{#img.text}

{@text | convertHTML}

{#images}

{%image}

{/images}

{/img.text}

|  |
| --- |
| {name} |
| WRITE-UP by {pseudo.text} |
| {date | convertDateLocale: 'fr': 'full'} |

Table des matières

Page de garde 1

Table des matieres 2

Informations générales 3

Porté 4

Résumé 5

Détails techniques 6

3) Informations générales

DÉCLARATION PRÉLIMINAIRE

Ce document est la propriété exclusive de {pseudo.text} . Il a été rédigé dans le cadre d'un entraînement basé sur un Capture The Flag (CTF) et a été réalisé de manière éthique, légale, et conforme aux règles établies par les organisateurs du CTF. Les actions décrites et les techniques utilisées l'ont été dans un environnement contrôlé et destiné à cet effet.

Il est interdit de reproduire, distribuer ou utiliser ce document ou une partie de ce document à des fins autres que la lecture personnelle sans le consentement écrit de son auteur.

Les informations contenues dans ce document sont fournies "en l'état" et sont basées sur les connaissances et les observations de l'auteur au moment de la rédaction. Aucune garantie n'est donnée quant à l'exhaustivité ou l'exactitude de ces informations.

L'objectif principal de ce write-up est éducatif. Il vise à partager des connaissances, des techniques, et des méthodes utilisées pour résoudre les challenges du CTF. Il ne doit en aucun cas être utilisé pour mener des activités illégales ou non éthiques.

4) Portée du CTF

Le challenge Capture The Flag (CTF) présenté dans le write-up "{name}" a été conçu par {client.title} pour permettre aux participants de découvrir et d'exploiter des vulnérabilités dans un environnement simulé et sécurisé. Le périmètre de ce CTF a été défini par {client.title} garantissant ainsi que seuls les composants prévus étaient inclus dans le challenge. Le CTF comprenait les composants réseau suivants :

* {-w:p scope}{name}{/scope}

*Les tests ont été menés à distance, en utilisant un VPN spécifiquement provisionné pour ce CTF.*

1. 5) résumé

Cette section offre un aperçu global des challenges résolus lors de cette participation au CTF. Les défis du CTF étaient conçus pour simuler des vulnérabilités réelles et permettre aux participants d'explorer les méthodes d'exploitation dans un cadre sécurisé et contrôlé.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **ID** | **Vulnerability** | **Affected Scope** |
| {#findings}{#cvss.baseSeverity == 'Critical'}  {cvss.baseSeverity} | {identifier} | {title} | {@affected | convertHTML}  {/cvss.baseSeverity == 'Critical'}{/findings} |
| {#findings}{#cvss.baseSeverity == 'High'}  {cvss.baseSeverity} | {identifier} | {title} | {@affected | convertHTML}  {/cvss.baseSeverity == 'High'}{/findings} |
| {#findings}{#cvss.baseSeverity == 'Medium'}  {cvss.baseSeverity} | {identifier | changeID: 'VULN-'} | {title} | {@affected | convertHTML}  {/cvss.baseSeverity == 'Medium'}{/findings} |
| {#findings}{#cvss.baseSeverity == 'Low'}  {cvss.baseSeverity} | {identifier} | {title} | {@affected | convertHTML}  {/cvss.baseSeverity == 'Low'}{/findings} |

Les détails complets de chaque etapes, incluant la description de la vulnérabilité, la preuve d'exploitation, l'impact potentiel dans un environnement réel, et les recommandations pour une sécurisation efficace, sont détaillés dans les sections ultérieures de ce write-up.

1. 6) Détails techniques

{#findings}

## {title}

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Gravité CVSS** | **{@cvss.cellColor}**  **{cvss.baseSeverity | criteriaFR}** | | **CVSSv3 Score** | | **{@cvss.cellColor}**  **{cvss.baseMetricScore}** | |
| **Critères CVSSv3** | Vecteur d'attaque : | **{cvssObj.AV| criteriaFR}** | | Porté : | | **{cvssObj.S| criteriaFR}** |
| Complexité de l'attaque : | **{cvssObj.AC| criteriaFR}** | | Confidentialité: | | **{cvssObj.C| criteriaFR}** |
| Required Privileges : | **{cvssObj.PR| criteriaFR}** | | Intégrité: | | **{cvssObj.I| criteriaFR}** |
| Interaction de l'utilisateur : | **{cvssObj.UI| criteriaFR}** | | Disponibilité  : | | **{cvssObj.A| criteriaFR}** |
| **Périmètre concerné** | {@affected | convertHTML} | | | | | |
| **Description** | {#description}  {@text | convertHTML}  {#images}  {%image}  Image 2 – {caption}  **{/images}**  {/description} | | | | | |
| **Observation** | {#observation}  {@text | convertHTML}  {#images}  {%image}  Image 3 – {caption}  **{/images}**  {/observation} | | | | | |
| **Test details**  {#poc}  {@text | convertHTML}  {#images}  {%image}  Image 4 – {caption}  {/images}  {/poc} | | | | | | |
| **Remédiation** | {#remediation}  {@text | convertHTML}  {#images}  {%image}  Image 5 – {caption}  **{/images}**  {/remediation} | | | | | |
| **References** | {#references}  {.}  {/references} | | | | | |

{/findings}

WRITE-UP :

{#reconnaissance.text}

{@text | convertHTML}

{#images}

{%image}

{/images}

{/reconnaissance.text}

{#Foothold.text}

{@text | convertHTML}

{#images}

{%image}

{/images}

{/Foothold.text}

{#privsc.text}

{@text | convertHTML}

{#images}

{%image}

{/images}

{/privsc.text}

{#Persistence.text}

{@text | convertHTML}

{#images}

{%image}

{/images}

{/Persistence.text}

{#Pivoting.text}

{@text | convertHTML}

{#images}

{%image}

{/images}

{/Pivoting.text}

{#libre.text}

{@text | convertHTML}

{#images}

{%image}

{/images}

{/libre.text}

### {company.name}.