


Why Penetration Testing Needs Continual Evolution: **Going Purple**

Adversaries continue to morph tactics and identify new ways of attacking organizations. The major methods of attack are predominantly through phishing, but the actual delivery system for the compromises is what becomes the hardest to detect. Regardless if it's a perimeter breach or a direct attack on the user population, it has never been more important to emulate attack patterns through the security industry. Penetration testing started off as a way for organizations to identify exposures and hopefully fix them before the attackers discover them.



The major methods of attack are predominantly through phishing, but the actual delivery system for the compromises is what becomes the hardest to detect.

As we've progressed as an industry, it has become apparent that there is so much attack surface for hackers that finding and fixing every vulnerability just isn't possible. This doesn't mean that we should stop identifying and fixing exposures as we find them, but what it means is that our layers of defense need to be designed in order to handle a flaw in our infrastructure or our users and respond appropriately. Penetration testing can absolutely help with this, but the focus needs to move further from traditional penetration testing and more towards performing overt testing in conjunction with the company undergoing the assessment.



This term is often called **"Purple Teaming"** which combines elements of the Blue Team (defense) and the Red Team (offense). By pairing the two groups together during every phase of the assessment, an understanding and knowledge transfer occurs in order to ensure that each phase can be appropriately tested for the three D's of security: Detect, Deflect, and Deter (3D). The concept of 3D breaks security controls into three criteria:



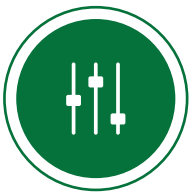
Detect

The overall detection capabilities of an organization and its ability to identify an attack in the early stages and through the lifecycle of a compromise.



Deflect

This is a traditional area of deflection such as anti-virus, intrusion prevention systems, or other methods that cause actual prevention for the organization.



Deter

This focuses on solid security practices such as patch management, network segmentation, password complexity, and other areas such as path of least resistance (honeypots).

In a 3D environment, baselining each of these and promoting growth through something such as a Purple Team engagement can have substantial areas of improvement on the overall security program and the 3D's. *Let's take an example:* during a traditional penetration test the monitoring and detection teams, as well as IT, are typically left in the dark and unaware of actual testing. Why this isn't as valuable for an organization is because the Red Team will typically perform the engagement, provide a list of findings, and from there walk away and wash their hands. Next year it's the same cycle - new exposures, new ways of exploitation, and always successful.

... in a Purple Team exercise, the objectives are still the identification of exposures, exploitation and post exploitation, ...

In a traditional assessment, the knowledge transfer that is happening is almost non-existent. The program, as far as the 3D criteria, is marginally increased and left in a state where it's back to firefighting mode. Instead, in a Purple Team exercise, the objectives are still the identification of exposures, exploitation, and post exploitation, but the engagement focuses on understanding what controls you have in place and where there may be gaps in 3D. The focus becomes less on the actual technical exposures and more on the attack patterns that were used and the level of coverage an organization has in handling the actual attack vectors.

Let's apply a Purple Team engagement to the 3D's and break down the phases of attack through the Penetration Testing Execution Standard (PTES)*:

Pre-Engagement Interaction

This phase should still focus on objectives such as trophies, understanding business objectives, and the overall success of the assessment. As part of this, understanding what type of 3D maturity levels are in place and the ability to understand what controls exist in a customer is helpful to the end deliverables of the engagement. This also helps on the success outcomes of the engagement.

Intelligence Gathering

In this area, it's one of the hardest to actually detect because it focuses heavily on open source intelligence gathering. However, as part of this phase, the communication of what information is exposed such as meta-data, personal information, and others can be used to improve the overall amount of information that is shared on the perimeter or through social media sites.

Threat Modeling

Through the threat modeling phase, working with the Blue Team on what controls are in place and effectively testing them is important. When building the threat model on an organization, understanding the tactics, techniques, and procedures (TTPs) of adversaries for simulation is important as well as building the threat model on what you know from the organization. Our goal is to bypass the controls in place, but also to test what current controls are in place and ensure that they are effective and working as intended.



Vulnerability Analysis

This phase focuses on understanding what exposures there are for the organization and applying the attack vectors to either ensure they are working appropriately or circumvent the controls in place. This can be obtained through performing more covert testing of controls, but in a Purple Team situation this could be something to the effect of actually testing the technical controls on an already compromised system or attempting to compromise a test laptop. You can still perform social-engineering/phishing efforts on the organization, but the primary goal is to work through multiple phases of the attack and focus on the identification of gaps in the D's.



Exploitation

This is an important phase for detection and early warning indicators. If you can detect the actual exploitation techniques used such as initial compromise methods (was it through a Java Applet, HTAs, or other avenues), is it possible to actually detect that method? Is it possible to improve or circumvent the controls and build better detection?



Post Exploitation

This phase by far has so many different components in it that it is literally the most important phase for detection criteria. What if your deterrence controls fail and the attacks are now establishing a command and control and have full access to the network behind the perimeter? At this point, the detection that needs to occur through these phases is more than critical; it's the ability to detect an attack or undergo several months of unnoticed breaches with massive amounts of exfiltration. In this phase, everything from persistence hooks, privilege escalation, lateral movement, further compromises, and more should all be a part of what is tested to ensure that it is working appropriately. We can't emphasize the importance of spending a bulk amount of time during a Purple Team engagement on these phases. The attack surface is so large, and attackers are extremely good at this phase regardless of the sophistication levels of the adversary.




Reporting

The reporting phase should focus on the technical exposures identified, but most importantly, how to improve on the Detect, Deflect, and Deter phases. Reports that solely focus on just the technical flaws fall right back into the cyclical effect of not promoting maturity in the information security program. Focusing on how to get better at the 3D's has to be the most important phase of the assessment.

How to track progress can also be difficult in most organizations. One of the early concepts around how to rank the 3D system was through the concept of a balanced scorecard. A good talk on this from BruCon called **“Building a Successful Internal Adversarial Simulation Team”** from Chris Gates and Chris Nickerson can be found here: <http://bit.ly/2sRGOW3>. The balanced scorecard concept is a living, breathing program that doesn't just focus on a once a year Purple Team engagement. It's how the 3D's are tracked through the organization and the level of confidence of the 3D's in the company.

Regardless of your maturity level in your company, the Purple Team exercise is one that has more than just finite benefits around technical exposures.

An amazing resource for a template on balanced scorecards can be found from Binary Defense's (sister company to TrustedSec) Mick Douglas here: <http://bit.ly/2toKXXM>. In Mick's balanced scorecard, each phase of an attack – everything from exploitation to post exploitation scenarios – is broken down and tracked based on the level of maturity in each of the organizations. The balanced scorecard approach can drastically improve the visibility you have into your maturity model in the organization as well as show the progress and return on specific investments, technology, or people.



Regardless of the terminology or what is being used, the Purple Team concept can be applied to each of these based on the level of maturity of the organization.

Regardless of your maturity level in your company, the Purple Team exercise is one that has more than just finite benefits around technical exposures. It promotes a healthy security program within the company and continues to move your 3D's to a much more mature state.

This industry has a number of acronyms, everything from penetration testing, Red Teaming, adversary simulation, threat emulation, and more. Regardless of the terminology or what is being used, the Purple Team concept can be applied to each of these based on the level of maturity of the organization. Regardless if your 3D's are at a starting point, or to some of the most sophisticated attacks out there, TrustedSec can help build your security program over time with some of the best resources in the industry.

Reach out to TrustedSec today to learn more about Purple Team exercises, deployment, and management.

www.trustedsec.com