WORLDSKILLS FRANCE

GUIDE DE PREPARATION AUX FINALES NATIONALES LYON 2020

Métier n° 54 – CYBERSECURITE

worldskills France

Table des matières

MOT DE MICHEL GUISEMBERT

PRESIDENT DE WORLDSKILLS FRANCE

Bonjour championne, bonjour champion,

Tu as brillamment été sélectionné(e) dans ton équipe régionale pour participer aux prochaines finales nationales de la compétition WorldSkills. Félicitations ! C'est le fruit de ton travail, de ta passion et de ton talent à pratiquer ton métier dans l'excellence.

Il nous importe que tu sois bien préparé(e) pour cette finale qui se déroulera à Lyon au Parc Eurexpo du 15 au 17 décembre. 3 jours de compétition intense pendant lesquels tu vas te mesurer aux autres candidats(es) des autres régions qui comme toi sont aussi des champions(nes) !

On ne vient pas à ce genre de compétition avec l'espoir d'obtenir la médaille d'or, c'est-à-dire d'intégrer l'Equipe de France des Métiers, sans une préparation sérieuse et intense.

Pour WorldSkills France qui organise cette magnifique manifestation, qui réunira plus de 700 candidats dans 60 métiers et accueillant 75 000 visiteurs, il est important que chacune et chacun ait bien les mêmes chances et les mêmes informations pour bien se préparer avant la compétition.

C'est la raison pour laquelle tu trouveras dans ce guide toutes les informations dont tu auras besoin à la fois pour l'organisation générale et à la fois pour les épreuves que tu auras à effectuer.

Très bonne préparation et à très vite.

Michel GUISEMBERT
Président de WorldSkills France

PRESENTATION DES DATES IMPORTANTES

De Février à Septembre 2020 : Les Sélections Régionales

Organisées dans les 15 régions de France métropolitaine et d'Outre-Mer par les Conseils Régionaux ou les organisations professionnelles, supervisées par des jurys de professionnels et d'enseignants, elles sélectionnent les meilleurs talents dans chaque métier. Cette étape permet ainsi aux médaillés d'or de chaque métier en compétition d'accéder aux 46ème Finales Nationales.

Séminaire WorldSkills France

Le séminaire WorldSkills France, appelé également Module 1, consiste à rassembler physiquement ou virtuellement, l'ensemble des délégations régionales afin de leur communiquer les informations relatives aux Finales Nationales de Lyon 2020. L'objectif de ce séminaire est de s'assurer que chaque participant bénéficie du même degré d'informations afin que leur préparation pour les finales soit la plus optimale possible. Des informations vous seront communiquées ultérieurement sur les dates et les types de regroupement.

Du 15 au 17 Décembre 2020 : Les Finales Nationales

Elles réunissent près de 700 champions régionaux venus de toute la France. Durant ces trois jours de compétition, les champions régionaux devront se confronter les uns aux autres et mesurer leur savoir-faire et leur talent. Cet événement, qui se déroulera du 15 au 17 décembre 2020 à Lyon, représentera une étape importante pour les futurs membres de l'Équipe de France des Métiers. Ces Finales Nationales rassembleront les meilleurs compétiteurs et constitueront les prémices d'une aventure mondiale avec la WorldSkills Competition Shanghai en 2021, et de la formidable expérience européenne avec les EuroSkills qui auront lieu à Saint-Pétersbourg en 2022.

De 22 au 27 Septembre 2021 : La compétition mondiale de Shanghai

A l'issue des finales nationales de Lyon 2020, les médaillés d'or et d'argent *(et éventuellement le médaillé de bronze)* des métiers présents à la compétition mondiale intégreront le pool de sélection de leur métier. Durant une période de 3 mois, ils participeront aux modules de préparation organisés par leur Expert et l'Equipe métier. Ces modules permettront de sélectionner le titulaire et le suppléant qui intègreront l'Equipe de France des métiers et qui iront défendre nos couleurs à Shanghai en Septembre 2021. Une fois sélectionnés, les membres de l'équipe de France bénéficieront d'une préparation technique, physique et mentale de haut niveau.

Septembre 2022 : La compétition Européenne de Saint-Pétersbourg

Au retour de la compétition de Shanghai 2021, une nouvelle sélection sur la base du pool issu des finales nationales de Lyon 2020, sera faite afin de constituer l'Equipe de France des Métiers qui concourra à la compétition Européenne de 2022 à Saint-Pétersbourg.

RETRO-PLANNING DE LA 46EME EDITION

PRESENTATION DES FINALES NATIONALES

Etape phare et incontournable dans le processus de sélections des équipes de France des métiers de Shanghai 2021 et Saint-Pétersbourg 2022, la 46ème finale nationale de la compétition WorldSkills France se tiendra au parc Eurexpo de Lyon du 15 au 17 décembre 2020.

Pendant les trois jours de compétition, chaque compétiteur et chaque compétitrice devra réaliser des ouvrages qui concentrent les difficultés techniques de chaque métier, dans des conditions très proches de la vie réelle des entreprises. Le respect des délais et des coûts, l'utilisation optimale du matériel et des matériaux, la sécurité… sont autant de contraintes à respecter, conformément aux exigences du monde économique actuel.

Les qualités qui feront la différence ? **La précision, la rapidité d'exécution, la créativité.**

À cela s'ajoute une difficulté supplémentaire : gérer le stress occasionné par les visiteurs qui défilent en nombre. La compétition constitue en effet un véritable défi qui nécessite une grande maîtrise de soi.

PLANNING DES FINALES NATIONALES 2020 :

- **Dimanche 13 Décembre 2020** : Arrivée de toutes les délégations régionales sur Lyon
  Les déplacements sont organisés par chaque délégation

- **Lundi 14 Décembre 2020** : Visite du site de compétition, familiarisation avec vos espaces de travail et cérémonie d'ouverture

- **Mardi 15 Décembre 2020** : 1er jour de compétition
- **Mercredi 16 Décembre 2020** : 2ème jour de compétition
- **Jeudi 17 Décembre 2020** : 3ème jour de compétition

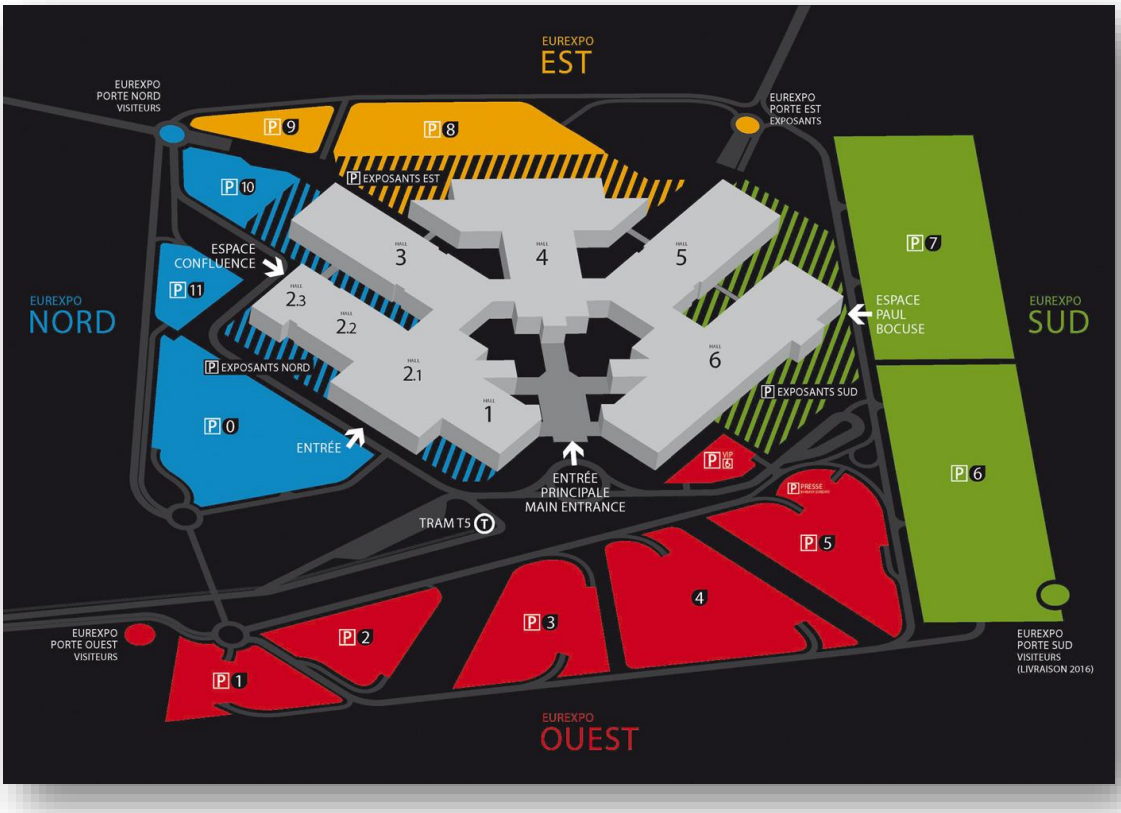
Le planning détaillé et personnalisé vous sera transmis par votre Expert Métier

- **Jeudi 17 Décembre 2020** : Cérémonie de clôture et annonce des résultats

- **Vendredi 18 Décembre 2020** : Réunion entre l'encadrement de WorldSkills France, les jeunes médaillés et leurs Jurés pour présenter la suite de l'aventure.

PRESENTATION DU SITE DE COMPETITION

EUREXPO LYON



PRESENTATION DES DOCUMENTS IMPORTANTS

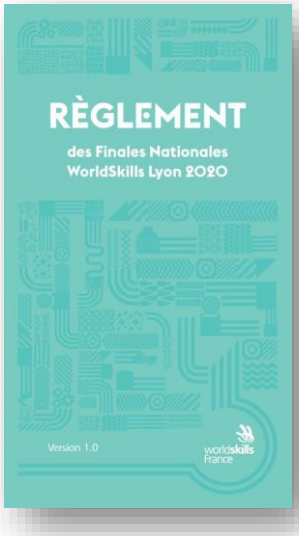
Pour performer durant les épreuves des finales nationales, la seule maîtrise technique ne suffit pas. Une bonne connaissance du règlement des finales nationales, ainsi que du descriptif technique, vous permettra de vous familiariser avec l'environnement de la compétition et d'adopter les bonnes attitudes durant les épreuves.

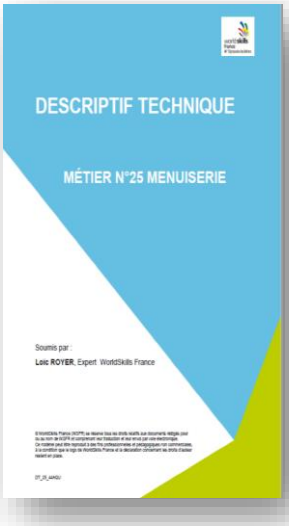
Le règlement des finales nationales de Lyon 2020

Le règlement des finales nationales rassemble l'ensemble des règles à respecter avant et pendant la compétition. Il précise également les règles de sélections et donne la définition du rôle et des missions de chaque acteur.

Le descriptif technique du métier

Le descriptif technique est propre à chaque métier. Ce document précise le cadre de la compétition et des épreuves à réaliser pendant les 3 journées du concours.





Ces documents sont accessibles en libre téléchargement depuis le site de WorldSkills France (www.worldskills-france.org) dans l'onglet « La Compétition » puis dans l'onglet « Les métiers en compétition ». Cliquez ensuite sur votre métier et téléchargez les documents dont les liens se trouvent en haut à gauche de la page.

Vous trouverez également dans cet onglet les anciens sujets de compétition propres à votre métier utiles pour vos entrainements.

CONSEILS DE PREPARATION TECHNIQUE

Damien Naviliat - Expert pour le métier Cybersécurité

Les métiers de la Cybersécurité sont multiples, et le niveau requis pour intégrer l'équipe de France est exigeant.
Parmi les métiers de la cybersécurité on citera le hardening de systèmes, services et réseaux, l'audit de sécurité d'une infrastructure et de services applicatifs (red team), le reverse engineering, la cyberdéfense (blueteam). Afin d'atteindre le niveau d'excellence requis pour intégrer l'équipe de France, votre duo devra être cohérent, communiquer très efficacement et réussir tous les challenges, sans l'aide d'internet, avec un haut niveau d'exigence.

Afin de vous aider à vous préparer à ce niveau d'excellence, je vous propose des exercices que vous devrez vous efforcer de savoir reproduire à la perfection et qui sont pensés pour vous préparer au mieux pour la compétition nationale, en vue de la compétition internationale. Les exercices proposés ne représentent pas la totalité des éléments que vous devez connaitre, ils sont majoritairement consignés dans le descriptif technique du métier, cependant, j'ai souhaité mettre l'accent sur les éléments qui nécessitent une attention particulière après lecture du descriptif technique.

EXERCICE 1 – HARDENING LINUX - REMOTE LOGGING

- Prérequis : Distribution CentOS

  Configurer un serveur CentOS (s1) pour qu'il envoie ses logs à distance sur un second serveur (s2), en sécurisant les communications au moyen d'un certificat. Les messages en provenance de s1 doivent être placés dans un dossier tel que /var/log/s1.log

Mots clé pouvant être utiles : certtool, rsyslog, elinks, chronyd
Délai de réalisation attendu finales nationales : 1h15
Délai de réalisation attendu finales internationales : 45 mins

EXERCICE 2 – HARDENING LINUX - REGLES D'AUDIT

- Prérequis : Distribution CentOS

Configurer une consignation systématique de toute saisie que pourrait effectuer l'utilisateur root au clavier, quel que soit le mode d'accès au système.

Toutes les modifications sur ou dans le dossier /etc doivent être monitorées.

Les règles d'audit doivent être "immutable"

Mots clé pouvant être utiles : pam, auditctl, ausearch
Délai de réalisation attendu finales nationales : 1h30
Délai de réalisation attendu finales internationales : 45 mins

EXERCICE 3 – HARDENING LINUX - VPN

- Prérequis : Distribution CentOS

Etablir un serveur OpenVPN (s1) et configurer s2 pour être un client VPN de s1.

Vous prendrez soin de tester plusieurs variantes pour établir le VPN : connexion par certificat, par utilisateur/certificat, par user/mot de passe, plusieurs sessions distinctes avec le même certificat.

Mots clé pouvant être utiles : easy-rsa
Délai de réalisation attendu finales nationales : 1h30 mins
Délai de réalisation attendu finales internationales : 45 mins

EXERCICE 4 – HARDENING LINUX - SECURISER GRUB

- Prérequis : Distribution CentOS

Sécuriser GRUB en y associant des utilisateurs et mots de passe, un utilisateur pourra modifier les entrées de GRUB, l'autre pourra choisir les entrées présentées, mais pas les modifier.

Mots clé pouvant être utiles : superusers
Délai de réalisation attendu finales nationales : 20 mins
Délai de réalisation attendu finales internationales : 10 mins

EXERCICE 5 – HARDENING LINUX - LUKS

- Prérequis : Distribution CentOS

Ajouter une partition au système, et la configurer comme un volume chiffré (via luks), ce volume sera monté de façon persistante dans le dossier /myluks

Mots clé pouvant être utiles : cryptsetup,
Délai de réalisation attendu finales nationales : 30 mins
*Délai de réalisation attendu finales internationales : 2*0 mins

EXERCICE 6 – HARDENING LINUX - SELINUX

- Prérequis : Distribution CentOS

Configurer un serveur FTP (vsftpd) sur un système SELinux

Mots clé pouvant être utiles : semodule, sestatus, semanage
Délai de réalisation attendu finales nationales : 1h15
Délai de réalisation attendu finales internationales : 45 mins

EXERCICE 7 – HARDENING LINUX - POLITIQUE DES MOTS DE PASSE

- Prérequis : Distribution CentOS

Appliquer la politique de mots de passe suivante : Les mots de passe doivent contenir au moins 2 Chiffres et 2 Majuscules, et doivent avoir une longueur d'au moins 12 caractères. Aucun utilisateur ne pourra avoir plus de 2 sessions ouvertes, sauf l'utilisateur "lambda" qui aura droit à 5 sessions.

Après 4 essais infructueux, un compte sera bloqué pour 5 minutes, un rapport contenant tous les accès infructueux sera envoyé toutes les heures à l'utilisateur root.

Délai de réalisation attendu finales nationales : 45 mins

Délai de réalisation attendu finales internationales: 30 mins

EXERCICE 8 – HARDENING LINUX - AUTHENTIFICATION CENTRALISEE

- Prérequis : Distribution CentOS

Un serveur d'authentification (s1) est équipé de freeIPA, il assigne des UID qui commencent à l'UID 4000. Les mots de passe expirent au bout de 10 jours, et les 10 derniers mots de passe ne pourront pas être réutilisés en cas de changement de mot de passe. Seul le premier utilisateur créé pourra utiliser ssh pour se connecter sur d'autres systèmes (par exemple depuis le serveur s2 vers s1).Le premier utilisateur dans IPA pourra faire sudo sur la commande fdisk, le second utilisateur pourra faire seulement sudo sur fdisk mais que s'il est sur une troisième machine (s3).

Mots clé pouvant être utiles : freeipa, ipa-server, ipa-client
Délai de réalisation attendu finales nationales : 45 mins

Délai de réalisation attendu finales internationales : 30 mins

EXERCICE 9 – HARDENING LINUX - PARTAGE

- Prérequis : Distribution CentOS

Créer un dossier /partage sur s1n et y accéder depuis s2, le dossier sera protégé par krb5p.

Mots clé pouvant être utiles : nfs-server
Délai de réalisation attendu finales nationales : 20 mins

Délai de réalisation attendu finales internationales : 10 mins

EXERCICE 10 – HARDENING LINUX – GPG

- Prérequis : Distribution CentOS

Créer une clé gpg pour un utilisateur (lambda1) et l'exporter pour un second utilisateur (lambda2). Créer un fichier (secret.txt) avec lambda2, il sera chiffré avec l'export réalisé pour lambda1. Lambda1 doit pouvoir lire ce fichier.

Mots clé pouvant être utiles : easy-rsa
Délai de réalisation attendu finales nationales : 20 mins

Délai de réalisation attendu finales internationales: 10 mins

EXERCICE 11 – ROOTME/HACKTHEBOX

- Prérequis : Compte gratuite sur le site root-me.org

Cette plateforme est "freemium", l'ensemble des exercices pour des comptes gratuits est totalement en phase avec l'étude de bien des domaines de la cyber-sécurité, je vous invite à réaliser le maximum d'exercices sur cette plateforme. Ces exercices vont renforcer un large panel de vos compétences. Si vous ne disposez que peu de temps libre, prenez soin de faire le maximum d'exercices relatif à la sécurité du code et applications.

En parallèle, et dès que vous aurez considéré avoir bien avancé sur rootme, je vous invite à vous inscrire sur le site hackthebox.eu, ici encore un compte gratuit est suffisant, vous disposerez de vraies machines à compromettre, de plusieurs challenges.

Temps à consacrer à cet exercice : autant que possible !

EXERCICE 12 – BLUETEAM – SECURITY ONION

- Une VM Security Onion

Installez une VM security onion, puis rejouez dedans les traces pcap ci-dessous, enfin cherchez à analyser : Les adresses (IP/MAC) source et destination incriminées dans l'attaque, ce qu'il est réalisé par l'attaquant. Les scénarios peuvent être variés...Vous aurez besoin des outils majeurs de securityonion pour effectuer vos analyses (Sguil/Squert ou Kibana, Wireshark, Bro, CapMe).

https://ee.lbl.gov/anonymized-traces.html

https://github.com/elcabezzonn/Pcaps

Un très gros travail proposé par FIRST en 2015 :

La doc :

https://download.netresec.com/pcap/FIRST-2015/Hands-on_Network_forensics.pdf

Les traces :

https://download.netresec.com/pcap/FIRST-2015/FIRST-2015_Hands-on_Network_Forensics_PCAP.zip

L'objet principal des exercices est de vous former à comprendre au moyen d'un NSM des attaques (ici elles sont rejouées via des PCAP dans security onion), de les qualifier, de cerner les attaquants et les équipements visés. Snort n'est pas sensé détecter systématiquement ce qu'il se passe (ou seulement une partie), à ce titre Kibana (outil de threat hunting) sera d'un grand secours.

En fonction du temps dont vous disposez, apprenez à personnaliser les règles SNORT pour mieux détecter les anomalies. Pour rappel, SNORT est un IDS opensource, et sa documentation suffit à apprendre à écrire les règles convenablement.

Temps à consacrer à cet exercice : Autant que nécessaire, jusqu'à ce que vous arriviez à cerner ce qu'il se passe dans ces traces PCAP. Vous pouvez uniquement utiliser Wireshark mais ce sera beaucoup plus long).

EXERCICE 13 – FORENSIC WINDOWS/LINUX

Vous devrez être en mesure de mener une live et dead analysis sur des postes soit windows, soit linux. L'objectif de la live analysis est de valider si une attaque s'est réellement déroulée sur un système et de prélever les premiers éléments système allumé. L'objectif de la dead analysis est d'analyser les dumps de mémoire et disque afin de retrouver les indices de compromission de l'attaque.

Un bon entrainement est avec la VM victoria de honeynet.org

-> Création du profil pour volatility: https://github.com/BuckBoost/volatility_victoria

Les images ne sont plus disponibles sur le site du concepteur, mais se trouvent encore ici: https://lepouvoirclapratique.com/big/vms/forensics/Forensic_Analysis_of_a_Compromised_Server.zip

Les questions pour ce challenge étaient les suivantes :

What service and what account triggered the alert? (1pt)
What kind of system runs on targeted server? (OS, CPU, etc) (1pt)
What processes were running on targeted server? (2pts)
What are attackers IP and target IP addresses? (2pts)
What service was attacked? (1pt)
What attacks were launched against targeted server? (2pts)
What flaws or vulnerabilities did he exploit? (2pts)
Were the attacks successful? Did some fail? (2pts)
What did the attacker obtain with attacks? (2pts)
Did the attacker download files? Which ones? Give a quick analysis of those files. (3pts)
What can you say about the attacker? (Motivation, skills, etc) (2pts)
Do you think these attacks were automated? Why? (1pt)
What could have prevented the attacks? (2pts)
Temps estimé pour s'approprier cet exercice : 35 heures

EXERCICE 14 – MALWARE ANALYSIS

Last but not least, re reverse engineering est également une composante importante de cette compétition.

Que vous procédiez avec ida (free ou pro edition), ghydra, immunity debugger, GDB, EDB, cuckoo sandbox, vous devez être capable d'effectuer la rétro ingénierie de malwares simples, et suite à cette analyse, d'indiquer ce que fait ce malware.

Un grand nombre d'ouvrages existent sur le sujet, mais je préfère vous orienter vers ce livre : https://nostarch.com/malware qui est excellent.

Un grand nombre d'ateliers y sont présents, je vous invite à en réaliser le plus possible.

https://practicalmalwareanalysis.com/labs/

Si vous rencontrez des difficultés, vous pouvez vous baser sur ces réponses :

https://github.com/sully90h/practical-malware-analysis

Temps estimé à consacrer à cet exercice en vue des finales nationales : 70 heures

EXERCICE 15 – AUDIT D'UNE INFRASTRUCTURE WINDOWS AD

- Connaissance de powershell type 'administrateur' (remote session, WMI, fournisseurs)

Connaissez-vous Mimikatz, bluehound, powershell empire ? Ces outils sont très utilisés pour auditer une infrastructure Windows AD.

Pour vous approprier ces outils, vous devrez installer un LAB composé à minima d'un serveur active directory, d'un ou deux clients, sur lesquels vous créerez des administrateurs locaux. Si possible, vous installerez un serveur SQL serveur qui sera intégré à l'active directory. Sur l'AD, vous créerez plusieurs comptes, dont des comptes administrateur délégués. Certains de ces comptes doivent s'être connectés sur des machines clientes.

Vous devrez générer des golden et silver tickets afin de gagner un maximum de droits sur toutes les machines (idéalement les droits administrateurs AD).

L'idée est de toujours démarrer depuis un PC client AD pour lequel vous n'avez qu'un compte "simple utilisateur". L'exercice est certes biaisé, car c'est vous qui créez le lab et les comptes, cependant vous devez maitriser ces processus pour la finale nationale.

BlueHound vous permettra de réaliser une cartographie de l'AD rapidement.

Si vous disposez de suffisamment de ressources, et si vous avez le temps, je vous invite, à créer plusieurs forêts, créer des approbations entre elles, et essayer de compromettre l'ensemble.

Afin de vous aider dans votre démarche de création de folden et silver tickets, je vous conseille les excellents documents ci-dessous :

- https://adsecurity.org/?p=556
- https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection-wp.pdf

Temps estimé à consacrer à cet exercice en vue des finales nationales : 70 heures, plus si vous ne connaissez pas powershell, et le double si vous construisez un laboratoire avec plusieurs forets.

EXERCICE 16 – SIEM SPLUNK

Vous devez être capable d'installer un SIEM splunk, transmettre à splunk les logs de vos équipements actifs et passifs du réseau.

Vous pouvez télécharger une version d'évaluation de Splunk entreprise ici :

https://www.splunk.com/en_us/download/splunk-enterprise.html

Et si vous avez du temps, tester durant 7 jours la version enterprise security une fois que vous aurez réussi à forwarder vos évènements dans splunk avec la version démo :

https://www.splunk.com/page/sign_up/es_sandbox?redirecturl=/getsplunk/es_sandbox

NB : Il est attendu que vous puissiez également interfacer splunk avec l'HIDS Wazuh.

NB2 : Les établissements scolaires peuvent demander une version complète de splunk (mais limitée en débit, rapprochez-vous de votre équipe pédagogique).

Temps à consacrer à cet exercice : 30 heures pour la configuration, et la prise en main.

EXERCICE 17 – BUFFEROVERFLOW

La recherche et l'exploitation de failles de type buffer overflow sous linux et windows est nécessaire dans cette compétition.

Afin de vous préparer, je vous invite à tester la machine vulnérable Tr0ll2 que vous pourrez trouver sur le site https://www.vulnhub.com/

Le même mécanisme est à répéter pour Windows, je vous conseille de vous préparer avec l'application vulnserver disponible ici: https://github.com/stephenbradshaw/vulnserver

Délai de réalisation attendu finales nationales : 2 heures
Délai de réalisation attendu finales internationales : 1 heure

EXERCICE 18 – COMMUNIQUER AVEC VOTRE BINOME

Vous ne pourrez pas maitriser totalement l'ensemble de ces compétences pour la finale nationale, c'est la raison pour laquelle la compétition en CyberSécurité se réalise en binôme. Il est indispensable que chacun ait des connaissances dans tous les domaines, cependant, il est préférable que vous approfondissiez les éléments en fonction des affinités des membres du binôme.

Le jour de la compétition nationale, la qualité des réalisations dépendra de votre préparation technique, mentale et physique, mais aussi grandement sur votre capacité à communiquer ensemble de façon rapide, concise et...discrète !

Il est donc fortement conseillé de réaliser des sessions de travail régulières avec votre binôme afin d'apprendre à communiquer ensemble et vous partager les activités !

CAISSE A OUTILS

Voici la liste des outils et équipements que vous êtes autorisés à emmener puis à utiliser pendant la compétition :

Aucun équipement n'est nécessaire, tout vous sera fourni le jour des épreuves. Vous pouvez prévoir une paire de bouchons pour oreilles, mais ceci vous empêchera de communiquer avec votre binôme !

CONSEILS DE PREPARATION PHYSIQUE ET MENTALE

STEPHANE RAYNAUD - PREPARATEUR DE L'EQUIPE DE FRANCE DES METIERS

Pour atteindre l'excellence, il vous faut une excellente préparation technique, un outillage performant et une bonne connaissance des documents de compétition mais il vous faut également une bonne condition physique et mentale. Le contexte d'une compétition génère fatigue et pression et pour y parer, il vous faut vous y préparer. Voici quelques conseils à suivre en complément de la préparation physique et mentale organisée par votre délégation régionale :

1 - Conservez le CAP pour « gagner sa place en Equipe de France des Métiers » :

« Je me fixe des objectifs quotidiens, hebdomadaires et mensuels »

2 - Gagnez en régularité :

« Je tiens un suivi quantifiable et rapidement observable du nombre d'heures d'entrainement par semaine et par mois »

3 - Sortez de votre zone de confort :

« Je transforme l'exception du dépassement de soi en dépassement de soi au quotidien : physiquement, mentalement et techniquement »

4 - Gagnez techniquement et évaluez chaque entrainement :

« Je chronomètre mes entraînements et tiens un classeur de scores avec un maximum de données : dates, meilleurs chronomètres à la seconde, nombres de répétitions, scorer les qualités… »

5 - Gagnez physiquement :

« Je m'entraine en endurance 2 à 3 fois par semaine et intègre de courts exercices de renforcement musculaire dans mon quotidien »

6 - Gagnez mentalement :

« Je veux devenir la meilleure version de moi-même au quotidien en construisant mes états d'esprit et attitudes de performance »

7 - Gagnez en esprit de compétiteur :

« Je me challenge très (très) régulièrement en créant ou en acceptant des défis pour perfectionner mon mental à travers la gestion de situations compétitives. »

8 - Soignez votre hygiène de vie et votre santé :

« Je gagne du « terrain positif » sur ma santé au quotidien : alimentation équilibrée, sommeil régulier, limitation de l'alcool, du tabac, instauration d'une dynamique de préparation physique »

9 - Créez votre bulle de préparation :

« Je m'entraîne en restant concentré, focus et pleinement présent sur mon objectif du jour … ma rigueur est égale à ma propre exigence »

10 - Entourez-vous de gens positifs :

« J'ai une grande responsabilité dans le fait d'associer les personnes proches et compétentes pour m'accompagner et m'encourager dans mon projet »

Et n'oubliez pas…

…il n'y a que dans le dictionnaire que « Réussite » arrive avant « Travail »

Bonne préparation !