

**Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike**

**Universiteti i Prishtinës**

**recon-ng**

Detyra 1 – Information Gathering, Siguria e Rrjetave

**Agon Hoxha**

**Përmbajtja**

[Hyrje 2](#_Toc529042971)

[Përdorimi 3](#_Toc529042972)

[Modulet 3](#_Toc529042973)

[Shembulli 1. use hackertarget 4](#_Toc529042974)

[Shembulli 2. use xssposed 4](#_Toc529042975)

[Shembulli 3. use threatcrowd 5](#_Toc529042976)

[Shembulli 4. use metacrawler 5](#_Toc529042977)

[Shembulli 5. use bing\_domain\_web 6](#_Toc529042978)

[API 7](#_Toc529042979)

[Workspaces 7](#_Toc529042980)

[Report 8](#_Toc529042981)

[Përfundim 9](#_Toc529042982)

**Tabela e Figurave**

[Figura 1. Pamja mirëseardhese 2](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444079)

[Figura 2. Erroret rreth API keys 3](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444080)

[Figura 3. Lista e moduleve 3](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444081)

[Figura 4. Rezultatet e hackertarget 4](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444082)

[Figura 5. Rezultatet e xssposed 4](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444083)

[Figura 6. Rezultatet e threatcrowd 5](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444084)

[Figura 7. Rezultatet e metacrawler 5](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444085)

[Figura 8. Rezultatet e metacrawler për rks-gov.net 6](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444086)

[Figura 9. Rezultatet e bing\_domain\_web 6](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444087)

[Figura 10. API keys 7](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444088)

[Figura 12. Lista e hapësirave pas shtimit 7](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444089)

[Figura 11. Shfaqja e hapësirave dhe shtimi 7](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444090)

[Figura 13. Pamja e raportit final 8](file:///C:\Users\agoni\Desktop\recon-ng.docx#_Toc528444091)

# **Hyrje**

Figura 1. Pamja mirëseardhese

“Recon”, shkurt për reconnaissance, nga gjuha Angleze – hulumtim. Nga ana tjetër, “ng” është shkurtes për Next Generation, apo në Shqip, Gjenerata e Ardhshme. Pra, të përkthejmë, recon-ng është hulumtues i gjeneratës të ardshme. Dhe duke e shqyrtuar funksionimin e tij, opsionet, dhe më së rëndësishmi, rastet e përdorimit me shembuj, do e vërtetojmë se me merit e ka këtë emër.

Një ndër veqantitë e shumëta të kësaj vegle është se mundëson gjenerimin e reporteve në bazë të rezultateve të fituara. Pra, nuk duhet të mbajmë në mend, apo të shënojmë rezultatet e hulumtimit tonë ngase kjo do bëhet automatikisht për neve.

Gjersa shumica e veglave në këtë kategori merren vetëm me “shikim” të caqeve, recon-ng shkon një hap më tej pasi që ka modula që mundësojnë edhe një penetration testing të nivelit të thjeshtë. Pra nuk holumton thjesht rreth porteve të hapura (si nmap) apo për ndërlidhshmëritë që mund të gjej (si maltego), por aktivisht mundësohet edhe të gjej mangësi apo vrima në siguri rreth atyre gjësendeve që i hulumton.

Për një hacking apo pentesting të suksesëshëm, nuk mund të shprehet mjaft se sa e rëndësishme është një hulumtim i mirëfilltë. Për këtë, përdorim recon-ng. Bëhet fjalë për një tool open source i shkruar në gjuhën Python, dhe i bazuar në Metasploit Framework, që është edhe arsyeja që i ngjan për nga ndërfaqja grafike dhe nga funksionimi me anë të moduleve, ndryshe nga veglat e tjera të këtij lloji. Mirëpo, gjersa është open source dhe nuk kushton aspak të instalohet, kjo nuk mund të thuhet për të gjitha modulet e mundshme të saj, dhe API që mund të shfrytëzohen, ngase jo të gjitha prej tyre janë pa pagesë.

# **Përdorimi**

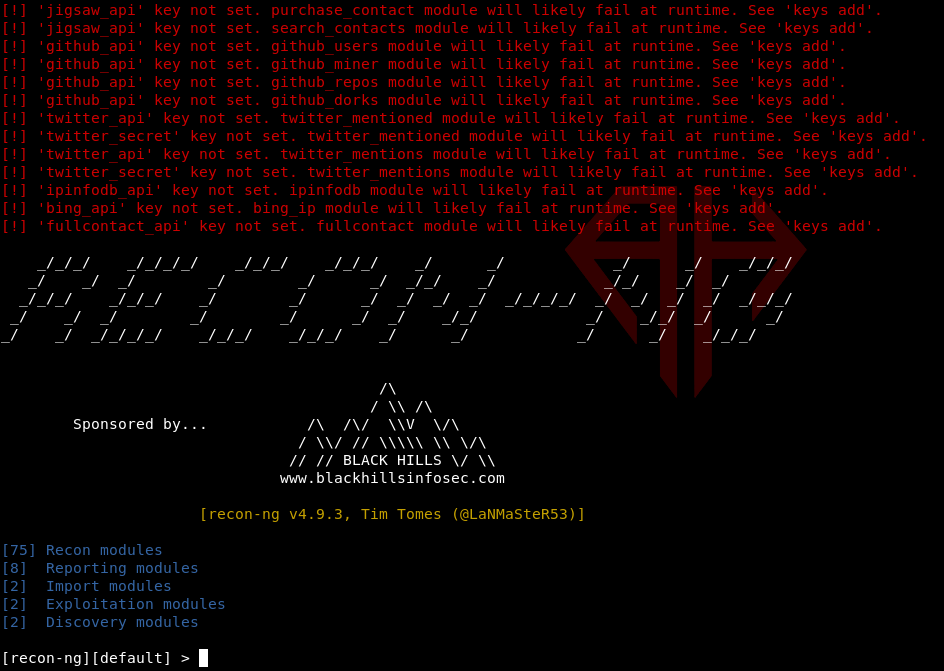
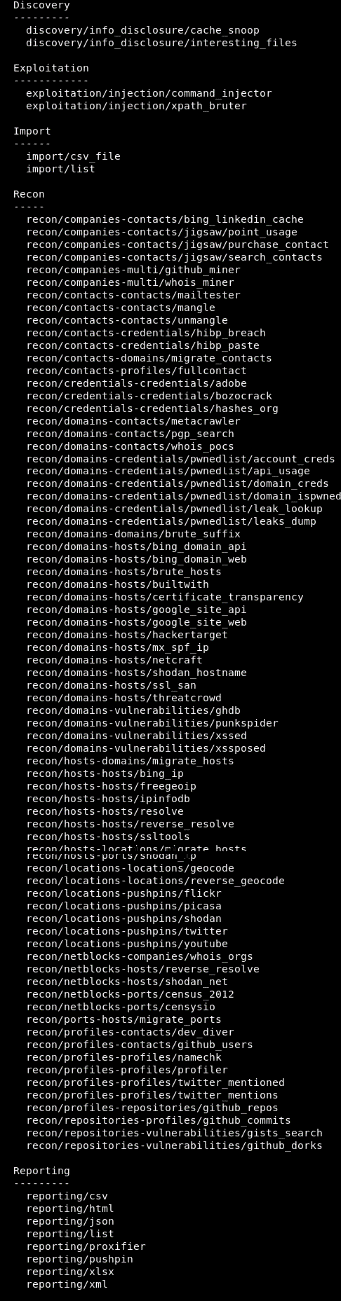
Për t’e startuar recon-ng, mjafton që t’e hapim një Terminal ne Kali dhe t’e shkruajmë emrin e veglës, pra recon-ng. Në hapjen e parë, para se të shohim pamjen mirëseardhëse, shohim një varg erroresh që mund edhe t'i injorojmë. Krejt qka tregojnë është se na mungojnë qelësat (lexo: access tokens) që të përdorim API të ndryshëm. Pra, nuk mund të shfrytëzojmë potencialin e plotë të kësaj vegle.

Figura 2. Erroret rreth API keys

Përndryshe, nëse nuk jemi në Kali Linux, kjo vegël mund edhe të shkarkohet dhe të instalohet pavarësisht prej cilës distro të Linux jemi. Procedura e instalimit është si me të gjitha aplikacionet tjera që instalojmë në Linux. Dokumenti do vazhdoj me supozim se jemi në Kali Linux.

## **Modulet**

Me komandën show modules na paraqiten të gjitha modulet që i ka recon-ng vetvetiu pa shtuar ndonjë, ku shumica mund të shihen se janë në kategorinë Recon, kuptueshmërishtë nga emri.

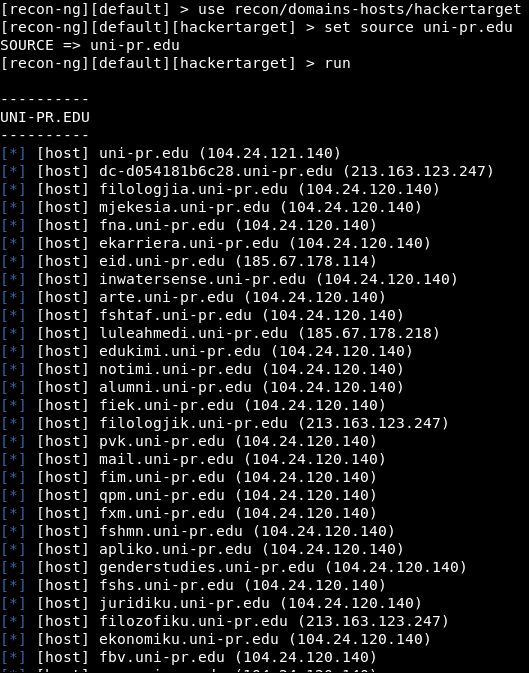
Mirëpo recon-ng nuk veqohet vetëm me përdorim të moduleve, mirëpo edhe me përdorim të API. Programerët përdorin API për të lehtësuar programimin e tyre. Përdorim të ngjajshëm gjejnë edhe në këtë vegël, vetëm se tani, përdoren për të shfrytëzuar resurset që i ofrojnë këto API. Për të mund të përdorur API, duhet të kemi një lloj qelësi të cilit i referohemi si access token. Me komandën  
keys list mund të shohim se cilët API i kemi, bashkë me qelësat (lexo: access token) e tyre që i kemi. Në një instalim të zakonshëm, pa përdorim dhe konfigurim paraprak, do dukej si në figurën 10.

Jo të gjitha modulet kërkojnë qasje në API, dhe rrjedhimisht kërkojnë access token që tani për tani nuk e kemi, mirëpo disa kërkojnë, siq është moduli për Twitter, Facebook, etj.

Metoda për qasje në një modul e përcjell formën e komandës:  
**use $type/$category/$module,** apo nëse ka emër unik, vetëm **use $module**.

Figura 3. Lista e moduleve

### **Shembulli 1**. use hackertarget

Ky modul shërben për gjetje të të gjitha domainave (sub-domains & domains) në lidhje me një webfaqe të caktuar. Me komandën show options, shohim se qka ka të konfigurueshme, ku në këtë rast do kemi si te konfigurueshëm fushën SOURCE, apo thënë më thjeshtë, duhet përcaktuar caku jon.

Për të bërë këtë, përdorim komandën  
**set source $domain**, në këtë shembull, set SOURCE uni-pr.edu. Tani, me komandën run, e lëshojmë modulin t’e kryj funksionin e vet, dhe fitohet një list e sub-domain të atij caku.

Nga lista shohim disa subdomaine të faqës të Universitetit të Prishtinës. Disa të njohur, por disa po thuajse fare, dhe jo të gjithë në IP të njejtë. Kjo na jep një ide se si është strukturuar shpërndarja e resurseve për këtë website, dhe na jep një list potenciale për caqe të sulmeve të ndryshme.

Figura 4. Rezultatet e hackertarget

### **Shembulli 2**. use xssposed

Një modul tjetër tejet i vyjshëm – është një kontroll se a është një cak i ndjeshëm ndaj XSS sulmeve. Siq e dimë XSS sulme janë tejet eficiente dhe të rrezikshme, mirëpo shumica e serverëve aplikojnë mbrojtje ndaj tyre out-of-the-box. Ky modul do përjashtonte qasjen per XSS sulm, apo do na jepte direksion se cili do jetë hapi i ardhshëm.

Ngjashëm me shembullin e parë, opsioni i vetëm që mund të ndryshojmë për këtë modul, është caku i tij. Komanda për këtë është identike, **set source $domain**, në rastin tonë   
  
set source uni-pr.edu. Dhe pastaj run që të ekzekutohen funksionet e modulit. Siq pritet nga një faqe me SSL, nuk është në fakt e ndjeshme ndaj XSS sulmeve kjo faqe. E njëjta vlen për shumicën e faqeve në internet. Rrallëherë mund të gjendet një faqe që ka ndjeshmëri ndaj XSS.

Figura 5. Rezultatet e xssposed

### **Shembulli 3**. use threatcrowd

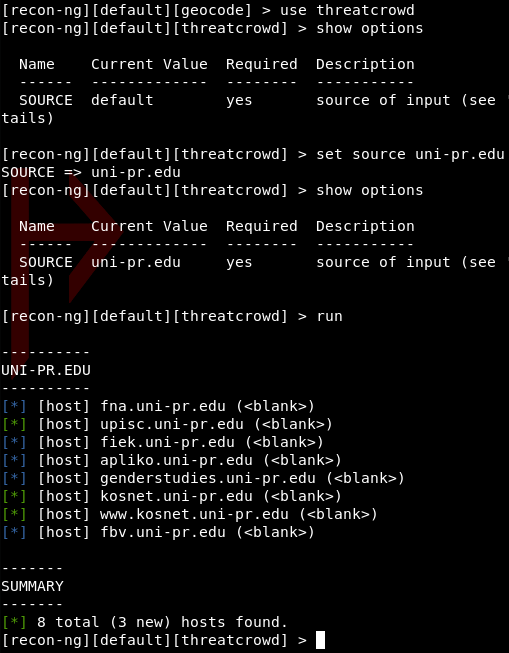
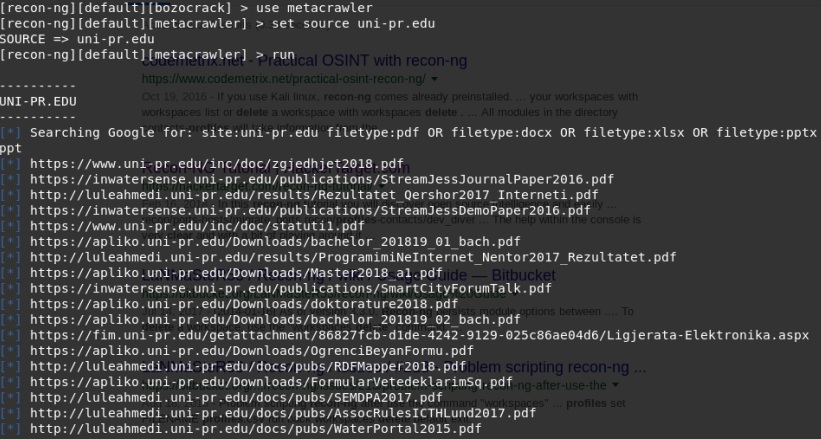
 Gjersa funksioni origjinal i aplikacionit të Threatcrowd është për të verifikuar se a është një faqe malicious apo jo, ajo e ka një funksionalitet të veqantë pasi që bënë skanim për qdo subdomain që mund t’e gjej. Këtë mund të e përdorim për të marrur informata të vyeshme. E vetmja e met e kësaj është që mund të ndodhin që ata subdomain që i gjen të mos jenë te qasëshëm më. Në këtë rast, kemi gjetur 3 subdomain të ri që nuk i dinim më parë prej përdorimit të hackertarget (shiko Figura 4).

Figura 6. Rezultatet e threatcrowd

Mirëpo, pas verifikimit manual, duke i kontrolluar këto adresa në web browser, na jepet vetëm përgjigjja e zakonshme e IIS Serverit që përdor uni-pr.edu, kur shtypim ndonjë adresë qe nuk ekziston.

### **Shembulli 4.** use metacrawler

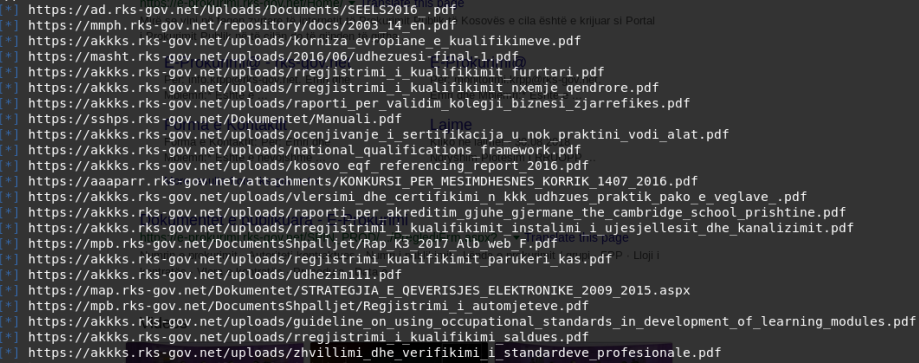
 metacrawler padyshim është një ndër modulet më të fuqishme të recon-ng. Me opsion të ngjajshëm, e përcaktojmë cakun tonë me anë të **set source $caku**. Ky modul mundohet të gjejë të gjitha dokumentet që Google i ka indexuar ndonjëherë në lidhje me atë cak. Në shembullin tonë është marrur uni-pr.edu, ngjashëm si në shembujt tjerë. Dhe ky modul ka gjetur 275 linka te ndryshëm ne uni-pr.edu për dokumente. Më saktësisht, gjetjet bëhen me kërkim për prapashtesat .pdf, .ppt, .doc, .xls dhe XML-capable verisonet e tyre (.docx, .pptx, .xlsx).

Në këtë rast, nuk janë këto informata edhe aq sensitive, edhe pse ka të perfshirë rezultate të studentëve nëpër provime, dokumente rreth zgjedhjeve, etj.

Figura 7. Rezultatet e metacrawler

Mirëpo, kur të njëjtin modul e aplikojmë në faqen e qeverisë të Republikës të Kosovës (rks-gov.net), fitojmë rezultate për të cilat një sulmues do mund të ishte tejet i interesuar.

Figura 8. Rezultatet e metacrawler për rks-gov.net

Ngjajshëm me uni-pr.edu, edhe në këtë rast kemi më shumë se 250 linqe për dokumente të ndryshme. Pra, ndër tjerash, recon-ng, përmes metacrawler mund të përdoret për auditim rreth sigurisë së webfaqeve dhe dokumentëve në të. Metacrawler gjithashtu kontrollon dokumentët për informata të autorit, duke dhënë emra në lidhje me atë faqe apo organizatë, që na jep list për ku të përdorim p.sh. SET.

Vlen të përmendet se në rks-gov.net kemi aplikuar edhe modulin hackertarget, rezultatet e të cilit veprim gjenden në raportin final.

### **Shembulli 5**. use bing\_domain\_web

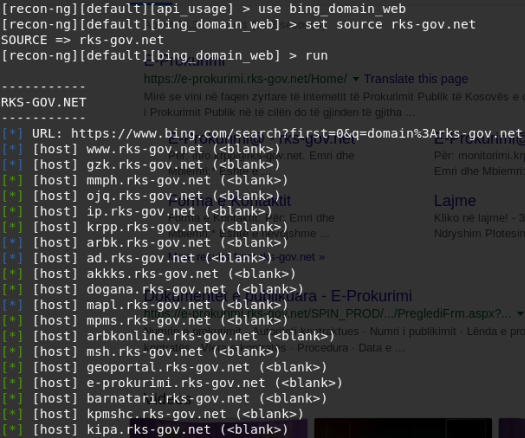
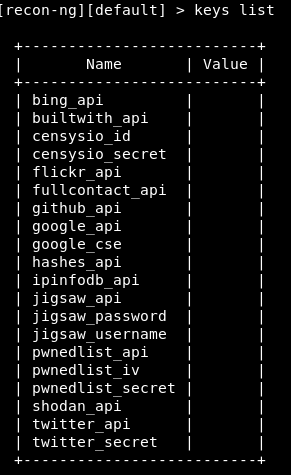
 Ngjajshëm me hackertarget, edhe bing\_domain\_web merret me gjetje të subdomaineve, mirëpo përdor faqën Bing si referencë. Qka mund të ceket rreth këtij moduli është se ka të aplikuar një timeout – edhe nëse rrjeti është jashtë mase i shpejtë, do merr pauza herdokurë që mos të bjerë në sy si malware potencial nga ana e Bing. Ndryshe nga hackertarget, i cili në të njejtën kohë i gjen edhe IP e subdomain që i ka identifikuar, bing\_domain\_web nuk e ka këtë funksionalitet.

Figura 9. Rezultatet e bing\_domain\_web

## **API**

 Për të përdorur API të ndryshëm, duhet që të kemi qasje në një API access token.

Për të shtuar API key të Facebook API, dhe e kemi marrur key 123456, do kishim keys add facebook\_api 123456. Formati i API key nuk është i tillë, por është vetëm marrur si shembull. Përdorimi i API është ngjajshëm me përdorimin e moduleve dhe nuk është recon-ng në fakt i fokusuar në APIs, andaj më shumë jam marrur me modulet që i ofron.

Figura 10. API keys

# **Workspaces**

recon-ng ndër tjerash ofron edhe mundësi për hapësira pune të ndara. Kështu, një hapësirë mund të përdoret për analiza të një rrjeti të caktuar, një hapësirë tjetër për përdorim profesional, një tjetër për hobby, e kështu me radh, dhe pa u ngërthye të dhënat. Pra, gjersa janë në hapësira pune të ndryshme, ngjan me një ndarje të files sipas përdoruesëve.

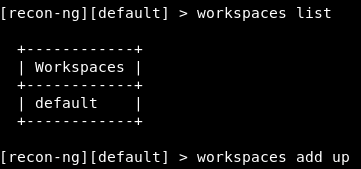
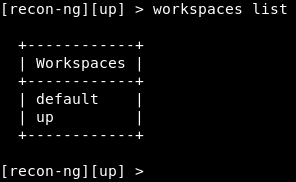
Workspace në të cilën do punojmë, përpos nëse e cekum ndryshe, do jetë si ‘default’. Për të parë hapësirat e punës përdoret komanda workspaces list. Kurse për të shtuar, e kemi komandën workspaces add $emri, dhe së fundmi, për të ndryshuar (zgjedhur) hapësirën: workspaces select $emri.

Figura 11. Lista e hapësirave pas shtimit

Figura 12. Shfaqja e hapësirave dhe shtimi

Ruajtja e të dhënave të arritura bëhet nëpër database files që gjenden në folder të caktuar që e krijon recon-ng në bazë të emrit. Lokacioni i workspaces dhe i databazave është **$username/.recon-ng/workspaces/$emri**. Kjo informat do jetë e rëndësishme në vijim.

# **Report**

Në mënyrë që të mos kemi nevoj t’i shkruajmë vet gjetjen tona, recon-ng mundëson krijimin e raporteve në formate të ndryshme, si: csv, json, xlsx, xml, etj. Ne do përdorim formatin html. Raporti do përmbaj vetëm ato të dhëna që kemi gjetur në këtë hapësirë pune – në rastin tonë, në default workspace.

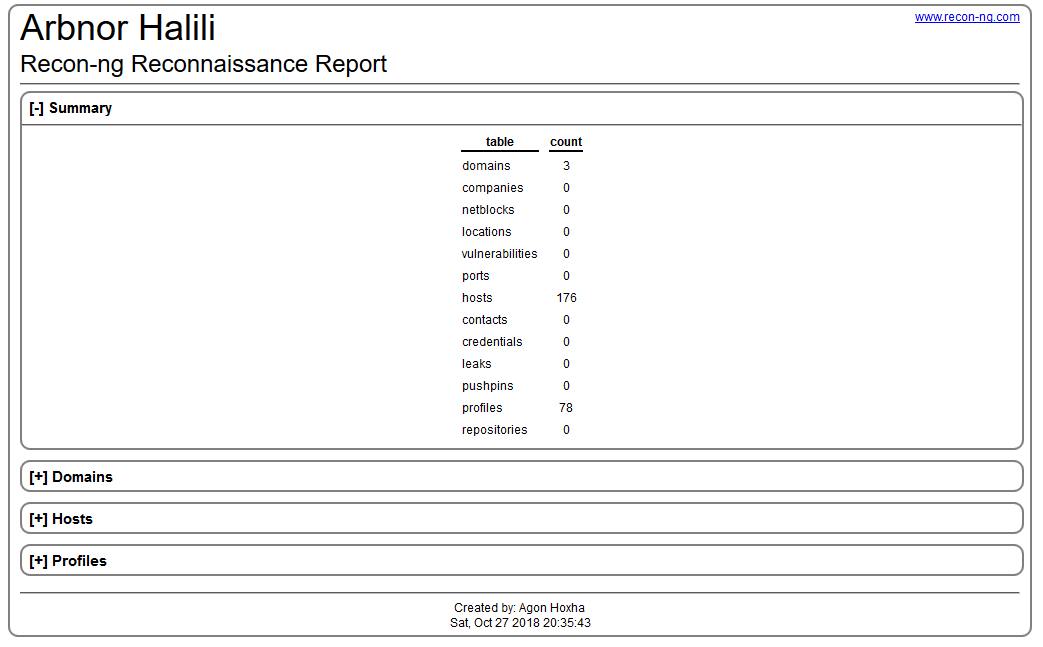
Me komandën use html, përdorim modulin e raportimit dhe shkruarjës të të gjeturave në format html. Ndryshe nga veglat që përdorëm deri tani, ky ka edhe opsione tjera. Më saktësisht, ka opsionin e CREATOR, CUSTOMER, FILENAME, SANITIZE. CREATOR shërben që të tregojmë se kush ishte hulumtues apo përdorues që i gjeti këto të dhëna. CUSTOMER shërben që të tregojmë se kujt i adresohen. FILENAME tregon vendin se ku do ruhet raporti, në rastin tonë, /root/.recon-ng/workspaces/default/results.html. SANITIZE është një opsion për True/False që na mundëson të vendosim se a do pastrohen të dhënat sensitive nga raporti. Të gjitha janë required (domosdoshme) andaj duhet plotësuar para se t’e krijojmë raportin. Pas plotësimit, me komandën run, e aktivizojmë modulin dhe ai e shkruan raportin komplet.

Figura 13. Pamja e raportit final

Në raport final ceket së pari se kujt i është adresuar raporti. Në fund te faqës ceket edhe kush e krijoj dhe një timestamp. Në summary (nga Angisht: përmbledhje), cekën totalet e domain, hosts, profiles, etj. që janë hulumtuar. Në këto do gjejmë tabelën që do shfaqej kur të ekzekutojmë p.sh. show domains. Kodi i burimit të raportit është vendosur online, në linkun **pastebin.com/EKJpj8sR** prej nga mund të shkarkohet si .html file dhe të shikohet në detaje.

# **Përfundim**

Pra, nga të dhënat e ndryshme të nxjerrura, dalim me konkludimin se recon-ng është një vegël tejet e fuqishme dhe e vyeshme për Information Gathering, dhe ofron shumë më shumë opsione se sa veglat e tjera të kategorisë të tillë, mirëpo kërkon pak më shumë kohë dhe ka një lakore më të theksuar të mësimit të shfrytëzimit, dhe më shumë lexim manual të të dhënave të nxjerrura.

Siq është ndoshta e qartë, në këtë raport, nuk është treguar funksioni i plotë i recon-ng, ngase siq tregon lista e moduleve (Figura 3), për t’e arritur këtë - raporti do duhej të ishte disa dhjetëra faqe, dhe me kompleksitet më të lartë. Mirëpo besoj që me demonstrim të vetëm këtyre moduleve të kësaj vegle, kam demonstruar se përse kjo vegël ka përdorim të madh për Information Gathering, dhe jep mundësi të madhe dhe të ndryshme për shfrytëzim. Mirëpo ngjajshëm si veglat tjera të llojit të tillë, nuk do ishte shumë i vyeshëm pa pasur qasje edhe në vegla të tjera, si:

1. nmap, të cilin do mundemi të e përdorim për te skanuar portet e IP-ve që kemi gjetur me hackertarget,
2. SET për personat në listën e emrave që kemi fituar nga metacrawler,
3. Sulme XSS në faqe ku tashmë e dimë që janë të ndjeshëm pas testimit me xssposed.