TLP:CLEAR

INCIDENT RESPONSE METHODOLOGY

IRM #20
RED TEAM DETECTION

Guidelines to Detect and Respond to Redteaming Activities

IRM Author: Alex Kouzmine / CERT SG
Contributor: CERT aDvens
IRM version: 1.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

C'EST VOUS L'AVENIR

SOCIETE GENERALE

TLP:CLEAR

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers for detecting and investigating security issues related to Red Team exercises within the organization.

WHO SHOULD USE IRM SHEETS?

- Blue team members
- SOCs (Security Operation Center)
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you think you have detected a Red Team exercise, follow the IRM, take notes, and contact your business line's Incident Response team, CERT or another applicable Blue team immediately if needed.

→ IRM CERT SG: https://github.com/certsocietegenerale/IRM

→ IRM CERT aDvens (French version): https://github.com/cert-advens/IRM

IRM's Objective: The objective of the Incident Response Methodology for Red Team Detection (IRM20) is to offer a well-structured and systematic approach to identify, manage, and address incidents involving the actions of a Red Team or any other offensive security entities targeting an organization's information systems. Intrinsically, this methodology aims to enhance the organization's overall capabilities to detect, investigate, and mitigate potential cyber threats perpetrated by advanced threat actors.

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: prepare to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal state
6. Lessons learned: identify and improve the process

IRM provides detailed information for each step of the incident response process. The steps stem from the NIST Computer Security Incident Handling Guide.

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT PERPETRATED BY A RED TEAM.

- Develop communication channels to inform stakeholders about detected Red Team exercises; keep in mind the potential existence of overlapping memberships in Blue and White teams to avoid conflict of interest.
- Identify the potentially existing White team members and establish contact points with them.
- Use network-based and host-based intrusion detection systems. Ensure these are configured correctly to effectively monitor network traffic and endpoint systems for malicious activities. Make sure secure logging and monitoring of network and system activities is in place, that the events are logged correctly, transmitted to SIEM and that applicable and tested rules exist to levy alerts.
- Configure and regularly test SIEM tools at your disposal to collect, analyze, and react to security events. These tools can be calibrated to detect indications of Red Team activities, such as login failures, configuration changes, and network reconnaissance attempts.
- Make sure your existing endpoint protection solutions provide adequate controls against malware through static and dynamic detection. Ensure all types of endpoints and servers are covered, including different desktop and server OS, mobile devices and BYODs (if applicable).
- Define specific 24/7 contact points and people to intervene in case of an emergency.
- Establish well-working operational bridges between existing Blue teams (SOC, CERT, other security counterparts); regularly conduct joint incident response exercises onboarding members from different Blue teams.
- Regularly review and assess your organization’s security controls, policies, and procedures.
- Implement a “Red Button” procedural control to halt or temporarily put on stop all redteaming activities in case of an operational need (concurring real incident, impact on production etc.).
- Prepare internal and external communication strategies, procedures, and tools to use during a Red Team incident, including alternative communication channels to exclude information leakage in between Blue and Red team members.
- Provide Blue team staff with an up-to-date understanding of cyber threats, the Red team's role, and methods they might use. This includes previous attack patterns, commonly employed TTPs and previously seen IOCs. Provide access to previously conducted Red Team mission reports and lessons learned if deemed possible.
- Make sure to prepare formal paperwork for the mission, including all applicable documents such as Rules of Engagement, Mission Objectives, Detailed Scenario description, Getting-out-of-Jail card, and any additional documentation of sponsorship from key stakeholders, such as CISO, CTO, etc.

Be prepared to notify C-level stakeholders if required during a Red Team incident.

IDENTIFICATION

OBJECTIVE: DETECT THE RED TEAM ACTIVITY, DETERMINE ITS SCOPE, AND INVOLVE APPROPRIATE PARTIES.

Detection

- Monitor for signs of compromise and unusual behavior in your environment (lateral movement, persistence mechanisms, etc.).
- Investigate security alerts and analyze logs for indicators of potential Red Team activity.
- Triage potential incidents to determine whether they may be part of a Red Team exercise.
- Evaluate the extent and potential consequences of the identified Red Team activity. Ask the White team in case of a doubt to avoid mistreating an incident generated by a real threat actor.
- Once the incident is validated, scope up which systems are affected, which data may have been exposed or exfiltrated, and what potential overall impact can this incident generate on business operations. Providing adequate answers may require envisioning the final objectives pursued by the Red Team.
- Involve all previously identified stakeholders including but not limited to Blue teams, business, infrastructure support, general Information security staff; evaluate potential impact based on available information on the incident and feedback received from business and IT counterparts.
- Evaluate possible remediation scenarios such as blocking interconnections, reinforcing monitoring based on the risk assessment vs. potential impacts on production. Be extremely cautious as to not reveal to the Red teamers they may have been identified.
- If validation and scoping-up affirm a known Red Team incident, escalate it to higher management. Provide them with all necessary details accurately and promptly.
- Have White team coordinators establish communication channels with applicable stakeholders to continuously share information about the ongoing exercise. If required by the incident's nature, set up dedicated alternative (non-corporate) channels to use for communication and data exchange during the exercise.

Consider consulting other IRMs which may be applicable to the suspected Red Team mission:
- IRM-2-Windows Intrusion
- IRM-3-Unix Linux Intrusion Detection
- IRM-7-Windows Malware Detection
- IRM-10 Social Engineering
- IRM-11-Information Leakage
- IRM-14 Scam
- IRM-16 Phishing
- IRM-17 Ransomware
- IRM-18 Large Scale Compromise

CONTAINMENT

OBJECTIVE: PREVENT FURTHER ATTACK DEVELOPMENT AND LIMIT ITS SCOPE.

- Isolate all compromised machines or affected systems to prevent further intrusion or attack propagation.
- Implement access controls and network segmentation to limit the scope of the attack.
- Set up regular meetings with the affected provider, onboarding applicable stakeholders.
- Coordinate with the impacted business stakeholders to implement containment measures, such as isolating compromised systems, blocking malicious IOCs, or changing credentials – in line with business safety requirements.
- Simulate risky or potentially impactful counter-measures to avoid production losses.

If business-critical traffic cannot be disconnected, allow it after putting in place additional security controls to timely detect and inhibit lateral propagation.

If applicable to the identified 'Red' IOCs (double check prior to applying as it may trigger nefarious reactions from the Red teamers):

- Block traffic to identified C2s.
- Block access to / from any applicable red infrastructure elements.
- Disable or restrict accounts compromised by the attackers.
- Send undetected samples to your endpoint security provider, AV vendors and sandbox platforms.
- Send uncategorized malicious URLs, domain names and IPs to your security providers.

You may consider simulating risky or potentially impactful counter-measures to avoid undesirable effects from the exercise on production.

REMEDIATION

OBJECTIVE: REMOVE RED TEAM'S ACCESSES AND SECURE YOUR SYSTEMS.

- Comprehensively review the findings from the previous phases. Ascertain the Red team's initial access points, footholds on systems, lateral activities, persistency mechanisms are well scoped up.
- Make sure the vulnerabilities exploited by the Red Team and other applicable attack methods are well understood.
- Once all tactics, methods and vulnerabilities are identified, prioritize them based on their potential security impacts. Begin patching with the highest-risk vulnerabilities, working down to the less critical ones.
- Based on the findings, harden system configurations to prevent future exploitations. This can involve measures like tightening security settings, limiting user privileges, disabling unnecessary services, and refining firewall rules. This is also applicable to the lessons learned phase.
- **Locate and remove any persistence mechanisms, backdoors or webshells the Red Team may have left on your systems during the exercise.** Perform a thorough investigation to make sure no derivative vulnerabilities or backdoor paths remain.
- Conduct validation tests to confirm that the remediation actions have effectively secured the compromised systems. Double check that the Red Team or any other offensive entity can no longer exploit earlier identified vulnerabilities.
- Duly document all remediation steps, their outcomes, and any challenges encountered during the process. Transmit summaries of remediation fixes and workarounds to relevant stakeholders, including the descriptions of how these vulnerabilities were exploited by the Red Team. This step also applies to the Lessons Learned phase.

Additional due care recommendations: in case of signs of lateralization, please refer to IRM 18 – Large Scale Compromise.

RECOVERY

OBJECTIVE: RESTORE TO NORMAL OPERATIONS.

All the following steps shall be made in a step-by-step manner and with technical monitoring from Blue, Red, White or Purple teams.

- Confirm the effectiveness of used remediation strategies. Double-check that vulnerabilities have been patched, system configurations hardened, and persistence mechanisms removed. The systems should be secure before restoring regular operations.
- Restore systems and services to their normal operational state. In some cases, this might involve additional steps such as rebuilding/remastering systems, restoring data from backups, or migrating to completely new platforms, depending on the extent of the Red Team attack.
- Once systems are effectively restored, conduct thorough functional and security tests to ensure your systems are working optimally and are not vulnerable to similar types of Red Team activities in the future. Work with the affected business owners to restore all affected services or systems, ensuring that they are secure and free from vulnerabilities.
- Monitor your systems' performance to detect any anomalies or potential security issues as a part of the Recovery phase. Make sure the systems are operating normally and have retained their performance levels prior to the Red Team exercise.
- Declare the end of the recovery phase only when you have confirmed that your systems are back to normal, secure and stable. Any anomalies or impact from the Red Team exercise should have been fully addressed.

Triple-check that the vulnerabilities have been patched, system configurations hardened, and persistence mechanisms removed. The system should be secure before restoring regular operations.

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE DETECTED RED TEAM EXERCISE, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

A Red Team mission report should be written and made available to all the involved stakeholders. Different formats of the report may be required to present to different audiences at different strategical, operational and tactical levels.

The following topics should be addressed:

- Initial cause of the compromise
- Actions and timelines of every important event
- What went right
- What went wrong
- TTPs
- Indicators of compromise

Capitalize

- Document the exercise's findings, including attack methods, vulnerabilities, and impact – this vetted knowledge may assist in future incident response missions.
- Assess the effectiveness of the detection and response controls.
- Identify areas for improvement and implement changes to processes and defenses.
- Share knowledge gained from the exercise with relevant stakeholders.
- Conduct a debriefing meeting with all involved parties. The Red Team should present their methodology, tactics, techniques, and procedures, and explain how they exploited system vulnerabilities.
- Perform a detailed analysis of the entire incident response operation, from detection to recovery. Identify what worked well, what didn't, and where there are opportunities for improvement.
- Document the insights gained from the exercise, detailing the challenges faced and their solutions. Compile a list of items that require further remediation actions, specifying who should be responsible for implementing these changes.
- Based on the lessons learned, develop a comprehensive action plan to address identified gaps. Prioritize activities based on their importance and urgency to make sure the highest risks are dealt with promptly (quick wins).
- Dedicate a person to follow up on the advancement of these implementations. This action could be handed over to the Purple Team.
- Communicated the findings and lessons learned to a broader spectrum of stakeholders. This could extend to the entire organization to enhance overall security awareness and behavior.
- Plan for a mid to long-term follow-up audit to verify the effective implementation of the action plan items derived from the Red Team mission findings.

A Redteam exercise may be considered as a pre-phase for a continuous improvement project such as Purple Team.