SCYTHE

PURPLE TEAM EXERCISE

Executive Summary

Purple Team exercises are an efficient and effective method of adversary emulation leading to the training and improvement of people, process, and technology. Red Teams and Blue Teams work together in a live, production environment, emulating a selected adversary that has the capability, intent, and opportunity to attack the target organization provided by Cyber Threat Intelligence. Purple Team exercises are ‘hands on keyboard’ exercises where Red and Blue teams work together with an open discussion about each attack procedure and how to detect and alert against it.

Quick Overview:

- Cyber Threat Intelligence identifies adversary and TTPs
- Stakeholders define exercise goals and select which TTPs Red Team will emulate
- Preparation is key for Purple Team exercises as various functions are taking members from their “Business As Usual” function

Want to run a Purple Team exercise?
We'll help you through it! Our CTO office led by Jorge Orchilles (Certified SANS instructor and industry leading Purple Team expert) will help you run your own with training, consulting, and custom threat emulation.

Challenges

Preparation time is by far the most consuming part of a Purple Team exercise. Choosing the Tactic, Techniques, and Procedures (TTPs) is the first challenge as it requires relevant Cyber Threat Intelligence to pick an adversary that has the capability, opportunity, and intent to attack your organization. Each adversary has a number of TTPs that have been observed in the wild. If your organization does not have an understanding of the detective and preventive controls of those TTPs, then choosing which ones to use will be even more difficult.

Choosing the correct TTPs to emulate. The TTPs that will be used during the Purple Team exercise should be test cases that the Blue Team have detective controls against. If the TTP is prevented, it will offer little value. If there is no visibility to the TTP, it will educate the rest of the team but not offer the most value. The ideal TTPs are those that are detected, logged, or alert so teams can learn to identify, escalate, and contain.

Emulating the TTPs consistently. The next step is for the Red Team to understand and document how to emulate the TTP. Prior to launching campaigns with SCYTHE, Red Teams would need to document every command that would be executed for every TTP that was being emulated in the Purple Team exercise. Even then, some commands would not execute exactly the same (no consistency). **Inconsistent TTP execution leads to inconsistent results.**

Benefit

Select TTPs for chosen adversary through the SCYTHE Threat Catalog. SCYTHE makes the Cyber Threat Intelligence function more efficient with its Threat Catalog. Select the adversary and it will automatically create an adversary campaign with TTPs. This allows for more efficient preparation: you don’t have to manually analyze third party cyber threat intelligence reports and everything is already mapped to MITRE ATT&CK.

Red Teams uses SCYTHE to create payloads for the selected TTPs. Instead of documenting each command that needs to be typed to emulate each TTP, the payload is created ahead of time using SCYTHE. The payload execution can be tested by the Red Team beforehand to ensure the TTPs trigger successfully. No wasted time with open source, manual, and inconsistent tools.

Red Teams execute the same TTP consistently and efficiently as many times as the Blue Team requires to tune their defenses. Consistent executions ensure the same TTPs, artifacts, and Indicators of Compromise (IoCs) are executed on the production environment allowing for the focus to be on Blue Teams activities: SOC looking at alerts, Hunt Team looking at EDR and logs, and incident responders doing forensics for each TTP.

Results

Valuable use of everyone's time. The Red Team has much of the burden during the preparation phase to figure out how to emulate the TTPs, set up the attack infrastructure, and document every single command to ensure it is executed consistently. With SCYTHE, all these steps are done through a simple workflow to create a payload that will execute consistently every time. This allows the exercise to flow without wasting resources.

Consistent execution of TTPs. No chances of mistyping, fat fingering, or pasting the wrong command. Focus should be on the Blue Team detecting and hunting for the TTP instead of the Red Team executing the TTPs. This facilitated the exercise coordinator to keep the exercise flowing and on time. All the selected TTPs were executed successfully and the Blue Team was able to detect and in some cases, improve the tools to detect and respond quicker to attacks.

Improvement of people, process, and technology. Purple Team Exercises improve both the Red Teams and the Blue Teams as everyone understands what artifacts and indicators of compromise (IoCs) each TTP generates and it improves the Blue Team since they would understand how the attack works and what IoCs to look for.