Document Reference: RAIRP-2
Document Name: Root Access Playbook

Effective Date: 30 July 2024
Expiry Date: 03 March 2025

Root Access Incident Response Playbook

Redback Operations

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 29 July 2024

Version	Modified By	Approver	Date	Changes made
1.0	Priyanshu		13 April 2024	First draft
1.1	Devika Sivakumar		10 May 2024	Changed the flowchart mentioned the stages, updated the incident response stages in part-5 and arranged the document with correct format. Added correct page number. Added the content table. Gave correct font size and theme
2.0	Devika Sivakumar		29 July 2024	A comprehensive update has been carried out throughout the playbook. The introduction part is updated Several new attack types and case studies have been added. A RACI chart has been included. The steps for monitoring threats have been included. New terminology has been introduced. The overall format of the playbook has been adjusted to align with other playbooks. The table has also been updated.

Contents

1. Introduction

1.1 Overview

Root access security is a critical aspect of contemporary cybersecurity. Root access, the highest level of administrative rights in a system or network, provides unrestricted power and control. Unauthorized access to root privileges poses significant threats to the availability, confidentiality, and integrity of vital systems and data. This playbook offers a comprehensive and strategic approach to efficiently handle and resolve root access incidents.

1.2 Purpose

The primary purpose of this playbook is to provide organizations with a strategic framework for navigating the complexities of root access incidents. It aims to equip stakeholders with the necessary information and resources to mount a coordinated and resilient response to such events, minimizing potential harm and disruption to business operations.

1.3 Attack Definition

A root access incident refers to any situation in which unauthorized individuals obtain access to the highest level of administrative rights on a system or network. This illicit use of root access can lead to data exfiltration, system modification, service interruption, and reputational harm.

1.4 Scope

This playbook covers all networks and systems within the organizational domain. It applies to on-premises servers, cloud-based infrastructures, legacy systems, and modern technologies, offering a flexible and scalable response structure for various environments and scenarios.

2. Attack Types

2.1 Insider Threat

Insider threats are a dangerous and sneaky threat that arises when people who are authorised to access organisational resources misuse their access rights for malevolent intent. Insiders are a serious threat to organisational security because they can bypass established safeguards and obtain unauthorised root access by using their in-depth knowledge of systems and protocols. Their motivations might range from financial gain to ideological vendettas.

Case Study: Edward Snowden (2013)
Overview: Snowden, a former NSA contractor, leaked classified information to the public.
Impact: The leaks exposed global surveillance programs and caused diplomatic tensions.
Response: The NSA reviewed and enhanced its access controls and insider threat programs.

2.2 External Attack

Another common way that root access breaches occur is through external attacks, in which remote-operating malefactors try to overcome organisational defences and obtain root rights. These adversaries try to take advantage of weaknesses in systems and networks that are visible to the outside world by using a variety of strategies such malware distribution, exploit kits, and brute force attacks to penetrate the organisational perimeter.

Case Study: SolarWinds Attack (2020)
Overview: Attackers infiltrated SolarWinds' Orion software, impacting multiple U.S. government agencies and private companies.
Impact: The breach compromised sensitive data and required extensive remediation efforts.
Response: SolarWinds implemented security enhancements, including improved software development practices and threat detection capabilities.

2.3 Data Breaches

Incidents involving root access frequently precede data breaches, in which adversaries utilise their enhanced privileges to steal confidential and private material from company archives. These criminals use their unrestricted access to vital systems to steal, exfiltrate, and profit from priceless data assets, harming the organization's reputation and finances greatly. Their motivations may range from corporate espionage to financial gain.

Case Study: Equifax Data Breach (2017)
Overview: Attackers exploited a vulnerability in Equifax's web application framework to gain access to sensitive information.
Impact: The breach exposed personal information of approximately 147 million individuals.
Response: Equifax enhanced its cybersecurity practices, implemented stronger access controls, and paid a settlement of up to $700 million.

2.4 Phishing Incidents

Phishing assaults are a pervasive and persistently frustrating form of cyberattack wherein adversaries utilise social engineering techniques to trick unsuspecting consumers into disclosing their login credentials or downloading harmful software. Phishing culprits aim to obtain sensitive information, such as root credentials, by posing as trustworthy organisations or forcing users to click on malicious links. This allows them to get beyond standard security measures and gain unauthorised access to organisational systems.

Case Study: Target Phishing Attack (2013)
Overview: Attackers used phishing emails to gain access to Target's network, stealing credit card information.
Impact: The breach affected over 40 million customers and resulted in significant financial losses.
Response: Target invested in cybersecurity improvements, including advanced threat detection and employee training programs.

2.5 Ransomware Attacks

The combination of cybercrime and extortion is best exemplified by ransomware assaults, in which adversaries use malicious software to encrypt important data and systems and then hold them captive until a ransom is paid. Root access criminals use their privileged access to launch ransomware campaigns that destroy corporate networks, sabotage operations, and demand astronomical costs—all of which highlight the serious repercussions of root access breaches.

Case Study: WannaCry Ransomware Attack (2017)
Overview: The WannaCry ransomware exploited a Windows vulnerability, encrypting data on affected systems.
Impact: The attack affected over 200,000 computers across 150 countries, causing widespread disruption.
Response: Organizations applied security patches, enhanced backup practices, and improved incident response plans.

2.6 Credential Theft

A nasty and widespread threat vector is credential theft, in which malicious actors use a variety of methods, including keylogging, credential phishing, and password spraying, to get user credentials—even root credentials—illegally. With these credentials in hand, attackers can pose as valid users, get around authentication restrictions, and access vital systems and resources without authorisation. This poses serious dangers to the security and integrity of the organisation.

Case Study: LinkedIn Data Breach (2012)
Overview: Hackers accessed LinkedIn's user database, stealing hashed passwords.
Impact: The breach exposed millions of user credentials, leading to unauthorized access.
Response: LinkedIn implemented stronger password hashing techniques and encouraged users to adopt two-factor authentication.

3. Stakeholders

The proficient handling and settlement of root access incidents require the coordinated endeavours and cooperation of a heterogeneous group of stakeholders, each possessing distinct knowledge, viewpoints, and roles. The following parties are essential to the incident response process, from frontline responders entrusted with containment and mitigation to senior leadership tasked with making strategic decisions:

1. The incident response team, which is made up of knowledgeable cybersecurity experts, incident responders, and forensic analysts, oversees identifying, containing, and resolving access incidents. It is the front line of organisational defence.

2. IT Security Team: Tasked with preserving the confidentiality and integrity of company data and systems, the IT security team is essential in coordinating preventative security actions in response to unusual activity and strengthening defences against root access threats.

3. System Administrators: Using their technical know-how and domain experience to restore system integrity and functionality, system administrators, as stewards of organisational systems and networks, have a significant impact on the identification, investigation, and resolution of root access issues.

4. Legal Department: Charged with managing the complex legal and regulatory environment that surrounds cybersecurity, the legal department offers priceless advice and assistance on contractual requirements, liability issues, and compliance obligations related to root access incidents.

5. Management: Setting organisational priorities, allocating resources, and spearheading strategic efforts aimed at bolstering the organization's resilience against root access threats are all crucial tasks performed by executive leadership, which includes C-suite executives and senior management.

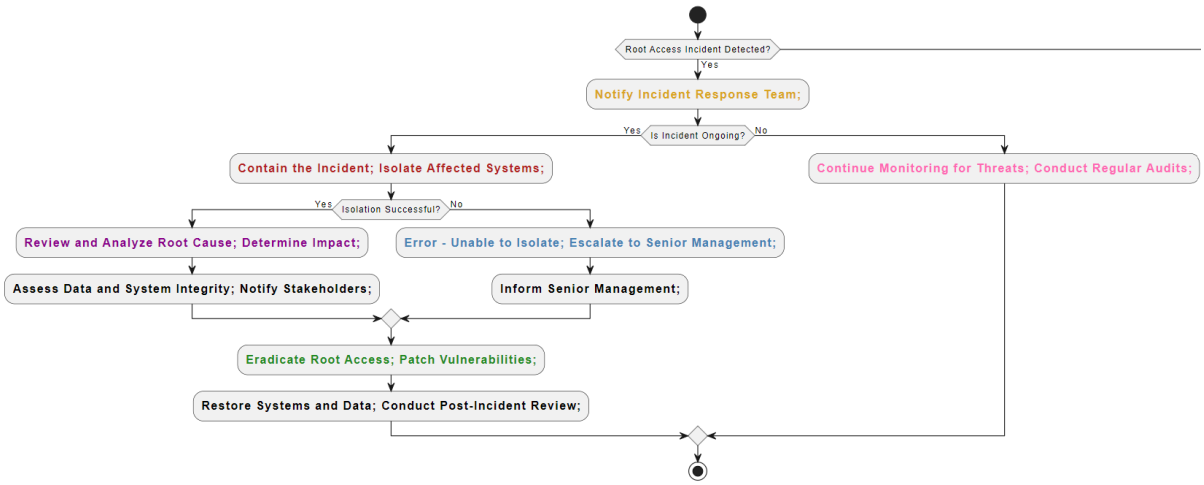
6. External Consultants: Organisations may hire outside consultants or third-party vendors to supplement their incident response capabilities in situations requiring specific knowledge or resources. These vendors can help with forensic analysis, threat intelligence, and remediation efforts.

RACI Chart for Incident Response

Task/Activity	IT Security Team	Incident Response Team	Legal and Compliance	System Administrators	Management	External Consultants
Preparation						
Establish incident response team	R, C	A, R	I	I	I	I
Develop response procedures	A, R	R, C	I	I	I	I
Conduct training sessions	A, R	R	I	I	I	I
Implement surveillance systems	A, R	R	I	I	I	I
Detection						
Monitor system logs and traffic	A, R	R	I	I	I	I
Use IDS and SIEM tools	A, R	R	I	I	I	I
Analyse alerts	A, R	R	I	I	I	I
Analysis						
Conduct forensic analysis	A, R	R	I	I	I	I
Determine impact	A, R	R	I	I	I	I
Identify threat actor tactics	A, R	R	I	I	I	I
Containment						

Isolate affected systems	A, R	R	I	I	I	I
Implement access controls	A, R	R	I	I	I	I
Block malicious activity	A, R	R	I	I	I	I
Eradication						
Remove unauthorized access	A, R	R	I	I	I	I
Patch vulnerable systems	A, R	R	I	I	I	I
Update security policies	A, R	R	I	I	I	I
Recovery						
Restore compromised systems	A, R	R	I	I	I	I
Recover data from backups	A, R	R	I	I	I	I
Reconfigure networks	A, R	R	I	I	I	I
Post-Incident Review						
Assess incident response	A, R	R	I	I	I	I
Document lessons learned	A, R	R	I	I	I	I
Update incident response protocols	A, R	R	I	I	I	I

4. Flow Chart



1. Preparation (Prep): Yellow

- Notify Incident Response Team: The first steps in becoming ready to handle a root access event are taken during this phase. The incident response team is instantly contacted to initiate the response process upon detection of a root access breach. This preliminary stage is symbolised by the colour yellow, which emphasises the necessity of being ready and moving quickly.

2. Identification (Identify): Red

- Contain the Incident; Isolate Affected Systems: At this point, the main priorities are locating the root access issue and containing it right away. Aims are set to contain the spread of unauthorised access and isolate compromised systems. Red emphasises the necessity for quick containment measures by signifying the urgency and crucial nature of this stage.

3. Notification (Notif): Violet

- Review and Update Antivirus Definitions; Perform Full System Scans: During this phase, early mitigation actions are implemented, and pertinent parties are notified. To lessen the effects of the root access breach, precautions including comprehensive system scans and antivirus definition updates are implemented. The stage of notice and early reaction that is symbolised by the colour violet emphasises the need of taking preventative action to reduce damage.

4. Containment (Contain): Sky Blue

- Error - Unable to Isolate; Escalate to Senior Management: In this case, attempts are made to stop additional unauthorised access and contain the root access situation. If the impacted systems cannot be isolated, top management is alerted right once so that the issue may be resolved. The containment measures intended to stop the spread of unauthorised access and stop escalation are represented by the colour sky blue.

5. Eradication (Erad): Light Green

- Eradicate Root Access; Patch Vulnerabilities: This phase is all about fixing the underlying vulnerabilities and getting rid of unwanted access. To stop such events in the future, steps are made to remove unauthorised users and repair security flaws. Ensuring that the organization's systems are secure and removing unauthorised access are symbolised by the colour bright green.

6. Recovery (Recover): Brown

- Monitor for Further Activity; Initiate Recovery Procedures: During this stage, the focus is on recuperating from the root access event and resuming regular operations. To find any remaining unapproved access, recovery steps are started, and continuous monitoring is carried out. The recovery phase, which aims to restore activities and strengthen security measures, is represented by the colour brown.

7. Post-Incident Actions (Post): Light Pink

- Continue Monitoring for Threats; Conduct Regular Audits: Post-event activities are carried out in the last phase to assess the response's efficacy and pinpoint areas that require improvement. Regular audits and continuous threat monitoring are carried out to improve incident response resilience. The post-event initiatives intended to improve future response efforts and learn from the occurrence are represented by the colour light pink.

5. Incident Response Stages

5.1 Preparation

- **Objective:** Putting in place the guidelines, practices, and tools required to handle root access issues in an efficient manner.
- **Activities:**
  - Putting together a team for incident response with clear roles and duties.
  - Creating strategies and processes for crisis response, such as escalation routes and communication guidelines.
  - Holding practice sessions and exercises on a regular basis to guarantee readiness and rehearse incident response protocols.
  - Putting security and surveillance technologies in place to find and stop instances of root access.
- **Outcome:** A fully equipped company with the ability to react to root access events quickly and efficiently.

5.2 Detection

- **Objective:** Recognising warning signs of illegal access to the organization's resources and systems.
- **Activities:**
  - Keeping an eye out for questionable activity, such as odd access patterns or unauthorised attempts at authentication.
  - Using security information and event management (SIEM) and Intrusion detection systems (IDS) to find possible root access occurrences.
  - Examining abnormalities and warnings to distinguish between authorised and unauthorised activity.
- **Outcome:** Rapid reaction and mitigation strategies are made possible by early root access event identification.

5.3 Analysis

- **Objective:** Recognising the kind and extent of the root access event.
- **Activities:**
  - Gathering information and carrying out forensic investigation to ascertain the origin and degree of the illegal entry.
  - Examining hacked networks and systems to find attack vectors and how they affect compromised data.
  - Recognising the tactics, methods, and procedures (TTPs) of threat actors and indicators of compromise (IOCs).
- **Outcome:** A thorough comprehension of the root access incident's origins, consequences, and accountability.

5.4 Containment

- **Objective:** Limiting the propagation and effects of the root access incident and stopping other illegal access or data leaks.
- **Activities:**
  - Dividing up susceptible networks and systems to stop intruders from moving laterally.
  - Putting safety measures and access restrictions in place to stop illegal access to sensitive data.
  - Limiting or preventing harmful data, software, or network flow to stop more damage.
- **Outcome:** Efficient handling of the root access issue, reducing harm to the data and systems of the company.

5.5 Eradication

- **Objective:** Eliminating threats and any lingering vulnerabilities from the company's networks and IT systems.
- **Activities:**
  - Removing illegal access and putting compromised systems back in a safe and secure condition.
  - Upgrading or patching susceptible systems and software to stop further exploitation.
  - Examining and revising security protocols and guidelines to fix flaws or vulnerabilities found.
- **Outcome:** Elimination of all evidence of the root access incident and mitigation of vulnerabilities to stop it from happening again.

5.6 Recovery

- **Objective:** Restarting company operations and returning impacted systems and data to normal functioning.
- **Activities:**
  - Restoring damaged systems and data backups to guarantee the integrity and accessibility of data.
  - Rebuilding or rearranging networks and systems to improve security and stop such incidents in the future.
  - Putting user awareness and education programmes into action to reduce unauthorised access events in the future.

- **Outcome:** Full restoration of operations and services, together with strengthened security measures to lessen the chance of recurrence.

5.7 Post-Incident Review

- **Objective:** Assessing the organization's reaction to the root access event, noting lessons learned and opportunities for improvement.
- **Activities:**
  - Evaluating the incident response procedure in-depth to find its advantages, disadvantages, and potential areas for development.
  - Recording best practices and lessons discovered to improve incident response skills in the future.
  - Modifying security setups, rules, and incident response protocols considering review results.
- **Outcome:** Improved preparedness for upcoming root access incidents and enhanced incident response capabilities.

6. Steps for Monitoring Threats

6.1 Establish a Monitoring Strategy

- **Objective:** Develop a comprehensive strategy specifically for monitoring root access threats.
- **Activities:**
    - Define clear objectives tailored to the detection and management of unauthorized root access.
    - Select and deploy specialized tools designed to monitor root-level activities, such as advanced Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) systems, and Endpoint Detection and Response (EDR) solutions.
    - Establish baselines for normal administrative and root-level user activity to differentiate between legitimate and suspicious behaviors.
- **Outcome:** A robust monitoring strategy aligned with the goal of detecting and mitigating root access threats effectively.

6.2 Deploy Monitoring Solutions

- **Objective:** Implement and configure monitoring tools to detect root access threats across the organization's infrastructure.
- **Activities:**
    - Deploy chosen monitoring tools specifically configured to track root access activities across all critical systems and networks.
    - Integrate monitoring tools with threat intelligence feeds to stay updated on the latest root access vulnerabilities and attack vectors.
    - Ensure comprehensive logging of all root access attempts, successes, and failures, along with detailed recording of administrative activities.
- **Outcome:** A well-deployed set of monitoring solutions providing in-depth insights into potential root access threats.

6.3 Continuous Monitoring and Analysis

- **Objective:** Maintain continuous surveillance and analysis to promptly detect and respond to unauthorized root access attempts.

- **Activities:**
    - Implement real-time monitoring to continuously observe root-level activities, including login attempts, command executions, and privilege escalations.
    - Utilize behavioral analytics and machine learning to identify anomalies in root access patterns, which could indicate unauthorized attempts.
    - Correlate events from various sources to identify and prioritize potential root access threats.
- **Outcome:** Enhanced capability to detect unauthorized root access promptly, enabling swift response and mitigation.

6.4 Alerting and Notification

- **Objective:** Ensure timely and effective response to detected root access threats through a robust alerting system.
- **Activities:**
    - Establish thresholds and triggers for different types of root access alerts, considering the severity and potential impact.
    - Configure automated alerts to notify the incident response team immediately when suspicious root access activities are detected.
    - Implement a prioritization system for alerts to ensure that critical root access threats are addressed promptly.
- **Outcome:** Timely and effective response to detected root access threats, reducing the risk of significant damage.

6.5 Investigate and Respond

- **Objective:** Conduct thorough investigations and implement appropriate actions to mitigate identified root access threats.
- **Activities:**
    - Perform initial triage to verify the validity and potential impact of root access alerts.
    - Conduct in-depth analysis of confirmed alerts to understand the root cause and potential extent of the threat.

- Initiate containment measures, such as isolating affected systems and revoking unauthorized root access and execute necessary eradication procedures.

- **Outcome:** Effective investigation and mitigation of root access threats, ensuring minimal impact on the organization.

6.6 Post-Incident Review

- **Objective:** Assess the effectiveness of the response to root access incidents and identify areas for improvement.
- **Activities:**
  - Record all details of the root access incident, including detection, analysis, and response actions taken.
  - Conduct a comprehensive review of the monitoring and response processes post-incident to identify strengths and areas for improvement.
  - Update monitoring tools, configurations, and thresholds based on findings to enhance future detection and response capabilities.
- **Outcome:** Continuous improvement of incident response and threat monitoring processes, specifically for root access incidents.

6.7 Continuous Improvement

- **Objective:** Maintain and enhance the organization's strategy and tools for monitoring root access threats.
- **Activities:**
  - Conduct regular audits to ensure the effectiveness of root access monitoring tools and strategies.
  - Provide ongoing training to security personnel, focusing on detecting and responding to root access threats.
  - Continuously adapt the monitoring strategy to address emerging root access threats and vulnerabilities.
- **Outcome:** A proactive and adaptive strategy for monitoring root access threats that evolves with the changing threat landscape.

7. Terminology

Terminology in incident response encompasses a range of concepts and terms essential for effective communication and understanding within the cybersecurity domain. It provides a common language for incident responders, enabling precise and unambiguous communication during incident response activities.

Root Access: The highest level of administrative access within a system or network, granting users unrestricted control over critical resources and settings.

Incident Response: A coordinated approach to managing and mitigating the impact of security incidents, encompassing detection, analysis, containment, eradication, recovery, and post-incident review stages.

Intrusion Detection System (IDS): A security tool designed to monitor network traffic and systems for signs of unauthorized access or malicious activity, generating alerts or notifications when suspicious behavior is detected.

Intrusion Prevention System (IPS): A security solution that goes beyond detection to actively block or prevent unauthorized access or malicious activity, helping to protect systems and networks from cyber threats.

User Behavior Analytics (UBA): The process of analyzing patterns of user behavior to detect anomalies or deviations from normal activity, helping to identify potential security incidents, including unauthorized access or insider threats.

Two-Factor Authentication (2FA): An authentication method that requires users to provide two forms of identification, typically a password or PIN combined with a second factor such as a code sent to a mobile device, to access a system or service.

Credential Theft: The unauthorized acquisition of user credentials, such as usernames and passwords, through various means such as phishing attacks, keylogging, or credential stuffing, enabling attackers to gain unauthorized access to systems or accounts.

Ransomware: Malicious software designed to encrypt or lock files and systems, typically demanding payment (ransom) from the victim in exchange for decryption keys or restoring access to the affected data.

Root Cause Analysis (RCA): A methodical investigation process used to determine the underlying cause or causes of a security incident.

Least Privilege Principle: The security principle that users, processes, and systems should be granted only the minimum level of access or permissions necessary to perform their intended tasks.

Privilege Escalation: The act of increasing the level of access or permissions granted to a user or application, typically to gain unauthorized control over system resources or sensitive data.

By understanding and utilizing these key terms, incident responders can effectively communicate, collaborate, and execute incident response activities, ultimately enhancing the organization's ability to detect, respond to, and recover from security incidents.