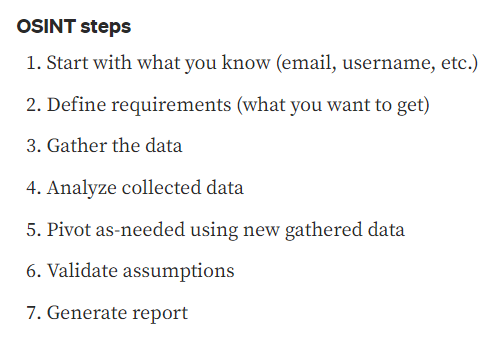
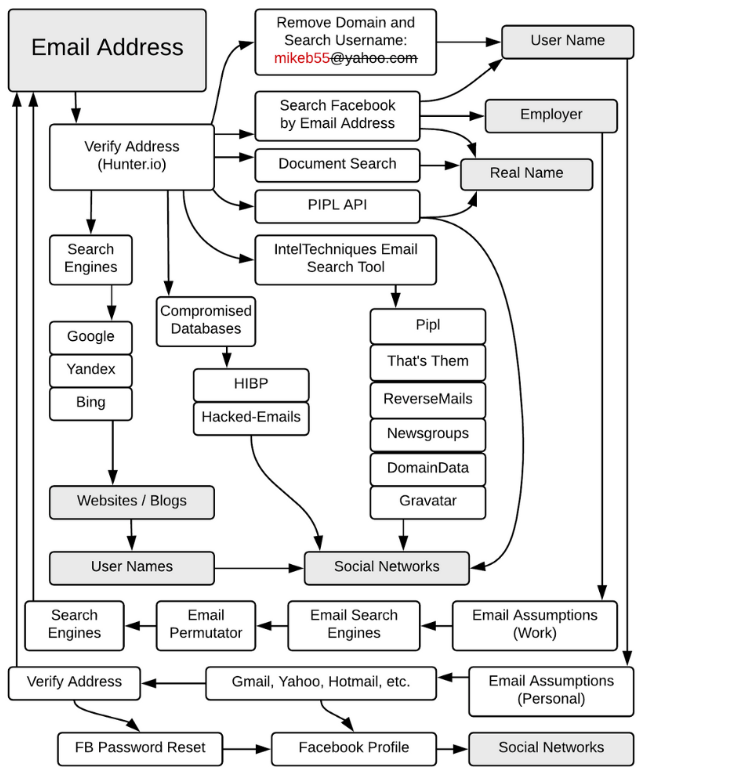
Bilješke

3.11

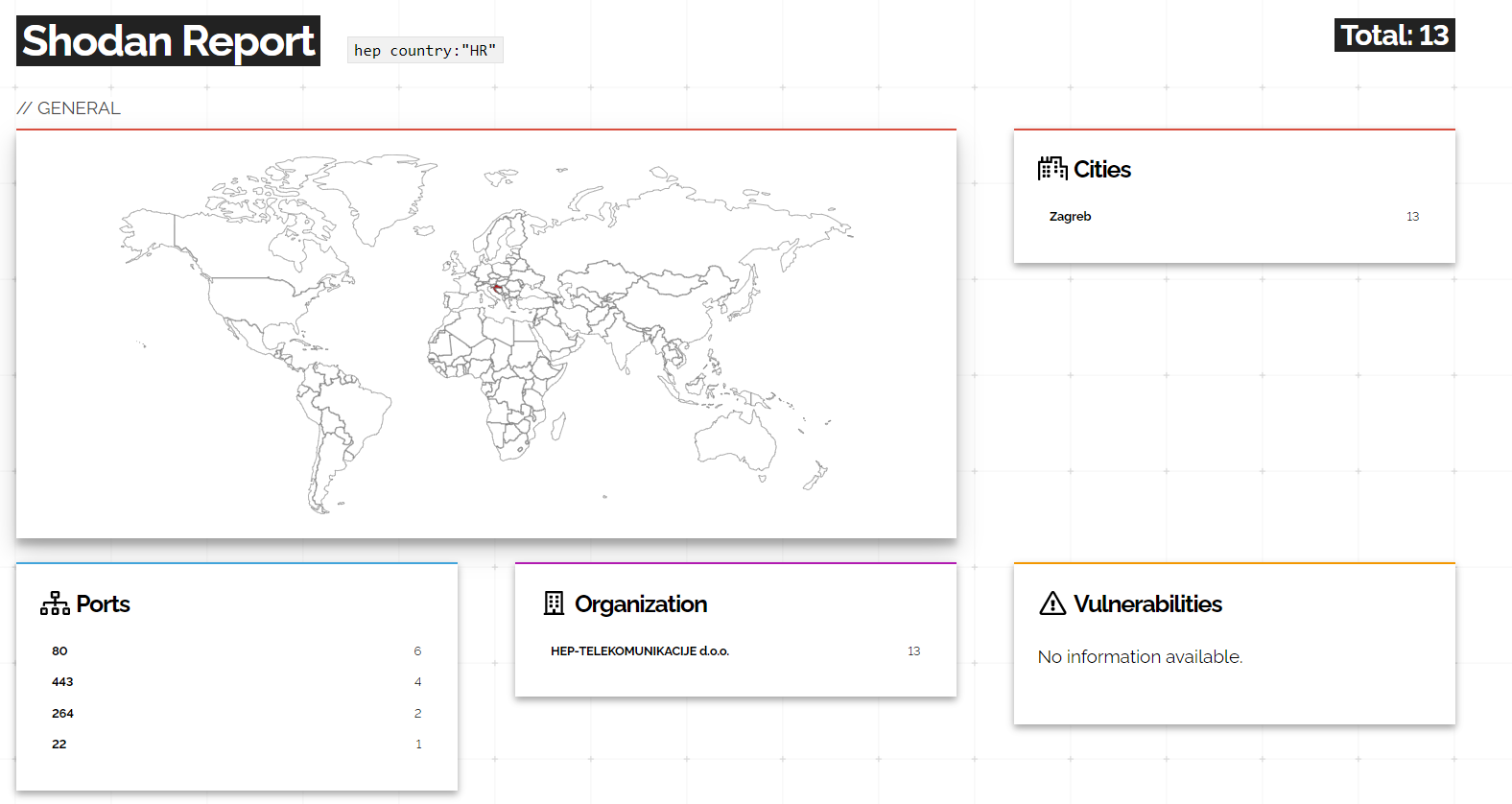
* pročitani uvodni materijali
* honeypot se koristi pri zaštiti nekog sustava i omogućuje detekciju pristupa na taj sustav
* zadnjih godina se primjećuje povećanje cyber napada razlomljenih na “stages”
* open source intelligence obuhvaća sakupljanje javno dostupnih informacija

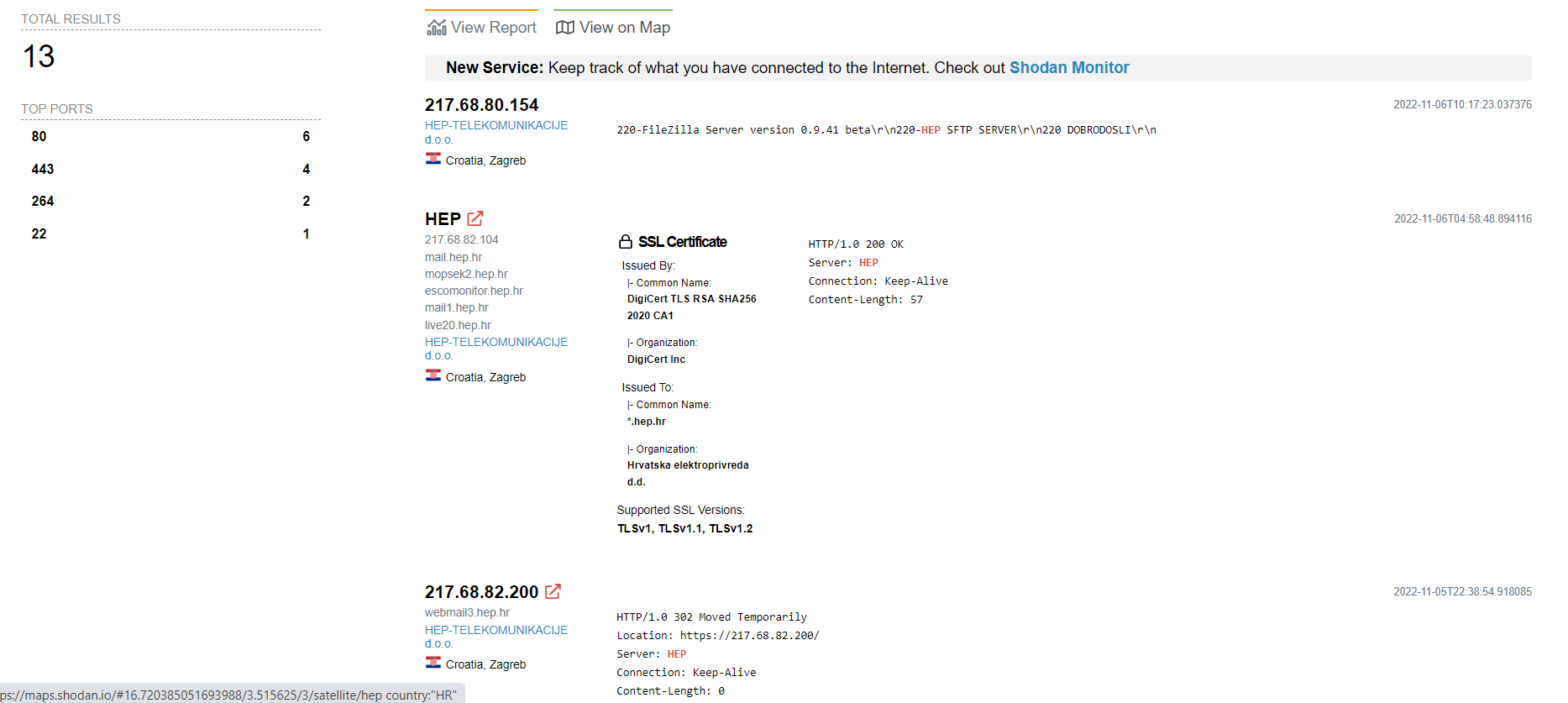


4.11

* neki od alata koji se koriste za osint su maltego, shodan i harvester
* neki od bitnih tipova podataka koje možemo naći su email adrese, imena, adrese
* 
* harvester pri analizi HEPa daje rezultate o njihovim zaposlenicima kroz jednostavnu pretragu



* 
* Shodan možemo gledati kao tražilicu poput google, ali umjesto web stranica on pretražuje sve IoT uređaje spojede direktno na internet
* također može pronaći koje tehnologije određene web stranice koriste
* 



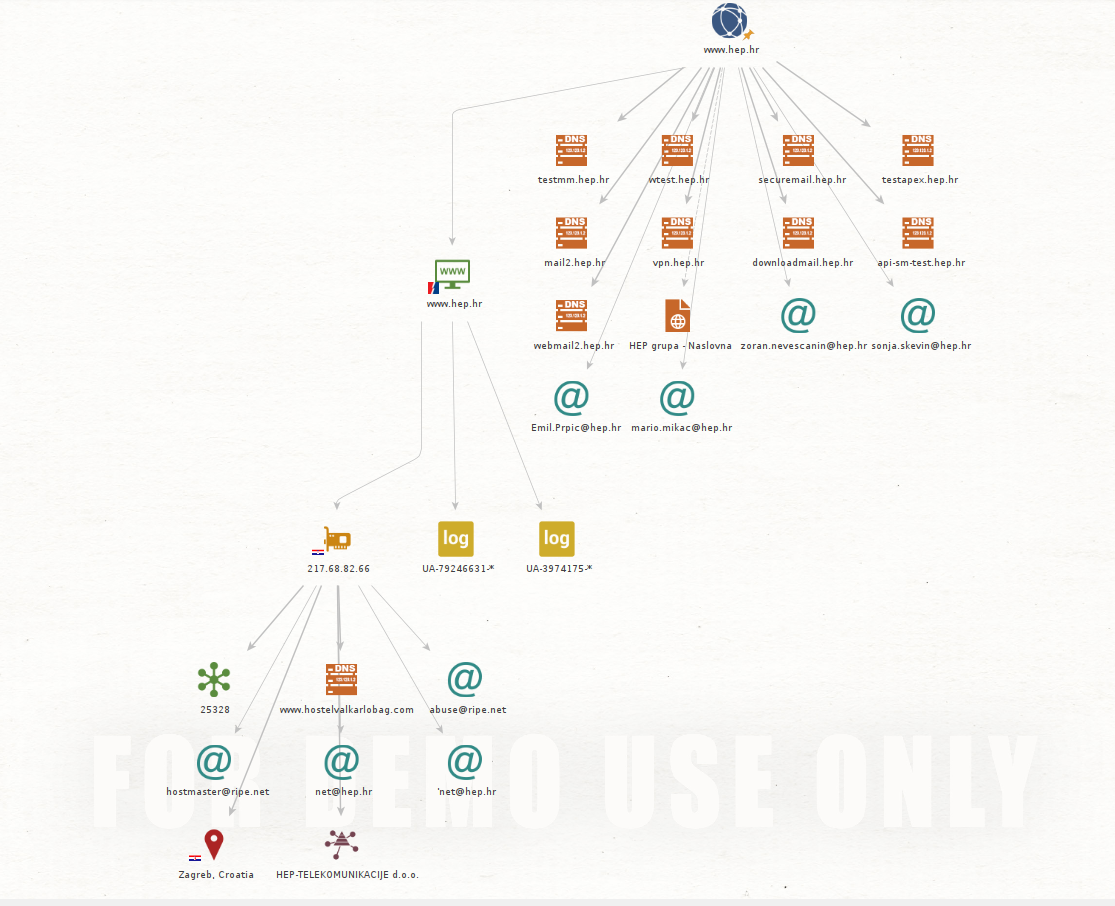
* u pretrazi sa shodanom sam našao nekolicinu ip adresa koje su vezane uz HEP a imaju otvorene određene portove
* većina su serveri za mail poštu
* nisam našao neke izravne ranjivosti kroz ovaj alat

primjer : <https://www.shodan.io/host/217.68.80.47>

5.11

zadnji alat koji sam u OSINTu koristio je maltego koji nudi sakupljanje informacija u realnom vremenu

* on mi se kroz korištenje činio najmoćniji



* uz razne upite sam od početnog čvora koji je samo naziv web stranice, graf povećao za nekoliko levela i dobio neke email adrese, logove, DNS servere, lokacije i IP adrese
* kada imamo email adrese, možemo istražiti poznate procurene informacije za poklapanja u adresama.
* kod stvaranja lažnog zaposlenika za određeni honeypot moraju se pružiti određeni podatci vezano uz našu zamišljenu osobu
* za to nam može poslužiti linkedin ili neka druga društvena mreža

<https://www.cybereason.com/blog/research/cybereason-honeypot-multistage-ransomware>

<https://medium.com/the-first-digit/osint-how-to-find-information-on-anyone-5029a3c7fd56>