ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

безопасности, таким как атаки Cross-Site Scripting или атаки с внедрением SQL. Кроме того, в ходе дальнейших исследований могут быть изучены потенциальные преимущества использования уязвимых контейнеров в сочетании с другими методами обучения, такими как CTF или симуляции команд красных и синих.

Список использованных источников

1. Mouat, A. (2015). Docker Security. O'Reilly Media.
2. Docker Bench for Security. (n.d.). https://github.com/docker/docker-bench-security (дата обращения:10.03.2023)
3. Twistlock. (n.d.). Docker Security - Best Practices for Your Containerized Environment. https://www.twistlock.com/lp/docker-security-best-practices-for-your-containerized-environment/ (дата обращения:10.03.2023)
4. The Docker Security Playground. (n.d.). https://github.com/giper45/Docker-Security-Playground (дата обращения:12.03.2023)
5. Red Hat. (2021). 10 Docker Image Security Best Practices. https://www.redhat.com/en/blog/10-docker-image-security-best-practices (дата обращения:14.03.2023)

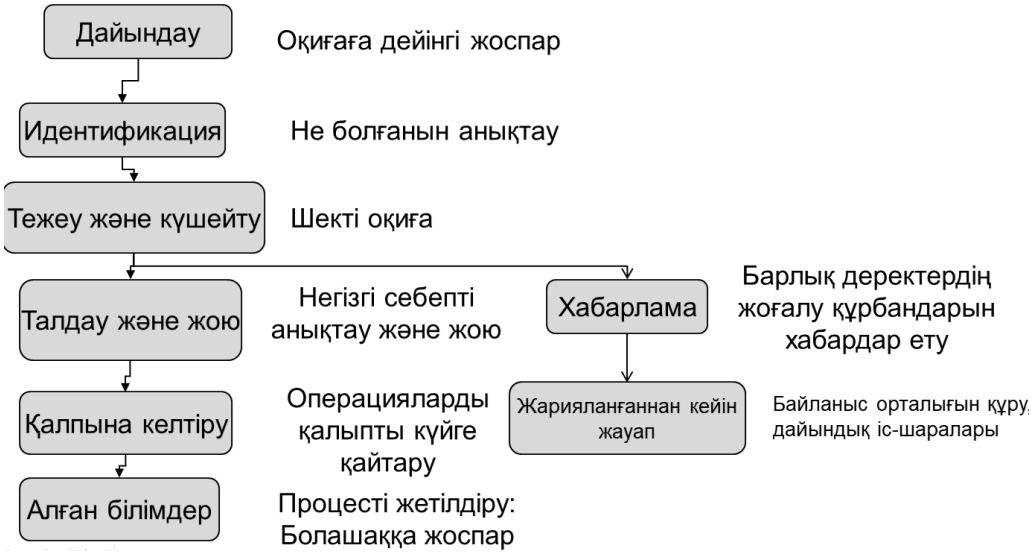
ӘОЖ 004.056

КОМПЬЮТЕРЛІК ИНЦИДЕНТТЕРДІ ЗЕРТТЕУ ТӘСІЛДЕРІ

Ғабитова Альбина Бауыржанқызы
akapon@mail.ru
Л.Н.Гумилев атындағы ЕҰУ ақпараттық технологиялар факультетінің
2-ші курс магистранты, Астана, Қазақстан
Ғылыми жетекші – Сагиндыков Каким Молдабекович

Қазіргі таңда біз дамитын цифрлық қоғамда өмір сүріп жатырмыз және осы эволюциядан көптеген мүмкіндіктер туындайды. Дегенмен, жаңа қауіптер орын алып, сонымен қатар әр түрлі инциденттер орын алуда. Ұйымдар кибер инциденттерді болдырмауға дайын болуы керек. Қауіпсіздіктің бұзылуына немесе компьютермен байланысты заңсыз әрекетке күдік туындағанда, компьютердегі және сақтау құралдарындағы деректерді қорғауды қамтамасыз ету үшін шаралар қабылдау маңызды. Сақталған деректер қауіпсіздік бұзылу деңгейін және рұқсат етілмеген немесе заңсыз әрекетке қатысты ықтимал дәлелдердің орнын анықтау үшін қажет. Компьютерлік қауіпсіздік инцидентіне алғашқы әрекет компьютерлік жүйені кейінірек техникалық талдаудан гөрі маңыздырақ болуы мүмкін. Күдікті компьютерлік инцидент болған жағдайда, дәлелдемелерді бастапқы күйінде сақтау керек. Жүйедегі файлдарды жай ғана қарау бастапқы медианы өзгертуге әкелмейтін сияқты көрінуі мүмкін, бірақ файлды ашу оны өзгертеді. Заңды мағынада ол енді бастапқы дәлел болып табылмайды және кез келген кейінгі сот немесе әкімшілік іс жүргізуде жол берілмейтін болуы мүмкін. Бұл мақалада жеке немесе жұмыс үстеліндегі компьютерлердегі оқиғаға жауап беруге және компьютерлік криминалистикаға назар аударылады.

Компьютерлік инциденттер көбінесе күрделі және көп факторлы мәселелерге әкеледі. Кез келген басқа күрделі техникалық мәселе сияқты, оқиғаға жауап беруді қара жәшік ретінде қарастыруға болады. Есептер құрамдас бөліктерге бөлінеді, содан кейін әрбір компоненттің кіріс және шығыс ақпараты зерттеледі. Осылайша, ұсынылған оқиғаға әрекет ету әдістемесі келесі процедуралардан тұрады:



Сурет 1. Инциденттерге әрекет ету кезеңдері

Коммерциялық криминалистикалық өнімдердің қымбаттығына байланысты көптеген сарапшылар ашық код құралдарын қолдануды жөн көреді. Бұл құралдардың тек кейбіреулері коммерциялық сияқты көптеген мүмкіндіктерге ие, ал көпшілігі белгілі бір функцияны орындау үшін жасалған шағын утилиталар. Олардың көпшілігі Linux ОЖ ортасында жұмыс істеуге арналған, бірақ кейбіреулері (мысалы, Autopsy, Volatility) Windows-қа тасымалданады. Солардың ішінде Volatility құралын қарастыруға болады.

Компьютерлік инциденттер кездейсоқ болады, сондықтан зерттеушілер келесі қауіпсіздік оқиғасы қашан болатынын алдын ала білмейді. Оның үстіне, тергеушілер әдетте бақылауды қолына ала алмайды және компьютерде оқиға орын алғанға дейін оған қол жеткізе алмайды. Дегенмен, жер сілкінісі немесе дауылдың ғылыми болжамы сияқты, оқиға болуы мүмкін деп айтуға болады. Және бұл келесі оқиғаға жақсы дайындалуға көмектеседі. Оқиғаға дайындық кезінде бағдарламалық құралдар мен технологияларды алу ғана емес, сонымен бірге инцидентке әрекет ету үшін алдын ала дайындық үшін жүйе мен желідегі кейбір әрекеттерді орындау көзделеді. Егер тергеушілер компьютерлер мен желіні біршама бақылауға алса, оқиға орын алған соң жауап беруді жылдамдатуға көмектесу үшін әртүрлі алдын ала әрекеттерді орындауға болады. Мысалы, хосттар мен желілерге кіру жолын жақсартуға және тұрақты сақтық көшірмелерді жасауға болады. Оқиғалардың ықтимал құрбандарына (яғни, хосттар мен желілерге) қол жеткізу өкілеттігіне қарамастан, оқиғаға ден қою тобының мүшелеріне рөлдерді алдын ала тағайындау, сондай-ақ осы әрекетке арналған аппараттық және бағдарламалық құралдарды дайындау қажет.

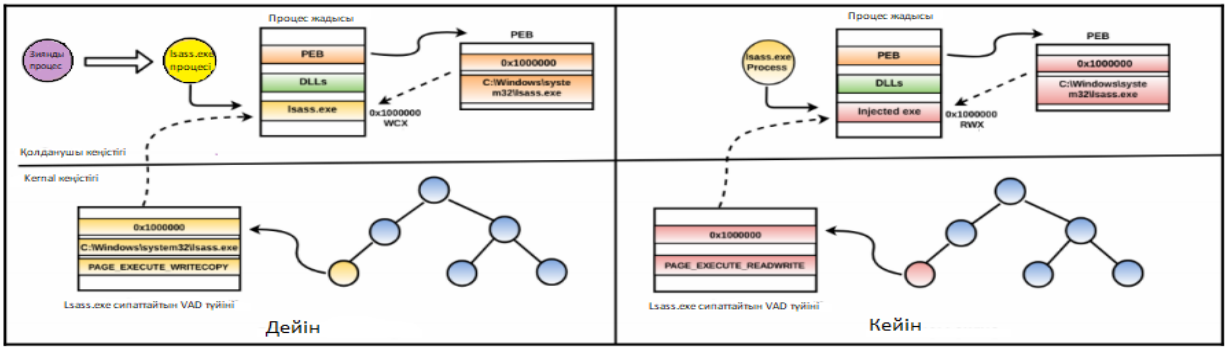
Инцидентке әрекет етудің ең тиімді әдістерін кез келген зерттеуге көмектесетін бірнеше нұсқаулар: барлық маңызды файлдардың криптографиялық бақылау сомасын; қауіпсіздік аудитін жақсарту немесе рұқсат ету; әрбір хост үшін жеке қауіпсіздік құралдарын құру; маңызды деректердің сақтық көшірмесін жасау және алынған мұрағаттық тасымалдағыштарды қауіпсіз жерде сақтау; пайдаланушыларды хосттарды жеке қорғау әдісімен оқыту; барлық хосттар жақсы қорғалған болса, көптеген қауіпсіздікті бұзу оқиғаларын болдырмауға болады. Инцидентке дайындық кезінде хосттың жеке қорғанысын ескеру қажет. Хост қауіпсіздігін арттыру әрекеттері инциденттер ықтималдығын азайтып қана қоймайды, сонымен қатар компьютерлік оқиға орын алған соң тергеуді жеңілдетеді. Көптеген онлайн құралдар компьютерлік оқиғаларға жауап беруге көмектеседі. Оқиғаларды желілік тіркеу қажет, ол көптеген жағдайларда кірудің даусыз фактілерін қамтамасыз етеді. Сондықтан желі әкімшісі оқиғаға жауап беруде маңызды рөл атқарады.

Инцидентті анықтау инцидентке жауап берудің алғашқы қадамы. Анықталғанға дейін тергеуші оқиғаның болу мүмкіндігі туралы хабарлануы тиіс. Осы мақсатта оқиғаны тергеу басталғанға дейін ақпарат алуға мүмкіндік беретін белгілі бір арналар бар. Келесі оқиғаның қашан

болатынын болжау мүмкін емес деп ойлауға болмайды. Операциялық жүйелер мен қолданбаларға ену туралы жарияланымдарға жүгінуге болады. Бұрын компьютерлік инциденттерге әрекет ету тобы (CERT, Compuiei Emergency Response Team) жүздеген іс-шараларды атап өтті. Болжалды инцидентті әртүрлі техникалық және ұйымдастырушылық құралдармен анықтауға болады. Техникалық құралдарға желідегі төтенше жағдайлар туралы хабарламаларды генерациялайтын шабуылдарды анықтау жүйелері (IDS) және брандмауэр кіреді. Әдеттегі жұмыс барысында әкімшілер мен пайдаланушылар әдеттен тыс тіркелгі немесе ресурстарды пайдалану әрекетін байқай алады. Келушілер дұрыс жұмыс істемейтін қызмет немесе бүлінген веб-сайт туралы хабарлауы мүмкін. Оқиғаның қалай анықталғанына қарамастан, алынған барлық ақпаратты жазып алу маңызды. Ол маңызды мәліметтер мен фактілерді жіберіп алмауға мүмкіндік беретін хабарландырулар тізімін пайдалану керек.

Киберқылмыстарды тергеу және дәлелдемелерді жинау моделін құру күшті жасырумен және виртуалды шындықпен сипатталады. Дәстүрлі қылмыстарды тергеу әдістерінен басқа, тергеу тергеу идеяларын өзгертуі, жаңа тергеу әдістерін зерттеуі және желіге негізделген жаңа тергеу шараларын қабылдауы керек. Көпөлшемді криминалистикалық үлгі (MDFM) криминалистикалық процестің уақыт бойынша тереңдеуін көрсетеді. Кез келген уақытта сандық криминалистика нақты криминалистикалық процеске сәйкес кез келген түйіннің күйіне оралуы мүмкін. Деректер мен білім базасы негізгі күйде болатын деңгейдің үш бөлігі, дәлелдемелерді алу негізгі жұмыс болып табылады және ең жоғары нүктеде қадағалау механизмі арқылы өтеді, бұл дәлелдер тізбегінің тұтастығын қамтамасыз етеді және дәлелдемелерді айтарлықтай жақсартады.

Stuxnet тізбесінің кілт параметрлерін, жасырын Dll файлдарын, файл нысандарын және басқа көптеген артефактілерді осы жад үлгісінен Volatility көмегімен таба алдық. Бұл мақалада біз құбылмалылық шеңберінің физикалық жадтың бейнелерімен өзара әрекеттесуінің кейбір жағдайларын қарастырдық. Бұл құрылым белгілі бір уақытта компьютерде қандай процестер жүретінін білуге мүмкіндік береді. Жад кескіндері жүйенің түсірілген уақыттағы толық күйін көрсетеді және оларды өзгерту мүмкін емес. Осылайша, Volatility зиянды бағдарламалық жасақтаманы, қателерді және жүйенің бұзылу себептерін табуға, сондай-ақ алынған барлық деректерді компьютерлік ақпаратқа қатысты қылмыстарды тергеу кезінде цифрлық дәлел ретінде пайдалануға болады.



Сурет 2. Lsass.exe сипаттайтын VAD түйіні

Бұл жұмыстың негізгі мақсаты ақпараттық технологиялардың қарқынды қолдану ақпараттық қауіпсіздік мәселелеріне көбірек назар аударуды қажет етеді. Ақпараттық қауіпсіздік оқиғаларын басқару мәселесі өте өзекті. Оқиғаға жауап беру кезінде ақпараттық жүйенің нақты осалдықтарын, шабуылдар мен олардың іздері қорғаныс механизмдерінің жұмыс деңгейі анықталады. Салыстырмалы түрде жады криминиластикасы талдаудың жаңа әдісі болып табылғандықтан ақпараттық технологиялардың қауіпсіздігінің қамтамасыз етілуі және Питон тілінде жазылған ең танымал жады бейнесін талдағыштардың бірі Volatility құралымен жұмыс жасалды. Талдау нәтижесінде құралдың дұрыс жұмыс қабілеттілігін тез және нақты артефактілерді анықтау арқылы қорытынды жасалды.

Қолданылған әдебиеттер тізімі

1. Ahmad, A., Hadgkiss, J., and Ruighaver, A. B. (2012). Incident response teams challenges in supporting the organisational security function.

2. Мандиа Кении, Просис Крис. Защита от вторжений: расследование компьютерных преступлений. М.: Издательство «ЛОРИ», 2005. 476 с.

3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО «ТИД ДС», 2001. 688 с.

4. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. Спб.: БХВПетербург, 2005. 752 с.

5. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. Горячая Линия – Телеком, 2002. 336 с. 5. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. Питер, 2008. 320 с.

УДК 004.056.5

ОСОБЕННОСТИ ПРИМЕНЕНИЯ АППАРАТНОГО МЕЖСЕТЕВОГО ЭКРАНА

Дауренбеков Нияз Хайнуллович
niyaz_daurenb@mail.ru
Магистрант факультета информационных технологий Евразийского национального университета имени Л.Н. Гумилева, Астана, Казахстан
Научный руководитель - Жүзбаев С.С.

Межсетевой экран, защищающий компьютерную сеть от сетевых атак, имеет определенные технические характеристики. Выбор модели необходимо осуществлять в зависимости от масштабов самой сети, степени конфиденциальности циркулирующей в ней информации, существующей в организации политики доступа в Интернет, подготовленности штатных администраторов и т.п.

Аппаратный межсетевой экран - программно-аппаратное устройство компьютерной сети, предназначенное для проверки на соответствие заданным правилам и дальнейшей фильтрации проходящего сквозь него сетевого трафика. Другие названия: брандмауэр (немецкий «brandmauer» - «противопожарная стена»), файрвол (английский «firewall» - «противопожарная стена»). [4]

Межсетевые экраны используются в корпоративных компьютерных сетях предприятий для защиты всей сети, её сегментов или отдельных компьютеров (серверов) от несанкционированного взлома, нарушения правил доступа, пользуясь уязвимостями в протоколах сетевой модели OSI, TCP/IP или в программном обеспечении, установленном на терминальном оборудовании сети. Межсетевые экраны могут пропускать или запрещать потоки данных, сравнивая его характеристики с настроенными шаблонами.

Значительное разнообразие межсетевых экранов вызывают у потребителя затруднения выбора модели, наиболее адекватно и эффективно решающую задачи по защите конкретной сети. Информация о межсетевых экранах, доступная непосредственно от производителя, чаще всего в рекламных целях преувеличивает достоинства и скрывает недостатки. В данной статье указываются параметры, на которые рекомендуется обращать внимание при подборе модели аппаратного межсетевого экрана предприятия, что поспособствует осознанному выбору продукта, оценивая его достоинства и недостатки.

Первые устройства, выполняющие функцию фильтрации сетевого трафика, появились в конце 1980-х, когда Интернет был новшеством и использовался в локальных, а не в глобальных масштабах. Этими устройствами являлись маршрутизаторы, инспектирующие трафик на основании содержащихся в заголовках протоколов сетевого уровня (например, заголовок IP пакета). Впоследствии, с развитием сетевых технологий, данные устройства получили возможность выполнять фильтрацию трафика, используя данные протоколов более высокого,