------|---|
- 
- |                  |   |
|------------------|---|
| 2. <b>Sensor</b> | Component of IDS that collects the data |
|------------------|---|
- 
- |                                 |   |
|---------------------------------|---|
| 3. <b>Statistical based IDS</b> | Which IDS has the highest number of false alarms? |
|---------------------------------|---|
- 
- |                     |   |
|---------------------|---|
| 4. <b>Honey pot</b> | A setup to capture information pertaining to the intruder in order to proactively strengthen security controls is known as: |
|---------------------|---|
- 
- |                                 |  |
|---------------------------------|--|
| 5. <b>To gather information</b> | What is the first action performed by an intruder/attacker in preparation for a system attack? |
|---------------------------------|--|
-