**GERENCIAMENTO DE RESPOSTA A INCIDENTES**

**GRI #2**

**UNIX/LINUX**

**DETECÇÃO DE INTRUSÃO**

Diretrizes para lidar com um Unix/Linux suspeito no ambiente



**RESUMO**

GRI Autor: William Lima

Empresa: Suricatoos

E-mail: [william.lima@suricatoos.com](mailto:william.lima@suricatoos.com)

GitHub: https://github.com/williamsouzadelima

### **METODOLOGIA DE RESPOSTA A INCIDENTES**

Este **Playbook de Resposta a Incidentes** é um **guia de referência** dedicado a profissionais responsáveis por investigar e mitigar incidentes de segurança específicos.

## **📌 QUEM DEVE USAR ESTE PLAYBOOK?**

🔹 **Analistas de Segurança** 🛡️

🔹 **Analistas de SOC (Centro de Operações de Segurança)** 👨‍💻

🔹 **CISOs, Gerentes e Coordenadores de Segurança** 📊

🔹 **Equipes CERTs (Computer Emergency Response Teams)** 🚨

🔹 **Blue Team** 🎯

## **📢 ORIENTAÇÕES IMPORTANTES DURANTE UM INCIDENTE**

✔️ **Siga o PLANO DE RESPOSTA A INCIDENTES** detalhado para minimizar impactos financeiros e a imagem da EMPRESA.

✔️ **Documente cada ação tomada** – isso ajudará na análise pós-incidente e na melhoria contínua.  
✔️ **Mantenha a calma e siga os procedimentos** – evite tomar decisões precipitadas.  
✔️ **Entre em contato com a equipe de Resposta a Incidentes** ou com o **CERT da sua organização** sempre que necessário.

📌 **Contato do GRI CERT Suricatoos:**

🔗 GitHub: [GRI CERT Suricatoos](https://github.com/williamsouzadelima)

📩 E-mail: **contato@suricatoos.com**

🚀 **Uma resposta estruturada a incidentes protege sua empresa de maiores danos e reduz o tempo de recuperação!**

**ETAPAS DE RESPOSTA A INCIDENTES**

A resposta eficaz a incidentes de segurança segue **6 etapas essenciais**, conforme definido pelo **Guia de Tratamento de Incidentes de Segurança de Computadores do NIST**.

## **PREPARAÇÃO** 🛠️

**📌 Objetivo:** Estabelecer contatos, definir procedimentos e reunir informações para economizar tempo durante um incidente.

✅ Desenvolver e documentar **políticas de resposta a incidentes (PRI)**.

✅ Definir **funções e responsabilidades** da equipe de resposta.

✅ Implementar **ferramentas de detecção e monitoramento** (SIEM, EDR/XDR).

✅ **Treinar e conscientizar** funcionários sobre ameaças cibernéticas.

✅ Criar um **plano de comunicação interna e externa** para resposta a incidentes.

✅ Automatizar **detecção e resposta** para reduzir o tempo de exposição.

✅ Integrar EDR com **SIEM/SOAR** para resposta automatizada.

✅ Priorizar o **isolamento da máquina** para evitar a movimentação lateral do atacante.

✅ **Backups e preservação de evidências:**

* Criar **cópias físicas forenses** do disco rígido e da memória RAM para análise pós-incidente.
* Manter **logs de auditoria centralizados** em local seguro para futuras investigações.

✅ **Monitoramento e detecção avançada:**

* Utilizar **Threat Intelligence Feeds** para melhorar a detecção de ameaças emergentes.
* Implementar **segurança baseada em comportamento** (UEBA) para detectar atividades anormais.

✅ **Implemente minimamente uma solução EDR** (Endpoint Detection and Response) em servidores e estações de trabalho.

* EDR é um dos pilares da resposta a incidentes, facilitando a identificação, contenção e remediação.
* Execute buscas no EDR e verificações de antivírus usando **regras de IOC** (Indicators of Compromise).
* Configure as políticas do EDR no modo **preventivo**.

✅ Caso **não haja um EDR disponível**, conceda **acesso local** ao sistema suspeito para um analista forense.

* O acesso local é **preferível ao remoto**, pois o invasor pode detectar as investigações.

✅ **Criação de backups forenses**:

* Uma cópia física do disco rígido pode ser necessária para fins forenses.
* Pode ser necessário desconectar o sistema da rede para preservar evidências.

✅ **Conhecimento da atividade usual da rede**:

* Mantenha um registro seguro das portas e serviços em uso.
* Use ferramentas como **Auditd** e logs do Linux (**syslog, messages, logs de aplicações como Apache e NGINX**).
* Utilize **AppArmor** para controle de acesso.

✅ **Lista de arquivos críticos**:

* Mantenha uma lista **atualizada e armazenada em local seguro** de arquivos críticos, especialmente arquivos **SUID e GUID**.
* Essa lista ajuda a distinguir arquivos legítimos de possíveis implantes maliciosos.
* Com um SIEM, faça uso do módulo FIM (File Integrity Monitoring) para monitorar pastas e arquivos críticos.

## **IDENTIFICAÇÃO** 🔍

**📌 Objetivo:** Detectar o incidente, determinar seu escopo e envolver as partes apropriadas.

✅ Monitorar **logs e alertas** de segurança em tempo real.

✅ Identificar **indicadores de comprometimento (IoCs)** e atividades anômalas.

✅ Confirmar a natureza do ataque (ransomware, phishing, malware, vazamento de dados).

✅ Determinar **quais sistemas e dados foram afetados**.

✅ Ativar **o plano de resposta a incidentes** e envolver as partes apropriadas.

### ✅ **Contas de usuários suspeitas:**

* Verifique entradas incomuns em /etc/passwd, especialmente **UID 0** (root).
* Verifique também /etc/group e /etc/shadow
* Procure por arquivos órfãos (podem ter sido deixados por uma conta deletada):

find / \( --nouser -o --nogroup \) --print

### ✅ **Arquivos incomuns**

* **Procure por arquivos** **SUID e GUID**:

find / -uid 0 \( --perm -4000 -o --perm 2000 \) –-print

* **Arquivos com nomes estranhos (como . , .. ou " "):**

find / --name " \*" –-print

find / --name ". \*" –-print

find / --name ".. \*" --print

* **Arquivos grandes (maiores que 10MB):**

find / -size +10MB --print

* **Processos rodando de ou para arquivos excluídos:**

lsof +L1

### ✅ **Serviços suspeitos:**

**Liste serviços ativos:**

chkconfig --list

* **Liste processos em execução:**

ps -aux

* **Identifique processos desconhecidos:**

lsof -p [pid]

### **✅ Atividade de rede incomum**

* **Identifique sniffers na rede:**

kernel: device eth0 entered promiscuous mode

ip link | grep "PROMISC"

* **Verifique portas e conexões ativas:**

netstat -nap

lsof -i

* **Identifique endereços IP e MAC suspeitos:**

arp -a

netstat -ntaupe  # Lista conexões ativas com detalhes dos usuários e processos

netstat -ant  # Exibe todas as conexões TCP ativas

watch ss -tt  # Monitora conexões TCP em tempo real

netstat -tulnp # Exibir conexões abertas

ss -atp # Monitorar conexões TCP em tempo real

nmap -sV --script=vuln # Escanear vulnerabilidades conhecidas

✅ **Tarefas automatizadas incomuns**

* **Verifique crons do root:**

crontab -u root -l

* Verifique **cron jobs do sistema**:

cat /etc/crontab

ls -la /etc/cron.\*

### ✅ **Entradas suspeitas nos logs**

* **Diretórios principais de logs:**

/var/log/messages  # Mensagens gerais e logs do sistema

/var/log/auth.log  # Registros de autenticação

/var/log/kern.log  # Logs do kernel

/var/log/cron.log  # Logs do cron (tarefas agendadas)

/var/log/maillog   # Logs do servidor de e-mail

/var/log/httpd/   # Diretório com logs de acesso e erro do Apache

/var/log/boot.log  # Logs da inicialização do sistema

/var/log/mysqld.log  # Logs do servidor MySQL

/var/log/secure   # Logs de segurança e autenticação

/var/log/utmp, wtmp  # Registros de logins de usuários

/var/log/syslog   # Logs do cron, Samba e outras atividades do sistema

/root/.\*history  # Histórico de comandos do usuário root

/home/\*/.\*history  # Histórico de comandos dos usuários comuns

* **Pesquisando eventos suspeitos:**

cat /var/log/httpd/access.log | grep "GET /signup.jsp"

grep "root login failure" /var/log/auth.log

cat /var/log/secure | grep "Invalid user"

grep -i "error" /var/log/syslog # Buscar erros gerais no sistema

grep -i "failed" /var/log/auth.log # Buscar falhas de autenticação

grep -i "denied" /var/log/secure # Buscar acessos negados

grep -i "segfault" /var/log/kern.log # Buscar falhas graves no kernel

grep -E -i "(attack|hacked|compromise)" /var/log/\* # Buscar palavras-chave suspeitas

grep -i "cron" /var/log/syslog | grep -v "CRON" # Buscar atividades incomuns no cron

grep -i "sudo" /var/log/auth.log # Monitorar comandos sudo executados

grep -i "ssh.\*Accepted" /var/log/auth.log # Identificar logins SSH bem-sucedidos

grep -i "ssh.\*Failed" /var/log/auth.log # Identificar tentativas de login SSH falhas

grep -i "password" /var/log/auth.log # Buscar tentativas de alteração de senha

grep -i "session opened" /var/log/secure # Monitorar sessões iniciadas

grep -i "session closed" /var/log/secure # Monitorar sessões encerradas

grep -i "suspicious" /var/log/\* # Buscar padrões de comportamento suspeito

grep -i "unknown" /var/log/auth.log # Buscar acessos de usuários desconhecidos

### ✅ **Entradas suspeitas nos logs do kernel**

* Examine os logs do kernel para identificar eventos anormais:

dmesg

* Liste todas as informações importantes sobre o kernel e o sistema:

lsmod # Exibe módulos do kernel carregados

lspci # Lista dispositivos PCI conectados

* **Verifique a presença de rootkits conhecidos**, utilizando ferramentas como rkhunter ou similares.

### ✅ **Verificação de integridade de arquivos (File Hashes)**

* **Verifique os hashes MD5/SHA dos binários críticos**, incluindo /bin, /sbin, /usr/bin, /usr/sbin e outros diretórios onde arquivos essenciais do sistema são armazenados.
* Utilize ferramentas como **AIDE** para essa verificação.

⚠️ **Atenção:** Esse procedimento pode alterar os timestamps dos arquivos. **Execute essa verificação apenas após finalizar as investigações** e se estiver seguro de que pode modificar os dados.

* Para verificar a integridade dos pacotes instalados em diferentes sistemas:
* Em sistemas **baseados em RPM**:

rpm -Va | sort

* Em algumas distribuições Linux, um script chamado **check-packages** pode ser utilizado.
* No **Solaris**:

pkg\_chk -vn

* No **Debian**:

debsums -ac

* No **OpenBSD** (método alternativo):

pkg\_delete -vnx

## **CONTENÇÃO** 🚧

**📌 Objetivo:** Mitigar os efeitos do ataque no ambiente alvo.

✅ **Faça um backup seguro dos dados importantes** da máquina comprometida, se possível, utilizando uma cópia física **bit a bit** de todo o disco rígido em um dispositivo de armazenamento externo.

✅ Além disso, **faça uma cópia da memória RAM** do sistema, que poderá ser analisada posteriormente para investigação forense.

✅ **Isole a máquina comprometida** utilizando uma solução **EDR** (Endpoint Detection and Response) e inspecione outros computadores e redes em busca de comprometimentos.

Ou

✅ **Isole a máquina usando firewall ou switches**, garantindo que o atacante não consiga se movimentar lateralmente na rede.

✅ **Se a máquina não for considerada crítica para a empresa e puder ser desconectada, desligue-a imediatamente e de forma forçada, removendo o cabo de energia.**

* Se for um laptop com bateria, mantenha pressionado o botão de **desligar** por alguns segundos até que o computador seja desligado completamente.

✅ **Investigações offline devem ser iniciadas imediatamente caso a etapa de Identificação não tenha fornecido resultados concretos, mas ainda haja suspeita de comprometimento.**

### ✅ **Busque evidências das ações do invasor**

* (Utilize ferramentas forenses como **Sleuth Kit/Autopsy** para análise detalhada.)

✅ **Encontre todos os arquivos utilizados pelo atacante**, incluindo arquivos excluídos. Verifique o que foi feito com esses arquivos ou sua funcionalidade para avaliar a ameaça.

✅ **Analise todos os arquivos acessados recentemente** para identificar possíveis atividades suspeitas.

✅ **Examine os arquivos de log** em busca de registros de ações incomuns.

✅**Investigue a origem do ataque:**

* Tente descobrir **como o atacante conseguiu acesso ao sistema**.
* **Considere todas as possibilidades**: se nenhuma evidência digital for encontrada, lembre-se de que a intrusão pode ter sido causada por **um insider** (alguém com acesso legítimo ao ambiente).
* **Aplique correções de segurança quando possível** para evitar novas intrusões, principalmente se o atacante explorou uma vulnerabilidade conhecida que já tenha sido corrigida.

✅ Bloquear **tráfego suspeito** e conexões C2 (Command & Control).

✅ Desativar **contas comprometidas** e redefinir credenciais afetadas.

## **REMEDIAÇÃO** 🔄

**📌 Objetivo:** Tomar ações para eliminar a ameaça e evitar futuros incidentes.

⚠️ **Atenção:** Somente inicie a remediação quando tiver **100% de certeza** de que o perímetro foi completamente **mapeado e contido**. Isso evita que o atacante detecte as ações e tente retaliar.

* **Revogue temporariamente todos os acessos** das contas envolvidas no incidente.
* **Remova arquivos maliciosos** identificados durante a investigação.

✅ **Remover malware** e fechar brechas exploradas.

✅ Verificar e restaurar **backups limpos**.

✅ Aplicar **patches de segurança** e reforçar configurações.

✅ Reinstalar sistemas comprometidos, se necessário.

✅ Revisar permissões e políticas de acesso.

## **RECUPERAÇÃO** 🔧

**📌 Objetivo:** Retomar operações normais de forma segura.

⚠️ **Atenção:** Independentemente da extensão do ataque e do conhecimento adquirido sobre o comprometimento, **se o sistema foi comprometido**, a **melhor prática** é **reinstalar completamente o sistema** e aplicar **todas as correções de segurança** disponíveis.

✅ Caso **a reinstalação não seja uma opção**, você deve:

* **Alterar todas as senhas das contas do sistema** e exigir que os usuários façam o mesmo de forma segura.
* **Verificar a integridade de todos os dados armazenados no sistema**, utilizando **hashes de arquivos** (exemplo: **SHA256**).
* **Restaurar todos os binários críticos** que possam ter sido alterados (**exemplo:**/bin/su).
* **Substituir todos os pacotes comprometidos** por versões seguras e confiáveis.

✅ Restaurar **operações críticas** de maneira controlada.

✅ Monitorar **atividade pós-ataque** para detectar possíveis reinfecções.

✅ Aplicar **melhorias de segurança** baseadas na análise do incidente.

## **LIÇÕES APRENDIDAS** 📖

**📌 Objetivo:** Aprimorar continuamente a resposta a incidentes.

✅ Elaborar um **relatório detalhado** do incidente.

✅ Revisar **o que funcionou e o que falhou** na resposta.

✅ Melhorar **planos de segurança e defesa** com base na experiência adquirida.

✅ Ajustar **políticas, ferramentas e processos** para evitar ataques futuros.

✅ **Treinar equipes** para lidar melhor com incidentes similares no futuro.