TIC-SEC5 / ColorSheep

TIC-SEC5

Type	Description
Dépôt	https://rendu-git.etna-alternance.net/module-9373/activity-50798/group-1004651
VM 1	172.16.233.14:student:hehK[7d@
VM 1	172.16.233.46:student:cN)s3src
Fichiers requis	Rapport final, support de présentation
Correction	Rapport final, soutenance
Durée	3 runs
Taille de groupe	4

Objectifs

Notion	Description
Repérage	Cartographie des services exposés sur les serveurs
Identification de vulnérabilités	Recherche et identification de vulnérabilités en boîte noire puis en boîte grise (avec et sans compte utilisateur)
Exploitation de vulnérabilités	Exploitation de ces vulnérabilités
Prévention	Remonter de mauvaises pratiques ou des habitudes menant à des risques en termes de sécurité
Recommandations	Adresser ses risques et proposer des recommandations pour corriger les éléments découverts

Consignes

La startup française **ColorSheep** a été créée afin de proposer des articles dédiés aux moutons.

Le marché étant très concurentiel et les attaques informatiques de plus en plus nombreuse, ils ont décidé de faire réaliser un test d'intrusion sur leur système d'information.

C'est vous qui avez été mandatés pour l'executer. Il s'agit d'un pentest de type "black box", autrement dit, vous n'avez pas plus d'information à votre disposition.

Pour présenter vos tests et leurs résultats, vous allez devoir réaliser :

- un rapport des tests d'intrusion avec l'ensemble des vulnérabilités découvertes et vos recommandations pour corriger ces failles de sécurité,
- une réunion de restitution des résultats de l'audit avec un support de présentation.

Note

Obtenir un accès `root` ne veut pas (forcément) dire que vous avez tout exploré !

Règle

Seuls les outils suivants sont autorisés :

- un scanner de ports : nmap
- un proxy HTTP : Burp Proxy
- les clients natifs de serveurs (exemples: clients de base de données comme MySQL ou MSSQL, clients SSH et FTP, etc..)
- John The Ripper
- patator.py + des dictionnaires de bruteforce

Aucun outil d'exploitation automatique n'est autorisé (Nessus, Nexpose, Acunetix, SQLMap, "scripts nmap / nmap -A", etc).
Les scripts de nmap sont interdits (options -sC, --script=* ou -A, etc). Leur utilisation sera considérée comme de la triche.

Liens utiles

https://www.owasp.org/index.php/Main_Page
https://www.owasp.org/index.php/Penetration_testing_methodologies
https://attack.mitre.org/wiki/Main_Page

Rapport de test d'intrusion

Le rapport final est le seul document durable et détaillé transmis à l'audité : il permet de démontrer et de valoriser votre travail.

Sont attendus dans ce rapport, les 4 sections suivantes :

- Une introduction
  - Le contexte
  - Les objectifs du test d'intrusion
  - Le rappel du périmètre (adresses IP)
- Une synthèse managériale destinée au directeur de ColorSheep (interlocuteur non technique)
  - L'évaluation du niveau de risque du périmètre
  - La mise en avant des risques métier associés aux vulnérabilités
- Une synthèse technique
  - La liste des vulnérabilités avec le niveau de risque associé
  - La liste des recommandations avec la difficulté de correction
  - Un résumé chronologique et méthodologique de vos tests
- Un rapport technique détaillé
  - Une sous-section pour chaque vulnérabilité identifiée
  - Une description détaillée de chaque vulnérabilité
  - Les détails permettant son exploitation (URL et paramètres associés)
  - L'évaluation de sa criticité
  - Le scénario d'exploitation de la vulnérabilité avec des preuves (vidéo, capture d'écran)
  - La / les recommandation(s) associée(s)

Soutenance et support de présentation (20 min)

Cette présentation sera structurée en 2 parties :

- présentation des résultats de votre audit de sécurité à des personnes non techniques (type président de l'entreprise ou COMEX) afin d'illustrer les risques et conséquences en cas d'attaque ciblant ColorSheep (7 minutes)
- échanges et questions / réponses techniques sur les failles découvertes durant les tests d'intrusion (8 minutes)

L'objectif de cette soutenance est d'évaluer votre capacité à restituer votre travail et votre communication. Vous serez évalué à la fois sur le fond et la forme.

Conseils

- Utilisez un vocabulaire adapté au contexte professionnel.
- Relisez-vous pour éviter les fautes d'orthographe.
- Préférez le "nous" à l'emploi du "je".