FORENSIC INCIDENT REPORT

IoT Honeypot System — ESP32 Based Intrusion Detection

Generated: 2026-06-04 17:39:24

1. Executive Summary

Field	Value
Total Attack Events Logged	4
First Attack Detected	2026-06-04 07:59:35
Most Recent Attack	2026-06-04 08:11:04
Unique Attack Types	2
Unique Attacker IPs	2
Monitored Ports	Port 23 (Telnet), Port 80 (HTTP)
Honeypot Device	ESP32 NodeMCU IoT Honeypot

2. Attack Type Analysis

Attack Type	Count	Percentage	Description
http_brute_force	3	75.0%	HTTP POST login attempt on admin panel
brute_force	1	25.0%	Repeated login attempts with credentials on Telnet

3. Top Attacker IP Addresses

Rank	IP Address	Total Attacks	Percentage
1	192.168.1.21	3	75.0%
2	192.168.1.28	1	25.0%

4. Full Attack Event Log

#	IP Address	Port	Attack Type	Payload	Timestamp
4	192.168.1.21	80	http_brute_force	user=fsdfnigga&pass=sdf	2026-06-04 08:11:04
3	192.168.1.21	80	http_brute_force	user=domain&pass=sdf	2026-06-04 07:59:57
2	192.168.1.21	80	http_brute_force	user=86687&pass=sdf	2026-06-04 07:59:50
1	192.168.1.28	23	brute_force	asd	2026-06-04 07:59:35

5. Conclusion & Recommendations

This forensic report documents 4 attack events detected by the ESP32-based IoT Honeypot system deployed on the office network. The honeypot simulated a vulnerable IoT device exposing Telnet (port 23) and HTTP (port 80) services to attract unauthorized access attempts. The most common attack type

detected was http_brute_force, accounting for 75.0% of all recorded events. All attack evidence has been preserved in the database with full forensic details including IP address, timestamp, port, attack classification, and payload.

Recommendations:

1. Block all IP addresses identified as port scanners at the firewall level.
2. Implement rate limiting on Telnet and HTTP services to slow brute force attempts.
3. Enable real-time email alerts for critical attack events.
4. Review attack logs weekly to identify new attack patterns.
5. Consider expanding honeypot to monitor additional ports (21, 22, 443, 8080).
