Méthodologie de vérification de la cybersécurité

Introduction

Le rapport actuel expose les résultats et les conclusions issus de l'évaluation d'intrusion réalisée au sein de la société Cyberexpert. L'initiative vise principalement à analyser en détail la solidité de l'infrastructure informatique de l'entreprise en termes de cybersécurité, face à diverses menaces potentielles.

Contexte et objectifs de la mission

La société Tryhack Pentesting a été chargée par Cyberexpert d'effectuer une évaluation de la sécurité de son système d'information. L'objectif principal de cette mission est de détecter toute vulnérabilité éventuelle, d'évaluer la capacité de résistance aux attaques, et de formuler des recommandations en vue d'améliorer la sécurité globale du système informatique.

Périmètre de la mission

La mission couvre l'ensemble des systèmes, réseaux et applications exploités par Cyberexpert. L'évaluation se focalise uniquement sur les adresses IP délimitées dans le périmètre suivant :

10.0.1.10 10.0.1.31 10.0.1.62 10.0.1.206
10.0.1.20 10.0.1.51 10.0.1.64 10.0.1.208
10.0.1.21 10.0.1.52 10.0.1.67 10.0.1.211
10.0.1.28 10.0.1.53 10.0.1.200
10.0.1.30 10.0.1.59 10.0.1.202

Ainsi que les domaines suivants sur l’active directory :

- middle-earth
- mordor

Il est important de noter qu’il nous a été signalé que les adresses IP ci-dessous ne rentraient pas dans le périmètre de la mission et n’ont donc pas été analysées :

- 10.0.1.40
- 10.0.1.230
- 10.0.1.8
- 10.0.1.7

Démarche méthodologique

Pour atteindre nos objectifs, les étapes suivantes ont guidé notre approche :

Analyse du réseau et ciblage des priorités : Évaluation approfondie du réseau pour déterminer les cibles prioritaires.
• Implémentation d'outils de surveillance du réseau : Déploiement stratégique d'outils visant à examiner le flux du réseau.
• Identification des failles de sécurité : Analyse précise pour repérer d'éventuelles vulnérabilités.
• Exploitation des vulnérabilités par des tests : Évaluation de la gravité des vulnérabilités via des essais d'exploitation.
• Pivoting à partir des cibles compromises : Exploration des opportunités d'utiliser les machines compromises comme points de pivot pour atteindre de nouvelles cibles.

Déroulement des travaux

Le test a eu lieu sur la période du 5 au 11 décembre 2023, englobant l'ensemble de ces dates. Un courriel marquant le début de l'évaluation a été envoyé à M. Florian Amette le 5 décembre 2023 à 11h, officialisant ainsi le commencement de nos

activités. De manière similaire, un courriel indiquant la fin du test a été transmis à M. Amette le 11 décembre 2023 à 18h00, confirmant la clôture de nos évaluations.

Restrictions

Il est important de noter que toute évaluation de sécurité présente des limites inhérentes. Il se peut que certaines vulnérabilités n'aient pas été détectées, et diverses contraintes, qu'elles soient liées au temps ou à la technique, peuvent influencer les résultats. Ces restrictions sont prises en compte lors de l'analyse des conclusions présentées dans ce rapport. Il est également crucial de souligner qu'en raison du grand nombre de vulnérabilités identifiées, certaines faiblesses potentielles de l'infrastructure n'ont pas été soumises à des tests. Afin de préserver l'intégrité de l'environnement de production, nous avons délibérément exclu toute tentative de "bruteforce" ainsi que toute action visant à surcharger le réseau (DDoS).

Remise en état

À la clôture du test d'intrusion, un serveur spécifiquement dédié à l'évaluation a été mis en place, incluant l'installation d'outils spécialisés nécessaires à l'analyse de la résilience de l'infrastructure. Cependant, en raison des risques potentiels liés à la persistance de ces outils sur le réseau, la première recommandation est de procéder à leur désinstallation immédiate. Cette mesure vise à réduire au minimum tout risque subsistant. Il est important de noter que l'environnement a été restauré à son état initial à la fin du test.

Lettre d’autorisation

Tryhack

Mr Sébastien P
Tryhack Pentesting
laaze@protonmail.com
06 06 06 06 06

Mr Florian Amette
Cyber Experts
12 rue de l'accompagnement
Jedha City 75003

Fait à Tatoine le 05/12/2023

Objet : Demande d'autorisation de Pentest pour le projet - "L'Attaque de l'Étoile de la Mort"

Monsieur Amette,

Je vous adresse la lettre pour solliciter votre autorisation afin de conduire des activités de pentest dans le cadre du projet "L'Attaque de l'Étoile de la Mort". Notre mission consiste à identifier et à exploiter les vulnérabilités présentes au sein de votre infrastructure.

Périmétre du Pentest :
L'exercice de test d'intrusion vise à simuler une attaque ciblée sur l'infrastructure de « l'Étoile de la Mort ». Le périmètre de l'intervention incluant les machines suivantes :

- **10.0.1.0/24** en excluant les cibles suivantes **10.0.1.40**, **10.0.1.230**, **10.0.1.8** et **10.0.1.7**.

Outils Autorisés :
Conformément aux règles strictes de la mission, nous utiliserons uniquement les outils autorisés par le règlement. Cette liste comprend, sans s'y limiter :

- Scanner de vulnérabilité
- Outils d'exploitation
- Scanner de réseaux

Notre promesse est de n'utiliser aucun outil interdit, garantissant ainsi une compétition équitable, transparente et conforme aux normes légales et éthiques.

Portée du Pentest :
Notre action se limitera strictement aux objectifs définis dans les règles de notre mandat. Aucune attaque ne sera dirigée vers l'équipe bleue ou l'infrastructure générale de l'Étoile de la Mort. Les vulnérabilités détectées seront signalées conformément à la politique établie, laquelle stipule que toutes les découvertes seront rapportées immédiatement à l'instructeur par le biais d'un rapport

détaillé, incluant la nature de la vulnérabilité, les étapes d'exploitation et les recommandations pour la mitigation.

Collaboration avec l'Équipe Rouge :
Notre participation active au sein de l'équipe Red Team sera caractérisée par une collaboration transparente et une communication constante. Les rapports détaillés sur nos stratégies, avancements et conclusions seront régulièrement partagés avec l'instructeur pour maintenir un haut niveau de coordination et d'efficacité.

Respect de la Confidentialité :
Dans le cadre de l'attaque, nous nous engageons à maintenir rigoureusement l'intégrité des systèmes cibles et à préserver la confidentialité des données utilisateurs. Aucune action ne sera entreprise en vue de la suppression ou de la modification irréversible des données. De plus, nous nous engageons à ne pas divulguer, partager ni utiliser à des fins autres que celles du présent exercice, toutes informations sensible ou données personnelles auxquelles nous pourrions avoir accès au cours du test d'intrusion.

Signalement des Vulnérabilités :
Toute vulnérabilité identifiée pendant le défi sera immédiatement signalée à l'instructeur, conformément à la politique établie.

Communication en Cas d'Incident :
En cas de découverte sensible ou d'incident, nous nous engageons à informer immédiatement l'instructeur ou l'assistant enseignant pour permettre une gestion rapide et adéquate de la situation. Nous sommes conscients que le non-respect des règles stipulées peut entraîner des sanctions, y compris l'exclusion de la mission.

Nous vous prions de bien vouloir donner votre approbation pour que nous puissions entreprendre cette mission avec intégrité et responsabilité. Mon équipe et moi-même restons à votre disposition pour toutes informations complémentaires.

Cordialement,

Sébastien P.
Manager Tryhack Pentesting

Signature du client
Précédé de la mention
« Bon pour accord » et de la date

Bon pour accord

Florian AMETTE

Lettre de mission

Tryhack

Objet : Lettre de mission pour un test d'intrusion (pentest)

Madame, Monsieur,

Nous vous remercions de nous avoir consulté dans le cadre de votre besoin de test d'intrusion.

Comme mentionné dans la proposition commerciale ci-jointe, nous vous proposons d'intervenir dans vos locaux pour mener à bien un test d'intrusion sur les systèmes d'informations de Cyber Experts.

Le test d'intrusion, sera réalisé dans le but d'évaluer la robustesse de la sécurité informatique de vos systèmes. Notre équipe d'experts en sécurité informatique utilisera des méthodologies avancées pour identifier les vulnérabilités potentielles qui pourraient être exploitées par des acteurs malveillants.

Le test d'intrusion sera effectué en suivant une méthodologie rigoureuse, incluant des phases de reconnaissance, de scanning, d'analyse de vulnérabilités, d'exploitation et de rapport. Toutes les activités seront menées de manière éthique et respecteront les lois et régulations en vigueur.

Durant cette période, nous solliciterons votre collaboration pour minimiser les impacts potentiels sur vos opérations quotidiennes.

Nous restons à votre disposition pour toutes informations complémentaires.

Nous vous remercions de votre confiance et sommes impatients de travailler avec vous.

Veuillez agréer Madame, Monsieur l'expression de mes sentiments les plus distingués,

Mr Sébastien P.

CEO Tryhack Pentesting

Signature du client

Précédée de la mention

« Bon pour accord »

Bon pour accord
Florian AMETTE

Lettre de fin de mission

Mr Sébastien P

Tryhack Pentesting

laaze@protonmail.com

06 06 06 06 06

Mr Florian Amette

Cyber Experts

12 rue de l'accompagnement

Jedha City 75003

Fait à Tatooine le 11/12/2023

Objet : Lettre de fin de mission de test d'intrusion

Monsieur Amette,

Par la présente, nous tenons à vous informer de la clôture de la mission de test d'intrusion que nous avons menée au sein de votre entreprise, mission qui a débuté le 05/12/2023 et s'est achevée ce jour le 11/12/2023

Dans le cadre de cette prestation, notre équipe a effectué une série de tests d'intrusion visant à évaluer la sécurité de vos systèmes informatiques. Ces tests ont permis de mettre en évidence plusieurs vulnérabilités, dont le détail vous a été communiqué dans notre rapport final, remis en date du 11/12/2023.

Nous espérons que les recommandations fournies dans ce rapport vous aideront à améliorer la sécurité de vos systèmes. Notre équipe reste à votre disposition pour toute question ou besoin supplémentaire concernant la sécurisation de votre infrastructure informatique.

Nous serions également heureux de collaborer à nouveau avec vous pour toute future mission de sécurité informatique.

Nous vous prions d'agréer, monsieur, l'expression de nos salutations distinguées.

Cordialement,

Sébastien P.

Manager Tryhack Pentesting