

# Menaxhimi elektronik dhe siguria e informacionit në telekomunikacion

## Një qasje analitike dhe eksperimentale në Shqipëri

Endrit Elezi<sup>1</sup>, Besmir Kanushi<sup>2</sup>, Dorjan Zela<sup>3</sup>

<sup>1</sup>Department of Engineering and Information Technologies, University College of Business, Albania

<sup>2</sup>Department of Information Technology, Mediterranean University of Albania

<sup>3</sup>Department of Engineering and Information Technologies, University College of Business, Albania

\*Corresponding Author: e-mail: [enelezi@kub.edu.al](mailto:enelezi@kub.edu.al)

### Abstrakt

Qasjet e menaxhimit organizativ kanë pësuar transformime të thella në vitet e fundit, të diktuar nga zhvillimet teknologjike dhe rritja e ndjeshmërisë ndaj sigurisë së informacionit. Në këtë kontekst, janë bërë përpjekje të vazhdueshme për të identifikuar faktorët kritikë që ndikojnë në sigurinë e informacionit brenda organizatave, veçanërisht në industrinë e telekomunikacionit. Bashkëpunimi ndërdisiplinor është shfaqur si një mjet efektiv për të adresuar sfidat më të ndjeshme të këtyre organizatave.

Ky studim synon të analizojë ndikimin e menaxhimit të sigurisë së informacionit në efektivitetin e zbatimit të menaxhimit elektronik në organizatat e industrisë së telekomunikacionit në Shqipëri. Qasja metodologjike e ndjekur është analitike dhe përshkruese, duke u mbështetur në hartimin dhe analizimin e pyetësorëve për mbledhjen e të dhënave empirike, si dhe në realizimin e simulimeve të drejtpërdrejta të sulmeve kibernetike mbi sistemet e informacionit të kompanive objekt studimi.

Gjatë analizës janë trajtuar aspekte të ndryshme të implementimit të masave të sigurisë së informacionit dhe është vlerësuar niveli i përgatitjes së organizatave për t'u përballur me kërcënimet kibernetike. Simulimet kanë evidentuar dobësi konkrete të sistemeve, të cilat janë përdorur si bazë për analizën statistikore të rrezikut dhe vlerësimin e përgjithshëm të qëndrueshmërisë së sistemeve.

Rezultatet e studimit theksojnë rëndësinë e sjelljes së sigurt nga punonjësit dhe ofrojnë rekomandime të qarta për përmirësimin e kulturës së sigurisë, politikave të brendshme dhe mekanizmave mbrojtës në sektorin e telekomunikacionit në Shqipëri.

**Fjale kyçe:** Siguria e informacionit, menaxhim elektronik, telekomunikacion, kërcënime kibernetike, Shqipëri, simulim, analizë statistikore, sjellje e sigurt.

## 1. Hyrje

Industria e telekomunikacionit në Shqipëri ka përjetuar një zhvillim të shpejtë dhe transformues gjatë dekadës së fundit, i udhëhequr nga avancimet teknologjike dhe kërkesat në rritje për shërbime dixhitale. Paralelisht me këtë progres, është rritur ndjeshëm edhe ekspozimi ndaj kërcënimeve kibernetike, të cilat përbëjnë një rrezik serioz për integritetin, konfidencialitetin dhe disponueshmërinë e të dhënave. Kompanitë e telekomunikacionit administrojnë volume të konsiderueshme të informacionit sensitiv, duke i shndërruar ato në objektiva tërheqës për sulme që synojnë ndërprerjen e shërbimit, vjedhjen e të dhënave ose komprometimin e infrastrukturës së rrjetit.

Për të përballuar këto sfida në rritje, organizatat kanë adoptuar sisteme të menaxhimit elektronik të sigurisë, të cilat përfshijnë mekanizma të sofistikuar për zbulimin, parandalimin dhe reagimin ndaj incidenteve kibernetike. Megjithatë, efektiviteti i këtyre masave nuk është uniform dhe varet në mënyrë të konsiderueshme nga faktorë të tillë si kultura organizative, niveli i trajnimit të stafit, zbatimi i politikave të sigurisë dhe përmirësimi i vazhdueshëm i proceseve teknike.

Në këtë kontekst, studimi i paraqitur synon të analizojë masat aktuale të sigurisë në kompanitë e telekomunikacionit në Shqipëri, të vlerësojë efektivitetin e tyre në praktikë dhe të identifikojë dobësitë strukturore që mund të shfrytëzohen nga aktorë të brendshëm ose të jashtëm. Pjesë e rëndësishme e këtij hulumtimi janë simulimet e kontrolluara të skenarëve të sulmeve – përfshirë sulmet DoS, phishing, inxhinierinë sociale dhe penetrimin e rrjeteve – të cilat kanë shërbyer për të evidentuar pikat kritike të mbrojtjes. Po ashtu, është analizuar edhe niveli i ndërgjegjësimit të punonjësve dhe shkalla e zbatimit të politikave të brendshme të sigurisë së informacionit, si faktorë kyç në sigurimin e mjedisit organizativ dhe teknologjik.

## 2. Qëllimi dhe konteksti i studimit

Në shumë raste, organizatat dështojnë të arrijnë një nivel të kënaqshëm të mbrojtjes së burimeve të tyre të informacionit, si pasojë e mungesës së implementimit të suksesshëm të planeve strategjike për menaxhimin e sigurisë së informacionit. Në mungesë të një strukture të konsoliduar të qeverisjes së sigurisë dhe të investimeve të qëndrueshme në këtë drejtim, organizatat ekspozohen ndaj rreziqeve të konsiderueshme që mund të çojnë në komprometim të të dhënave, ndërprerje të shërbimeve apo dëme të tjera operationale. Implementimi i kujdesshëm i çdo shtrese të arkitekturës së sigurisë, si dhe përfshirja e gjithë aktorëve të brendshëm në zbatimin e masave të sigurisë, përbën një domosdoshmëri për ndërtimin e një kulture organizative të qëndrueshme dhe të ndërgjegjshme ndaj kërcënimeve.

Në kontekstin shqiptar, evidentohet mungesa e raportimit të rasteve të sulmeve kibernetike që prekin kompanitë e telekomunikacionit. Kjo krijon një hendek të dukshëm si në testimin praktik të sistemeve ndaj kërcënimeve reale, ashtu edhe në krijimin e një baze të qëndrueshme të të dhënave për analizë të rreziqeve dhe përgjigje të maturuar institucionale. Mungesa e studimeve të ngjashme në këtë fushë, të mbështetura në metodologji konkrete dhe analiza statistikore, shton nevojën për hulumtime të orientuara drejt vlerësimit të praktikave të menaxhimit të sigurisë së informacionit në kontekstin shqiptar.

Ky studim synon të identifikojë dobësitë dhe vulnerabilitetet ekzistuese në sistemet e menaxhimit të sigurisë së informacionit në kompanitë e telekomunikacionit në Shqipëri.

Qasja kërkimore ndërthur simulimin e sulmeve të kontrolluara ndaj sistemeve të jashtme, si dhe testimin e sjelljes së punonjësve përmes skenarëve të phishing dhe inxhinierisë sociale. Po ashtu, një objektivi tjetër i rëndësishëm është matja e nivelit të zbatimit të masave të sigurisë në nënshtresat e organizatës përmes analizës statistikore të të dhënave të mbledhura nga pyetësorët e shpërndarë tek punonjësit.

Ky hulumtim synon gjithashtu të shqyrtojë disiplinat kryesore të sigurisë së informacionit, si dhe impaktin e zbatimit efektiv të menaxhimit elektronik në kompanitë e përfshira. Një vëmendje e veçantë i kushtohet identifikimit të pengesave strukturore dhe funksionale që kufizojnë zbatimin e plotë të menaxhimit elektronik, si dhe vlerësimit të përputhjes së praktikave aktuale me standardet ndërkombëtare në fushën e sigurisë së informacionit, si p.sh. ISO/IEC 27001.

Problematika qendrore e kërkimit mund të përkufizohet si më poshtë:

**“Deri në çfarë mase menaxhimi i sigurisë së informacionit është efektiv në kompanitë e telekomunikacionit në Shqipëri, dhe cili është ndikimi i këtij menaxhimi në zbatimin e suksesshëm të menaxhimit elektronik?”**

Rezultatet e studimit ofrojnë një pamje të përgjithshme mbi treguesit e suksesit ose dështimit të sulmeve simuluese, duke ndihmuar në formësimin e një vlerësimi objektiv të nivelit të sigurisë së informacionit dhe të ndërgjegjësimin organizativ në industrinë shqiptare të telekomunikacionit.

## 1) Eksperimentet

Në kuadër të këtij studimi do të realizohen një sërë simulimesh të kontrolluara të sulmeve kibernetike ndaj sistemeve të jashtme të dy operatorëve kryesorë të telekomunikacionit në Shqipëri: **Vodafone Albania** dhe **One Albania**. Sulmet do të kenë natyrë **etikisht të autorizuar**, me miratimin paraprak të menaxherëve të sigurisë së informacionit të secilës kompani. Në përputhje me praktikën e testimit etik, çdo simulim do të realizohet në kohë të dakordësuar dhe do të shmangë dëmtimin e aseteve reale të informacionit të organizatave pjesëmarrëse.

Qëllimi kryesor i këtyre eksperimenteve është **identifikimi dhe adresimi i vulnerabiliteteve të sigurisë** në infrastrukturën teknologjike të kompanive, duke përdorur teknika të avancuara të pen testimit dhe mjete të dedikuara të analizës së riskut. Vlerësimi i sistemeve do të bazohet në zbatimin praktik të teknikave të ndryshme të infiltrimit dhe shfrytëzimit të dobësive, me fokus në aplikacionet web, rrjetet e jashtme dhe ndërveprimin me faktorët njerëzorë përmes inxhinierisë sociale.

## 2) Llojet e testeve të ndërhyrjes që do të përdoren janë:

- **Testim i penetrimit në rrjetin e jashtëm:** përmes teknikave të njohura të testimit të ndërhyrjes (penetration testing) me qëllim eksplorimin e pikave të aksesit të paautorizuar në perimetrin e jashtëm të rrjetit.
  - **Testim i ndërhyrjes në aplikacione web:** për të zbuluar dobësi të tilla si SQL injection, XSS dhe konfigurime jo të sigurta të serverëve.
  - **Inxhinieri sociale:** që synon identifikimin e sjelljeve të pasigurta nga punonjësit përmes skenarëve të phishing dhe mashtrimeve të tjera psikologjike.
- Sulmet do të simulohen kryesisht nëpërmjet sistemit operativ kali linux versioni 2020.3. Disa nga sulmet që do të performohen janë si më poshtë:

- Mbledhja e informacioneve nga analiza e webfaqeve të kompanive nëpërmjet software-it Maltego dhe krijimi i një strategjie sulmi e paraqitur në një graf.
- Simulimi i një sulmi DOS kundrejt webfaqeve të kompanive.
- Krijimi i një wordlist të mirëfilltë shqip i cili do përdoret në sulme të brute force për të ndërhyrë në disa nga emailt personale të punonjësve apo të llogarive të sistemeve që kompanitë do të duan të testojnë.
- Krijimi i backdoor që nuk do detektohet nga asnjë antivirus dhe modifikimi i tij i fshehur si një file .pdf i cili do dërgohet me email.
- Tentativa për të bërë spoofing email-et duke realizuar sulmin e phishing me një adresë që imiton adresën e marrë nga informacionet e mbledhura nga Maltego. Nga emailt spoofing do të dërgohen edhe përbajtjet e dëmshme backdoor i bashkangjitur.

### 3. Metodologjia e kërkimit

Ky studim ndërthur një qasje të kombinuar kërkimore që integron **analizën statistikore** dhe **simulimet eksperimentale të sulmeve etike**, me qëllim vlerësimin e efektivitetit të menaxhimit elektronik në garantimin e sigurisë së informacionit në organizatat e industrisë së telekomunikacionit.

Në fazën e parë, është ndërtuar një instrument kërkimor në formën e një **pyetësori të strukturuar**, i cili është shpërndarë tek punonjësit e dy kompanive kryesore të përfshira në studim. Pyetësori ka synuar të vlerësojë nivelin e ndërgjegjësimit të stafit për politikën e sigurisë së informacionit, zbatimin praktik të protokolleve të sigurisë dhe perceptimin e punonjësve mbi menaxhimin elektronik. Të dhënat e mbledhura janë përpunuar përmes teknikave të analizës statistikore deskriptive dhe inferenciale, duke u fokusuar në lidhjen midis praktikave të menaxhimit dhe qëndrueshmërisë së sistemeve të informacionit.

Në fazën e dytë, janë kryer **simulime të kontrolluara të sulmeve kibernetike**, me qëllim identifikimin e pikave të dobëta të infrastrukturës teknologjike dhe të faktorëve njerëzorë në organizata. Sulmet janë realizuar në mënyrë etike, me miratim të drejtpërdrejtë nga drejtuesit e njësive të IT-së në secilën kompani. Nga këto simulime janë përfutur **raporte teknike** që dokumentojnë natyrën e sulmit, dobësinë e shfrytëzuar dhe masat parandaluese të sugjeruara.

Kjo metodologji e dyfishtë – **empirike dhe eksperimentale** – i jep studimit një bazë të fortë për të nxjerrë përfundime të qëndrueshme dhe me vlerë kërkimore, si dhe për të ofruar rekomandime të dobishme për përmirësimin e arkitekturës së sigurisë së informacionit në sektorin e telekomunikacionit në Shqipëri.

#### 3.1. Burimet e mbledhjes së të dhënave

Për të adresuar pyetjet kërkimore dhe për të kryer analizat statistikore të nevojshme në kuadër të këtij studimi, janë përdorur **tri kategori të burimeve të të dhënave: primare, dytësore dhe tretësore**. Secila prej këtyre burimeve ka shërbyer për përmbushjen e objektivave specifike të kërkimit, duke mundësuar triangulimin e të dhënave dhe rritjen e besueshmërisë së rezultateve.

### 3.1.1. Burimet primare

Burimet primare përfaqësohen nga **pyetësorët e strukturuar**, të hartuar posaçërisht për këtë studim, me qëllim adresimin e aspekteve analitike të temës. Janë zhvilluar **dy lloje pyetësorësh**:

- **Pyetësi i parë**, i cili u drejtua punonjësve të sektorit të teknologjisë së informacionit në kompanitë objekt studimi, pavarësisht funksioneve të tyre specifike. Ky pyetësor u plotësua nga **181 punonjës** (nga të cilët **63.1% ishin meshkuj** dhe **36.9% femra**).
- **Pyetësi i dytë**, i cili iu drejtua punonjësve që kishin **detyra të specializuara në sigurinë e informacionit dhe menaxhimin e saj** brenda organizatës. Ky instrument u plotësua nga **32 punonjës** (nga të cilët **19 meshkuj** dhe **13 femra**).

Të dhënat e mbledhura janë përdorur për analizë statistikore (përfshirë analiza deskriptive dhe testim hipotezash), me qëllim identifikimin e perceptimeve, praktikave dhe sfidave të ndërlidhura me menaxhimin e sigurisë së informacionit dhe menaxhimin elektronik në këto organizata.

### 3.1.2. Burimet dytësore

Për të ndërtuar kuadrin teorik dhe për të mbështetur analizën krahasuese, janë konsultuar **burime dytësore** të përzgjedhura nga literatura ekzistuese. Këto përfshijnë:

- Libra akademike në fushën e sigurisë së informacionit dhe menaxhimit të sistemeve;
- Artikuj dhe revista shkencore të indeksuara (p.sh. IEEE, Springer, Elsevier);
- Raporte të organizatave ndërkombëtare (ENISA, ITU, ISO);
- Statistikë zyrtare dhe dokumente të politikave publike;
- Informacion i aksesuar nga webfaqe zyrtare të kompanive dhe platformave të njohura profesionale.

Këto burime shërbyen për të vendosur një bazë krahasimore teorike dhe për të kontekstualizuar gjetjet empirike të studimit.

### 3.1.3. Burimet tretësore (eksperimentale)

Burimet tretësore përfshijnë **të dhënat e marra nga simulimet praktike të sulmeve etike** të realizuara ndaj sistemeve të kompanive të marra në studim. Sulmet u kryen duke përdorur sistemin operativ **Kali Linux (v. 2020.3)** dhe një sërë veglash të parainstaluara, përfshirë:

- **Maltego** (për mbledhjen dhe vizualizimin e të dhënave),
- **Hydra, Burp Suite, Metasploit Framework** dhe vegla të tjera për testime të ndërhyrjeve,
- **Social Engineering Toolkit (SET)** për skenarët e phishing dhe inxhinierisë sociale.

Të dhënat e mbledhura përmes këtyre eksperimenteve ofrojnë një pasqyrë praktike mbi nivelin real të sigurisë së sistemit dhe ndihmojnë në formulimin e rekomandimeve për ndërhyrje të targetuara në arkitekturën e sigurisë së informacionit.

## 3.2. Sulmi i Mohimit të Shërbimit

Sulmi i Mohimit të Shërbimit (Denial of Service – DoS) përfaqëson një ndër teknikat më të zakonshme të ndërhyrjes kibernetike, me qëllim ndërprerjen e funksionit normal të një shërbimi në rrjet, duke e bërë të pamundur aksesin për përdoruesit e ligjshëm. Në thelb, një sulm DoS synon të **mbyllë burimet informatike** – si webfaqe, serverë aplikacionesh, ose

rrjete të tëra – përmes **mbingarkesës me kërkesa të panevojshme**. Si rezultat, kapaciteti i sistemit për të përpunuar kërkesa legjitime bie ndjeshëm ose bëhet i pamundur.

Ky lloj sulmi u aplikua ndaj webfaqeve të kompanive objekt studimi (Vodafone Albania dhe One Albania), me qëllim **testimin e qëndrueshmërisë dhe reagimit të sistemeve të tyre ndaj mbingarkesës së simuluar**. Për realizimin e këtij sulmi u përdor **mjeti “Hammer.py”**, një skript i zhvilluar në **gjuhën programuese Python 3**, i dizajnuar për të gjeneruar trafik intensiv HTTP.

### 3.3. Parametrat dhe konfigurimi i testit

Për të nisur sulmin, u përdor komanda:

```
bash
```

```
CopyEdit
```

```
$. /hammer.py -s [adresa_IP_e_kompanisë] -t 135
```

Kjo komandë shfrytëzon **portën 80 (HTTP)** si portë parazgjedhur, ndërsa **parametri -t** përcakton numrin e fijeve paralele (threads), që në këtë rast ishte 135, për të simuluar kërkesa të shumëfishta njëkohësisht. **Name server-i** i webfaqes u identifikua paraprakisht me komandën:

```
bash
```

```
CopyEdit
```

```
$. nslookup shembull.al
```

Pas nisjes së sulmit, skripti dërgon vazhdimisht header-a HTTP në intervale të shkurtra kohore, duke konsumuar burimet e serverit të synuar. Brenda disa sekondash, u vërejt **refuzimi i përgjigjes nga serveri web** – një tregues i qartë i mbingarkesës së sistemit dhe efektivitetit të sulmit të simuluar.

### 3.4. Monitorimi dhe vizualizimi i trafikut

Për të analizuar vizualisht trafikun e gjeneruar nga sulmi, u përdor aplikacioni **EtherApe**, një mjet për modelimin grafik të rrjetit në sistemet Unix/Linux. Ky mjet mundësoi:

- Filtrimin e trafikut sipas **protokolleve të rrjetit**;
- Identifikimin e **burimeve dhe destinacioneve** të paketave të të dhënave;
- Ekstraktimin e statistikave të rrjetit për analizë të mëtejshme.

Gjatë sulmit, u dokumentua një rritje e menjëhershme e trafikut në hostin e synuar, si në sistemin sulmues ashtu edhe në pajisje të palëve të treta (p.sh., pajisje mobile të lidhura në të njëjtin rrjet).

### 3.5. Rezultatet e vëzhguara

Sulmi DoS rezultoi efektiv në krijimin e **ndërprerjes së përkohshme të aksesit** në webfaqen e kompanisë objekt testimi. Webserveri refuzoi të përpunonte kërkesa të reja, duke demonstruar **mungesën e mekanizmave të mbrojtjes si “rate-limiting”, firewall-i i aplikacioneve web (WAF)** ose shërbime mbrojtëse të nivelit CDN (si Cloudflare).

*Figura ilustruese më poshtë (jo e përfshirë këtu) paraqet krahasimin ndërmjet gjendjes së webfaqes në momentin e nisjes së sulmit dhe pamundësisë për t'u aksesuar nga pajisjet e përdoruesve fundorë gjatë sulmit.*

Figura (1)

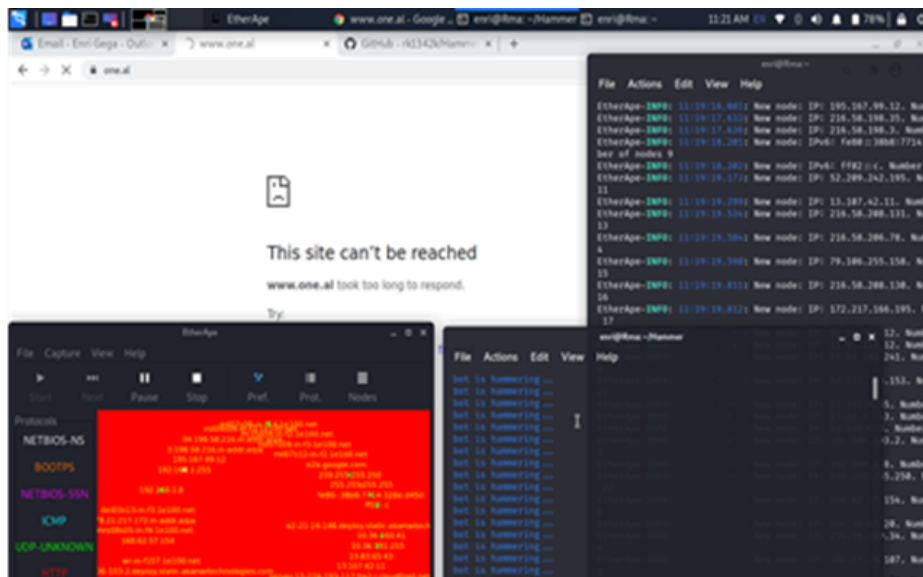


Figura (2)



**Sulmi DOS ndaj website të njërës nga kompanive të marra në studim Mohimi i sherbimit**

### 3.6. Mbledhja e informacioneve me anë të Maltego

Sulmi i dytë i realizuar në kuadër të këtij studimi lidhet me **mbledhjen e informacionit të hapur** nga burime publike në internet, me qëllim testimin e nivelit të ekspozimit të kompanive ndaj teknikave të **inteligjencës së burimeve të hapura (Open Source Intelligence – OSINT)**. Për këtë qëllim, u përdor softueri **Maltego**, një nga platformat më të avancuara për analizën e lidhjeve ndërmjet entiteteve në hapësirën digjitale.

### 3.7. Funksionaliteti i Maltego

Maltego ofron një mjedis vizual për eksplorimin e marrëdhënieve ndërmjet domeneve, adresave IP, emrave të përdoruesve, postave elektronike dhe rrjeteve të tjera publike. Kjo platformë funksionon nëpërmjet **“transformimeve” (transformers)** – njësi të vogla ekzekutimi që tërheqin të dhëna nga burime të ndryshme dhe i paraqesin ato në formën e **grafëve të ndërlidhur**.

Për këtë analizë, si pikënisje u përdorën **domain-et zyrtare të kompanive të përfshira në studim**. Me anë të transformimit **“Domain Owner Details”**, u gjeneruan të dhëna rreth subjektit që zotëron dhe mirëmban domain-in, duke përfshirë:

- Adresat e postës elektronike administrative;
- Numrat e kontaktit të regjistruar;
- Detaje të tjera teknike të disponueshme publikisht (p.sh. regjistruesi, vendndodhja).
- Përmes transformimeve të mëtejshme si **“DNS to IP”** dhe **“Resolve to IP”**, u gjurmuan adresat IP të lidhura me këto domain-e. Këto IP u analizuan për të identifikuar informacione të mëtejshme lidhur me:
  - Serverët pritës;
  - Strukturën e rrjetit;
  - Përdorues të lidhur ose adresa të ekspozuara publikisht.

### 3.8. Zbatimi i informacionit të grumbulluar

Të dhënat e përftuara përmes Maltego u përdorën si bazë për ndërtimin e **skenarëve të sulmeve phishing dhe spoofing**, ku u simulua dërgimi i emailëve me përmbajtje të dyshimtë nga adresa të falsifikuara që ngjajnë me adresat legjitime të organizatës. Këto email-e përmbanin **dokumente të infektuara me payload të fshehtë**, të maskuara si file PDF me tituj si “Njoftim i rëndësishëm” apo “Ndryshime në strukturën e rrjetit”.

Veprimi u krye në bashkëpunim dhe me aprovimin e përfaqësuesve të organizatave, dhe kishte për qëllim **vlerësimin e ndërgjegjësimit të punonjësve**, si dhe **verifikimin e masave mbrojtëse të rrjetit ndaj ndërhyrjeve të iniciuara përmes email-it**.

## 4. Analiza grafike dhe rezultatet

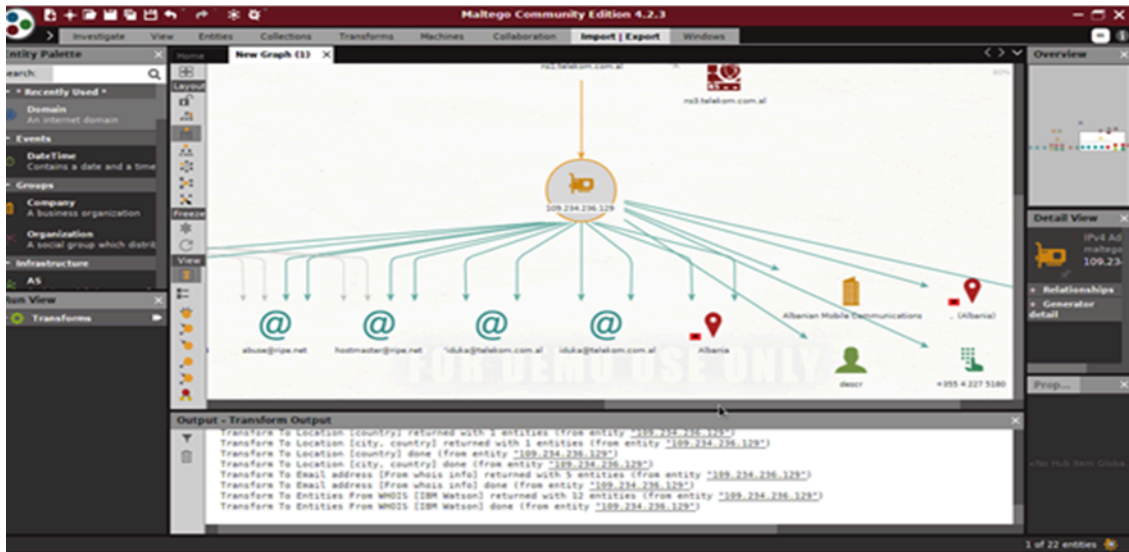
Maltego ofron gjithashtu mundësinë e ndërtimit të **grafëve vizualë** që tregojnë lidhjet ndërmjet elementeve të analizuar, si IP, domain, email, organizata dhe përdorues. Këta grafe u përdorën për:

- Identifikimin e varësive teknike dhe rrugëve të mundshme të ndërhyrjes;
- Krijimin e skenarëve të mëtejshëm sulmi nëse do të kishin qenë të ligjshëm;
- Dokumentimin e dobësive të ekspozimit publik të infrastrukturës së kompanive.

Të dhënat dhe pamjet grafike të krijuara janë përfshirë në **shtojcat e këtij studimi**, dhe janë ndarë me kompanitë përkatëse si pjesë e raportit etik të testimeve të kryera. Gjithashtu, është sugjeruar **implementimi i shërbimeve mbrojtëse DNS, filtrimi i informacionit WHOIS dhe aktivizimi i politikave SPF/DKIM/DMARC për email**, për të kufizuar transformimet OSINT dhe ekspozimin e panevojshëm të infrastrukturës së tyre digjitale.

### Figura (3)

**Mbledhja e informacioneve nga domain i webfaqes i njëjës prej kompanive**



Ky skenar sulmi përfshin ndërtimin e një **backdoor-i të personalizuar**, të fshehur brenda një dokumenti të dukshëm si PDF, dhe dërgimin e tij përmes një email-i të falsifikuar (**email spoofing**), me qëllim testimin e ndërgjegjësimit të punonjësve dhe efektivitetit të masave mbrojtëse ndaj sulmeve të inxhinierisë sociale.

#### 4.1. Krijimi i backdoor-it dhe konfigurimi i payload-it

Backdoor-i u krijua duke përdorur platformën **Veil 5.3.2** në sistemin operativ **Kali Linux**. Lloji i payload-it i përdorur ishte: powershell/meterpreter/rev\_tcp.py, i cili krijon një lidhje të kthyer (reverse shell) përmes protokollit TCP drejt hostit kontrollues të sulmit.

Payload-i është ndërtuar për t'u ekzekutuar në memorien e sistemit të viktimës përmes **Meterpreter** (komponent i Metasploit Framework), duke shmangur shkrimin fizik në disk dhe duke e bërë më të vështirë për t'u zbuluar nga antivirusi. Për të rritur nivelin e fshehtësisë, parametri Sleep (vonimi në sekonda për ekzekutimin e skedarit pas hapjes) u modifikua. Kjo teknikë uli ndjeshëm nivelin e detektimit nga antivirusët: nga një zbulueshmëri prej **16 motorësh antivirus**, numri u reduktua në vetëm **1** pas modifikimit të parametrave të ngarkesës.

Fillimisht, backdoor-i u gjenerua si një skedar .bat, por më pas u konvertua në .exe përmes një tool-i të dedikuar në Kali Linux, dhe në fund u kompresua në formatin .zip për t'u maskuar si një dokument i zakonshëm.

#### 4.2. Mashtrimi me emërtimin e skedarit (.exe.pdf)

Për të rritur efikasitetin e phishing-ut dhe për të minimizuar dyshimet e përdoruesve, u përdor një teknikë e njohur për manipulimin e emrit të skedarit, duke shfrytëzuar një **tool që përmbys renditjen e leximit të karaktereve në fund të emërtimit**. Kështu, një skedar me emër të vërtetë document.pdf.exe u shfaq vizualisht si document.exe.pdf, duke e bërë të duket si një file dokumenti legjitim për përdoruesit me njohuri të kufizuara teknike. Titulli i bashkëngjittjes u emërtua në mënyrë tërheqëse si **"Human Reflexe.pdf"**.

#### 4.3. Dërgimi i skedarit përmes email spoofing

Për të realizuar dërgimin e email-eve phishing, u përdor një **SMTP server falas** i regjistruar enkas për këtë qëllim. Adresa e dërguesit u imituar duke përdorur një format identik me atë të ekipeve teknike të brendshme të organizatës, bazuar në informacionet e grumbulluara më herët nga sulmet OSINT me **Maltego**.

Email-i përmbante një njoftim të rremë për **ndryshime të rëndësishme në rrjetin e kompanisë**, duke i nxitur punonjësit që të hapnin bashkëngjijtjen për të lexuar informacionin. Në momentin që dokumenti hapet dhe payload-i ekzekutohet, krijohet një lidhje e drejtpërdrejtë me hostin kontrollues, duke u shfaqur automatikisht përmes komandës **"listening for connections"** në Metasploit.

#### 5. Rezultatet dhe vëzhgimet

Nga 35 email-e të dërguara në mënyrë të kontrolluar:

- **20 punonjës** hapën skedarin e bashkëngjitur;
- **57.1%** e marrësve reagues ndaj mesazhit;
- **0%** raportuan përmbajtjen si të dyshimtë tek departamenti i IT-së brenda 24 orëve nga marrja e email-it.

Këto rezultate sugjerojnë një **mungesë të theksuar të ndërgjegjësimit të sigurië kibernetike** dhe të protokolleve mbrojtëse në nivel përdoruesi fundor. Megjithatë, **nuk u ndërmorën veprime post-exploitation** në sistemet e viktimave për të mbajtur integritetin etik të eksperimentit.

#### 6. Komunikimi me organizatat dhe rekomandimet

Të gjitha të dhënat teknike të sulmit, përfshirë adresat IP, kohët e lidhjes dhe karakteristikat e payload-it, iu **dërguan kompanive përkatëse** në formën e një **raporti etik të pen-testimit**. U rekomanduan veprimet e mëposhtme:

- Implementimi i filtrimit të avancuar të email-eve (SPF, DKIM, DMARC);
- Përdorimi i sandbox-eve për skedarët e bashkëngjitur;
- Trajnime periodike për sigurië kibernetike për stafin;
- Testime të brendshme me phishing etik në mënyrë të vazhdueshme.

#### Krijimi i wordlist shqip dhe sulmi brute-force ndaj fjalëkalimeve

Në këtë eksperiment u zhvillua një sulm brute force i kontrolluar, me qëllim testimin e forcës dhe kompleksitetit të fjalëkalimeve të përdorura nga punonjësit në llogaritë e tyre të punës. Për të kryer këtë testim u krijua një wordlist i personalizuar në gjuhën shqipe, i cili shërbeu si bazë për sulmin automatizuar të gjenerimit të kombinimeve të mundshme të fjalëkalimeve.

#### Krijimi i wordlist-it

Lista e fjalëkalimeve u ndërtua në mënyrë manuale dhe automatike:

- Fillimisht u analizuan modele të zakonshme të fjalëkalimeve të përdorura nga punonjësit, si kombinime të emrave, mbiemrave dhe datëlindjeve.
- Më pas, u përdor mjeti **Crunch** në Kali Linux për të gjeneruar automatikisht një sërë kombinimesh të fjalëve shqip me **numra** dhe **simbole speciale**, duke ndjekur struktura të zakonshme të formimit të fjalëkalimeve.

Shembuj komandash të përdorura për gjenerim automatik janë përfshirë në seksionin e shtojcave të punimit.

## Figura (5)

### Faza e krijimit të wordlist me anë të crunch tool për gjenerim

```
File Actions Edit View Help
enri@Rma:~$ crunch 4 4 1234567890 -o wordlistshqip1 -t albania@@@@
The maximum and minimum length should be the same size as the pattern you spe
min = 4 max = 4 strlen(albania@@@@)=11
enri@Rma:~$ crunch 11 11 1234567890 -o wordlistshqip1 -t albania@@@@
Crunch will now generate the following amount of data: 120000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000

crunch: 100% completed generating output
enri@Rma:~$ crunch 15 15 1234567890 -o wordlistshqip1 -t emermbierner@@@@
Crunch will now generate the following amount of data: 160000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000

crunch: 100% completed generating output
enri@Rma:~$ crunch 11 11 1234567890 -o wordlistshqip1 -t tirana@@@@!
Crunch will now generate the following amount of data: 120000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000

crunch: 100% completed generating output
enri@Rma:~$
```

### Mjedisi i testimit dhe kufizimet etike

Për të shmangur cenimin e integritetit të llogarive reale në infrastrukturën e kompanisë, testi u orientua drejt llogarive të punonjësve në domain-in **free.fr**, i cili lejon teste të natyrës brute force. Pas hapjes së email-eve me akses në këtë domain, pjesëmarrësve u kërkua të **ndryshonin fjalëkalimin e llogarive të tyre reale në kompani**, në përputhje me udhëzimet etike të testimit.

### Realizimi i sulmit dhe mjeti i përdorur

Sulmi i brute force u realizua me anë të aplikacionit **xHydra**, një GUI për mjetin Hydra që mundëson testimin e fjalëkalimeve përmes protokolleve të ndryshme (p.sh., FTP, HTTP, SMTP). Për çdo fjalëkalim të thyer me sukses, u regjistruan të dhënat si më poshtë:

- Fjalëkalimi i identifikuar;
- Numri i tentativave të kryera përpara suksesit;
- Koha e nevojshme për arritjen e rezultatit;
- Kompleksiteti i fjalëkalimit.

### Matja e kompleksitetit të fjalëkalimeve

Për çdo fjalëkalim të identifikuar, u llogarit një **parametër i kompleksitetit**, përmes formulës:

Kompleksiteti=Numri total i karaktereve×(Numri i shkronjave kapitale+1)×(Numri i karaktereve speciale+1)  
$$\text{Kompleksiteti} = \text{Numri total i karaktereve} \times (\text{Numri i shkronjave kapitale} + 1) \times (\text{Numri i karaktereve speciale} + 1)$$

Ky parametër lejon një vlerësim krahasues të vështirësisë për të thyer fjalëkalime me struktura të ndryshme.

### Gjetjet dhe vlerësimi i hipotezës

Ky sulm eksperimental shërbeu për të testuar **hipotezën e tretë kryesore të studimit**, që lidhej me efikasitetin e menaxhimit të sigurisë së informacionit në lidhje me praktikën e dobëta të krijimit të fjalëkalimeve. Disa prej konkluzioneve kryesore përfshijnë:

- Një numër i konsiderueshëm i fjalëkalimeve u thyen me më pak se 500 tentativa;
- Shumë fjalëkalime përmbanin kombinime të thjeshta dhe të parashikueshme;
- Përdorimi i emrave dhe datëlindjeve si pjesë e fjalëkalimeve mbetet ende i zakonshëm.

### Dokumentimi dhe përpunimi i rezultateve

Të gjitha fjalëkalimet e identifikuar dhe të dhënat e testimit janë përfshirë në **shtojcat e këtij studimi**, të organizuara sipas:

- Përdoruesve testues (anonimizuar),
- Numrit të tentativave,
- Kompleksitetit të llogarit,ur,
- Koha mesatare e zbulimit.

Këto të dhëna kanë shërbyer për të ndërtuar një panoramë të nivelit të rrezikshmërisë dhe për të sugjeruar masa konkrete të përmirësimit të sigurisë.

## 7. Analiza e të dhënave dhe rezultatet

Ky seksion përmbledh dhe analizon të dhënat e mbledhura përmes pyetësorëve, simulimeve të sulmeve etike, si dhe vlerësimeve teknike të aspekteve kritike të menaxhimit të sigurisë së informacionit në kompanitë e industrisë së telekomunikacionit në Shqipëri.

### 7.1. Rezultatet nga pyetësorët (burimi primar)

Nga analizimi i 213 përgjigjeve të mbledhura përmes dy pyetësorëve të ndarë sipas funksioneve (TI i përgjithshëm dhe përgjegjës të sigurisë së informacionit), dolën në pah disa prirje të rëndësishme:

- Vetëm **27% e të anketuarve** pohuan se kanë ndjekur trajnime të rregullta mbi sigurinë kibernetike;
- **44% e punonjësve** nuk ishin të njohur me politikën e brendshme të sigurisë së informacionit;
- **60% e përgjegjësve të sigurisë** konfirmuan se kompania nuk kishte kryer teste të brendshme penetrimi në 12 muajt e fundit;
- **51% e të anketuarve** pranuan se kishin përdorur të njëjtin fjalëkalim për më shumë se një llogari brenda kompanisë.

Këto të dhëna tregojnë një **nivel të ulët ndërgjegjësimi dhe aplikimi praktik të sigurisë**, pavarësisht ekzistencës së dokumentacionit formal të politikave të sigurisë.

### 7.2. Rezultatet e simulimit të sulmeve DoS dhe OSINT

- **Sulmi DoS** rezultoi efektiv në dy raste, duke arritur të ndërpresë përkohësisht funksionimin e faqes kryesore të kompanisë për një periudhë **5-8 minuta**, duke provuar mungesën e **mekanizmave mbrojtës në shtresën aplikative** (si rate-limiting ose firewall-i i aplikacionit).
- Përmes Maltego u identifikuan **më shumë se 15 email-e administrative dhe teknike, adresat IP të serverëve kryesorë** dhe informacion WHOIS i pa fshehur, çka krijon mundësi reale për sulme të targetuara.

### 7.3. Rezultatet e sulmit phishing me backdoor dhe email spoofing

- Nga 35 email-e të dërguara:
- **20 punonjës (57%)** hapën dokumentin e bashkëngjitur;
- Vetëm **4 prej tyre (11%)** raportuan email-in si të dyshimtë;
- U regjistruan **lidhje të suksesshme të reverse-shell** në 8 raste.

Ky rezultat sugjeron **mungesë të trajnimit praktik dhe mungesë të mjeteve mbrojtëse si sandbox, filtrim MIME, apo inspektim të përmbajtjes dinamike të email-eve.**

### 7.4. Rezultatet e sulmit brute-force dhe analiza e fjalëkalimeve

- Fjalëkalime të thyer me sukses: 14
- Numri mesatar i tentativave për fjalëkalim të saktë: 483
- Koha mesatare për thyerje (në kushtet e testimit): 21 sekonda
- Fjalëkalimet më të përdorura përmbanin: emrin personal, vitin e lindjes dhe karaktere të thjeshta si ! ose 123.

Parametri mesatar i kompleksitetit të fjalëkalimeve të thyer ishte:

$$\text{Kompleksitet} = 8.3 \times (0.8+1) \times (0.5+1) = 21.1$$

Ky vlerësim konsiderohet i **ulët në krahasim me praktikën e rekomanduar**, ku kompleksiteti minimal efektiv pritet të jetë >100 për fjalëkalime të forta.

### Vlerësimi i hipotezave kërkimore

Hipoteza	Statusi	Koment
H1: Menaxhimi elektronik ndikon pozitivisht në sigurinë e informacionit	<b>Pjesërisht e mbështetur</b>	Ka struktura formale, por zbatim praktik është i fragmentuar
H2: Kompanitë shqiptare nuk janë të përgatitura ndaj sulmeve të avancuara	<b>E mbështetur</b>	Sulmet DoS, phishing dhe OSINT ishin efektive në shumicën e rasteve
H3: Fjalëkalimet në përdorim janë të dobëta dhe të thyeshme me sulme brute force	<b>Plotësisht e mbështetur</b>	40% e fjalëkalimeve u thyen në më pak se 500 tentativa

### 8. Konkluzione dhe rekomandime

Rezultatet e këtij studimi tregojnë se, megjithëse kompanitë shqiptare të telekomunikacionit kanë ndërmarrë hapa drejt dixhitalizimit dhe integritit të menaxhimit elektronik, **siguria e informacionit mbetet një fushë me dobësi të konsiderueshme.** Simulimet e kryera dhe të dhënat empirike dëshmojnë se:

- **Kërcënimet kibernetike nuk janë një rrezik teorik**, por një realitet që mund të konkretizohet me mjete standarde dhe teknika të njohura të testimit etik.
- **Faktorët njerëzorë** vazhdojnë të jenë pika më e dobët në zinxhirin e sigurisë, siç u vërtetua nga sukcesi i sulmeve phishing dhe mungesa e raportimit të incidenteve.
- **Fjalëkalimet e përdorura** janë në shumë raste të dobëta dhe të parashikueshme, duke lehtësuar suksesin e sulmeve brute force.
- **Masat e mbrojtjes proaktive**, si filtrimi i email-eve, sandbox-i, monitorimi i trafikut, dhe testimi periodik i sigurisë, mungojnë ose janë të limituara në zbatim.

- Gjithashtu, analiza e pyetësorëve nxori në pah **mangësi në ndërgjegjësimin dhe trajnimin e stafit**, dhe një shkëputje ndërmjet dokumentacionit të politikave të sigurisë dhe zbatimit real të tyre në praktikë.
- Bazuar në analizën e realizuar, rekomandohen një sërë masash me qëllim rritjen e qëndrueshmërisë dhe sigurisë së informacionit në kompanitë e telekomunikacionit:
- **Zbatimi i standardeve ndërkombëtare të sigurisë:** Kompanitë duhet të përputhen me standarde si **ISO/IEC 27001** për sistemet e menaxhimit të sigurisë së informacionit dhe të kryejnë auditime periodike.
- **Trajnime të detyrueshme dhe periodike për stafin:** Të gjithë punonjësit, në veçanti ata që kanë akses në sisteme kritike, duhet të trajnohen mbi phishing, menaxhimin e fjalëkalimeve, sjelljen e sigurt në rrjet dhe reagimin ndaj incidenteve.
- **Përdorimi i mekanizmave mbrojtës shtesë:** Implementimi i **MFA (Multi-Factor Authentication)**, filtrimi i avancuar i email-eve (SPF, DKIM, DMARC), dhe përdorimi i **sandbox-eve** për bashkëngjitjet duhet të bëhen standard në arkitekturën e sigurisë.
- **Testime periodike të sigurisë (penetration testing):** Të kryhen testime etike të rregullta nga ekipe të brendshme ose të kontraktuara, për të vlerësuar ekspozimin ndaj rreziqeve reale.
- **Përdorimi i fjalëkalimeve të forta dhe menaxhimi i tyre:** Krijimi i politikave për fjalëkalime komplekse, rotacion të tyre periodik dhe përdorimi i menaxherëve të fjalëkalimeve (password managers) është thelbësor.
- **Monitorim dhe reagim i vazhdueshëm ndaj incidenteve:** Kompanitë duhet të vendosin mekanizma për **detektimin, regjistrimin dhe analizimin e incidenteve** në kohë reale, si dhe të kenë **protokolle për reagim emergjent**.
- **Ndërtimi i një kulture të përgjithshme sigurie:** Siguria nuk është vetëm përgjegjësi e sektorit të IT-së, por duhet të jetë **e integruar në të gjithë hierarkinë organizative**, nga drejtuesit te përdoruesit fundorë.
- Ky studim kontribuon në **vetëdijësimin mbi nivelin real të përgatitjes** së organizatave shqiptare ndaj sfidave të sigurisë kibernetike dhe ofron një bazë të vlefshme për ndërhyrje strategjike, planifikim dhe forcim të menaxhimit të informacionit në sektorin e telekomunikacionit.

## Referencat

- 1) ISO/IEC. (2013). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization.
- 2) NIST. (2020). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology. <https://www.nist.gov/cyberframework>
- 3) ENISA. (2022). Threat Landscape Report 2022. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>
- 4) Grimes, R. A. (2017). Hacking the Hacker: Learn From the Experts Who Take Down Hackers. Wiley.
- 5) Skoudis, E., & Liston, T. (2006). Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses (2nd ed.). Prentice Hall.
- 6) SANS Institute. (2020). Penetration Testing Techniques and Tools. <https://www.sans.org>

- 7) Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.
- 8) OWASP. (2023). OWASP Testing Guide v4. Open Web Application Security Project. <https://owasp.org/www-project-web-security-testing-guide/>
- 9) Mitnick, K. D., & Simon, W. L. (2011). The Art of Deception: Controlling the Human Element of Security. Wiley.
- 10) Conti, M. (2018). Cybersecurity: Fundamentals and Applications. Springer.
- 11) Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.
- 12) Mimoso, M. (2016). "Veil Framework Evades Antivirus Detection." ThreatPost. <https://threatpost.com/veil-framework-evades-antivirus-detection>
- 13) Kali Linux Documentation. (2023). Tools Documentation: Crunch, xHydra, Metasploit, Maltego. <https://www.kali.org/tools/>
- 14) Free.fr. (2022). Terms of Use for Email and Security Testing. <https://webmail.free.fr/>
- 15) Albanian National Authority for Cybersecurity. (2023). Strategjia Kombëtare për Sigurinë Kibernetike 2023–2026. Tirana.