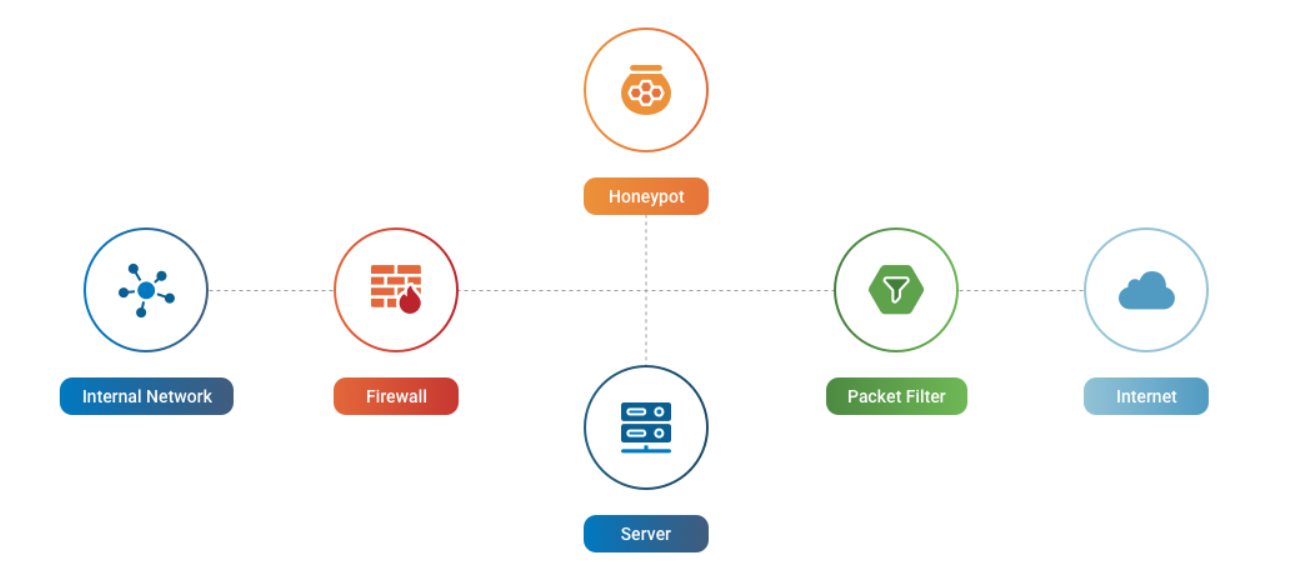
8.12

<https://techtalk.gfi.com/honeypot-security-system-strategy/>

* kako bi uspjesno zavarali napadace s nasim honeypotom on ne smije biti samo server koji je otvoren nego u njega moramo pohraniti na razna mjesta informacije zbog kojih bi napadač mislio da nije u honeypotu. (info mozemo stavljati lazne)



pitanje koje mi se ispostavilo teze nego sto sam mislio je kako razluciti dezinformacije od tocnih informacija u OSINTu

<https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html>

ovo su neki od alata koji nam mogu pomoću u autentifikaciji podataka

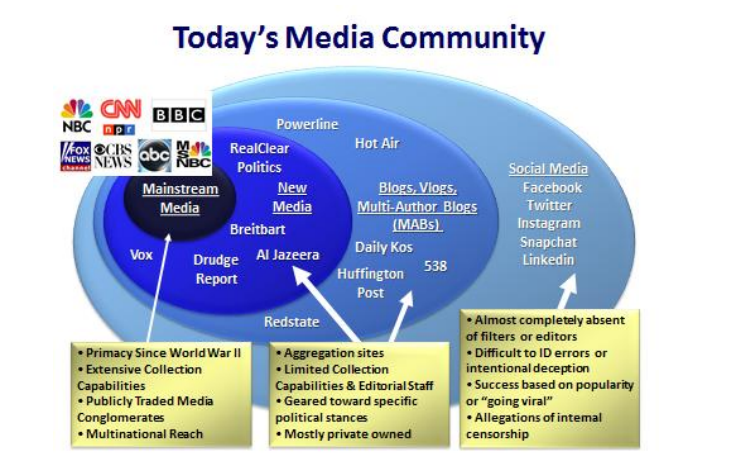
9.12

<https://www.afahc.ro/ro/rcic/2018/rcic'18/volum_2018/391-396%20Olaru%20Stefan.pdf>

jako zanimljiv rad koji mi je pomogao doći do zaključaka o OSINTu

zapravo je poanta da stvaramo cjelokupnu sliku i indukcijom i dedukcijom ispitujemo podatke i kako se odnose prema drugima, trazimo nepraviljnosti.

Ovaj proces moze zahtjevati puno vremena.



takoder sam kroz svoje istrazivanje naisao na alate kao BotSlayer koji omogućuje prepoznavanje laznih informacija na twitteru

10.12

poceo sam istrazivati CyberSecurity forume na internetu što mi se pokazalo učinkovito jer postoji puno već riješenih problema koji su dobro objašnjeni i argumentirani

<https://www.youtube.com/playlist?list=PL423I_gHbWUUOs09899rex4t2l5py9YIk>

do sada najzanimljiviji pronalazak tutorijala kako razne OSINT tehnike koristiti



11.12

<https://github.com/Ph055a/OSINT_Collection>

ovdje je vec velika kolekcija prikupljenih OSINT podataka iz razlicitih domena sto bi moglo biti dosta korisno u prakticnoj provedbi OSINTa nad nekim

takoder postoji fact checking odjeljak koji je nama za potrebe honeypota mozda i najbitniji

Još jedino pitanje koje mi ostaje za odgovoriti je kako na svom honeypotu postavljati “dummy” podatke da bi napadač potencionalno nasjeo na to