Operations Security For Red Teams (RED OPSEC)

By

Mohamed Tarek

LinkedIn: https://www.linkedin.com/in/mohamed-tarek-159a821ba/

GitHub: https://github.com/motarekk

TABLE OF CONTENTS

OPSEC in Military

OPSEC Overview

OPSEC or Operations Security is a military-based concept which can be defined as the process of identifying and protecting critical information during running or planned operations that if revealed by an adversary, the operation could fail, obstacle, or the adversary's countermeasures could be improved.

OPSEC is implemented in military as a second nature and is critical to be implemented by all personnel in a daily life basis. It is a continuous process, and it must be considered from early planning for operations. If OPSEC fails, there is a high risk of failing to achieve the operation's objectives or to degrade its success.

Critical Information

Specific facts needed by adversaries to know the intents, plans, and capabilities of the friendly operations, so that they can act and plan for counteractions. The compromise of this information could put the operations in high risk of being terminated or degraded.

Critical Information can be classified or unclassified. OPSEC measures are implemented to protect both classified information and the unclassified information that could reveal indicators of classified information.

Examples of Critical Information

Forces, unit locations and movements, logistics, supplies, command and control communications, computer systems, intelligence and counterintelligence capabilities, vulnerabilities of defenses and arms, security plans, polices, allies, ongoing operations, deception plans and techniques, deception vulnerabilities, research and development, medical information, technologies, and other military information.

OPSEC Measures

All activities and actions that must be taken to protect the critical information from being exposed and collected by adversaries are considered OPSEC measures. This could include encrypting communications, concealing locations, jamming, randomizing actions, avoiding patterns, maintaining cybersecurity measures, and reviewing any information before being published.

An OPSEC measure could be implemented for one or many critical information pieces. Hence, solving Interactions must be considered while implementing OPSEC measures. An interaction occurs when one OPSEC measure that was implemented to protect a piece of critical information causes revealing of an indicator of another piece of critical information.

OPSEC Programs

In order to implement the OPSEC culture in an organization, an OPSEC program must be prepared, and all personnel must have the proper OPSEC training depending on the level of access they have to critical information. The OPSEC program must be compliant with the regulations and effective to both protecting the critical information and to not obstacle the operation's performance. Also, it must be updated periodically depending on the ongoing situations and the changes of the threat landscape and the capabilities of the adversary.

An OPSEC program can be prepared following these steps:

Identify critical information	Determine what information needs to be protected.
Analyze threats	Identify adversaries and their capabilities to collect your critical information.
Analyze vulnerabilities	Analyze what critical information you are exposing.
Assess risk	Assess levels of risk of exposing such critical information and the risk of implementing OPSEC measures on the operations performance.
Implement OPSEC measures	Decide what are the appropriate actions to be implemented to protect the critical information and apply them.

OPSEC Reviews

All documents or activities must be reviewed by the responsible managers/leads to ensure implementing OPSEC measures on any critical information before being exposed to the public. For example, any web content, photographs, video clips, paper documents, wasted garbage, or specific actions must be compliant with the implemented OPSEC program.

OPSEC Assessments

Assessments help to evaluate the application of the OPSEC program and the level of its effectiveness to achieve the OPSEC goals. Assessments must be conducted by experts after reviewing OPSEC reports that are assigned periodically to document the OPSEC status.

OPSEC Vulnerabilities

A vulnerability exists when the adversary manages to collect an indicator of critical information and correctly analyze it to take an action that prevents or degrade operation objectives. OPSEC measures must be implemented to fix those vulnerabilities. Sometimes, vulnerabilities still exist after implementing the measures. In this situation, using deception techniques could help mitigating or reducing the risk of those vulnerabilities.

Deception

Deception is performing specific actions to prevent adversary’s intelligence from following and collecting information about operations and to cause confusion and loss of their interest in the operation’s activities.

Examples of Poor OPSEC

- **Russo-Ukrainian Conflict:**

During the Russo-Ukrainian conflict, it has been found that due to some pictures of military troops carelessly token by the Russian soldiers, Ukrainian troops were able to identify their locations and then target them.

- **Natanz Nuclear Facility:**

Due to some photos and video clips publicly shared for the Natanz Nuclear Facility including details of some equipment and devices in the facility, the adversaries of Iran were able to exploit that information to help them in the development of their sophisticated malware (known as Stuxnet) to target these specific systems, and therefore their operation ended up being successful and achieved its objectives.

OPSEC in Offensive Security

OPSEC in Red Teaming

Red Team is a group of ethical hackers who are authorized to perform Tactics, Techniques, and Procedures (TTPs) on a target environment to emulate a real-world threat in order to train and measure the effectiveness of the people, process, and technology used to defend that environment.

The main goal of Red Team engagements is to exercise the Blue Team with a real-world scenario and to have a whole look of the environment's security from different adversary's perspectives. Therefore, the level of OPSEC required in Red Team engagements depends on the type of the operation.

In an adversary emulation engagement, the level of required OPSEC depends on the level of the adversary being emulated. If the objective is to emulate a certain adversary or group of adversaries, OPSEC measures and used techniques would be limited to that adversary's TTPs and capabilities that are found to be used in the wild, collected by threat intelligence, and profiled before the operation. For example, some low-profile adversaries use open-source tools without modification and are cureless to their OPSEC. Also, some high-level adversaries use the same TTPs of low-level adversaries if they don't want to burn their custom techniques on certain environments. On the other hand, other high-profile adversaries prefer using sophisticated techniques to achieve their objectives and to preserve their OPSEC.

If it is an in-depth Red Teaming operation, unique techniques must be developed to avoid detection and to maintain OPSEC during the whole engagement until achieving the required objectives.

Responsible Red Teaming

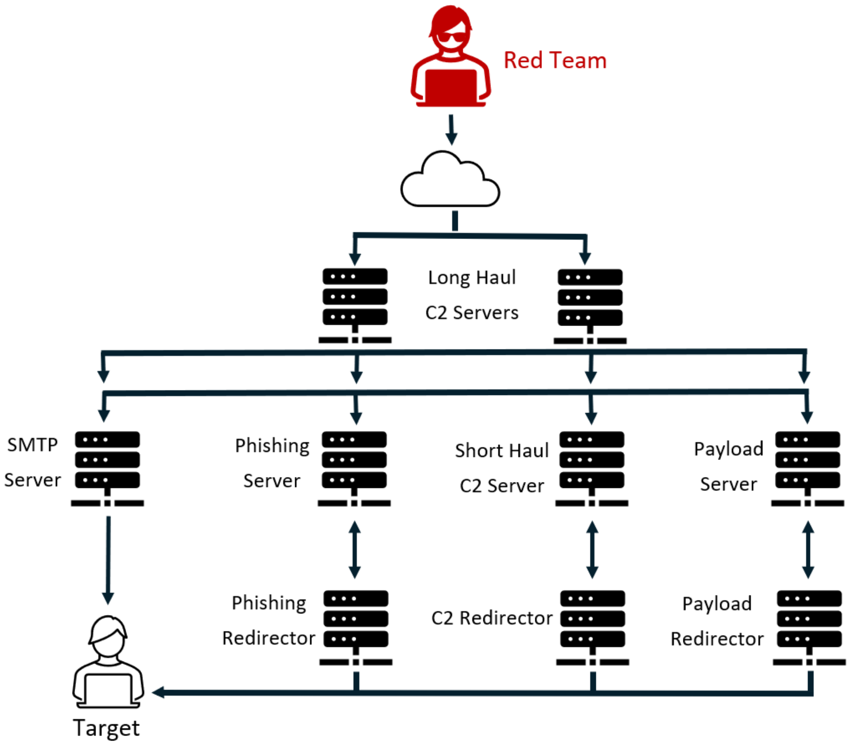
When it comes to OPSEC in Red Teaming, two things are critical to consider being responsible of; the security of the operation and the security of customer's data being processed during the operation. Both are considered parts of OPSEC. To simplify, a Red Team must keep their activities hidden from the Blue Team until the end of the operation to achieve the required objectives, and they also must secure the customer's data from actual threat actors during the operation. The data stored in the Red Team's infrastructure are information about the vulnerabilities, exploitations, exfiltrated data of the customer. Hence, it is critical to implement the proper security measures to protect this information.

OPSEC Measures for Red Teams

Red Team operators must be careful and responsible of each action they are performing during the engagement. OPSEC measures must be implemented in early planning of the engagement. Here are some recommended OPSEC measures to be implemented by Red Teams:

- **Measures to preserve invisibility of Red Team activities:**

- Prepare a responsible Red Team infrastructure that ensures the invisibility and continuity of the operation. This includes redirectors, short and long haul C2 servers, previously registered and categorized domains, etc.



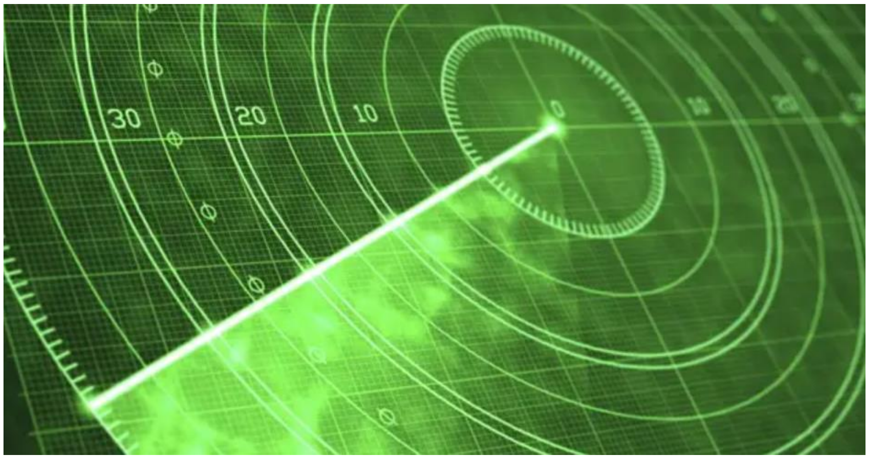
- Never use your identifiable data. This includes your real IP addresses, MAC addresses, User Agents, etc. Use spoofed ones instead.
- For User Agents, you can use Googlebot, Shodan, or Censys User Agents.
- Use domain names instead of IP addresses in your reverse shells, as they are easily changeable if burned.
- Consider performing passive instead of active reconnaissance as much as possible.
- Develop your own unique techniques in the whole cyber kill chain from reconnaissance, weaponization, exploitation, until the data exfiltration.
- Consider using the 'Exploitation Without Exploits' technique, which aims to use the system against itself.
- Be aware of all the forensic traces that your tools or payloads produce.
- Consider modifying and customizing used open-source tools or frameworks to match your only needs and to avoid being signatured.

○ **Measures to protect client's data during the engagement:**

- Consider protecting, monitoring and auditing your Red Team infrastructure as it is an extension of your organization.
- Maintain the security of your C2 servers by managing patches, implementing strong authentication, IP whitelisting and proper firewall configurations to prevent unauthorized access.
- Classify the sensitivity of client's data with the trusted agent (white cell) before the engagement.
- Never exfiltrate sensitive data without encryption from the target's environment.
- Consider encrypting client's data at rest in your teamservers.

- To avoid confliction between Red Team activities and real adversary’s activities, always log all your actions during the operation including used tools, payloads, commands, terminal outputs, screenshots, timestamps, and artifacts.
- In case of a ransomware simulation, ensure with the trusted agent that the customer’s data to be encrypted is not sensitive and is backed up before the encryption action in case of any data loss in a worst case scenario.
- Never access or take screenshots of customer’s highly sensitive data without an explicit authorization.
- Always review scripts, tools, payloads, open-source projects before using them in the engagement to protect customer’s environment from unintended damages or malicious activities.
- Do not cause denial of service (DOS) to any part of the customer’s production environment.

Deception in Red Teaming



preserve being under the radar

Red Teams should consider implementing deception as a part of their TTPs by performing some actions that distracts analysts' efforts and lead them to investigate in the wrong path. This gives the Red Team an advantage in time and a cover of their actual activities.

For example, after gaining an initial access to the target's network, a port scan could be conducted from different spoofed IP addresses to mislead the Blue Team to investigate and respond as if it is a reconnaissance activity being conducted from an external adversary. This could give time and cover for the actual activity of the red team inside the target's network. Also, deception could be done by performing trivial actions that indicates complexity, so that the Blue Team could conduct unnecessary additional investigations, which could give more time for the Red Team as well.

SOC teams will likely look for the red alerts before the orange or the yellow ones. In other words, if a red team is going to perform an activity that will produce a low- or medium-level alert in the SIEM solution for the SOC team, they should consider performing another activity in an untargeted part of the network that will produce a high-level alert to distract SOC's attention.

Keep in mind that even deception activities need OPSEC, because you don't want the Blue Team to realize your deception techniques. So, deception helps mitigating OPSEC vulnerabilities, but it needs OPSEC for its activities as well. In the previous example, conducting the port scan was a deception activity, and the use of spoofed IP addresses was the OPSEC measure for that deception activity. In general, deception activities must be believable for the Blue Team.

Finally, always remember that Red Team’s work is to help the Blue Team improve their skills and enhance the environment’s readiness to cyber-attacks. Red Teams exist to reduce the risk, not to increase it. Red Team’s work is to improve the security by revealing its vulnerabilities and limitations in an ethical responsible way.

Reference

- Joe Vest & James Tubberville, 2019, *Red Team Development and Operations*, Zero-Day Edition.

- Army Regulation 530–1: Operations Security (Septemper, 2014):

https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/r530_1.pdf

- Joint Publication 3-13.3: Operations Security (January, 2016):

https://media.defense.gov/2020/Oct/28/2002524944/-1/-1/0/JP%203-13.3-OPSEC.PDF

- WIRED: Their Photos Were Posted Online. Then They Were Bombed (August, 2022):

https://www.wired.com/story/wagner-group-osint-russia-ukraine/

- itnews: Stuxnet a 'perfect match' to Iran nuclear facility, photo reveals (December, 2011):

https://www.itnews.com.au/news/stuxnet-a-perfect-match-to-iran-nuclear-facility-photo-reveals-282735