10.11

<https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/#:~:text=A%20honeypot%20is%20a%20cybersecurity,methods%20and%20motivations%20of%20adversaries>.

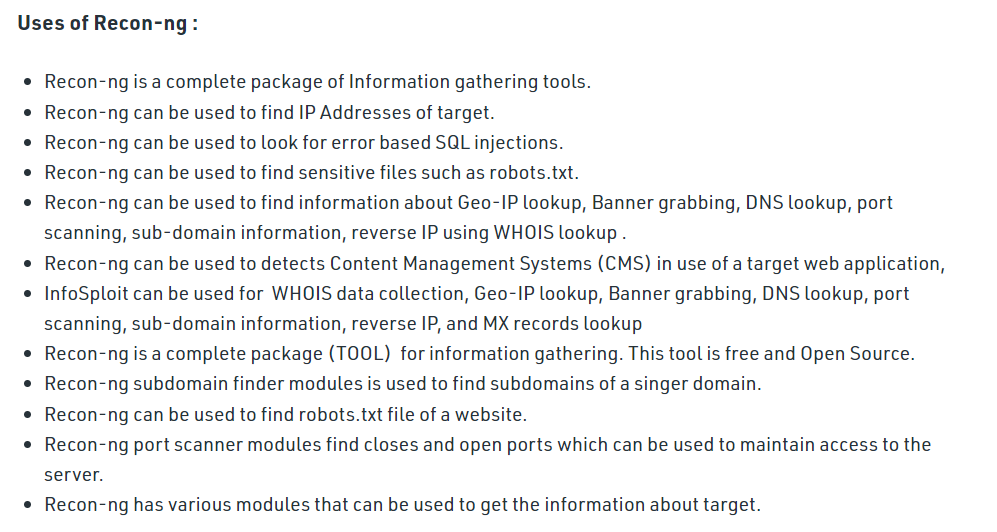
https://www.comparitech.com/net-admin/how-to-establish-a-honeypot-on-your-network/

procitao ove clanke

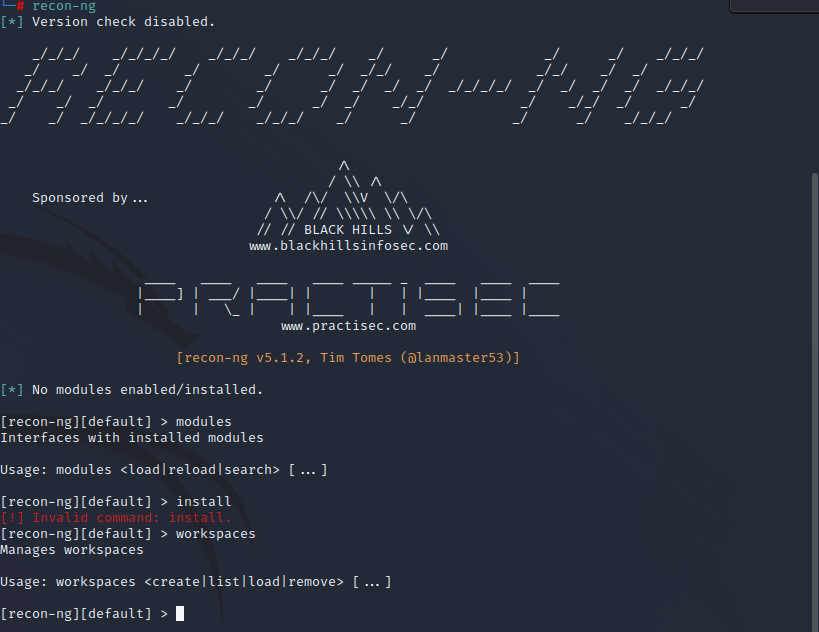
11.11

Recon-ng

ovo je alat koji se koristi u OSINTu i ima mnoge primjene ali jedna od najbitnijih stvari za reci je da s ovim alatom mozemo naci neciju IP adresu



12.11



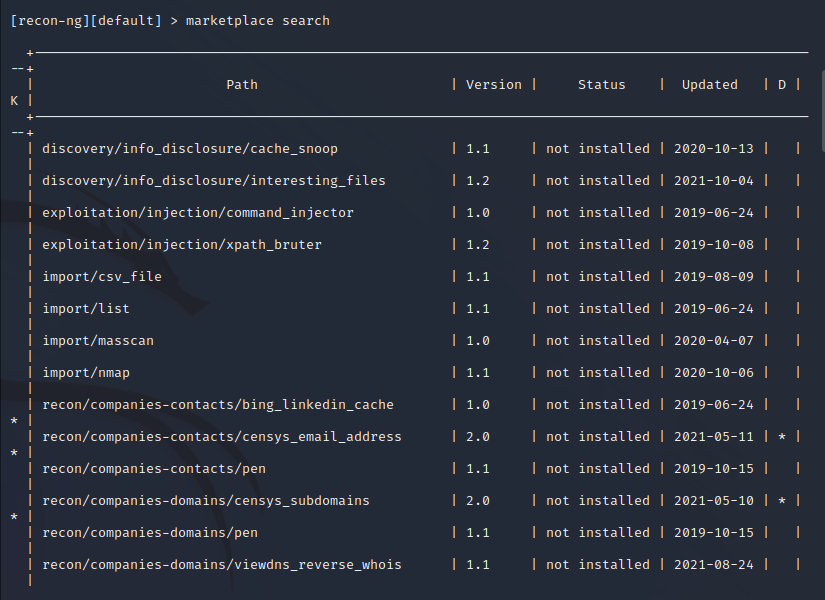
aplikacija dolazi instalirana sa kali linux virtualnim strojem

alat je besplatan i jedan od najkoristenijih na trzistu

runna na dockeru pa je system independant

unutar aplikacije mogu odrzavati vise workspaces, postoji markeplace s kojeg mogu instalirati module koji mi trebaju i loadam ih po zelji

osim pasivnih metoda recona ovaj alat cak sadrzi i par intruzivnih metoda kao sto se moze vidjeti na slici



zanimljivi su i moduli pronalaska linked in profila gdje sam našao nekolicinu za hepove zaposlenike

13.11

<https://security.stackexchange.com/questions/90642/is-it-possible-to-detect-a-honeypot>

<https://www.hindawi.com/journals/scn/2019/2627608/>

citao sam o tome kako prepoznati kada se nalazim unutar honeypot sustava i je li to uopce moguce