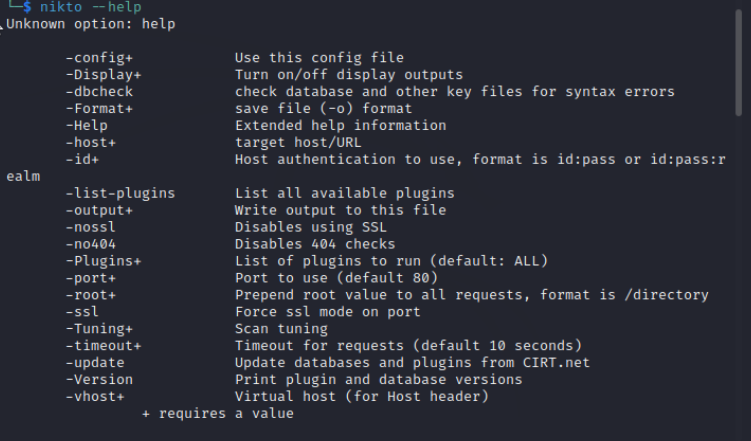
***Nikto***

Nikto je open source web scanner i web scanner aplikacija. Može provesti sveobuhvatne testove protiv web poslužitelja za nekoliko prijetnji, uključujući preko 6700 potencijalno opasnih programa/datoteka. Nikto također može izvršiti provjere zastarjelog softwera web poslužitelja i specifičnih problema. Može detektirati nekoliko stvari:

* Pronaći *SQL injections, XSS* i druge poznate ranjivosti.
* Identificirati instalirani softver( pomoću headera, favicona i fileo-va)
* Pogoditi subdomene
* Uključiti podršku za *SSL(HTTPS*)stranice
* Spremanje izvještaja u obliku *HTML, XML* ili *CSV*
* Izvještava o nepoznatim *headerim-a*
* U potrazi je za nepoznatim konfiguracijama servera poput višestrukih indeks fileov-a, *HTTP*
* Sadrži punu*HTTP* proxy podršku
* Pogađa podatke za autorizaciju( uključujući veliki broj lozinki i korisničkih imena)
* Konfiguriran je sa defaultnim poslužiteljem kako bi lakše generirao izvještaj
* Exporta se na *Metasploit*

Ukoliko se upiše ***nikto –help*** mogu  se vidjeti različite opcije koje se mogu izvršiti koristeći ovaj alat:



Prvo se Nikto može isprobati na lokalnoj mreži kako bi se otkrili embedded server, primjerice login stranice za ruter ili HTTP uslugu drugog stroja koji je samo server bez stroja.

Prvi korak je upisivanje naredbe *ifconfig* u terminal kako bi se upisala ip adresa:

Text

Description automatically generated

Nakon uspivanja naredbe ipcalc kako bi se dobio raspon dobije se navedeni prikaz na slici ispod:

A picture containing graphical user interface

Description automatically generated

Nakon dobivenog raspona slijedeći korak je  pokretanje *Nmap-a* kako bi se pronašle usluge koje se izvršavaju na zadanom servisu. Prvo se skenira mrežni raspon, specificirajući zastavicu ***-oG*** kako bi se prikazali svi hostovi koji su trenutno aktivni. Potrebno je spremiti prikaz u file i nazvati ga svojevoljno kako želimo, ovdje je nazvan ehacking.txt.

Text

Description automatically generated

Kako bi se pročitao prikaz sačuvanog file-a koristi se *cat* naredba. *Cat* naredba se koristi sa *awk, Linux* alatom koji će skenirati uzorke gdje “UP” znači da je host aktivan i da je port otvoren, dok s druge strane *‘print2$’* će isprintati svaku slijedeću riječ, točnije *IP* adresu. Podatci će biti sačuvani u novom ‘targetIP.txt’ budući da Nikto lako raspoznaje alate poput navedenog.

Text

Description automatically generated

To su hostovi koji se pokreću na portu 80. Potrebno je pokrenuti Nikto na *targetIP.txt.*

Text

Description automatically generated

Skeniranje domena:

Za skeniranje domena se koristi -h zastavica. Nikto će izvršiti skeniranje domena na portu 80 i dati kompletan izvještaj na temelju izvršenog skeniranja:

1. <https://brodplin-poc.apps.thingstalk.eu/>

Text

Description automatically generated

Do sada je napravljeno skeniranje web stranica sa omogućenim SSL-om i IP adresom na lokalnoj mreži, slijedeći korak je skeniranje web stranica pomoću priključka 80, tj nezaštićene web domene:

b)

Text

Description automatically generated

1. <https://fieldservice-api.apps.thingstalk.eu/>

a)

Text

Description automatically generated

b)

Text

Description automatically generated

3. <https://fieldservice-api-stage.apps.thingstalk.eu/>

a)

Text

Description automatically generated

b)

Text

Description automatically generated

4.  [http://sync.oklopac.com](http://sync.oklopac.com/)

a)

Graphical user interface, text, application

Description automatically generated

5. <https://cp521-frontend-cp521.apps.ocp4.heptk.hr/>

a)

Text

Description automatically generated

b)

Text

Description automatically generated

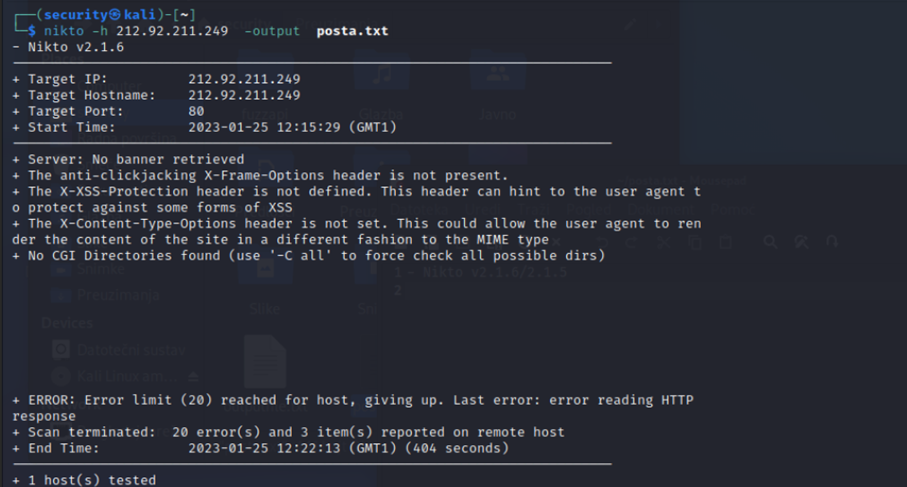
6. <https://hposta.apps.thingstalk.eu/>

a)

A screenshot of a computer

Description automatically generated with medium confidence

b)



7. .<https://cas.bss.comping.hr/>

a)

Graphical user interface, text

Description automatically generated

Skeniranje domena koristeći SSL:

 1.  <https://brodplin-poc.apps.thingstalk.eu/>

Text

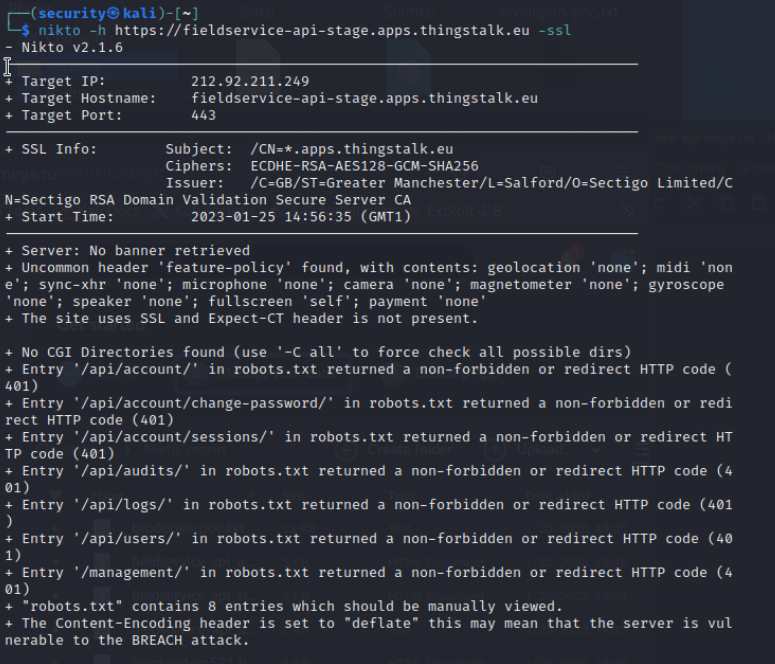
Description automatically generated

      2. <https://fieldservice-api.apps.thingstalk.eu/>

Text

Description automatically generated

3. <https://fieldservice-api-stage.apps.thingstalk.eu/>



4. [http://sync.oklopac.com](http://sync.oklopac.com/)

Graphical user interface, text, application, website

Description automatically generated

5. <https://cp521-frontend-cp521.apps.ocp4.heptk.hr/>

Text

Description automatically generated

6. <https://hposta.apps.thingstalk.eu/>

Text

Description automatically generated

7. <https://cas.bss.comping.hr/>

Text

Description automatically generated