# Cyber Security Network Vulnerability Report Instructions

**Objective:** This exercise aims to develop your skills in analyzing network security logs to identify Indicators of Compromise (IOCs) and construct a timeline of a cyberattack. You will utilize Security Onion 16.04 and Kabana to analyze the provided logs and assess the effectiveness of mitigation efforts.

**Resources:**

* Security Onion 16.04 virtual machine (pre-loaded with attack logs)
* Kabana

**Instructions:**

1. **Review the Network Logs:**
   * Access the Security Onion VM and utilize tools to examine the provided network security logs.
   * Utilize the filtering techniques learned in previous exercises.
   * Focus on logs generated during the timeframe of the simulated attack.
2. **Identify Indicators of Compromise (IOCs):**
   * Analyze the logs for suspicious activities such as:
     + Unauthorized access attempts
     + Unusual network traffic patterns
     + File modifications or deletions
     + Failed login attempts from unknown sources
     + System resource anomalies
3. **Construct a Timeline of Events:**
   * Based on the identified IOCs, build a chronological sequence of events leading up to the attack and potential compromise.
   * Include timestamps, affected systems, and types of suspicious activities in the timeline.
4. **Verify Mitigation Effectiveness:**
   * Analyze logs post-mitigation efforts to identify if the compromised hosts remain secure.
   * Look for continued malicious activity or recurring IOCs.
   * Determine if additional mitigation steps are necessary.
5. **Document Your Findings:**
   * Utilize the provided report template (see below) to record your analysis.
   * Include the constructed timeline, identified IOCs, and conclusions regarding mitigation effectiveness.

**Guiding Questions for Analysis:**

* What types of suspicious activities did you identify in the logs?
* Can you correlate specific IOCs with different stages of the attack?
* Based on the timeline, what was the potential entry point for the attackers?
* Did the implemented mitigations successfully remove the attackers and secure the compromised systems?
* What additional recommendations would you suggest for improving the network security posture?

**Cyber Security Analyst Program**

**CYBERRANGE CAPSTONE PROJECT**

****

**Cyber Security Network Vulnerability Report**

**Tremaine Hinds**

**Due Date: August 23rd, 2024**

Table of Contents

[1. Introduction: IV](#_Toc174198062)

[2. Methodology: IV](#_Toc174198063)

[3. Findings: V](#_Toc174198064)

[Unusual Activity and Geographic Dispersion V](#_Toc174198065)

[4. Timeline of Events: VI](#_Toc174198066)

[5. Mitigation Effectiveness: VIII](#_Toc174198067)

[6. Recommendations: VIII](#_Toc174198068)

[7. Conclusion: X](#_Toc174198069)

[**8. Appendices**: XI](#_Toc174198070)

[Appendix A: Detailed Network Map of Identified Hosts XI](#_Toc174198071)

[Appendix B: External IP Addresses and Geographic Dispersion XI](#_Toc174198072)

**Report Title:** Indicators of Compromise Comprehensive Report

**Investigator Name:** Tremaine Hinds

**Date:** 20/02/2022

**Executive Summary:** This report provides a comprehensive analysis of the cybersecurity incident that occurred on February 18, 2022, affecting the Foundation for Atropistan K-series-Graphene from Exfoliation (FAKE). The incident was identified during a beta testing phase of FAKE's new remote access and continuous development pipeline initiatives. The Elite Eyes&Ears team (E3), responsible for FAKE's IT security, reported breaches and initiated the Incident Response (IR) process.

Key findings of the report include:

* Indicators of Compromise (IOCs)
* Event Timeline
* IR Actions and Effectiveness
* Network Map and Host Analysis
* Lateral Movement and Persistence
* Critical Hosts and Attack Goals

This report aims to provide actionable insights and recommendations to strengthen FAKE's cybersecurity posture, ensuring enhanced readiness against future threats. The findings will assist in refining the Incident Response process and improving overall network security.

**Scope of The Assessment**

The scope of this assessment includes the following key tasks and objectives:

Analyze the logs leading up to the Incident Response (IR) intervention.

Examine logs post-intervention to understand the sequence of events and any subsequent activities.

Ensure that no malware remains on the compromised systems.

Verify the effectiveness of the IR team's actions in eradicating any threats.

Identify IOCs that led to the discovery of compromised machines.

Use these IOCs to understand the nature and extent of the attack.

Event Identification:

Determine the types of events that most likely occurred based on the identified IOCs.

Assess whether the IR team's actions were successful in mitigating the attack.

Determine if the attack resumed after the IR team's intervention.

Construct a detailed timeline of the events leading up to and following the IR intervention.

Identify key moments and actions taken during the incident.

Network Map Creation:

Create a network map of all identified hosts based on the provided data.

Highlight any unexpected protocols and types of network traffic that should be actively searched for.

Identify Anomalies:

Determine which workstation first exhibited significant unlikely activities.

Identify any files indirectly associated with the network activity.

Pinpoint which admin user was compromised shortly after the incident.

Assess Lateral Movement Techniques:

Identify the living off the land techniques used by the attacker to move laterally within the network.

Report on Attack Goals:

Determine the attackers' goals and which critical hosts were targeted.

Report the achieved goals to the IR team for immediate action.

The assessment aims to provide a comprehensive understanding of the incident, confirm the effectiveness of the response, and identify any areas for improvement in FAKE's security posture.

## 1. Introduction:

* **In the digital age, robust cybersecurity is essential for all organizations. Foundation for Atropistan K-series-Graphene from Exfoliation (FAKE) outsourced IT protection to Elite Eyes&Ears (E3) and provided in-house security training. However, increased collaboration and remote access expanded FAKE's attack surface. To safeguard their systems during beta testing, FAKE's web team used open-source and proprietary code while E3's red team simulated attacks. This proactive approach aimed to identify vulnerabilities and improve incident response (IR) procedures. On February 18, 2022, multiple security breaches were reported. The IR team promptly shut down affected systems and reset passwords. The blue team is currently investigating logs for malware. This report analyzes the incident, identifies Indicators of Compromise (IOCs), and evaluates the IR team's response. Its goal is to understand the attack, determine its impact, and ensure the network is secure**.

## 2. Methodology:

* The tools and techniques used for analyzing the network logs include Security Onion 16.04 and Kibana.

## 3. Findings:

### Unusual Activity and Geographic Dispersion

Our network traffic analysis detected suspicious activity originating from various countries, indicating a potential coordinated attack.

* **Global Origin:** Network connections were traced to multiple countries, including Spain, Portugal, China, the USA, Jamaica, Iran, the Netherlands, Singapore, and Ukraine. This widespread activity is highly unusual.
* **Threat Actor Indicators:** Specific IP addresses displayed behaviors linked to known malicious actors, such as Cobalt Strike, Trickbot malware, and SQL injection attempts.
* **Credential Compromise:** Evidence of brute-force attacks, particularly from Ukraine, suggests attempts to steal user credentials.

A detailed breakdown of IP addresses, locations, and malicious actions is provided in Appendix C.

* Phishing Incident

During our analysis of network traffic, several logs have flagged potential phishing activities. On February 18, 2022, emails originating from the IP address 13.248.65.126 and sent to 10.0.100.10 exhibited multiple signs of suspicious activity. These emails, which lacked TLS encryption, were vulnerable due to the insecure nature of the communication. For instance, an email from promos@walmart.com with the subject line "Scoops scoops" was directed to recipient jlouis, while another from toyota@toyota.atr with the subject "Gotta love this" targeted mdoe. These emails utilized a questionable HELO identifier ([149.6.203.167]) and were successfully queued despite these irregularities. Additionally, HTTP connections involving 149.6.203.167 and the internal IP 172.16.10.10 showed brief durations and minimal data exchanges, suggesting possible command and control (C2) communications. These observations are consistent with known phishing strategies designed to evade security filters.

* Privilege Escalation Incident

On February 18, 2022, instances of Event Code 4672 were recorded, signaling the creation of new logon sessions with elevated privileges. One of these sessions, initiated by the SYSTEM account, was granted permissions such as SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, and SeDebugPrivilege. These are high-level permissions typically reserved for administrative or system accounts. The presence of such log entries is essential for security monitoring, as unauthorized access to these privileges can indicate a potential security breach.

* Suspicious inbound traffic targeting MySQL

On the 18th at 1:33:50 PM, the network intrusion detection system identified unusual inbound traffic targeting a MySQL database server. This suspicious activity originated from an external IP address (31.217.252.15) and was directed towards an internal server (10.0.10.10). The system's alert mechanism was triggered due to a pattern matching known malicious behaviors associated with MySQL servers. While the traffic was permitted to pass through the network for further analysis, it was flagged as potentially harmful and requires additional investigation.

* Data Exfiltration Attempt

On February 18, 2022, a command-line action was executed by the user FAKENode, utilizing the Windows Command Prompt to checkout files from an internal Subversion repository for instance the repository located at http://10.0.18/svn/admin\_tools. This operation, requiring authentication with the credentials 'rbronrone' and 'potato', was initiated by the process cmd.exe (Process ID 2884). Such command-line interactions with HTTP servers, especially those involving credentialed access to internal repositories, warrant close examination due to their potential implications for security and unauthorized data access. This log is crucial for understanding the command-line activities that interact with external or internal web servers, which could be part of an attacker's toolkit for data exfiltration or unauthorized access

## 4. Timeline of Events:

| **Start Time** | **End Time** | **Event Description** | **IOC (Indicator of Compromise)** | | **Rationale** |
| --- | --- | --- | --- | --- | --- |
| February 18, 2022 09:15 AM | February 18, 2022 09:30 AM | Data Exfiltration Attempt | Command-line action by user FAKENode executing svn checkout to retrieve files from http://10.0.10.8/svn/admin\_tools. | This action indicates potential unauthorized access to sensitive data. The checkout command can be used to extract internal resources, suggesting a possible data breach. Additionally, saving data locally enables attackers to stage exfiltration without immediate detection. | |
| February 18, 2022 10:00 AM | February 18, 2022 10:05 AM | Phishing Incident | Multiple logs flagged emails from IP 13.248.65.126 to internal address 10.0.100.10. The emails may contain suspicious links or attachments. | | This action indicates potential unauthorized access to sensitive data. The checkout command can be used to extract internal resources, suggesting a possible data breach. Additionally, saving data locally enables attackers to stage exfiltration without immediate detection. |
| February 18, 2022 11:00 AM | February 18, 2022 11:10 AM | Privilege Escalation Incident | Instances of Event Code 4672 recorded, indicating special privileges assigned to users, particularly via Wks1 at 8:27:36 and other logins at 17:20:49. | | This action indicates potential unauthorized access to sensitive data. The checkout command can be used to extract internal resources, suggesting a possible data breach. Additionally, saving data locally enables attackers to stage exfiltration without immediate detection. |

## 5. Mitigation Effectiveness:

Despite immediate countermeasures such as system shutdowns and password resets, ongoing network activity detected post-incident (detailed in Appendix U) suggests the initial response may not have fully contained the threat:

Subsequent to the mitigation attempt, several instances of malicious activity were observed. At 1:43 PM, a remote desktop protocol (RDP) connection was confirmed to a known bad IP address, 317.217.252.15, indicating a potential compromise of the system. Following this, at 2:57 PM, data exfiltration was detected to an IP located in Iran (91.92.231.67), raising concerns about significant data transfer potentially linked to malware activity. This trend of data exfiltration continued at 5:04 PM, with ongoing connections to the same malicious IP, further suggesting sustained malicious activity targeting sensitive information within the network.

Later, at 5:20 PM, a successful logon was recorded on the domain controller (DC1), which may indicate further unauthorized access or potential account compromise. The activity persisted at 5:29 PM when privileged logon activity continued, signaling that attackers remained active within the system, highlighting a critical need for immediate investigation and remediation to mitigate the potential damage from these incidents.

Furthermore, at 6:28 PM, Cobalt Strike beacon activity was detected on the internal IP address 10.0.0.52, occurring after mitigation actions were taken, suggesting that attackers may have regained access despite these efforts. Later in the day, at 10:19 PM, a possible TrickBot malware activity alert was triggered from the internal IP 172.16.10.8, further indicating persistent threats within the network and underscoring the necessity for enhanced security measures and continuous monitoring to address these ongoing risks.

## 

## 6. Recommendations:

To combat the malicious activities indicated by the various indicators of compromise (IOCs), the following potential remediations can be implemented:

**Incident Response and Containment:**

* + Immediately isolate affected systems from the network to prevent further spread of the attack and limit data exfiltration.
  + Conduct a thorough investigation to assess the extent of the compromise and identify any other affected systems.

**Network Traffic Monitoring:**

* + Implement robust network monitoring tools to detect unusual or suspicious traffic patterns, especially involving known bad IP addresses and unusual connections.
  + Utilize intrusion detection and prevention systems (IDPS) to identify and block malicious traffic in real-time.

**Malware Removal:**

* + Conduct malware scans using up-to-date antivirus and anti-malware solutions on affected systems to remove any detected malicious software, including TrickBot and Cobalt Strike payloads.
  + Ensure that all systems have the latest security patches and updates to minimize vulnerabilities.

**User Access Management:**

* + Review user accounts and permissions to ensure that no unauthorized accounts exist and that existing accounts have appropriate access levels.
  + Enforce the principle of least privilege (PoLP) by limiting user access to only those resources necessary for their roles.

**Logging and Monitoring:**

* + Enhance logging and monitoring capabilities to capture detailed logs of user activity, system changes, and network connections.
  + Implement a Security Information and Event Management (SIEM) system to aggregate and analyze logs for suspicious activity patterns.

**Phishing Awareness Training:**

* + Conduct training sessions for employees to raise awareness about phishing tactics and other social engineering attacks.
  + Establish a protocol for reporting suspicious emails or messages to the IT/security team.

**Incident Response Plan Review:**

* + Review and update the incident response plan based on lessons learned from the incidents to improve response times and effectiveness in future incidents.
  + Conduct tabletop exercises to simulate various attack scenarios and test the readiness of the incident response team.

**Threat Intelligence Integration:**

* + Leverage threat intelligence feeds to stay informed about the latest threats, including IOCs associated with known malware such as TrickBot and Cobalt Strike.
  + Use this information to proactively block known malicious IP addresses and domains.

**Data Protection Measures:**

* + Implement data encryption to protect sensitive data both in transit and at rest.
  + Utilize data loss prevention (DLP) tools to monitor and prevent unauthorized data transfers.

**System Hardening:**

* + Conduct regular security assessments and vulnerability scans to identify and address weaknesses in the environment.
  + Apply security hardening techniques to all systems, such as disabling unnecessary services and using firewalls to restrict incoming and outgoing traffic.

By implementing these remediations, organizations can enhance their security posture, reduce the likelihood of successful attacks, and improve their ability to detect and respond

## 7. Conclusion:

In conclusion, the investigation into the recent incidents of malicious activity has revealed a concerning array of security threats, including phishing attempts, privilege escalation, and the presence of malware such as Cobalt Strike and TrickBot within the network. The detection of suspicious inbound traffic targeting MySQL, coupled with indicators of compromise from internal systems, underscores the need for immediate and comprehensive remediation efforts.

The proposed remediations aim to fortify the organization's defenses against such threats by enhancing incident response capabilities, improving network monitoring, and promoting user awareness. By isolating affected systems, conducting thorough malware removal, and implementing stringent access controls, the organization can significantly reduce the risk of further breaches. Additionally, ongoing user education regarding phishing and other social engineering tactics will help cultivate a security-conscious culture among employees.

Moreover, integrating advanced logging and threat intelligence solutions will enable the organization to proactively detect and respond to emerging threats. As technology continues to evolve, regular security assessments and updates to incident response plans will be critical in ensuring that defenses remain robust and adaptive.

Ultimately, by taking these decisive actions, the organization will not only mitigate the current threats but also strengthen its overall security posture, enhancing its resilience against future attacks. Continuous vigilance and adaptation to the evolving threat landscape will be key to safeguarding sensitive information and maintaining operational integrity.

## 8. Appendices:

### Appendix A: Detailed Network Map of Identified Hosts

|  |  |
| --- | --- |
| Name | IP Address |
| DNS Server | 10.0.0.1 |
| Domain Controller | 10.0.0.25 |
| Wks1 | 10.0.0.50 |
| Wks2 | 10.0.0.51 |
| Wks3 | 10.0.0.52 |
| Wks4 | 10.0.0.53 |
| Wks5 | 10.0.0.54 |
| Wks6 | 10.0.0.55 |
| Wksadmin | 10.0.0.100 |
| Subversion Code Repository | 10.0.10.8 |
| Webdev | 10.0.10.10 |
| SMTP Server | 10.0.100.10 |
| File Server | 172.16.10.8 |
| Web Server | 172.16.10.10 |
| vpnclient | 172.16.100.12 |

### 

### Appendix B: External IP Addresses and Geographic Dispersion

|  |  |  |  |
| --- | --- | --- | --- |
| External IP Addresses | Geographic Location | Action Associated | Appendix |
| 13.248.65.6 | Spain | Possible SQL Injection |  |
| 13.248.65.126 | Spain | Network Connection | H |
| 20.86.173.234 | Netherlands | User Agent | M |
| 31.217.252.15 | Ukraine | Confirmed RDP connection | F |
| 52.188.50.245 | USA | User Agent | M |
| 60.253.130.182 | China | Network Connection - MS Terminal Server Root Login | I |
| 60.253.130.193 | China | Network Connection |  |
| 66.249.150.78 | Jamaica | Cobalt Strike | J |
| 91.92.231.67 | Iran | Potential Trickbot Malware | K |
| 104.132.26.40 | Portugal | Potential Trickbot Malware | K1 |
| 104.132.26.168 | Portugal | Network Connection |  |
| 142.250.112.127 | USA | Attempted User Privilege Gain |  |
| 149.6.203.167 | Spain | Phishing email | D |
| 168.63.250.82 | Singapore | User Agent | M |
| 184.25.66.88 | Canada | User Agent | M |