Security Incident Management Runbook

Local Privilege Escalation

Revision: 1
Date: 14/08/2024

Group: 3

Ananthu Krishna Vadakkeppatt
Ramachandra Muralidhara
Syed Mujahid Hamid Ali
Yannish Kumar Ballachander Sreedevi

Table of Contents

Introduction

In the event of an incident, a runbook provides an effective and efficient way to handle the incident. This runbook provides the procedure to calculate the impact, determine the escalation protocol, and list the action items for each role within the incident response team.

Data Classification

The Organization's Data Classification Standard is used to determine the overall impact.

Classification	Definition	Example
Confidential	Data that may cause harm to the company and/or public if compromised.	• SIN • Payment Card information
Internal	Data that is owned by the organization that may result in financial loss if compromised.	• Meeting agenda • Memo • Internal policies
Public	Data that is made available to the public consumption.	• Contact information • Business hours

Technologies, Systems, Services, Process

Name	Definition	Capabilities
Endpoint Detection and Response (EDR)	Advanced endpoint security.	Monitors and alerts on suspicious activity, including privilege escalation attempts.
Endpoint Protection Platform (EPP)	Endpoint security suite.	Includes antivirus, anti-malware, firewall, and intrusion prevention capabilities.
Vulnerability Management Tools	Tools to identify and manage vulnerabilities.	Scans systems for misconfigurations and known vulnerabilities, provides patch management guidance.
Cyber Deception Systems	Deceptive technologies to lure attackers.	Deploys honeypots, honeytokens, and other deceptive tools to detect and analyze attacker behaviors.

Response Procedures

Detection Phase

Role/Team/System	Description	Objectives	Action
EDR System	Monitors and logs endpoint activities.	Detect suspicious processes or privilege escalations.	Identify unusual activities like process injections or privilege escalations using Meterpreter post-exploitation scripts.
Security Operations Center (SOC)	Monitors alerts from EDR and cyber deception systems.	Validate potential local privilege escalation.	Review alerts generated by EDR and analyze decoy assets deployed by cyber deception systems for unauthorized access attempts.
Endpoint Security Analyst	Reviews endpoint protection data.	Ensure protection against unauthorized access.	Analyze security logs and endpoint activities for signs of bypasses or escalated privileges using DLLHijackTest and SharpUp.

Analysis Phase

Role/Team/System	Description	Objectives	Action
Incident Response Team	Coordinates the investigation.	Confirm the vulnerability or misconfiguration exploited.	Use PowerSploit's PowerUp to identify and validate the specific vulnerability or misconfiguration leveraged for privilege escalation.
Forensic Analyst	Conducts a detailed forensic analysis.	Gather evidence and assess the impact.	Perform deep dive forensics on affected systems using memory dumps and log analysis to identify the extent of privilege escalation.

Containment Phase

Role/Team/System	Description	Objectives	Action
System Administrator	Isolates compromised systems.	Prevent further exploitation of the vulnerability.	Disconnect the compromised systems from the network, block any backdoor communications, and disable the affected user accounts.
Network Administrator	Secures the network environment.	Restrict the attacker's lateral movement.	Implement network segmentation and use access control lists (ACLs) to isolate compromised or vulnerable segments.

Eradication Phase

Role/Team/System	Description	Objectives	Action
System Administrator	Remediates compromised systems.	Remove malicious code and fix misconfigurations.	Use PowerSploit and SharpUp to identify and remove malicious persistence mechanisms, patch vulnerabilities, and reconfigure the systems.
Security Analyst	Ensures system integrity.	Verify that no residual threats remain.	Perform a full system scan using EPP tools and validate that the misconfiguration has been corrected and no backdoors remain.

Recovery Phase

Role/Team/System	Description	Objectives	Action
System Administrator	Restores affected systems.	Safely restore systems to normal operation.	Restore systems from clean backups, re-enable services with updated security configurations, and monitor for any signs of re-compromise.
IT Support Team	Provides user support.	Ensure that user access is securely restored.	Assist users in resetting passwords, re-authenticating, and ensuring their devices are secure before reconnecting to the network.

Post-Incident Phase

Role/Team/System	Description (optional)	Objectives	Action
CISO	Oversees incident review.	Document the incident and update security policies.	Compile a detailed report outlining the incident, response actions, and lessons learned. Recommend policy updates to prevent future occurrences.