УДК 00.4.4; 004.057.4; 004.9

© 2015 р., О.Є. Іларіонов[1], С.О. Кудренко[2], М.М. Іванчук[1]

[1] Вищий навчальний заклад «Університет економіки та права «КРОК», Київ
[2] Національний авіаційний університет, Київ

АНАЛІЗ ТЕХНОЛОГІЙ ТА ІНСТРУМЕНТІВ ДЛЯ МЕРЕЖЕВОЇ ФОРЕНЗІКИ

Проведено огляд популярних технологій та інструментів для проведення мережевої форензіки. Описані архітектурні особливості інструментів, виділені основні переваги та недоліки з точки зору функціональності та зручності використання.

The review of popular technologies and tools for network forensic. We describe the architectural features of the tools, the main advantages and disadvantages in terms of functionality and ease of use.

Вступ

Використання Інтернету різко зросло в останні десять років. По мірі збільшення числа людей, що використовують Інтернет посилюється, кількість незаконної діяльності, такої, як крадіжка даних, крадіжки особистих даних, тощо, що збільшуються в геометричній прогресії. Ідентифікація та аналіз подібних випадків є сферою форензіки.

Форензіка (комп'ютерна криміналістика) займається збором і аналізом даних з комп'ютерних систем, мереж, комунікаційних потоків та зберігання інформації в порядку, допустимого в суді [1, 2]. З самого початку, цифрову та мережеву форензіку розглядали як тісно пов’язані технології, але насправді, вони дуже відрізняються. Цифрова форензіка розвивається значною мірою завдяки потребам силових структур і повинна отримати достовірні (вагомі) докази для розкриття кримінальних злочинів. Мережева форензіка розвинулась у відповідь на хакерські загрози і має тісний зв’язок з архітектурою безпеки, включаючи файерволи, блокування та фільтрування портів, оцінку загроз та нагляд, виявлення втручань та попередження втрати даних.

До найбільш загальних причин застосування мережевої форензіки відносять:

• відновлення даних у випадку збоїв обладнання чи програмного забезпечення;

• аналіз комп’ютерних систем після збоїв;

• отримання інформації про те, як працюють комп’ютерні системи з метою знаходження помилок, оптимізації їхньої роботи;

• збір та аналіз пакетів даних, які передаються у даний момент, з метою визначення та попередження небезпечних атак;

• збір інформації для використання в суді;

• отримання додаткової інформації про атаки типу *“0-day”*, особливо через використання honeypots та honeynets [3].

Цей перелік є далеко не повним і лише поверхнево відображає те, що може робити мережева форензіка у рамах оцінки ризику та відновлення інформації.

Деякі вторгненнядуже важко виявити, і, відповідно, проаналізувати – наприклад, просте сканування порту може містити серйозну приховану атаку на життєво важливі ресурси системи. Аналіз вторгнення та збір вагомих з точки зору форензіки даних, мають за мету отримати відповідь на наступні питання:

- хто генерує (вхідний) вторгнення чи їх (вихідну) передачу даних?
- яке обладнання та сервіси були залучені при отриманні доступу?
- звідки прийшло вторгнення і на які частини інфраструктури це вплинуло?
- що привело до можливості атаки – обмеження чи слабкі сторони вхідних чи вихідних механізмів безпеки?

Процес аналізу у реальному часі передбачає збір, збереження та відслідковування даних, а потім відновлення системи, все під час постійного сканування трафіку та журналів (логів). Як показано на рис.1., процес відновлення починається з забезпечення безпеки і потім продовжується до форензійного аналізу – хто здійснює атаку і звідки, далі система працює по циклу.

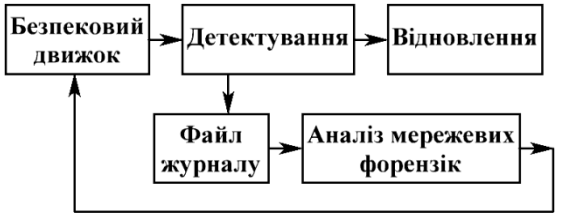

Рис. 1. Процес форензійного аналізу мережевого трафіку у реальному часі.

1. Загальний стан мережевої форензіки

1.1. Еволюція мережевої форензіки.

Спеціалісти у області цифрової та мережевої форензіки вимагають нових інструментів і технологій насамперед тому, що вектори атак переходять у нові сфери, такі як хмарні та соціальні мережі.

Декілька відкритих інструментів доступні для загального форензійного аналізу відкритих портів, підключених дисків та відкритих чи підключених зашифрованих файлів на "живих" (онлайн) комп'ютерних системах. На сьогодні доступні такі відкриті інструменти як: *Sleuth Kit* [4]; *Scalpel* [5]; *Digital Evidence and Forensics Toolkit Linux* [6]; так і комерційні продукти: *EnCase* [7]; *Forensic ToolKit* [8]; *Helix* [9]

1.2. Деякі важливі особливості мережевої форензіки

Традиційно, дослідники здійснювали комп'ютерну форензіку на збережених чи статичних даних – наприклад, зміст файлів чи зображень та жорстких дисках. Але в останні роки посилилась важливість аналізу систем «вживу» - дослідження мережевого трафіку в той момент, коли він виникає.

Останні роботи з мережевої форензіки роблять ще один крок уперед, фокусуючись на захопленні пакетів «вживу», так як пакети, як правило, зберігаються після надходження до свого адресата. Інший вид захоплення «вживу» фокусується на атаках, як не залишають слідів на жорсткому диску комп'ютера, так як нападники лише виявляють (зчитують) інформацію з оперативної пам'яті комп'ютера, включаючи коди (ключі) доступу.

Мережева форензіка займається моніторингом мережевого трафіку з метою визначення наявності аномалій, а також чи ці аномалії означають атаку і чи можуть привести до неї. Метою є визначення природи атаки, її захоплення, збереження таким чином, щоб це можна було використати для аналізу (форензіки), аналізу і, нарешті, представлення її у деякій візуальній формі. Так як нападник може видалити всі файли журналів на скомпрометованому хості, мережеві докази можуть бути єдиним матеріалом для проведення форензік аналізу.

На відміну від цифрової форензіки, яка отримує інформацію з комп'ютерних дисків та інших пристроїв збереження інформації, мережева форензіка добуває і трафік і інформацію про те, які порти використовуються для доступу до мережі. Часто, слідчі та «противники»використовують однакові інструменти: одні для того, щоб створити інцидент, інші для того, щоб дослідити його. На сьогодні доступні: *Wireshark[26], TCPDum*p[25]; *NetScanTools Pro toolkit [28]*.

Інколи можливо прослідкувати атаку до її джерела – або, принаймні, до *ISP* атаки – під час здійснення атаки, але у багатьох випадках такий аналіз здійснюється після події. Основним аспектом «живої» мережевої форензіки є можливість збору інформації з мережі достатньо швидко для того, щоб ця інформація не зникла, а це вимагає дуже швидких процесів та пристроїв вводу/виводу, а також значних сховищ для збереження даних. Найкращим шляхом для захоплення даних є використання змінних проміжків часу, які обмежуються часом очікування атаки. Стійкі атаки навіть на 10Gbps висувають значні вимоги до місткості сховища даних і до обробки мережевих форензік даних, наприклад, 10 Gbps потік трафіку з двогодинним рухливим вікном вимагає 10Тбайт пам'яті, а 20 Gbps потік трафіку з 12-годинним рухливим вікном вимагає 1 Пбайт пам'яті [10]. Через такі розміри, можна зберегти лише зразки пакетів для подальшого аналізу. Обробка даних мережевої форензіки у режимі реального часу вимагає великомасштабних розподілених та паралельних процесингових потужностей, а також гнучкості для кастомізації процесів. Навіть рухоме вікно в декілька годин, яке охоплює трафік за визначений час може вимагати терабайти пам'яті. Найбільша *DDoS* атака на *ISP* була зафіксована у 2010 році і займала майже 100 Gbps [10]. *DDoS* атаки такого розміру за останні 10 років зросли у сотні разів, тому сучасна мережева форензіка може вимагати впровадження паралельної обробки з використанням суперкомп'ютерів або кластерних обчислень.

Важливим є також досягнення прийнятного компромісу між безпекою та продуктивністю. Складні інструменти та технології можуть значно впливати на систему і мати серйозні наслідки

– наприклад, втручання у комунікації, викликані складністю інструментів мережевої форензіки можуть переривати (порушувати, заважати) базовому функціоналу інфраструктури в силу їх значної взаємозалежності.

1.3. Загальні інструменти і технології

Інструменти, які допомагають у мережевій форензіці, дуже різні: деякі з них - це просто сніфери пакетів, тоді як інші можуть вивчати те, як люди друкують, деякі використовують *мепінг* - визначення місцезнаходження, проходження електронних листів, та інші. У **таблиці** подано зведену таблицю деяких інструментів, які широко застосовуються у процесі мережевої форензіки, а також їх характеристики.

Не можна сподіватися, що один інструмент буде достатнім для будь-якого дослідження, скоріш за все, буде використовуватись комбінація інструментів. Наприклад, якщо аналізується трафік і дослідник розуміє природу шкідливого трафіку, то інструменти для UNIX – Ngrep, TCPDump або Omnipeek будуть достатніми, але коли дослідження проводяться за допомогою машини аналізу трафіку, потрібні будуть такі інструменти як WireShark, NetMiner, DriftNet або Xplico.

Таблиця.

Інструменти, що застосовуються у процесі мережевої форензіки, і їх характеристики.

Інструмент	***Особливості та переваги***	***Атрибути****
Airmon-ng [12]	Набір програм, призначених для виявлення бездротових мереж, перехоплення переданого через бездротові мережі трафіку, аудиту WEP і WPA / WPA2-PSK ключів шифрування, у тому числі пентеста бездротових мереж.	F, L, R, C
Argus [13]	Використовується для мережевих форензік для виявлення дуже повільних сканів і підтримок «атак типу 0-day»	F, L
DeepNines [14]	Забезпечує захист контенту і додатків в режимі реального часу на основі ідентифікації мережі, а також основних мережевих форензік	F
Dragon IDS [15]	Забезпечує виявлення мережевих, host вторгнень, використовується для форензійного аналізу мережевих захоплень	F, R, L, C
Driftnet [16]	“Слухає” мережевий трафік і вибирає зображення; використовується в Backtrackv5.	F
EtherApe [17]	Графічний мережевий монітор для захоплення мережевого трафіку	F
Honeyd [18]	Покращує кібербезпеки шляхом надання механізмів для моніторингу трафіку, виявлення загроз та оцінки	F
Kismet [19]	мережевий аналізатор для бездротових мереж стандарту 802.11b. Він дозволяє прослуховувати трафік за допомогою практично будь-яких підтримуваних бездротових мережевих адаптерів, що використовують драйвери Airo, HostAP, Wlan-NG і Orinoco	F
NetDetector [20]	Пристрій для мережевих форензік, спостереження безпеки мережі, виявлення аномалій на основі сигнатур	F, R, C, A
Ngrep [21]	Простий інструмент, для налагодження низькорівневого мережевого трафіку	F
Omnipeek [22]	Низькорівневий аналізатор трафіку для форензійного аналізу	F, L, R
RSA EnVlslon [23]	Забезпечує аналіз мережевого трафіку, управління журналом, спостереження мережевої безпеки, захист від витоків	F, L, R, C, A
Savant [24]	Пристрій для живого форензійного аналізу, нагляду, аналізу мережі та критичних репортажів інфраструктури	F,R
Snort [25]	Мережева система запобігання вторгнень і виявлення вторгнень, здатна виконувати реєстрацію пакетів і в реальному часі здійснювати аналіз трафіку в IP-мережах.	F
TCPDump [26]	Аналізатор мережевих пакетів (працює з командної стрічки), який підтримує експертизи мережевої форензіки	F
Wireshark [27]	Поширений мережевий інструмент для аналізу трафіку; основний інструмент форензійних досліджень.	F
Xplico [28]	Мережевий інструмент форензік, використовується для захоплення даних трафіку; використовується в Backtrack v5	F

**** F: фільтр і накопичувач; L: аналіз журналів; P: переасемблювання потоку даних; C: кореляція даних; A: перегляд на рівні додатків***

1.4. Виклики хмарних обчислень

На сьогодні, хоча багато систем переносяться у хмари, зовсім мало досліджень проводяться з використанням інструментів, процесів та методологій, які необхідні для отримання доказів, які можна буде використовувати у суді (у правовому полі). Більшість розслідувань вимагають одержання доказів з фізичних джерел, тому мережева хмарна форензіка повинна бути спроможна фізично локалізувати дані з, наприклад, визначеним маркером часу і прослідкувати мережеві дані у визначений часовий період, враховуючи правове поле у різних місцях [29].

Хоча поняття "живої" та "мертвої" форензіки все ще існують, хмарні моделі висувають нові виклики тому що мережеві дані часто складно локалізувати, тому їх отримання може бути складним або навіть неможливим. Аналіз без отримання мережевих даних неможливий, тому інструменти мережевої форензіки повинні розвинутися, сформувавши суміш сучасних "живих" та "мертвих" методів збору та аналізу, а також використання нових підходів для знаходження та передбачення доказів на основі евристичної форензіки.

Коли спрацьовують звичні інструменти мережевої форензіки, єдиним аспектом, який можуть змінити хмарні інструменти, це методи збору. Для ситуацій, в яких отримання є складним, нові мережеві інструменти форензік повинні будуть візіалізувати фізичне чи логічне місцезнаходження даних. На додачу до візуалізації, інструменти форензіки повинні будуть використовувати хмари, як дослідницький інструмент у мережевому форензік аналізі. Таким чином, наприклад, мережева форензік-компіляція, що містить дані, які неможливо отримати, повинна бути розміщена у середовищі хмари для евристичного аналізу та аналізу сигнатур.

Це схоже на те, як мережеві форензіки використовують антивірусні машини для того, щоб звести неповні дані в надійну картину, коли кількість даних зростає.

2. Нові горизонти у мережевих вторгненнях

Системи виявлення вторгнень (*IDSs*) моніторять мережеву та системну активність на предмет підозрілої поведінки чи порушень політики безпеки. Деякі системи можуть намагатися зупинити таке вторгнення, але роботи з розвитку можливості динамічно модифікувати правила файерволу під час атак все ще у зародку. Комбінація мережевої форензіки і виявлення вторгнень може бути адекватною для домашніх систем користувача, коли можливе ручне втручання, але більшість систем виявлення вторгнень чи систем попередження фокусуються лише на ідентифікації можливих інцидентів, інформації журнали про підключення (логи) і повідомленні про такі спроби. У цьому є проблема: будь-яка система справжнього розміру, яка підтримує важливі для клієнта дані, повинна включати автоматичну комбінацію аналізу вторгнень з мережевим форензік аналізом підключень (логів), а також динамічний зворотній зв'язок для того, щоб модифікувати правила доступу при виникненні атак у реальному часі.

Деякі нападники вивчають мережу перед тим, як проводити атаку. Складні системи виявлення вторгнень повинні бути спроможними передбачати атаку, або отримати кращі форензійні докази під час (або після) атаки. Але, хоча в останній час досягнутий деякий прогрес систем виявлення вторгнень з розподіленими архітектурами.

На рис.2 показано компоненти, необхідні для забезпечення достатніх з точки зору форензіки систем виявлення та попередження вторгнень. Комбінація таких систем з реактивними файерволами, збереженням трафіку та подальним аналізом забезпечує потужну архітектуру безпеки з погляду форензіки.

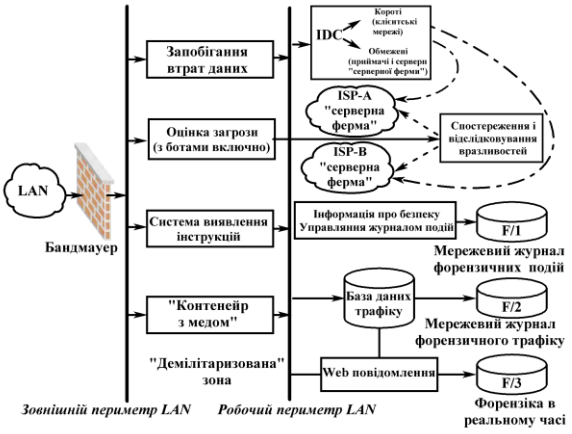

Рис.2. Адаптивний захист мережі, включно з детектуванням інструкцій мережі і журналом форензіки

2.1. Ботнети

Середовище, в якому збільшується база операцій користувачів організації стає більш небезпечною з появою складних та поліморфних шкідливих програм, таких як Conficker, Koobface та Zbot. DDoS-атаки з ботнетів є особливо серйозною глобальною загрозою. Ботнети зараз можна арендувати у кримінальних синдикатів і можуть бути використані для формування DDoS атак, а

також для збору особистих даних і фінансових доручень тощо.

Процес мережевої форензіки повинен бути спроможним виявити сканування поза межами файерволу і потім використати ці дані для інформування системи SIEM (*Security information and event management* - управління інформацією про події безпеки), що включає аналітичні інструменти мережевої форензіки. Прогресивна оцінка загроз вимагає від моніторів програмного забезпечення включати повідомлення про небезпеку коли виникає незвичний часовий профіль IP адреси всередині безпечного периметру, що свідчить про потенційне втручання ботнету.

Мережева форензіка може відігравати ключову роль в оцінці загроз атак ботнетів тому що SIEM система не лише управляє лог-файлами так, що це можна використати у форензійному розслідуванні, але також зберігає рухоме вікно лог-даних як доказ потенційної діяльності у майбутньому. Адаптивний зворотній зв'язок у реальному часі, який є результатом цього аналізу, може попереджувати або мінімізувати потенційні атаки у реальному часі через адаптацію правил файерволу.

2.2. Бездротові мережі

Бездротова форензіка, підрозділ мережевої форензіки, пропонує методологію і інструменти, необхідні для збору та аналізу бездротового мережевого трафіку. Ця нова сфера має деякі технології, спільні з фіксованими мережами, але є і деякі відмінності. Оцінка бездротових мереж з точки зору комп'ютерної форензіки допомагає зрозуміти поточний стан використання (неправильного використання) бездротових каналів, а також різноманітних інструментів та технологій, що використовуються для ідентифікації, збереження та аналізу. Деякі комерційні дослідники на ринку фіксованої мережевої форензіки заявляють про те, що вони можуть працювати і з бездротовими мережами, принаймні з WLAN [30]. Бездротова мережева форензіка потребує ці інструменти для аналізу 802.11 заголовків і відповідних потоків даних протоколу. З точки зору відкритого програмного забезпечення, немає відомих альтернатив, присвячених бездротовому мережевому форензік аналізу.

2.3. Провали (Sinkholes)

Sinkhole – це інструмент безпеки, який має можливість отримувати, аналізувати і зберігати трафік атаки у вигляді, який підходить для форензіки. З самого початку, ISP використовували *sinkholes* для відведення трафіку атаки від клієнта; в останній час, вони використовують їх для моніторингу атак, виявлення сканування з інфікованих машин, проведення форензік аналізу, і загального моніторингу підозрілої діяльності. На рис.3 показано, як *sinkholes gateway* роутер може бути використаний для передачі атаки на sinkholes цільовий роутер через світч для базових Wireshark and TCPDump shiffing, виявлення вторгнень та форензік аналізу.

На Рис.3 представлено, як *sinkhole* може бути використаний для моніторингу внутрішньо генерованого розмножения «черв'яків».

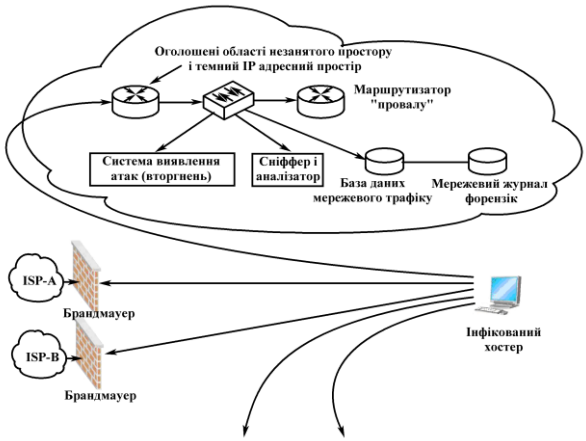

Рис. 3. Моніторинг та аналіз поширення «черв'яка», використовуючи "провали". У цьому прикладі, заражений вузол сканує інші цілі для інфікування. Так як така ситуація виникла у внутрішньому трафіку, що призначений для мережевої форензіки, провал може виявити скануючи діяльність черв'яка.

У цьому прикладі, інфікований хост сканує інші комп'ютери для інфікування. Він притягує будь-який внутрішній трафік на *bogon* адресу чи темну IP адресу. (bogon це IP-адреси, які не повинні зустрічатися в таблицях маршрутизації в Інтернет. Цим терміном описуються зарезервовані діапазони адрес, які не повинні використовуватися, групи адрес, які не виділені офіційно, а також приватний діапазон адрес; темна IP-адреса – має місце, але не використовується). Відповідно, у *sinkholes* можна виявити те, що «черв'як» сканує. Моніторинг темних IP адрес важливий, тому що майбутні «черв'яки» можуть бути написані так, щоб ігнорувати таке блокування адрес.Крім цього, *sinkhole* може видалити інший шум з мережі, наприклад, відображений чи зворотнього трафіку, який відображає початок атаки спеціальних інструментів «черв'яків» для DDoS атаки. *Backscatter* трафік може виникнути у результаті широкомасштабної DDoS атаки, яка використовує хибне джерело адреси.

Значне зростання *backscatter* трафіку може бути першим показником нової версії «черв'яка». Запис (логи) подій, які можна використати у форензіці та збереження мережевого трафіку є при цьому надзвичайно важливими.

3. Форензіка у нових мережах

Мережева форензіка відіграє важливу роль у нових сферах, що стосуються соціальних медіа, обміну даними і цифровими зображеннями, візуалізації даних.

3.1. Соціальні мережі

Сайти соціальних мереж, такі як "ВКонтакте", "Facebook", "Google+", "Одноклассники.ru", "Facebook", "Linkedin", "Вконтакте", "Instagram", та інші значно поширилися за останні роки, але так, як успіх таких сайтів залежить від кількості користувачів, існує тиск на розробників розробляти системи, які заохочують поведінку, яка збільшує як число користувачів, так і їхню взаємодію. Безпека не була при цьому на першому місці, що привело до виникнення невід'ємних ризиків безпеки.

Очевидно, існує необхідність в розробці мережевої форензіки у цій сфері, але на сьогодні доступні лише традиційні цифрові та мережеві інструменти форензіки.

3.2. Data mining

Форензік-профілі можуть бути створені з використанням технологій накопичення даних, які надають можливість виявляти релевантні тенденції, таким чином генеруючи профілі з великої кількості даних. Хоча вже є значна кількість робіт у сфері видобування та аналізу цифрових свідчень з фізичних пристроїв, таких як жорсткі диски, набагато менше уваги приділялося накопичувачам даних на портабельних пристроях пам'яті, таких як флеш-накопичувачі, телефони, цифрові камери, FRID, компактні диски та iPods [31].

3.3. Цифрові зображення та візуалізація даних

Дослідники розробили чисельні сучасні інструменти для допомоги у проведенні цифрових кримінальних розслідувань. Але, цифрові розслідування стають більш складними та вимагають все більше часу через те, що залучаються значні обсяги даних. Візуалізація отриманих з таких розслідувань даних є новою сферою, що розвивається і має потенціал подачі значних обсягів даних у випадках, коли масштабність, складність та обсяги не дозволяють проводити ручний аналіз [32].

Візуалізація даних – це графічна інтерпретація широкомасштабних даних, що особливо доречно для отримання цілісної картинки і встановлення важливих аспектів всередині набору даних. Це корисно у мережевій форензіці тому що дані, які використовуються у цифрових розслідуваннях, часто значні за розміром, багатовимірні та складні. Відповідно, отримання цілісного бачення може допомогти цифровим слідчим отримати краще розуміння даних і визначити важливі аспекти з тим, щоб полегшити відновлення необхідних цифрових доказів.

Висновки

Правоохоронні органи намагаються попередити такі атаки і схопити нападників використовуючи останні інструменти безпеки та форензіки. Але, ці роботи вимагають розробки та впровадження архітектур, які є безпечними та дають можливість формувати форензік-докази. Обмеження ресурсів є проблемою, і процес розвитку інноваційних рішень потребуватиме включення розробників програмного забезпечення, постачальників інструментів безпеки, противірусних організацій, постачальників інструментів форензіки, інтернет провайдерів та комунікаційні компанії. Це також потребуватиме зусиль кінцевих користувачів.

Незалежно від того, які конкретно інструменти використовуються, розробники повинні вбудовувати можливості форензіки в системи безпеки. Ботнет-атаки, наприклад, генерують логи трафік і їх відслідковування у режимі реального часу вимагає прогресивної оцінки загрози, оскільки атаки рухаються по системі. Визначення того, як нападник отримав доступ чи як інформація "витекла" з організації з одночасним кількісним оцінюванням масштабів і впливу атаки в момент її здійснення є основою надійної безпеки та процесу форензіки

СПИСОК ЛІТЕРАТУРИ

1. *Kessler G.* Online Education in Computer and Digital Forensics// Proceedings of the 40th Hawaii International Conference on System Sciences, 2007.
2. *Федотов Н.Н.* Форензіка - компьютерная криминалистика – М.: Юридический мир, 2007.
3. *Yasinsac A.. Manzano Y.* Honeytraps, A Network Forensic Tool // Proceedings of the 6th World Multiconference on Systemics, Cybernetics, and Informatics (SCI 02), July 15-19, 2002

4. Офіційний сайт Sleuth Kit [Электронный ресурс] // Режим доступу: www.sleuthkit.org
5. Офіційний сайт Scalpel [Электронный ресурс] // Режим доступу: www.digitalforensicssolutions.com/Scalpel
6. Офіційний сайт Digital Evidence and Forensics Toolkit Linux [Электронный ресурс] // Режим доступу: www.deftlinux.net
7. Офіційний сайт EnCase [Электронный ресурс] // Режим доступу: www.guidancesoftware.com
8. Офіційний сайт Forensic ToolKit [Электронный ресурс] // Режим доступу: www.accessdata.com
9. Офіційний сайт Helix [Электронный ресурс] // Режим доступу: www.e-fense.com/products.php
10. *Miller C., Glendowne D., Dampier D., Blaylock K.* (2014). Forensicloud - An Architecture for Digital Forensic Analysis in the Cloud. Journal of Cyber Security and Mobility. 3(3), 231-262.
11. Офіційний сайт Aircrack-ng [Електронний ресурс] // Режим доступу: http://aircrack-ng.org/
12. Офіційний сторінка програми Argus [Електронний ресурс] // Режим доступу http://www.qosient.com/argus/index.shtml
13. Офіційний сторінка програми DeepNines [Електронний ресурс] // Режим доступу http://www.deepnines.com/
14. Офіційний сторінка програми Dragon IDS [Електронний ресурс] // Режим доступу http://www.intrusion-detection-system-group.co.uk/dragon.htm
15. Офіційний сторінка програми Driftnet [Електронний ресурс] // Режим доступу http://linux.softpedia.com/get/System/Networking/Driftnet-15905.shtml
16. Офіційний сторінка програми EtherApe [Електронний ресурс] // Режим доступу http://etherape.sourceforge.net/
17. Офіційний сторінка програми Honeyd [Електронний ресурс] // Режим доступу http://www.honeyd.org/index.php
18. Офіційний сторінка програми Kismet [Електронний ресурс] // Режим доступу http://www.kismetwireless.net/
19. Офіційний сторінка програми NetDetector [Електронний ресурс] // Режим доступу https://niksun.com/product.php?id=4#go3
20. Офіційний сторінка програми ngrep [Електронний ресурс] // Режим доступу http://ngrep.sourceforge.net/
21. Офіційний сторінка програми Omnipeek [Електронний ресурс] // Режим доступу http://www.wildpackets.com/products/omnipeek_network_analyzer
22. Офіційний сторінка програми RSA EnVlslon [Електронний ресурс] // Режим доступу http://www.emc.com/securlty/rsa-envlslon.htm
23. Офіційний сторінка програми Savant [Електронний ресурс] // Режим доступу http://www.intrusion.com
24. Офіційний сторінка програми Snort [Електронний ресурс] // Режим доступу https://www.snort.org/
25. Офіційний сторінка програми TCPDump [Електронний ресурс] // Режим доступу http://www.tcpdump.org/
26. Офіційний сторінка програми Wireshark [Електронний ресурс] // Режим доступу https://www.wireshark.org/
27. Офіційний сторінка програми Xplico [Електронний ресурс] // Режим доступу http://www.xplico.org/
28. Офіційний сторінка програми NetScanTools [Електронний ресурс] // Режим доступу http://www.netscantools.com/
29. NIST (2010) Definition of cloud computing v15, Computer Security Division, Computer Security Resource Center, http://csrc.nist.gov/groups/SNS/cloud-computing/ (18 June 2010).
30. *Raul Siles* Wireless Forensics: Tapping the Air - Part One // Symantec [Электронный ресурс] // Режим доступу: http://www.symantec.com/connect/articles/wireless-forensics-tapping-air-part-one
31. *Sindhu K. K., Meshram B. B.* Digital Forensics and Cyber Crime Datamining // Journal of Information Security, 2012, 3, 196-201 [Электронный ресурс] // Режим доступу: http://dx.doi.org/10.4236/jis.2012.33024
32. *Ken Fowle* Visualising forensic data: investigation to court / Australian Digital Forensics Conference [Электронный ресурс] // Режим доступу: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1095&context=adf

M.M. Ivanchuk, O.E. Ilarionov, S.O. Kudrenko. **Analysis technology and instruments for network forensic.**

М.М. Иванчук, О.Е. Иларионов, С.А. Кудренко. **Анализ технологий и инструментов для сетевой форензики**.

Проведен обзор популярных технологий и инструментов для проведения сетевой форензик. Описанные архитектурные особенности инструментов, выделены основные преимущества и недостатки с точки зрения функциональности и удобства использования