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

4. Қорытынды

Қорытындылай келе, SASE шекара қызметінің қауіпсіз қол жеткізу моделі қазіргі заманғы қауіпсіздік стратегияларының маңызды құрамдас бөлігі болып табылады. Бұл ұйымдарға желіні және соңғы нүктелерді киберқауіптерден қорғай отырып, әртүрлі қауіпсіздік мүмкіндіктерін басқару үшін үнемді, бірыңғай платформаны ұсынады. Қашықтан жұмыс істеудің жоғарылауымен және цифрлық трансформация қажеттілігімен SASE моделі кез-келген көлемдегі ұйымдар үшін маңызды бола түсуде.

Ұсынылған модельдің артықшылықтары бар брандмауэр, басып кіруді анықтау және алдын алу, VPN және т.б. сияқты желілік қауіпсіздік мүмкіндіктерін қауіпсіз веб-шлюздер және нөлдік сенімді желіге қол жеткізу сияқты бұлттық қызметтермен біріктіретін желілік қауіпсіздікке кешенді тәсілді қамтамасыз ету сияқты. Бұл қауіпсіздікке төнетін қатерлерді анықтауды және олардың әсерін азайтуды жеңілдететін желілік трафик пен пайдаланушылардың белсенділігін көбірек көруге және бақылауға мүмкіндік беретін тиімдірек және үнемді қауіпсіздік стратегиясына әкеледі.

Алайда, SASE моделін енгізу инфрақұрылымға және сараптамалық білімге қомақты инвестицияларды талап етуі мүмкін, өйткені бұл көптеген технологиялар мен қауіпсіздік қызметтерін біріктіруді және шоғырландыруды көздейді. Жалпы, SASE желілік қауіпсіздік тұрғысынан айтарлықтай артықшылықтар бере алады.

Пайдаланылған әдебиеттер тізімі

1. Gartner. (2019). The Future of Network Security Is in the Cloud. https://www.gartner.com/smarterwithgartner/the-future-of-network-security-is-in-the-cloud/
2. Mather T., Kumaraswamy S., Latif S., «Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance», 2009, O'Reilly Media, Inc 292.
3. Cobb C., «Network Security for Dummies», 2011, For Dummies, 499.
4. Hines C., «SASE: Cloud Native Security for the Enterprise», 2022, O'Reilly Media, 515.
5. Adkins H., Beyer B., Blankinship P., «Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems», 2020, O'Reilly Media, 558.
6. Lowe D., «Networking All-in-One For Dummies», 2021, For Dummies, 1056.
7. Arundel J., «Cloud Native DevOps with Kubernetes: Building, Deploying, and Scaling Modern Applications in the Cloud», 2019, O'Reilly Media, 344.
8. Erl T., Puttini R., Mahmood Z., «Cloud Computing: Concepts, Technology & Architecture», 2013, Pearson, 528.
9. Nagendra P., Gupta R., Zacharia M., «Cloud Security Automation: Get to Cloud Securely Using DevOps Practices», 2018, Manning, 384.
10. Zscaler. (2021). What is SASE? https://www.zscaler.com/SASE/what-is-SASE
11. AT&T Business. (2021). Secure Access Service Edge (SASE). https://www.business.att.com/solutions/secure-access-service-edge-SASE.html

УДК 004.056

ИСПОЛЬЗОВАНИЕ УЯЗВИМЫХ КОНТЕЙНЕРОВ DOCKER В ПРОЦЕССЕ ОБУЧЕНИИ БАКАЛАВРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Боранбай Жандос Асылханұлы
boranbay.zhandos@gmail.com
магистрант 1 курса (7М06306 – Системы информационной безопасности), ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Д.Ж.Сатыбалдина

Введение. Контейнеры Docker становятся все более популярной технологией упаковки и развертывания приложений. Для студентов, изучающих информационную безопасность, важно понимать как нужно эксплуатировать уязвимости и как их устранять. В этой статье

рассматривается использование уязвимых контейнеров Docker в качестве учебной лаборатории для бакалавров в области информационной безопасности. Мы обсудим преимущества использования уязвимых контейнеров Docker в обучении, предоставим пример по созданию уязвимого контейнера и шаги для использования уязвимого контейнера, а также опишем рекомендации по использованию данных контейнеров.

Преимущества использования уязвимых контейнеров Docker в обучении. Использование уязвимых контейнеров Docker в обучении дает учащимся несколько преимуществ. Во-первых, это позволяет студентам получить практический опыт в безопасной и контролируемой среде. Во-вторых, это помогает учащимся развивать критическое мышление и навыки решения проблем, когда они работают над выявлением и устранением уязвимостей в системе безопасности[1]. Наконец, он знакомит студентов с реальными сценариями, с которыми они могут столкнуться в своей будущей карьере.

Создание уязвимого контейнера Docker. Например уязвимость Drupal под CVE-2019-6341.

После запуска тестовой среды нужно:

Объяснить уязвимость: предоставить обзор уязвимости CVE-2019-6341, ее влияния и того, как ее можно использовать. Объясните, как злоумышленник может использовать эту уязвимость для удаленного выполнения вредоносного кода.

Продемонстрировать уязвимость: использовать известный эксплойт, чтобы продемонстрировать уязвимость и ее последствия.

Обсудить стратегии смягчения последствий: обсудить стратегии смягчения этой уязвимости, включая обновление до последней версии Drupal или применение исправлений, и объяснить, почему важно поддерживать программное обеспечение в актуальном состоянии, чтобы предотвратить использование подобных уязвимостей[1].

Предоставить практическое упражнение: Предоставить учащимся практическое упражнение, чтобы попрактиковаться в обнаружений и устранении этой уязвимости.

Подчеркнуть этические соображения. Подчеркнуть этические соображения при тестировании и использовании уязвимостей. Объяснить, что учащиеся должны выполнять эти действия только в предоставленной тестовой среде и никогда за ее пределами.

Рекомендации по использованию уязвимых контейнеров Docker.

При использовании уязвимых контейнеров Docker важно следовать рекомендациям по обеспечению безопасности студентов и сети в целом[2]. К ним относятся:

Использование изолированных сетей. Уязвимые контейнеры следует запускать в изолированных сетях, чтобы предотвратить распространение потенциальных атак за пределы контейнера. Предоставление четких инструкций: студентам должны быть предоставлены четкие инструкции о том, как использовать контейнер и что делать, если у них возникнут какие-либо проблемы. Мониторинг активности. Активность внутри контейнера должна контролироваться, чтобы убедиться, что студенты случайно или намеренно не причиняют вреда сети или другим контейнерам[3].

Подготовка задачи:

Чтобы подготовиться к этой практической задаче, студент должен иметь базовые знания по следующим темам:

Безопасность веб -приложений

PHP программирование

Drupal CMS

Кроме того, для этой задачи рекомендуются следующие инструменты:

Редактор кода(например, Notepad++ или Sublime Text)

Сканер веб -уязвимости (например, Owasp Zap или Burp Suite)

Выполнение задачи:

Студент должен начать с определения уязвимости в CVE-2019-6341. Уязвимость связана с модулем Drupal RESTful Web Services и позволяет злоумышленнику отправить специально

созданный запрос, который может привести к выполнению произвольного кода PHP[4]. Студент должен прочитать отчет об уязвимости и понять детали эксплойта.

Напишите эксплоит: как только уязвимость обнаружена, учащийся должен написать эксплойт для ее использования. Эксплойт должен отправить специально созданный запрос на сайт Drupal, который запускает уязвимость и позволяет выполнить произвольный код. Студент должен использовать веб-сканер уязвимостей, чтобы протестировать скрипт и убедиться, что эксплойт успешно работает.

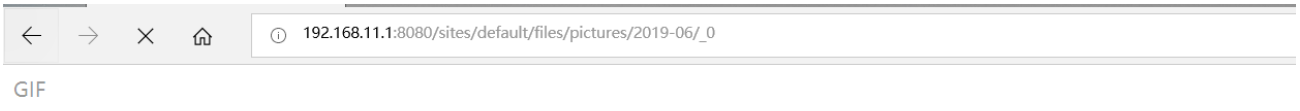
Обеспечьте исправление: наконец, учащийся должен предоставить рекомендацию для исправления уязвимости. Учащийся должен понять основную причину уязвимости и предложить решение для ее устранения.

```
1  version: '2'
2  services:
3   web:
4     image: drupal:8.5.0
5     ports:
6      - "8080:80"
```

Рис. 1 docker-compose.yml

```
/var/www/html$ php cve-2019-6341-exp.php 192.168.11.1 8080
uploading file, please wait...
please check /var/www/html/drupal/sites/default/files/pictures/YYYY-MM
```

Рис. 2 Выполнение эксплойта



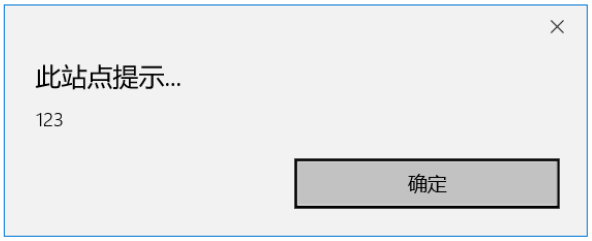


Рис. 3 Результат выполнении эксплойта

Заключение. Уязвимые контейнеры Docker — ценный учебный инструмент для бакалавров в области информационной безопасности[5]. Предоставляя учащимся практический опыт в безопасной и контролируемой среде, уязвимые контейнеры помогают учащимся развивать практические навыки, а также знакомят их с реальными сценариями, с которыми они могут столкнуться в своей будущей карьере. Хотя уязвимые контейнеры Docker являются полезным инструментом для обучения бакалавров информационной безопасности, в этой области еще много возможностей для изучения и совершенствования. Будущие исследования могут изучить эффективность использования уязвимых контейнеров для обучения конкретным концепциям

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: