LUNDI DE LA CYBERSÉCURITÉ

ORGANISATION D'UNE PURPLE TEAM : OPTIMISATION DES TESTS D'INTRUSION ET MISE EN PLACE DE PLANS DE REMÉDIATION

PRÉSENTÉE PAR : SABINE PIROU

LUNDI 18 MAI 2026

1

SOMMAIRE

1. Présentation d'un test d'intrusion « classique »
2. L'apport d'une Purple Teams à un test d'intrusion
3. La Purple Team au l'aube des réglementations NIS 2 & DORA

2

PARTIE 1

PRÉSENTATION DU TEST D'INTRUSION « CLASSIQUE »

3

DÉFINITION DU TEST D'INTRUSION

- Mandat donné à une entreprise ou un expert en cybersécurité pour pénétrer dans un système d'information selon un cadre défini.
- Réalisé par un pentesteur ou hacker éthique, salarié ou indépendant ou consultant d'une entreprise spécialisée.
- Reproduit une attaque cyber, en direct, pour identifier les vulnérabilités qui pourraient être exploitées par un acteur malveillant.

4/34

4

OBJECTIFS

- Evaluer la solidité du système d'information d'une organisation
- Identifier des vulnérabilités pouvant être exploitées
- Proposer des correctifs
- Sensibiliser les différents acteurs au sein de l'entreprise (management, équipe IT, utilisateurs…)

5/34

5

LES ACTEURS

Red Team :

- Coté offensif de la cybersécurité
- Rattaché au SOC*, parfois à un VOC**
- Doit penser, agir et travailler comme le ferait un acteur malveillant
- Interne ou externe à l'organisation pentestée
- Doit percer les défenses du système d'information pentesté

Blue Team :

- Coté défensif de la cybersécurité
- Rattaché au SOC*
- Souvent composé de plusieurs sous-équipes (NIST : Detect / Protect / Recover)
- Interne à l'organisation ou déléguée à un prestataire
- Doit défendre le système d'information pentesté

*SOC : Security Operations Center
**VOC : Vulnerability Operations Center

6/34

6

LE CADRAGE DU PENTEST

- Phase obligatoire pour que le pentest ne soit pas assimilé à une infraction, et qui est complète la convention de pentest
- Permet d'expliquer le fonctionnement du pentest et ses objectifs tels que la détection de failles, identifier ce qui a été correctement élaboré, les propositions de correctifs si besoin, et le renforcement de la sécurité.
- Permet de présenter les équipes, et de définir le contexte, le périmètre, le planning, et les modalités du pentest

7/34

7

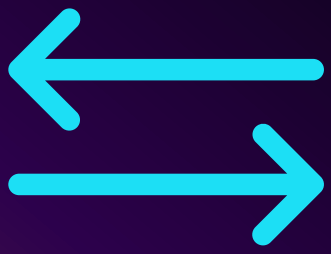
PARTICIPANTS AU CADRAGE

- Le commanditaire du pentest
- Un membre de la sécurité informatique
- Un membre connaissant l'environnement ou l'application pentestée
- Un membre représentant les utilisateurs de l'environnement ou de l'application pentestée
- Un membre représentant la Red Team

8/34

8

INFORMATIONS ÉCHANGÉES LORS DU CADRAGE

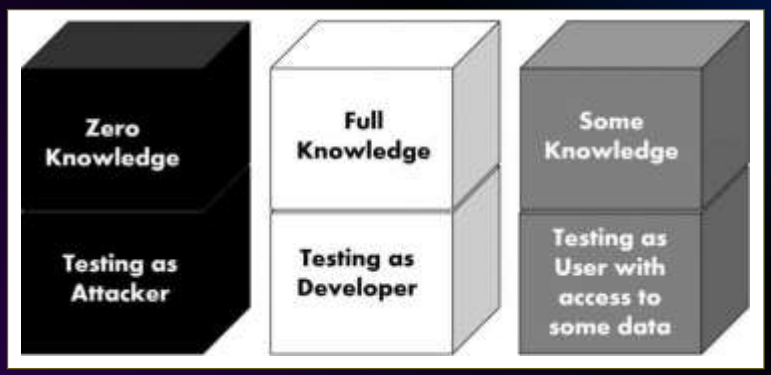


- Comprendre l'activité de l'entité : taille de l'entreprise, secteur d'activité, périmètre géographique, entité réglementée ou sur un secteur stratégique
- Comprendre l'utilisation de l'informatique au sein de l'entité pentestée : IT interne ou externe, usages et outils utilisés au quotidien, historique des cyber-attaques subies, audits/pentests précédents
- Comprendre le périmètre qui sera testé : cible, criticité, risques identifiés, informations techniques comme l'exposition sur internet, les rôles, méthode d'identification
- Planning du test

9/34

9

MODALITÉS DU PENTEST : BLACK/GREY/WHITE BOX



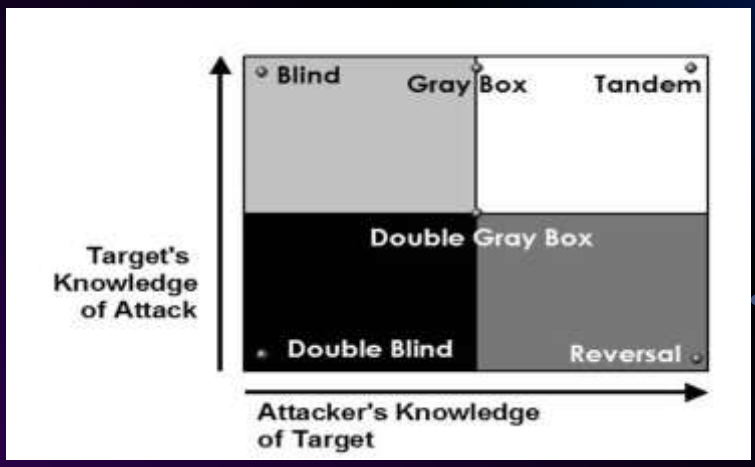
Différences entre Black, White et Grey Box par devopedia.org

10/34

10

MODALITÉS DU PENTEST : LES STRATÉGIES

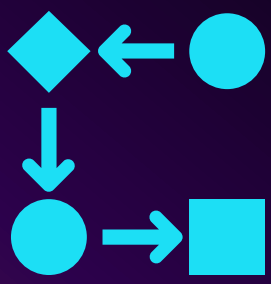
Grille des types de tests de la méthode OSSTMM 3



11/34

11

LES MÉTHODOLOGIES DE PENTEST



- Aide pour les équipes pour l'organisation du pentest
- Produites par des fondations, des centres de recherches, des organismes professionnels, les régulateurs locaux
- Donne une structure et les bonnes pratiques
- Méthodologies souvent développées aux USA
- Quelques exemples : OSSTMM, OWASP, NIST 800-115, MITRE ATT&CK Framework, Unified Cyber Kill Chain, TIBER-EU Framework

12/34

12

PHASE DE CLÔTURE : LE RAPPORT DE PENTEST

- Rédaction d'un rapport par le pentesteur, partagé avec les personnes conviées au cadrage
- Classification des vulnérabilités par criticité
- Explication des méthodes utilisées et des failles découvertes pendant le test
- Recommandations pour corriger les vulnérabilités identifiées
- Délai conseillé pour la remédiation
- Nouveau pentest pour évaluer les correctifs

13/34

13

NE PAS CONFONDRE

- Red Teaming : scénario sophistiqué, pas de contrainte de temps, utilisation de social engineering ou de l'intrusion physique
- Bug Bounty : challenge proposé à toute la communauté de la cybersécurité contre prime pour tester la solidité d'un nouveau produit, ou d'une nouvelle version d'un logiciel
- Scan de vulnérabilités : contrôle automatisé pour identifier les défauts de conception ou les points d'entrée qui pourraient être exploités sur un réseau ou un logiciel
- Audit de sécurité / White box : travail de concert entre les auditeurs et le service informatique, accès direct à toutes les informations techniques, long, cher, mais très complet.

14/34

14

A NE PAS OUBLIER

- Ce n'est pas une évaluation exhaustive de toutes les vulnérabilités d'un système d'information.
- Cela ne donne pas l'assurance d'un environnement informatique entièrement sécurisé.
- Exercice qui devra se répéter dans le temps pour maintenir un système à jour

15/34

15

PARTIE 2

APPORT D'UNE PURPLE TEAM À UN TEST D'INTRUSION

16

PROBLÉMATIQUES DU TEST D'INTRUSION CLASSIQUE

- Offre de pentest difficilement lisible pour les non-experts
- Difficultés à prioriser les vulnérabilités
- Non-coordination entre les équipes
- Manque de temps et de budget pour mettre en place les correctifs
- Multiplication et silotage des outils rendant la remédiation difficile, voir impossible
- Volume trop important de données à traiter
- Problème de communication avec le management

17/34

17

DÉFINITION DU LA PURPLE TEAM

- Activité collaborative qui implique à la fois la Red Team et la Blue Team, étudiant ensemble les vulnérabilités identifiées lors d'un pentest sur scénario réel et les remédiations à mettre en place
- Permet d'approfondir les connaissances de chaque équipe en matière de méthode d'attaque côté Blue Teams et de méthode de protection côté Red Team
- Piste d'amélioration au niveau des personnes, des processus et des outils employés.
- Traitement plus performant des vulnérabilités identifiées, et mise en place des remédiations.

18/34

18

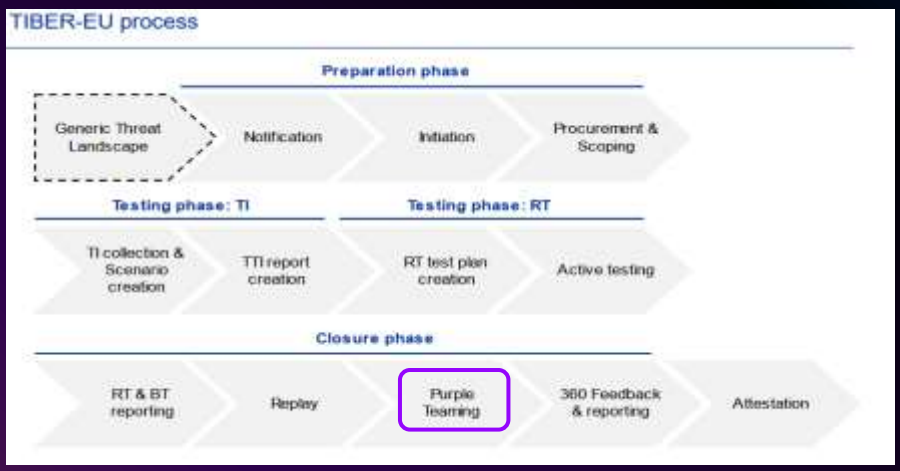
LA PURPLE TEAM : UN CONCEPT RÉCENT & DES MÉTHODOLOGIES PEU DOCUMENTÉES

- Peu de méthodes de pentest proposent d'intégrer le concept de Purple Team
- Souvent proposé pour les pentests dans le secteur de la banque/finance : TIBER-EU (EU), AASE (Singapour), iCast (HK)
- Autres méthodes : Atomic Purple Team Framework, SCYTHE Purple Team Exercice Framework
- Quand une méthode de pentest intègre le concept de Purple Team, c'est souvent sur des phases très courtes

19/34

19

EXEMPLE : LA PURPLE TEAM DE TIBER-EU



Synthèse des étapes TIBER-EU produite par la Banque Centrale Européenne

20/34

20

LA PURPLE TEAM COMME MÉTHODE SOUS-EXPLOITÉE

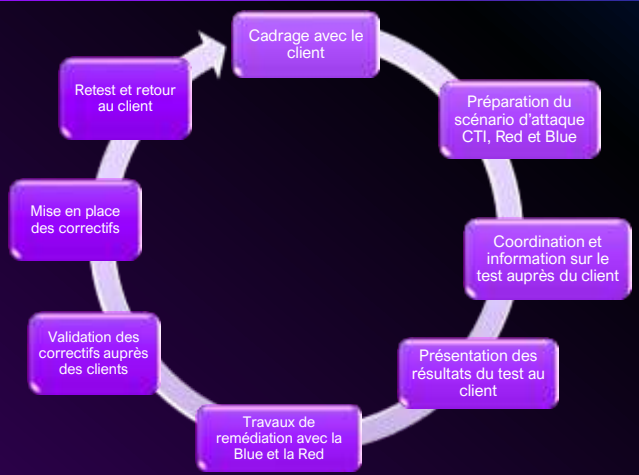
- Aucun accompagnement du client lors du cadrage du pentest, alors que l'offre et les modalités d'un pentest sont peu comprises.
- Aucune coordination pour aider à la création d'un scénario d'attaque pour le pentest en combinant les besoins de la Blue Team et les connaissances de la Red Team, souvent seule la Red Team travaille sur le sujet, avec parfois le CTI*.
- Quasiment aucune intervention lors du test en lui-même pour informer le client de l'avancement du test, alors que des problèmes de communications et de visibilités sont régulièrement remontés.
- Aucun accompagnement du client post-pentest pour comprendre les vulnérabilités identifiées, alors que leur criticité et leur priorisation sont peu comprises pour mettre en place des correctifs, et surtout débloquer les budgets nécessaires.

21/34

*CTI :Cyber Threat Intelligence

21

AVOIR UN RELAIS DE BOUT EN BOUT SUR UNE PURPLE TEAM



22/34

22

LA PURPLE TEAM : AVOIR UN VRP

- Besoin d'un profil dédié Purple :
  - Personne hors Blue et Red Team,
  - Pédagogue,
  - Approche commerciale,
  - Vernis cyber
- Aura pour mission :
  - Accompagner le client sur l'offre de pentest,
  - Préparer le scénario avec les deux équipes sur des cas réels
  - Définir les indicateurs de réussites avec toutes les parties prenantes

LA PURPLE TEAM : AVOIR UN FACILITATEUR

- Le profil Purle sera un relais pendant le test
- Il informe le client de l'avancement du test
- Il coordonne les équipes Red et Blue Teams
- Il peut demander l'arrêt du test en cas d'impacts trop importants chez le client (impact sur les données, sur les actifs, sur des fonctions critiques…), d'événements extérieurs (véritable attaque en cours) ou pour respecter le planning défini dans le cadrage

LA PURPLE TEAM : AVOIR UN TRADUCTEUR

- Le profil Purple va jouer un rôle central dans la rédaction du rapport de test avec un rôle neutre de rédacteur
- Il sera un traducteur pour que le rapport puisse être facilement appréhendé par les décideurs (executive summary)
- Le rapport devra rappeler les objectifs, les résultats, les recommandations, le coût de l'inaction, et les procédures de crises si le correctif est impossible à mettre en place dans l'immédiat
- Pour aider à l'évaluation des priorités et des failles les plus critiques à corriger, il pourra s'aider des méthodes EBIOS-RM, ISO 27 005, MEHARI…

25/34

25

LA PURPLE TEAM : AVOIR UN ANIMATEUR

- Le profil Purple sera le coordinateur pour aider la Blue Team et la Red Team à travailler ensemble sur le plan de remédiation.
- Il sera en charge de l'animation des sessions de travail en utilisant des méthodes collaboratives et créatives.
- Il devra créer de la cohésion entre deux équipes qui ne se parlent pas en temps normal.
- Il devra faciliter la créativité avec des méthodes comme le design thinking, des brainstormes, ou des outils de la méthodologie Agile.

26/34

26

EXEMPLE DE MÉTHODE CRÉATIVE – DESIGN THINKING

Schéma du Design Thinking par SimpliLearn.com

27

27

LA PURPLE TEAM : AVOIR UN CHEF DE PROJET

- Dans le cadre de la remédiation, il sera le garant du bon déroulé des travaux avec des objectifs et des rôles clairs, un planning et un suivi précis.
- A la fin des travaux, il devra présenter les résultats auprès du client pour valider les solutions, les plannings et les coûts de la remédiation
- Il prendra enfin le rôle de chef de projet pour mettre en place concrètement les solutions avec l'aide des équipes techniques et de la Blue Team, et le retest avec la Red Team.

28/34

28

LES AVANTAGES DE LA PURPLE TEAM DE BOUT EN BOUT

- **Amélioration continue** : Les équipes ont besoin d'une vision et de percevoir leur rôle central dans l'amélioration global de la sécurité de l'organisation
- **L'humain et la collaboration** : Développer des softskills et la pédagogie est essentiel, au-delà de la technique pour organiser une Purple Teams
- **Un accompagnement pour une meilleure satisfaction client** : être présent du début à la fin du projet, de la présentation de l'offre de pentest à la mise en place des correctifs
- **Un coordinateur pour laisser les équipes techniques travailler exclusivement sur la technique**: optimisation des ressources, des travaux rythmés pour plus d'efficacité
- **Recréer de la cohésion entre les équipes** : des équipes qui ne travaillent pas ensemble, deviennent des partenaires et communiquent pour résoudre des problématiques hors Purple Team.

29

PARTIE 3

LA PURPLE TEAM À L'AUBE DES RÉGLEMENTATIONS NIS2 & DORA

30

PURPLE TEAM & NIS 2

Rappel de la réglementation :

- Directive européenne entrée en vigueur en octobre 2024, transposition française en cours
- Mise en place d'un socle minimum de mesures techniques et organisationnelles sur le risque cyber
- 18 secteurs d'activités impactés et environ 15 000 entités seront concernées en France

Impact de NIS 2 pour les tests d'intrusion et les Purple Team :

- Art 21 impose la « gestion des risques fondée sur la preuve ». En mars 2026 dans son référentiel Cyber France (ReCyF), confirmation de l'ANSSI que des pentests réguliers sont un moyen de preuve solide de cette diligence.
- Mettre en place une Purple Team permettra de rentabiliser vos pentests et de garantir la mise en place de correctifs pour la bonne gestion de votre risque cyber.

31/34

31

PURPLE TEAM & DORA (ET FUTURE NIS 3?)

Rappel de la réglementation :

- Règlement européen entré en vigueur depuis janvier 2025, pas de transposition nécessaire en droit français, DORA s'applique directement.
- Harmonise la réglementation cyber au niveau UE et renforce la résilience numérique face au risque des Technologies de l'Information et de la Communication (TIC) du secteur bancaire et financier
- 20 types d'entités impactées (banques, assurances, paiements) et leurs fournisseurs critiques

Impact de DORA pour les tests d'intrusion et les Purple Team :

- Art 25 rend obligatoire des tests de pénétration avancés (TLPT : Threat-Led Penetration Testing)
- DORA se base du TIBER-EU qui intègre les Purple Team dans sa méthodologie
- Avoir une Purple Team de bout en bout garantit des tests solides et documentés en cas d'audit des régulateurs (ACPR et Banque de France)

32/34

32

LIENS UTILES

TIBER-EU Purple Teaming best practices

Red Team: Adversarial Attack Simulation Exercise - Guidelines for the Financial Industry in Singapore

Cyber Resilience Assessment Framework (iCast - HK)

Atomic Purple Team

SCYTHE Purple Team Exercice Framework

ANSSI - (ReCyF) - Version 2.5 du 17/03/2026

33

MERCI

34