****

**Kauno technologijos universitetas**

Informatikos fakultetas

**Duomenų srauto įrašo tyrimas**

Kompiuterių tinklų sauga (T120M151)

Atliko:

IFM-1/3 gr. studentas

Eligijus Kiudys

2021 m. lapkričio 29 d.

Priėmė:

lekt. Dangis Rimkus

**Kaunas, 2021**

Turinys

[Paveikslų sąrašas 3](#_Toc88429798)

[1. Įvadas 4](#_Toc88429799)

[2. Tyrimo eiga 5](#_Toc88429800)

[2.1. Aplankytų svetainių analizė 6](#_Toc88429801)

[2.2. Elektroninio pašto analizė 10](#_Toc88429802)

[2.1. Naudoto serverio analizė 13](#_Toc88429803)

[2.1. Pokalbių kambario analizė 16](#_Toc88429804)

[2.1. Užkuoduotų paketų analizė 17](#_Toc88429805)

[3. Išvados 19](#_Toc88429806)

Paveikslų sąrašas

[pav. 1 Wireshark „Protocol Hierarchy“ langas 5](#_Toc88429807)

[pav. 2 Wireshark „Conversations“ langas 5](#_Toc88429808)

[pav. 3 Wireshark „Endpoint“ langas 5](#_Toc88429809)

[pav. 4 Wireshark „HTTP object list“ langas 6](#_Toc88429810)

[pav. 5 Filtras skirtas youtube.com svetainei 7](#_Toc88429811)

[pav. 6 Filtras skirtas apple.com svetainei 7](#_Toc88429812)

[pav. 7 Filtras skirtas unimelb.edu.au svetainei 8](#_Toc88429813)

[pav. 8 Filtras skirtas yahoo.com svetainei 8](#_Toc88429814)

[pav. 9 Filtras skirtas google.com svetainei, pirma dalis 9](#_Toc88429815)

[pav. 10 Filtras skirtas google.com svetainei, antra dalis 9](#_Toc88429816)

[pav. 11 Filtras skirtas wikipedia.org svetainei 10](#_Toc88429817)

[pav. 12 Filtras skirtas ox.ac.uk svetainei 10](#_Toc88429818)

[pav. 13 Elektroninio laiško protokolo filtravimas 11](#_Toc88429819)

[pav. 14 Filtruojama informacija su prisijungimo duomenimis 11](#_Toc88429820)

[pav. 15 Elektroninio pašto naudotojo vardas ir elektroninis paštas. 11](#_Toc88429821)

[pav. 16 Elektroninio pašto laiškų informacija 12](#_Toc88429822)

[pav. 17 Išsiųstas el. laiškas 12](#_Toc88429823)

[pav. 18 Išsiųsto el. laiško vidus naudojant „Wireshark“ 13](#_Toc88429824)

[pav. 19 Išsiųsto el. laiško vidus naudojant „NetworkMiner“ 13](#_Toc88429825)

[pav. 20 „FTP“ protokolo filtras 14](#_Toc88429826)

[pav. 21 „FTP“ protokolo filtras su naudotojo prisijungimu 14](#_Toc88429827)

[pav. 22 „FTP-DATA“ protokolo filtras 14](#_Toc88429828)

[pav. 23 „LIST“ komandos panaudojimas serveryje 15](#_Toc88429829)

[pav. 24 „LIST“ komandos rezultatai 15](#_Toc88429830)

[pav. 25 README failo vidus 16](#_Toc88429831)

[pav. 26 „IRC“ protokolo filtras 16](#_Toc88429832)

[Pav. 27 „WHO“ komandos rezultatai 17](#_Toc88429833)

[pav. 28 „TLS“ paketų filtravimo daliniai rezultatai 17](#_Toc88429834)

[pav. 29 Paketo sekimo rezultatas 18](#_Toc88429835)

[pav. 30 Paketo sekimo rezultatas 18](#_Toc88429836)

# Įvadas

Inžinerinio projekto metu reikia išanalizuoti naudotojo tinklą, kuriame galima rasti naudotojo veiksmus. Analizuojant naudotojo veiksmus galima pamatyti, kokiuose puslapiuose naudotojas lankėsi, galima rasi naudotojo IP adresus bei jo duomenis.

Varianto numeris: 12a.pcap

Įrašo datą ir laikas: 2012-04-12

Trukmė: 269.755436 sekundės

Esminio vartotojo IP: 10.0.2.15

MAC adresus: 08:00:27:8a:d6:9d

OS: Windows NT 5.1 – Windows XP

Klientinės programos: Safari 5.0.5, Thunderbird 11.0.1

# Tyrimo eiga

Atsidarius failą kurį analizuojama naudojant „Wireshark“ programą, kur paspaudžiame ant **Statistics->Protocol Hierarchy**, atsivertus informacijos langą (pav. 1) matome, kad buvo apsilankyta puslapiuose, buvo siunčiami elektroniniai laiškai.

Graphical user interface, application, table

Description automatically generated

pav. 1 Wireshark „Protocol Hierarchy“ langas

Pasinaudojus „Wireshark Conversations“ langu (pav. 2) matome du pagrindinius MAC adresus, tarp kurių vyko komunikacija, viso įrašymo laikotarpiu.

Graphical user interface, application, Word

Description automatically generated

pav. 2 Wireshark „Conversations“ langas

Atsivertus „Endpoint“ langą (pav. 3), matome tokius pačius MAC adresus kaip ir „Conversations“ lange (pav. 2).

Graphical user interface, application, table, Excel

Description automatically generated

pav. 3 Wireshark „Endpoint“ langas

Išanalizavus „Conversations“ ir „Endpoint“ langus tarp naudotojo ir galimo interneto šaltinio vykusius duomenų mainus galime analizuoti naudotojo veiklą toliau. Rastų adresų pagalba galime toliau analizuoti naudotojo veiklą.

## Aplankytų svetainių analizė

Norint išsiaiškinti naudotojo aplankytus puslapius bei jų tipą reikia pasirinkti **File->Export Objects->HTTP**. Pasirinkus šitą pasirinkimą atsidarys langas su naudotojo aplankytais puslapiais. Išanalizavus puslapius buvo aišku, kokiuose puslapiuose naudotojas naršė. Paaiškėjo jog naudotojas naršė puslapiuose: [www.apple.com](http://www.apple.com), [www.youtube.com](http://www.youtube.com), [www.unimelb.edu.au](http://www.unimelb.edu.au), [www.yahoo.com](http://www.yahoo.com) [www.google.com](http://www.google.com), [www.wikipedia.org](http://www.wikipedia.org), [www.ox.ac.uk](http://www.ox.ac.uk). Pasinaudojus šia komanda buvo galima pamatyti ne vien puslapius, bet ir kartu su puslapiais atsiunčiamus paveikslėlius, JavaScript priedus ir t.t. Žemiau pateiktoje nuotraukoje (pav. 4) galima pamatyti panaudotos komandos rezultatų dalį.

Table

Description automatically generated with medium confidence

pav. 4 Wireshark „HTTP object list“ langas

Suradus puslapius, galima juos atfiltruoti ir patiksinti pasirinkto puslapio užklausas. Tokių užklausų filtravimui bus naudojamas GET užklausos filtravimas su pasiriktu puslapiu.

Suradus informaciją apie puslapius galime jų paketus atfiltruoti ir išsiaiškinti, ką naudotojas veikė tokiuose puslapiuose. Bendram puslapių filtravimui yra naudojama *http.request.method == “GET”* filtras. Norint sumažinti visų puslapių paketus iki pasirinkto puslapio reikia pridėti prie filtravimo *and frame contains „youtube.com“*. Atfiltravus pirmąjį puslapį [www.youtube.com](http://www.youtube.com) yra matomi atfiltruoti rezultatai (pav. 5). Iš viso buvo rasta 32 paketai, kurių pagalba yra išanalizuojama veikla youtube.com puslapyje.

A picture containing graphical user interface

Description automatically generated

pav. 5 Filtras skirtas youtube.com svetainei

Išfiltravus pirmąjį puslapį, galime filtruoti sekantį puslapį, kuris yra apple.com. Pasirinkto puslapio filtras yra: *http.request.method == "GET" and frame contains "apple.com"*. Atfiltravus pasirinktą puslapį buvo rasti 27 paketai (pav. 6). Pirmas paketas yra skirtas puslapio atidarymui, o kiti paketai yra skirti nuotraukų ar kitokių failų atsisiuntimui.

Text

Description automatically generated with medium confidence

pav. 6 Filtras skirtas apple.com svetainei

Tęsiame puslapių paketų filtravimą su kitu naudotojo naršytu puslapiu. Kitas pasirinktas puslapis buvo unimelb.edu.au. Filtravimui yra naudojamas toks filtras: *http.request.method == "GET" and frame contains "unimelb.edu.au"*. Atfiltravus paketus buvo rasta 41 paketas (pav. 7). Pirmasis paketas yra skirtas pačio puslapio atvertimui, kiti paketai yra skirti nuotraukų ir kitų failų atidarymui.

Text

Description automatically generated

pav. 7 Filtras skirtas unimelb.edu.au svetainei

Išfiltravus kitą pasirinktą puslapį, kuris yra yahoo.com, buvo gauti išfiltruoti pasirinkto puslapio paketai. Puslapio paketų filtravimui yra naudojamas filtras: *http.request.method == "GET" and frame contains "yahoo.com"*. Atfiltruotų paketų kiekis yra 88 paketai. Kadangi buvo atfiltruota tiek daug paketų, nuotraukoje yra matoma ne visi paketai (pav. 8). Pirmasis paketas yra skirtas puslapio užklausai, visi kiti paketai yra skirti failų atsiuntimams, kaip ir kituose puslapiuose.

Table

Description automatically generated with medium confidence

pav. 8 Filtras skirtas yahoo.com svetainei

Kitas puslapis, kuris filtruojamas yra google.com. Šis puslapis yra populiariausias paieškos puslapis. Filtravimui yra naudojamas filtras: *http.request.method == "GET" and frame contains "google.com"*.

Atfiltravus pasirinktą puslapį buvo gauti 43 paketai. Pirmoje nuotraukoje (pav. 9) pagal URL adresą galima nustatyti, kad naudotojas po paieškos bandė eiti į nesaugų puslapį. Einant į nesaugius puslapius per google.com pasikeičia URI kuris pradžioje yra „safebrowsing“.

Text

Description automatically generated

pav. 9 Filtras skirtas google.com svetainei, pirma dalis

Toliau išanalizavus atfiltruotus google.com paketus galime pastebėti ko naudotojas ieškojo ir kur toliau lankėsi (pav. 10). Paketų rezultatuose matoma, kad naudotojas ieškojo „cross site scripting“ raktažodžio. Atvertus paieškos rezultatą naudotojas atsivertė wikipedia.org puslapį apie „cross site scripting“. Grįžęs iš wikipedia.org puslapio į google.com puslapį naudotojas atliko kitą paiešką apie „denial of service“. Google pateikus paieškos rezultatą naudotojas atsivertė kitą wikipedia.org puslapį kuris buvo apie „Denial-of-service attack“.

Text

Description automatically generated

pav. 10 Filtras skirtas google.com svetainei, antra dalis

Filtruojam toliau internetinių puslapių užklausas. Kitas internetinis puslapis kurio paketai filtruoti yra wikipedia.org. Atfiltravus pasirinkto puslapio paketus yra rasta tik 17 paketų (pav. 11). Tarp atfiltruotų paketų yra du paketai, kurie skirti pačio puslapio atvertimui, kiti paketai yra skirti gauti puslapio failus.

Graphical user interface, text

Description automatically generated

pav. 11 Filtras skirtas wikipedia.org svetainei

Atfiltruojame paskutinio rasto puslapio paketus, kuris yra ox.ac.uk. Puslapio filtras yra: *http.request.method == "GET" and frame contains "ox.ac.uk"*. Šio filtro pagalba buvo rasti 48 paketai, kurie netelpa į bendrą nuotrauką (pav. 12). Pirmasis paketas kaip ir kituose puslapiuose buvo pačio puslapio užklausa, visi kiti paketai yra skirti puslapio informacijos ir funkcionalumui užkrauti.

Graphical user interface

Description automatically generated with medium confidence

pav. 12 Filtras skirtas ox.ac.uk svetainei

## Elektroninio pašto analizė

Filtravus visus paketus naudojant „IMAP“ protokolo filtrą, yra matoma, kad buvo jungiamasi prie elektroninį paštą. Galima aptikti kokią programą naudotojo elektroniniams laiškams valdyti, bei paprastą informaciją apie naudojamo elektroninio pašto informaciją (pav. 13).

Graphical user interface, text, application

Description automatically generated

pav. 13 Elektroninio laiško protokolo filtravimas

Išsiaiškinus, kad naudotojas naudojo elektroninį paštą buvo toliau ieškoma paketų su informacija apie naudotoją. Panaudojus *imap and frame contains "login"* filtrą buvo rasti penki paketai kurie yra susieti su prisijungimo informacija (pav. 14). Pirmame pakete iškarto yra matomas naudotojo prisijungimas ir slaptažodis prie elektroninio pašto paskyros. Esminiai paketai: 1969 2022 2054 ir 2222 atskleidžia naudotojo prisijungimo vardą "frederickflintstone" ir slaptažodį „1234abcd“.

A screenshot of a computer

Description automatically generated with medium confidence

pav. 14 Filtruojama informacija su prisijungimo duomenimis

Pakeitus filtro nustatymus į *imap and frame contains "frederickflintstone"* aptikome paketą su naudotojo elektroniniu pašto adresu ir vardu, iš kurio buvo siųstas elektroninis laiškas. Paketo numeris: 4475. Rastas vardas „frederick“ ir elektroninis paštas [frederickflintstone@aol.com](mailto:frederickflintstone@aol.com).

Graphical user interface

Description automatically generated with medium confidence

pav. 15 Elektroninio pašto naudotojo vardas ir elektroninis paštas.

Pasinaudojus filtru *imap and frame contains "STATUS"* galima atfiltruoti elektroninio pašto informaciją su elektroninių laiškų kiekiu (pav. 12). Elektroninio pašto juodraščiuose yra 7 laiškai, išsaugotų laišku yra 17, parašytų IM žinučių yra 259, išsiųstu žinučių yra 294, šlamšto žinučių yra 5 ir į šiukšliadėžę perkeltų žinučių yra 301.

Graphical user interface, text, application

Description automatically generated

pav. 16 Elektroninio pašto laiškų informacija

Išsiaiškinus el. pašto statusą, atfiltravau galimus išsiųstų laiškų paketus. El. laiškų filtras: *imap and contains „Message“*. Atfiltravus paketus yra matoma, kad buvo išsiųstas vienas el. laiškas, kurio paketo numeris yra: 4447 (pav. 17).

Graphical user interface, application

Description automatically generated

pav. 17 Išsiųstas el. laiškas

El. laiško skaitymui galima panaudoti „Follow TCP Stream“ funkcionalumą, pritaikant ant el. laiško paketo (pav. 18). Taip pat pasinaudojau „NetworkMiner“ programa, kuri lengviau leidžia perskaityti išsiųstus laiškus (pav. 19). Rastame turinyje matome, kad laiškas buvo siųstas iš [frederickflintstone@aol.com](mailto:frederickflintstone@aol.com) į [h138869@rppkn.com](mailto:h138869@rppkn.com). Išsiųsto laiško tema yra: „User Information“, o laiško viduje yra siunčiama prisijungimo informacija.

Graphical user interface, text, application, email

Description automatically generated

pav. 18 Išsiųsto el. laiško vidus naudojant „Wireshark“

Graphical user interface, text, application, Word

Description automatically generated

pav. 19 Išsiųsto el. laiško vidus naudojant „NetworkMiner“

## Naudoto serverio analizė

Filtruojant „FTP“ protokolą matome, kad naudotojas naudojosi failo perkėlimą iš serverio (pav. 20). Paketas, kurio numeris: 4486. Šis paketas rodo, kad naudotojas prisijungė kaip anonimas (nežinomas naudotojas).

Graphical user interface, text, application

Description automatically generated

pav. 20 „FTP“ protokolo filtras

Atfiltravus naudotojo prisijungimo vardą su „FTP“ protokolu galima surasti kiek kartų naudotojas jungėsi prie serverio (pav. 21). Šio atveju naudotojas jungėsi du kartus su „anonymous“ prisijungimu. Serverio adresas į kurį jungėsi yra: 208.118.235.20.

A screenshot of a computer

Description automatically generated with medium confidence

pav. 21 „FTP“ protokolo filtras su naudotojo prisijungimu

Panaudojus *ftp-data* filtrą yra atfiltruoti trys paketai su duomenimis (pav. 22). Šio filtro pagalba galima surasti naudotus failus, ar terminalo komandos rezultatus.

Table

Description automatically generated with medium confidence

pav. 22 „FTP-DATA“ protokolo filtras

Filtruojant „FTP“ paketus su *ftp and frame contains „LIST“* filtru (pav. 23). Yra matoma, kad „LIST: komanda buvo naudojama tik vieną kartą, kai naudotojas buvo pagrindiniame serverio aplankale.

Graphical user interface, text, application, email

Description automatically generated

pav. 23 „LIST“ komandos panaudojimas serveryje

Galime paanalizuoti, kokie rezultatai buvo pateikti panaudojant „list“ komandą. Paveikslėlyje buvo pateiktas paketas su „list“ komandos rezultatu paketu kurį galime išanalizuoti (pav. 22). Peržiūrima 4592 paketo informaciją (pav. 24), pasinaudojus „Follow TCP Stream“ funkciją. Atsidarius „list“ komandos rezultatą matome esančius failus, serverio pagrindiniame aplankale. Pateikta informacija atskleidžia failų pavadinimus ir prieiga prie jų.

Text, table

Description automatically generated

pav. 24 „LIST“ komandos rezultatai

Panaudojus „Follow TCP Stream“ komandą ant failo paketo galime atsiversti failą ir pamatyti failo vidų (pav. 25). Šitas failas susidaro iš dviejų paketų.

Graphical user interface, text, application

Description automatically generated

pav. 25 README failo vidus

## Pokalbių kambario analizė

Panaudojus *irc* filtrą randame paketus, kurie yra skirti žinučių siuntimui (pav. 26). Matome, kad buvo panaudota ne viena komanda. Pasirinkau analizuoti „WHO“ komandą, kurią panaudojus yra išvedami visi prisijungę prie pokalbio kambario naudotojai.

Table

Description automatically generated

pav. 26 „IRC“ protokolo filtras

Pasinaudojus „Follow TCP Stream“ funkciją yra gaunami pasirinkto paketo rezultatai. Pasirikus „WHO“ komandos paketą, galima pamatyti. Kas buvo prisijungę tuo metu prie pokalbio kambario (Pav. 27).

Text

Description automatically generated

Pav. 27 „WHO“ komandos rezultatai

## Užkuoduotų paketų analizė

Pritaikius *tsl* filtrą pavyko atfiltruoti 29 paketus. Atfiltravus paketus buvo surasti trys du IP adresai, kurie gražino aplikacijos duomenis (pav. 28). Kadangi duomenys yra užšifruoti, bandysime bent jau surasti kur naudotojas kreipėsi.

Graphical user interface, application

Description automatically generated

pav. 28 „TLS“ paketų filtravimo daliniai rezultatai

Pasirinkus antrąjį paketą numeriu: 2000, galime atsekti kur naudotojas kreipėsi kai gavo šį paketą.

Pasinaudojus „Follow TCP Stream“, buvo galima atsekti į kokį puslapį naudotojas kreipėsi (pav. 29). Sekant pavyko aptikti puslapį kuriame naudotojas lankėsi. Surastas puslapis yra: http://live.mozillamessaging.com.

Graphical user interface, text, application

Description automatically generated with medium confidence

pav. 29 Paketo sekimo rezultatas

Pasirinkus paketą kurio numeris yra: 4415, galime sekti kaip sekėme ir praėjusi paketą. Sekant paketą buvo aptiktas serveris į kurį kreipėsi naudotojas (pav. 30). Serverio pavadinimas: smtp.aol.com.

Graphical user interface, table

Description automatically generated

pav. 30 Paketo sekimo rezultatas

# Išvados

Darbo metu atliktas srauto tyrimas. Buvo išsiaiškinta, jog naudotojas naudotojo Windows XP operacinę sistemą bei naudojo Safari naršyklę ir Thunderbird 11.0.1 el. pašto klietntą. Atlikus interneto srauto filtravimą buvo atrasta, kad naudotojas lankėsi google.com puslapyje iš kurio ėjo du kartus į wikipedia.org puslapį. Taip pat pavykto aptikti su „FTP“ protokolu susijusį failą, kurio turinys buvo peržiūrėtas naudojant „Follow TCP Stram“ funkciją. Išanalizavus „IRC“ protokolą pavyko aptikti, kad naudotojas naudojosi pokalbių kambariu, kuriame panaudojo komandas, kaip „WHO“. Atkurti pranešimą pavyko tik vieną, kitų pranešimų atkurti nepavyko, kadangi jie buvo užšifruoti. Iš užšifruoto srauto pavyko aptikti aplankytą adresą. Puslapių analizės metu, nepavyko aptikti užpildytu formų informacijos. Atlikus analizę buvo išanalizuota ir aptikta, daugiau duomenų negu tikėtasi. Buvo pagilintos žinios naudojantis filtrais.