**Universiteti i Prishtinës “Hasan Prishtina”**

**Fakulteti Inxhinierisë Elektrike dhe Kompjuterike**

****

**Dokumentim teknik i projektit**

**Lënda: Siguria në Internet**

**Titulli i projektit: THC-Hydra**

**Emri profesorit/Asistentit Emri & mbiemri studentëve / email adresa**

|  |  |  |
| --- | --- | --- |
| Prof. Dr. Blerim REXHA  PhD.c Mërgim H. HOTI | 1. Arlinda Kastrati | arlinda.kastrati4@student.uni-pr.edu |
| 2. Alberiana Tofaj | alberiana.tofaj@student.uni-pr.edu |
| 3. Elona Rashica | elona.rashica@student.uni-pr.edu |
| 4. Elsa Vitija | elsa.vitija@student.uni-pr.edu |

Prishtinë, 2021

**Përmbajtja**

[**Abstrakti** 3](#_Toc87795770)

[**Hyrje** 4](#_Toc87795771)

[**1.** **Qëllimi i punimit** 6](#_Toc87795772)

[**1.1** **Avantazhet e THC Hydra** 6](#_Toc87795773)

[**1.2** **Disavantazhet e THC Hydra** 8](#_Toc87795774)

[**2.** **Pjesa kryesore** 9](#_Toc87795775)

[**2.1 Instalimi i veglës** 10](#_Toc87795776)

[**2.2** **Modet e punës** 11](#_Toc87795777)

[2.2.1 Modi një emër i shfrytëzuesit dhe një fjalëkalim 11](#_Toc87795778)

[2.2.2 Modi nje listë e emrave të shfrytëzuesve dhe një fjalëkalim 13](#_Toc87795779)

[2.2.3 Modi një emër i shfrytëzuesit dhe një listë e fjalëkalimeve 13](#_Toc87795780)

[2.2.4 Modi një listë me emra të shfrytëzuesve dhe një listë me fjalëkalime të mundshme 14](#_Toc87795781)

[**3. Shembuj konkret** 16](#_Toc87795782)

[**3.1 Brute force mail** 16](#_Toc87795783)

[**3.2 Brute Force ueb faqe** 21](#_Toc87795784)

[**3.3 Brute Force Metasploitable Server** 22](#_Toc87795785)

[**4. Konkluzione** 25](#_Toc87795786)

[**Referencat** 26](#_Toc87795787)

# **Abstrakti**

Ky raport paraqet një përmbledhje të informatave në lidhje me përshkrimin, instalimin, vetitë, funksionet, përdorimin dhe ekzekutimin e veglës softuerike THC Hydra (The Hacker’s Choice Hydra) në kuadër të lëndës Siguria në Internet. THC Hydra është një vegël e cila përdoret për testimin aplikacioneve dhe ueb faqeve të ndryshme lidhur me sigurinë e fjalëkalimeve të përdoruesëve në mënyrë që të eleminohen dobësitë e tyre dhe të parandalohen mundësitë e qasjes nga persona tjerë të paautorizuar.Vegël kjo e cila është e njohur për shpejtësinë, efikasitetin dhe fleksibilitetin e saj. Kjo vegël hyn në mesin e top 10 veglave më të përdorura për detektimin e fjalëkalimeve. Aftësia që kjo vegël mbështet më shumë se 50 protokolleve, përkrah një numër të madh të bazave të të dhënave dhe ka një disponueshmëri, pothuajse në të gjitha sistemet operative bën që kjo vegël të ketë një popullaritet të madh dhe të përdoret shumë nga ekspertë dhe studiues të ndryshëm nga fusha e sigurisë së fjalëkalimeve.Objektivat kryesore të këtij raporti jane studimi i detajizuar i veglës THC Hydra, procesi i instalimit, mënyrat dhe modet se si mund të përdoret duke përfshirë edhe disa shembuj konkret se si THC Hydra mund të detektojë fjalëkalimet me procese shumë të thjeshta.

# **Hyrje**

Studimi dhe përdorimi i veglës THC Hydra është shumë interesant, për arsye se na bën të kuptojmë që asgjë në rrjet nuk është e sigurte, çdo fjalëkalim i mundshëm mund të thyhet apo mund të gjendet nga vegla në fjalë. Fjalëkalimet janë po aq të rëndësishme sa mjetet e tjera që përdorim për të verifikuar identitetin tonë – si patentat e shoferit, kartat identifikuese apo kartat e sigurimeve shoqërore. Për të mos e lejuar qasjen e personave të paautorizuar në llogaritë tona personale duhet të studiohet edhe punohet vazhdimisht në këtë fushë për rritjen e sigurisë sepse fjalëkalimet ofrojnë linjën e parë të mbrojtjes kundër qasjes të paautorizuar në pajisjen tonë dhe informacioneve personale. Sa më i fortë fjalëkalimi ynë, aq më i mbrojtur do të jetë pajisja jonë nga njerëzit e këqij dhe programet me qëllim të keq. Dhe në qoftë se ne nuk tregojmë një kujdes të veçantë për mbrojtjen e tyre, ato mund të keqpërdoren lehtë.

Në Figuren 1 mund ta shohim numrin e sulmeve kibernetike brute force që ndodhin në botë brenda orës.

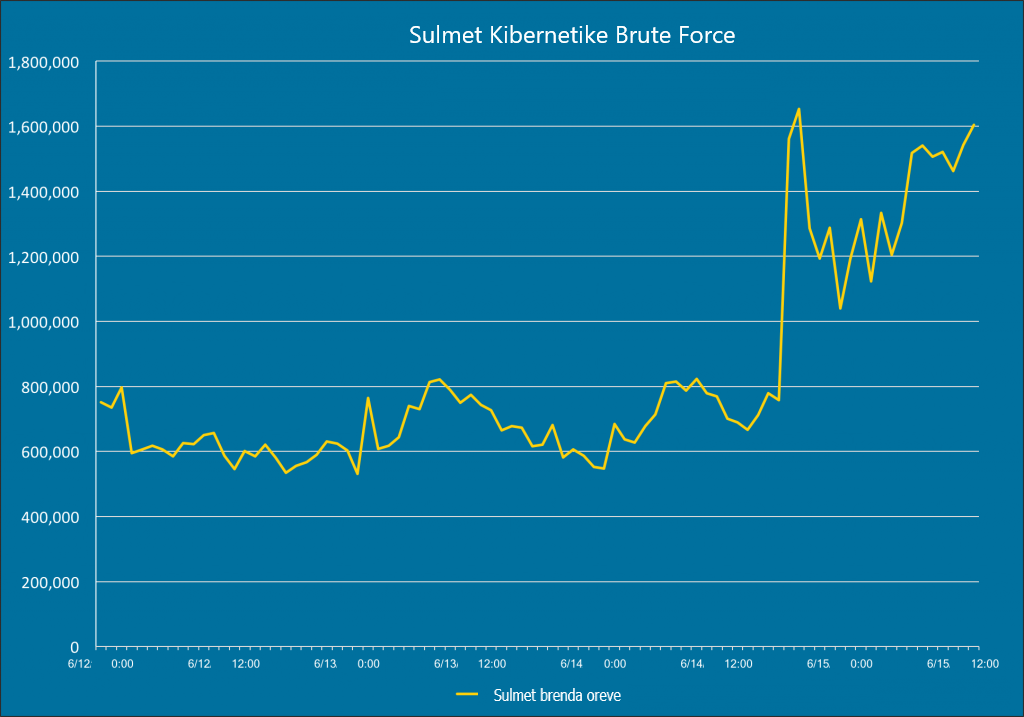


Figura 1: Numri i sulmeve kibernetike Brute Force brenda orëve sipas HIVE SYSTEMS

Nëse nuk dëshironi që të dhënat e juaja të keqpërdoren atëherë ekzistojnë edhe disa rregulla që duhet ndjekur në lidhje me mbrojtjen e një fjalëkalimi. Çelësi për të qëndruar të sigurtë nga sulmet e THC Hydra është të siguroheni që përdorni fjalëkalime me gjatësi të mjaftueshme. Ngase sa më të gjata dhe komplekse të jenë fjalëkalimet, atëherë edhe koha për thyerjen e tyre do të rritet. Këtë mund ta shohim edhe në figurën e mëposhtme, Figura 2.

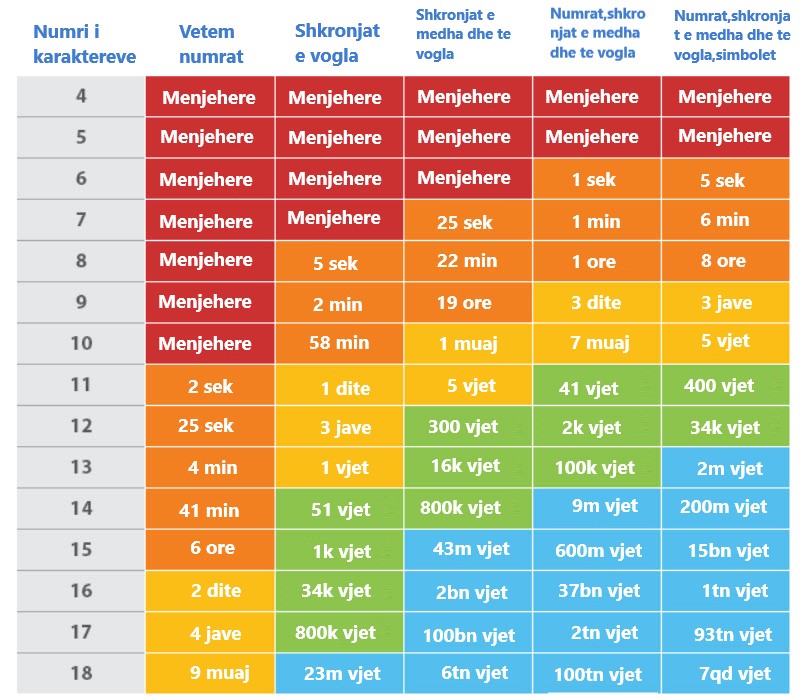


Figura 2: Koha për të cilën mund të thyhet një fjalëkalim

Çdo gjë prej 16 karakteresh ose më shumë duhet të jetë e mjaftueshme duke pasur parasysh teknologjinë aktuale, por në mënyrë ideale do të jetë e sigurt për veten duke përdorur një frazë fjalëkalimi që është aq e gjatë sa maksimumi i lejuar nga shërbimi në të cilin po regjistroheni. Shmangien e përdorimit të çdo shërbimi që nuk ju lejon të krijoni një fjalëkalim më të gjatë se 8 ose 10 karaktere rritë sigurinë tuaj të të dhënave.

# **Qëllimi i punimit**

Njëra nga pikat kryesore të sigurisë është fjalëkalimi, këtë e tregon çdo studim i bërë në lidhje me sigurinë dhe mbrojten e informatave personale. Thyerja e fjalëkalimit është metodologji e gjetjes së fjalëkalimeve nga bazat e të dhënave në të cilën janë ruajtur. Shumica e njerëzve veçanërisht ata që nuk kanë njohuri në IT do ti bazojnë fjalëkalimet e tyre 'sekret' në fjalë dhe emra që nuk do t'i harrojnë lehtë si: emrat e të dashurve, emrat e fëmijëve, adresat e rrugëve, ekipi i preferuar i futbollit, vendi i lindjes etj. Këto fjalë janë të zakonshme dhe konsiderohen si fjalëkalime shumë të dobëta ngase shume shpesh ato mund të hamendësohen lehtë dhe të lejojnë persona të paautorizuar qasje.

THC Hydra është një dëshmi, për t'u dhënë studiuesve, ekspertëve të sigurisë dhe konsulentëve mundësinë për të treguar se sa e lehtë do të ishte për të fituar qasje të paautorizuar nga distanca në një sistem kompjuterik.

THC Hydra përdoret zakonisht nga testuesit së bashku me një sërë programesh si Crunch, Cupp etj, të cilat përdoren për të gjeneruar lista fjalësh. Pastaj, sulmojnë programet e krijuara duke përdorur listat e fjalëve të gjeneruara për të testuar sigurinë e tyre.

Me kalimin e kohës THC Hydra përditësohet dhe numri i shërbimeve që mbështet ajo rritet. Krijuesi i THC Hydra publikon punën dhe përditësimin e veglës në llogarinë e tij në GitHub.

## **Avantazhet e THC Hydra**

Ekzistojnë tashmë disa vegla të disponueshme për hakerat e hyrjes, megjithatë, asnjë nuk mbështet më shumë se një protokoll për të sulmuar ose mbështetur lidhjet paralele.

THC Hydra është projektuar me versione të linjës së komandës dhe linjës grafike. Gjithashtu, është e paralelizuar, vegël shumë e shpejtë, fleksibile, mund të përdoret online dhe offline.

**Platformat e mbështetura nga THC Hydra:**

* Windows/ Cygwin
* Linux
* MacOS
* Solaris
* FreeBSD/OpenBSB
* QNX(Blackberry 10)

**Protokollet/shërbimet e mbështetura nga THC Hydra:**

* Asterisk
* AFP
* Cisco AAA
* Cisco auth
* Cisco enable
* CVS
* Firebird
* FTP
* HTTP-FORM-GET
* HTTP-FORM-POST
* HTTP-GET
* HTTP-HEAD
* HTTP-POST
* HTTP-PROXY
* HTTPS-FORM-GET
* HTTPS-FORM-POST
* HTTPS-GET
* HTTPS-HEAD
* HTTPS-POST
* HTTP-Proxy
* ICQ
* IMAP
* IRC
* LDAP
* MEMCACHED
* MONGODB
* MS-SQL
* MYSQL
* NCP
* NNTP
* Oracle Listener
* Oracle SID
* Oracle
* PC-Anywhere
* PCNFS
* POP3
* POSTGRES
* Radmin
* RDP
* Rexec
* Rlogin
* Rsh
* RTSP
* SAP/R3
* SIP
* SMB
* SMTP
* SMTP Enum
* SNMP v1+v2+v3
* SOCKS5
* SSH (v1 and v2)
* SSHKEY
* Subversion
* Teamspeak (TS2)
* Telnet
* VMware-Auth
* VNC
* XMPP

**Llojet e sulmeve që mund të trajtohen nga THC Hydra:**

* Brute force
* Dictionary
* Paralel Dictionary (16 threads by default)
* Kontroll për null, të kundërt
* Paralel në disa server të ndryshëm

## **Disavantazhet e THC Hydra**

Krahas përdorimit për qëllime ligjore dhe testime të programeve për të rritur sigurinë, kjo vegël mund edhe të keqpërdoret nga hakerët për qëllime të ndryshme ngase është e qasshme në të gjitha platformat dhe konfigurimi i saj është i lehtë. Tjetër disavantazh konsiderohet edhe koha e nevojshme për të provuar kombinimet e emrave të përdoruesit dhe fjalëkalimeve, fakti që këto lloj sulmesh janë jashtëzakonisht të zhurmshme. Zhurma, në këtë rast, nënkupton se sulmet me brute force gjenerojnë shumë trafik, dhe potencialisht mjaft prova të sulmit. Është madje e mundur të kryhet një sulm i mohimit të shërbimit duke përdorur veglat të cilat përkrahin brute force në këtë rast THC Hydra. Dhe duke tentuar vërtetimin në mënyrë të përsëritur gjatë periudhave kohore, mund të jetë e mundur të lidhen burimet e sistemit në një masë të tillë që përdoruesit legjitimë të mos mund të kenë qasje në burim.

Ekzistojnë tashmë disa vegla të disponueshme për qasje të paautorizuar, megjithatë, asnjë nuk mbështet më shumë se një protokoll për të sulmuar dhe përkrah lidhjet paralele përveçse THC Hydra.

# **Pjesa kryesore**

THC Hydra është vegël e thjeshtë për tu instaluar dhe njëkohësisht e lehtë edhe për tu përdorur.

Vegla THC Hydra mbështetet vetëm në sistemet Linux andaj gjendet edhe e instaluar në versionet Kali Linux dhe Parrot. Në sistemet tjera mund të instalohet me ndihmën e emulatorëve të Linux.

Për më tepër, ekzistojnë dy versione të THC Hydra: versioni **CLI-hydra** (Command Line Interface) dhe versioni **GUI–xhydra**(Graphical User Interface).

Për të parë të gjitha komandat të cilat mund të përdoren në THC Hydra shkruajm komandën **hydra -h** si në figurën e mëposhtme.

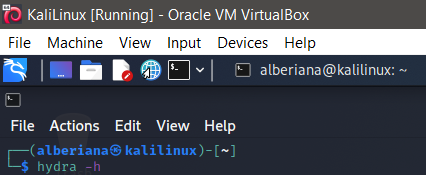


Figura 3: Komanda për shfaqjen e informatave rreth tool-sit Hydra

Komandat e Thc Hydra të paraqitura në terminal pas ekzekutimin të komandës së shkruar janë paraqitur në figurë:



Figura 4: Opsionet e komandave që mund të përdoren në THC Hydra

## **2.1 Instalimi i veglës**

Nëse përdorim sisteme tjera operative atëhere duhet ta instalojmë THC Hydra. Hapat e instalimit të THC Hydra i kemi paraqitur me poshtë.

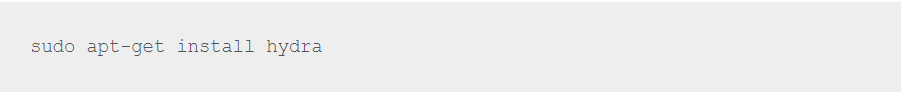


Figura 5: Komanda për instalimin e Hydra

Filloni duke përdorur git për të klonuar nga folderi përkatës në GitHub,

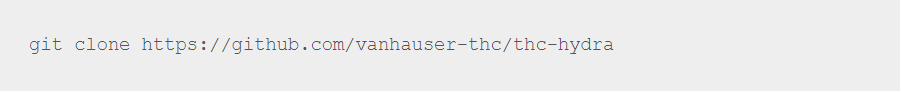


Figura 6: Komanda për klonim nga Github

ndryshimi i direktoriumit të THC-Hydra,

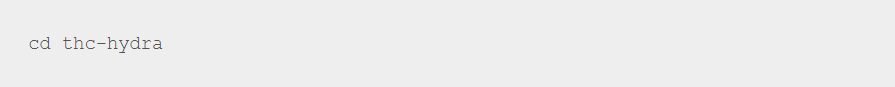


Figura 7: Ndryshim i direktoriumit

tani thjesht konfigurimi.

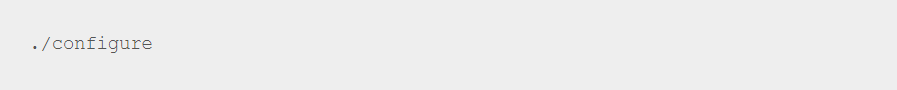


Figura 8: Konfigurimi

Pastaj instalimi…

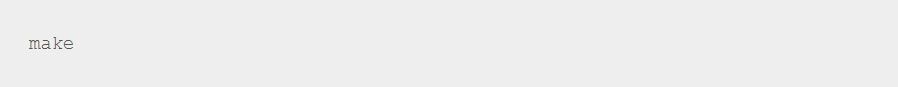


Figura 9: Komanda për instalim të mëtutjeshëm të Hydra

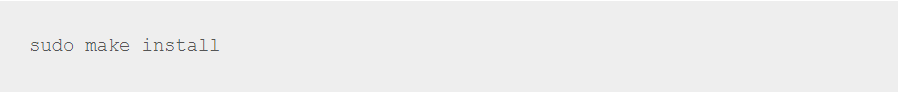


Figura 10: Komanda e fundit për instalim të Hydra

## **Modet e punës**

Hydra punon në 4 mode:

1. Një emër i shfrytëzuesit dhe një fjalëkalim
2. Një liste e emrave të shfrytëzuesve dhe një fjalëkalim
3. Një emër i shfrytëzuesit dhe një listë e fjalëkalimeve
4. Një listë me emra të shfrytëzuesve dhe një listë me fjalëkalime të mundshme

### 2.2.1 Modi një emër i shfrytëzuesit dhe një fjalëkalim

Përdorimi i modit për Brute Force mail në terminal dhe në xhydra:



Figura 11: Komanda per ekzekutim sipas modit 1 në terminal

Mënyrë tjetër e përdorimit të veglës THC Hydra është edhe **xhydra** e cila jepet si komandë në terminalin e KaliLinux pastaj hapet GUI versioni i hydra për të pasur qasje në xhydra.



Figura 12: Komanda për ekzekutimin e xhydra

Pastaj pas ekzekutimit te komandës shfaqet forma

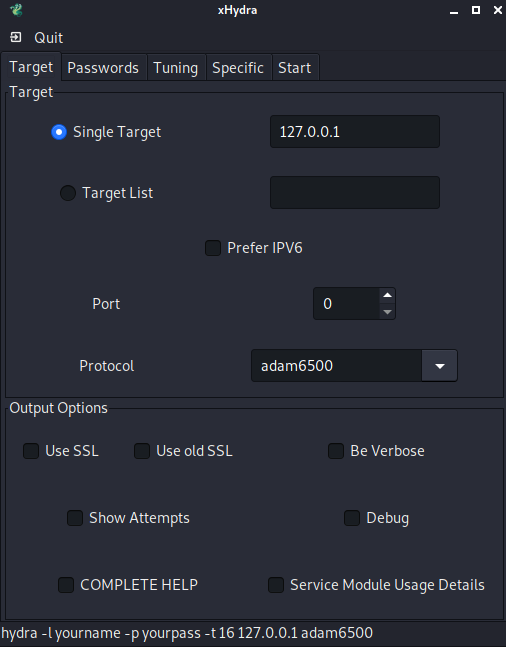


Figura 13: Dritarja e hapur pas ekzekutimit te komandes xhydra ne terminal

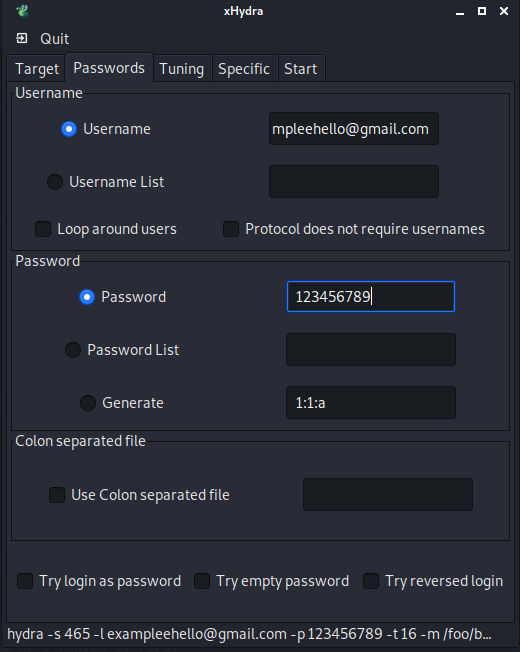


Figura 14: Komandat për ekzekutim sipas modit 1 në xhydra

### Modi nje listë e emrave të shfrytëzuesve dhe një fjalëkalim



Figura 15: Komanda për ekzekutim sipas modit 2 në terminal

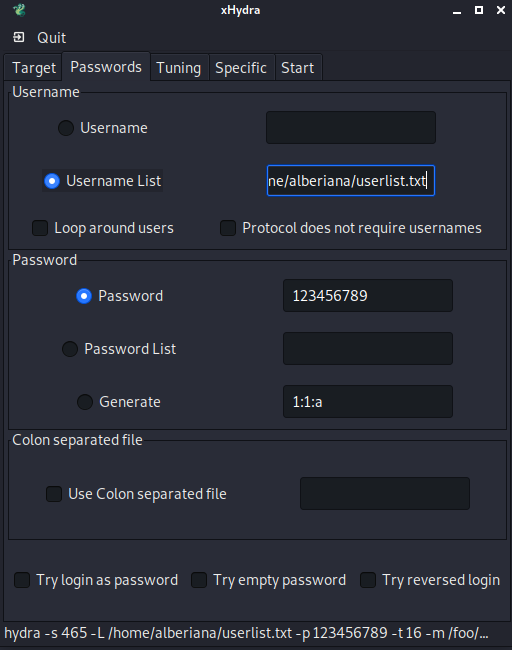


Figura 16: Komandat për ekzekutim sipas modit 2 në xhydra

### Modi një emër i shfrytëzuesit dhe një listë e fjalëkalimeve



Figura 17: Komanda për ekzekutim sipas modit 3 në terminal

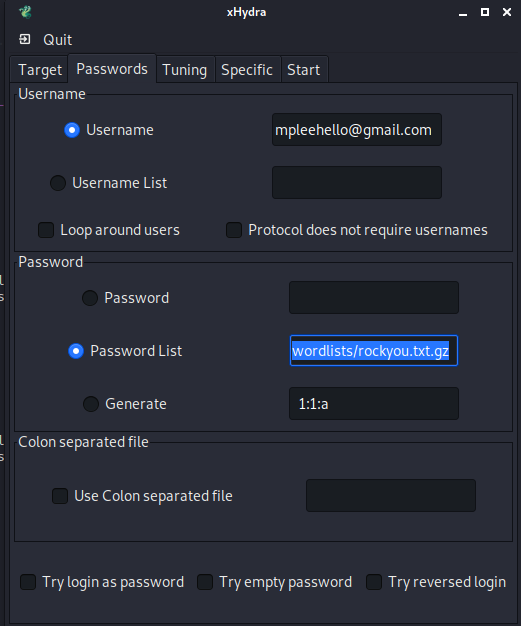


Figura 18: Komandat për ekzekutim sipas modit 3 në xhydra

### Modi një listë me emra të shfrytëzuesve dhe një listë me fjalëkalime të mundshme



Figura 19: Komanda për ekzekutim sipas modit 4 në terminal

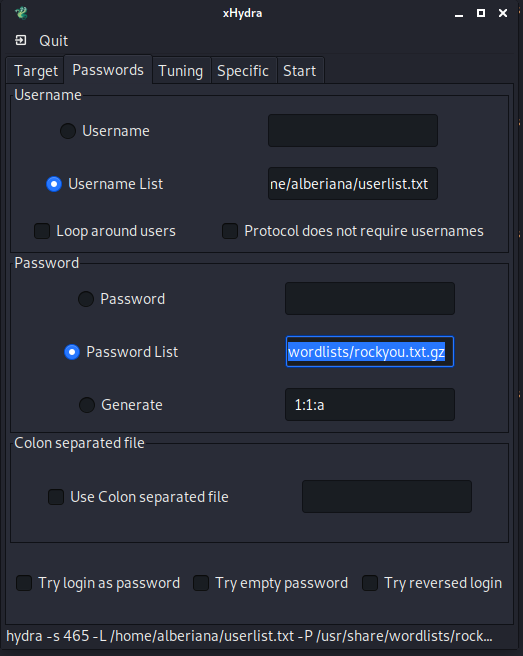


Figura 20: Komandat për ekzekutim sipas modit 4 në xhydra

# **3. Shembuj konkret**

## **3.1 Brute force mail**

Për të përdorur listat me emra të shfrytëzuesve dhe fjalëkalimeve, listat e gatshme gjenden në KaliLinux dhe mund të ju qasemi sipas path-it **/usr/share/wordlists/.**

Të gjitha mail serviset e kanë të aktivizuar mbrojtjen e fjalëkalimeve, kanë bllokuar IP adresat, falsifikimin e rezultateve të fjalëkalimeve. Nëse provojmë të gjejmë fjalëkalimin e një gmail shembull do të kthehet si përgjigje një fjalëkalim tjetër(jo të saktin) i cili do te duhej të kthej për të iu qasur gmail-it dhe sipas krijuesit të veglës THC Hydra i cili citoi në github që “Vegla Hydra nuk është e gabuar, serveri i gmail e zbulon që është bërë përpjekje të zbuluar fjalëkalimin e vërtetë kështu ai jep një përgjigje të rreme” [1].

Në figurën më poshtë kemi paraqitur edhe përgjigjen e serverit të gmail në terminal pas ekzekutimit të komandës:

**hydra -s -S -v -V -l** [**exampleehello@gmail.com**](mailto:exampleehello@gmail.com) **-P /usr/share/wordlists/rockyou.txt.gz** të zbulimit të fjalëkalimit.

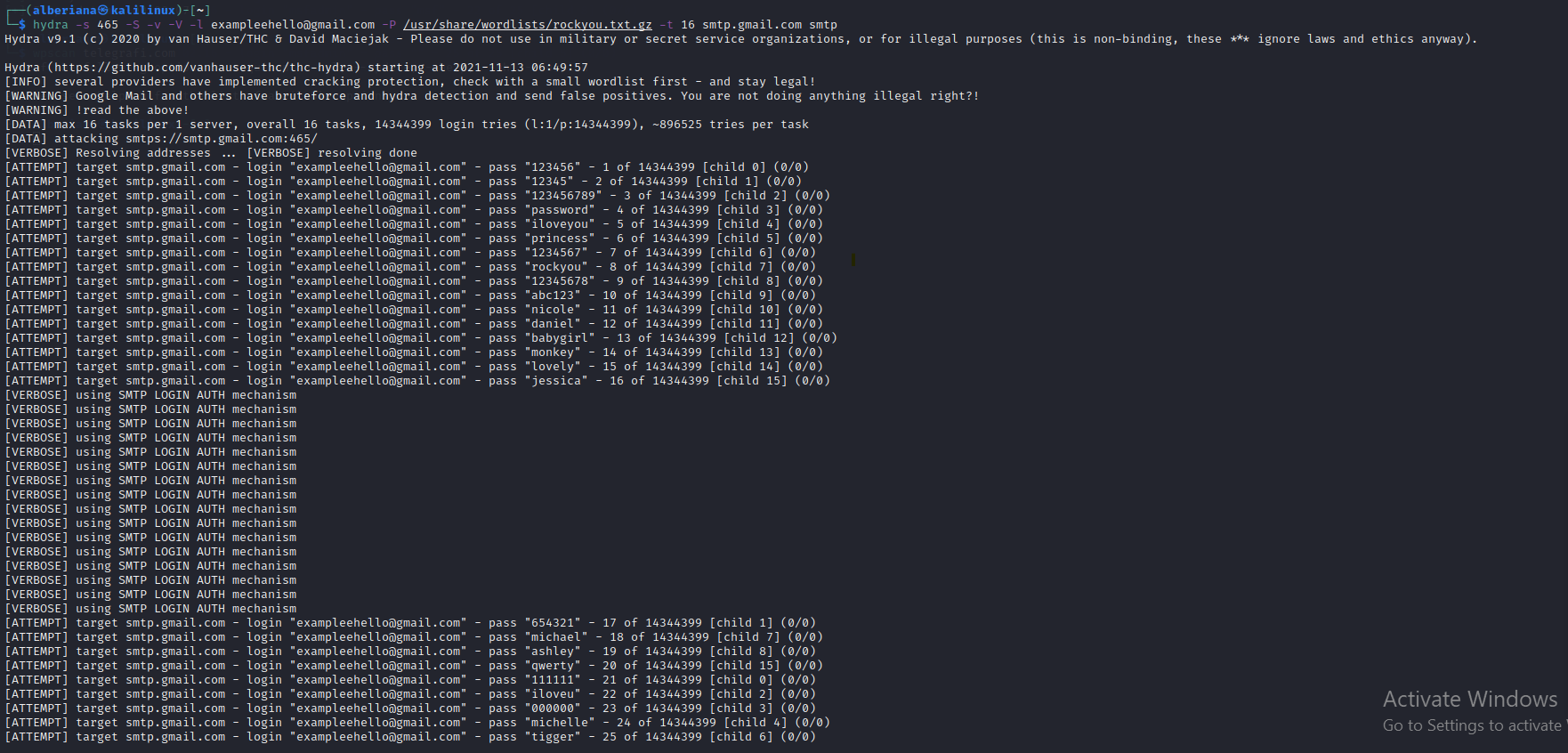


Figura 21: Ekzekutimin i komandës për Brute Force mail

Kështu në rezultatet e fituara shkruan që fjalëkalimi është cookies por nuk është i saktë.

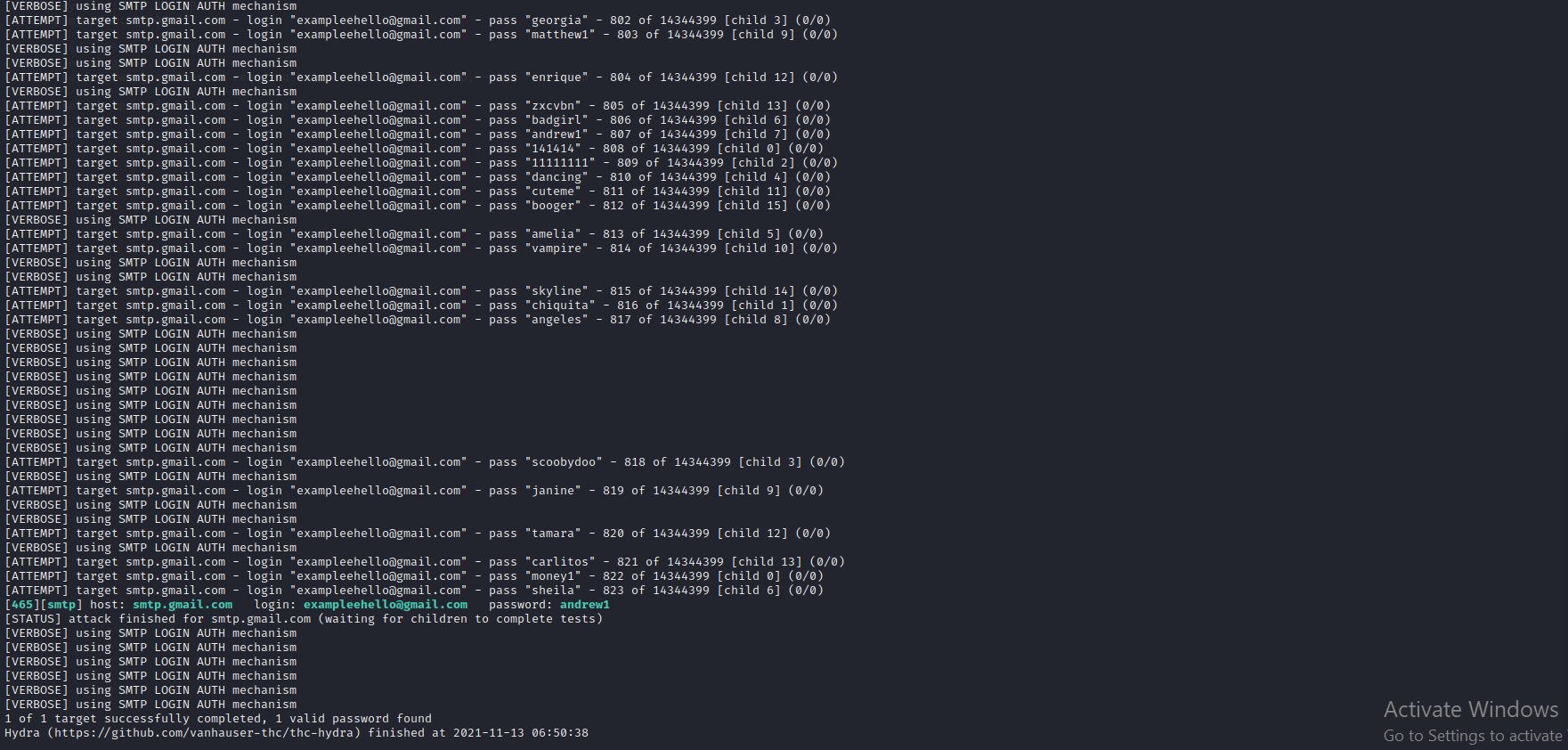


Figura 22: Rezultatet e hydra për Brute Force mail

Si shembull kemi marrë brute force adresën gmail në xhydra.

Tek meny-ja **Target** në pjesën Target shënohet path i URL-se tek Single Target ndërsa në pjesën e fundit Output Options përcaktohet se si duam që të shfaqet dalja do të thotë të shfaqen të gjitha përpjekjet për të zbuluar fjalëkalimin e gmail adresa.

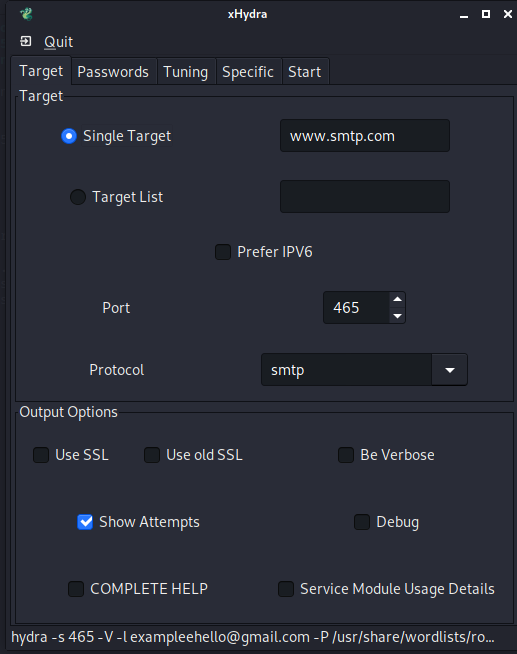


Figura 23: Komandat e nevojshme për ekzekutimin e Brute Force mail në xhydra tek menyja Target

Tek meny-ja **Passwords** form ndahet në tri pjesë në pjesën e parë: Username kemi zgjejdhur checkbox-in Username dhe kemi shkruar në kuti adresën të cilës dëshirojmë ti gjejmë fjalëkalimin ndërsa tek pjesa e dytë Password kemi klikuar të checkbox-i password list dhe kemi zgjedhur fajllin me fjalëkalimi i cili gjendet në Kali Linux **/usr/share/wordlists/rockyou.txt.gz**.

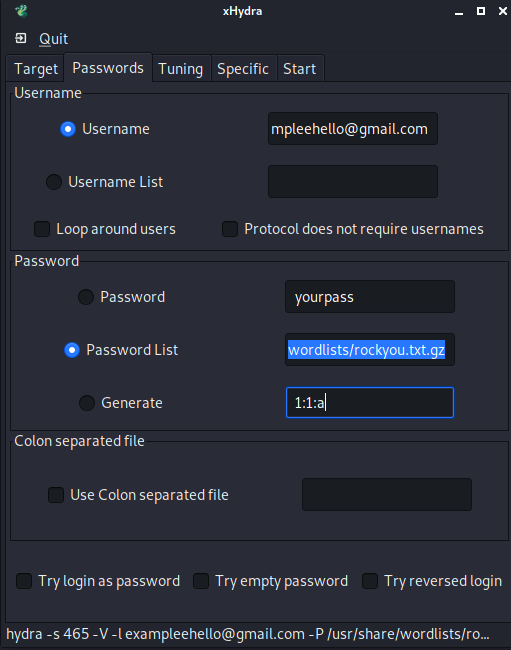


Figura 24: Komandat e nevojshme për ekzekutimin e Brute Force mail në xhydra tek menyja Passwords

Pastaj tek meny-ja **Start** në pjesën output klikojmë butonin Start.

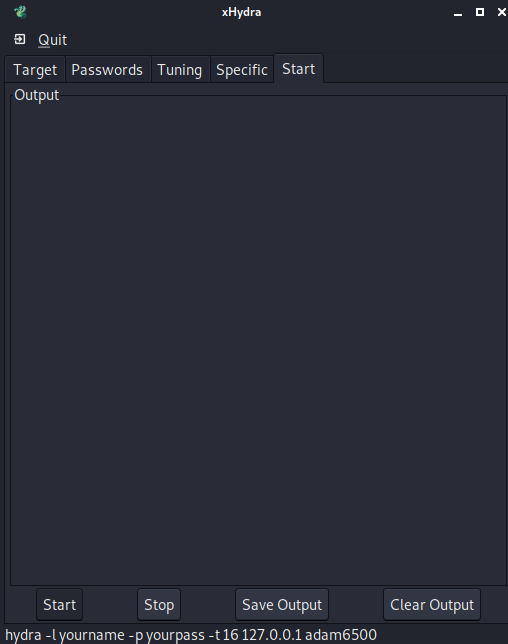


Figura 25: Komanda e fundit për ekzekutim në xhydra

Programi ekzekutohet dhe fillon kërkimin për fjalëkalimin e adresës se kërkuar.

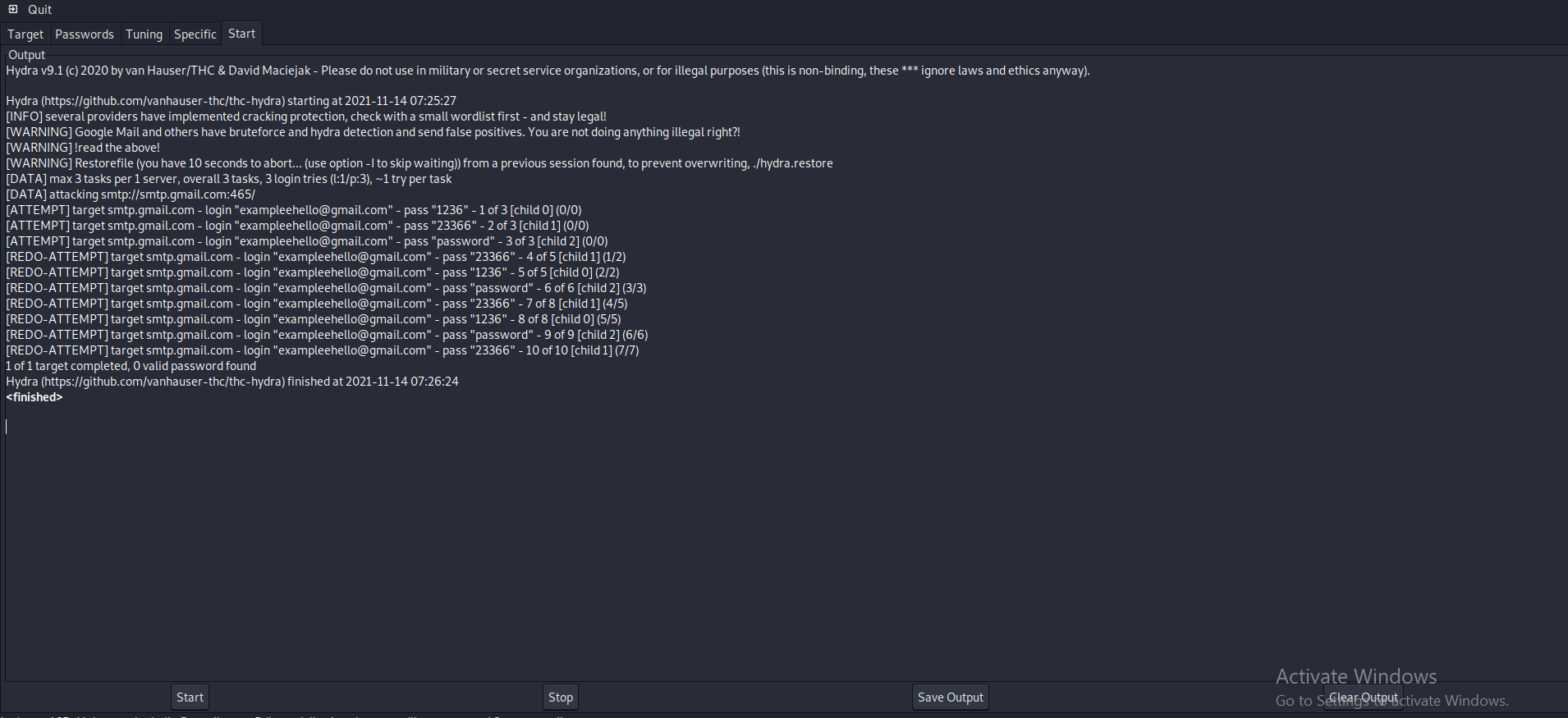


Figura 26: Pjesa kur programi teston fjalëkalimet

## **3.2 Brute Force ueb faqe**

Brute force login form të ueb faqes kompjuterika.tk me komandën :**hydra -l 190718100030 -P /us/share/wordlists/rockyou.txt.gz http-post-form:// 51.15. 226. 11/login/index** është paraqitur ne figurën e mëposhtme komanda:

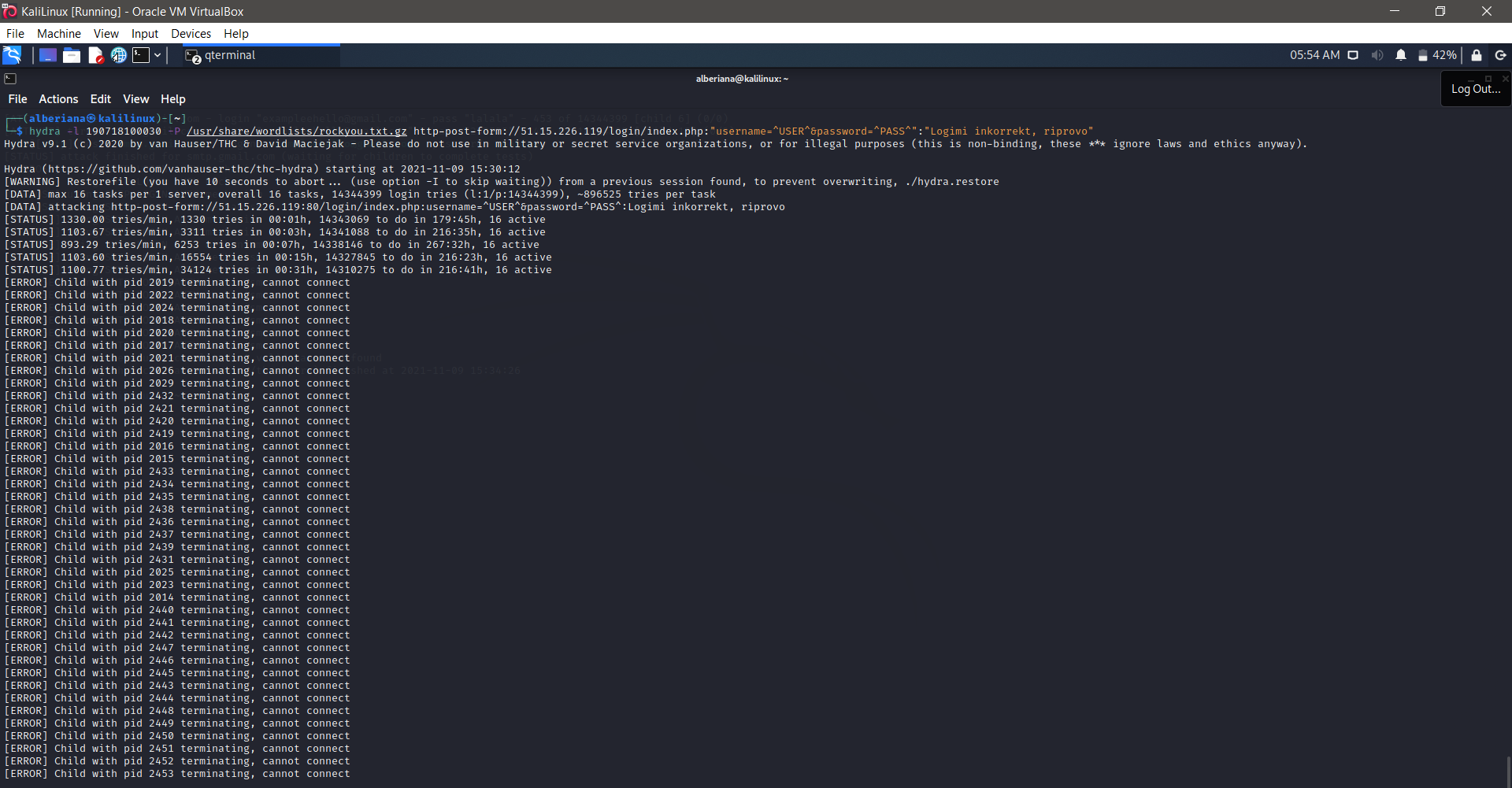


Figura 27: Komanda për ekzekutimin e Brute Force ueb faqe në terminal

Rezultati i fituar pas ekzekutimit të komandës së shkruar:

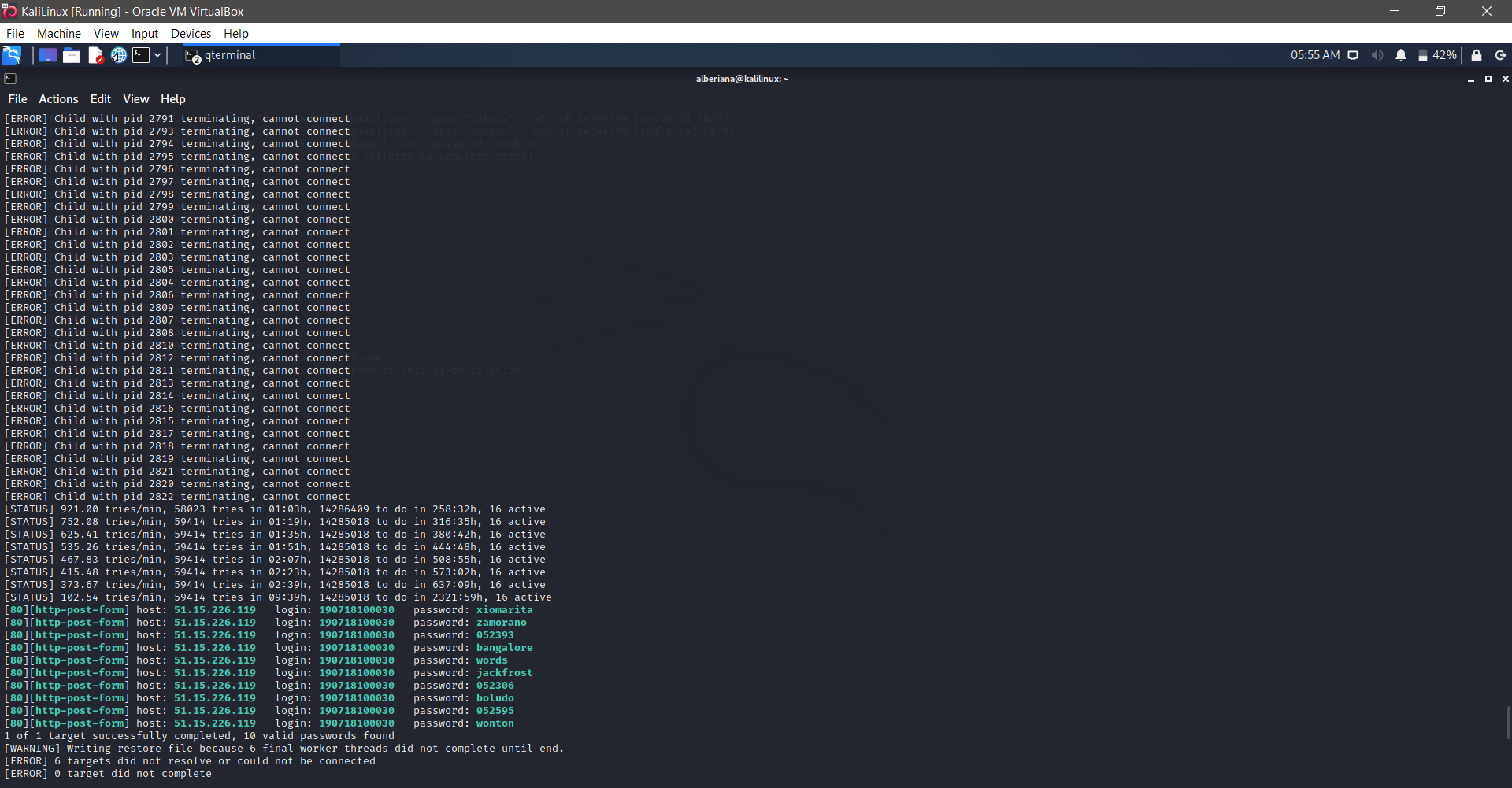


Figura 28: Rezultatet pas ekzekutimit të komandës

## **3.3 Brute Force Metasploitable Server**

Gjetjen e fjalëkalimit të një serveri të cilin e kemi instaluar në VirtualBox që quhet **Metasploit**. Në KaliLinux i ekzekutojmë komandat e nevojshme të cilat janë paraqitur në figurat e mëposhtme. Në terminalin e KaliLinux shkruajmë komandën **nano shfrytëzuesit.lsl** për të krijuar fajllin dhe shkruajmë emrat e shfrytëzueseve.



Figura 29: Komanda për krijimin e fajllit user.lsl

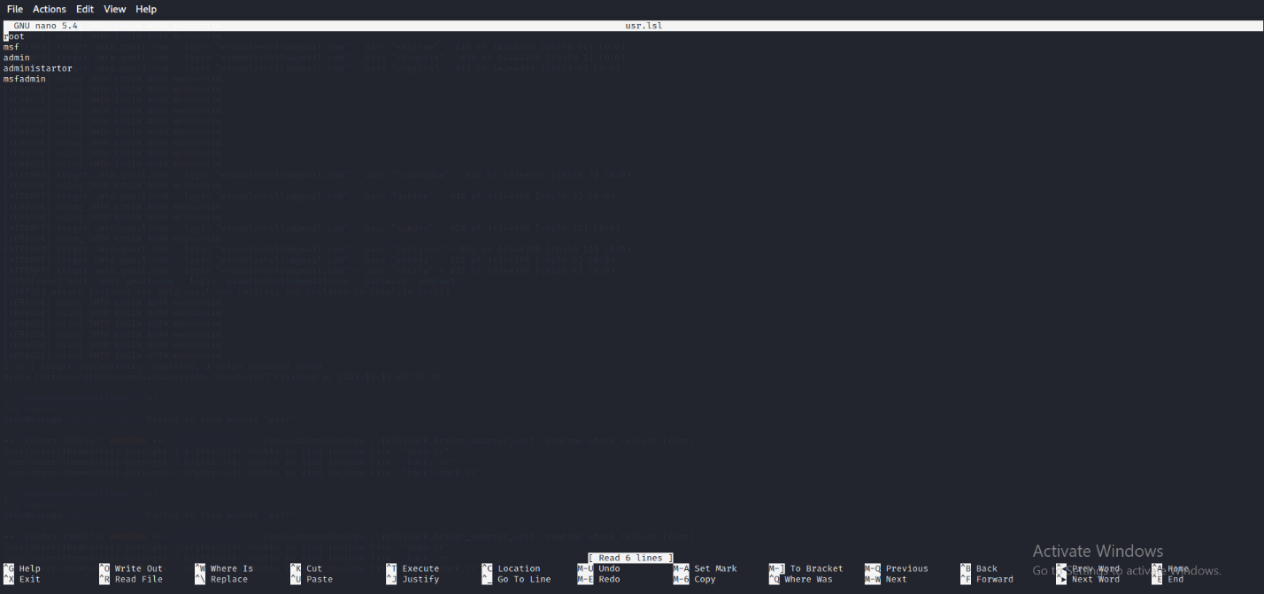


Figura 30: Mbushja e listës user.lsl me të dhëna

Pastaj me komandën **nano fjalëkalimet.lsl** për të krijuar listën me fjalëkalimet e mundshme dhe shkruajmë fjalëkalimet në atë listë të krijuar.



Figura 31: Komanda për krijimin e fajllit pas.lsl



Figura 32: Mbushja e fajllit me të dhëna

Me komandën **ls** mund të shikojmë fajllat e krijuar së fundmi.

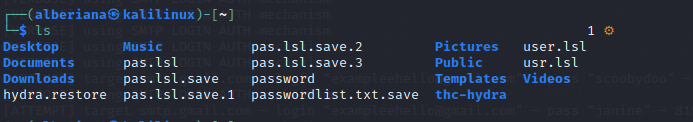


Figura 33: Pasqyre e të gjithë follderëve dhe përmbajtja e tyre

Tani punojmë në **Metasploit.**

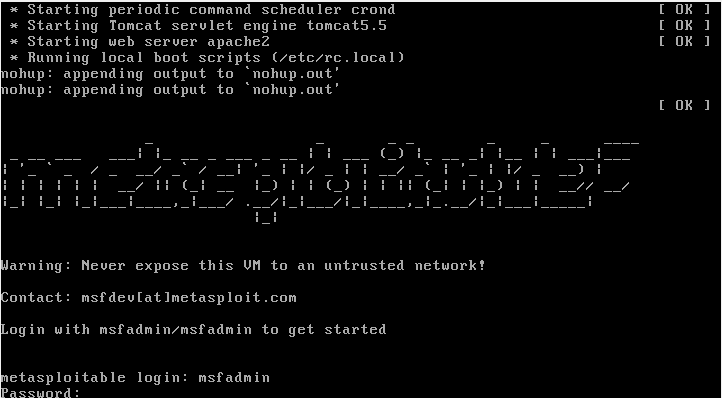


Figura 34: Pamja e parë pas hapjes së Metasploit

Me komandën **ifconfig** në Metasploit mund të shohim edhe ip adresën e serverit.

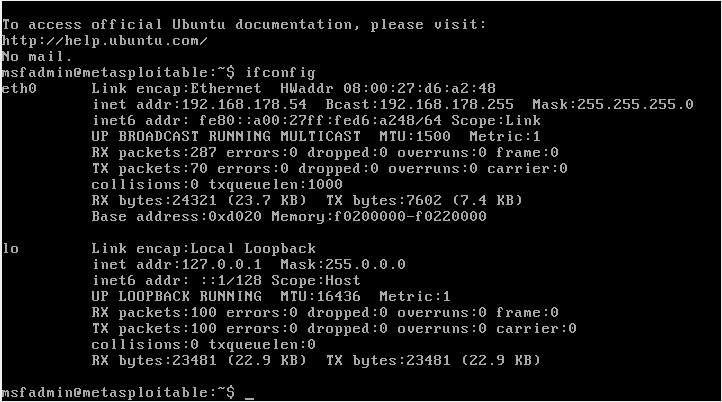


Figura 35: Ekzekutimi i komandës ifconfig

Pastaj ne KaliLinux shkruajmë komandën: **hydra -V -L /home/Alberiana/user.lsl -P /home/Alberiana/psw.lsl -t18 10.180.102.16 ftp**

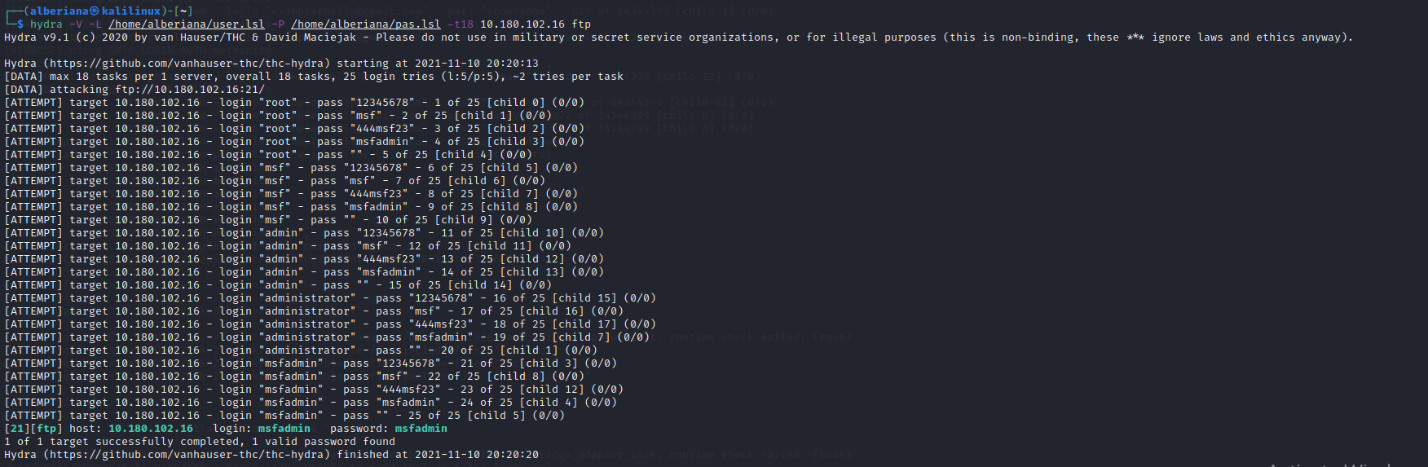


Figura 36: Rezultati pas ekzekutimit të komandës

# **4. Konkluzione**

Realizimi i gjithë projektit ishte shumë sfidues por njëkohësisht edhe argëtues. Ky projekt është projekti i parë që e kemi punuar i kësaj natyre, dhe si student fillestar në këtë lëmi kemi hasur në disa pengesa gjatë realizimit të projektit, por me ndihmën e literaturës, koncepteve themelore të marra nga ligjëratat dhe ushtrimet e lëndës Siguria në Internet, bashkëpunim, ide të përbashkëta dhe me hulumtime të shumta ne besojmë se kemi arritur me sukses studimin e veglës THC Hydra për thyrjen e fjalëkalimeve.

Me anë të këtij projekti ne kemi arritur të kuptojmë dhe të përforcojmë më shumë njohuritë tona rreth mbrojtjes së të dhënave. Ky dokumentim përmban të gjitha informacionet rreth vegles THC Hydra, duke përfshirë instalimin, mënyrat dhe shembujt konkret se si mund të përdoret kjo vegël.

Meqë në shumicën e rasteve THC Hydra duhet të bashkëpunoj me veglat tjera për skanimin e dobësive andaj krijimi i një moduli për një skanim të tillë brenda saj në të ardhmen do ta fuqizonte më shumë funksionalitetin e saj.

# **Referencat**

|  |  |
| --- | --- |
| [1] | V. Huser, «www.github.com,» 11 March 2021. [Në linjë]. |
| [2] | «HackTriks,» 11 October 2021. [Në linjë]. Available: https://book.hacktricks.xyz/brute-force. |
| [3] | «Kali Tutorials,» 22 June 2018. [Në linjë]. Available: https://kalilinuxtutorials.com/hydraonline/?fbclid=IwAR1TAROhk78994yl2OSETirLbtBijnzrvrAZojQe2rAInaniaKpLKZyaNnk. |
| [4] | «Kali,» 10 November 2021. [Në linjë]. Available: https://www.kali.org/tools/hydra/?fbclid=IwAR2ptw\_6xFwgCq8qd8Ysj8a24lOCVeLAibm87wy1DP9i0xoQbU-CVXNyLV4. |
| [5] | «Security Tutorials,» 20 June 2020. [Në linjë]. Available: https://securitytutorials.co.uk/brute-forcing-passwords-with-thc-hydra/?fbclid=IwAR18reiyuhLqOF2A6R5qEw9hKdZjsARZxBa0ArspB5BuxPvUSPM3ic-KePg. |
| [6] | [Në linjë]. Available: http://www.cs.toronto.edu/~arnold/427/19s/427\_19S/tool/thc/thcHydra.pdf?fbclid=IwAR0Vb2wzvPNSJjodu7qFJ\_P\_fm7GTRo-bWoysnci6UDtp1zgLirExn4SaVA. |
| [7] | «Cyber Pratibha,» 22 June 2021. [Në linjë]. Available: https://www.cyberpratibha.com/dictionary-attack-tool-thc-hydra-tutorial/?fbclid=IwAR0W2RImm0rAJZ09Qu0GkfmHbIwJyOeXxMxiYWRvNMEFji9smd1o5AWltuo. |
| [8] | «Cyber Punk,» 2018. [Në linjë]. Available: https://www.cyberpunk.rs/password-cracker-thc-hydra?fbclid=IwAR1UOyykqJ0jq35mHj-tdxX-nZztG3\_oaGoopabXuYVWl6xR0dJqx2pDxqA. |
| [9] | «Concise Courses,» 2021. [Në linjë]. Available: https://www.concise-courses.com/hacking-tools/password-crackers/. |
| [10] | «Hacker Academy,» 2021. [Në linjë]. Available: https://www.hackeracademy.org/how-to-hack-windows-10-with-a-image-in-depth-tutorial/. |
| [11] | «Wikipedia,» 29 July 2021. [Në linjë]. Available: https://en.wikipedia.org/wiki/Hydra\_(software)#:~:text=www.thc.org%2Fthc,right%20username%20and%20password%20combination.. |
| [2] | «Associum,» [Në linjë]. Available: https://associum.com/strong-passwords/?fbclid=IwAR0xGFfYHtAQ66XLcerf4oik\_3ejVW\_C1KKt2L34yepOLKZrWdbv\_Sl1q\_8. |
| [13] | «Wordfence,» 15 June 2017. [Në linjë]. Available: https://www.wordfence.com/blog/2017/06/home-router-botnet-resumes-attacks/?fbclid=IwAR1zUiBHOJUq8o\_GMFzJbiraqtCehkloWkVUZc9cEU6jQ4gOI26GAI\_KgNc. |