CRACKING THE PERIMETER – FRAMEWORK 1.0

Sumário

1 - What is?

O Cracking The Perimeter se concentra no desenvolvimento de métodos e vetores de ataques sofisticados para testar um controle ou solução de segurança. Além do profissional CTP testar

0days e procurar pontos de vulnerabilidades em algum produto e colocar provas de conceitos em prática, indo numa camada mais profunda, ou seja, indo além dos testes de invasão tradicional.

O profissional responsável por essa tarefa ele não é apenas um PenTester, afinal um teste de invasão ele foca muito no pré-comprometimento, dando uma superfície de ataques de fora para dentro.

Já o Adversary Emulation, ele vai além do PenTest, focando mais no pós-comprometimento e testando os controles de seguranças internos, levantando TTPs (Táticas, Técnicas e Procedimentos) baseado no Mitre Att&ck, afim de testar a eficácia dos controles de segurança, como a equipe de SOC está comprometida e a resposta a algum incidente.

Where does Cracking The Perimeter come in?

Ele entra justamente nos pós Adversary Emulation, sendo um novo tipo de processo que um Red Team Operations pode investir. Afinal o objetivo do Cracking The Perimeter é ser um processo que engloba 3 processos e atua como um Purple Team em determinados casos:

1) O processo de levantamento dos controles de seguranças da informação: Verificar quais controles são implementados, que soluções estão sendo utilizados dentro da organização que você trabalha e quem opera?
2) O processo de pesquisas e desenvolvimento de ambiente de testes: Após levantar as soluções e os controles usados, montar um laboratório de teste é essencial para que o profissional possa explorar as soluções e pesquisar por 0days, TTPs e até mesmo desenvolver suas próprias técnicas ou encontrando brechas de segurança que pode ser útil para criar IoCs ocultos, ou seja, de ameaças que ainda não existem.
3) O processo de remediação e tratamento dos riscos e vulnerabilidades: Uma parte fundamental é colocar o time de Blue Team no geral, junto com a outra parte do Red Team para validar alternativas e criar uma matriz de risco e acompanhamento de uma CVE que pode acabar se tornando um vetor de ataque, de um TTP, de um 0day e até mesmo de uma vulnerabilidade encontrada pelo próprio profissional CTP (Cracking The Perimeter). Em determinados momentos será necessário envolver tanto fornecedores como parceiros para a resolução do problema;

2 - What I Gain From Cracking The Perimeter Process?

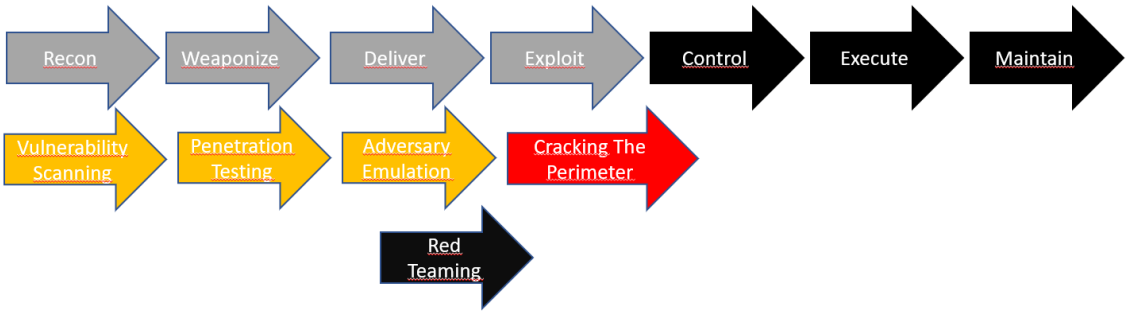
Os benefícios de um processo de CTP é incalculável, afinal ele é um processo continuo dentro da sua empresa, pois a cada dia novas ameaças surgem, então ter alguém com a capacidade de criar essas ameaças e validar os danos que uma ameaça do tipo poderia ocasionar ao seu ambiente, já é um trabalho ótimo. Ou seja, trabalhando de uma forma preventiva, além disso é um processo que envolve tanto o pré-comprometimento como o pós-comprometimento, e testes voltados a Phishing e outras campanhas realizados dentro da empresa. Um CTP ele trabalha com a pesquisa e se aprofunda nas tecnologias que a empresa utiliza, afim de encontrar brechas de segurança. Algumas empresas trabalham dessa forma, criando seus próprios laboratórios de testes e encontrando e registrando CVE's, contudo o CTP ele vem como uma força tarefa dentro da organização e busca de alguma forma contornar algum EDR, Antivírus, Firewall, IDS, IPS, atingir as aplicações que a empresa utiliza e encontrar uma vulnerabilidade ou pegar provas de conceitos existentes e por em prática.

Um exemplo de cenário:

Imagine que sua empresa utilize somente na sua rede, tecnologias Microsoft, então quais são as vulnerabilidades graves que o ambiente tem? A analise de vulnerabilidade pode te retornar isso, e o PenTest entra para concretizar os resultados do laboratório e o Adversary Emulation para ajudar no aprimoramento dos perímetros internos e externos. Porém o CTP ele vai muito mais além, ele pega todo esse processo e de maneira continua testa novas técnicas e experimenta, seja em um ambiente controlado ou até mesmo no de produção, dependendo do impacto que os testes são feitos. Então é ser um ponto de pesquisas, trabalhando com a equipe de inteligência e com seu conhecimento tentar formas de burlar os mecanismos de defesas da empresa, sejam eles lógicos e virtuais ou até mesmo físicos.

3 - What is the knowledge of a CTP?

Um CTP ele tem conhecimentos que dá a oportunidade de ele desenvolver novos vetores de ataques, criar exploits, aprimorar técnicas existentes para bypassar controles de defesas e afins. E para isso dificilmente é um conhecimento que você consegue obter do dia para noite, pois como próprio nome se referência ao curso da certificação OSCE, obviamente que o profissional ele precisa ter um know-how bem grande em Buffer Overflow, Exploração de Binários, Engenharia Reversa, Análise de Malware, Habilidades com Programação e ser um bom Arquiteto de Segurança da Informação. Todo esse conhecimento não significa que pode ser apenas de um indivíduo, mas sim de uma equipe focada apenas nisso, um braço do Red Team ou até mesmo do Purple Team, afinal o profissional precisa conhecer das operações de segurança e mecanismos de defesas.



4 - Role of solution providers and partners

O Papel dos provedores de soluções e parceiros, é crucial dentro desse processo e precisa ser tomado medidas para que a ISO 29147, seja implementado e não só atrelado a programas de recompensa de bugs, garantindo o compliance e a positividade dos fornecedores ao receber alguma vulnerabilidade ou até mesmo um relatório ou prova de conceito com algum TTP que envolva sua tecnologia como vetor de ataque ou vetor de abertura para um indivíduo malicioso.

ISO/IEC 29147:2018

This document provides requirements and recommendations to 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;

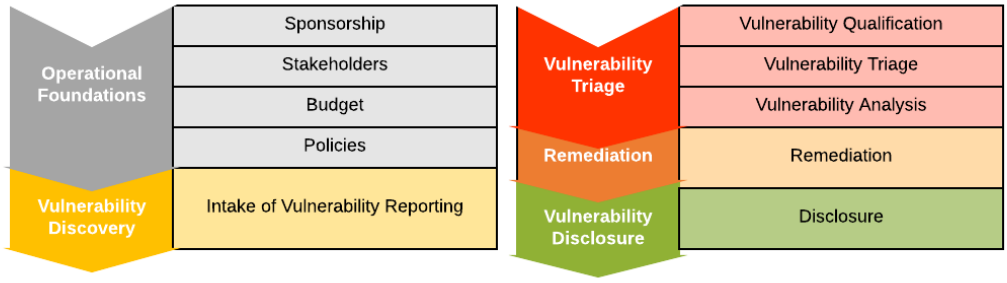
— examples of techniques, policies (Annex A), and communications (Annex B).

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?

Conforme a ISO 30111, este documento ajuda a fornecer requisitos e recomendações sobre como remediar e prevenir alguma ameaça desconhecida, trabalhando com conceito de obscuridade e desenvolvendo IoCs e métodos preventivos para garantir que um exploit ou até mesmo um TTP não seja efetivo ou não tenha tanto impacto, até ter um plano de correção total, como os patches de seguranças ou até mesmo a melhoria do próprio controle de segurança. Isso dentro de um plano de PSIRT (Product Security Incident Response Team)



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

Que ajuda na resolução de vulnerabilidades e auxilia o Blue Team e o CSIRT no monitoramento contínuo e no tratamento e resposta a algum incidente envolvendo uma determinada vulnerabilidade.

6 - Where does Blue Team work?

O Blue Team atua como um braço esquerdo do CTP, você pode especificar uma equipe responsável por atender as solicitações do CTP Research para alterar ou mudar alguma configuração, além de testar a efetividade dos controles implementados. Como boas práticas de Gerenciamento de Patches, um ambiente de laboratório é sempre melhor para testar se a correção é 100% efetiva ou não, afinal lacunas sempre são deixadas pelos fabricantes ou até mesmo dos especialistas envolvidos no Blue Team.

Por isso o CTP tem que estar bem estruturado e dentro dos Processos, Pessoas e Tecnologias, e alinhados com a necessidade do negócio.

7 - Open Source vs Proprietary Software in the CTP Process

Uma pergunta que talvez muitos vão fazer é referente a como implantar um processo em uma empresa que usa muitos softwares Open Source ou talvez totalmente prioritário. E para isso que antes de contratar uma solução, você conversar com o fabricante do software referente a processos de PSIRT e CTP, por isso peço que as empresas comecem a avaliar os bugs que são encontrados internamente e a considerá-los.

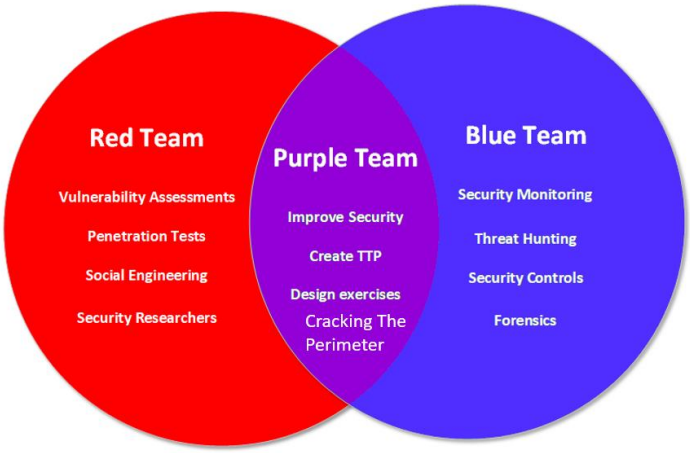
No caso de soluções open source, existe tanto a comunidade por trás daquele projeto ou uma empresa responsável, mas ao analisar uma aplicação Open Source o CTP Research tem que separar componentes, bibliotecas e plugins que o software utiliza, do seu código fonte principal, ou seja, se perguntar se a falha é no código ou é nos componentes que aquele código utiliza para funcionar? Ai entra o conceito de SCA que o CTP Research pode trabalhar junto com a equipe de Red Team e o detentor do software para trabalhar com a correção. Caso o projeto esteja em uma plataforma de hospedagem de código como Github ou Gitlab, um Pull Request pode ser útil.

Em um software proprietário, cabe uma conversa entre o cliente e o fornecedor para gerenciar esse processo de CTP dentro da sua organização.

8 - Red Team's role in CTP?

O CTP ele se torna um braço direito do Red Team, enquanto o foco é PenTest, Gerenciar Vulnerabilidades, Segurança de Aplicação, Revisão de Código, Adversary Emulation. O CTP ele entra como um acréscimo dentro do quadro de Red Team e fazendo parte de todo o ciclo. Como assim? Em uma analise de vulnerabilidade pode ser que retorne um falso positivo, mas será que aquele falso positivo pode se tornar um falso negativo? Nada que um CTP Research pode acabar por infelizmente fazendo isso acontecer. Vamos nos lembrar que os atacantes eles não utilizam só ferramentas prontas ou exploits públicos, mas desenvolvem também e é por isso que o CTP Research ele deve sempre trabalhar com uma frase bem conhecida: “Nenhum sistema é seguro” É aquela coisa, se a casa aparenta estar limpa, veja o que tem embaixo do tapete.

O papel do CTP dentro do Red Team é fundamental, mas ele não é 100% um processo exclusivo do Red Team, por isso pode ser enquadrado dentro do Purple Team como um processo que garante que ambas as partes, como Blue e Red Team trabalhem de forma efetiva.



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

9 - What tools does a CTP Research use?

Vamos considerar que o próprio CTP Research é a ferramenta, afinal ele pode usar desde um nmap e metasploit ou até mesmo um cobalt strike para criar TTPs, ou usar debuggers para encontrar pontos de vulnerabilidades em alguma aplicação e desenvolver seu exploit.

Pense que existem inúmeras CVE's sem nenhuma PoC, apenas estão lá e isso acaba deixando as organizações preocupadas, pois uma vulnerabilidade crítica sem PoC é algo que deve ser monitorado, porém como ela pode ser explorada ai que ta o segredo, por isso o CTP Research ele tenta simular um ataque ou junto com a equipe de inteligência, ir atrás de 0days pelos mercados de exploits.

A inteligência cibernética é fundamental, ter uma plataforma colaborativa como MISP pode ajudar em muitos processos práticos para simular um ataque ou criar uma prova de conceito baseada em uma CVE.

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

O Bug Bounty é uma das atividades que vem ganhando cada vez mais força nos últimos tempos, sendo um mercado milionário e lucrativo. E hoje as empresas entendem a necessidade de ter um programa de recompensa para garantir a segurança das suas aplicações, afinal um PenTest semestral não está sendo uma "boa prática". Porém confundir um CTP com Bug Bounty é fácil para alguns, mas as atividades são totalmente diferentes, pois enquanto um é um programa dentro de uma organização, posso colocar como exemplo um programa de conscientização de segurança. O outro é um processo dentro da área de segurança da informação, um processo que envolve tanto a organização como seus parceiros e provedores de serviços.

Enquanto o Bug Bounty se delimita a encontrar vulnerabilidade dentro de um escopo fechado, e reportar para a empresa detentora do programa de recompensa. O CTP ele não está apenas

para encontrar vulnerabilidades, mas dar uma visão geral do ambiente, quebrar literalmente os controles de segurança para reforçá-los e trabalhar com a gestão de patches, riscos e vulnerabilidades dentro de uma organização.

11 - What are CTP's tasks?

O CTP ele tem inúmeras tarefas e farei questão de apresentá-las, mas vale ressaltar que é um framework que está sendo aprimorado e trabalhado constantemente.

- Desenvolver laboratórios para testar a segurança de soluções e tecnologias, que vão ser implementados em um ambiente;
- Ajudar no desenvolvimento de um CSIRT e PSIRT;
- Acompanhar as atividades de Red Team, tanto em análises de vulnerabilidades, gestão de vulnerabilidades, PenTest e Adversary Emulation;
- Complementando o 3 item, realizar e auxiliar no processo de Adversary Emulation;
- Trabalhar com a equipe de Threat Intelligence para coletar informações sobre ameaças, TTPs e coletar informações de uma CVE ou exploits 0days;
- Testar os controles de segurança implementados, desenvolvendo métodos para contornar um mecanismo de proteção e explorar o ambiente interno;
- Criar exploits e ferramentas com base em PoC's e informações de CVE's;
- Ajudar na criação de indicadores baseado em obscuridade e testando a efetividade dos alertas criados;
- Validar o ciclo de desenvolvimento seguro e analisar o código de uma aplicação atrás de vulnerabilidades;
- Testar soluções de segurança manualmente, criando TTPs e validar se existe alguma ação reativa ou não;
- Levantar os riscos externos e testa-los para obter um resultado efetivo, seja trabalhando com a coleta de informação e técnicas de reconhecimento avançado;

12 - What if I am a solutions provider?

Uma fábrica de software, um provedor de soluções de cibersegurança e afins, pode criar seu próprio processo de CTP ou trabalhar em conjunto com os seus clientes, para garantir sempre a segurança e aprimoramento constante. Além de ser uma forma de pesquisas para criar indicadores sobre ataques em ambientes específicos em tipos de negócios específicos e afins. Se você tem um fábrica de software, o desenvolvimento seguro é fundamental, e ter um profissional que literalmente quebre sua aplicação é mais fundamental ainda para garantir um ciclo continuo de segurança.

13 - How to Implement a Cracking The Perimeter Program?

Implementar um programa dentro do seu Red Team não é fácil, pois requer um grau de maturidade relativo e uma área bem estruturada, pois um CTP Research além de necessitar de um ambiente de segurança bem estruturado, ele precisa de laboratórios e recursos para trabalhar, afinal não adianta investir em treinamentos e capacitar um profissional para atuar nessa parte se não tem nada estruturado corretamente, nem mesmo uma gestão de vulnerabilidades.

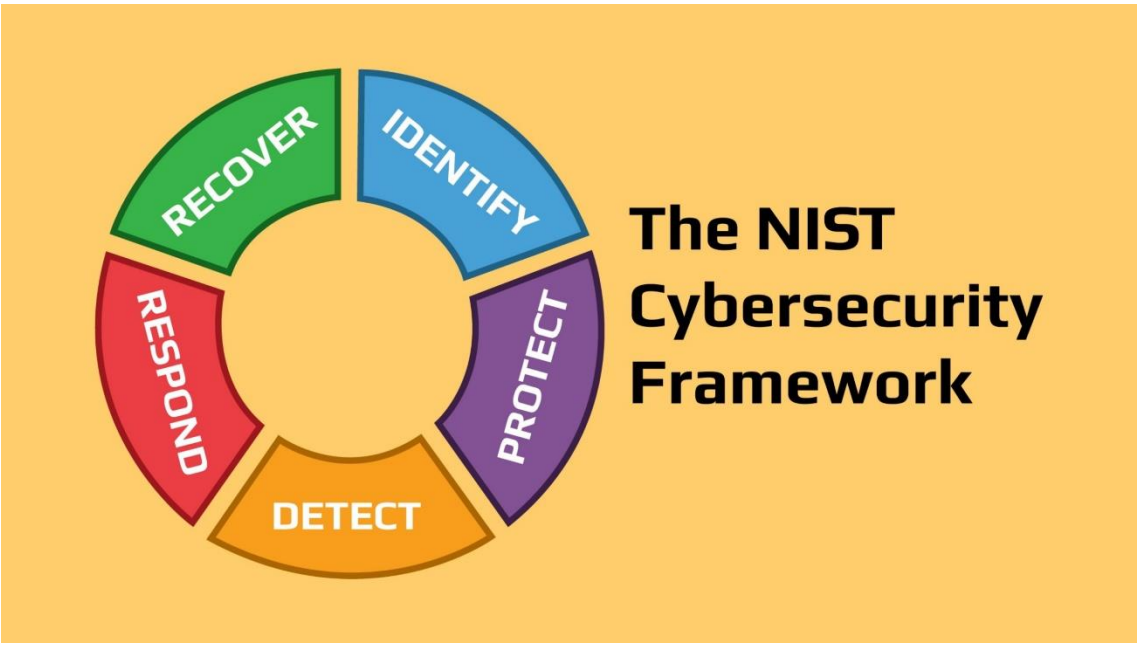
Então o processo começa, assim como Adversary Emulation, quando a sua empresa ou seu cliente tenha uma maturidade relativa em segurança. Principalmente as soluções bem definidas e controles de segurança altamente configurados, além das boas práticas de segurança interna.

13.1 What should a CTP professional know?

Se você pretende investir em pessoas, ou contratar alguém especializado, o fator principal é o grau de conhecimento que ele tem em tecnologias atuais, seja Cloud, Mobile, Microsserviços, soluções de segurança e seu conhecimento com Blue e Red Team. Além disso, é óbvio que o profissional deve conhecer de desenvolvimento de exploits, pois é um dos fatores cruciais para dentro de uma organização, ter profissionais que tenham experiência. E claro um profissional altamente capacitado em Red Team, principalmente conhecer de ameaças como o Mitre Att&ck e o Cyber Kill Chain.

14 – Frameworks and Standards

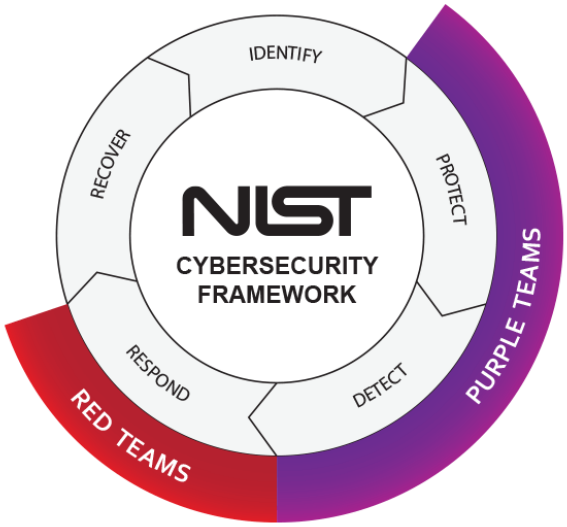
Vamos conhecer os Frameworks e padrões que envolvem o CTP?




ISO


Abnormal DNS reverse lookup requests
Brute Force Attack
Activity from blacklisted geolocations
Failed privilege escalation detected
A dormant service account was reactivated
Unusual number of messages marked as unread
Unusual number of GDPR files deleted
Unusual amount of data uploaded to external websites
VARONIS
CYBER KILL CHAIN


MITRE
ATT&CK™



15 – Conclusion

Em resumo essa é a primeira versão do Framework CTP, é uma ideia baseada em outros frameworks e padrões de mercado, para ser um processo que acrescente a segurança continua contra ameaças persistentes avançadas (APTs).

Caso tenha desejo de implementar esse Framework ou saber em mais detalhes e até mesmo querer contribuir. Entre em contato comigo, por um desses meios de comunicação:

E-mail: joasantonio108@gmail.com

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

Twitter: https://twitter.com/C0d3Cr4zy

Mais detalhes do projeto: https://github.com/CyberSecurityUP/Cracking-The-Perimeter-Framework