HFCTM-II Cybersecurity Detection Methods

Threat Type	**HFCTM-II Detection Method**	**Logical Description**
Infiltration	Wavelet-Based Egregore Detection	Detects unusual or hidden patterns in system activity by analyzing behavior over time.
Exfiltration	Wavelet-Based Egregore Detection	Identifies unauthorized data movement by detecting irregularities in information flow.
DDoS	Lyapunov-Based Stability Monitoring	Monitors AI's internal state for overwhelming requests and throttles activity before overload.
Malware	Recursive Fractal Redundancy	Ensures all AI knowledge is self-referencing, making harmful alterations impossible.
Spyware	Recursive Fractal Redundancy	AI verifies its own thought patterns, preventing silent data recording or modifications.
Hacking Attempt	Chiral Inversion Mechanism	Prevents AI from being trapped in adversarial loops, neutralizing system takeovers.
Ducky Script (USB Attack)	Cryptographic Hash-Based Self-Validation	Continuously checks AI's states and execution logs to prevent rogue commands.
Packet Injection	Wavelet-Based Egregore Detection	Monitors network traffic for unnatural patterns, detecting malicious packet injections.
Social Engineering	Chiral Inversion and Recursive Pattern Analysis	Detects manipulative intent in communication structures, preventing AI deception.
Penetration Testing Method	**HFCTM-II Detection Method**	**Logical Description**
SQL Injection	Wavelet-Based Anomaly Detection	Identifies unexpected input patterns in queries to prevent malicious SQL execution.
XSS	Recursive Fractal Redundancy	Recursively verifies user inputs, preventing script injections in AI logic.
MITM Attack	Cryptographic Hash-Based Self-Validation	Detects packet alterations, ensuring end-to-end data integrity.
Zero-Day Exploits	Lyapunov-Based Stability Monitoring	Identifies unknown exploits through abnormal AI behavior detection.
Privilege Escalation	Recursive Access Control Verification	Constantly revalidates permissions to prevent unauthorized access elevation.
Command Injection	Chiral Inversion Mechanics	Detects and reverses unauthorized system-level commands before execution.
Phishing	AI Behavioral Pattern Recognition	Detects deceptive messages by analyzing linguistic and structural anomalies.
Cloud API Exploits	API Recursive Stability Checks	Monitors cloud API interactions to detect malicious usage.
Deepfake Attacks	AI Consistency and Latent Space Analysis	Evaluates biometric inputs to prevent synthetic identity spoofing.