Čo je honeypot

Last updated March 18, 2025

Honeypot je termín používaný v oblasti počítačovej bezpečnosti, ktorý označuje pascu na hackerov a ďalších neautorizovaných používateľov. Ide o server, službu alebo dáta zámerne vystavené na internete, ktoré sa **maskujú ako relevantný cieľ pre útočníkov**, ale v skutočnosti sú od zvyšku infraštruktúry izolované a starostlivo monitorované.

Cieľom honeypotu je prilákať útočníkov, aby sa pokúsili o prenik alebo útok, čo umožní správcom siete identifikovať a analyzovať používané nástroje, metódy a techniky.

Na základe týchto cenných dát môžu spoločnosti následne lepšie zabezpečiť svoju infraštruktúru.

Honeypoty sa líšia podľa zamerania a zložitosti na:

- **Nízku interakciu**: Tieto honeypoty zvyčajne simulujú len určité sieťové služby a protokoly, aby prilákali základné útoky. Sú relatívne jednoduché na nasadenie a správu.
- **Vysokú interakciu**. Tieto systémy poskytujú realistickejšie a komplexnejšie prostredie, ktoré môže zahŕňať celé operačné systémy a aplikácie. Cieľom je prilákať pokročilejších útočníkov a získať podrobnejšie informácie o ich metódach.
- **Spam traps**: Tento typ honeypotu je navrhnutý na zachytenie nevyžiadanej pošty (spamu). Poskytuje falošné e-mailové adresy, ktoré by mali byť používané len spamermi.
- **Honeynets**: Ide o siete obsahujúce viac honeypotov, ktoré spoločne simulujú realistické sieťové prostredie, aby prilákali sofistikovanejších útočníkov.