Зборник радова Факултета техничких наука, Нови Сад

UDK: 004.633
DOI: https://doi.org/10.24867/28BE19Stojakovic

ФОРЕНЗИКА РАЧУНАРСКИХ МРЕЖА

NETWORK FORENSICS

Јелена Стојаковић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИЧКО И РАЧУНАРСКО ИНЖЕЊЕРСТВО

Кратак садржај – *Рад представља истраживање у једној од подобласти дигиталне форензике – форензици рачунарских мрежа. Циљ рада је преглед и анализа методологија и алата који се користе у процесу форензике рачунарских мрежа. Сходно рапидном напретку технологије, рачунарске мреже су погодно тло за различите видове злоупотреба. У циљу приказивања потенцијалног случаја у оквиру форензике рачунарских мрежа, спроведена је студија случаја кроз све фазе које су неопходне за доношење конкретног закључка.*

Кључне речи: *дигитална форензика, рачунарске мреже*

Abstract – *This work presents research in one of the subfields of digital forensics – computer network forensics. The aim of the work is to review and analyze the methodologies and tools used in the forensics process of computer networks. Due to the rapid advancement of technology, computer networks are a fertile ground for various types of abuse. In order to present a potential case within the forensics of computer networks, a case study was conducted through all the stages that are necessary to reach a concrete conclusion.*

Keywords: *digital forensics, computer networks*

1. УВОД

Дигитална форензика је грана форензичке науке која се фокусира на идентификацију, прикупљање, обраду, анализу и извештавање о потенцијалним доказима који су представљени у дигиталном облику. Неопходно је да све спроведене активности користе добре форензичке технике како би се осигурало да су докази прихватљиви на суду [1].

Мрежна форензика је подобласт дигиталне форензике која се бави праћењем и анализом саобраћаја рачунарске мреже у сврху прикупљања информација, форензичких доказа или откривања упада. За разлику од неких других области дигиталне форензике, предмет мрежне форензике су обично ефемерне информације [2].

1.1. Рачунарске мреже

Рачунарска мрежа представља систем који се састоји од активних и пасивних елемената. Активни елементи су мрежни и крајњи уређаји, док пасивне елементе представљају различите врсте каблова нпр. UTP или оптички каблови чија је сврха преношење података између рачунара. Дакле, рачунарске мреже омогућавају међусобно комуницирање више уређаја, те представљају комуникациони систем.

НАПОМЕНА:
Овај рад проистекао је из мастер рада чији ментор је био др Стеван Гостојић, ред. проф.

1.2 Врсте рачунарских мрежа

Рачунарске мреже се могу делити према више различитих критеријума. Једна од њих по подручју распростирања. По тој особини мреже се деле на:

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Internet

По типу комуникационог медијума мреже се деле на:

- Жичне
- Бежичне

По распореду уређаја и веза у мрежи, мреже се деле на:

- Потпуно повезану мрежу
- Магистралу
- Звезду
- Прстен

1.3 OSI модел

OSI модел (енг. Open Systems Interconnection Model) је модел који се користи за описивање функција мрежног система. Он као такав карактерише рачунарске функције у универзални скуп правила и захтева како би подржао интероперабилност између различитих производа и софтвера [3].

Према овом моделу комуникација између рачунара се дели на седам слојева апстракције:

- Физички слој
- Слој везе
- Мрежни слој
- Транспортни слој
- Слој сесије
- Презентациони слој
- Апликациони слој

Сваки ниво OSI модела обавља одређени посао и комуницира са слојевима изнад и испод себе. Конкретне технологије и комуникациони протоколи могу да одговарају једном или више OSI нивоа. OSI модел пре свега може да помогне приликом изолације извора проблема.

Физички ниво је први и најнижи ниво OSI модела**,** бави се преносом сирових података преко мреже од физичког слоја уређаја за слање до физичког слоја уређаја за пријем.

У **слоју везе**, односно другом слоју OSI модела постоје директно повезани чворови који се користе за

обављање преноса података од чвора до чвора где се подаци пакују у такозване оквире (енг. frame).
Мрежни слој је одговоран за олакшавање преноса података између две мреже.
Транспортни слој је задужен за контролу протока и контролу грешака.
Слој сесије је одговоран за отварање и затварање комуникације између два уређаја.
Слој презентације је задужен за припрему података тако да их може користити слој апликације.
У **слоју апликације** дешава се директна комуникација са подацима корисника.

Hyper-Text Transfer Protocol (HTTP) је комуникациони протокол петог, шестог и седмог нивоа OSI модела осмишљен и дизајниран тако да преноси информације између умрежених уређаја.
Улога HTTP је комуникација између клијента и сервера. Типичан ток путем HTTP-а укључује клијентску машину која шаље захтев серверу који потом шаље одговор.
У оквиру HTTP протокола постоје HTTP захтев и HTTP одговор. Помоћу HTTP захтева веб претраживачи захтевају информације које су им потребне да би учитали одређени вебсајт.
HTTP одговор је оно што веб клијенти добијају од сервера као одговор на HTTP захтев. Ови одговори пружају информације које су тражене путем HTTP захтева. Сваки HTTP одговор се састоји од статусног кода и од заглавља HTTP одговора и опционо од тела HTTP одговора.

Simple Mail Transfer Protocol (SMTP) је такође протокол петог, шестог и седмог нивоа OSI модела. Његова сврха је размена електронске поште између корисника на истим или различитим рачунарима, а поред тога служи и за:

- слање поруке једном или више прималаца
- слање текстуалног, аудио или видео садржаја
- слање поруке на мрежама ван интернета

Post Office Protocol 3 (POP3), је највише коришћени протокол за пријем електронске поште преко интернета. Овај стандардни протокол користи се за примање електронске поште са удаљеног сервера и слање локалном клијенту.

2. МЕТОДЕ ФОРЕНЗИКЕ РАЧУНАРСКИХ МРЕЖА

Процес форензике рачунарских мрежа представља истраживање дигиталних података прикупљених путем различитих мрежа или разних мрежних уређаја. Током самог процеса истраге прати се процедура корак по корак у којој истражитељи идентификују, прикупљају, чувају, прегледају и анализирају доказе.
Свака истрага у оквиру дигиталне форензике се састоји од наредних корака [4]:

2.1 Идентификација доказа

Први корак форензичке истраге, углавном укључује информације о доказима који су присутни, где се чувају и како се чувају тј. у ком су формату.
Извори доказа се могу поделити у следеће две категорије:

- Докази који се могу добити унутар мреже
- Докази који се могу добити ван мреже

2.2 Прикупљање доказа

Након што се успешно идентификују, доказе је неопходно прикупити на исправан начин помоћу одређених процедура или смерница како би остали ваљани. Ова фаза се бави обезбеђењем места које је предмет форензичке истраге од неовлашћених приступа и очувањем интегритета доказа како не би постали компромитовани и услед тога неупотребљиви.
Прикупљање доказа се сврстава у две категорије [5]:

- Прикупљање променљивих доказа
- Прикупљање непроменљивих доказа

2.3 Чување доказа

Врло је важно сачувати доказе тако да они у што већој мери остану непромењени.
Кад год се докази преносе од особе до особе, неопходно је очувати информације о такозваном ланцу доказа (енг. „chain of custody“) [6].
Ланац доказа је једна од три методе коју форензичари треба да користе како би сачували доказе пре него што започне фаза анализе. Поред ове методе, постоје још и „DriveImaging“ и „Hash Values“.

2.4 Прегледање доказа

Прикупљени подаци се класификују и групишу у одређене групе како би даљи процеси анализе били једноставнији и како би управљање самим доказима било једноставније.
Главни задатак ове фазе форензичке истраге јесте уклонити сувишне информације и неповезане податке и издвојити потенцијално најрелевантније доказе за истрагу. Такође, у оквиру ове фазе истраге потребно је повратити податке које је нападач потенцијално покушао да сакрије или камуфлира.

2.5 Анализа доказа

Главни циљ ове фазе је издвојити потенцијално релевантне податке и испитати их.
Евиденција догађаја на мрежи је најважније средство за форензичку анализу проблема у систему.
Фаза анализе се може извршити на два начина. Прва је стратегија „ухвати што можеш“ (енг. “*Catch it as you can*”), која подразумева снимање целокупног мрежног саобраћаја ради анализе.
Стратегија „заустави, погледај и слушај“ (енг. “*Stop, look and listen*”) подразумева анализу сваког пакета података који путује кроз мрежу и прикупљање само онога што се сматра сумњивим и вредним даље истраге.
Један од веома корисних извора за анализу саобраћаја на мрежи је и NAT механизам (енг. *Network Address Translation*).

3. АЛАТИ ФОРЕНЗИКЕ РАЧУНАРСКИХ МРЕЖА

Користећи алате за мрежну форензику, могуће је пратити е-пошту, открити лозинке, одредити веб странице које неко посећује, чак и шпијунирати садржај корпе за онлајн куповину. Огромна моћ ових система над данашњим мрежама чини их предметом злоупотребе.

Алати за мрежну форензику омогућавају надгледање мреже и прикупљање информација о саобраћају, али такође помажу у истрази разних врста злочина на мрежи.
Сваки алат форензике рачунарских мрежа у идеалном случају би требало да има следеће особине:

- Ефикасна обрада великих датотека за чување података о мрежи
- Екстраховање информација високог нивоа или индексирање кључних речи
- Могућност поткрепљивања сваког извученог закључка

3.1 Autopsy

Једна од карактеристика Autopsy-ја је тзв. „plug-in“ архитектура. Оваква архитектура сваком програмеру даје могућност да креира и додаје сопствене прилагођене модуле или да бира између неколико унапред направљених.
Постоје три опште групације модула:

- анализа фајлова
- модул за извештаје
- графички приказ аналитике

Неки од засебних модула које је могуће су:

- модул недавне активности,
- модул за идентификацију типа датотеке,
- модул за претрагу кључних речи и
- модул за парсирање електронске поште.

3.2 Wireshark

Овај алат је анализатор мрежних протокола. Омогућава хватање односно снимање и прегледање саобраћаја који се одвија на мрежи.
Корисне карактеристике које поседује овај алат:

- Филтрирање
- Снимање података уживо и „offline“ анализа
- Читање или писање из различитих датотека за снимање
- Декрипција

Wireshark такође омогућава идентификацију различитих врста напада на мрежу. Једна врста напада коју је могуће идентификовати помоћу овог алата је такозвано „малициозно преузимање“, помоћу ког нападач може са интернета да преузме датотеке у систем.
Друга врста напада је позната под скраћеницом „DDOS“ тј. *Distributed Denial Of Service*. У овој врсти напада нападачи ускраћују ресурсе у оквиру једног система или чак на нивоу читаве мреже.
Последња врста напада је такозвано скенирање порта. Нападачи се користе овом методом како би пронашли осетљиве уређаје и како би скенирали портове односно „пронашли отворена врата кроз која могу лако да уђу“.

3.3 Xplico

Циљ овог алата је да из интернет саобраћаја сними податке који су на нивоу апликације.
Фокус овог алата нису сами мрежни протоколи па Xplico сврставамо у групу алата за форензичку анализу мрежа, чији је фокус реконструкција података који су се слали преко самих протокола.
Xplico такође нуди могућност „извожења“ података и информација у SQLite или MySQL базу података.

3.4 NetworkMiner

NetworkMiner је алат отвореног изворног кода који спада у групу алата за форензичку анализу мреже. Овај алат се може користити као пасивни „network sniffer“ или као алат за хватање пакета у циљу откривања оперативног система, сесија, имена хостова, отворених портова итд. без стављања било каквог саобраћаја на мрежу.
Још једна веома корисна карактеристика овог алата је то што корисник може да врши претрагу кључних речи у сачуваним или такозваним „снифованим“ подацима.

3.5 NetDetector

NetDetector континуирано бележи сав саобраћај мрежа на које је повезан. Док се саобраћај снима, овај алат у исто време анализира снимљене податке у циљу откривања аномалија у самом саобраћају и одмах даје упозорења ако се одређени прагови премаше. Ови прагови се могу програмирати од стране корисника, а кад се испуне, брзи механизми NetDetector-а обезбеђују континуирано снимање/чување и анализу тј. упозорења без пропуштања пакета, тока или протока на мрежи.

3.6 Xtractor

Овај алат је посебно дизајниран за издвајање података и информација из скоро свих врста датотека електронске поште, па тако може да се користи за екстракцију адреса електронске поште, бројева телефона и порука. Са друге стране, Xtraxtor може послужити за пренос електронске поште са e-mail клијента директно ка различитим провајдерима који пружају услуге везане за електронску пошту.
Кључне карактеристике овог алата су:

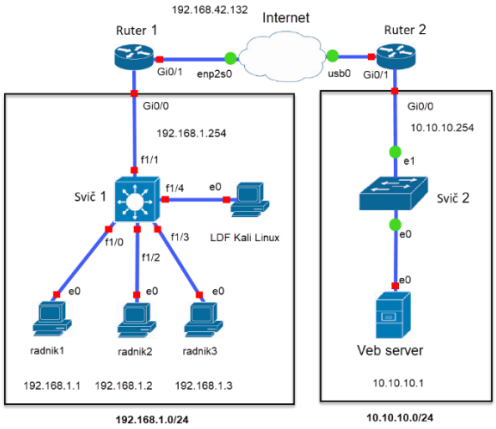
- Преглед електронске поште
- Чување метаподатака
- Одржавање хијерархије фолдера
- Неограничена конверзија

4. СТУДИЈА СЛУЧАЈА

Кроз студију случаја приказан је ток истраге кроз фазе које су неопходне у свакој истрази када је у питању дигитална форензика.
На слици 1 је представљена шема рачунарске мреже која ће бити предмет истраге.
Претпоставка је да је у десном делу представљен веб сервер неке компаније који хостује одређени сервис, а у левом делу рачунарске мреже појединачни уређаји запослених људи у другој компанији.
Циљ истраге јесте утврђивање ко је од запослених приступао веб сервису од интереса.

4.1 Идентификација доказа

На основу приложене шеме рачунарске мреже можемо да идентификујемо потенцијалне изворе доказа који ће бити од значаја за ток истраге. Кључни актери у овој истрази ће бити веб сервер и рутер који је конфигурисан у оквиру компаније.



Слика 1. Шема рачунарске мреже

4.2 Прикупљање доказа

Помоћу одређених алата неопходно је прикупити лог фајлове поменутих уређаја од значаја у оквиру рачунарске мреже на основу којих ће се даље вршити процес анализе. Најчешће компоненте у мрежи које су одговорне за NAT лог фајлове су рутери и firewall-ови. Начин на који је могуће прикупити ове лог фајлове зависи од самог уређаја, неки уређаји имају одговарајући веб интерфејс док други захтевају приступ преко командне линије.

4.3 Чување доказа

Најбитнији аспект чувања доказа је очување интегритета истих.
Смернице очувања доказа су:

- Документовање ланца доказа
- Коришћење хеш алгоритама
- Генерисање резервне копије

4.4 Прегледање доказа

У фази прегледања доказа неопходно је да се форензичари упознају са конфигурацијом мрежних уређаја. Циљ фазе прегледања доказа је заправо филтрирање свих прикупљених доказа како би се припремили само они докази који ће бити анализирани у наредној фази истраге.

4.5 Анализа доказа

Увидом у лог фајл веб сервера који хостује поменути сервис могуће је издвојити јавне IP адресе компаније са којих је приступано веб сервису. Уколико се погледа шема рачунарске мреже (*слика 1*) може се видети да је јавна IP адреса рутера компаније 192.168.42.132. Након увида у лог фајл веб сервера видеће се да се ова IP адреса појављује неколико пута уз различите портове.
Даље, прегледом лог фајла NAT сервиса који је конфигурисан на рутеру компаније могуће је одредити приватне IP адресе запослених људи у фирми који су приступили одређеном веб сервису.
Након што су докази прикупљени, на одговарајући начин сачувани и прегледани потребно је анализирати их и донети одговарајуће закључке.

4.6 Презентација доказа

Након што су извршени сви неопходни кораци форензичке истраге почевши од идентификације доказа завршно са анализом истих, неопходно је креирати налаз и мишљење који је даље потенцијално потребно приложити и бранити на суду.
Докази од значаја који су коришћени у оквиру истраге су:

- Шема рачунарске мреже
- Лог фајлови веб сервера
- Лог фајлови NAT сервиса конфигурисаног на рутеру саме компаније

5. ЗАКЉУЧАК

Са појавом интернета, годинама уназад, број и обим рачунарских мрежа се повећава великом брзином. Сходно томе расте и вероватноћа за потенцијална кривична дела путем рачунарских мрежа. Као одговор на такве претње јавља се потреба за константним развојем форензике рачунарских мрежа.
Мотивација овог рада јесте представљање процеса и значаја форензике рачунарских мрежа као и техника и алата у њеној примени. Изазов који потенцијално може да омета форензику рачунарских мрежа јесте чињеница да познавање начина функционисања алата и процедура које се користе у форензици, омогућавају нападачима да манипулишу потенцијалним доказима и смером истраге.

6. ЛИТЕРАТУРА

[1] Interpol Digital forensics, доступно на https://www.interpol.int/How-we-work/Innovation/Digital-forensics. [посећено април 2021].
[2] Network Forensics Encyclopedia, Science News & Research Reviews, доступно на https://academic-accelerator.com/encyclopedia/network-forensics. [посећено април 2023].
[3] NetworkWorld, доступно на https://www.networkworld.com/article/3239677/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html [посећено април 2023]
[4] Милана Писарић, Elektronski zapisi kao dokazi u krivičnom postupku, Правни факултет, Нови Сад, фебруар 2009
[5] Mr. Ankit Agarwal, Ms Megha Gupta, Mr Saurabh Gupta, Prof Subhash Chandra Gupta, „Systematic Digital Forensics Investigation Model“
[6] R. C. Joshi, Emmanuel S. Pilli, Fundamentals of Network Forensics

Кратка биографија:

Јелена Стојаковић рођена је 1997. године у Суботици.
Мастер рад на Факултету техничких наука из области Електротехнике и рачунарства – Форензика рачунарских мрежа одбранила је 2024. године.
контакт: jekibp@gmail.com