Bonjour, je suis **Michel KARTNER** et j'ai créé ce document pour vous permettre d'accéder à divers liens/fichiers/programmes que vous trouverez tout au long des vidéos du cours que vous visionnez.

IMPORTANT [À LIRE AVANT DE CONTINUER]

- ➔ Par l'évidente volatilé des liens sur Internet, il se peut que certaines informations soient devenues **obsolètes** depuis, ou le deviennent ensuite.
- ➔ Je m'efforce à rendre ce document à jour, mais le meilleur moyen d'obtenir de l'aide et du contenu à jour est de vous rendre sur https://cyberini.com/.
- ➔ La plupart des étudiants choisissent d'opter pour le PACK de cours complet (dont les cours futurs qui seront accessibles **sans frais**)

Rejoignez Cyberini aujourd'hui et bénéficiez des avantages suivants :

- Des **Quiz** et **Challenges** pour vous entraîner
- Un **Support en ligne pour poser vos questions**
- Du contenu **mis à jour régulièrement**
- Une **Attestation de Complétion** à la fin de chaque cours
- Des formations **Qualifiantes** ou **Certifiantes**
- La possibilité d'apprendre TOUT sur le hacking éthique, l'anonymat en ligne et la programmation en un seul endroit.

Cliquez ici pour acquérir le pack complet et apprendre Tout sur le hacking éthique à -30% (réservé aux lecteurs de ce guide)

Vous pourrez voir le sommaire complet de tous les cours en cliquant sur le lien ci-dessus, ainsi que les bénéfices que vous pourrez en tirer. Mais si vous avez des questions, le support est là pour vous : support@cyberini.com.

Voici pourquoi il est intéressant d'apprendre la sécurité informatique

- Bounty Factory : https://bountyfactory.io/fr/index.html
- Akaoma (certification CEH) https://www.akaoma.com/formation/ceh-certified-ethical-hacker
- EC-Council (organisme officiel) https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

  Vos compétences seront **très intéressantes sur le marché du travail**, je vous le démontre à travers quelques exemples en vidéo. Vous verrez notamment que les offres d'emploi en sécurité informatique sont **très nombreuses**. La situation est inverse par rapport à d'autres jobs plus classiques : les employeurs **ne trouvent pas assez de monde**, et vos compétences sont donc très recherchées, on se battra pour vous et non pas l'inverse !

  ATTENTION: suite à certains malentendus, je précise tout de même que ce cours (comme n'importe quel autre cours) ne vous rendra pas automatiquement expert en sécurité ni même ne vous assurera automatiquement une place sur le marché du travail ! Il faut tout de même beaucoup de pratique et de l'expérience, mais avec de l'envie et de la détermination, rien n'est impossible !

Piégez maintenant vos systèmes et découvrez si vous avez été piraté(e) !

- Grabify : https://grabify.link/
- IPLogger : https://iplogger.org/
- Le fichier PDF « Endroits où placer votre piège » vous donnes des exemples de placements.
- Détecter une intrusion n'est PAS empêcher une intrusion. La technique présentée dans cette vidéo vous permet de récupérer une adresse IP d'un potentiel coupable pour entamer diverses démarches (par exemple un dépôt de plainte ou une preuve à un dossier). Les solutions de sécurité doivent être utilisées en conséquence pour lutter concrètement contre les intrusions détectées.

Vulnérabilités, Menaces et Exploits

- Liste des identifiants CVE sur Mitre.org : https://cve.mitre.org/
- Exemple vulnérabilité Wordpress CVE 2016-5834 : https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5834
- Exploit PHP Mailer : https://www.exploit-db.com/exploits/40969

Télécharger et Installer Virtualbox

- https://www.virtualbox.org/wiki/Downloads

- Lien vers la documentation officielle et à jour pour installer Virtualbox sous Windows, Mac et Linux (en anglais) : https://www.virtualbox.org/manual/ch02.html#idm856
- Manuel d'utilisateur pour Virtualbox en Français : http://download.virtualbox.org/virtualbox/UserManual_fr_FR.pdf

Installation Facile de Kali Linux en tant que machine virtuelle sous Windows

- Téléchargez ici le fichier .OVA pour Virtualbox : https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/
- Résolution de soucis : voir la vidéo appelée **"Résoudre les erreurs courantes avec Virtualbox & Kali Linux"**
- En cas de soucis récalcitrants (voir les sujets déjà créés) : https://forums.kali.org/
- Forum Kali Français : https://www.kali-linux.fr/forum/index.php
- Ce que doit contenir votre fichier /etc/apt/sources.list après installation : https://docs.kali.org/faq/kali-sources-list-faq

Premiers pas avec Kali Linux

- Apprendre en détail (Kali) Linux : https://openclassrooms.com/courses/reprenez-le-controle-a-l-aide-de-linux
- Si pas de ping : désactiver le pare-feu Windows et tester d'autres mode de connexion (pont ou NAT). Voir les autres pistes dans la session sur l'installation de Metasploitable, ou dans la vidéo de dépannage des erreurs courantes.
- Les commandes de base : https://doc.ubuntu-fr.org/tutoriel/console_commandes_de_base

Télécharger et Installer Metasploitable

- Lien de téléchargement : https://sourceforge.net/projects/metasploitable/

Si vous rencontrez un problème de connexion (ping) entre machines virtuelles et/ou machine hôte, vérifiez les points suivants :

- Les adresses IP sont-elles associées et appartiennent-elles au même sous-réseau ? Essayez la commande **ifconfig** sous Metasploitable et Kali (et Mac), et **ipconfig** sous Windows. Vous devez voir une adresse Ipv4 du type 192.168.1.X avec X variant par exemple sous chaque machine. S'il n'y a pas d'adresses IP, éteignez toutes les machines virtuelles et redémarrez votre box Internet puis réessayez. S'il y a des adresses IP de sous-réseaux différents, observez les paramètres réseau dans Virtualbox pour chaque machine virtuelle, et choisissez bien le mode de connexion par pont. Puis redémarrez-

les. Au pire, choisissez le mode de connexion NAT pour temporairement débloquer la situation.
- Vérifiez que le pare-feu de la machine virtuelle Windows soit désactivé. Pour cela, vous pouvez passer par le panneau de configuration, ou taper "pare-feu" dans la barre de recherche du menu démarrer Windows (machine virtuelle).
- Si vous avez une carte réseau Wi-fi et que les problèmes persistent, il faut mettre à jour le pilote de la carte et peut-être d'autres pilotes plus généralement (utilisez le site driverscloud.com). Si possible, essayez avec un câble Internet.
- Vérifiez également que votre connexion Internet fonctionne, et que votre box Internet vous autorise les connexions (ce qui peut ne pas être le cas sur certaines installations partagées/publiques).

Télécharger et Installer (gratuitement) une machine virtuelle Windows 7

[IMPORTANT] Mise à jour : N'oubliez pas de **désactiver le pare-feu Windows de la machine virtuelle** et de mettre le mode de connexion par pont dans Virtualbox.

Dernière partie de notre labo : la machine virtuelle Windows 7. Vous allez apprendre comment installer une machine virtuelle Windows 7 100% fonctionnelle et de façon entièrement légale. On pourra ensuite s'en servir pour réaliser nos démonstrations de tests d'intrusion.

- Voir document « Reactiver-win-7-apres-expiration-licence.docx »
- Téléchargez la machine virtuelle ici : https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

Le Google Hacking : Explications et contre-mesures

- http://exif.regex.info/exif.cgi
- http://robots-txt.com/

Le Google Hacking partie 2 (introduction à Shodan et à la recherche Facebook)

- https://www.google.fr/advanced_search
- https://www.exploit-db.com/
- https://www.shodan.io/
- https://tineye.com/

Le cas des adresses e-mail

- Exemple d'une (ancienne) faille dans Hotmail exploitant la sous estimation des adresses e-mail et des questions de sécurité : https://www.leblogduhacker.fr/comment-pirate-pouvait-hacker-un-compte-hotmail/
- Comment créer un alias Microsoft : https://support.microsoft.com/fr-fr/help/12407/microsoft-account-manage-aliases
- Créer un alias avec Gmail : https://support.google.com/mail/answer/22370?hl=fr

Récupérer des informations publiques sur un site web (whois, adresses IP...etc)

- https://www.iplocation.net/
- https://archive.org/
- Introduction aux réseaux informatiques : https://baptiste-wicht.developpez.com/tutoriels/reseau/introduction/
- Introduction à TCP/IP : https://laissus.developpez.com/tutoriels/cours-introduction-tcp-ip/

Collecter et Analyser des données avec Maltego

- https://www.paterva.com/web7/

Utilisation de recon-ng pour accélérer la recherche d'informations

[IMPORTANT] Mise à jour : À 3:45, le serveur DNS visible dans NAMESERVER n'existe plus. Vous pouvez essayer le suivant à la place : **162.159.25.80**. Sinon libre à vous de choisir celui de votre choix. Il existe plusieurs listes de serveurs DNS publics sur Internet, comme https://www.lifewire.com/free-and-public-dns-servers-2626062

Découvrir des services avec NMap

- https://nmap.org/

Se protéger du Scanning réseau (pare-feu Linux)

- Code source du pare-feu fourni dans le dossier de ressources additionnelles (parefeu.zip).
- Documentation d'UFW (Uncomplicated Firewall) : https://doc.ubuntu-fr.org/ufw

UFW permet d'éviter les commandes fastidieuses d'iptables. Voici un exemple commenté d'utilisation de ufw :

```
sudo ufw enable #active ufw
sudo ufw status verbose #affiche les ports/protocoles autorisés/refusés
sudo ufw allow 1234 #autorise l'accès au port 1234
sudo ufw allow https #autorise l'accès au port https par défaut (443)
sudo nano /etc/ufw/ufw.conf #édite les configurations d'ufw
sudo cat /var/log/ufw.log #affiche les logs
sudo ufw deny 53 #refuse un port
sudo ufw app list #affiche la liste des applications pouvant interagir avec ufw
sudo ufw allow in "Apache Full" #autorise l'application apache (autorise automatiquement les bons ports)
```

Découvrir des vulnérabilités Web avec Nikto et les corriger

- https://cirt.net/Nikto2

Découvrir des vulnérabilités Web avec OWASP Zed Attack Proxy (ZAP)

- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Les Bases de Metasploit (architecture et fonctionnalités)

- https://www.metasploit.com/

Metasploit en pratique (exploitation d'une vulnérabilité dans Metasploitable)

NOTE : Si la commande **msfupdate** ne fonctionne pas, c'est que Metasploit a changé ou n'est plus maintenu à jour. Vous pouvez essayer de mettre à jour Metasploit tout entier à la place en tapant les commandes suivantes :
apt update
apt install metasploit-framework
Cette erreur de mise à jour est due à la version 32 bits non maintenue à jour selon : https://blog.rapid7.com/2016/07/06/announcement-end-of-life-metasploit-32-bit-versions/
La solution radicale est de désinstaller la version Metasploit de Kali puis de réinstaller la dernière version officielle via les commandes et procédures suivantes :

- Désinstaller Metasploit avec : **apt remove metasploit-framework**

- Se rendre tout en bas de la page suivante et choisir la dernière version amd64 : https://apt.metasploit.com/
- Télécharger la version et l'installer avec : **`wget https://apt.metasploit.com/pool/main/m/metasploit-framework/metasploit-framework_VOTRE_LIEN_A_JOUR; dpkg -i metasploit-framework_VOTRE_LIEN_A_JOUR`**
- Vous pouvez ensuite mettre Metasploit à jour avec **`msfupdate --force-yes`**

Plus d'informations via le site officiel :
https://metasploit.help.rapid7.com/docs/installing-metasploit-pro

Prise de contrôle à distance de la machine virtuelle Windows 7 (exploitation)

- http://www.oldversion.fr/windows/acrobat-reader-9-0

Mise en place du Système de Prévention d'Intrusion fail2ban (partie 2)

Exemple de fichier jail.local en ressource additionnelle (jail.zip)

Commandes Fail2Ban :

Démarrer, arrêter ou recharger la configuration de Fail2ban:
`service fail2ban start OU stop OU reload`
Obtenir le statut de Fail2Ban :
`fail2ban-client status`
Obtenir le statut d'une prison :
`fail2ban-client status <NOM_PRISON>` exemple `fail2ban-client status sshd`
Vérifier que les règles Fail2Ban fonctionnent :
`fail2ban-regex -v /var/log/apache2/error.log /etc/fail2ban/filter.d/apache-noscript.conf` (remplacer le fichier de log et de conf pour le fichier à tester et les règles à lui appliquer)

Mise en place de notre site web vulnérable sur mesure

- Fichiers sources à utiliser intitulé **sitevulnerable.zip**
- Informations sur les dossiers partagés (Virtualbox) : https://docs.kali.org/general-use/kali-linux-virtual-box-guest

Si des problèmes de connexion se produisent :

- Vérifier qu'apache et mysql soient lancés : **sudo service apache2 start** et **sudo service mysql start**

- Vérifiez également les droits, ou dans le doute faire : **sudo chmod -R 755 /var/www/**
- Vérifiez que la connexion est bien par **pont** (et que les machines se pinguent)
- Vérifier que les fichiers sont au bon endroit, en testant par exemple sur la machine contenant les fichiers sources, que le site soit accessible via http://127.0.0.1/demo/ (ou alors déplacer les fichiers dans le bon répertoire)
- Si besoin de réinitialiser le mot de passe mysql (perdu ou problème de connexion) :

```
1. sudo mysql -u root
2. use mysql;
3. update user set plugin='' where User='root';
4. flush privileges;
5. exit;
```

Démonstration de la faille CSRF, et comment s'en prémunir

- Fichier source « csrf.zip » à utiliser

Scannons notre site vulnérable ! et autres conseils de sécurité des serveurs web

- Fichier source « htaccess.txt » à utiliser.

Introduction à la Sécurité Wi-Fi (notions de WEP, WPA(2), WPS)

[IMPORTANT] Mise à jour : à 3:58, nous parlons de Weplab qui semble ne plus être disponible en ligne. Le voici ci-dessous en téléchargement.

Nous parlerons des mécanismes de sécurité WEP et WPA afin de comprendre comment ils fonctionnent et quelles sont leurs faiblesses. Vous aurez également des notions concernant les WPS.

- Fichier source « weblab.zip » à utiliser.
- Fichiers sources « fichiers-pcap.zip » à utiliser.

La méthode certaine pour savoir si un programme est malveillant ou non

- https://malwr.com/
- https://virustotal.com/
- https://hybrid-analysis.com