

ОТНОСНО ВЕРИФИКАЦИЯ НА СЦЕНАРИЙ ЗА РАЗУЗНАВАНЕ НА КИБЕРЗАПЛАХИ

Иван Христов, Веселина Гагъмова, Иван Чакъров, Росен Ангелов
Военна академия „Г. С. Раковски“

Резюме: В този доклад авторите представят изследване, насочено към проверката на процедура за киберразузнаване. Основната цел е да се разработи ефективна методика за откриване и анализ на киберзаплахи, насочени към информационните активи на организациите. За постигане на тази цел са използвани възможностите на езика за моделиране Unified Modeling Language. Разработени са диаграми за случаите на употреба, за дейностите и за резултатите от процедурата за киберразузнаване, които детайлно визуализират съответстващия процес. Предложена е експериментална проверка на възможността процедурата за разузнаване на киберзаплахите да доведе до очакваните резултати. За целта е разработен конкретен сценарий за изпълнение на процедурата, включващ подходяща инфраструктура и инструменти за провеждане на експеримент. Резултатите от изследването доказват значителното подобрене на ефективността на киберразузнаването чрез използването на UML. Прилаганият емпиричен подход за верификация на процедурата чрез експеримент доказва потенциала му за адаптиране и прилагане и в други информационни домейни и възможността да бъде приложен за повишаване на сигурността на информационните системи в различни организации.

Ключови думи: киберразузнаване; процедура; проверка; техники; тактики

ВЪВЕДЕНИЕ

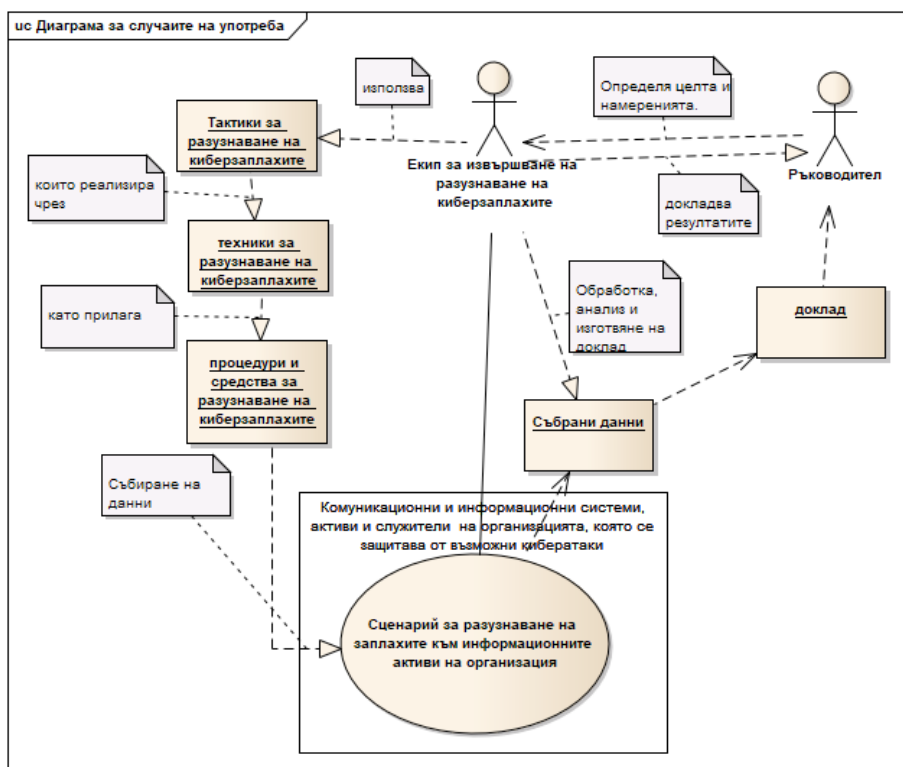
Темата за ефективното киберразузнаване е изключително актуална поради нарастващата честота и сложност на киберзаплахите, особено за организациите в сферата на сигурността и отбраната. Съвременната информационна среда се характеризира с бърза еволюция на атакуващите техники, включително автоматизирани инструменти, социално инженерство и целенасочени атаки срещу критична инфраструктура. Способността на организациите да идентифицират, анализират и неутрализират заплахи в реално време, е от решаващо значение за поддържане на оперативната устойчивост и гарантиране на националната сигурност. Разработването и верификацията на надеждни методики за киберразузнаване, базирани на утвърдени модели и подходи, представляват наложителна и стратегически значима задача.

В настоящия доклад са предложени процедура за разузнаване на киберзаплахи към информационните активи на дадена организация и постановка за нейната верификация.

В изследването е избрано използването на езика за моделиране Unified Modeling Language (UML), който предлага стандартизирани графични средства за визуализация, специфициране и документиране на сложни процеси и

системи. Използването на UML позволява ясно структуриране и анализ на сценарии за киберразузнаване, като улеснява комуникацията между технически и нетехнически участници в процеса.

Диаграмата на фиг. 1 илюстрира основните участници, действия и взаимодействия в рамките на предложената процедура. Тя визуализира как различните роли (например „Екип за извършване на разузнаване на киберзаплахите“, „Ръководител“) взаимодействат с функционалните компоненти на системата за киберразузнаване. Този тип диаграми е особено полезен за дефиниране на обхвата на системата на стратегическо ниво и изясняване на функционални изисквания на нотацията (use case) „Сценарии за разузнаване на заплахите към информационните активи на организация“.



Фиг. 1. Диаграма на случая на употреба (use case) „Сценарии за разузнаване на киберзаплахите“

МЕТОДОЛОГИЯ НА ИЗСЛЕДВАНЕТО

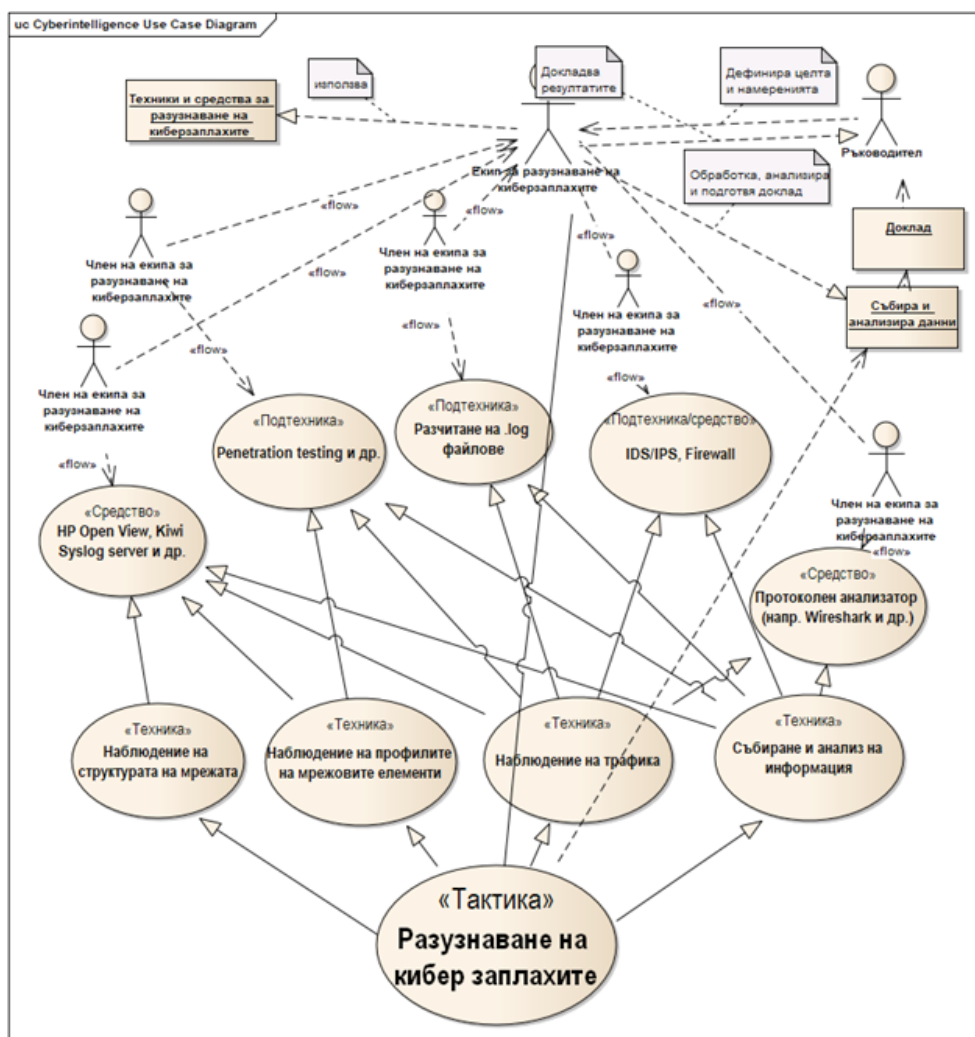
Самата процедура като тактика включва прилагане на редица техники, под-техники и средства, конкретизирани във фиг. 2 като:

- ▷наблюдение на структурата на мрежата с използване на софтуерния продукт HP Open View (Hewlett-Packard 2002; 2003) или Kiwi Syslog Server;
- ▷наблюдение на профилите на мрежовите елементи;

▷наблюдение на натовареността на мрежата, тестване за възможности за пробиви и анализ на .log файлове или съобщенията на мрежовите устройства, устройства за защита на мрежите, като например Intrusion Detection/Intrusion Prevention Systems (IDS/IPS);

▷събиране и анализ на информация от работно място на служител по киберсигурност, т.е. анализатор по киберсигурност, с помощта на редица софтуерни инструменти, например WireShark, Snort и др.;

▷Друпи (Kostadinov 2023; Krumova 2022; Vasileva 2020).

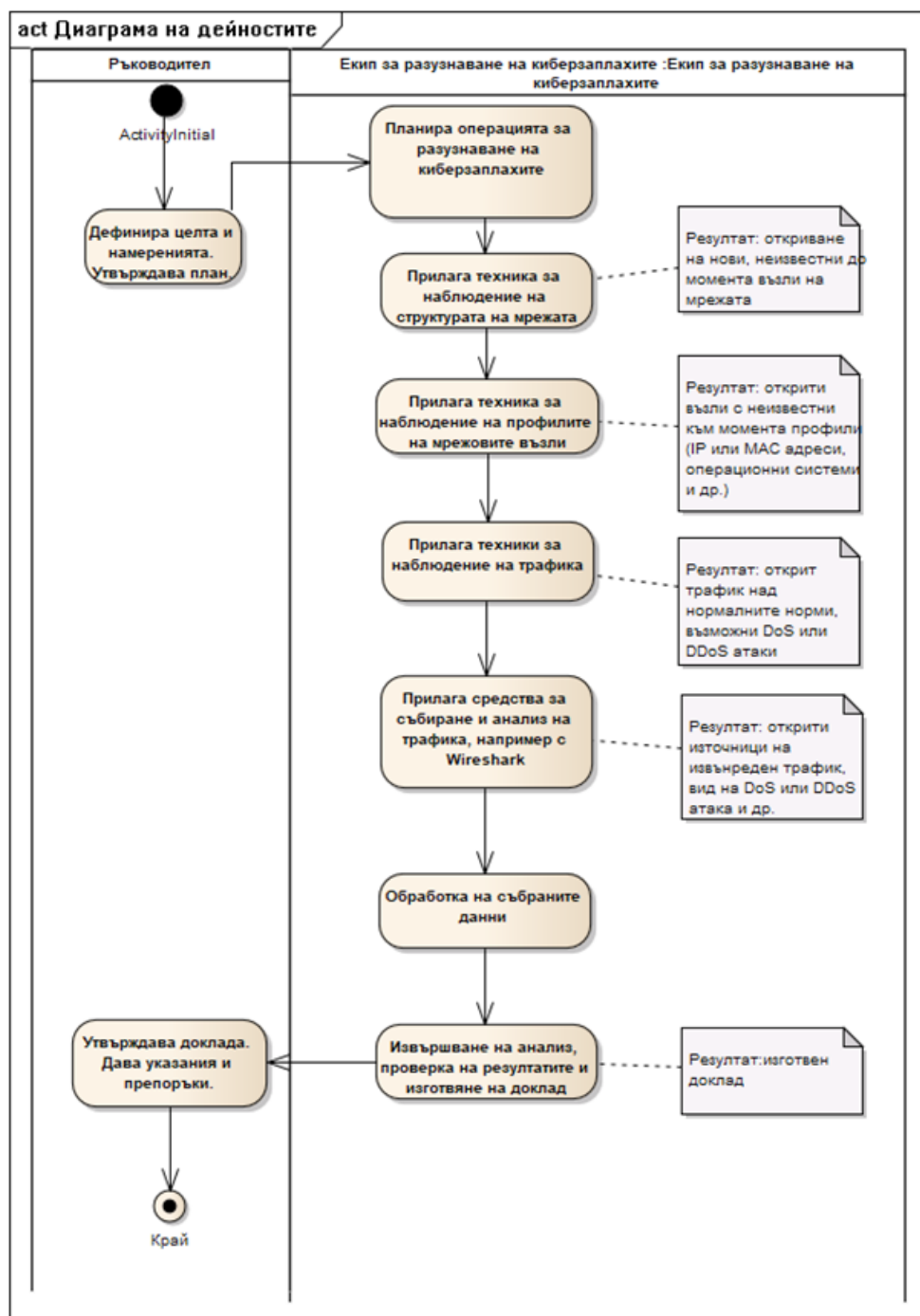


Фиг. 2. Диаграма на случаи на употреба (use case) на някои конкретни техники и средства при изпълнение на тактиката „Разузнаване на киберзаплахите“

РЕЗУЛТАТИ

На фиг. 3 са показани някои от предполагаемите резултати, които биха се получили вследствие на прилагане на техниките и средствата за разузнаване на киберзаплахите.

Тъй като тактиката „Разузнаване на киберзаплахите“ включва последователност от действия, е целесъобразно тази тактика, която се разглежда и като функционалност (use case), да бъде представена като процес (Krumova 2024). За целта се използва методологията на езика Unified Modeling Language (UML), широко прилагана в софтуерното инженерство. Техниките и средствата за разузнаване на киберзаплахите, както и предполагаемите резултати, които биха се получили вследствие на прилагането им, са представени чрез разработване на диаграма на дейностите (Activity diagram) на езика UML.



Фиг. 3. Процес на разузнаване на киберзаплахите с очаквани резултати, представени чрез диаграма на дейностите (Activity diagram) на езика UML

В настоящата разработка се предлага извършване на експеримент с цел да се докаже, че с представената на фиг. 2 процедура може да бъдат постигнати показаните на фиг. 3 резултати посредством използване на известни методи и средства. Приложеният емпиричен метод за верификация успешно може да бъде приложен по аналогичен начин за верификацията на техники и процедури в други информационни домейни.

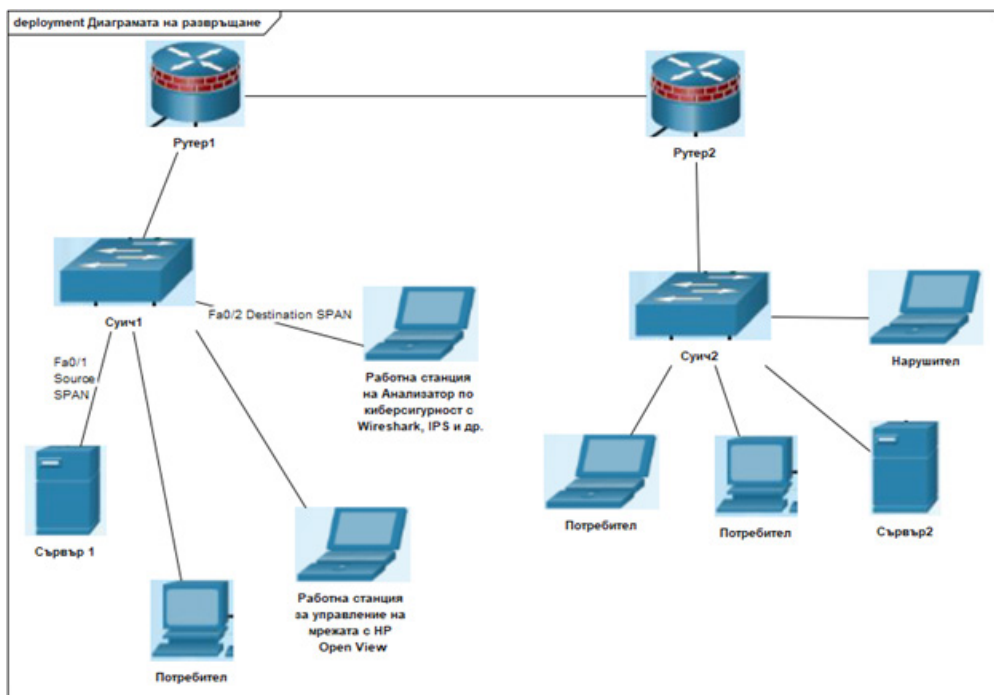
Основни принципи на верификацията са следните (Cheredaev 2024):

- данните трябва да бъдат потвърдени по експериментален път и да не противоречат на общоприети факти;
- данните трябва да бъдат познаваеми, не абстрактни;
- информацията трябва да бъде обективна.

Верификацията се използва за проверка на факта, че система, програма или апаратно устройство в действителност притежава очакваните свойства и изпълнява съответните функционалности.

За извършването на експеримента е създаден сценарий, като е разработена опитна постановка от компютърна мрежа, която симулира локално-регионална мрежа. Тя включва три отделни сегмента – две локални мрежи и връзката между тях през рутери (фиг. 4). Един от критичните информационни ресурси за тази мрежа е Сървър 1. Предполага се, че към Сървър 1 може да има кибератака. За случая се провежда атака с използване на инструмента Advanced IP scanner (Advanced IP Scanner, n.d.).

Очаква се с предложената процедура да бъдат открити както тази атака, така и нейният източник.

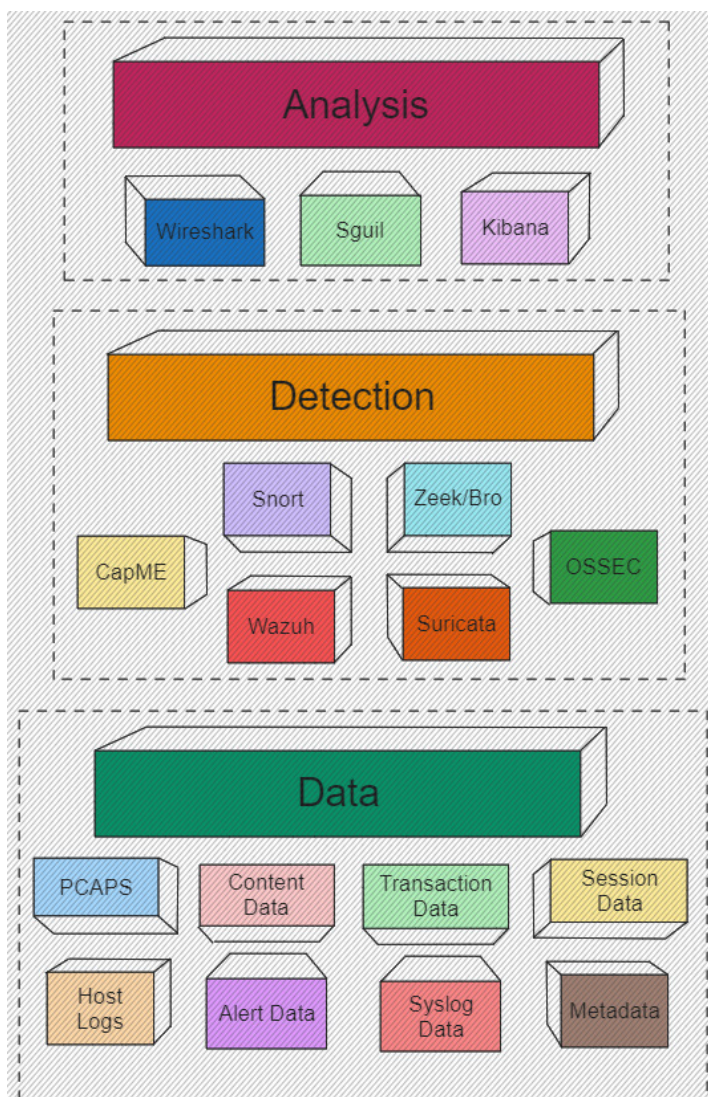


Фиг. 4. Диаграма на развързване (Deployment diagram) на опитната постанова за верификация на процедурата за разузнаване на киберзаплахите

Наблюдението и управлението на мрежата се извършват с използване на софтуерния продукт HP OpenView, инсталиран на работна станция за управление на мрежата.

Анализаторът по киберсигурност трябва да бъде снабден с устройство лаптоп или настолен компютър със специализирани инструменти за събиране на данни, откриване на опити за пробив на мрежата и анализ на данните. Като вариант се предлага използването на примерна трислойна среда – машината Security Onion. Нейната трислойна архитектура е представена на фиг. 5. Тя предоставя възможности за специализирани инструменти, които извършват дейностите по събиране на данни (слоей 1), откриване на опити за пробив на мрежата (слоей 2) и анализ на данните (слоей 3). Security Onion е безплатна и отворена платформа за откриване на киберзаплахи, мониторинг на корпоративната сигурност и управление на случаите, изследване на регистрационни файлове и събиране на данни. Тя включва и други инструменти, като osquery, CyberChef, Elasticsearch, Logstash, Kibana, Suricata и Zeek [<https://github.com/Security-Onion-Solutions/securityonion>].

Security Onion може да се инсталира като самостоятелна инсталация или като сензорна и сървърна платформа. Някои компоненти на Security Onion са собственост на корпорации, като Cisco и Riverbend Technologies, но са достъпни и като такива с отворен код.



Фиг. 5. Трислойна архитектура за Security Onion

Събирането и обработката на информацията в разглеждания случай се извършват от работно място на анализатор по киберсигурността с протоколен анализатор Wireshark.

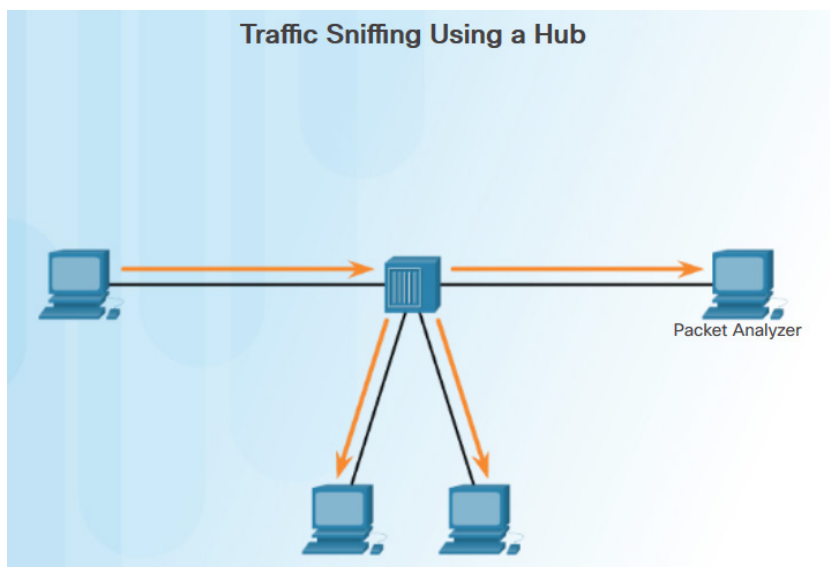
Пакетният анализатор може да бъде ценен инструмент, който да помогне за наблюдение и отстраняване на проблеми в мрежата. Анализаторът на пакети (известен също като снифер на пакети или снифер за трафик) обикновено е софтуер, който улавя пакети, влизащи в и излизащи от мрежовата интерфейсна карта (Network Interface Card – NIC). Невинаги е възможно или желателно да има анализатор на пакети на устройството, което се наблюдава. Понякога

е по-добре той да е на отделна работна станция, предназначена за улавяне на пакетите.

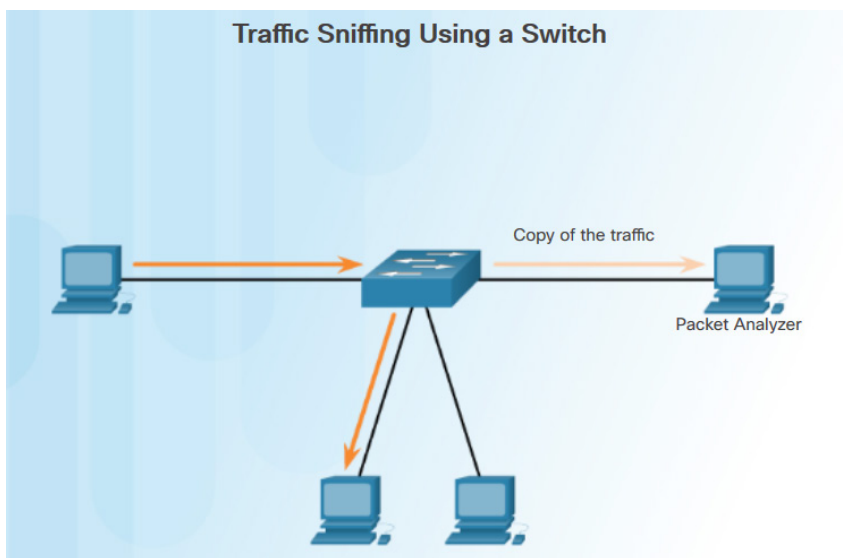
Когато LAN мрежите бяха базирани на хъбове, свързването на пакетен анализатор беше просто, както е показано на фиг. 6. Когато хъбът получи Ethernet рамка, битовете, получени на един порт, се изпращат на всички останали портове с изключение на порта, на който е влязла рамката. Анализаторът на пакети е просто свързан към хъба и може да приема целия трафик, свързан към този хъб.

Съвременните локални мрежи са по същество комутирани мрежи. Превключвателят на слой 2 (суич) попълва таблицата с MAC адреси, известна също като таблица за препращане на слой 2, въз основа на MAC адреса на източника и входящия порт на Ethernet рамката. След като бъде изградена тази таблица за препращане, превключвателят препраща трафика, предназначен за MAC адрес, директно към съответния порт. Това филтриране не позволява на анализатор на пакети, който е свързан към друг порт, да получава едноадресния трафик.

Дублирането на портове (port mirroring) е функция, която позволява на комутатор да направи дублирано копие на входящ Ethernet кадър и след това да го изпрати на порт с прикачен пакетен анализатор за улавяне. Оригиналната рамка се препраща по обичайния начин. Пример за дублиране на портове е илюстриран на фиг. 7.



Фиг. 6. Свързване на анализатор на пакети към хъб



Фиг. 7. Свързване на анализатор на пакети към свич

Функцията Switched Port Analyzer (SPAN) на комутаторите на Cisco изпраща копия на рамката (frame), влизаща в даден порт, към друг порт на същия комутатор. Хост, работещ с анализатор на пакети или IDS, може да е включен в другия край на този порт.

Изходният порт е порт, който се следи за анализ на трафика. SPAN отразява трафика, който е получен и/или изпратен на един или повече портове източник към порт дестинация за анализ. Портовете Layer 2 и Layer 3 могат да бъдат конфигурирани като SPAN източници. Трафикът се копира към порта на дестинацията (наричан още монитор).

Връзката между портове източник и порт дестинация се нарича SPAN сесия. В една сесия може да се наблюдават един или множество източникови портове. На някои комутатори на Cisco може да се копира сесиен трафик към повече от един дестинационен порт.

Функцията SPAN на комутаторите на Cisco изпраща копие на всеки кадър, влизащ в порта източник, към порта дестинация и към анализатора на пакети или IDS.

Сървър 1 е свързан към F0/1, а работното място на анализатора по киберсигурност е свързан към F0/2 (фиг. 4). Целта е да се улови целият трафик, който се изпраща на или получава от Сървър 1 на порт F0/1, и да се изпрати копие от тези кадри към анализатора на пакети на порт F0/2. SPAN сесията на комутатора ще копира целия трафик, който изпраща и получава на порта източник F0/1 към порта дестинация F0/2.

ИЗВОДИ

Представянето на сценария за разузнаване на киберзаплахите като процедура позволява систематичното описание и прилагане на редица подтехники и средства и очакваните резултати от тях.

Предложеният сценарий и разгледаните средства и инструменти могат успешно да верифицират описаната процедура на техниката за разузнаване на киберзаплахите.

Анализът на процедурата налага извода, че е необходимо изграждане на компетенции у потребителите, за да се определи кога и кой инструмент е целесъобразно да бъде използван.

Предположеният подход за верификация има интердисциплинарен характер, тъй като успешно може да бъде приложен за други области поради факта, че верификацията на други техники и процедури може да бъде представена по аналогичен начин.

ЗАКЛЮЧЕНИЕ

В заключение, настоящото изследване представя разработка и проверка на процедура за киберразузнаване, насочена към идентифициране на киберзаплахи към информационната инфраструктура на организацията. Методологията на езика за моделиране Unified Modeling Language (UML) е приложена успешно, като са създадени диаграми за случаите на употреба, дейностите и резултатите на процедурата. Допълнително е предложен сценарий със съответстваща инфраструктура и са подбрани подходящи инструменти за провеждане на експеримент с цел последваща верификация на процедурата с подходящ софтуерен продукт. Резултатите от изследването подчертават значението на систематичния подход към киберсигурността и предоставят основа за бъдещи подобрения и оптимизации в областта на киберразузнаването.

Благодарности: Докладът е осъществен благодарение на финансиране от Министерството на образованието и науката в изпълнение на Националната стратегия за развитие на научните изследвания 2017 – 2030 по Национална научна програма „Сигурност и отбрана“, приета с решение на Министерския съвет № 731 от 21 октомври 2021 г.

ЛИТЕРАТУРА

ЧЕРЕДАЕВ, Василий, 2024. *Верификация: что это простыми словами, принципы и примеры*. Available from: <https://zvonobot.ru/blog/verifikatsiya-chto-eto-prostymi-slovami-printsipy-i-primery>.

КРУМОВА, К., 2022. *Аспекти на мрежово-центричните операции и сигурността на информацията в тях*. Годишна научна конференция „110 години традиция, качество, престиж“, Военна академия „Георги Стойков Раковски“, София.

КРУМОВА, К., 2022. *Анализ на аспектите на оперативна съвместимост на КИС в коалиционна среда*. „Съвременни аспекти на сигурността – предизвикателства, под-

ходи, решения“ – годишна студентска научна сесия на факултет „Командно-щабен“, Военна академия „Георги Стойков Раковски“, София, с. 329 – 338. ISSN 2738-7526.

КРУМОВА, К., 2023. Анализ на концепцията за мултидомейнови операции и интегриране на нововъзникващата идея за „боен облак“. *АзБуки, Професионално образование*, кн. 2, с. 179 – 185. ISSN 1314-555X (Print), ISSN 1314-8567 (Online).

КРУМОВА, К., 2024. *Киберектите в операции – проекция на сила в киберпространството*. Научна конференция с международно участие „20 години България в НАТО и НАТО в България“, 2 – 4 април 2024 г., Военна академия „Георги Стойков Раковски“, София, с. 346 – 356. ISBN (online) 978-619-7711-52-3.

REFERENCES

- ADVANCED IP Scanner (Н.А.). Available from: <https://www.advanced-ip-scanner.com/>.
- CHEREDAEV, V., 2024. *Verifikacija: chto jeto prostymi slovami, principy i primery*. Available from: <https://zvonobot.ru/blog/verifikatsiya-chto-eto-prostymi-slovami-printsipy-i-primery>.
- HEWLETT-PACKARD, 2002. *Administrative Guide HP Open View*. San Francisco.
- HEWLETT-PACKARD, 2003. *OpenView Training Course. HP OpenView Network Node Manager on Windows and UNIX, Essentials of Use and Administration. Student Workbook*. San Francisco.
- KOSTADINOV, C., D. M., 2023. Actions of structures from the energy sector in conditions of a cyberattack. *INTED Proceedings*, pp. 591 – 596. DOI:10.21125/inted.2023.
- KRUMOVA, K., 2022. *Aspekti na mrezhovo-tsentrirnite operatsii i sigurnostta na informatsiyata v tyah*. Godishna nauchna konferentsia „110 godini traditsia, kachestvo, prestizh“, Voenna akademia „Georgi Stoykov Rakovski“, Sofia.
- KRUMOVA, K., 2022. *Analiz na aspektite na operativna savmestimost na KIS v koalitsionna sreda*. „Savremenni aspekti na sigurnostta – predizvikatelstva, podhodi, reshenia“ – godishna studentska nauchna sesia na fakultet „Komandno-shtaben“, Voenna akademia „Georgi Stoykov Rakovski“, Sofia. ISSN 2738-7526.
- KRUMOVA, K., 2023. *Analiz na kontseptsiyata za multidomeynovi operatsii i integrirane na novovaznikvashtata ideya za „boen oblak“*. *AzBuki, Profesionalno obrazovanie*, 2, s. 179 – 185.
- KRUMOVA, K., 2024. *Kiberektite v operatsii – proektsia na sila v kiberprostranstvoto*. Nauchna konferentsia s mezhdunarodno uchastie „20 godini Bulgaria v NATO i NATO v Bulgaria, 2 – 4 April 2024, Voenna akademia „Georgi Stoykov Rakovski“, Sofia, s. 346 – 356. ISBN (online) 978-619-7711-52-3.
- VASILEVA, V., 2020. *Information Sharing Processes in Public Sector Cybersecurity Structures*. 9th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education. Sofia: Publishing Complex – UNWE, pp. 136 – 147. Available from: <http://icaictsee.unwe.bg/past-conferences/ICAICTSEE-2019.pdf>.

ON VERIFICATION OF CYBER THREAT INTELLIGENCE SCENARIO

Abstract: *In this paper, the authors present a study aimed at verifying a cyber intelligence procedure. The main goal is to develop an effective methodology for detecting and analyzing cyber threats targeting organizations' information assets. To achieve this goal, the capabilities of the Unified Modeling Language have been used. Diagrams have been developed for the use cases, for the activities and for the results of the cyber intelligence procedure, which visualize in detail the corresponding process. An experimental verification of the possibility of the cyber threat intelligence procedure to lead to the expected results has been proposed. For this purpose, a specific scenario for implementing the procedure has been developed, including appropriate infrastructure and tools for conducting an experiment. The results of the study prove the significant improvement in the effectiveness of cyber intelligence through the use of UML. The applied empirical approach for verifying the procedure through an experiment proves its potential for adaptation and application in other information domains and the possibility of its application to increase the security of information systems in various organizations.*

Keywords: *cyber intelligence; procedure; verification; techniques; tactics*

Assoc. Prof. Ivan Hristozov, PhD

ORCID iD: 0009-0005-1168-676X

Communication and Information Systems Chair

Command and Staff Faculty

Rakovski National Defence College

Sofia, Bulgaria

E-mail: ihristoz@rndc.bg

Assoc. Prof. Veselina Gagamova, PhD

ORCID iD: 0000-0002-9119-4618

Communication and Information Systems Chair

Command and Staff Faculty

Rakovski National Defence College

82, Evlogi i Hristo Georgievi Blvd.

Sofia, Bulgaria

E-mail: v.gagamova@rndc.bg

Col. Assoc. Prof. Ivan Chakarov, PhD

ORCID iD: 0000-0002-6062-4806

Communication and Information Systems Chair

Command and Staff Faculty

Rakovski National Defence College

82, Evlogi i Hristo Georgievi Blvd.

Sofia, Bulgaria

E-mail: i.chakarov@rndc.bg

Major Rosen Angelov, PhD
ORCID iD: 0009-0002-8920-9574
Communication and Information Systems Chair
Command and Staff Faculty
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
Sofia, Bulgaria
E-mail: r.angelov@rndc.bg