CRACKING THE PERIMETER – FRAMEWORK 1.0

Summary

1 - What is?

Cracking The Perimeter focuses on developing sophisticated attack vectors and methods to test a security control or solution. In addition to the CTP professional testing 0days and looking for vulnerabilities in a product and putting proof of concepts into practice, going deeper, that is, going beyond traditional penetration testing.

The professional responsible for this task he is not just a PenTester, after all a penetration test he focuses a lot on pre-commitment, giving an attack surface from the outside to the inside.

Adversary Emulation, on the other hand, goes beyond PenTest, focusing more on post-commitment and testing internal security controls, raising TTPs (Tactics, Techniques and Procedures) based on Miter Att&ck, in order to test the effectiveness of security controls, such as the SOC team is committed and the response to any incident.

Where does Cracking The Perimeter come in?

It enters precisely in the Adversary Emulation post, being a new type of process that a Red Team Operations can invest. After all, the purpose of Cracking The Perimeter is to be a process that encompasses 3 processes and acts as a Purple Team in certain cases:

1. The process of surveying information security controls: Check which controls are implemented, what solutions are being used within the organization you work for and who operates?
2. The test environment research and development process: After raising the solutions and controls used, setting up a test laboratory is essential so that the professional can explore the solutions and search for 0days, TTPs and even develop their own techniques or find Security loopholes that can be useful for creating hidden IoCs, meaning threats that don't yet exist.
3. The process of remediation and treatment of risks and vulnerabilities: A key part is to put the Blue Team team in general, together with the other part of the Red Team to validate alternatives and create a risk matrix and follow-up of a CVE that could end up making it an attack vector, a TTP, a 0day and even a vulnerability found by the professional CTP (Cracking The Perimeter). At certain times it will be necessary to involve both suppliers and partners to solve the problem;

2 - What I Gain From Cracking The Perimeter Process?

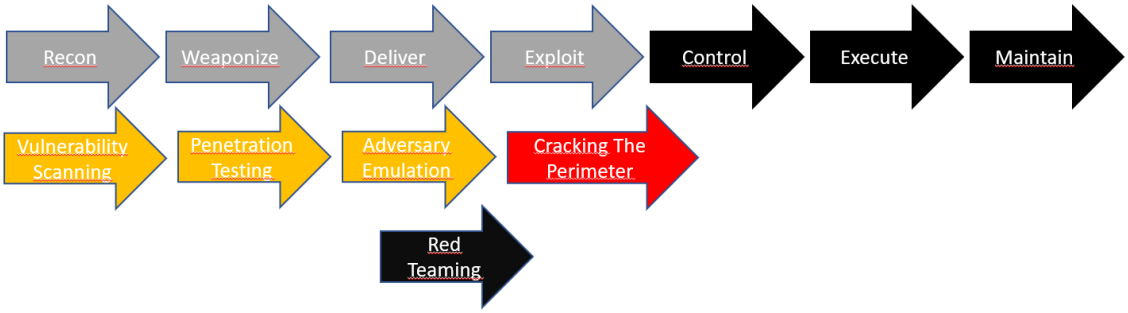
The benefits of a CTP process are incalculable, after all, it is an ongoing process within your company, as new threats emerge every day, so having someone with the ability to create these threats and validate the damage that such a threat could cause to your environment, it's already a great job. In other words, working in a preventive way, it is also a process that involves both pre-commitment and post-commitment, and tests aimed at Phishing and other campaigns carried out within the company. A CTP he works with research and delve into the technologies that the company uses, in order to find security breaches. Some companies work this way, creating their own testing labs and finding and registering CVE's,

An example scenario:

Imagine that your company only uses Microsoft technologies on your network, so what are the serious vulnerabilities that the environment has? Vulnerability analysis can get that back to you, and PenTest comes in to materialize lab results and Adversary Emulation to help improve internal and external perimeters. But CTP goes much further, it takes this whole process and continuously tests new techniques and experiments, whether in a controlled environment or even in production, depending on the impact that the tests are made. So it's being a research point, working with the intelligence team and with their knowledge, trying to find ways to circumvent the company's defense mechanisms, whether logical and virtual or even physical.

3 - What is the knowledge of CTP?

A CTP he has knowledge that gives him the opportunity to develop new attack vectors, create exploits, improve existing techniques to bypass defense controls and the like. And for that, it's hardly a knowledge you can get overnight, as its name refers to the OSCE certification course, obviously the professional needs to have a very large know-how in Buffer Overflow, Binary Exploration, Engineering Reverse, Malware Analysis, Programming Skills and being a good Information Security Architect. All this knowledge does not mean that it can be just an individual, but a team focused only on that, an arm of Red Team or even Purple Team, after all, the professional needs to know about security operations and defense mechanisms.



4 - Role of solution providers and partners

The role of solution providers and partners is crucial within this process and measures need to be taken so that ISO 29147 is implemented and not only linked to bug reward programs, ensuring compliance and positivity of suppliers when receiving any vulnerability or even a report or proof of concept with some TTP that involves your technology as an attack vector or opening vector for a malicious individual.

ISO/IEC 29147:2018

This document provides requirements and recommendations for vendors on the disclosure of vulnerabilities in products and services. Vulnerability disclosure enables users to perform technical vulnerability management as specified in ISO/IEC 27002:2013, 12.6.1[1]. Vulnerability disclosure helps users protect their systems and data, prioritize defensive investments, and better assess risk. The goal of vulnerability disclosure is to reduce the risk associated with exploiting vulnerabilities. Coordinated vulnerability disclosure is especially important when multiple vendors are affected. This document provides:

— guidelines on receiving reports about potential vulnerabilities;

— guidelines on disclosing vulnerability remediation information;

— terms and definitions that are specific to vulnerability disclosure;

— an overview of vulnerability disclosure concepts;

— techniques and policy considerations for vulnerability disclosure;

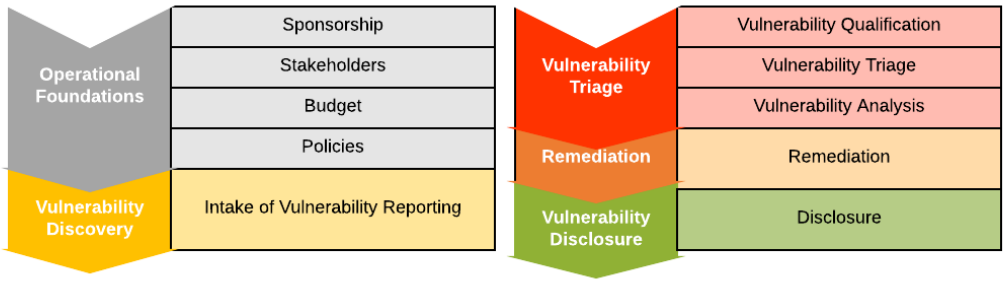
— examples of techniques, policies (Annex A), and communications (Annex B).

Other related activities that take place between receiving and disclosing vulnerability reports are described in ISO/IEC 30111.

This document is applicable to vendors who choose to practice vulnerability disclosure to reduce risk to users of vendors' products and services.

5 - What are the action plans involved in CTP?

According to ISO 30111, this document helps provide requirements and recommendations on how to remediate and prevent some unknown threat, working with the concept of obscurity and developing IoCs and preventive methods to ensure that an exploit or even a TTP is not effective or does not have as much impact, until it does. a total remediation plan, such as security patches or even improving security control itself. This within a PSIRT (Product Security Incident Response Team) plan



https://www.first.org/standards/frameworks/psirts/psirt_maturity_document

That helps in the resolution of vulnerabilities and helps Blue Team and CSIRT in the continuous monitoring and in the treatment and response to any incident involving a certain vulnerability.

6 - Where does Blue Team work?

Blue Team acts as a left arm of CTP, you can specify a team responsible for fulfilling requests from CTP Research to change or change some configuration, in addition to testing the effectiveness of the implemented controls. As good Patch Management practices, a lab environment is always better to test if the patch is 100% effective or not, after all gaps are always left by manufacturers or even specialists involved in Blue Team.

Therefore, the CTP has to be well structured and within the Processes, People and Technologies, and aligned with the business needs.

7 - Open Source vs Proprietary Software in the CTP Process

A question that maybe many will ask is regarding how to implement a process in a company that uses a lot of Open Source software or maybe a high priority. That's why before hiring a solution, you talk to the software manufacturer regarding PSIRT and CTP processes, that's why I ask companies to start evaluating the bugs that are found internally and considering them.

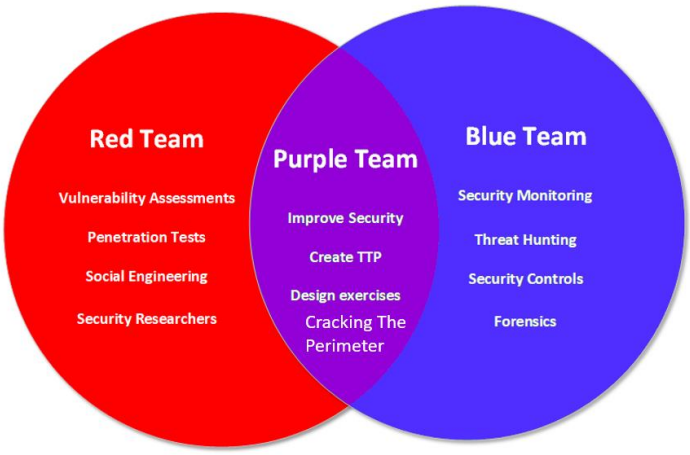
In the case of open source solutions, there is either the community behind that project or a responsible company, but when analyzing an Open Source application, CTP Research has to separate components, libraries and plugins that the software uses, from its main source code, or that is, wondering if the fault is in the code or is it in the components that that code uses to function? There comes the concept of SCA that CTP Research can work together with the Red Team team and the software owner to work with the fix. If the project is on a code hosting platform like Github or Gitlab, a Pull Request can be useful.

In proprietary software, there is a conversation between the customer and the supplier to manage this CTP process within your organization.

8 - Red Team's role in CTP?

CTP he becomes a right hand man of the Red Team, while the focus is PenTest, Vulnerabilities Management, Application Security, Code Review, Adversary Emulation. The CTP comes as an addition within the Red Team framework and is part of the entire cycle. Like this? In a vulnerability analysis it may return a false positive, but can that false positive turn into a false negative? Nothing a CTP Research can unfortunately end up making this happen. Let's remember that attackers don't just use ready-made tools or public exploits, but develop as well and that's why CTP Research should always work with a well-known phrase: “No system is secure” It's that thing, if the house looks clean, see what's under the rug.

The role of CTP within Red Team is fundamental, but it is not 100% a process exclusive to Red Team, so it can be framed within Purple Team as a process that ensures that both parties, such as Blue and Red Team, work from effectively.



https://www.sqa-consulting.com/infosec-colour-team-structure-the-purple-team/

9 - What tools does CTP Research use?

Let's consider that CTP Research itself is the tool, after all it can use from an nmap and metasploit or even a cobalt strike to create TTPs, or use debuggers to find points of vulnerabilities in some application and develop its exploit.

Think that there are numerous CVE's without any PoC, they are just there and this ends up making organizations worried, because a critical vulnerability without PoC is something that must be monitored, but how can it be exploited there is the secret, that's why CTP Research he tries to simulate an attack or together with the intelligence team, go after 0days through the exploit markets.

Cyber intelligence is critical, having a collaborative platform like MISP can help with many practical processes to simulate an attack or create a proof of concept based on a CVE.

10 - Bug Bounty vs CTP: what's the difference

The Bug Bounty is one of the activities that has been gaining more and more strength in recent times, being a millionaire and profitable market. And today companies understand the need to have a reward program to ensure the security of their applications, after all, a half-yearly PenTest is not a “good practice”. However, confusing a CTP with a Bug Bounty is easy for some, but the activities are totally different, as while one is a program within an organization, I can use a security awareness program as an example. The other is a process within the area of information security, a process that involves both the organization and its partners and service providers.

While the Bug Bounty limits itself to finding vulnerabilities within a closed scope, and reporting to the company that owns the reward program. CTP is not just about finding vulnerabilities, but giving an overview of the environment, literally breaking security controls to enforce them, and working with the management of patches, risks and vulnerabilities within an organization.

11 - What are CTP's tasks?

The CTP has numerous tasks and I will make a point of presenting them, but it is worth mentioning that it is a framework that is constantly being improved and worked on.

- Develop laboratories to test the security of solutions and technologies, which will be implemented in an environment;
- Help in the development of a CSIRT and PSIRT;
- Monitor Red Team activities, both in vulnerability analysis, vulnerability management, PenTest and Adversary Emulation;
- Complementing item 3, perform and assist in the Adversary Emulation process;
- Work with the Threat Intelligence team to gather information about threats, TTPs and collect information from a CVE or 0days exploits;
- Test the implemented security controls, developing methods to circumvent a protection mechanism and explore the internal environment;
- Create exploits and tools based on PoC's and CVE's information;
- Help in creating indicators based on obscurity and testing the effectiveness of alerts created;
- Validate the secure development cycle and analyze an application's code for vulnerabilities;
- Test security solutions manually, creating TTPs and validating whether there is any reactive action or not;

- Raise the external risks and test them to obtain an effective result, whether working with information gathering and advanced recognition techniques;

12 - What if I am a solutions provider?

A software factory, a provider of cybersecurity and related solutions, can create its own CTP process or work together with its customers to always ensure security and constant improvement. In addition to being a form of research to create indicators on attacks in specific environments in specific types of businesses and the like. If you have a software factory, secure development is critical, and having a professional who literally breaks your application is even more critical to ensuring a continuous security cycle.

13 - How to Implement the Cracking The Perimeter Program?

Implementing a program within your Red Team is not easy, as it requires a relative degree of maturity and a well-structured area, as a CTP Research, in addition to needing a well-structured security environment, needs laboratories and resources to work, after all it's no use investing in training and training a professional to work in this part if you don't have anything properly structured, not even vulnerability management.

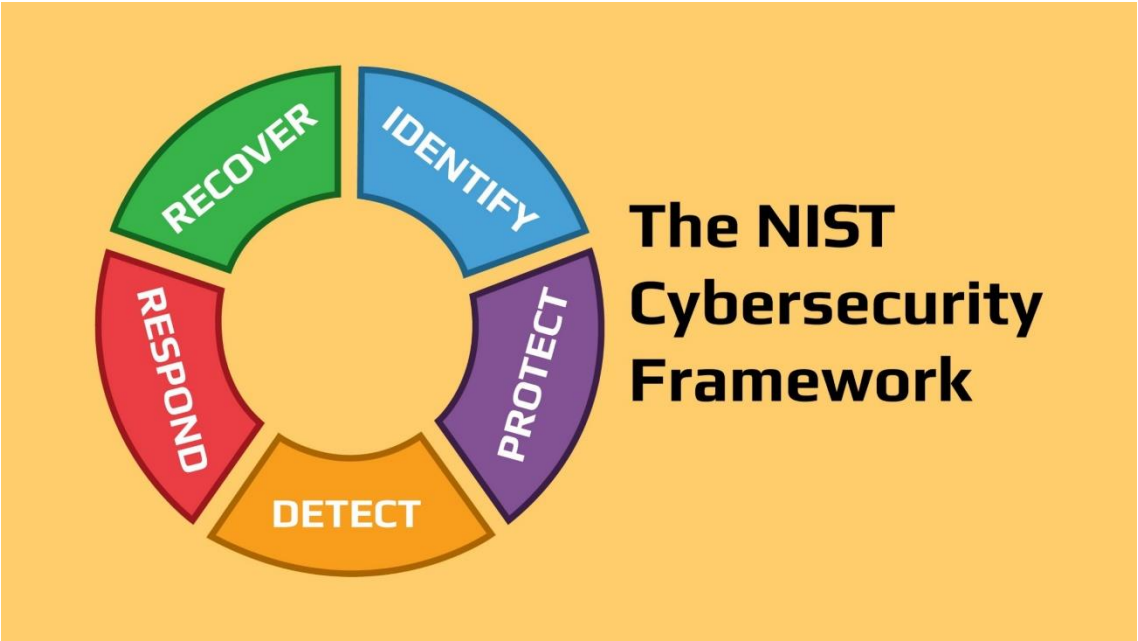
Then the process begins, just like Adversary Emulation, when your company or your customer has a relative maturity in security. Mainly well-defined solutions and highly configured security controls, in addition to good internal security practices.

13.1 What should a CTP professional know?

If you intend to invest in people, or hire someone specialized, the main factor is the degree of knowledge they have in current technologies, whether Cloud, Mobile, Microservices, security solutions and their knowledge of Blue and Red Team. In addition, it is obvious that the professional must know about exploit development, as it is one of the crucial factors for an organization to have professionals who have experience. And of course a highly skilled Red Team professional, especially knowing about threats such as Miter Att&ck and Cyber Kill Chain.

14 – Frameworks and Standards

Let's get to know the Frameworks and standards that involve CTP?



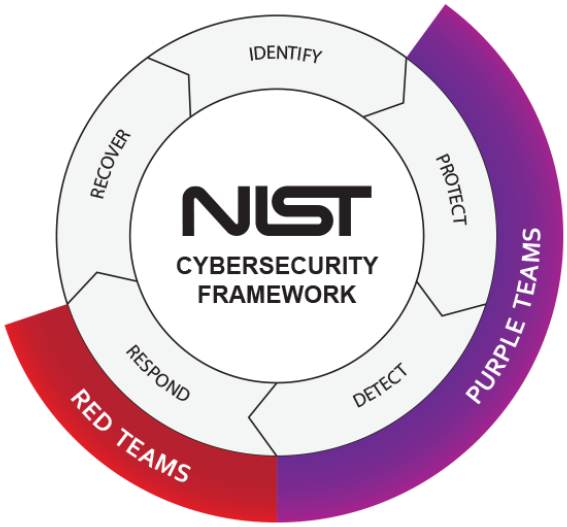
PENETRATION TESTING EXECUTION STANDARD
PTES
Technical Guidelines

Open Source Security Testing Methodology Manual
OSSTMM
www.osstmm.org

OWASP®

ISO

MITRE | ATT&CK™



15 – Conclusion

In summary this is the first version of the CTP Framework, it is an idea based on other frameworks and industry standards, to be a process that adds continuous security against advanced persistent threats (APTs).

If you want to implement this Framework or know in more detail and even want to contribute. Get in touch with me through one of these means of communication:

Email: joasantonio108@gmail.com

LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos

Twitter: https://twitter.com/C0d3Cr4zy

More project details: https://github.com/CyberSecurityUP/Cracking-The-Perimeter-Framework