AUTOMATIC EXPLOITATION SOFTWARE (PAL-AES) DATASHEET

The PALAMYS system (Controlled/Customizable Strategic DDoS) is a purpose-built DDoS simulation and penetration-testing platform designed for special units and cyber-range operators who need the most realistic, operationally relevant attack emulation. Developed from real-world cyber-warfare observations and modern DDoS trends, PALAMYS combines powerful, field-proven attack techniques with an operator-friendly control surface so teams can design, schedule, execute and analyze realistic denial-of-service scenarios without excessive operational overhead.

PALAMYS replicates modern adversary behavior across volumetric, protocol and application layers while giving defenders the observability and repeatability required for high-value training and readiness exercises. The system was architected to reflect cyber threat evolution — from amplified reflection attacks and IoT/VM-based botnets to sophisticated HTTP/2 and browser-emulation application floods — and to let blue teams test detection, mitigation and incident-response playbooks under controlled but realistic pressure.

Key capabilities:

- High-impact volumetric & reflection attacks: generate amplified/reflective traffic against web apps, DNS, NTP, COAP, WSD and other vulnerable services to emulate real amplification campaigns.
- Autonomous discovery & augmentation: continuously scan the Internet to discover additional reflector/attack nodes and automatically incorporate them into campaigns.
- Botnet lifecycle management: add, remove and orchestrate attack nodes (bot/VM/reflector fleets) with fine-grained control over behavior, persistence and geographic distribution.
- Scheduled, automated campaigns: create reusable scenarios and run full attack playbooks on demand or on a calendar to support exercises and long-term readiness validation.
- Target reconnaissance & adaptive strategy: automated target profiling (application fingerprinting, API discovery, CDN/WAF detection, origin IP tracing) and automated selection of the most effective attack vectors.
- Visual attack path mapping: interactive visualizations of attack flows, vectors and impact metrics so operators can explain lessons learned to technical and non-technical stakeholders.

Automatic Exploitation Software (PAL-AES)

The Automatic Exploitation Software or The Exploit & Scan module is the offensive automation engine within the PALAMYS platform. It contains programmable traffic generators, multi-vector reflection orchestrators, active and passive reconnaissance tools, and automated exploitation routines. The module is engineered to deliver realistic, high-fidelity attack traffic and to expand the controlled attack asset pool while preserving strict governance, auditability and safety controls required for sanctioned cyber-range exercises.

Attack traffic capabilities

UDP-based traffic vectors

The engine supports multiple UDP flood variants, including:

- **Large-packet UDP floods (UDP-BIG)** — transmits oversized, randomized UDP packets to exhaust target network capacity and state handling.
- **Small-packet high-rate UDP floods (UDP-PPS)** — generates extremely high-packet-per-second loads using small-sized UDP packets to stress packet-processing and interrupt handling on the target.

TCP-based traffic vectors

Comprehensive TCP-layer attacks are supported, including:

- **TCP window-size manipulation (TCP-WIN)** — issues TCP SYN packets with crafted window header values to stress connection state and resource tracking.
- **SYN flood (TCP-SYN)** — aggressive SYN stream generation to exploit TCP three-way handshake mechanism.
- **ACK flood (TCP-ACK)** — high-volume ACK packets sent to targets in order to to amplify connection churn and CPU/network load.
- **TCP Fast Open abuses (TCP-TFO)** — Exploit the TCP Fast Open mechanism to initiate attacks .
- **TLS-targeted load (TCP-TLS)** — Exploits TCP connections protected by the Transport Layer Security (TLS) protocol, targeting the TLS handshake process, flooding the server with computational intensity cryptographic computation requests, thereby overloading server resources.

Reflection & amplification attack orchestration

Multi-vector reflective attacks are orchestrated using a variety of misconfigured or amplifying services:

- **Mixed amplification (MIX-AMP)** — Combines multiple reflection/amplication attack vectors to initiate an attack .
- **DNS amplification (DNS-AMP)** — Exploits open DNS servers to generate response traffic that floods the target with DNS responses.
- **ARD amplification (ARD-AMP)** — Exploiting vulnerabilities in application-layer protocols to generate amplified traffic aimed at the target .
- **WSD amplification over UDP (WSD UDP)** — Exploits the dynamic Web service discovery protocol (WSD), which operates on UDP, generating response traffic to the target.
- **CoAP amplification over UDP (COAP UDP)** — exploits Constrained Application Protocol COAP endpoints (commonly IoT), generate response traffic from IoT devices or COAP-enabled servers to the target.

- **SADP amplification (SADP AMP)** — Exploit the SADP protocol, generate response traffic from devices using SADP towards the target.

Target reconnaissance & profiling

The module offers both active and passive scanning, reconnaissance of the target, provide information and report to the control component & planning:

- **Firewall and network-layer detection** — identify DNS firewall layers in use (if any), presence of WAFs, and defensive intermediaries.
- **Backend & origin discovery** — detect backup servers and actual servers behind (if any), origin servers and upstream/backup hosts behind CDNs or reverse proxies.
- **Application fingerprinting** — enumerates running services, versions and potential attack surfaces; identifies high-probability exploitation points.
- **System/Vendor informaion & success-probability estimation** — correlates vendor footprints and historical vulnerability data to estimate exploit likelihood.
- **Proposal for Effective attack-plan** — synthesizes reconnaissance data to propose the most effective attack plan and sizing for a given objective.

All reconnaissance activities are logged in detail and presented as readable reports for operator review.

Scanning, acquisition & expansion of Botnet

- **Automated discovery scans** — actively probe the Internet to find hosts and services exhibiting exploitable misconfigurations (includes, at minimum, common reflector and IoT services).
- **Asset onboarding workflows** — discovered, qualifying hosts can be queued for controlled exploitation, tagging, and inclusion into the managed asset registry.
- **Inventory management** — maintain status (susceptible, exploited, quarantined), per-host metadata and contribution capacity metrics.

These mechanisms are governed by policy constraints and safety checks to prevent uncontrolled or illegal operations.

Automated exploitation & persistence

- **Vulnerability Exploitation and Backdoor Installation (Backdoor Agent)** — automatically exploit vulnerabilities on the target, install backdoor control software (Backdoor Agent) on targets where command-execution privileges are available, serving the purpose of maintaining access connections, exploiting and using for other purposes.
- **Agent lifecycle management** — deployed agents are tracked, updated, and may be safely removed; all actions are auditable.
- **Use-cases** — long-term red-team persistence within contained testbeds, capability demonstrations, and repeatable scenario creation for defender training.

Table 1: Performance Maintenance (system-wide)

Metric	Minimum
Maximum sustained attack throughput (aggregate)	**≥ 80 Gbps**
Initial & maintained real compromised asset pool (real distributed vulnerable hosts (compromised/controlled assets)	**≥ 100,000** nodes

Safety, governance & observability

- **Policy enforcement** — pre-execution checks against allowed-target lists, geographic constraints, vector whitelists/blacklists, and time windows.
- **Human-in-the-loop gating** — destructive or high-risk operations require multi-role approvals before execution.
- **Kill-switch & throttles** — immediate global stop controls and per-target throttling to limit collateral impact.
- **Detailed telemetry** — per-vector metrics (pps, bps, error rates), per-host participation, amplification ratios, and attack outcome summaries are collected and stored for analysis.
- **Audit trail** — full recording of scan/exploit attempts, operator decisions, and agent actions retained for after-action reviews.

Integration & reporting

- **Controller integration** — full orchestration via the platform Controller for planning, scheduling and coordination with Connector and Command Distribution services.
- **Exportable reports** — standardized, human-readable reports and machine-readable logs for post-exercise analysis, compliance reviews and training documentation.

Licensing & initial asset provisioning

- **Usage license**: Perpetual or year-base.
- **Installation license**: Unlimited/limited installations permitted.
- **Update & maintenance**: Maintenance service for updates, security patches and support.
- **Initial supplied exploited-asset baseline**: System is provisioned with and maintains access to **no fewer than 100,000** real distributed vulnerable hosts (compromised/controlled assets) as part of the platform offering; this pool is actively maintained and refreshed during the contracted maintenance term.