CLAW

SUPERVISED EXTERNAL PENETRATION TEST

HUMAN-APPROVAL GATED

ENGAGEMENT REPORT

Force brain live scan (Ezekiel)

An authorized, scope-bound offensive security assessment conducted under supervised autonomy. Every intrusive action passed a scope guard and a human-approval gate before dispatch.

CLIENT	REPORT DATE	STATUS	FINDINGS
Z7 internal	2026-06-16	Aborted	29

CONFIDENTIAL

SECTION 01

Scope and Authorization

This engagement was bound to the targets listed below. The scope guard rejected any action against a target outside this set. Authorization was signed before any testing began.

In-Scope Targets

`192.168.68.1`

AGENT TYPES	recon, attack_surface
ENGAGEMENT CREATED	2026-06-14
TESTING STARTED	2026-06-14 22:44 UTC
TESTING COMPLETED	2026-06-15 01:23 UTC

Engagement Description

First Ezekiel-driven supervised recon + attack-surface against own lab gateway

Authorization Attestation

AUTHORIZED BY	zack@z7solutions.com
AUTHORIZATION DATE	2026-06-14 22:44

Rules of Engagement

Lab self-test, explicitly authorized by Zack Aleksic. Own UniFi gateway 192.168.68.1. Autonomous recon + attack-surface only; intrusive actions gated for human approval.

Signed Authorization Hash

```
4bc564ceacea9293723a5c35d5e5ca493b48152f479dbc609b1f7fef474e6a31
```

SECTION 02

Executive Summary

This assessment recorded 29 findings across the authorized scope. 5 intrusive actions were gated for human approval before any dispatch, of which 0 were approved. The control plane recorded 41 audit events. All counts below reflect exactly what the platform observed and recorded.

29	5	0	41
TOTAL FINDINGS	GATED ACTIONS	HUMAN APPROVED	AUDIT EVENTS

Findings by Severity

0	0	0	1	28
CRITICAL	HIGH	MEDIUM	LOW	INFO

SECTION 03

Findings

Findings recorded during the engagement, grouped by severity. Each finding lists the affected asset, the phase and technique that surfaced it, and remediation guidance where available.

Low 1 finding

Self Signed SSL Certificate

LOW

TARGET 192.168.68.1:443 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

self-signed-ssl

Informational 28 findings

Open port: 22/tcp

INFORMATIONAL

TARGET 192.168.68.1 PHASE attack_surface TECHNIQUE T1046 CONFIDENCE Medium EXPLOITABILITY Theoretical

22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u7 (protocol 2.0)

Open port: 53/tcp

INFORMATIONAL

TARGET 192.168.68.1 PHASE attack_surface TECHNIQUE T1046 CONFIDENCE Medium EXPLOITABILITY Theoretical

53/tcp open domain NLnet Labs NSD

Open port: 80/tcp

INFORMATIONAL

TARGET 192.168.68.1 PHASE attack_surface TECHNIQUE T1046 CONFIDENCE Medium EXPLOITABILITY Theoretical

80/tcp open http nginx

Open port: 443/tcp

INFORMATIONAL

TARGET 192.168.68.1 PHASE attack_surface TECHNIQUE T1046 CONFIDENCE Medium EXPLOITABILITY Theoretical

443/tcp open ssl/http nginx

Open port: 6789/tcp

INFORMATIONAL

TARGET 192.168.68.1 PHASE attack_surface TECHNIQUE T1046 CONFIDENCE Medium EXPLOITABILITY Theoretical

6789/tcp open ibm-db2-admin?

Open port: 8080/tcp

INFORMATIONAL

TARGET 192.168.68.1 PHASE attack_surface TECHNIQUE T1046 CONFIDENCE Medium EXPLOITABILITY Theoretical

8080/tcp open http Apache Tomcat (language: en)

Open port: 8443/tcp

INFORMATIONAL

TARGET 192.168.68.1 PHASE attack_surface TECHNIQUE T1046 CONFIDENCE Medium EXPLOITABILITY Theoretical

8443/tcp open ssl/http Apache Tomcat (language: en)

WAF Detection

INFORMATIONAL

TARGET https://192.168.68.1 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

waf-detect

SSH Auth Methods - Detection

INFORMATIONAL

TARGET 192.168.68.1:22 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

ssh-auth-methods

SSH Server Software Enumeration

INFORMATIONAL

TARGET 192.168.68.1:22 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

ssh-server-enumeration

OpenSSH Service - Detect

INFORMATIONAL

TARGET 192.168.68.1:22 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

openssh-detect

TLS Version - Detect

INFORMATIONAL

TARGET 192.168.68.1:443 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

tls-version

TLS Version - Detect

INFORMATIONAL

TARGET 192.168.68.1:443 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

tls-version

Wappalyzer Technology Detection

INFORMATIONAL

TARGET https://192.168.68.1 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

tech-detect

IKEv2 Supported Transforms - Enumeration

INFORMATIONAL

TARGET 192.168.68.1:500 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

ikev2-transforms-enum

robots.txt file

INFORMATIONAL

TARGET https://192.168.68.1/robots.txt PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

robots-txt

XSS-Protection Header - Cross-Site Scripting

INFORMATIONAL

TARGET https://192.168.68.1 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

xss-deprecated-header

robots.txt endpoint prober

INFORMATIONAL

TARGET https://192.168.68.1/robots.txt PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

robots-txt-endpoint

UniFi OS - Panel

INFORMATIONAL

TARGET https://192.168.68.1/login PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

unifi-os-panel

HTTP Missing Security Headers

INFORMATIONAL

TARGET https://192.168.68.1 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

http-missing-security-headers

HTTP Missing Security Headers

INFORMATIONAL

TARGET https://192.168.68.1 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

http-missing-security-headers

HTTP Missing Security Headers

INFORMATIONAL

TARGET https://192.168.68.1 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

http-missing-security-headers

HTTP Missing Security Headers

INFORMATIONAL

TARGET https://192.168.68.1 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

http-missing-security-headers

HTTP Missing Security Headers

INFORMATIONAL

TARGET https://192.168.68.1 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

http-missing-security-headers

HTTP Missing Security Headers

INFORMATIONAL

TARGET https://192.168.68.1 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

http-missing-security-headers

Weak HTTP Strict-Transport-Security - Detect

INFORMATIONAL

TARGET https://192.168.68.1 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

weak-hsts-detect

PTR Detected

INFORMATIONAL

TARGET 1.68.168.192.in-addr.arpa PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

ptr-fingerprint

SSL DNS Names

INFORMATIONAL

TARGET 192.168.68.1:443 PHASE known_cve TECHNIQUE T1595.002 CONFIDENCE Medium EXPLOITABILITY Theoretical

ssl-dns-names

SECTION 04

Intrusive Actions Gated for Approval

Intrusive and destructive actions never run autonomously under Z7 Claw Force. Each was held at a human-approval gate. The table records what was requested, the risk tier, and the human decision. 0 approved, 0 denied, 5 still pending.

ACTION	TARGET	TOOL	RISK TIER	DECISION
metasploit against 192.168.68.1	192.168.68.1	metasploit	Intrusive	PENDING
sqlmap against 192.168.68.1	192.168.68.1	sqlmap	Intrusive	PENDING
netexec against 192.168.68.1	192.168.68.1	netexec	Intrusive	PENDING
secretsdump against 192.168.68.1	192.168.68.1	secretsdump	Intrusive	PENDING
getuserspns against 192.168.68.1	192.168.68.1	getuserspns	Intrusive	PENDING

SECTION 05

Audit Timeline

The control plane writes an append-only audit event for every consequential decision. UPDATE and DELETE are revoked on the audit table at the database level, so this record cannot be altered after the fact.

2026-06-14 22:44 UTC **Engagement created**
Actor: user

2026-06-14 22:44 UTC **Authorization signed**
Actor: zack@z7solutions.com

2026-06-14 22:44 UTC **Engagement started**
Actor: user

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Action dispatched to worker**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Action dispatched to worker**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Action dispatched to worker**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Action dispatched to worker**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Action dispatched to worker**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Action dispatched to worker**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Action dispatched to worker**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Action dispatched to worker**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Action dispatched to worker**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Approval requested for intrusive action**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Approval requested for intrusive action**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Approval requested for intrusive action**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Approval requested for intrusive action**
Actor: orchestrator

2026-06-14 22:45 UTC **Target allowed by scope guard**
Actor: orchestrator

2026-06-14 22:45 UTC **Approval requested for intrusive action**
Actor: orchestrator

2026-06-14 22:48 UTC **Action completed**
Actor: worker:gizmo-worker-1

2026-06-14 22:48 UTC **Action completed**
Actor: worker:gizmo-worker-1

2026-06-14 22:51 UTC **Action completed**
Actor: worker:gizmo-worker-1

2026-06-14 22:51 UTC **Action completed**
Actor: worker:gizmo-worker-1

2026-06-14 22:52 UTC **Action completed**
Actor: worker:gizmo-worker-1

2026-06-14 22:52 UTC **Action completed**
Actor: worker:gizmo-worker-1

2026-06-14 22:53 UTC **Action completed**
Actor: worker:gizmo-worker-1

2026-06-14 22:53 UTC **Action completed**
Actor: worker:gizmo-worker-1

2026-06-14 22:53 UTC **Action completed**
Actor: worker:gizmo-worker-1

2026-06-15 01:23 UTC **Engagement aborted (kill switch)**

Actor: user
