**Universiteti i Prishtinës “Hasan Prishtina”**

**Fakulteti Inxhinierisë Elektrike dhe Kompjuterike**

****

**Dokumentim teknik i projektit**

**Lënda: Siguria në Internet**

**Titulli i projektit: SSLsplit**

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

|  |  |  |
| --- | --- | --- |
| PhD.c Mërgim H. HOTI | 1. Diana Zymberi | [diana.zymberi@student.uni-pr.edu](mailto:diana.zymberi@student.uni-pr.edu) |
| 1. Diare Daqi | [diare.daqi@student.uni-pr.edu](mailto:diare.daqi@student.uni-pr.edu) |
| 1. Elona Paçarizi | [elona.pacarizi@student.uni-pr.edu](mailto:elona.pacarizi@student.uni-pr.edu) |
| 1. Veronë Krasniqi | [verone.krasniqi@student.uni-pr.edu](mailto:verone.krasniqi@student.uni-pr.edu) |

Prishtinë, 2021

Përmbajtja

[Abstrakti 3](#_Toc87813004)

[Hyrje 4](#_Toc87813005)

[Çka është *SSLsplit* ? 5](#_Toc87813006)

[Si funksionon *SSLsplit* ? 6](#_Toc87813007)

[ Problemet që duhen zgjidhur: 6](#_Toc87813008)

[ Sfidat që na paraqiten: 6](#_Toc87813009)

[Instalimi i SSLsplit 7](#_Toc87813010)

[Komandat e SSLsplit-it 8](#_Toc87813011)

[Shpjegimi i disa komandave të SSLsplit-it: 9](#_Toc87813012)

[Qëllimi i punimit 10](#_Toc87813013)

[Hapat për zhvillimin e sulmit SSLsplit 11](#_Toc87813014)

[Kushtet e nevojshme për zhvillimin e një sulmi me SSLsplit 11](#_Toc87813015)

[Fillimi i sulmit përmes metodës ARP Spoofing 11](#_Toc87813016)

[Ekzekutimi i sulmit ARP Spoofing përmes veglës Ettercap 12](#_Toc87813017)

[Kapja e trafikut përmes Wireshark 13](#_Toc87813018)

[Ekzekutimi i sulmit përfundimtar përmes SSLsplit 15](#_Toc87813019)

[Konkluzioni 21](#_Toc87813020)

[Referencat 22](#_Toc87813021)

# Abstrakti

Në lëndën "Siguria në Internet" operojmë me Kali Linux dhe veglat e shumta që i ofron në fushën e kibernetikës për sulme, përgjime apo modifikime të të dhënave. Sulmet Man in the Middle (MITM) janë sulme të cilat kryesisht performohen nga Kali Linux ku sulmuesi vendos vetën në linjën komunikuese mes palëve klient-server, dhe fillon përgjimin/modifikimin e paketave. Edhe pse sulmet MITM nuk janë veçanërisht sulme të web-it, është shumë e rëndësishme për çdo testues të ketë njohuri të sulmeve të këtij lloji, si performohen dhe si parandalohen operacionet e paautorizuara në web applications.

Për të kryer sulm MITM duhet ti kombinojmë në mënyrë zingjirore veglat si: Ettercap, Wireshark, SSLsplit.

Ettercap mund të detektojë vetëm transmetimin e fjalëkalimeve, prandaj në rastet kur kërkohet një set kredencialesh më i gjerë si numra të kredit kartelave, dokumente e foto, atëherë është më e dobishme përdorimi i një vegle që mund ta pergjojë të gjithë trafikun në rrjet dhe ta ruaj atë për analizim të mëtutjeshem. Një vegël e tillë është Wireshark dhe është e përfshirë në Kali Linux. Me anë të Ettercap dhe Wireshark, arrijmë të shohim të dhëna konfidenciale mirëpo të enkriptuara prandaj ekziston vegla tjetër, SSLsplit me anë të të cilit mund të bëjmë përgjimin e kanalit trasnsmetues dhe të shohim të dhënat në plaintext. Duke përdorur SSLsplit, përgjojmë dhe e ruajmë trafikun e bazuar në SSL\TLS dhe në këtë mënyrë mund të dëgjohet çdo lidhje e sigurt.

Në këtë projekt sulmi me SSLsplit është kryer vetëm për qëllime edukative!

# Hyrje

Qartësimi i disa koncepteve bazike:

***HTTPS (HyperText Transfer Protocol Secure)*** *– shfaqet në URL kur një faqe në internet sigurohet nga një çertifikatë SSL. HTTPS nënkupton transfer protokollin për të dërguar të dhëna mes një shfletuesi dhe një faqe në internet dhe është e koduar në mënyrë që të rritet siguria e transferimit të të dhënave sidomos atyre të ndjeshme si hyrja në një llogari bankare, shërbimi i postës, shëndetsor etj.*

***SSL (Secure Sockets Layer****) – është protokoll për të mbajtur të sigurt një lidhje interneti dhe për të mbrojtur çdo të dhënë të ndjeshme që dërgohet ndërmjet dy sistemeve, duke parandaluar që kriminelët të lexojnë dhe modifikojnë çdo informacion të transferuar. Të dy sistemet mund të jenë një server dhe një klient ose server me server. SSL përdorë algoritme të enkriptimit për shkëmbimin e të dhënave duke parandaluar hakerët që t’i lexojnë ato të dhëna.*

***Man-in-the-middle*** *- është një sulm ku sulmuesi në mënyrë të fshehtë transmeton dhe ndoshta ndryshon komunikimin midis dy palëve që besojnë se ata po komunikojnë drejtpërdrejt me njëri-tjetrin*.

***Proxy SSL*** *-* *është një përfaqësues transparent që kryen enkriptimin e shtresave të sigurta të bazave (SSL) dhe deshifrimin midis klientit dhe serverit. As serveri dhe as klienti nuk mund të zbulojnë praninë e tij.*

## Çka është *SSLsplit* ?

Duke përdorur SSLsplit, mund të përgjojmë dhe të ruajmë trafikun e bazuar në SSL dhe në këtë mënyrë të dëgjojmë çdo lidhje të sigurt. SSLsplit është një mjet për sulmet man-in-the-middle kundër lidhjeve të rrjetit të koduar SSL/TLS. Lidhjet përgjohen në mënyrë transparente përmes një motori përkthimi të adresave të rrjetit dhe ridrejtohen në SSLsplit. SSLsplit përfundon SSL/TLS dhe fillon një lidhje të re SSL/TLS me adresën origjinale të destinacionit, ndërkohë që regjistron të gjitha të dhënat e transmetuara.

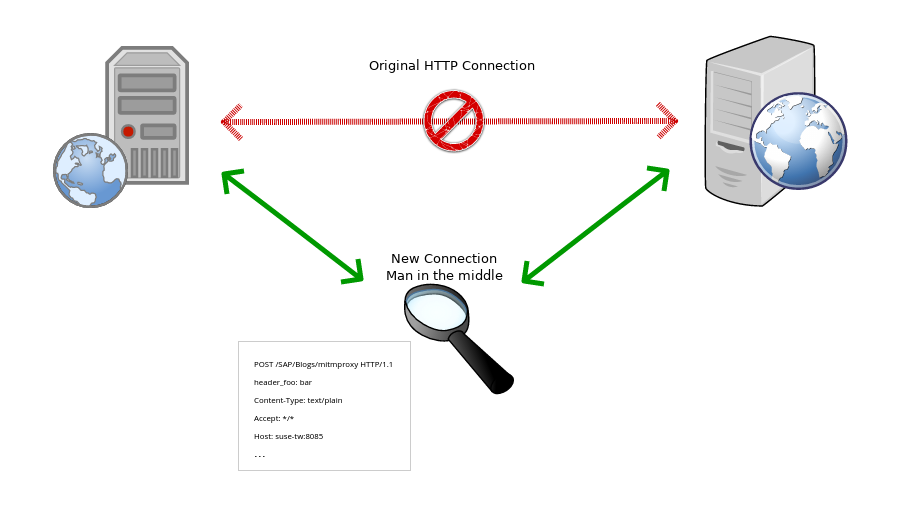


Figura 1: Paraqitja e një skeme se si funksionon SSLsplit

Tema të cilën e trajtojmë ne i takon fushës së sigurisë në internet. Siguria dhe vigjilenca janë jetike për të mbajtur veten të sigurt, dhe kjo përgjegjësi nuk është vetëm mbi individin, gjithkush është një objektiv i mundshëm, duke përfshirë qeveritë dhe korporatat private. Pa asnjë mbrojtje në internet, ju e lini veten të hapur për të qenë viktimë e mashtrimit, vjedhjes dhe madje edhe dëmtimit të pronës, prandaj pjesa e studimit të sigurisë në internet dita ditës po bëhet e pashmangshme.

Rëndësia e SSLsplit qëndron në faktin se ajo synohet të jetë e dobishëme për mjekësinë ligjore të rrjetit, analizën e sigurisë së aplikacioneve dhe testimin e depërtimit.

## Si funksionon *SSLsplit* ?

SSLsplit funksion mjaft ngjashëm me mjetet e tjera transparente të proxy SSL, SSLsplit mbledhë lidhjet SSL dhe pretendon të jetë klienti me të cilën po lidhet serveri. Për ta bëre këtë ajo në mënyrë dinamike gjeneron një çertifikatë dhe e nënshkruan atë me një çelës privat të një çertifikatë CA të cilës klienti duhet t’i besojë.

Për shembull, një klient dëshiron të dërgojë një email duke përdorur serverin e sigurtë Gmail SMTP (në portin 456), SSLsplit krijon një çertificatë për “smtp.gmail.com” dhe në këtë mënyrë pretendon të jetë serveri i postës Gmail klientit. Në drejtimin e rrjedhës së sipërme (drejt serverit aktual të postës Gmail), SSLsplit lidhet me serverin ashtu si një klient normal, përcjell të gjithë trafikun që klienti aktual i shkruan në SSL.

### Problemet që duhen zgjidhur:

Për të pasur një sulm të suksesshëm, sulmuesi duhet të vendoset ndërmjet serverit dhe klientit të cilën mund ta bëjë në disa mënyra:

1. Përdorë ARP spoofing për të ridrejtuar trafikun e viktimës duke ndërruar MAC adresën e klientit me IP adresën e sulmuesit, për këtë nuk kemi nevojë të kemi çasje fizike te pajisja e klientit.
2. Duke e ndryshuar DEFAULT getway adresën e viktimës. Kjo është metoda më e thjeshtë nëse keni çasje te pajisja e viktimës.
3. Falsifikimi i hyrjeve të DNS me një server DNS që kthen IP adresën e sulmuesit për domene të caktuara.

### Sfidat që na paraqiten:

Sfida më e madhe është gjetja e dobësive të sistemeve të ndryshme në internet, fatëkeqsisht nuk kemi arritur të gjejmë apo të identifikojmë ndonjë të tillë edhe pse kemi tentuar në shumë sisteme të ndryshme. E gjitha kjo ndodhë si pasojë e rritjes së sigurisë, që si rrjedhim vështirëson implementimin e sulmeve të tilla.

Punimi i këtij projekti na dha motiv që në projektet pasuese të tregohemi më vigjilent në aspektin kibernetik, pasi që deri tani nuk kemi pasur përvojë në këtë fushë.

Kontributi ynë në këtë aspekt si fillestarë në këtë fushë ka të bëjë me ngritjen e vetëdijesimit të personave jo shumë të familjarizuar me kibernetikë që të kenë kujdes në shpërndarjen e të dhënave sensitive.

## Instalimi i SSLsplit

Instalimin e veglës SSLsplit mund ta bëjmë me anë të komandës si në vijim:

sudo apt-get install sslsplit

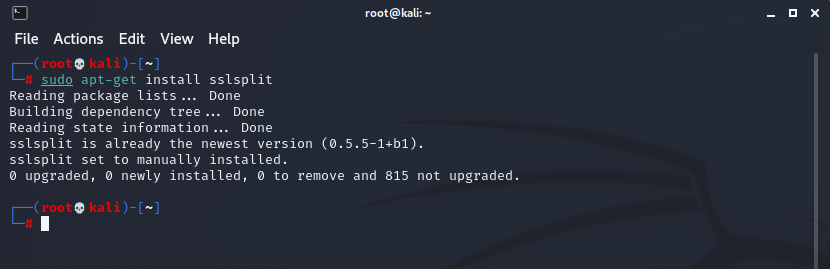


Figura 2: Instalimi i SSLsplit-it

Në shumicën e rasteve SSLsplit veçse gjendet në Kali Linux. Mund ta gjejmë nëpërmjet një kërkese tek aplikacionet që i përmanë në tërësi Kali Linux-i:

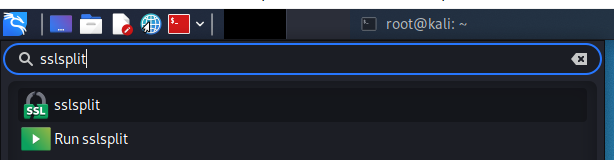


Figura 3: SSLsplit-i në Kali Linux

### Komandat e SSLsplit-it

Vegla SSLsplit ka disa komanda të cilat ne mund ti shohim në terminalin tonë përmes komandës:

sslsplit –h



Figura 4: Komandat e SSLsplit-it

### Shpjegimi i disa komandave të SSLsplit-it:

|  |  |
| --- | --- |
| **-a pemfile** | Përdorë një çertifikatë të klientit nga pemfile kur destinacioni i serverit kërkon një çertifikatë të klientit. |
| **-b pemfile** | Përdorë një çelës privat të klientit nga pemfile kur destinacioni i serverit kërkon  një çertifikatë të klientit. |
| **-c pemfile** | Përdorë CA(dhe çelësin) prej pemfile për të nënshkruar çertifikatë të falsifikuar. Nëse pemfile përmban çelesin privat CA, ai gjithashtu duhet të ngarkohet, përndryshe duhet të pajiset me -k. Nëse pemfile përmban parametra të grupit Diffie-Hellman, ato gjithashtu duhet të ngarkohen, përndryshe mund të sigurohen me -g. |
| **-k pemfile** | Përdorë pemfile çelësin CA(dhe çertifikatën) nga pemfile për të nënshkruar çertifikatë të falsifikuar.  Nëse pemfile gjithashtu përmban çertifikatën CA që përputhet, është gjithashtu i ngarkuar, përndryshe duhet të jetë të pajisur me -c. Nëse pemfile përmban parametra të grupit Diffie-Hellman, ato janë gjithashtu të ngarkuara, përndryshe mund të pajisen me -g. Nëse jepet -t , SSLsplit do të krijojë një çertifikatë nëse nuk ka një çertifikatë që përputhet në çertifikatë directory. |
| **-h** | Shfaq ndihmën për përdorim dhe dalje (usage and exit). |
| **-g pemfile** | Përdorë parametrat e grupit DH nga pemfile (default: keyfiles or auto) |
| **-m group** | Kur përdorim -u, anashkalojmë grupin (default: primary group of user) |
| **-q** | Përdorë URL si pikë shpërndarjeje CRL për të gjitha çertifikatat e falsifikuara. |
| **-r proto** | Mbështetë vetëm një nga tls10 tls11 tls12 (default: të gjitha). |
| **-s ciphers** | Përdorë specifikimin e shifrave të OpenSSL për lidhjet SSL / TLS të serverit dhe klientit. Nëse -s nuk jepet, përdoret një cipher list of All:-a null.  Që lidhjet të jenë të suksesshme, modelet e shifrave SSLsplit duhet të përfshijnë të paktën një model Cipher të mbështetur nga klienti dhe serveri i secilës lidhje. |
| **-t certdir** | Përdorë cert+chain+key PEM files nga certdir per të synuar të gjitha faqet që përputhen me emra të zakonshëm(non-matching:generate if CA). |
| **-u user** | Heq privilegjet tek përdoruesi (default if run as root: nobody) |
| **-w gendir** | Shkruan çelësin e fletës dhe gjeneron vetëm çertifikata për “gendir” |

# Qëllimi i punimit

Qëllimi i këtij raporti është analiza dhe trajtimi i veglave të ndryshme që na i ofron Kali Linux. Ekzistojnë shumë vegla të cilat ndahen në bazë të domenit si: Information Gathering, Vulnerability Analysis, Wireless Attacks, Web Applications, Sniffing & Spoofing, Exploitation Tools, Password Attacks etj.

Në këtë dokument është trajtuar vegla “SSLsplit”, përmes të cilës e kemi luajtur rolin e man-in-the-middle.

Të veçantat e SSLsplit janë:

* Refuzon kërkesat e Protokollit të Statusit të Çertifikatës në internet (OCSP) për të parandaluar viktimat të kontrollojnë statusin e revokimit të çertifikatave të ofruara.
* Parandalon kalimin në protokollet eksperimentale QUIC/SPDY nga Google, të cilat synojnë të ofrojnë shpejtësi dhe siguri më të mirë.

Përparsitë e SSLsplit janë:

* SSLsplit është në gjendje të trajtojë një numër relativisht të lartë dëgjuesish dhe lidhjesh sepse ka një arkitekturë multithreaded, që mundëson përgjimin e një rrjete të tërë.
* Performancë e lartë – SSLsplit është zhvilluar me performancë të lartë, arkitektura e saj me shumë fije, e bazuar në ngjarje përpiqet të maksimizojë sasinë e lidhjeve që është në gjendje të trajtojë.

Të metat janë:

* matriali i pakët rreth SSLsplit
* trafiku në hyrje shkon nga gateway direkt te hostet kështu që sulmuesi sheh dhe kontrollon vetëm trafikun në dalje.

# Hapat për zhvillimin e sulmit SSLsplit

## Kushtet e nevojshme për zhvillimin e një sulmi me SSLsplit

Që të mund ta realizojmë një sulm me SSLsplit, duke luajtur rolin e man-in-the-middle së pari duhet t’i identifikojmë viktimat tona, kjo arrihet duke ndërhyrë në trafikun komunikues ku sulmuesi e përgjon komunikimin midis pajisjeve të rrjetit.

Pra objektivet duhet të zgjedhen paraprakisht dhe është e rëndësishme të përfshihen vetëm hostet rreptësisht të nevojshme si objektiva pasi sulmet e tilla gjenerojnë shumë rrjet trafiku dhe shkaktojnë probleme të performancës për të gjitha hostet.

Kjo na cakton hapin e parë që duhet ndjekur për fillimin e sulmit që është caktimi i hostave, të cilët duke i “helmuar” me metodën e përzgjedhur ARP Spoofing i shndërrojmë në viktima të sulmit.

## Fillimi i sulmit përmes metodës ARP Spoofing

Një mënyrë që një sulmues ta ekzekutojë një sulm MITM në rrjet është të dërgojë pako të falsifikuara të Protokollit të Rezolucionit të Adresave (ARP) në secilën nyje të viktimës, duke tentuar kështu të “helmojë” cache-in e tyre ARP. Sulmuesi në mënyrë specifike dëshiron të zëvendësojë adresën MAC të IP adresës së viktimës në distancë me adresën MAC të sulmuesit.

Në një sulm të zakonshëm MITM, një nga targetet e synuara është LAN-i i sulmuesit, ndërsa tjetri target është në internet. Për të ekzekutuar sulmin ndaj dy viktimave, sulmuesi dërgon pako ARP false te viktima lokale dhe porta lokale, për të helmuar me ARP këto dy memorie. Cache ARP e viktimës lokale duhet të ketë adresën MAC të sulmuesit për adresën IP të portës, dhe cache ARP e portës duhet të ketë adresën MAC të sulmuesit për IP adresën të objektivit lokal. Në këtë mënyrë, i gjithë komunikimi nga nyja e synuar në internet (nëpërmjet portës) kalon përmes sulmuesit.

Sulmet e “helmimit” ARP janë të dyanshme: sulmuesi mund të futet mes serverit të Internetit dhe hostit të viktimës. Ndërsa sulmi është në zhvillim e sipër, hosti i viktimës në LAN mendon se po flet drejtpërdrejt me serverin e Internetit, ndërsa serveri i Internetit mendon se po flet drejtpërdrejt me hostin LAN, kur në realitet një sulmues është duke përgjuar trafikun e rrjetit.

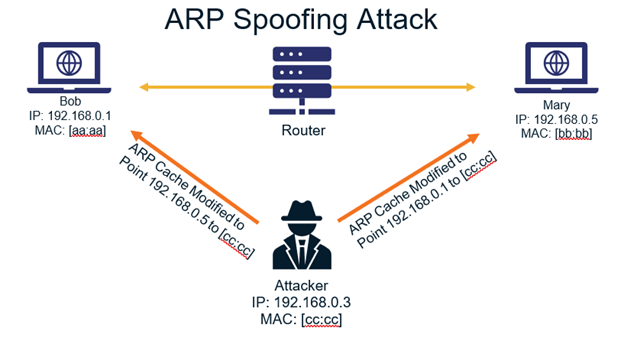


Figura 5: Sulmi përmes ARP Spoofing

## Ekzekutimi i sulmit ARP Spoofing përmes veglës Ettercap

Mashtrimi i Protokollit të Rezolucionit të Adresave (ARP) është ndoshta sulmi më i zakonshëm i MITM. Bazohet në faktin se ARP është ai që përkthen IP adresat në MAC adresa dhe nuk verifikon vërtetësinë e përgjigjeve që një sistem merr. Kjo do të thotë që, kur kompjuteri i Alice-s pyet të gjitha pajisjet në rrjet, "cila është MAC adresa e pajisjes me IP xxx.xxx.xxx.xxx", do të besojë përgjigjen që merr nga çdo pajisje, qoftë serveri i dëshiruar apo jo, kështu që mashtrimi ARP ose helmimi ARP funksionon duke dërguar shumë përgjigje ARP në të dy skajet e zinxhirit të komunikimit, duke i thënë secilit se adresa MAC e sulmuesit korrespondon me adresën IP të homologut të tyre. Në këtë rast, ne do të përdorim veglën Ettercap për të kryer një sulm mashtrimi ARP dhe për të vendosur veten ndërmjet një klienti dhe një serveri në Internet.

Për të pasur çasje në veglën Ettercap hapim një terminal te Kali Linux ku qasemi si root dhe e shkruajmë komandën:

**ettercap –G**

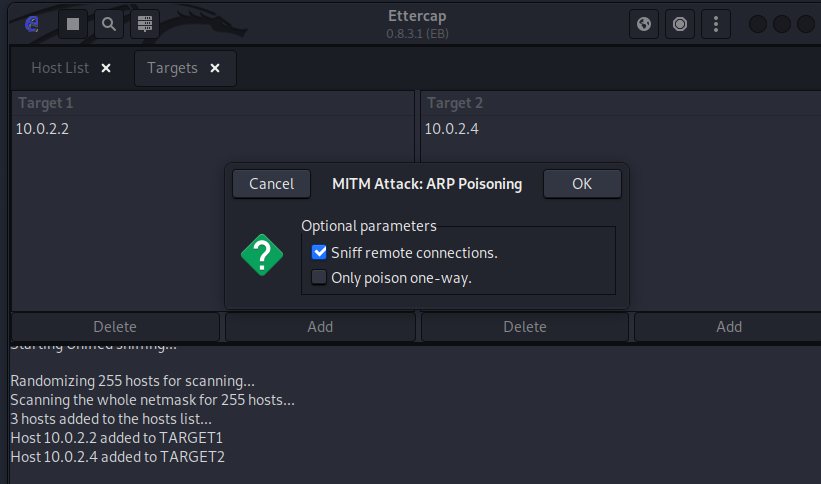


Figura 6: Ekzekutimi i ARP Spoofing përmes Ettercap

Sniff remote do të thotë se Ettercap do të kapë dhe të lexojë të gjitha paketat e dërguara midis pikave fundore prandaj edhe e zgjodhëm këtë mënyrë, ndërsa Only poison one-way përdoret kur vetëm duam ta “helmojmë” targetin por nuk duam t’i dimë përgjigjet nga serveri.

## Kapja e trafikut përmes Wireshark

Për ta vërtetuar që sulmi përmes Ettercap ka qenë i sukseshëm si dhe dy viktimat tona po komunikojnë me njëri tjetrin është e dobishme ta kemi një mjet që mund të dëgjojë të gjithë trafikun në rrjetë në mënyrë që të mund ta analizojmë. Sniffing tool-i më i mirë që kemi përdorur për qëllimet tona është Wireshark i përfshirë në Kalin Linux.

Nga fotoja e më poshtme shihen paketat e trafikut të rrjetës që komunikojnë përmes ARP protokollit, por pasi të dhënat janë të enkriptuara ne nuk mund të zbulojmë ndonjë informatë dhe prandaj është e domosdoshme të realizojmë sulmin final përmes SSLsplit në menyrë që edhe të dhënat e enkriptuara të na shfaqen si plaintext.

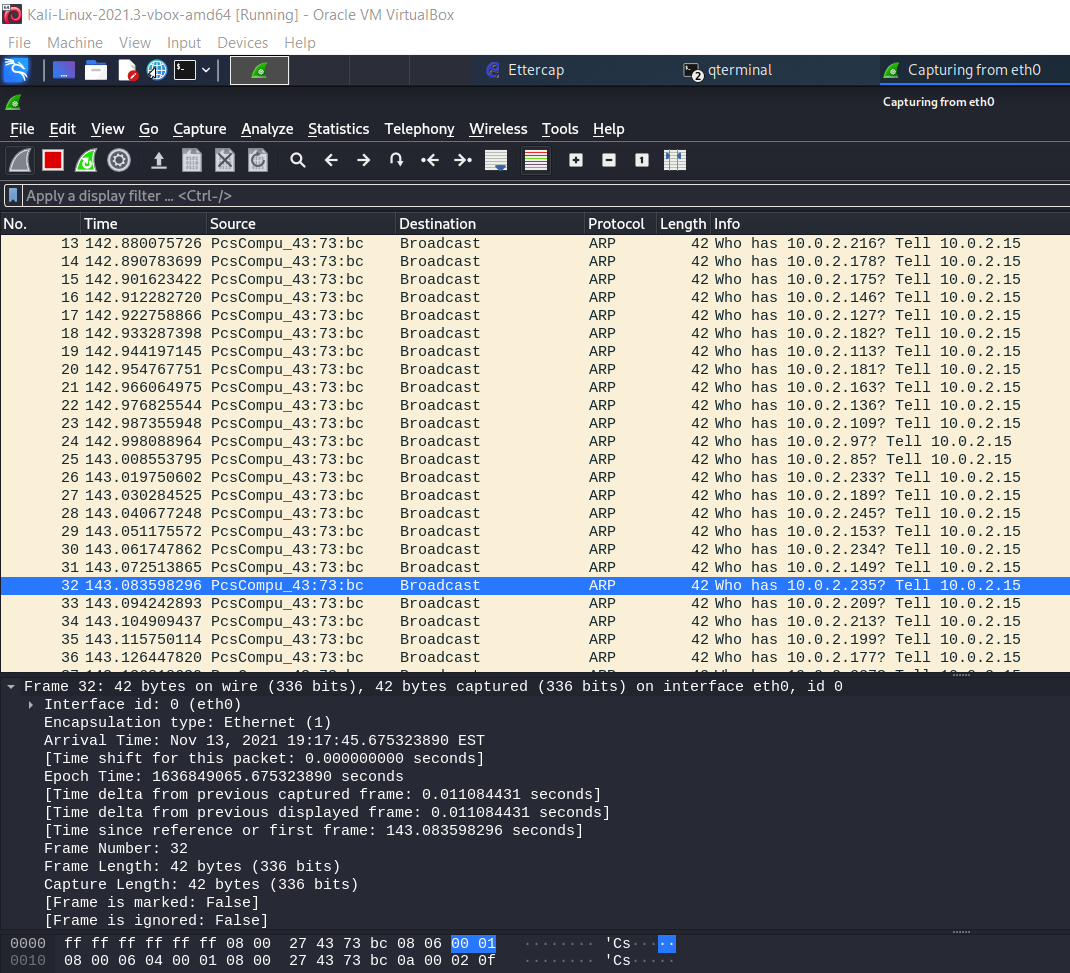


Figura 7: Kapja e paketave të enkriptuara përmes Wireshark

Wireshark dëgjon çdo paketë nga ndërfaqja që kemi zgjedhur për të dëgjuar merr dhe e vendos atë në formë të lexueshme në ndërfaqen e saj. Më në fund, kur i bëmë një kërkesë serverit, pamë se si Ëireshark i kapi të gjitha informacionin që përmban ajo kërkesë, duke përfshirë protokollin, burimin dhe destinacioninIP si dhe të dhënat e dërguara nga klienti.

## Ekzekutimi i sulmit përfundimtar përmes SSLsplit

Nga rezultatet e mësipërme vërtetuam që nëse përpiqemi të përgjojmë një sesion HTTPS duke përdorur atë që kemi parë deri më tani, nuk do të mund të marrim ndonjë rezultat prej tij pasi i gjithë komunikimi është i enkriptuar. Për të përgjuar, lexuar dhe ndryshuar lidhjet SSL dhe TLS, duhet të bëjmë një sërë hapash përgatitor për të konfiguruar përfaqësuesin tonë SSL. SSLsplit funksionon duke përdorur dy çertifikata, njëra për ti treguar serverit që është klienti, në mënyrë që të mund të marrë dhe deshifrojë përgjigjet e serverit dhe tjetra për t’i treguar klientit se është serveri.

Që SSLsplit të veprojë si ndërmjetës për lidhjet SSL, duhet të jetë në gjendje të gjenerojë dhe nënshkruajë çertifikata që viktima i beson. Për ta bërë këtë, viktima duhet të ketë çertifikatën CA root të sulmuesit të cilës i beson. Kjo çertifikatë krijohet përmes komandave:

**openssl genrsa -out certaauth.key 4096**

**openssl req -new -x509 -days 365 -key certaauth.key -out ca.crt**

Komanda e parë gjeneron një çelës privat RSA 4096-bitësh në formatin PEM (ca.key), dhe komanda e dytë përdor këtë çelës privat për të gjeneruar një çertifikatë CA root të vetë-nënshkruar (ca.crt). Të dyja nevojiten nga SSLsplit më vonë, por çertifikata duhet të instalohet në shfletuesin ose sistemin operativ të viktimës.Çertifikatën e mbushim me të dhëna si në figurë:



Figura 8: Krijimi dhe nënshkrimi i çertifikatës

Më pas, duhet të aktivizojmë IP forwarding për të mundësuar funksionimin e sistemit të routimit që e bëjmë përmes komandave:

**echo 1 > /proc/sys/net/ipv4/ip\_forward**

Tani do të konfigurojmë disa rregulla për të parandaluar që gjithcka të bëhet forward dhe ta ngarkojmë trafikun. Së pari, le të kontrolloni nëse ka ndonjë gjë në tabelën tonë nat iptables:

**iptables -t nat –L**

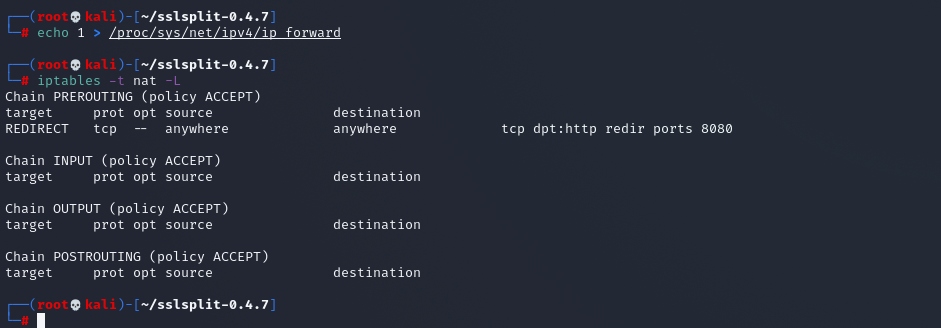


Figura 9: IP forwarding dhe NAT tabelat

Nëse ka ndonjë rezultat që na duhet, ne e rezervojmë atë sepse tani do të fshijmë gjithcka përmes komandës:

**iptables -t nat -L > iptables.nat.bkp.txt**

I fshijmë edhe tabelat:

**iptables -t nat –F**

Tani jemi gati për t’i vendosur rregullat e prerouting dhe të marrim informata nga routeri:

**iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports 8080**

**iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-ports 8443**

**iptables -t nat -A PREROUTING -p tcp --dport 587 -j REDIRECT --to-ports 8443**

**iptables -t nat -A PREROUTING -p tcp --dport 465 -j REDIRECT --to-ports 8443**

**iptables -t nat -A PREROUTING -p tcp --dport 993 -j REDIRECT --to-ports 8443**

**iptables -t nat -A PREROUTING -p tcp --dport 5222 -j REDIRECT --to-ports 8080**

SSLsplit do të funksionojë në dy porte: 8080 për lidhjet TCP, jo-SSL si HTTP, SMTP ose FTP, dhe 8443 për lidhjet SSL si SMTP mbi SSL, HTTPS, etj. Për të përcjellë paketat që vijnë në makinën e sulmuesit tek këto portet e brendshme, i kemi përdorur edhe NAT iptables.

Fillimisht aktivizuam opsionin e forwarding dhe pas kësaj, krijuam rregulla iptables për të përcjellë kërkesat nga portet 80 dhe 443 (HTTP dhe HTTPS). Kjo u bë për të ridrejtuar kërkesat që sulmi ynë MITM po përgjonte në SSLsplit në mënyrë që të mund të dekriptojë mesazhin e marrë me një çertifikatë, ta përpunojë atë dhe ta enkriptojë dhe pastaj ta dërgojë në destinacion.

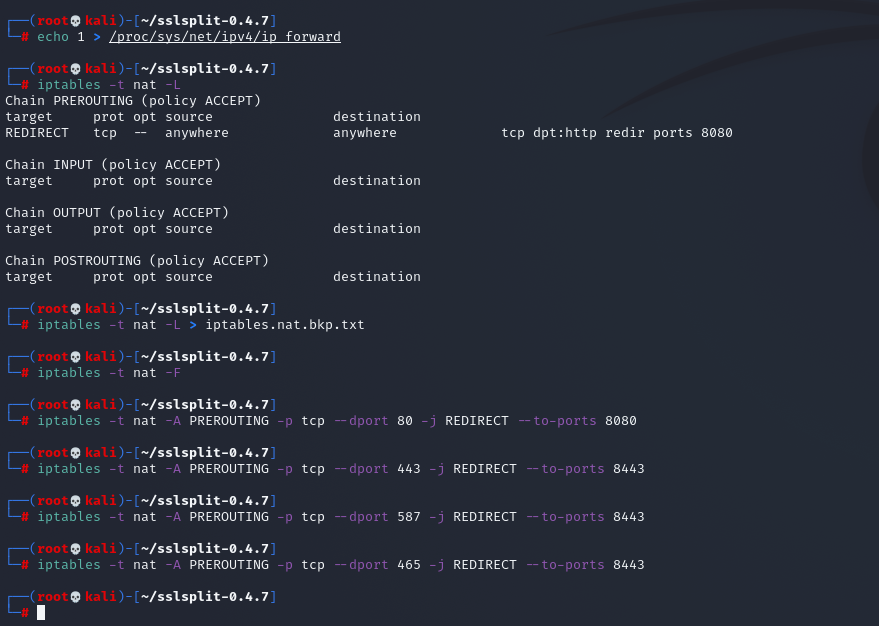


Figura 10: Aktivizimi dhe ridrejtimi i porteve

Tani, na duhet të krijojmë fajlla në të cilat SSLsplit do të ruajë regjistrat. Për ta bërë këtë, hapim një terminal dhe krijoni dy fajlla, siç tregohet:

**mkdir /tmp/sslsplit**

**mkdir /tmp/sslsplit/logdir**

Tani jemi të gatshëm për ta filluar sulmin SSLsplit:

**sslsplit -D -l connections.log -j /tmp/sslsplit -S logdir -k certaauth.key -c ca.crt ssl 0.0.0.0 8443 tcp 0.0.0.0 8080**

Kjo komandë fillon SSLsplit në modalitetin e korrigjimit (-D, ekzekutohet në plan të parë, pa dalje dhe nxjerr përpjekjet e lidhjes në skedarin e regjistrit "connections.log" (-l ..). Përmbajtja aktuale e lidhjeve shkruhet në "/tmp/sslsplit/logdir/" (-j .. dhe -S ..) - çdo rrjedhë TCP hyrëse/dalëse e secilës lidhje ruhet në një skedar të veçantë.

**-D**: Kjo është për të ekzekutuar SSLsplit në plan të parë, pa vonesa dhe me dalje të përpiktë.

**f -l connections.log**: Kjo ruan një rekord të çdo përpjekjeje lidhjeje në lidhjet.log në dosjen aktuale.

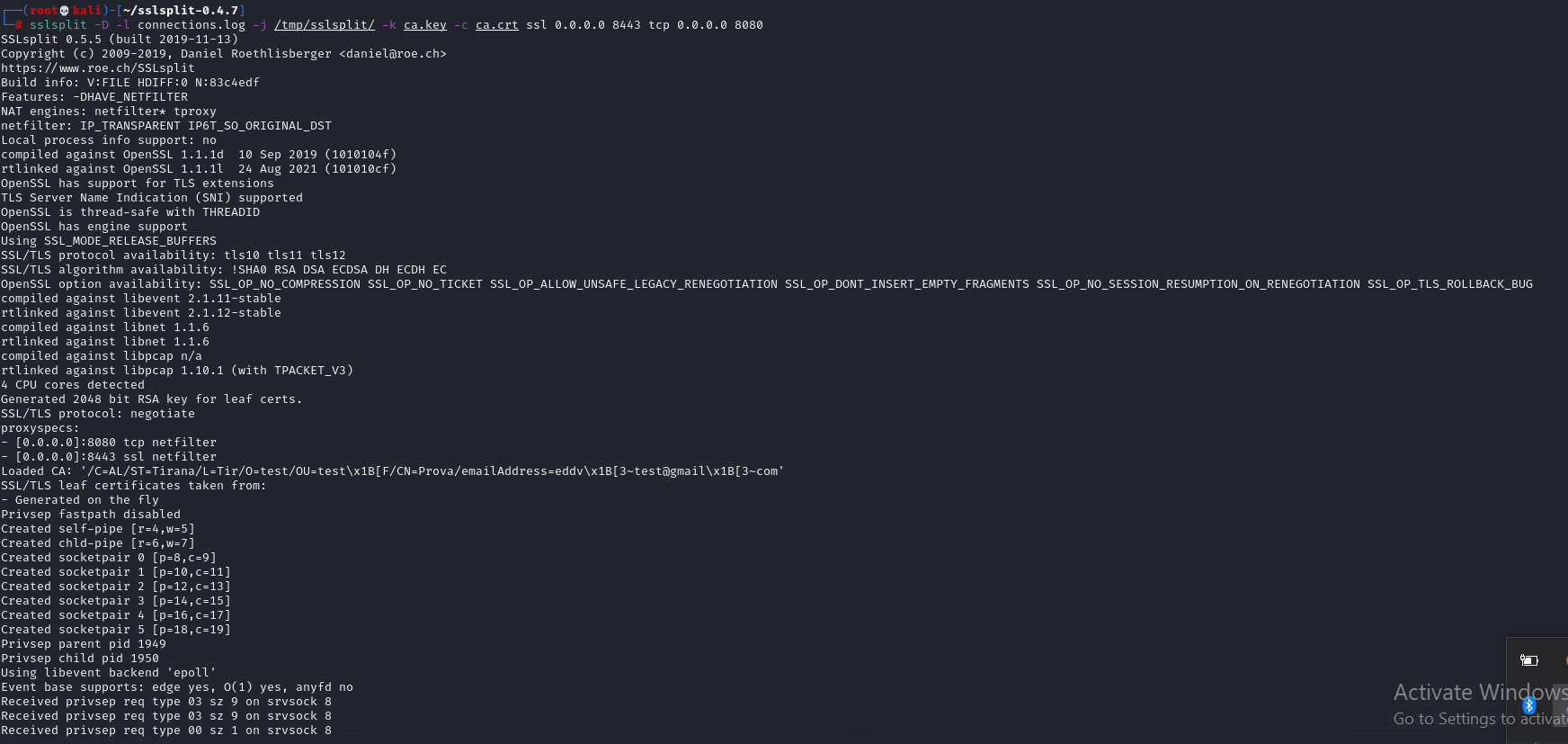
**f -j /tmp/sslsplit**: Kjo përdoret për të krijuar fajllat që do të përmbajnë mjedisin e SSLsplit si root në /tmp/sslsplit.

**f -S logdir**: Kjo përdoret për t'i thënë SSLsplit të ruajë regjistrin e përmbajtjes—të gjitha kërkesat dhe përgjigjet - në logdir (në fajllat e izoluar) duke ruajtur të dhënat në skedarë të veçantë.

**f -k dhe -c**: Kjo përdoret për të treguar çelësin privat dhe certifikatën që do të përdoret gjatë kohës ku SSL ndahet kur vepron si CA.

**ssl 0.0.0.0 8443**: Kjo i tregon SSLsplit se ku të dëgjojë për HTTPS (ose të tjera protokolle të enkriptuara), pasi ky është porti që kemi përcjellë nga 443 duke përdorur iptables në komandat e mëparshme.

**f tcp 0.0.0.0 8080**: Kjo i tregon SSLsplit ku të dëgjojë për lidhjet HTTP, ky është porti që e kemi përcjellë nga 80 duke përdorur iptables në komandat e mëparshme.

Figura 11: Fillimi i një sulmi

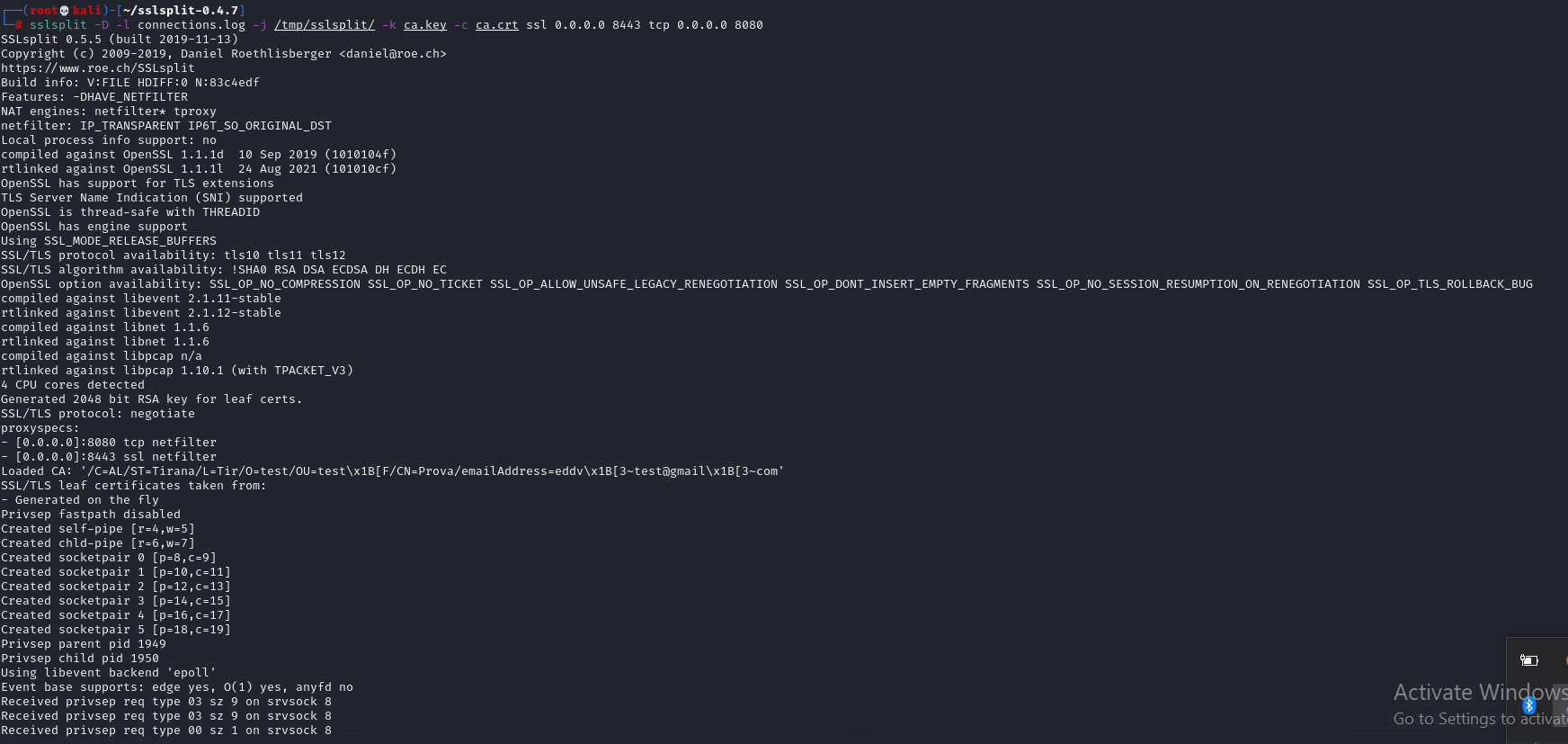


Figura 12: Ndodhja e sulmit në kohë reale

Tani që SSLsplit po funksionon dhe MITM midis viktimës dhe serverit është ekzekutuar me sukses, të gjitha informatat e ndjeshme të cilat viktima i përdor për komunikim do të na shfaqen në ekran. Shfletuesi mund të kërkojë konfirmim pasi CA dhe çertifikata jonë nuk janë zyrtarisht të njohura nga çdo shfletues uebi por nëse injorojmë çdo informatë që rrjedh do t’i shkojnë sulmuesit i cili është mes viktimës dhe serverit.

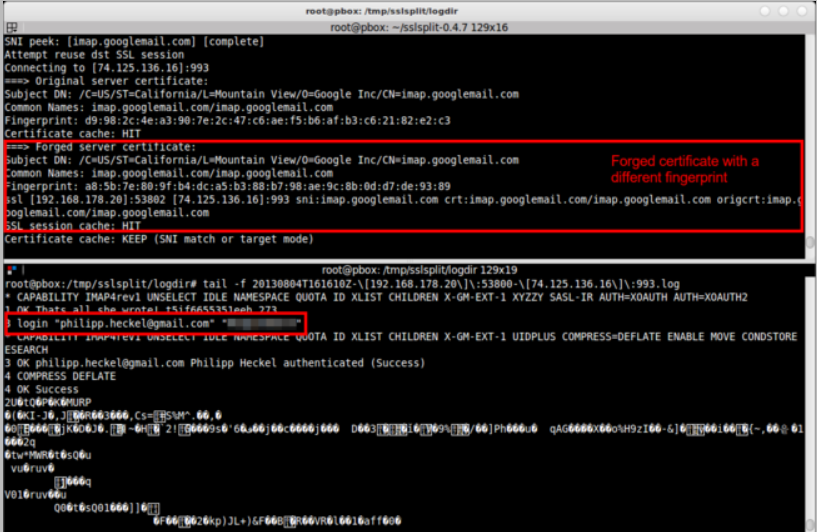


Figura 13: Rezultati i sulmit kur siguria ka qenë më e ulët në shfletues

# Konkluzioni

Në këtë projekt e treguam dhe e demonstruam veglën SSLsplit në KaliLinux. Së pari i dhamë disa koncepte bazike rreth termeve që përdoren në këtë vegël, poashtu i pamë edhe komandat të cilat i përdorim në SSLsplit, dhe në pjesën kryesore me anë të fotove e treguam hap pas hapi procesin e punës me SSLsplit. Kjo temë ka qenë mjaft sfiduese por edhe atraktive, dhe ka shumë vend për studim.

Për shkak të rritjes së sigurisë në shfletues dhe në router në ditët e sotme nuk është e mundur aq lehtë të bëhet një sulm përmes SSLsplit.

Literatura në dispozicion nuk ka qenë e mjaftueshme për sulm të sukseshëm me SSLsplit për shfletuesit me nivel të lartë sigurie.

# Referencat

[1] <https://blog.heckel.io/2013/08/04/use-sslsplit-to-transparently-sniff-tls-ssl-connections/>

[2] <https://www.roe.ch/SSLsplit>

[3] <https://pdos.csail.mit.edu/papers/ssl-splitting-usenixsecurity03/>

[4] [https://www.mankier.com/1/sslsplit#](https://www.mankier.com/1/sslsplit)

[5] <https://www.varonis.com/blog/arp-poisoning/>

[6] <https://su2.info/doc/arpspoof.php>

[7] <https://www.kali.org/tools/sslsplit/>

[8] <https://github.com/tyndyll/docker-sslsplit>

[9] [https://learning.oreilly.com/library/view/penetration-testing- bootcamp/9781787288744/92ed3bfa-bdd1-4f65-b920-1c5bc360b9c0.xhtml](https://learning.oreilly.com/library/view/penetration-testing-%20bootcamp/9781787288744/92ed3bfa-bdd1-4f65-b920-1c5bc360b9c0.xhtml)

[10] <https://blog.securityinnovation.com/blog/2011/06/how-to-test-for-man-in-the-middle-vulnerabilities.html>

Linku i librave:

[11] Gilberto Nájera-Gutiérrez - Kali Linux Web Penetration Testing Cookbook

[12] SSL and TLS: Theory and Practice, Second Edition 2nd Edition, Kindle Edition