AK

Abel Kolawole

Document Title:	Security Incident Investigation Report
Case ID:	NSM-5T-2024-001
Author:	Abel Kolawole
Date:	January 5, 2024

1. Objective

The primary objective of this investigation was to identify the source and scope of a network compromise involving unauthorized command execution and data exfiltration. Using 5-tuple analysis, the goal was to reconstruct the attacker’s timeline, identify the specific data stolen, and provide actionable remediation steps to isolate the compromised host and secure the infrastructure.

2. Tools & Environment

- Security Onion: Intrusion Detection and Network Security Monitoring (NSM) suite.
- Sguil: Triage of high-priority security alerts.
- Wireshark: Deep Packet Inspection (DPI) and TCP stream reconstruction.
- Kibana: Historical log correlation and file metadata analysis.
- Wormhole.app: Utilized via an in-VM anonymous browser for secure, encrypted, and ephemeral transmission of evidence files and logs to external stakeholders while maintaining host anonymity.

3. Observations

- Initial Detection: A high-priority alert was flagged in Sguil (GPL ATTACK_RESPONSE) indicating an unauthorized whoami command.
- Attacker Profile: Through 5-tuple analysis, the source was identified as 209.165.200.235 (Source Port 1234) targeting an internal host 192.168.0.11 (Destination Port 80) via TCP.
- Privilege Escalation: Packet analysis in Wireshark confirmed exploitation of the r3d_dr4g0n vulnerability, escalating privileges to root.
- Data Exfiltration: Kibana logs confirmed an FTP session where confidential.txt was transferred externally (MIME: text/plain).
- Evidence Handling: Evidence was securely transferred using Wormhole.app via an anonymous in-VM browser.

4. Conclusion

The investigation confirmed a successful root-level compromise of the target host. The adversary pivoted from a web-based exploit to full system control and data theft. Mitigation relied on rapid 5-tuple identification and subnet isolation.

5. Recommendations

- Immediate Isolation: Disconnect host 192.168.0.11 to prevent lateral movement.
- Identity Overhaul: Mandatory credential reset for all accounts.
- Vulnerability Remediation: Immediate patching of exploited services.
- Firewall Hardening: Blacklist the malicious 5-tuple and IP range.

6. References

- Cisco CyberOps Associate Curriculum - Lab: Isolate Compromised Host Using 5-Tuple
- Community Insights: r/Cybersecurity Subreddit - Incident Response Best Practices