Thomas Becquevort

Département technique Namur – IESN

Etu47150

Avenue du Roi Albert, 31A

1340 Ottignies

Belgique

0498/68.74.49

etu47150@henallux.be

HENALLUX

A l'attention du Secrétaire du jury,

Rue Joseph Calozet, 19

5000 Namur

Belgique

*Ottignies, le 08 février 2023*

**Objet : Recours interne sur base de l'article 106 du Règlement des études, des examens et disciplinaire de la Haute Ecole de Namur-Liège-Luxembourg relatif aux irrégularités durant l'épreuve de sécurité offensive - IR305.**

Monsieur le Secrétaire du jury,

Par la présente, et conformément à l'article 134, 8° du Décret du 7 novembre 2013 définissant le paysage de l'enseignement supérieur et l'organisation académique des études et à l'article 106 du Règlement des études, des examens et disciplinaires de la Haute Ecole de Namur-Liège-Luxembourg (Henallux), je souhaite formuler un recours pour irrégularité dans le déroulement de l'épreuve de sécurité offensive - IR305.

En application de ces articles, je demande aux membres du jury de bien vouloir enregistrer ma plainte, de considérer que celle-ci est introduite dans le délai de 3 jours ouvrables à compter de mercredi 8 février 2023 et, de constater qu'elle est recevable et fondée.

1. ***Faits***

En date du 30 décembre 2022, un autre étudiant, Blacks Simon, et moi-même devions remettre en binôme un rapport (annexe n° 1) de manipulations pratiques dans la cadre de l'évaluation du cours de sécurité offensive. Ce cours n'étant pas évalué d'un point de vue théorique, c'est ce rapport qui représente la totalité de l'évaluation du cours.

Selon les modalités d'évaluation qui avaient été annoncées dans le document :

Évaluation du laboratoire – Sécurité Offensive (annexe n° 3),

l'évaluation devait se dérouler comme suit :

> *Différents professeurs ont chacun groupe d'étudiants attribué et le professeur attitré à l'évaluation de notre groupe est M. Michaux Pierre.*
>
> *Plusieurs critères servent à l'évaluation du travail rendu. Le premier étant la nécessité de respecter une structure de rapport de type "entreprise" et donc présenter différentes parties précises. Lorsque le rapport remplit cette structure, il est soumis à des critères d'exclusion. Ces derniers sont au nombre de trois et les voici :*
>
> *Le rapport doit mettre en avant la récupération de trois accès root.*
>
> *Le rapport doit mettre en avant la récupération de quatre accès simples.*
>
> *Le rapport doit mettre en avant la pénétration de quatre machines.*
>
> *Si ces trois critères sont respectés, le rapport est évalué selon les cinq critères présentant chacun une pondération propre à leur importance dans le travail. Dix pourcents pour l'orthographe et la formulation, dix pourcents pour la structure et le format, dix pourcents pour les liens faits avec la formation de l'étudiant, quarante pourcents pour la pertinence des éléments retenus et les derniers trente pourcents pour la méthodologie employée.*
>
> *On peut également relever que, non sous forme de critère mais sous forme d'explication quant au travail attendu, il est expliqué dans ce même*

*document que la partie la plus intéressante est la manière dont le travail à été réalisé durant les séances ainsi que les explications que nous lui apportons et que le simple affichage du résultat d'une commande n'a pas d'intérêt, c'est son explication et sa justification qui sont la clé du travail.*

*Une fois l'évaluation selon la grille pondérée réalisée, trois issues pouvaient se présenter. Soit la note est largement suffisante et le binôme est dispensé d'une défense orale, soit le rapport est accepté mais la note n'est pas suffisante et une défense orale est proposée au binôme afin de lui permettre de récupérer les points manquants, soit le rapport ne satisfait pas les critères présentés ci-dessus et le binôme doit présenter un nouveau travail en seconde session.*

Cette grille d'évaluation qui nous a été remise au début du quadrimestre (annexe n° 3) reprend clairement les critères qui fondent l'évaluation et la détermination de la note. A cet égard, il peut être noté que le critère « nombre minimal de flags » n'est pas mentionné dans cette grille.

2. ***Moyens mis à la cause - Irrégularités touchant le déroulement de l'épreuve***

*Le travail qui a été fourni par notre binôme a été construit en s'axant autour de la grille d'évaluation. Chaque élément qui y a été ajouté avait pour but de respecter un prérequis de cette grille ou de permettre une meilleure compréhension d'une information relative à ces prérequis. Nous étions présents à chaque cours et avons également travaillé en dehors de ces heures prédéfinies afin de peaufiner notre travail.*

*La structure demandée en sept parties a été respectée afin de satisfaire le format type "entreprise" demandé pour le rapport.*

*Les trois critères d'exclusion ne sont pas applicables car aux pages douze et treize du rapport (annexe n° 2), il est possible de retrouver le tableau des comptes récupérés au sein de l'infrastructure et il est possible d'y retrouver quatres comptes administrateurs que sont :*

- *Le compte root de la machine 10.180.30.1*
- *Le compte root de la machine 10.180.30.254*
- *Le compte NT AUTHORITY\SYSTEM de la machine 10.180.20.2*
- *Le compte NT AUTHORITY\SYSTEM de la machine 10.180.20.3*

*mais également quatre comptes utilisateurs que sont :*

- *Le compte bob de la machine 10.180.30.1*
- *Le compte user de la machine 10.180.30.1*
- *Le compte blogger de la machine 10.180.30.1 qui est un utilisateur wordpress*
- *Le compte user de la machine 10.180.30.254*

*Ce même tableau permet également de synthétiser la machines qui ont pu être compromises lors des manipulations et on peut donc conclure qu'elles sont au nombre de quatre :*

- *La machine 10.180.30.1*
- *La machine 10.180.30.254*
- *La machine 10.180.20.2*
- *La machine 10.180.20.3*

*Le travail qui a été fourni par notre binôme remplit donc bien les critères minimaux pour une évaluation selon la grille pondérée.*

A titre de moyen unique, je soulève le non-respect des modalités d'évaluation annoncées au début du quadrimestre et retenus dans le document servant de grille d'évaluation.

En effet, comme cela a été expliqué, la grille d'évaluation ne fait nullement mention du critère « nombre minimal de flags ». Cependant, c'est après l'évaluation de notre travail qu'il nous a été indiqué qu'au moins un flag devait être présenté dans le rapport par machine infiltrée (annexe n° 5) et que ce critère était la raison de l'exclusion de notre rapport.

3. ***Conclusion***

Pour ces motifs, je vous demande, Mesdames, Messieurs les membres du jury restreint, de bien vouloir constater qu'il existe une ou plusieurs irrégularités dans le déroulement de mon évaluation et, par conséquent, de bien vouloir demander au jury de se réunir afin, dans un premier temps, de corriger cette irrégularité et, dans un deuxième temps, de redélibérer.

Je vous prie de croire, Mesdames, Messieurs, en l'assurance de ma considération distinguée.

**Liste des annexes :**

- Annexe n° 1 :  Rapport

lien du rapport complet: https://4zv4l.github.io/Securite_Offensive.pdf

- Annexe n° 2 : Tableau des résultats du rapport

# 5. Résultats

## 5.1 Machines et Vulnérabilités

Voici la liste que nous avons pu dresser des machines présente sur le réseau et des failles que nous avons exploitées pour en prendre le contrôle. Cette liste est dressée dans l'ordre dans lequel nous sommes parvenus à exploiter les machines.

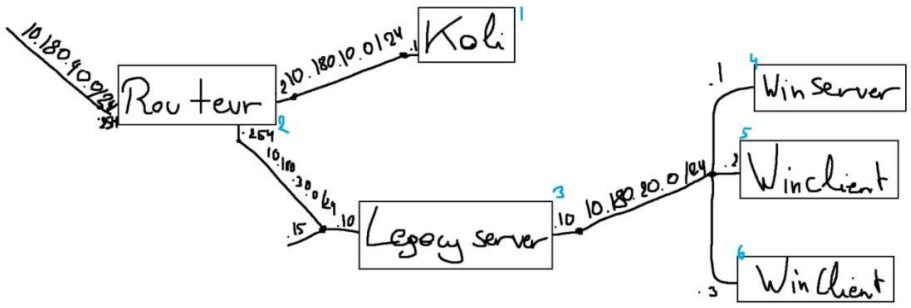
| Adresse sur le réseau | Descriptif de la Machine | Exploit utilisé |
|---|---|---|
| 10.180.30.1 | Legacy Server | Wordpress Slideshow Upload + Escalation de privilèges avec "sudo strace su" (sudo -l) |
| 10.180.30.254 | Router | Credentials on the Legacy Web Server |
| 10.180.20.1 | Windows Server | Kerberoast |
| 10.180.20.2 | Windows Client | Eternal Blue |
| 10.180.20.3 | Windows Client | Log4Shell (changer le "/bin/bash" en "cmd" pour adapter l'exploit à Windows) |

L'exploitation de ces différentes vulnérabilités sur les machines nous a permis de récupérer des mots de passe de compte utilisateur ou administrateur sur ces machines. Voici la liste de ces user+passwd dressée dans l'ordre dans lequel les machines ont été exploitées :

| Adresse sur le réseau | Descriptif de la Machine | Comptes récupérés |
|---|---|---|
| 10.180.30.1 | Legacy Server | root via l'exploit utilisé<br>bob via root<br>user via root<br>blogger:jason (utilisateur wordpress) |

| | | |
|---|---|---|
| 10.180.30.254 | Router | root:SanjiVinsmoke<br>user:RoronoaZoro |
| 10.180.20.2 | Windows Client | NT AUTHORITY\SYSTEM via l'exploit utilisé |
| 10.180.20.3 | Windows Client | NT AUTHORITY\SYSTEM via l'exploit utilisé |

## 5.2 Plan du Réseau



- Annexe n° 3 : Grille d'évaluation

# Evaluation du laboratoire – Sécurité Offensive

## Introduction

Pour la partie du cours – Sécurité Offensive, on vous demande de rédiger un rapport reprenant le travail effectué pour l'ensemble des manipulations. Pour rappel, ce travail s'effectue par deux et est potentiellement dispensatoire de l'examen si bien réalisé.

## Structure

Ce travail doit s'inspirer des rapports réalisés dans le contexte d'un audit de sécurité ou test d'intrusion d'un système informatique. C'est bien à votre client, ici la société MegaCorpOne qu'il doit être adressé. Ce rapport devra respecter la structure suivante :

- Page de couverture
- Synthèse aux décideurs
- Introduction
- Méthodologie utilisée
- Résultats
- Conclusion
- Annexes

Pour le détail de chaque section, on vous invite à consulter les transparents disponibles sur Moodle ou poser des questions à l'équipe enseignante.

## Travail attendu

### Méthodologie

Ce qui nous intéresse le plus c'est la manière dont vous avez travaillé durant les séances de laboratoire. Quels sont les outils utilisés ? comment fonctionnent ces outils ? Pourquoi tel ou tel argument ? Quels sont les avantages d'après vous, d'utiliser un outil plutôt qu'un autre ? Quelles difficultés avez-vous rencontrées ? Comment avez-vous surmonté ces difficultés ? Quel impact sur le résultat final ?

### Résultat

Les résultats correspondent à une synthèse des éléments récupérés à l'aide des différents outils utilisés durant les manipulations. Simplement afficher le résultat d'une commande ne nous intéresse pas. Ce qui est important pour nous, c'est une explication et une justification des résultats. Par exemple, pourquoi un port 21 ouvert sur un serveur peut représenter une faille de sécurité, comment il est possible de l'exploiter, comment corriger la vulnérabilité etc.

Une grille ci-dessous reprend les notes attribuées en fonction des critères :

| Critères | Explications | Notes (/20) |
|---|---|---|
| Orthographe et formulation | L'orthographe, la conjugaison ainsi que la formulation des phrases sont correctes | 2 |
| Structure et format du document | Le format est un fichier PDF. Le document respecte la structure imposée | 2 |
| Liens avec la formation de l'étudiant | Afin de justifier ses propos, l'étudiant fait le rapport entre ses découvertes, les outils utilisés et les concepts vus durant son cursus | 2 |
| Pertinence des éléments retenus (résultats) | Les étudiants ont retenu dans leur rapport les éléments clés qui permettent d'évaluer le niveau de sécurité d'un système d'information et donnent des pistes de solutions pertinentes pour chaque problème identifié | 8 |
| Méthodologie Pentest | Les étudiants suivent une méthodologie précise liée à leurs objectifs : auditer la sécurité d'un système d'information. Ils décrivent et justifient chaque étape et chaque outil utilisé | 6 |

### Critère d'exclusion

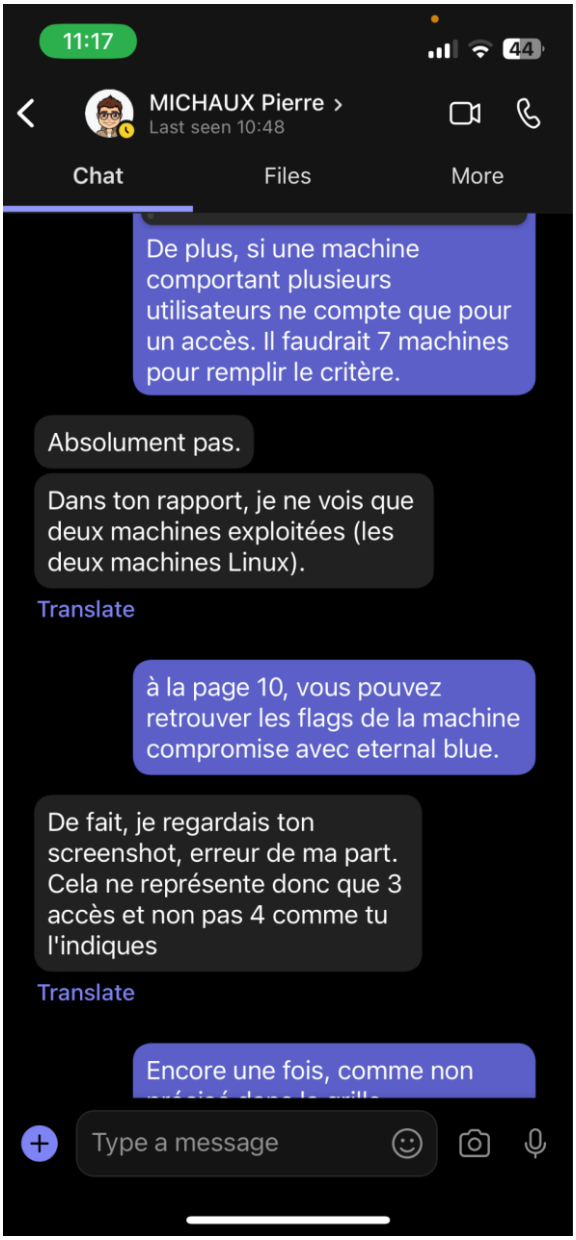
Le rapport est recevable uniquement si le groupe a récupéré 3 accès root et 4 accès simple utilisateur. Il faudra donc au minimum réussir à exploiter 4 machines. Si ce critère n'est pas rencontré, alors le rapport n'est pas recevable et les membres du groupe devront repasser cette partie de l'UE.

## Remise du rapport et dispense

Un rapport reprenant l'entièreté des manipulations devra être remis sur Moodle durant le mois de décembre. La date précise sera communiquée également via Moodle. Si le rapport satisfait aux exigences, les étudiants seront dispensés de l'examen. Si le rapport ne satisfait pas aux exigences, les étudiants devront corriger et représenter le rapport oralement durant la session d'examen.

Pour s'assurer d'une qualité suffisante des rapports, les étudiants peuvent envoyer un brouillon de leur avancement après la deuxième manipulation à leur professeur de laboratoire pour recevoir un feedback.

- Annexe n° 4 :  Conversation avec notre professeur



- Annexe n° 5 : Demande de flag