Red Team OPSEC

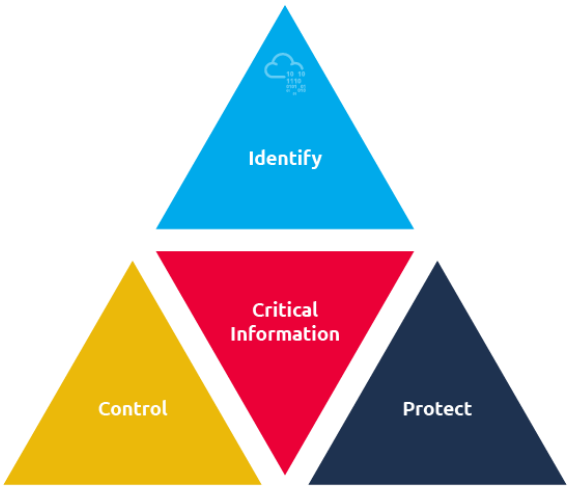
Introduction

Operations Security (OPSEC) is a term coined by the United States military. In the field of cybersecurity, let's start with the definition provided by NIST:

"Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analyzis of threats, analyzis of vulnerabilities, assessment of risks, and application of appropriate countermeasures."

Let's dive into the definition from a red team perspective. As a red team member, your potential adversaries are the blue team and third parties. The blue team is considered an adversary as we are attacking the systems they are hired to monitor and defend. Red vs. blue team exercises are common to help an organization understand what threats exist in a given environment and better prepare their blue team if a real malicious attack occurs. As red teamers, even though we are abiding by the law and authorized to attack systems within a defined scope, it does not change the fact that we are acting against the blue team's objectives and trying to circumvent their security controls. The blue team wants to protect their systems, while we want to penetrate them.

Denying any potential adversary the ability to gather information about our capabilities and intentions is critical to maintaining OPSEC. OPSEC is a process to identify, control and protect any information related to the planning and execution of our activities. Frameworks such as Lockheed Martin's Cyber Kill Chain and MITRE ATT&CK help defenders identify the objectives an adversary is trying to accomplish. MITRE ATT&CK is arguably at the forefront of reporting and classifying adversary tactics, techniques, and procedures (TTPs) and offers a publicly accessible knowledge base as publicly available threat intelligence and incident reporting as its primary data source.



The OPSEC process has five steps:

1. Identify critical information
2. Analyze threats
3. Analyze vulnerabilities
4. Assess risks
5. Apply appropriate countermeasures

If the adversary discovers that you are scanning their network with Nmap (the blue team in our case), they should easily be able to discover the IP address used. For instance, if you use this same IP address to host a phishing site, it won't be very difficult for the blue team to connect the two events and attribute them to the same actor.

OPSEC is not a solution or a set of rules; OPSEC is a five-step process to deny adversaries from gaining access to any critical information (defined in Task 2). We will dive into each step and see how we can improve OPSEC as part of our red team operations.

Critical Information Identification

What a red teamer considers critical information worth protecting depends on the operation and the assets or tooling used. In this setting, critical information includes, but is not limited to, the red team's intentions, capabilities, activities, and limitations. Critical information includes any information that, once obtained by the blue team, would hinder or degrade the red team's mission.

To identify critical information, the red team needs to use an adversarial approach and ask themselves what information an adversary, the blue team, in this case, would want to know about the mission. If obtained, the adversary will be in a solid position to thwart the red team's attacks. Therefore, critical information is not necessarily sensitive information; however, it is any information that might jeopardize your plans if leaked to an adversary. The following are some examples:

- Client information that your team has learned. It's unacceptable to share client specific information such as employee names, roles, and infrastructure that your team has discovered. Sharing this type of information should kept on need-to-know basis as it could compromise the integrity of the operation. The Principle of Least Privilege (PoLP) dictates that any entity (user or process) must be able to access only the information necessary to carry out its task. PoLP should be applied in every step taken by the Red Team.
- Red team information, such as identities, activities, plans, capabilities and limitations. The adversary can use such information to be better prepared to face your attacks.
- Tactics, Techniques, and Procedures (TTP) that your team uses in order to emulate an attack.
- OS, cloud hosting provider, or C2 framework utilised by your team. Let's say that your team uses Pentoo for penetration testing, and the defender knows this. Consequently, they can keep an eye for logs exposing the OS as Pentoo. Depending on the target, there is a possibility that other attackers are also using Pentoo to launch their attacks; however, there is no reason to expose your OS if you don't have to.
- Public IP addresses that your red team will use. If the blue team gains access to this kind of information, they could quickly mitigate the attack by blocking all inbound and outbound traffic to your IP addresses, leaving you to figure out what has happened.
- Domain names that your team has registered. Domain names play a significant role in attacks such as phishing. Likewise, if the blue team figures out the domain names you will be using to launch your attacks, they could simply block or sinkhole your malicious domains to neutralize your attack.

- Hosted websites, such as phishing websites, for adversary emulation.

****

Answer the questions below:

Click on View Site and follow through till you get the flag.

Answer: THM{OPSEC_CRITICAL_INFO}

****

Threat analyzis

After we identify critical information, we need to analyze threats. Threat analyzis refers to identifying potential adversaries and their intentions and capabilities. Adapted from the US Department of Defense (DoD) Operations Security (OPSEC) Program Manual, threat analyzis aims to answer the following questions:

1. Who is the adversary?
2. What are the adversary's goals?
3. What tactics, techniques, and procedures does the adversary use?
4. What critical information has the adversary obtained, if any?

The task of the red team is to emulate an actual attack so that the blue team discovers its shortcomings, if any, and becomes better prepared to face incoming threats. The blue team's main objective is to ensure the security of the organization's network and systems. The intentions of the blue team are clear; they want to keep the red team out of their network. Consequently, considering the task of the red team, the blue team is considered our adversary as each team has conflicting objectives. We should note that the blue team's capabilities might not always be known at the beginning.

Malicious third-party players might have different intentions and capabilities and might pause a threat as a result. This party can be someone with humble capabilities scanning the systems randomly looking for low-hanging fruit, such as an unpatched exploitable server, or it can be a capable adversary targeting your company or your client systems. Consequently, the intentions and the capabilities of this third party can make them an adversary as well.

Adversary	Intentions	Capabilities
Blue Team	Keep intruders out	Not always known
Malicious third-party	Varies	Varies

We consider any adversary with the intent and capability to take actions that would prevent us from completing our operation as a threat:

- threat = adversary + intent + capability

In other words, an adversary without the intent or capability does not pose a threat for our purposes.

Vulnerability analyzis

After identifying critical information and analyzing threats, we can start with the third step: analyzing vulnerabilities. This is not to be confused with vulnerabilities related to cybersecurity. An OPSEC vulnerability exists when an adversary can obtain critical information, analyze the findings, and act in a way that would affect your plans.

To better understand an OPSEC vulnerability as related to red teaming, we'll consider the following scenario. You use Nmap to discover live hosts on a target subnet and find open ports on live hosts. Moreover, you send various phishing emails leading the victim to a phishing webpage you're hosting. Furthermore, you're using the Metasploit framework to attempt to exploit certain software vulnerabilities. These are three separate activities; however, if you use the same IP address(es) to carry out these different activities, this would lead to an OPSEC vulnerability. Once any hostile/malicious activity is detected, the blue team is expected to take action, such as blocking the source IP address(es) temporarily or permanently. Consequently, it would take one source IP address to be blocked for all the other activities use this IP address to fail. In other words, this would block access to the destination IP address used for the phising server, and the source IP address using by Nmap and Metasploit Framework.

Another example of an OPSEC vulnerability would be an unsecured database that's used to store data received from phishing victims. If the database is not properly secured, it may lead to a malicious third party compromising the operation and could result in data being exfiltrated and used in an attack against your client's network. As a result, instead of helping your client secure their network, you would end up helping expose login names and passwords.

Lax OPSEC could also result in less sophisticated vulnerabilities. For instance, consider a case where one of your red team members posts on social media revealing your client's name. If the blue team monitors such information, it will trigger them to learn more about your team and your approaches to better prepare against expected penetration attempts.

****

Answer the questions below:

Your red team uses THC-Hydra to find the password for a specific login page. Moreover, they are using the Metasploit framework on the same system as THC-Hydra. Would you consider this an OPSEC vulnerability? (Y/N)
Answer: Y

One of the red team members posts a photo of his cat every day. Would this be considered an OPSEC vulnerability? (Y/N)
Answer: N

Your red team went for dinner, took a photo, and tagged every team member on a popular social media platform. Would you consider this an OPSEC vulnerability? (Y/N)
Answer: Y

Your red team posts on its website a list of clients you regularly conduct red team exercises with. Would you consider this an OPSEC vulnerability? (Y/N)
Answer: Y

One of your red team members posted a photo of her morning coffee. Would you consider this an OPSEC vulnerability? (Y/N)
Answer: N
****

Risk Assessment

We finished analyzing the vulnerabilities, and now we can proceed to the fourth step: conducting a risk assessment. NIST defines a risk assessment as "The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system." In OPSEC, risk assessment requires learning the possibility of an event taking place along with the expected cost of that event. Consequently, this involves assessing the adversary's ability to exploit the vulnerabilities.

Once the level of risk is determined, countermeasures can be considered to mitigate that risk. We need to consider the following three factors:

1. The efficiency of the countermeasure in reducing the risk
2. The cost of the countermeasure compared to the impact of the vulnerability being exploited
3. The possibility that the countermeasure can reveal information to the adversary

Let’s revisit the two examples from the previous task. In the first example, we considered the vulnerability of scanning the network with Nmap, using the Metasploit framework, and hosting the phishing pages using the same public IP address. We analyzed that this is a vulnerability as it makes it easier for the adversary to block our three activities by simply detecting one activity. Now let’s assess this risk. To evaluate the risk related to this vulnerability, we need to learn the possibility of one or more of these activities being detected. We cannot answer this without obtaining some information about the adversary’s capabilities. Let’s consider the case where the client has a Security Information and Event Management (SIEM) in place. A SIEM is a system that allows real-time monitoring and analyzis of events related to security from different sources across the network. We can expect that a SIEM would make it reasonably uncomplicated to detect suspicious activity and connect the three events. As a result, we would assess the related risk as high. On the other hand, if we know that the adversary has minimal resources for detecting security events, we can assess the risk related to this vulnerability as low.

Let’s consider the second example of an unsecured database used to store data received from a phishing page. Based on data collected from several research groups using honeypots, we can expect various malicious bots to actively target random IP addresses on the Internet. Therefore, it is only a matter of time before a system with weak security is discovered and exploited.

****

Answer the questions below:

Your red team uses THC-Hydra to find the password for a specific login page. Moreover, they are using the Metasploit framework on the same system as THC-Hydra. Knowing that your target uses a properly configured Intrusion Detection System (IDS), would you consider this vulnerability as high risk? (Y/N)

Answer: Y

****

Countermeasures

The final step is applying countermeasures. The US Department of Defense (DoD) Operations Security (OPSEC) Program Manual states, “Countermeasures are designed to prevent an adversary from detecting critical information, provide an alternative interpretation of critical information or indicators (deception), or deny the adversary’s collection system.”

Let’s revisit the two examples we presented in the Vulnerability analyzis task. In the first example, we considered the vulnerability of running Nmap, using the Metasploit framework, and hosting the phishing pages using the same public IP address. The countermeasure for this one seems obvious; use a different IP address for each activity. This way, you can ensure that if one activity was detected the public IP address is blocked, the other activities can continue unaffected.

In the second example, we considered the vulnerability of an unsecured database used to store data received from a phishing page. From a risk assessment perspective, we considered it as high risk due to malicious third parties potentially looking for random easy targets. The countermeasure, in this case, would be to ensure that the database is adequately secured so that the data cannot be accessed except by authorized personnel.

More Practical Examples

In this task, we apply the five elements of the OPSEC process as we focus on different examples of critical information related to red team tasks. We will follow the following steps:

1. Identify critical information
2. analyze threats
3. analyze vulnerabilities
4. Assess risk
5. Apply appropriate countermeasures

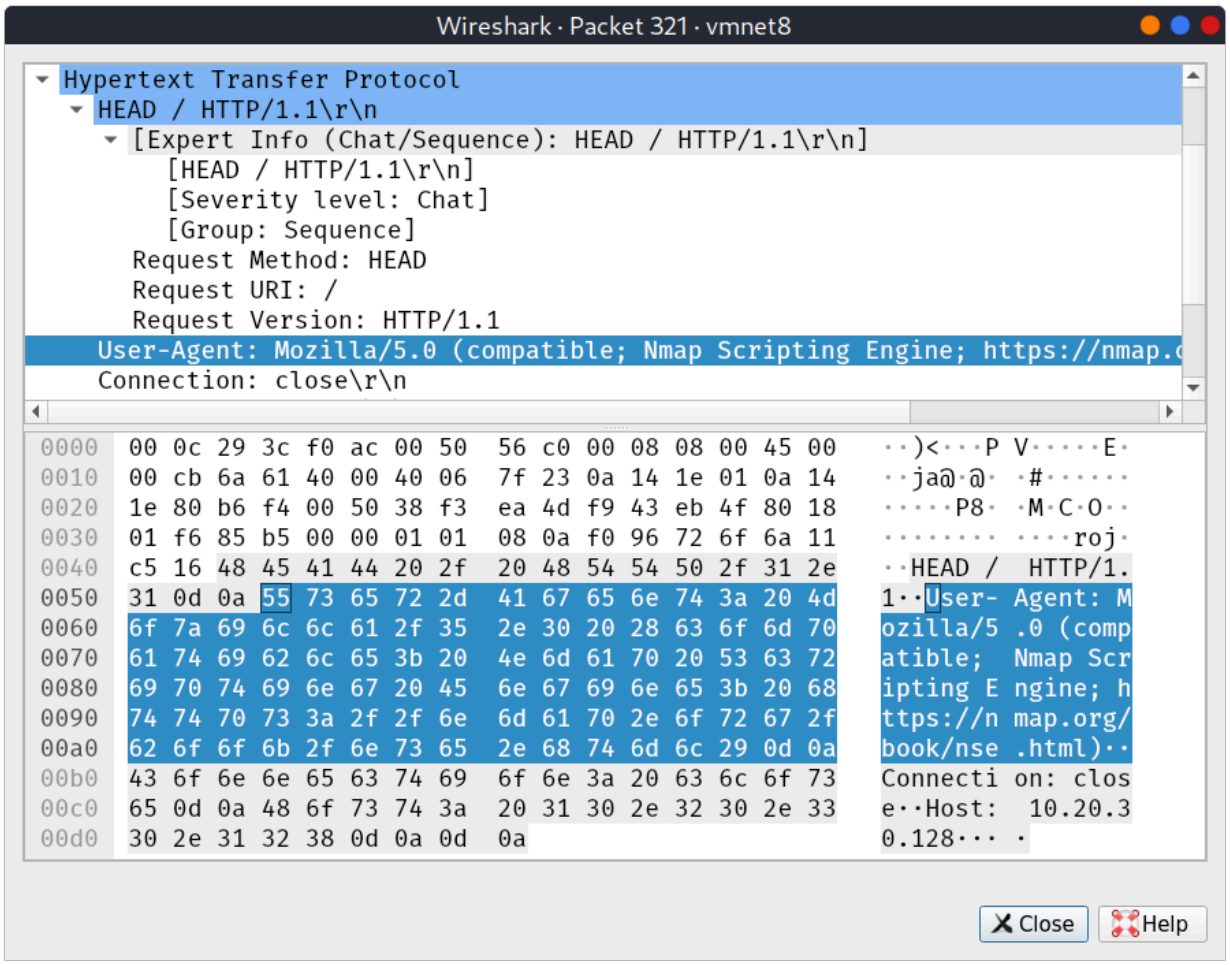
Programs/OS/VM used by the red team:

- Critical information: We are talking about the programs, the operating system (OS), and the virtual machine (VM) together.
- Threat analyzis: The blue team is looking for any malicious or abnormal activity on the network. Depending on the service we're connecting to, it's possible that the name and the version of the program we're using, and the OS version and VM hostname could be logged.
- Vulnerability analyzis: If the OS chosen for the given activity is too unique, it could make it easier to link activities back to your operation. The same applies to VMs with hostnames that stand out. For instance, on a network of physical laptops and desktops, if a new host joins with the hostname kali2021vm, it should be easy to spot by the blue team. Likewise, if you use various security scanners or for instance you don't use a common user agent for web based activities.
- Risk Assessment: The risk mainly depends on which services we're connecting to. For instance, if we start a VPN connection, the VPN server will log plenty of

information about us. The same applies to other services to which we might connect.

- Countermeasures: If the OS we are using is uncommon, it would be worth the effort to make the necessary changes to camouflage our OS as a different one. For VMs and physical hosts, it's worth changing the hostnames to something inconspicuous or consistent with the client's naming convention, as you don't want a hostname such as AttackBox to appear in the DHCP server logs. As for programs and tools, it is worth learning the signatures that each tool leaves on the server logs.

Example: The figure below shows the User-Agent that will be logged by the remote web server when running Nmap scans with the -sC option when Nmap probes the web server. If an HTTP user agent isn't set at the time of running the given Nmap script, the logs on the target system could log a user agent containing Nmap Scripting Engine. This can be mitigated using the option --script-args http.useragent="CUSTOM_AGENT".



****

Answer the questions below:

Click on View Site and follow through till you get the flag.
Answer: THM{OPSEC-RED-TEAM}
****

Conclusion

In this room, we have covered how the OPSEC process can be applied to red team operations. OPSEC process has five elements:

1. Identify critical information: “Critical information includes, but is not limited to, red team’s intentions, capabilities, activities and limitations.”
2. analyze threats: Threat analyzis refers to identifying potential adversaries and their intentions and capabilities.
3. analyze vulnerabilities: An OPSEC vulnerability exists when an adversary can obtain critical information, analyze the findings, and act in a way that would affect your plans.
4. Assess risks: “Risk assessment requires learning the possibility of an event taking place along with the expected cost of that event.”
5. Apply appropriate countermeasures: Countermeasures are designed to prevent an adversary from detecting critical information, provide an alternative interpretation of critical information or indicators (deception), or deny the adversary’s collection system.

OPSEC is a process that can be applied outside the military. This room covered how it is applied to red team operations; furthermore, it is not difficult to apply it to other fields, such as marketing or industry. This process will help prevent the adversary from putting the pieces together, thus preventing them from taking timely action.