Document Reference:	RAIRP-1	Effective Date:	12 May 2024
Document Name:	Root Access Playbook	Expiry Date:	12 May 2025

Root Access Incident Response Playbook

Redback Operations

Document Owner:	Purple Team	Last Modified By:	Priyanshu
Next Review Date:	17 June 2024	Last Modified on:	10 May 2024

Version	Modified By	Approver	Date	Changes made
0.1	Priyanshu		13 April 2024	First draft
0.2	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
1.0	Devika Sivakumar, Priyanshu	Joel Daniel	12 May 2024	Approved for Publishing

Contents

1. Introduction

1.1 Overview

It is impossible to overestimate the importance of root access security in the context of contemporary cybersecurity. The key to the kingdom is root access, the highest level of administrative rights in a system or network, which provides unrestricted power and control. The availability, confidentiality, and integrity of vital systems and data are seriously threatened by instances of unauthorised access to root privileges, which can happen even with strong security measures in place. This playbook offers an extensive and carefully planned method to efficiently handle and resolve root access incidents in response to this ongoing danger.

1.2 Purpose

This playbook's main goal is to give organisations a strategic framework for negotiating the intricate and varied world of root access issues. It aims to equip stakeholders with the necessary information and resources to mount a coordinated and resilient reaction in the event of such exigencies by outlining precise and doable steps. This playbook also acts as a cornerstone for building organisational resilience, making it possible to quickly limit, mitigate, and recover from root access breaches, minimising potential harm and business operations disruption.

1.3 Attack Definition

Any situation in which unauthorised individuals obtain unauthorised access to the highest level of administrative rights on a system or network is referred to as a root access event. In addition to giving the criminals complete control over vital resources, this illicit use of root access has a host of other harmful effects, such as data exfiltration, system modification, service interruption, and reputational harm.

1.4 Scope

This playbook covers a broad scope that includes all networks and systems that are part of the organisational domain. Every aspect of the organisational ecosystem is vulnerable to the threat of root access incidents, whether it be on-premises servers or cloud-based infrastructures, legacy systems, or state-of-the-art technologies. Because of this, the playbook's scope is purposefully broad to offer a thorough response structure that is flexible and scalable to a variety of settings and situations.

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.

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.

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.

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.

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.

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.

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.

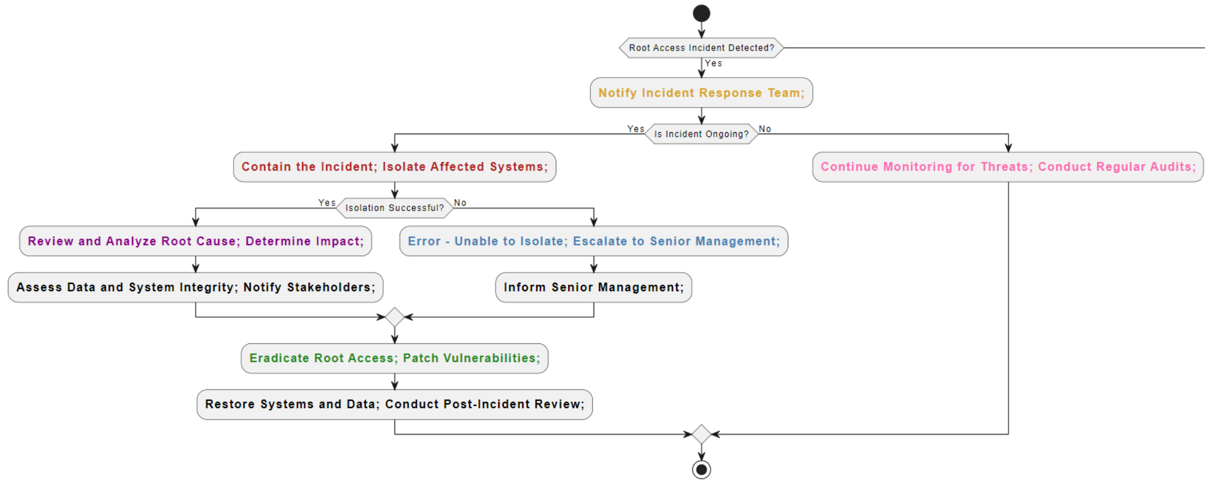
3. System Administrators: Using their technical know-how and domain experience to restore system integrity and functionality, system administrators, as stewards of organisational systems and networks, have a significant impact on the identification, investigation, and resolution of root access issues.

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.

4. Flow Chart


Root Access Incident Detected?
Yes
Notify Incident Response Team;
Yes
Is Incident Ongoing?
No
Contain the Incident; Isolate Affected Systems;
Continue Monitoring for Threats; Conduct Regular Audits;
Yes
Isolation Successful?
No
Review and Analyze Root Cause; Determine Impact;
Error - Unable to Isolate; Escalate to Senior Management;
Assess Data and System Integrity; Notify Stakeholders;
Inform Senior Management;
Eradicate Root Access; Patch Vulnerabilities;
Restore Systems and Data; Conduct Post-Incident Review;

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. 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.

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.