О. Ю. САПОЖНИКОВ, А. М. ШАБАЛИН
Тюменский государственный университет, г. Тюмень
УДК 004.056.53

ОЦЕНКА УЯЗВИМОСТЕЙ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОРГАНИЗАЦИИ УЧЕБНОГО ЛАБОРАТОРНОГО СТЕНДА (НА ПРИМЕРЕ ВИРТУАЛЬНОЙ СРЕДЫ PROXMOX VE)

Аннотация. Статья посвящена выявлению критичных уязвимостей в базовой конфигурации системы Proxmox VE и построение модели потенциальных угроз с использованием методологии MITRE ATT&CK. Проведен практический аудит системы виртуализации с применением распространенных инструментов тестирования, результаты которого классифицированы по тактикам злоумышленников и оценены по шкале CVSS.

Ключевые слова: угрозы информационной безопасности, учебный лабораторный стенд, Proxmox VE, MITRE ATT&CK, hardening.

Введение. Современные образовательные учреждения активно применяют технологии виртуализации для построения учебных стендов, что позволяет повысить гибкость, доступность и эффективность учебного процесса [1, 2, 3]. Одним из популярных решений для реализации таких инфраструктур является гипервизор Proxmox VE. Однако его использование в базовой конфигурации несет определенные риски, связанные с отсутствием базовой предварительной настройки защитных механизмов и наличием уязвимостей, потенциально доступных даже при минимальной технической подготовке [4].

Для систематизации и анализа возможных угроз в виртуальных средах все шире применяется матрица MITRE ATT&CK — структурированная база знаний, описывающая тактики и техники, используемые злоумышленниками [5]. Ее применение в инфраструктурах, построенных на базе Proxmox VE, позволяет не только глубже понимать потенциальные сценарии атак, но и классифицировать выявленные уязвимости в привязке к типовым методам вторжений [6].

Одним из ключевых направлений обеспечения защищенности виртуальных стендов остается реализация комплекса мер по их укреплению. В сообществе пользователей Proxmox обсуждаются как вопросы изменения стандартных конфигураций, так и особенности внедрения регулярных обновлений, жестких политик аутентификации и контроля целостности. Отдельного внимания заслуживают исследования, демонстрирующие эффективность встроенного в Proxmox межсетевого экрана, способного при должной настройке противостоять сетевым угрозам [7].

В условиях, когда в инфраструктуре учебных заведений активно внедряются виртуальные среды, возникает необходимость в целенаправленном анализе уязвимостей базовой установки гипервизора Proxmox VE с опорой на современные методики моделирования угроз. Настоящее исследование направлено на решение этой задачи с использованием подходов, основанных на MITRE ATT&CK.

Проблема исследования. Несанкционированное вмешательство в работу учебного виртуального стенда может повлечь за собой ряд критических инцидентов, включая утечку конфиденциальных данных, несанкционированный доступ к ресурсам, компрометацию ком-

понентов системы и отказ в обслуживании. Учитывая потенциальную открытость учебной инфраструктуры и разнообразный уровень подготовки ее пользователей, нужно отметить, что даже незначительные уязвимости могут привести к серьезным последствиям.

Поэтому цель данного исследования заключается в выявлении потенциальных угроз с использованием методологии MITRE ATT&CK, что позволит разработать приоритетные меры защиты, направленные на повышение устойчивости и безопасности учебной виртуальной среды. В рамках исследования решались следующие задачи:

1. Проанализировать базовую конфигурацию гипервизора Proxmox VE, применяемого в учебной инфраструктуре, с целью выявления потенциальных уязвимостей;

2. Провести практическое тестирование системы с использованием инструментов информационной безопасности (Nmap, OWASP ZAP, Nikto, Lynis, Hydra) для оценки текущего состояния защищенности;

3. Сопоставить обнаруженные уязвимости с техниками, описанными в MITRE ATT&CK, с целью выявления сценариев возможного вмешательства;

4. Оценить критичность выявленных уязвимостей с применением шкалы CVSS.

Материалы и методы. Оценка защищенности гипервизора Proxmox VE проводилась в условиях лабораторного стенда, имитирующего работу учебной виртуальной среды. В качестве тестовой платформы использовалась базовая конфигурация Proxmox VE без предварительного hardening или применения дополнительных средств защиты. Это позволило получить объективное представление о возможных уязвимостях, которые остаются незакрытыми при стандартной установке системы.

Тестирование включало как пассивные, так и активные методы воздействия. Особое внимание уделялось воспроизведению сценариев, характерных для потенциальных нарушителей, обладающих различным уровнем подготовки (от типичного студента, обладающего базовыми навыками, до условно квалифицированного атакующего, использующего специализированные инструменты и документацию).

Анализ проводился с применением набора утилит, распространенных в практике информационной безопасности. Сканер Nmap использовался для выявления открытых портов и запущенных сервисов. Состояние веб-интерфейса анализировалось с помощью OWASP ZAP и Nikto, что позволило выявить уязвимости, связанные с HTTP-заголовками, SSL-сертификатами и доступностью страницы авторизации. Утилита Hydra применялась для подбора паролей к административным интерфейсам, а Lynis — для общего аудита системы, включая проверку конфигураций, политик доступа и наличия механизмов контроля целостности.

Для интерпретации полученных данных использовался комплексный подход. Каждая выявленная уязвимость классифицировалась в соответствии с тактиками и техниками, представленными в матрице MITRE ATT&CK, что позволило связать технические недостатки с потенциальными сценариями атак. Оценка критичности уязвимостей осуществлялась по шкале CVSS (Common Vulnerability Scoring System), обеспечивающей объективную количественную интерпретацию уровня риска. Дополнительно использовалась модель STRIDE, позволившая систематизировать возможные угрозы по следующим категориям: подмена, нарушение целостности, отказ от действий, раскрытие информации, отказ в обслуживании и повышение привилегий.

Тестовая инфраструктура включала гипервизор Proxmox VE, атакующий компьютер на базе Kali Linux с необходимым набором инструментов, а также изолированный сегмент виртуальной сети, воспроизводящий конфигурацию типичной лабораторной учебной среды.

Результаты. Проведенное тестирование позволило зафиксировать ряд системных, сетевых и конфигурационных уязвимостей, способных существенно снизить уровень защищенности учебной виртуальной среды при использовании Proxmox VE в стандартной установке. Полученные данные свидетельствуют о наличии уязвимостей на уровне веб-интерфейса и в конфигурации сетевых сервисов (например, SSH). Нарушения касаются как отсутствия базовых защитных механизмов, так и допущений в политике доступа, что создает возможности для реализации типовых векторов атак.

Например, в ходе анализа веб-интерфейса были выявлены отсутствующие HTTP-заголовки, повышающие риск известных типов атак (например, clickjacking, MIME-sniffing), а также обнаружено отсутствие политики HSTS, что допускает проведение атак типа downgrade. Использование неподписанного SSL-сертификата и доступность страницы входа без ограничений делают интерфейс уязвимым для атак с перебором учетных данных.

Сканирование сетевых портов показало наличие открытых служб, не требующихся для функционирования среды: устаревший протокол RPC, работающий на 111-м порту, и прокси-сервер Squid на 3128-м, не имеющий настроек фильтрации. Кроме того был зафиксирован активный SSH-сервис с разрешенным входом под root-пользователем и отсутствием ограничений по IP.

Дополнительный анализ конфигурации средствами Lynis выявил отсутствие контроля целостности файловой системы, ненастроенные политики блокировки при ошибках аутентификации и ряд других нарушений, снижающих устойчивость среды к попыткам несанкционированного доступа. Проведенная атака перебора паролей с использованием Hydra показала успешный подбор root-учетной записи при помощи стандартного словаря, что дополнительно подтверждает необходимость внедрения многофакторной аутентификации и ограничения числа попыток входа.

Систематизация всех выявленных уязвимостей, их классификация в соответствии с MITRE ATT&CK и оценка по шкале CVSS представлены в таблице 1.

Таблица 1

Классификация выявленных уязвимостей Proxmox VE

№	*Уязвимость*	*Инструмент*	*Категория ATT&CK*	*CVSS*	*Критичность*
1	Отсутствие заголовков безопасности	OWASP ZAP, Nikto	Defense Evasion (T1204.001)	6.1	Средняя
2	Слабая конфигурация SSH	Hydra, Nmap	Initial Access (T1110)	8.2	Высокая
3	Доступность RPC и Squid	Nmap	Discovery (T1046)	5.9	Средняя
4	Уязвимый загрузчик и отсутствие контроля целостности	Lynis	Privilege Escalation (T1547.001)	7.8	Высокая
5	Нет блокировки при брутфорсе	Hydra	Initial Access (T1078)	7.5	Высокая

Заключение. Анализ базовой конфигурации гипервизора Proxmox VE показал, что при отсутствии дополнительных мер по защите данная платформа подвержена ряду уязвимостей, способных быть использованными как в рамках учебной среды, так и за ее пределами. Особенно уязвимыми оказались компоненты, связанные с аутентификацией, конфигурацией SSH-сервера и веб-интерфейса, что создает условия для реализации атак на начальных этапах проникновения и последующего повышения привилегий.

Классификация уязвимостей по методике MITRE ATT&CK позволила не только описать технические недостатки, но и связать их с типовыми сценариями злоумышленной активности, что значительно повышает прикладную ценность проведенного анализа. Использование шкалы CVSS помогло определить приоритетность устранения каждой из уязвимостей, а применение модели STRIDE обеспечило всесторонний охват потенциальных рисков.

Таким образом, практическое тестирование подтвердило необходимость комплексного подхода к защите виртуальных сред, особенно при использовании гипервизоров в стандартной установке. В дальнейшем планируется разработка комплекса методических рекомендаций по безопасному внедрению и эксплуатации Proxmox VE, а также проведение повторного аудита после внедрения защитных мероприятий, направленных на повышение устойчивости системы к внешним воздействиям.

СПИСОК ЛИТЕРАТУРЫ

1. Шабалин А. М. Организация виртуальной облачной лаборатории для развития профессиональных компетенций в области сетевого и системного администрирования при подготовке будущих IT-специалистов / А. М. Шабалин, А. А. Захаров, Е. А. Калиберда, Н. В. Кенжалинова // Динамика систем, механизмов и машин. — 2023. — Т. 11, № 4. — С. 87-93. — DOI 10.25206/2310-9793-2023-11-4-87-93. — EDN GKBNYZ.
2. Шабалин А. М. Разработка программно-аппаратного стенда с применением современных средств виртуализации для изучения компьютерных сетей стандарта IEEE 802.11 / А. М. Шабалин, Е. А. Калиберда // Динамика систем, механизмов и машин. — 2022. — Т. 10, № 3. — С. 92-98. — DOI 10.25206/2310-9793-2022-10-3-92-98. — EDN YGCXTJ.
3. Овчинников Д. А. Использование технологии виртуализации в образовательном процессе / Овчинников Д.А., Газизов Т.Т. // Информация и образование: границы коммуникаций. — 2021. — № 13 (21). — С. 282–284. — EDN MTBBWE.
4. Obasuyi G. C. Security challenges of virtualization hypervisors in virtualized hardware environment / Obasuyi G. C., Sari A. // International Journal of Communications, Network and System Sciences. — 2015. — № 8(8). — P. 260–273. — DOI 10.4236/ijcns.2015.87026.
5. Xiong W. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix / Xiong W., Legrand E., Åberg O., Lagerström R. // Software and Systems Modeling. — 2022. — Т. 21, № 1. — С. 157–177. — DOI 10.1007/s10270-021-00898-7.
6. Фатеев А. Г. Защита среды виртуализации для обеспечения безопасности персональных данных / Фатеев А. Г., Алексеев В.М. // Труды Международного симпозиума "Надежность и качество". — 2016. — Т. 2. — С. 353–355. — EDN WHWMIX.
7. Ariyanto Y. Performance analysis of Proxmox VE firewall for network security in cloud computing server implementation / Ariyanto Y., Harijanto B., Firdaus V.A.H., Arief S.N. // IOP Conf. Series: Materials Science and Engineering. — 2020. — Т. 732, № 1 — С. 012081. — DOI 10.1088/1757-899x/732/1/012081.