- формирование управления;
- обучение (адаптация)',
- синхронизации и управления всеми компонентами.

Очевидно, что каждая из этих задач непосредственно связана с работой определенного компонента системы управления поведением мобильного робота и должна рассматриваться отдельно. Отметим, что в зависимости от того, какого класса система рассматривается (в соответствии с рисунком 2), некоторые из перечисленных задач либо вообще не стоят, либо имеют принципиально различные решения, поэтому требуется отдельное их рассмотрение в контексте обоих классов.

Список литературы:

Киселев Д.В., Ющенко А.С. Нечеткое управление поведением мобильных роботов // Вестник МГТУ. Приборостроение. - 2000. - № 1. - С.86 - 99.

Поспелов Д.А. Ситуационное управление. Теория и практика. - М.: Наука, 2010.- 285 с.

Ющенко А.С., Киселев Д.В., Григорьев А.А. Ситуативное поведение манипуляционных роботов в условиях неопределенности // Интегрированные модели и мягкие вычисления в искусственном интеллекте: Сборник научных трудов международного научно- практического семинара,- Коломна, 2001. - С.305-310.

ӘОЖ 004.772

ЖЕЛІЛІК ТРАФИКТІ ТАЛДАУ НӘТИЖЕЛЕРІН ҰСЫНУ ТӘСІЛДЕРІ

Карина Ж.М.
А.Байтұрсынов атындағы Қостанай Мемлекеттік Университеті, Қостанай қ.

Ғылыми жетекшісі: Атанов С.К.
Л.Н. Гумилев атындағы Еуразия Ұлттық Университеті, Нұр-сұлтан қ.

Ғылыми жетекшісі: Калакова Г.К.
А.Байтұрсынов атындағы Қостанай Мемлекеттік Университеті, Қостанай қ.

Аннотация: Мақалада желілік ақпараттық қауіпсіздікті қамтамасыз ету міндеттерінде қажеттілігі туындайтын желілік трафикті талдау нәтижелерін ұсынудың әр түрлі тәсілдері ұсынылған. Сонымен қатар, желілік өзара әрекеттесудің толық бағанын құру, сонымен қатар дестелерді таратудың уақытша диаграммасын құру мүмкіндігі қарастырылды. Бұл компоненттер ақ бұзылу инциденттерін тексеру кезінде қолданылады. Уақытша диаграмма, сондай-ақ

қолданылады және талдау жасау кезінде туннель хаттамалар, өйткені, талдау анықтау, қандай тақырыптар хаттамалар қажет визуализация үшін. Кері инженериямен, сондай-ақ желілік хаттамаларды баптаумен байланысты тапсырмалар үшін хаттамалардың тақырыптарын талдау қателері тіркелетін журналды пайдалану ұсынылады. Ұсынылған графикалық компоненттер немесе opensource-құралдары арасында аналогтары жоқ, немесе қазіргі opensource-шешімдерін жақсартады.

Түйінді сөздер: желілік трафикті талдау; желілік хаттамаларды жөндеу; желілік өзара іс-қимыл графалары; визуализация; талдау қателері журналы.

Аннотация: В статье предложены различные способы представления результатов анализа сетевого трафика, необходимость в которых возникает прежде всего в задачах обеспечения сетевой информационной безопасности. Рассмотрена возможность построения полного графа сетевых взаимодействий, а также создания временной диаграммы передачи пакетов. Эти компоненты используются при расследовании инцидентов нарушения ИБ. Временная диаграмма также применяется при анализе туннельных протоколов, поскольку позволяет аналитику определить, какие именно заголовки протоколов необходимо визуализировать. Для задач, связанных с обратной инженерией, а также отладкой сетевых протоколов, предлагается использовать журнал, в котором фиксируются ошибки разбора заголовков протоколов. Представленные графические компоненты либо не имеют аналогов среди opensource-инструментов, либо улучшают уже существующие opensource-решения.

Ключевые слова: анализ сетевого трафика; отладка сетевых протоколов; граф сетевых взаимодействий; визуализация; журнал ошибок разбора.

Abstract: The article proposes different methods of presenting network traffic analysis results, the need for which arises primarily in the area of network security. One of the most important tasks is to identify malicious traffic. For this purpose both the complete graph of network interactions and time-based packet diagram are presented. These components are used during investigation of information security violation incidents. The timing diagram is also used in analysis of tunneling protocols because it allows the analyst to determine which protocol headers are necessary to visualize. For tasks associated with reverse engineering and debugging of network protocols, it is proposed to use a journal which records protocol header parsing errors. Presented graphic components either have no analogues among the opensource tools or improve on existing opensource solutions.

Keywords: network traffic analysis, network protocols debugging, graph of network interactions, visualization, error log.

Көптеген есептерде желілік ақпараттық қауіпсіздікті қамтамасыз ету желілік трафикті егжей-тегжейлі талдау талап етіледі. Мұндай міндеттердің ішінде:

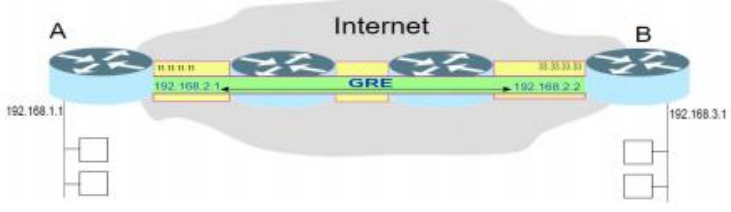
- ақ бұзылған инциденттерді тергеу
- желілік жағдайды талдау
- кері инженерия/желілік хаттамаларды жөндеу

Мұндай есептер әдетте "ағында" емес, бағдарламаның көмегімен трафиктің кейбір фрагментін бөлу арқылы сниффер және оны кейінгі талдау арқылы шешіледі. Бұл міндеттерді шешу кезінде жылдамдық пен тиімділікке әсер ететін сыни факторлар талдау ортасында желілік өзара әрекеттесудің түрлі аспектілерін визуализациялауға мүмкіндік беретін графикалық компоненттердің болуы және осы компоненттер арасындағы ауыстырып қосу және синхрондау мүмкіндіктері болып табылады.

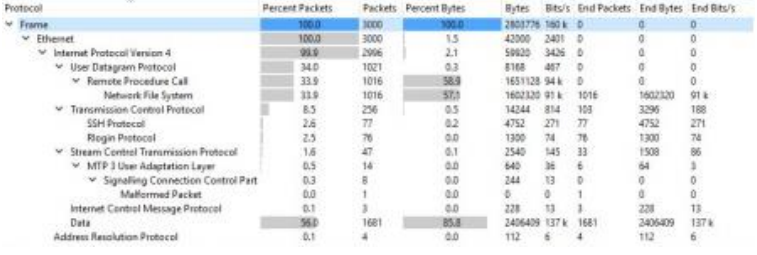
Қолданыстағы талдау құралдарына шолу.

Ең танымал құралдарын талдау желілік трафикті немесе графикалық интерфейс (Snort [1], The Bro Network Security Monitor [2]), не бастапқыда әзірленген үшін басқа да міндеттерді шешу және қанағаттандырады көрсетілген талаптарға ішінара ғана [3]. Екінші топтың ең танымал құралы-Wireshark құралы. Желі трассасын ұсынудың негізгі құралы-тізім түрінде бөлшектелген пакеттер болып табылады, бұл ретте тек бір бөлінген пакет үшін ғана хаттамалардың толық стегі және осы хаттамалардың тақырыптарындағы жолдардың мәндері көрсетіледі. Пакет, тізім элементі ретінде желілік деңгей протоколының (IP-мекенжай) атауында бөлінген тіркелген өрістер жиынтығы мәндерінен тұратын жол, сондай-ақ бөлшектелген ең жоғары деңгейдегі хаттама тақырыбы өрістерінен тұратын жол арқылы ұсынылады. Пакеттерді ұсыну нақтылығы көптеген жағдайларда қиындықтар тудыруы мүмкін. Атап айтқанда, бұл туннель хаттамаларын талдау кезінде көрінеді. Сондықтан GRE хаттамасы [5] (Сурет 1). IP-пакетте OSI моделінің желілік деңгейі пакеттерін инкапсуляциялауға арналған: желілік пакет, осылайша IP хаттамасының екі тақырыбы бар.

Wireshark желілік қосылымдарды визуалдаудың басқа тәсілі трассада бар протоколдар иерархиясын қарау болып табылады. Бірақ көрсету қосылыстардың кейбір жиынтық статистикасын көрсете отырып, хаттамалардың жалпы ағашы түрінде жүзеге асырылады, бірақ осы қосылыстардың параметрлерін қарау және оларды одан әрі талдау үшін хаттамалардың салынуының берілген түріне сәйкес келетін қосылыстардың нақты өкілдеріне көшу (Сурет 2).



Сурет 1. GRE-туннельді ұйымдастыру мысалы.



Сурет 2. Wireshark өзара іс-қимыл тіркесімін көрсету мысалы.

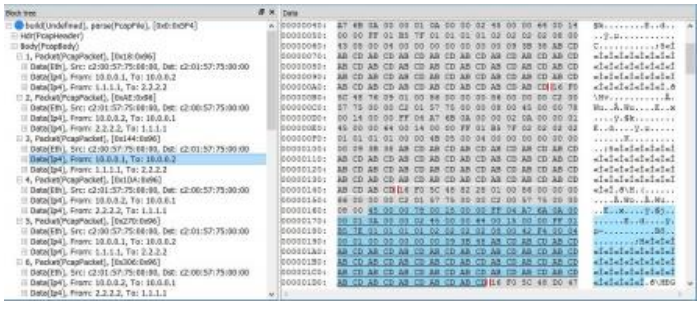
Талдау нәтижелерін ұсынудың іске асырылған нысандары және оларды қолдану

АҚ бұзылуының инцидентін тексеру кезінде осы инцидент уақыт аралығында пайда болған және дамыған желілік қосылыстарды оқшаулау қажет: талдаушы желілік пакеттердің ішіндегі кейбір критерийлерге (немесе осындай критерийлердің жиыны) ие болуы тиіс. Локализация мәселесін шешудегі тәсілдердің бірі-бұл баған арқылы желілік өзара іс-қимылдарды ұсыну болып табылады, онда шыңдарға желілік өзара іс-қимыл жақтары сәйкес келеді, ал қабырғалар өзара іс-қимыл фактісін және қарқындылық сияқты оның кейбір сипаттамаларын көрсетеді. Бұл ретте бір Тарап бірден бірнеше өзара іс-қимылға қатыса алады. Бұдан әрі бөлінген қосылыстарға егжей-тегжейлі талдау жүргізу қажет:

- пакеттерді жіберу / алу тәртібін қадағалау
- қажетті хаттамалар өрістерінің мәндерін қарау
- қолданбалы деңгейдегі хаттамаларды қалпына келтіру

Қарастырылған opensource-құралдар осындай сценарийлермен жұмыс істеу үшін графикалық компоненттерді ұсынбайды.

Талдау нәтижелерін ұсынудың ұсынылған компоненттері РҒА СБ-да әзірленген талдау жүйесінің ядросы пайдаланатын деректерді сипаттау моделіне сүйенеді. Wireshark-ге қарағанда, барлық желілік пакеттер (пайдаланушы таңдаған ғана емес) таңдалған инкапсуляцияланатын хаттамалардың тақырыптары бар ағаш арқылы бейнеленеді (сурет 3). Осылайша, туннель хаттамаларымен жұмыс істеу кезінде қиындықтар туындамайды.



Сурет 3. Бірнеше пакеттер үшін хаттамалар стегін көрсету мысалы.

Желілік өзара әрекеттесудің екі жолы ұсынылады:

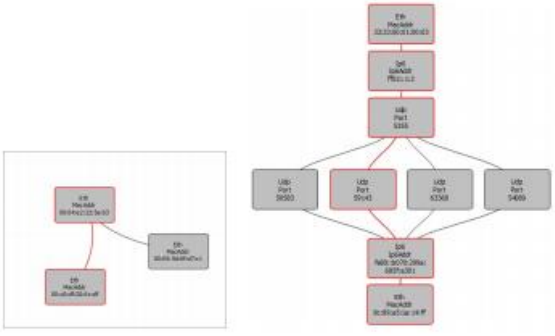
- соңғы түйіндер бағандары (Endpoints)
- таңдалған соңғы түйіннің желілік өзара әрекеттесуін (Nodes)

Екі баған желі түйіндерінің ағашына салынады. Желілік торап-желілік хаттамалар үшін жіберуші мен алушы ұғымдарын жинақтау. Мысалы, IPv4 протоколы үшін желілік торап IP мекенжайын сипаттайды, ал TCP протоколы үшін-порт. Егер B жіберушіні (алушыны) жіберуші (алушы) бөлінген төмендегі хаттаманың тақырыбына

(OSI моделіне сәйкес) салынған кейбір хаттаманың тақырыбында сипаттаса, ағаштың B шыңы a шыңына қатысты еншілес болып табылады.

Endpoints графасы (Сурет 4a) талданатын файлда ең төменгі деңгейдегі хаттамаға қатысты желілік қосылыстарды көрсетеді. Мұнда шыңдар ретінде әдетте MAC немесе IP адрестері әрекет етеді. Қабырғалар арасында ең болмағанда бір желілік пакет берілген желілік тораптарды қосады.

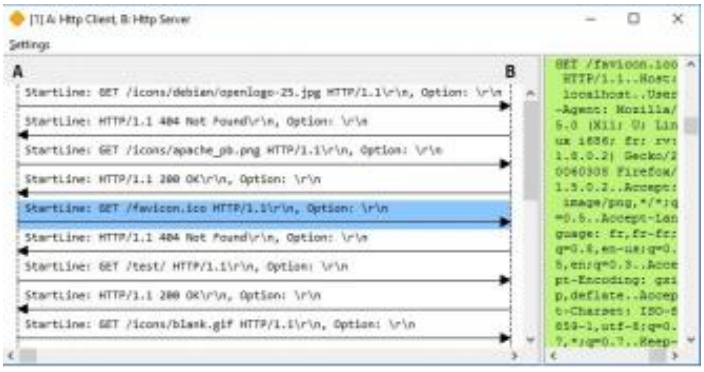
Сонымен қатар, егер желі серверінде қандай желілік қызметтер (қосымшалар) желіде іске қосылғанын анықтау қажет болса, желілік жағдайды тексеру есебінің нәтижелерін визуализациялауға мүмкіндік береді.



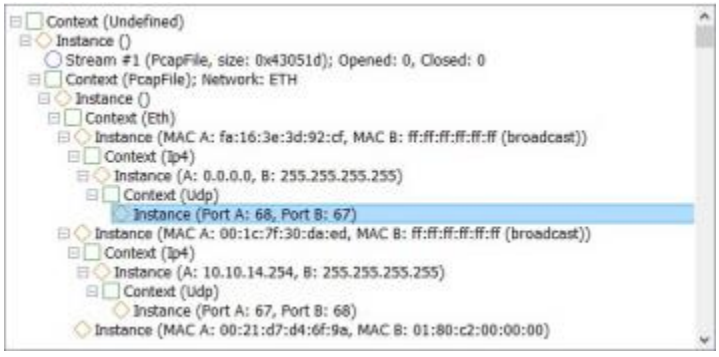
Сурет 4. (а) мысал бағаң Endpoints (б) мысал бағаң Nodes.

Жеке өзара іс-қимылдың егжей-тегжейлі талдауын жүргізу үшін уақытша диаграмма ұсынылады, онда әрбір пакет жөнелтуші мен алушы көрсетілген көрсеткі түрінде көрсетіледі (сурет. 5). Бұл ретте хаттамалардың қандай тақырыптары және оларда қандай өрістер көрсеткілердің үстінде көрсетілуі тиіс екенін көрсетуге болады. Осылайша, талдаушы графикалық компонентті өз қажеттіліктеріне бейімдей алады. Wireshark талдағышында ұқсас компонент бар екенін атап өткен жөн ,алайда, мәндер әр пакет үшін көрсетілетін өрістерді теңшеу мүмкіндігі жоқ, бұл қызықты өріс жоқ болса, ыңғайсыз болуы мүмкін немесе өрістер тым көп болса, көрінудің шамадан тыс жүктелуіне алып келуі мүмкін.

Қосылыстар параметрлері көрсетілген өзара әрекеттесулердің салынымы талдау ағашында бейнеленеді (Сурет 6). Дәл осы түрде құралдың ядросы талдау нәтижелерін сақтайды.



Сурет 5. Уақыт диаграммасының үлгісі.



Сурет 6. Қосылым параметрлерін көрсететін талдау ағашының үлгісі.

Кері инженериямен, сондай-ақ желілік хаттамаларды баптаумен байланысты міндеттерді шешу кезінде осы хаттамалардың тақырыптарын талдау кезінде туындайтын қателерді тіркеу қажеттілігі туындайды. Желі трафигін талдағыштар әдетте модульдік құрылымға ие: уақыт өте келе жаңа желілік хаттамалар пайда болады және оларды қолдау қажет. Қолдау жаңа хаттамамен жұмыс істеу бойынша функционалдығы локализацияланған модульді құру болып табылады. Модульді пайдалану кезінде талдау қателері пайда болуы мүмкін – бөлшектеуші коды мен осы бөлшектеуші арқылы талдау жүзеге асырылатын деректер арасындағы сәйкессіздік. Жүйеде іске асырылған қателер журналы қателерді тез оқшаулауға мүмкіндік береді. Талдау қатесі мәтіндік хабарламамен және оның пайда болу орнына сілтеме – тиісті пакет немесе желілік сеанспен сипатталады. Журналмен жұмыс істегенде хаттама бойын ша қателерді сүзу мүмкіндігі сақталады.

Берілген графикалық компоненттер бір-бірімен синхрондалған және желілік трафикті талдаудың қолданбалы есептерін шешу тиімділігін арттыру үшін әртүрлі көріністер арасында жылдам ауысуға жол береді.

Әдебиеттер тізімі:

1. Гетьман А.И., Маркин Ю.В., Падарян В.А., Тихонов А.Ю.. Модель представления данных при проведении глубокого анализа сетевого трафика. Труды ИСП РАН, том 27, вып. 4, 2015 ж., 5-22 бет. DOI: 10.15514/ISPRAS-2015-27(4)-1

2. Ю. В. Маркин, А. С. Санаров. Обзор современных инструментов анализа сетевого трафика. Препринты ИСП РАН, № 27, 2014

3. IETF RFC 2784. D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, Generic Routing Encapsulation, March 2000

4. Robert Shimonski. The Wireshark Field Guide: Analyzing and Troubleshooting Network Traffic. Elsevier Science & Technology Books, 2013, 128 бет.

5. Snort. https://www.snort.org/

6. The Bro Network Security Monitor. https://www.bro.org/

7. The Protocol Hierarchy window. https://www.wireshark.org/docs/wsug_html_chunked/ ChStatHierarchy.html

8.Wireshark. https://www.wireshark.org/, дата обращения: 10.10.2016

ӘОЖ 004.9

КОМПЬЮТЕРЛІК КӨЗДІҢ КӨМЕГІМЕН ОБЪЕКТІЛЕРДІ ТИІМДІ ИДЕНФИКАЦИЯЛАУ

Құлажан Ә.Е.
А.Байтұрсынов атындағы Қостанай Мемлекеттік Университеті
Қостанай қ.

Ғылыми жетекшісі: Абатов Н.Т.
А.Байтұрсынов атындағы Қостанай Мемлекеттік Университеті
Қостанай қ.

Аннотация: В данной статье были проведены приемы и методы для выполнения задач, исследование процесса распознавания символов и слов, идентификация объектов текста с помощью компьютерного (машинного) зрения.Они представляют собой определенную видеосигнальную цепь, из различных камер или трехмерных данных, отсканированных изображений и т. д. б. отбирается информация с рисунками, которые представляются на рисунках.

Ключевые слова**:** компьютерные источники; информационная безопасность; идентификация; теория распознавания образа, видеоаналитика ,OPC, бинаризация