ORCHESTRA

Harmony Purple: Automated Purple Team Whitepaper

Effective Cyber Risk Assessment, Management, and Operations

Release Date: December 2020

Copyright

The “original instructions” of this manual are published in the English language.

The information conveyed in this document has been carefully checked and is believed to be reliable at the time of printing. However, Orchestra Group Ltd makes no warranty regarding the information set forth in this document and assumes no responsibility for any errors or inaccuracies contained herein. Orchestra Group Ltd is not obligated to update or correct any information contained in this document. Orchestra Group Ltd reserves the right to change products or specifications at any time without notice.

Mention of third-party products or services is for informational purposes only and does not constitute an endorsement or recommendation.

Contents

Overview

In this paper we will address the main questions every organization needs to continually answer in order to implement an effective cyber security program:

- How secure are my digital assets from a cyberattack?
- Is my level of cyber protection in line with my risk appetite?
- What is the most effective way to lower my cyber risk and increase my security?

Answering these basic questions should be simple, but it’s not because these questions combine several very complex and diverse challenges. The first challenge is the cyber security adversarial landscape. We all know that cyber complexity is through the roof. So far this year (November 2020) there have been over 16,000 new common vulnerabilities and exploits (CVEs) reported and we are on track to reach about 20,000 by year’s end. Mitre ATT&CK catalogues over 300 unique adversarial techniques.

The next challenge is to provide a true assessment of your current cyber security posture. This means finding and assessing your existing assets relative to the current adversarial landscape and your risk appetite.

Finally, there is the challenge of creating an actionable and measurable improvement plan, and tracking its progress over time. Of course, defining the plan is not enough. It is also key that you execute the plan as a continuous improvement process.

Given all these challenges, the most cost-effective way of addressing these questions is by a purple (combined red and blue) team. However, cost effectiveness doesn’t translate into cheap. Dedicated red and blue teams are expensive and well beyond the budget of most organizations. The next best thing is an automated purple team. Even if you can afford a dedicated purple team, assuming that you have unlimited resources, providing them with tools and automation is also critical.

Why Purple?

Red teams, like penetration testers, are focused on breaking into an organization and demonstrating how an organization can be breached. They are the security "test team." They test the organization's security, and just like any tester, focus on ways to make it fail. However, the real goal, as it is for any test or audit organization, is to provide insights on how to better secure the organization. If the testers can easily break into an organization, it is a failure of the red team or the penetration testing, as much a blue team issue.

When a red team works on its own, many times the targets are the easy pickings, not the most valuable targets for the blue team. Not all tests are of equal value. The best tests find the riskiest issues, and the most valuable assets, for the least cost. Purple teams look at both sides of the testing equation, which is why purple teams provide more bang for the buck than penetration testers, or red teams, alone.

The job of the blue team is to make sure no one, including the red team, can breach an organization without using extreme measures exceeding the organization's appetite. This means adversarial techniques that are just too expensive to protect against. For example, protection against a state-level attack is probably prohibitively expensive for most organizations. Luckily, most organizations are not at risk from state-level attacks, just everyday cyber criminals.

A blue team continuously updates and tracks the processes and controls used to prevent adversaries from breaching an organization, as well as the state of the adversarial landscape. It is a complex, never-ending task because systems and applications are hard to keep up to date. In addition, users inadvertently provide attackers with a foothold in an organization and the adversarial landscape continually changes.

On a positive note, as it becomes more difficult to break into an organization, attackers are inclined to give up and move to easier targets. As with all security, cyber security is a tradeoff between effort and reward for you, as well as your adversaries. With enough time, effort, and resources, any organization can be breached. Therefore, your goal must be to provide as effective a cyber defense as possible within your budget. You must also create a budget and plan that is within your risk appetite.

A purple team approach combines red and blue teams into a continuous improvement team. The purple team's job is to translate red team test failures (breaches) into blue team corrective and preventative actions (or CAPA, using the terminology of process improvement). The purple team provides continuous improvement for your security processes and controls. Continuous improvement is the most effective way to provide proactive security and protect your organization from cyberattack.

As opposed to penetration testing, purple team automation does not place a primary focus on initial access or on an audit. Purple team uses credentials, especially to high-risk assets (“white box”), which could have serious consequences when compromised. The reason is that most assets have more vulnerabilities after authentication. This is especially true if the asset is high risk, since it identifies the potential threats in advance of the scenario where credentials are compromised and enables the blue team to provide proactive, even predictive, protection.

Purple Team’s Process

Purple teams should provide a continuous improvement cycle that includes the following:

- Find and prioritize cyber security issues for your environment (red team).
- Propose primary control processes and actions for new issues (blue team).
- Apply recommended actions (IT).
- Assess and propose compensating control processes for unresolved issues (blue team).

Just like in any continuous improvement process, the purple team must go back to the beginning and start again.

Find and Prioritize Cyber Security Issues for Your Environment (Red Team)

There are many issues that must be considered and prioritized by a purple team. In any organization, there are hundreds or even thousands of technical security issues, which are too many to handle at once, or maybe at all. The key is understanding what the most critical issues are given your specific environment and risk appetite, and then start a process of selecting the most important ones, fixing them, testing the results, and then moving to the next issues.

The purple team’s primary focus is on several adversarial tactics. These include initial access, privilege escalation, defense evasion, credential access, and lateral movement. The goal of the purple team is to prevent an attacker from entering the infrastructure. In addition, should an attacker breach the infrastructure, the purple team wants to prevent the attacker moving around unnoticed until they find something worthwhile to steal or disrupt. This is different than penetration testers and standalone red teams that pay more attention to the initial breach than how to move about the organization’s infrastructure unnoticed. Purple teams have more freedom to find and fix issues that are important to the organization, but not obvious.

Purple teams need knowledge of the organization to ensure that the results are the most relevant and prioritized correctly. That knowledge is used to apply vulnerability, configuration, access, and audit (logging) management controls for maximal effect. Knowledge of the organization enables a purple team to provide better feedback and prioritization on what is wrong and how to fix it.

The following are the main security issues that the blue teams look for:

- Vulnerable assets
  - Lateral movement weaknesses
    - RCE vulnerabilities
  - Initial access weaknesses
    - Social vulnerabilities
- Misconfiguration issues
  - Security-baseline issues
  - Compliance-related issues
- Asset access (and privilege) issues
  - Credential or password exposures
  - Privilege escalation vulnerabilities
- Missing, or misconfigured, system and application logs

Propose Primary Control Processes and Actions for New Issues

In many organizations, the purple team makes control recommendations and it is up to the IT group to accept/apply or reject those recommendations. This is especially true for automated purple teams—at least for the moment. As organizations become more comfortable with automated purple teams, automation will grow to include mitigation.

The primary protective control for vulnerability management is patching. The goal of the purple team is prioritizing patches to ensure that the highest organizational risks are covered first. This is not simply which vulnerability has the highest CVSS, but must also take into account the organizational context of the vulnerability. In the end, the blue team suggests the patches and it is up to the IT group to deploy them.

The purple team's primary control is configuration. Correct configuration is critical to cyber defense, both at the OS and application level. Configuration can be used to harden assets based on compliance needs, or simply to apply sensible guidance on ensuring safe configurations. Here too it is up to the IT group to apply the appropriate configurations as recommended by the purple team.

Exposed credentials and lax administrative access management is another critical security exposure and a popular tactic for adversaries. Purple teams need to point out insecure credentials and inappropriate access practices and propose more secure alternatives.

Finally, logging is critical for both proactive and reactive cyber defense. The absence of appropriate logging can cripple any attempt to find or remediate a security issue. Compromising logging is a way for an adversary to blind the organization to an on-going attack. The purple team needs to ensure that all logs are available and at the appropriate level, relative to the organization's risk appetite.

Of course, these are just the basic tasks of purple teams, but they can do much more, The lower an organization's risk appetite, the more they'll need from the purple team. The purple team also needs to make the tradeoffs between different control applications to ensure that the IT group's actions are as effective as possible, with respect to the organization's risk appetite.

Apply Recommended Actions (IT)

Applying or modifying recommended controls is done by the IT group. It is the job of the blue team to manage the IT group's activities, as detailed in the next step.

Assess and Propose Compensating Control Processes (Blue Team)

The job of the purple team is to recommend the actions needed, and then, in this step, verify that the action took place and was successfully implemented. This validation step is critical for any continuous improvement process.

When the results of the validation do not match the recommendation, is the cause is usually:

- Procedure was not completed.
- Procedure handoff issues or miscommunication.
- Implementation issues.

To avoid the first issue, the blue team's recommendations should have a firm deadline. For example, recommended patches to critical assets must be applied within 30 days and non-critical assets within 60 days.

Note: Until the deadline has passed, it is not clear whether the patch was not applied because of the deadline or there is an issue with the patch procedure. Once the deadline has passed, it is clear that the issue must be with the patch procedure. Therefore, it is critical to have a standard operating procedure to follow up regarding missed deadlines.

When validation fails, there needs to be a standard operating procedure for the blue team to have it flagged and handed back to the IT group. One option is to raise the severity level of the issue in the next iteration. In addition, the blue team should track issues that reoccur and use them to raise the overall risk metric for the organization. Another alternative is escalation.

Implementation issues might occur because a recommended control cannot be implemented. For example, not being to patch a server because of incompatibility with a critical application. That is when the blue team should recommend a temporary compensating control, which is essentially a workaround until the control can be applied. This type of remediation must be flagged and monitored carefully.

Harmony Purple in Action

In this section we will show how Harmony Purple uses its proprietary attack path scenario (APS) capabilities to create realistic attack scenarios that simulate how an attacker could breach your organization and compromise your enterprise's crown jewels. Just like a driving simulator, it checks out all possible scenarios, including those that are too dangerous, or too difficult, to perform in real life.

Harmony Purple's first phase is a scan to find weaknesses and vulnerabilities in your existing system by collecting information about your network topology, as well as system services, application services, configuration status, and device state. This is the step where weaknesses are collected and categorized into the type of adversarial tactic they support. Continuing with the driving metaphor, these are the stops and markers showing where an attacker can regroup and continue to the next step in their travels through your systems and applications.

Once this information has been collected, the next step is a purple team automated scan. Back to our driving metaphor, this scan finds the paths that can be used to get to the next stop– both the highways and the hidden back roads. This step requires credentials, otherwise these scenarios would miss paths, systems, and applications that attackers can find that are not visible to a black box scan (that is, attackers leveraging compromised credentials or multistage attackers).

Once complete, Harmony Purple's patented attack path scenario methodology provides a map of how attackers can leverage different types of weakness to both gain a foothold and silently traverse through your infrastructure looking for valuable data that can be exploited or processes that can be disrupted.

This unique APS capability breaks down the barriers among siloed approaches to cyber defense. It combines multiple types of weakness discovery into a holistic attack scenario and then suggests possible mitigations– exactly like a true purple team.

Attack Path Example

This scenario demonstrates how Harmony Purple creates an Attack Path Scenario to an enterprise's crown jewels.

- The "attack" starts when Harmony Purple finds a Local File Inclusion vulnerability (CAPEC-252: PHP Local File Inclusion) on a PHP application hosted on an Apache server (192.168.109.81).
- From this server, Harmony Purple uses standard protocols to scan the network in search of vulnerable hosts. As a result of the scanning, Harmony Purple finds a host (192.168.100.57)

vulnerable to SMB Vulnerability ms17-010 which was first described in 2017. The vulnerability on this device is on port 445 and there is a known, verified exploit.

- Harmony Purple then calculates that the CAPEC-252 File Inclusion penetration vulnerability can be linked to the SMB Vulnerability ms17-010 lateral movement vulnerability. The resulting insight is that 192.168.109.81 is a strong candidate for exploitation, which also makes it a good candidate for the start of an attack path scenario.
- Harmony Purple then continues by using 192.168.100.57 as its new foothold to move forward and continue to search for valuable targets in the network.
- From this foothold, Harmony Purple eventually finds a crown jewel in the form of a CRM server. Harmony Purple recognizes that the server's role is CRM.
- Harmony Purple then scans the CRM server for RCE Vulnerabilities and finds that the host is vulnerable to an RDP (remote desktop) vulnerability (cve-2019-0708). This vulnerability also has a known exploit.
- After successful exploitation of the vulnerability, the attack acquires the organization's confidential documents.

HOST: 192.168.109.81

- **Operating System**: Ubuntu 14.04 LTS
- **Role**: Web Server
- **Port**: 80
- **Service**: HTTPD
- **Web Server**: Apache/1.3
- **PHP Version**: 5
- **Vulnerability**: LFI Vulnerability in web application parameter (CAPEC 252) allows an attacker to read files from the underlying operating system. Using an Apache log file, the LFI technique the attacker employed was able to take over the operating system and get shell access.

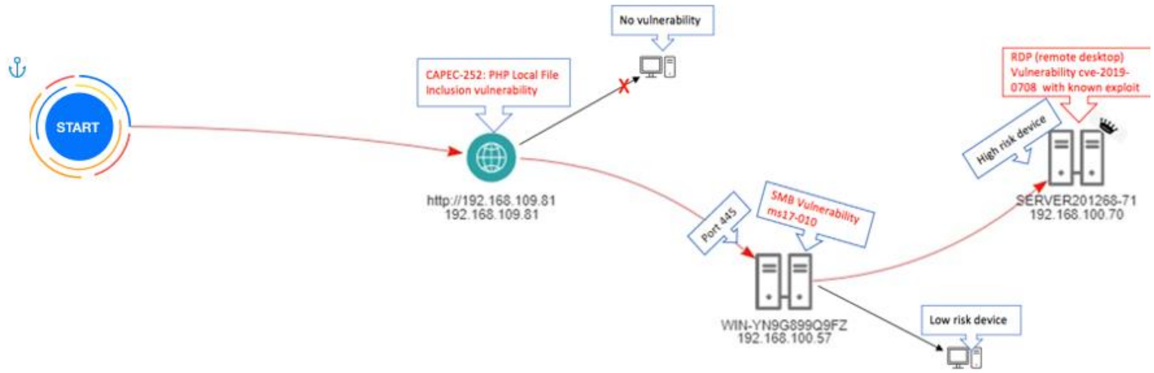
HOST: 192.168.100.57

- **Operating System**: Microsoft Windows server 2008
- **Role**: SQL Server
- **Port**: 445
- **Service**: SMB (NETBIOS-DS)
- **Vulnerability**: Vulnerability in SMB Block version 1.0 (MS-17-010) allows the attacker to gain full control of the host.

HOST: 192.168.100.70

- **Operating System**: Microsoft Windows Server 2008 SP2
- **Role**: CRM Server

- **Port**: 3389
- **Service**: RDP (MSTSC)
- **Vulnerability**: Vulnerability in RDP Service (CVE-2019-0708) allows the attacker to gain full control of the host.



Harmony Purple Remediation Recommendations

HOST 192.168.109.81:

- Do not allow a file patch to be appended directly by the user. Instead, create a selectable form with hard-coded path lists via an indexed variable, to prevent user-injected file paths.
- Do not allow unexpected characters to be added to the user supply input. If possible, allow only (A-Z-0-9) based characters.

HOST 192.168.100.57:

- Install Patch (KB 4012598) - https://support.microsoft.com/en-us/help/4012598/title

HOST 192.168.100.70:

- Install Patch (KB4499180) - https://support.microsoft.com/kb/4499180
- If necessary, a compensating control can be applied: virtual patch for Port: 3389 Service: RDP (MSTSC) (future capability).