??
??
•$Distributed Denial of Service (DDoS)$
•$Click fraud$
•$Extortion$
•$Spambots$
•$Password - cracking$
•$Bitcoin mining$
•$Decoys$
•$Sensors$
•$Mimic existing systems$
•$Inside the network$
•$Extensive Logging Potential$
•$Goal - oriented$
•$Few False Positives$
•$Offensive and Defensive$
•$It is actively maintained by a dedicated community, with quick response times to queries and bug - fixes.$
•$It enables attackers to gain access to the honeypot using SSH and Telnet, both protocols widely exploited by IoT botnets.$
•$Cowrie fully emulates a Debian installsation, with an out - of - the - box configurable file system that an attacker can int$
•$It is an open - source project, allowing users to adapt the honeypot to suit their specific needs.$
•$Cowrie records interactions between the attacker and the honeypot, logging everything from commands executed and files do$
•$Cowrie does not limit the number of simultaneous sessions, and can present a mock file system and shell to each attacker inde$
•$The fact that the Cowrie software doesn't call on any external sofware to operate makes it much less vulnerable to third - par$
??