**Universiteti i Prishtinës**

**“Hasan Prishtina”**



**Projekti 1**

**Lënda:** “Siguria në Internet”

**Tema:** Veglat për marrjen e informacioneve

(Eng. “Information gathering tools”)

**“dnsmap”**

*Prof. Asoc. Blerim Rexha Punoi:*

*Msc. Arbnor Halili Ndriçim Halili*

*Prishtinë, 2021*

Table of Contents

[Hyrje 3](#_Toc64925097)

[Instalimi 3](#_Toc64925098)

[Përdorimi 4](#_Toc64925099)

[Përdorime të mundshme të “dnsmap”: 4](#_Toc64925100)

[Karakteristika kryesore të “dnsmap” 4](#_Toc64925101)

[Funksionet e “dnsmap” 4](#_Toc64925102)

[Shembuj dhe testime 5](#_Toc64925103)

[Rast interesant 9](#_Toc64925104)

[Përfundim 10](#_Toc64925105)

[Referencat 10](#_Toc64925106)

# Hyrje

E krijuar në vitin 2006, ku si frymëzim është marrë libri “The thief no one saw” nga Paul Craig, “dnsmap” është një vegël shumë e thjeshtë, mirëpo e fuqishme. Kjo vegël mundëson gjetjen e domeneve dhe sub-domeneve të uebsajteve të ndryshme me anë të “Brute Force Attack”.

“dnsmap” është një vegël në Kali linux i cili mund të përdoret në pjesën e “Information gathering” të “Penetration testing”, më saktësisht në “Enumeration stage”. Kjo fazë është me rëndësi se këtu bëhet nxjerrja e “user names”, “machine names”, “network resources” etj. [[1]](#endnote-1)

“dnsmap” është kompatibil me Linux dhe me Windows, por testimet janë bërë në “Kali Linux”.

## Instalimi

Instalimi i “dnsmap” është shumë i thjeshtë, për këtë rast është përdorur komanda

Apt install dnsmap

Pasi bëhet instalimi, si testim se a funksionon vegla, në terminal mund të shkruhet “dnsmap”, më pas dalin të dhëna rreth veglës.

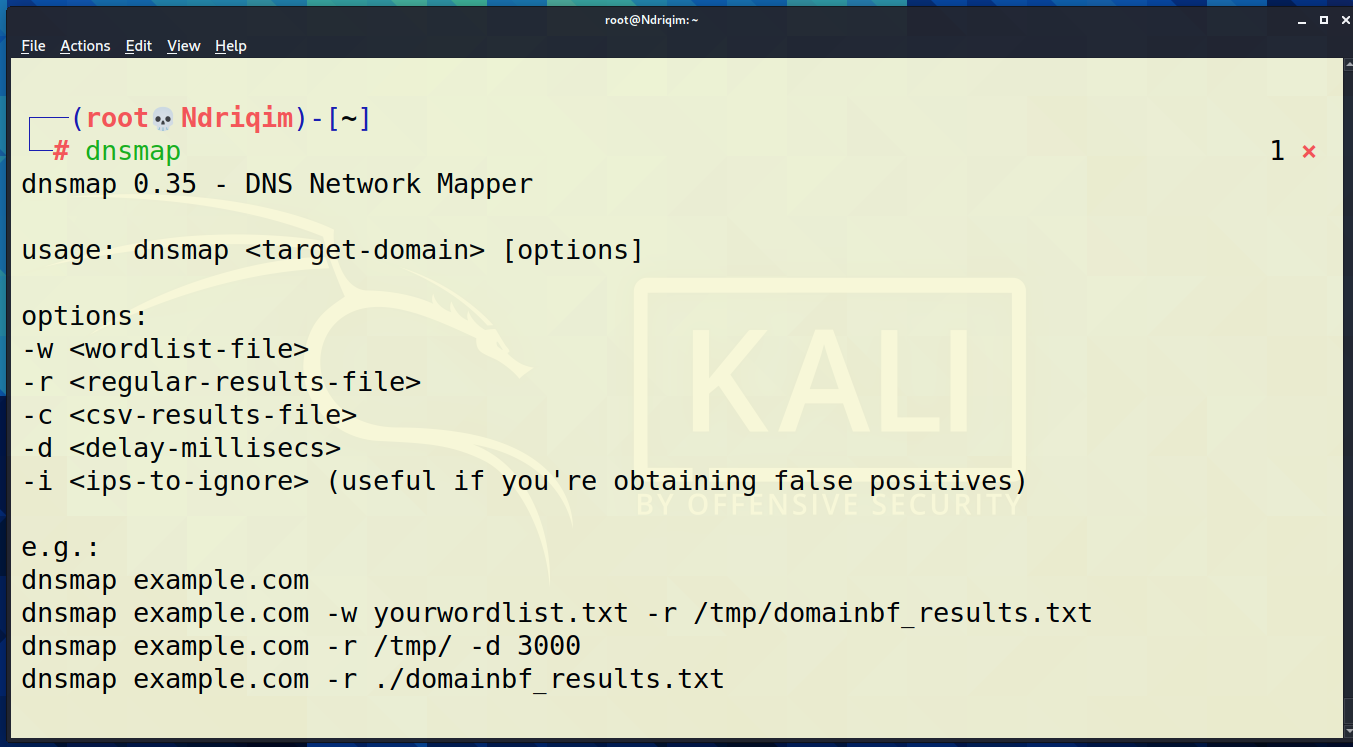


Figura Testimi se a funksionon "dnsmap"

## Përdorimi

“dnsmap” shpesh përdoret në fazën e renditjes (Ang. “Enumeration stage”) së “Penetration testing”, vegla nxjerrë emrat dhe IP adresat e sub-domeneve të uebsajteve. Kjo e bën shumë të vyeshëm për “Pentesters”.

## [[2]](#endnote-2)Përdorime të mundshme të “dnsmap”:

1. Gjetjen e serverave me qasje në largësi;
2. Gjetjen e serverave të keqkonfiguruar ose të ndrequr jomirë;
3. Gjetjen e emrave dhe Ip adresave të reja që mund të lejojnë hartimin e blloqeve të rrjetit, të cilat mund të jenë të vështira për t’ju qasur.
4. Gjetjen e paisjeve “embedded” të konfiguruara me përdorimin e serviseve dinamike të DNS.

Karakteristika kryesore të “dnsmap”

1. Nxjerr të gjitha Ip-të e sub-domeneve të cilat shoqërohen me çdo sub-domen të “Brute-forced”, në vend të 1 IP-adresë për sub-domen;
2. Abortimi i procesit “Brute-force” në rastin kur domeni përdorë “wildcards”;
3. Mundësia e përdorimit të veglës pa përdorur “wordlist”, pasi që vegla ka fjalë të gatshme që mund të përdoren;
4. Në të kundërtën nga pika 3, mundësia e përdorimit të “wordlist” të dhëna nga përdoruesi; [[3]](#footnote-1)

Funksionet e “dnsmap”

* -w <wordlist-file>, kjo mund të përdoret për të caktuar kushte se çfarë sub-domene kërkojmë.
* -r <regular-result-file>, mund të përdoret për të ruajtur rezultatin e nxjerrur në një tekst file, (si google.txt).
* -c <csv-result-file, njëjtë sikur “-r”, por për dallim, formati I të dhënave do të jetë si “csv”, (comma separated value).
* -d <delay-milliseconds), “dns-map” i bën kërkesa uebsajtit në mënyrë periodike, vlera që merr -d mund të jetë perioda që mund të caktohet, vlerë “default” është 10 milisekonda.
* -i <ips-to-ignore>, për të injoruar IPS – “intrusion prevention system”, mund të nevojitet kur kemi shumë “false-positive”.

“dnsmap gjithashtu ka opsionin, “dnsmap-bulk <domains-file>”, nëse kemi një tekst fajll që përmban linqe të uebsajteve, atëherë “dnsmap” mund të hap këtë fajll për t’i analizuar të gjitha linqet e dhëna në atë fajll.

# Shembuj dhe testime

Vegla është relativisht e thjeshtë që të përdoret,

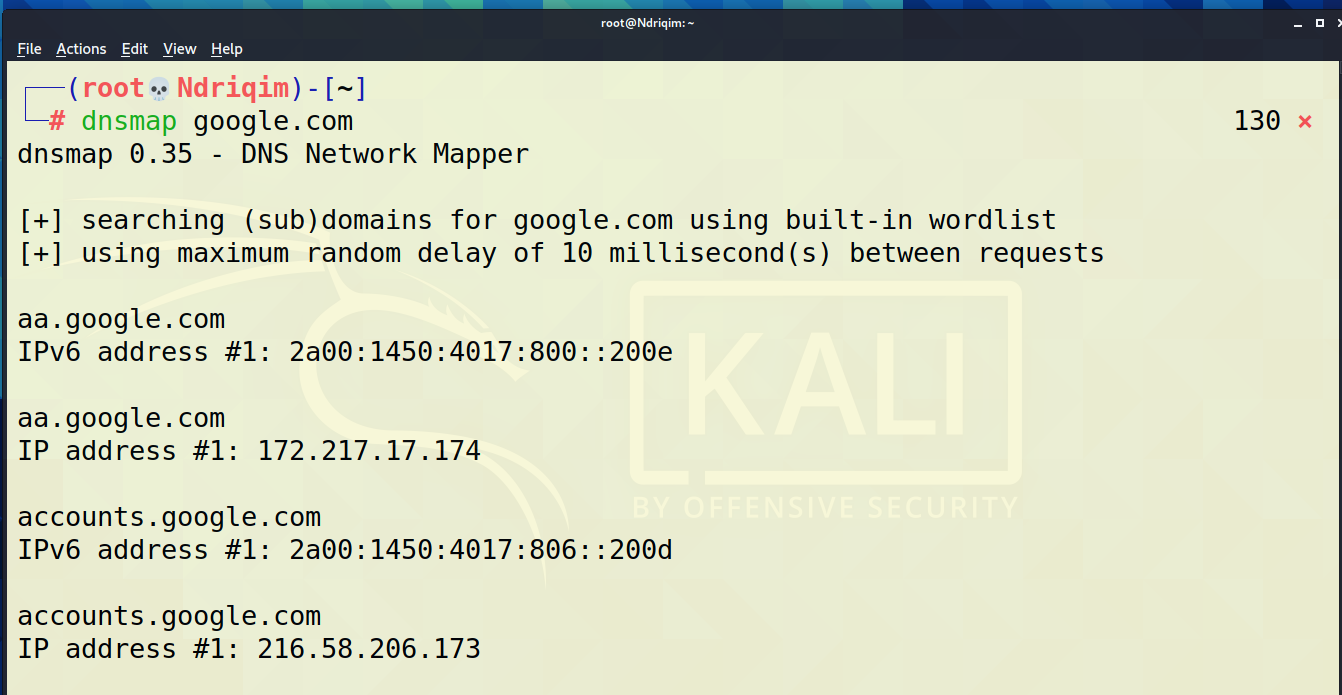


Figura Përdorimi i "dnsmap" në "Google.com"

Në figurë shihet se si mund të përdoret “dsnmap” për gjetjen e sub-domeneve të “Google.com”. Siç shihet, kjo vegël është jashtëzakonisht e thjeshtë, por mund të nxjerrë informacion shumë të çmuar rreth një uebsajti. Si shembull mund të ndodh që një uebsajt të ketë faqe të papërfunduara, që mund të krijojnë qasje në të gjithë uebsajtin.

Kur përfundon komplet komanda kemi:



Figura Përfundimi i komandës "dnsmap google.com"

Shohim se “dnsmap” ka zbuluar 133 subdomene edhe 150 ip adresa që janë të lidhura me ato domene, si dhe sa kohë morri për t’i gjetur të gjitha, në këtë rast, 94 sekonda.

Komandë tjetër që mund të përdoret është përdorimi i -w, ku më këtë mund të kërkojm domene specifike,

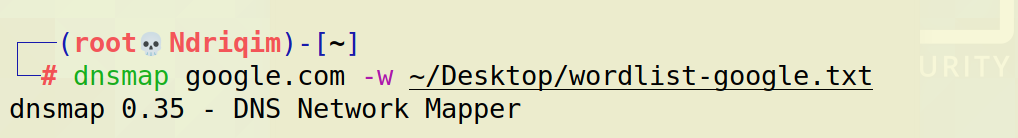


Figura Përdorimi i "-w" për "dnsmap"

Përmabjtja e fajllit “wordlist-google.txt” është:

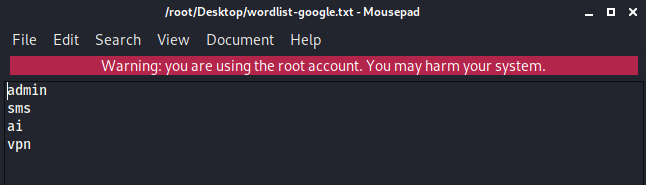


Figura Përmbajtja e fajllit "wordlist-google.txt"

Dhe në dalje do të kemi:



Figura Dalja e komandës nga [figura 4](#Figura_4)

D.m.th. Vegla ka gjetur vetëm subdomenet që kanë fjalët e shkruara në fajllin që i kemi treguar.

Ne gjithashtu mund të përdorim edhe funksione të tjera si “-r” dhe “-c”, e paraqitur poshtë:

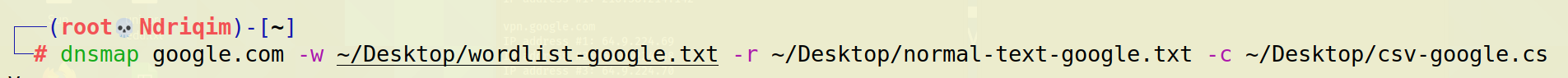


Figura Përdorimi i opsioneve "-r" dhe "-c"

Ku dalja është e njëjtë sikur te [figura 6](#Figura_6), por me dallim që shkruhen (ose krijohen e më pas shkruhen nëse nuk ekzistojnë fajllat e treguar) 2 fajlla që do të ndodhen në shtegun (“path”) që e kemi drejtuar komandën. Përmbajtja e tyre është si më poshtë:

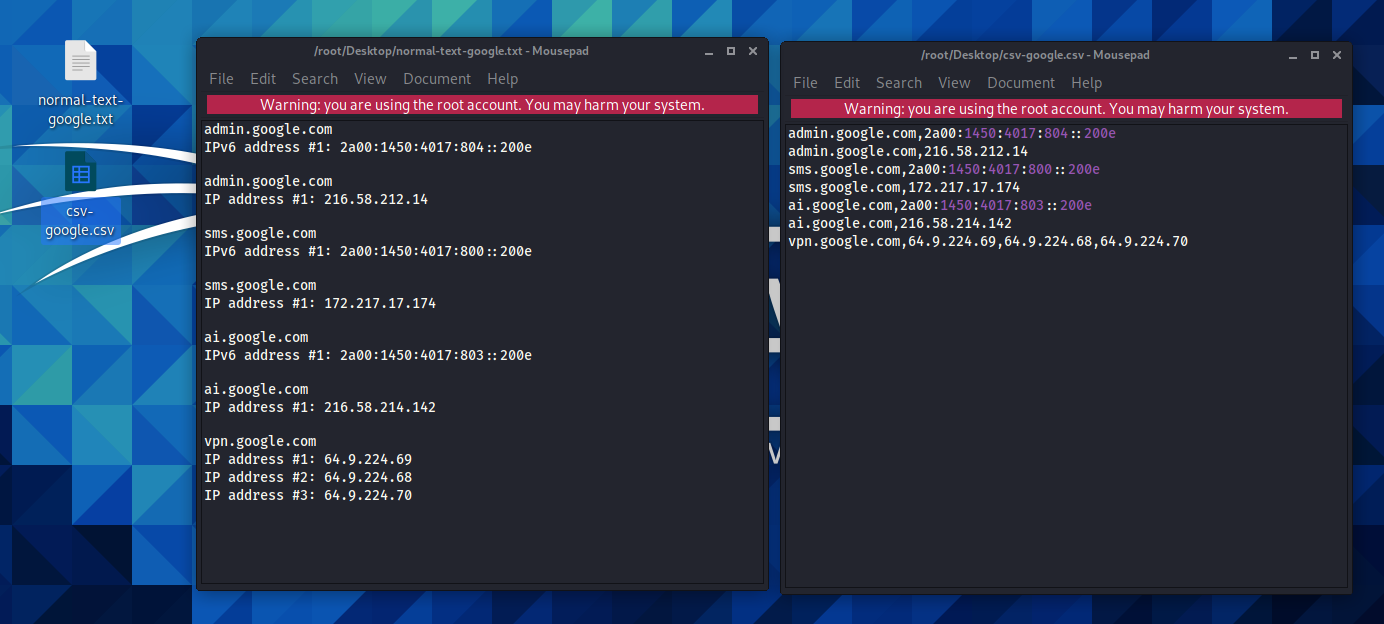


Figura Fajllat e krijuara nga komanda në [figurën 7](#Figura_7), si dhe përmbajtjet e tyre. Gjenden si tekst i thjeshtë (majtas) ose si “comma seperated values” (djathtas)

Pas kësaj kemi edhe përdorimin e komandës “dnsmap-bulk”, poshtë shohim se si duket:

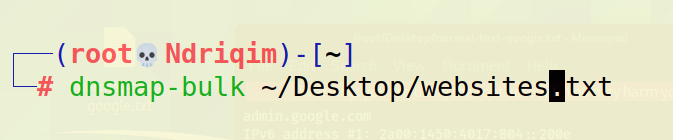


Figura Përdorimi i komandës "dnsmap-bulk"

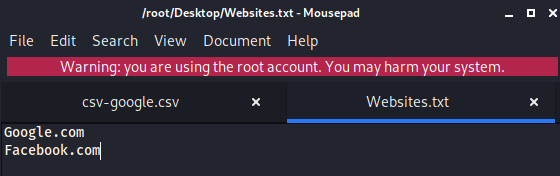


Figura Përmbajtja e "websites.txt, përmban domenet që duam t’i shikojmë"

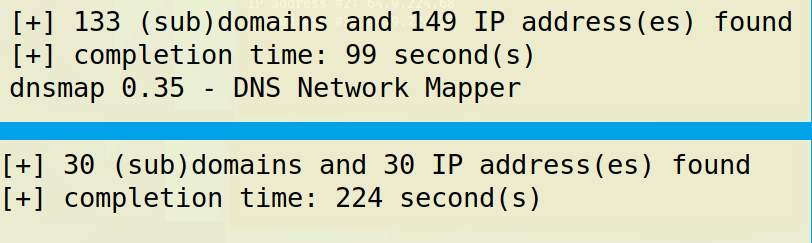


Figure Fundet e daljes së komandës nga [figura 9](#Figura_9), lart është për domenet e “Google.com”, kurse poshtë për “Facebook.com”

Sigurisht që në këtë fajll mund të ketë më shumë domene. Kjo komandë është vetëm për të thjeshtuar punën e një “Pentester” kur teston shumë uebsajta njëherësh.

## Rast interesant

Shembull interesant është rasti kur e kam testuar veglën në faqen e universitetit “Hasan Prishtina”, kur “dnsmap” ka nxjerrë sub-domene të papërfunduara, si p.sh.

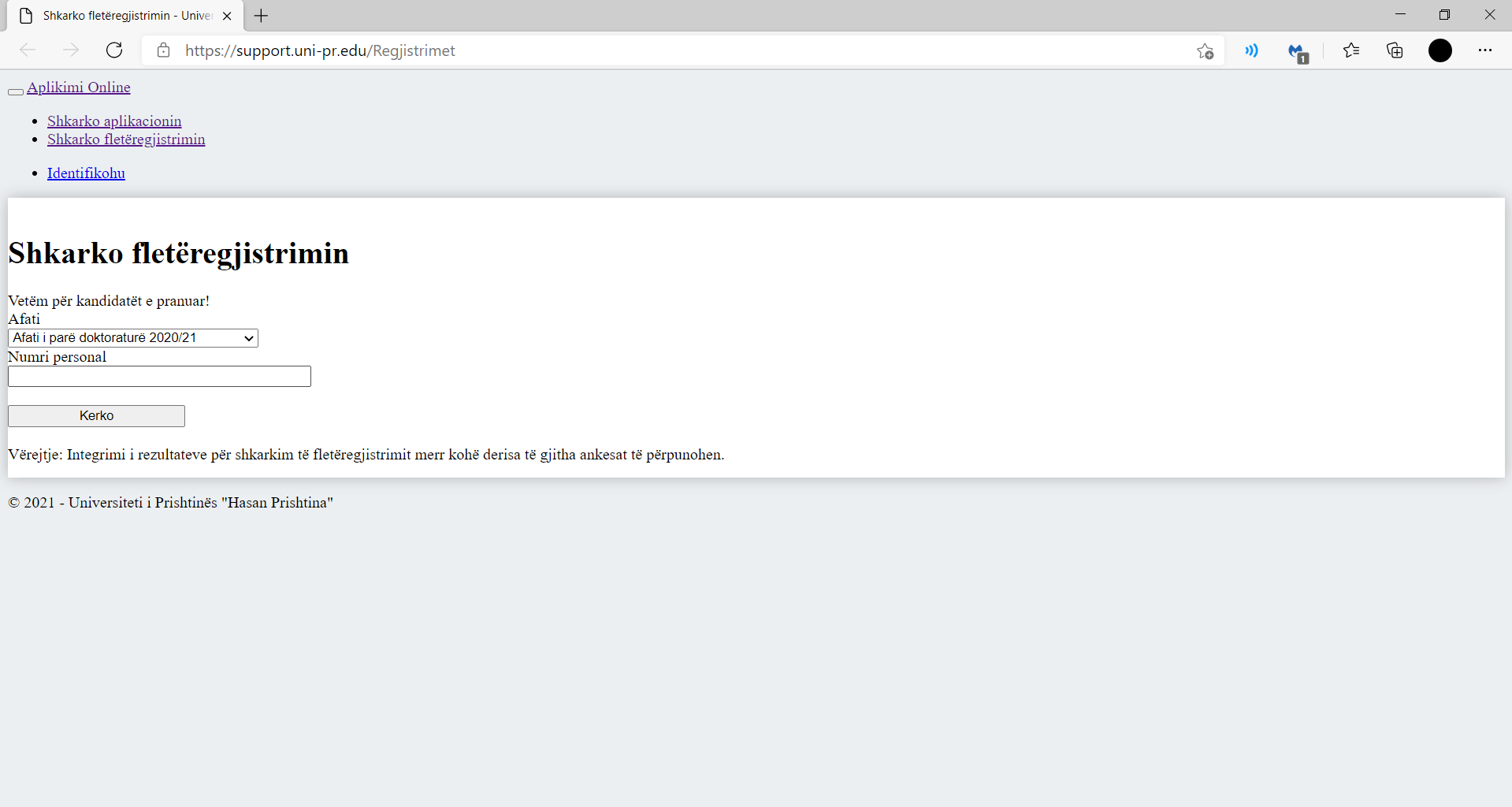


Figura "Support.uni-pr.edu" e nxjerrur nga "dnsmap"

Vërehet se faqja është e papërfunduar dhe ndoshta është e mundshme që të jetë një “vulnerability” për uebsajtin “Uni-pr.edu”, siç është përmendur në [pikën 2](#Pika_2) te përdorimet.

Gjithashtu gjatë përdorimit të veglës në uebsajtin e Universitetit është hasur “wildcards” nga njëri prej sub-domeneve që po kërkon, siç është përmendur tek [karakteristika 2](#Karakteristika_2). Në këtë rast IP-adresa : 213.163.123.247 që tregon te një server i Windows: [IIS Windows Server](http://213.163.123.247/).

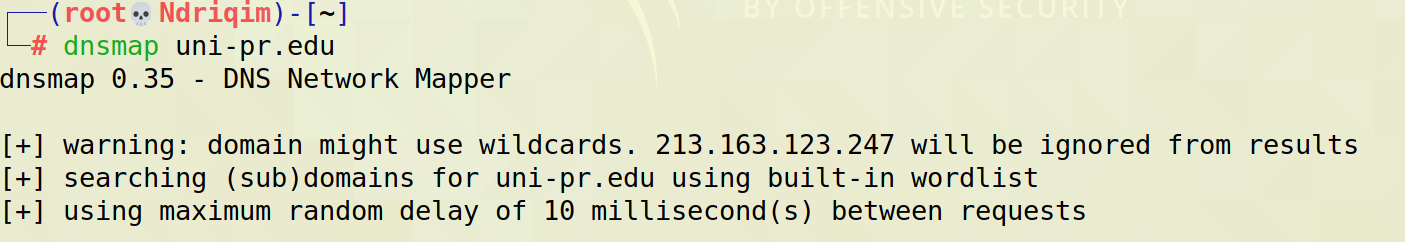


Figure 13 Abortimi i "dnsmap" në rastin kur has një "wildcard" nga njëri prej sub-domeneve që kërkon

# Përfundim

Si përfundim, “dnsmap” është një vegël e thjeshtë, por kjo thjeshtësi e bën shumë të fuqishme këtë vegël, sepse mund të mësohet lehtë edhe nga nje përdorues i ri i “Kali Linux”. Gjithashtu, [karakteristikat](#_Karakteristika_kryesore_të) dhe mundësitë për [përdorimin](#_Përdorime_të_mundshme) e saj bëjnë të dobishme dhe unike nga veglat e tjera të “Kali Linux”.

Kjo vegël mund të përdoret nga çdokush edhe për të mësuar rreth uebsajtit që frekuenton shpesh. P.sh. nuk e kam ditur që Google ka subdomene si “ai.google.com” ose “research.google.com”.

# Referencat

Vegla në tools.kali.org - [dnsmap | Penetration Testing Tools (kali.org)](https://tools.kali.org/information-gathering/dnsmap)

1. Përgjithësimi i “dnsmap” - [Google Code Archive - Long-term storage for Google Code Project Hosting.](https://code.google.com/archive/p/dnsmap/) [↑](#endnote-ref-1)
2. Përdorimi dhe karakteristikat e “dnsmap” - [dnsmap | DNS Domain name system brute force attacks beginner's guide (cyberpratibha.com)](https://www.cyberpratibha.com/dnsmap-dns-domain-name-brute-forcing-tool/) [↑](#endnote-ref-2)
3. “Wordlist” ka kuptimin e një listë fjalësh që përdoren nga vegla, shembull për “wordlist” janë “Dictionary attacks”, një haker mund të ketë një listë fjalë-kalishmesh të gatshme, të cilat i teston për t’ju qasur llogarisë së një përdoruesi. [↑](#footnote-ref-1)