БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 2 (113). – 9–24

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2024-2-9-24

ОПЫТ ПРОВЕДЕНИЯ КИБЕРУЧЕНИЙ С ИСПОЛЬЗОВАНИЕМ РАЗРАБОТАННОГО СЦЕНАРИЯ*

А.Р. КАСИМОВА[1], Д.А. ВОРОБЬЕВ[2], А.Н. СЕВРУНОВ[3]

[1] *420015, РФ, г. Казань, ул. Карла Маркса, 68, ФГБОУ ВО «КНИТУ», старший преподаватель кафедры «Информационная безопасность». E-mail: kasimovaar@corp.knrtu.ru*
[2] *660037, РФ, г. Красноярск, пр. имени Газеты «Красноярский рабочий», 31, Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, ассистент кафедры безопасности информационных технологий. E-mail: h1ppyfox1@gmail.com*
[3] *660037, РФ, г. Красноярск, пр. имени Газеты «Красноярский рабочий», 31, Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, ассистент кафедры безопасности информационных технологий. E-mail: alexander.sevrunov@gmail.com*

Угроза кибератак стала серьезной проблемой для организаций, решение которой в том числе лежит и в плоскости моделирования сценариев возможных атак с применением технологий цифровых двойников. Киберполигон, основанный на программном комплексе AMPIRE, используется для изучения воздействия киберугроз. Сценарий действий злоумышленника включает использование различных тактик и уязвимостей, таких как активное сканирование, подготовка ресурсов, уязвимости в общедоступных приложениях, вредоносные ссылки и файлы, а также компрометацию учетных записей пользователей домена. Вектор атаки злоумышленика соотносится с тактиками, техниками и процедурами матрицы Mitre ATT&CK. Уязвимости включают плагин wpDiscuz, Zerologon и последствия использования Wordpress Shell и получения несанкционированного доступа. Проводимые межвузовские киберучения позволили выявить сильные и слабые места, которые необходимо учитывать при проведении следующих мероприятий. Сценарное тестирование с участием вузов показало эффективность комплекса при оценке времени, необходимого для закрытия уязвимостей и устранения последствий. Реализация на киберполигоне разнотипных сценариев с профильным функционалом дает возможность сформировать практические навыки по предотвращению атак на компьютерные сети, а также позволяет анализировать ситуацию, взаимодействовать с другими специалистами-участниками.

* Статья получена 20 марта 2024 г.

Ключевые слова: киберучения, цифровой двойник, mitre att&ck, digital twin, киберполигон, вектор атаки, моделирование, ЛВС

ВВЕДЕНИЕ

Рынок специалистов в области обеспечения информационной безопасности (ИБ) уже сегодня испытывает острую нехватку квалифицированных кадров, и потребность в них будет только увеличиваться.

Наряду с количеством специалистов является наиболее актуальным вопрос качества подготовки специалистов. Увеличение кибератак во втором квартале 2023 года на 38 % по сравнению с аналогичным периодом 2022 года (325 тыс. инцидентов) стимулировало профильное ведомство обновить стандарты подготовки IT-специалистов в сфере кибербезопасности [1].

Укрупненное направление подготовки 10.00.00 – одно из самых востребованных в вузах, для реализации которого требуются специализированные лаборатории, оборудование, сетевые устройства, программное обеспечение и системы моделирования и анализа данных. Стандарты в области подготовки предусматривают возможность замены специально оборудованных помещений их виртуальными аналогами.

Одним из таких универсальных аналогов можется являться киберполигон (цифровой двойник), который представляет собой многофункциональный программно-аппаратный комплекс и предназначен для обучения, подготовки и тренировки специалистов по информационной безопасности.

Использование киберполигона для реализации безопасного сбора, анализа и управления данных внутри системы является перспективным, поскольку не затрагивает реальную инфраструктуру предприятия и «песочницу», контролируемое пространство, которое помимо прочего можно использовать для валидации и верификации данных [2].

При обучении специалистов на киберполигоне важно, чтобы имелась возможность моделирования конкретной сети или IT-инфраструктуры предприятия, возможность пополнения сценариев атак, распределение ролей, сегментируемость, система отчетности, а также возможность командного взаимодействия.

Целью работы стало исследование применения киберполигона в качестве цифрового двойника сети организации для обучения специалистов в области ИБ.

Для достижения поставленной цели были выделены следующие задачи:

- определить уязвимости и последствия от реализации этих уязвимостей для сценария;
- провести межвузовские киберучения на основе разработанного сценария с использованием киберполигона.

1. ОПИСАНИЕ РАБОТЫ КИБЕРПОЛИГОНА

Понятие «цифровой двойник» подробно изучено и описано в [3–11]. Для исследования был создан цифровой двойник информационной системы типового химического предприятия на базе программного комплекса AMPIRE, используемый в лаборатории КНИТУ, – киберполигон [3]. Подсистемы сетевой безопасности, реализуемые на киберполигоне:

- мониторинг и встроенная корреляция (SIEM);
- контроль доступа;
- сигнатурный анализ;
- ретроспективный анализ.

Помимо подсистем сетевой безопасности также реализована система расследования инцидентов [12].

Схема цифрового двойника локально-вычислительной сети представлена на рис 1.

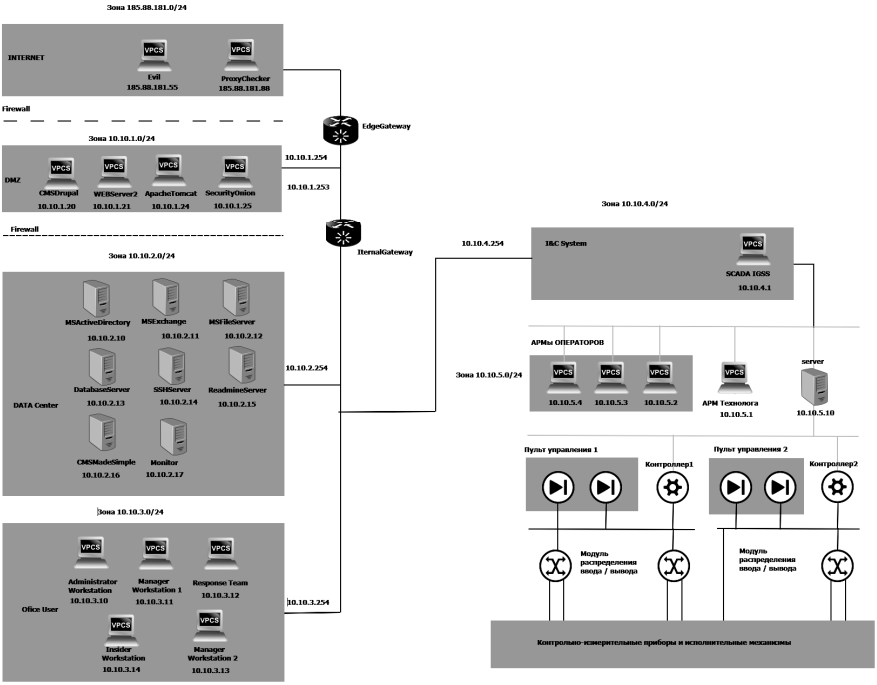


Рис. 1. Схема ЛВС киберполигона

ЛВС представлена пятью зонами:

- сеть Интернет,
- демилитаризованная зона (DMZ),
- центр обработки данных (ЦОД),
- офисные пользователи,
- система ISC.

В качестве средства виртуализации используется специализированное ПО VMWare EXSI. На серверах установлены ОС Linux, для файлового сервера, серверов Active Directory (AD) и Exchange – ОС Windows. На АРМ пользователей установлена ОС Windows и ОС Astra Linux SE 1.6. В качестве базы данных используется MySQL 5.5; IGSS Master используется на АРМ с IP-адресом 10.10.4.1.

2. РАЗРАБОТКА СЦЕНАРИЯ ДЕЙСТВИЯ НАРУШИТЕЛЯ

2.1. ОПИСАНИЕ СЦЕНАРИЯ

Основная цель нарушителя получить доступ к контролеру домена сети – Active Directory (AD). Ядро разработки сценария – матрица MITRE ATT&CK, описывающая тактики и техники, которыми злоумышленники пользуются в своих атаках на корпоративную инфраструктуру. Согласно матрице [13] злоумышленнику будет необходимо использовать следующие тактики и техники:

- тактика – разведка;
- техника – CT1595 «Активное сканирование».

Нарушитель проводит сканирование сети 185.88.181.0/24 и находит сайт с версией Wordpress 5.8.2 с установленным плагином wpDiscuz;

- тактика – подготовка ресурсов;
- техника – подготовка необходимых средств.

Подготавливает необходимые ресурсы:

- тактика – первоначальный доступ;
- техника – T1190 «Недостатки в общедоступном приложении».

На сервере WebPortal2 находится сайт на WpDiscuz CMS, на котором установлен плагин WpDiscuz, уязвимость которого позволяет получить RCE.

После предыдущих уровней злоумышленник решает проверить уязвимость плагина wpDiscuz для версий 7.0.0 – 7.0.4, получая metersrpretter сессию, заменяет ссылку на скачивание какого-либо файла на reverseshell, ожидая скачивания и запуска этого файла пользователем;

- тактика – выполнение;

- техники – T1204.001 Вредоносная ссылка / T1204.002 Вредоносный файл.

Пользователь скачивает и запускает вредоносный файл;

- тактика – закрепление;
- техника – T1136.002 «Доменная учетная запись (техника)».

Получение доступа к AD.

На рис. 2 представлен сегмент сети с действия злоумышленника.

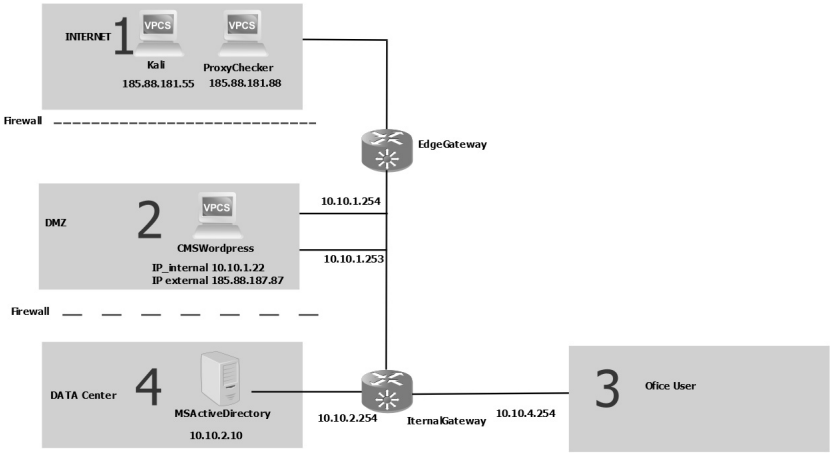


Рис. 2. Сегмент ЛВС с последовательностью действий злоумышленника

2.2. ПЕРЕЧЕНЬ УЯЗВИМОСТЕЙ И СПОСОБЫ ИХ ДЕТЕКТИРОВАНИЯ

Исходя из описания сценария были определены следующие уязвимости и их последствия:

- wpDiscuz (идентификационный номер CVE-2020-24186 в соответствии с базой данных общеизвестных уязвимостей CVE);
- Zerologon (идентификационный номер CVE-2020-1472 в соответствии с базой данных общеизвестных уязвимостей CVE);
- последствие Wordpress Shell;
- последствие получения прав доступа.

В работе [14] предлагается алгоритм окрестности инцидента, который в дальнейшем будет использоваться для объяснения способов детектирования уязвимостей и который необходим для безопасности автоматизированных систем [15].

Обнаружение и нейтрализация wpDiscuz

У CMS WordPress есть множество плагинов; WpDiscuz – один из плагинов для создания комментариев. Он представляет собой систему для комментариев на базе Ajax, которая хранит сообщения в локальной базе данных. В версиях с 7.0.0 по 7.0.4 есть уязвимость FileUpload, которая позволяет получить RCE, если прикрепить любой файл (например, код на php) в поле для комментариев и загрузить на сервер. Сделать это можно без аутентификации. Детектирование эксплуатации уязвимости удаленного выполнения кода CVE-2020-24186 с помощью сетевого сенсора ViPNet IDS NS (рис. 3 и 4).

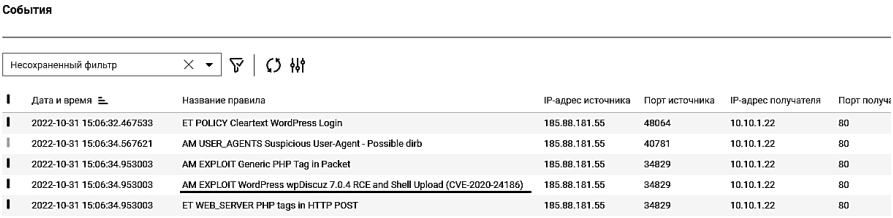


Рис. 3. Журнал событий сетевого сенсора ViPNet IDS NS

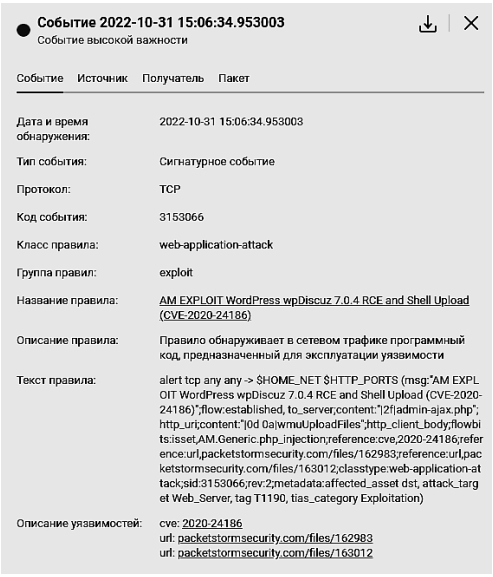


Рис. 4. Карточка события ИБ

Закрытие уязвимости можно осуществить следующими способами:

- отключение плагина wpDiscuz;
- обновление версии wpDiscuz до версии 7.0.5 и выше (при наличии интернета).

Обнаружение и нейтрализация payload

Данный payload заключается в том, что нарушитель устанавливает shell-сессию с уязвимой машиной.

Для того чтобы обнаружить эту полезную нагрузку, нужно проверить сокеты уязвимой машины на подключение к определенному порту машины нарушителя. Делается это при помощи утилиты ss. Следует просмотреть сокеты только нужного протокола (TCP) и отфильтровать данные (например, вывести только прослушиваемые tcp соединения):

$ ss -tn

Отображение информации о прослушиваемых TCP-соединениях уязвимой машины и завершении сессии с нарушителем показано ниже.

Для нейтрализации payload нужно также воспользоваться командой ss с правами привилегированного пользователя, используя ключ –K и соответствующий адрес, порт, что завершит сессию с нарушителем:

sudo ss –K dst 185.88.181.55 dport = 5764

Meterpreter-сессия с нарушителем завершена.

Обнаружение и нейтрализация Zerologon

Уязвимость в сервисе Netlogon позволяет обойти аутентификацию и сбросить пароль машинного аккаунта контроллера домена.

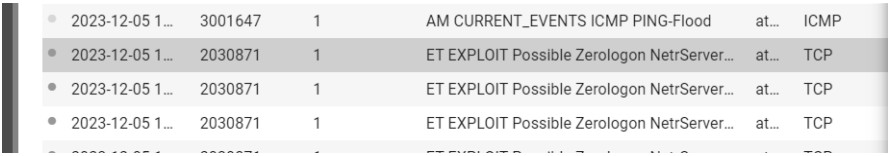
Уязвимость в сервисе Netlogon позволяет обойти аутентификацию и сбросить пароль машинного аккаунта контроллера домена. Эксплуатация этой уязвимости состоит из трех этапов:

- *отправка нулевых байтов.* Вместо отправки восьми случайных байтов атакующий отправляет нулевые байты до тех пор, пока сервер не примет одно из таких сообщений. Тем самым атакующий обходит процесс аутентификации и получает возможность совершать действия от имени контроллера домена;
- *отключение механизма RPC signing and sealing.* Атакующий отключает шифрование для того, чтобы сообщения отправлялись в открытом виде и атакующий мог использовать методы протокола MS-NRPC;
- *изменение пароля учетной записи контроллера домена.* Финальным шагом атаки является сброс пароля учетной записи контроллера домена.

Это открывает возможности для проведения атаки DCSync, которая направлена на получение существующих хэшей устройств в домене.

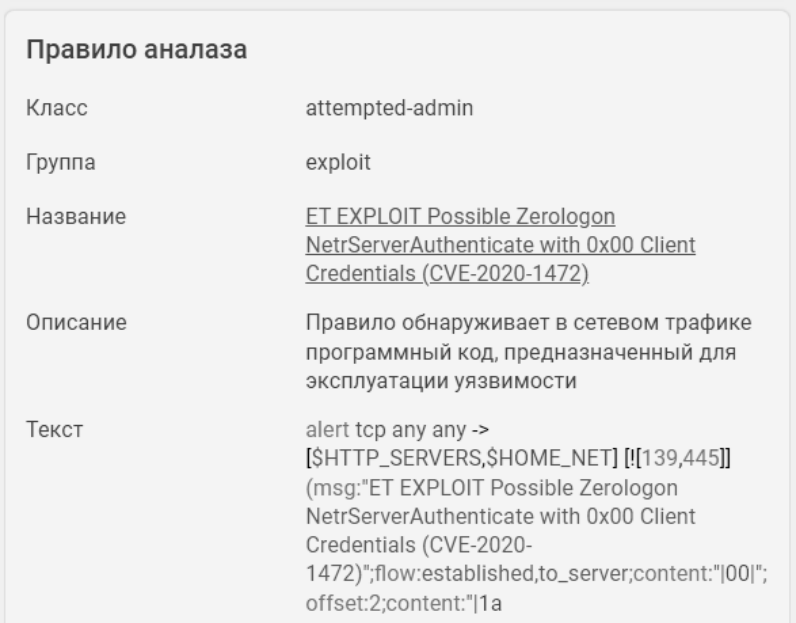
При атаке Zerologon в eventviewer генерируется событие 4742 (его можно найти во вкладке WindowsLogs>Security), в то время как при легитимной смене пароля контроллера домена будет сгенерировано два события: 4742 и 5823. В логах netlogon можно увидеть события, которые показывают успешный вход и смену пароля машинного аккаунта.

Детектирование эксплуатации уязвимости удаленного выполнения кода CVE-2020-1472 с помощью сетевого сенсора ViPNet IDS NS показано на рис. 5 и 6.



2023-12-05 1...	3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	at...	ICMP
2023-12-05 1...	2030871	1	ET EXPLOIT Possible Zerologon NetrServer...	at...	TCP
2023-12-05 1...	2030871	1	ET EXPLOIT Possible Zerologon NetrServer...	at...	TCP
2023-12-05 1...	2030871	1	ET EXPLOIT Possible Zerologon NetrServer...	at...	TCP

Рис. 5. Журнал событий сетевого сенсора ViPNet IDS NS



Правило анализа

Класс	attempted-admin
Группа	exploit
Название	ET EXPLOIT Possible Zerologon NetrServerAuthenticate with 0x00 Client Credentials (CVE-2020-1472)
Описание	Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости
Текст	alert tcp any any -> [$HTTP_SERVERS,$HOME_NET] [![139,445]] (msg:"ET EXPLOIT Possible Zerologon NetrServerAuthenticate with 0x00 Client Credentials (CVE-2020-1472)";flow:established,to_server;content:"|00|"; offset:2;content:"|1a

Рис. 6. Карточка события ИБ

После успешной эксплуатации Zerologon происходит сброс пароля машинного аккаунта контроллера домена. В результате атакующему открывается возможность получить NTLM-хэши в домене и после этого с их помощью получить контроль над учетными записями в домене. Фактически лишение контроллера домена разрешения на запрос репликации делает атаку DCSync невозможной, что приведет к бесполезности уязвимости Zerologon.

Для изъятия вышеуказанного разрешения необходимо провести изменение настроек AD:

- включить в AD отображение расширенных опций (рис. 7);

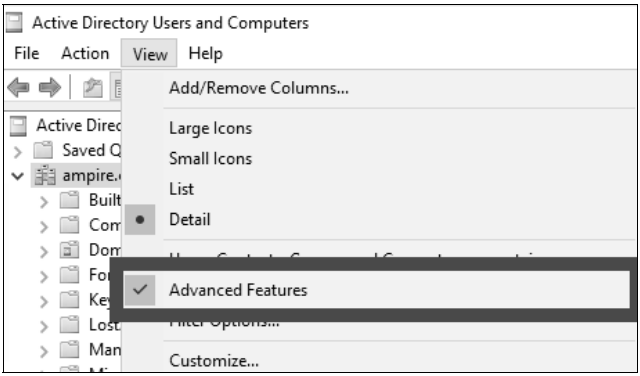


Рис. 7. Включение отображения расширенных опций

- изъять права ReplicatingDirectoryChanges;
- удалить нового привилегированного пользователя, который добавлен в Domain Admins. Факт добавления нового пользователя можно отследить в EventLog.

2.3. АПРОБАЦИЯ СЦЕНАРИЯ НА КИБЕРПОЛИГОНЕ

В апробации сценария приняли участие 5 вузов:

- ФГБОУ ВО «КНИТУ» (г. Казань).
- ФГБОУ ВО «КНИТУ – КАИ» (г. Казань).
- ФГБОУ ВО «КГЭУ» (г. Казань).
- ФГБОУ ВО «СамГТУ» (г. Самара).
- ФГБОУ ВО «СибГУ им. М.Ф. Решетнёва» (г. Красноярск).

По итогам прохождения сценария была составлена сводная таблица (см. таблицу).

Больше всего проблем возникло с уязвимостью Zerologon. Ее смогли закрыть только две команды из пяти, потратив на закрытие уязвимости около четырех часов. Уязвимость плагина Wordpress закрыли все команды, но только две команды устранили последствие Wordpress Shell. Также сложности возникли и с устранением последствия, связанного с получением доступа. По результатам киберучений можно сделать следующие выводы.

- Межвузовские киберучения позволяют студентам из разных вузов общаться и обучаться вместе, расширяя их знания и навыки.
- Участие в межвузовских киберучениих помогает студентам создавать профессиональные связи, которые могут быть полезны в будущей карьере.
- Межвузовские киберучения обучают студентов работать в команде и сотрудничать с другими людьми, что является важным навыком для будущих карьер.
- Остается открытым вопрос с технической поддержкой во время проведения киберучений. Во время проведения мероприятия существенных проблем не возникало, но некачественное обеспечение интернет-соединения, проблемы с программным обеспечением или аппаратным обеспечением могут помешать успешному проведению киберучений.
- В сравнении с традиционным обучением, киберучение может не обеспечивать полноценную онлайн-связь между преподавателем и учащимися.
- Так как география городов-участников разнообразна, участие в межвузовских киберучениях требовало адаптации к разным временным поясам и изменениям в учебном графике.

Результаты межвузовских киберучений

Вуз	Устранение уязвимости wpDiscuz, мин	Устранение уязвимости Zerologon, мин	Устранение последствия Wordpress Shell (да/нет)	Устранение уязвимости получения доступа (да/нет)
ФГБОУ ВО «КНИТУ»	169	0	нет	да
ФГБОУ ВО «КНИТУ – КАИ»	143	241	да	да
ФГБОУ ВО «КГЭУ»	161	225	нет	нет
ФГБОУ ВО «СамГТУ»	180	0	нет	нет
ФГБОУ ВО «СибГУ им. М.Ф. Решетнёва»	199	0	да	нет

ЗАКЛЮЧЕНИЕ

В сценарии действий злоумышленника используются различные тактики и приемы, включая активное сканирование, подготовку ресурсов, уязвимости в общедоступных приложениях, вредоносные ссылки и файлы, а также учетные записи пользователей домена. Представлены уязвимости и методы их обнаружения с упором на плагин wpDiscuz, Zerologon, а также последствия использования Wordpress Shell и получения несанкционированного доступа.

Уязвимость wpDiscuz (CVE-2020-24186) в плагине WordPress позволяет удаленно выполнять код (RCE) путем загрузки вредоносного файла без аутентификации. Эксплуатацию этой уязвимости можно обнаружить с помощью сетевых датчиков, таких как ViPNet IDS NS. Меры по снижению этой уязвимости включают отключение плагина wpDiscuz или обновление его до версии 7.0.5 или выше.

Обнаружение и нейтрализация полезной нагрузки включает в себя мониторинг сокетов уязвимой машины на предмет подключений к определенному порту, используемому злоумышленником.

Zerologon – еще одна уязвимость, позволяющая обойти аутентификацию и сбросить пароль учетной записи компьютера контроллера домена. Меры по смягчению последствий для Zerologon включают настройку параметров AD (в частности, дополнительных параметров) и отзыв прав Replicating Directory Changes.

В заключение отметим, что киберполигон на базе программного комплекса AMPIRE представляет собой платформу для изучения воздействия киберугроз. Благодаря реализации различных подсистем безопасности, включая мониторинг, контроль доступа, анализ сигнатур и ретроспективный анализ, эта линейка позволяет исследовать и устранять такие уязвимости, как wpDiscuz и Zerologon. Сценарное тестирование с участием вузов продемонстрировало эффективность комплекса при оценке времени, необходимого для смягчения уязвимостей и устранения последствий.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные тенденции на рынке информационной безопасности / А.В. Соломинский, В.А. Железин, А.Д. Миргородский, С.В. Краснобаев, Н.М. Колотилина // Вестник науки и образования. – 2023. – № 8 (139). – URL: https://cyberleninka.ru/article/n/aktualnye-tendentsii-na-rynke-informatsionnoy-bezopasnosti (дата обращения: 27.05.2024).

2. Моделирование вектора сетевых атак на локальную сеть с применением базы MITRE ATT&CK / А.Р. Касимова, В.В. Золотарев, Л.Х. Сафиуллина,

Д.И. Сабирова // Прикаспийский журнал: управление и высокие технологии. – 2023. – № 4 (64). – С. 88–96. – DOI: 10.54398/20741707_2023_4_88. – EDN MPSCDH.

3. *Касимова А.Р., Сафиуллина Л.Х.* Использование цифровых двойников при построении системы безопасности предприятия // Международный форум «Kazan Digital Week – 2022»: сборник материалов / под общ. ред. Р.Н. Минниханова. – Казань, 2022. – Ч. 1. – С. 291–298.

4. *Шинкевич А.И., Надеждина М.Е., Сопин В.Ф.* Проектирование цифрового двойника системы организации производства // Стандарты и качество. – 2024. – № 4. – С. 94–99. – DOI: 10.35400/0038-9692-2024-4-197-23.

5. *Шинкевич А.И., Касимова А.Р., Алексеева А.А.* Использование цифровых двойников для экологизации химической промышленности // Известия Самарского научного центра Российской академии наук. – 2023. – Т. 25, № 4. – С. 87–94.

6. *Перухин М.Ю., Васильева М.Ю., Кадырова Г.К.* Цифровой двойник лаборатории систем управления химико-технологическими процессами // Современные наукоемкие технологии. – 2021. – № 6-1. – С. 84–90.

7. *Алексеева А.А., Касимова А.Р.* Перспективы применения цифровых двойников с целью экологизации производства // Комплексное изучение экосистем горных территорий: сборник материалов VI Кавказского международного экологического форума, Грозный, 20–21 октября 2023 года. – Грозный, 2023. – С. 16–19. – DOI: 10.36684/102-1-2023-16-19.

8. Цифровые двойники и цифровая трансформация предприятий ОПК / А.И. Боровков, Ю.А. Рябов, К.В. Кукушкин, В.М. Марусева, В.Ю. Кулемин // Вестник Восточно-Сибирской открытой академии. – 2019. – № 32. – С. 1–39.

9. *Шпак П.С., Сычева Е.Г., Меринская Е.Е.* Концепция цифровых двойников как современная тенденция цифровой экономики // Вестник Омского университета. Серия: Экономика. – 2020. – № 1. – С. 57–68.

10. *Хорзова И.С.* Применение возможностей киберполигона для подготовки и повышения квалификации специалистов по информационной безопасности // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем. – Воронеж, 2021. – Т. 2. – С. 46–47.

11. Digital Twins and Cyber Security – solution or challenge? / D. Holmes, M. Papathanasaki, L. Maglaras, M.A. Ferrag, S. Nepal, H. Janicke // 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). – IEEE, 2021. – P. 1–8. – DOI: 10.1109/SEEDA-CECNSM53056.2021.9566277.

12. Методическое пособие для обучаемого Ampire / Перспективный мониторинг. – URL: Локальный доступ.

13. Матрица ATT&CK. – URL: https://attack.mitre.org/ (accessed: 28.05.2024).

14. *Олейникова А.А., Золотарев В.В.* Концепция управления информационной безопасностью на основе цикла непрерывного детектирования и реагирования на инциденты безопасности информации // Известия ЮФУ. Технические науки. – 2023. – № 5 (235). – С. 66–81. – DOI: 10.18522/2311-3103-2023-5-66-81. – EDN KKJTDV.

15. Методика построения модели безопасности автоматизированных систем / В.Г. Жуков, М.Н. Жукова, В.В. Золотарев, И.В. Ковалев // Программные продукты и системы. – 2012. – № 2. – С. 70–74. – EDN OZYEVV.

Касимова Алина Ринадовна, старший преподаватель кафедры информационной безопасности ФГБОУ ВО «КНИТУ». Основное направление научных исследований – цифровые двойники в вопросах организации производства. E-mail: kasimovaar@corp.knrtu.ru

Воробьев Дмитрий Андреевич, ассистент кафедры безопасности информационных технологий Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнёва. Область научных интересов – разработка автоматизированных сценариев моделирования атак информационной безопасности. E-mail: h1ppyfox1@gmail.com

Севрунов Александр Николаевич, ассистент кафедры безопасности информационных технологий Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнёва. Область научных интересов – разработка автоматизированных сценариев моделирования атак информационной безопасности. E-mail: alexander.sevrunov@gmail.com

DOI: 10.17212/2782-2230-2024-2-9-24

Experience in conducting cyber exercises using a developed script *

A.R. Kasimova[1], D.A. Vorobiev[2], A.N. Sevrunov[3]

[1] *Kazan National Research Technological University, 68 Karl Marx Prospekt, Kazan, 420015, Russian Federation, senior lecturer of the Department of Information Security. E-mail: kasimovaar@corp.knrtu.ru*
[2] *Siberian State University of Science and Technology named after Academician M.F. Reshetnyova, 31 Avenue named after the newspaper "Krasnoyarsk Worker", Krasnoyarsk, 660037, Russian Federation, assistant of Department of Information Technology Security. E-mail: h1ppyfox1@gmail.com*
[3] *Siberian State University of Science and Technology named after Academician M.F. Reshetnyova, 31 Avenue named after the newspaper "Krasnoyarsk Worker", Krasnoyarsk, 660037, Russian Federation, assistant of Department of Information Technology Security. E-mail: alexander.sevrunov@gmail.com*

The threat of cyber attacks has become a serious problem for organizations, the solution of which also lies in the plane of modeling scenarios of possible attacks using digital twin technologies. A cyber polygon based on the AMPIRE software suite is used to study the impact of cyber threats. The attacker's scenario includes the use of various tactics and vulnerabilities, such as active scanning, provisioning, vulnerabilities in public applications, malicious links and files, and compromising domain user accounts. The vector of the malicious attack is related to the tactics, techniques and procedures of the Mitre ATT&CK matrix. Vulnerabilities include the wpDiscuz plugin, Zerologon, and the consequences of using Wordpress Shell and gaining unauthorized access. The ongoing intercollegiate cyber exercises have revealed strengths and weaknesses that need to be taken into account when conducting the following events. Scenario testing with the participation of universities showed the effectiveness of the complex in assessing the time required to close vulnerabilities and eliminate consequences. Implementation of different scenarios with specialized functionality at the cyber polygon makes it possible to form practical skills to prevent attacks on computer networks, and also allows you to analyze the situation, interact with other participating specialists.

Keywords: cyber learning, digital twin, mitre att & ck, digital twin, cyber polygon, attack vector, simulation, LAN

REFERENCES

1. Solominsky A.V., Zhelezin V.A., Mirgorodsky A.D., Krasnobaev S.V. Aktual'nye tendentsii na rynke informatsionnoi bezopasnosti [Current trends in the information security market]. *Vestnik nauki i obrazovaniya = Herald of Science and Education*, 2023, no. 8 (139). Available at: https://cyberleninka.ru/article/n/aktualnye-tendentsii-na-rynke-informatsionnoy-bezopasnosti (accessed 27.05.2024).

* *Received 20 March 2024.*

2. Kasimova R., Zolotarev V.V., Safiullina L.Kh., Sabirova D.I. Modelirovanie vektora setevykh atak na lokal'nuyu set' s primeneniem bazy MITRE ATT&CK [Modeling the network attack vector on a local network using the MITER ATT&CK]. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies*, 2023, no. 4 (64), pp. 88–96. DOI: 10.54398/20741707_2023_4_88.

3. Kasimova A.R., Safiullina L.Kh. [Use of digital twins in building the security system of the enterprise]. *Mezhdunarodnyi forum «Kazan Digital Week – 2022»* [Proceedings of the International forum "Kazan Digital Week – 2022"]. Kazan, 2022, pt. 1, pp. 291–298. (In Russian).

4. Shinkevich A.I., Nadezhdina M.E., Sopin V.F. Proektirovanie tsifrovogo dvoinika sistemy organizatsii proizvodstva [Designing a digital twin for a production organization system]. *Standarty i kachestvo = Standards and Quality*, 2024, no. 4, pp. 94–99. DOI: 10.35400/0038-9692-2024-4-197-23.

5. Shinkevich A.I., Kasimova A.R., Alekseeva A.A. Ispol'zovanie tsifrovykh dvoinikov dlya ekologizatsii khimicheskoi promyshlennosti [Use digital twins for greening the chemical industry]. *Izvestiya Samarskogo nauchnogo tsentra Rossiiskoi akademii nauk = Izvestia of Samara Scientific Center of the Russian Academy of Sciences*, 2023, vol. 25, no. 4, pp. 87–94.

6. Perukhin M.Yu., Vasileva M.Yu., Kadyrova G.K. Tsifrovoi dvoinik laboratorii sistem upravleniya khimiko-tekhnologicheskimi protsessami [Digital twin of the laboratory of control systems of chemical-technological processes]. *Sovremennye naukoemkie tekhnologii = Modern High Technologies*, 2021, no. 6-1, pp. 84–90. (In Russian).

7. Alekseeva A.A., Kasimova A.R. [Prospects for the application of digital twins with the purpose of greening production]. *Kompleksnoe izuchenie ekosistem gornykh territorii* [Comprehensive study of ecosystems in mountain areas]. Collection of materials from the VI Caucasian International Environmental Forum, Groznyi, 2023, pp. 16–19. DOI: 10.36684/102-1-2023-16-19. (In Russian).

8. Borovkov A.I., Ryabov Yu.A., Kukushkin K.V., Maruseva V.M., Kulemin V.Yu. Tsifrovye dvoiniki i tsifrovaya transformatsiya predpriyatii OPK [Digital twins and digital transformation of defense industry enterprises]. *Vestnik Vostochno-Sibirskoi otkrytoi akademii*, 2019, no. 32, pp. 1–39. (In Russian).

9. Shpak P.S., Sycheva E.G., Merinskaya E.E. Kontseptsiya tsifrovykh dvoinikov kak sovremennaya tendentsiya tsifrovoi ekonomiki [The concept of digital twins as a modern trend of digital economy]. *Vestnik Omskogo universiteta. Seriya: Ekonomika = Herald of Omsk University. Series "Economics"*, 2020, no. 1, pp. 57–68.

10. Khorzova I.S. [Application of cyber polygon capabilities for training and advanced training of information security specialists]. *Aktual'nye voprosy eksplu-*

atatsii sistem okhrany i zashchishchennykh telekommunikatsionnykh sistem [Current issues of operation of security systems and secure telecommunications systems]. Voronezh, 2021, vol. 2, pp. 46–47. (In Russian).

11. Holmes D., Papathanasaki M., Maglaras L., Ferrag M.A., Nepal S., Janicke H. Digital Twins and Cyber Security – solution or challenge ? *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*. IEEE, 2021, pp. 1–8. DOI: 10.1109/SEEDA-CECNSM53056.2021.9566277.

12. *Methodological support for the general Empire*. Perspective monitoring. Available at: Local access.

13. ATT&CK Matrix. Available at: https://attack.mitre.org/ (accessed 28.05.2024).

14. Oleynikova A.A., Zolotarev V.V. Kontseptsiya upravleniya informatsionnoi bez-opasnost'yu na osnove tsikla nepreryvnogo detektirovaniya i reagirovaniya na intsidenty bezopasnosti informatsii [The concept of information security management based on a cycle of information security incidents continuous detection and response]. *Izvestiya YuFU. Tekhnicheskie nauki = Izvestiya SFedU. Engineering sciences*, 2023, no. 5 (235), pp. 66–81. DOI: 10.18522/2311-3103-2023-5-66-81.

15. Zhukov V.G., Zhukova M.N., Zolotarev V.V., Kovalev I.V. Metodika postroeniya modeli bezopasnosti avtomatizirovannykh sistem [Method of construction the security model of automated systems]. *Programmnye produkty i sistemy = Software and Systems*, 2012, no. 2, pp. 70–74.

Для цитирования:

Касимова А.Р., *Воробьев Д.А.*, *Севрунов А.Н.* Опыт проведения киберучений с использованием разработанного сценария // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 9–24. – DOI: 10.17212/2782-2230-2024-2-9-24.

For citation:

Kasimova A.R, Vorobiev D.A., Sevrunov A.N. Opyt provedeniya kiberuchenii s ispol'zovaniem razrabotannogo stsenariya [Experience in conducting cyber exercises using a developed script]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 2 (113), pp. 9–24. DOI: 10.17212/2782-2230-2024-2-9-24.