Guide TLS-SEC

Sommaire

Magazines / E-zine....2
Podcasts....3
News / Veille....4
Livres....5
Challenges....6
    Root-me....6
    Autres....7
Cours....8
Autres....9

TLS-SEC

Magazines / E-zine

Nom	Idée générale	Commentaire
MISC	Articles sur des cas concrets de l'application de la sécurité (ex: Bonnes pratiques pour un mot de passe robuste, démo de CVE récentes..). Des trouvailles, trucs funs, dossiers d'actualité...	Très bon magazine sur la sécurité dans tous les domaines. Plus adressé aux "passionés" que "grand public". Reste dans l'ensemble accessible avec les connaissances info / réseau (N7 / INSA / etc…).
WIRED	Magazine US couvrant l'actu info, electronique, reseaux sociaux et aussi sécurité	Très complet avec des articles de bon niveau en sécurité notamment. Permet de prendre connaissance de sujets emergents à creuser.
Phrack http://phrack.org/	E-zine	"Phrack est un magazine électronique underground international de langue anglaise édité par et pour des hackers depuis 1985." Référence en la matière, tous les numéros depuis 1985 sont disponibles sur le site. On citera "*Smashing the stack for fun and profit*"

Podcasts

Lien	Contenu	Commentaire
NoLimitSecu	Podcasts hebdomadaires, francophones. Chaque épisode est centré sur un thème / attaque récente...	Sujets variés, format sympa (20min à 1h, audio), en français, pas mal pour se tenir informé sur le thème de la sécurité. Auteurs : passionnés, chercheurs, pros...
Comptoir Sécu	Podcast mensuel, par trois ingé en sécurité. Traite des sujets autour du thème de la sécurité, veille / news, invités, présentation de conférences sécu...	Un peu moins technique que NoLimitSecu. Et un peu plus “fouilli” à écouter, mais reste sympa, avec des thèmes différents.
Sophos Security	En anglais, discussion sur les faits sécu du mois. Pas technique plus culturel.	Bien pour se tenir au courant des faits. Et on peut chercher pour plus de détails.

News / Veille

Lien	Contenu	Commentaire
Comptes Twitters	A trier selon les tweets mais mine d'or de la veille et pour faire des blagues de sécurité informatique. Gros partages de connaissances, quelques comptes pour commencer (complément choisi au hasard parmi des centaines mais vous permettra de follow ceux dont le sujet vous intéresse)	Tous les comptes officiels (ANSSI, NIST, cecyf, blogueurs, blabla et les boites qui vous intéressent). Et les particuliers : @InfosecurityMag, @hacks4pancakes, @da_667, @FioraAeterna, @binitamshah, @jeromesaiz, @Cyb3rOps , @Hexacorn, @geeknik, @aeris22, @nixcraft, @kevinmitnick, @0xmitsurugi, @OkotoSecure, @SwiftOnSecurity (<3), @Snowden, @J0hnnyXm4s, @lojikil @pentesteur (pour les trolls)
Quelques flux RSS qui peuvent être intéressants à suivre (juste quelques uns…)	Blogueur (en) : Mad Irish Blogueurs (fr) : Korben (à trier) / Zataz Kaspersky Lab : alerte/news + interview/articles Data Security Breach : idem LeMagIT: ContentSyndication RSS Feed Krebs on Security	
https://news.ycombinator.com/	News populaire sur l'informatique. Top des news avec vote des users.	Il y a de tout mais les trucs de sécu montent très vite !
http://www.information-security.fr/	Blog en français avec plein de ressources.	
TechWorm	News en anglais, surtout autour de la sécurité (thème principale) mais aussi élargi sur d'autres thèmes liés.	Site actif et articles de bonne qualité.

Livres

Titre	Thème	Commentaire
Hacking: The art of exploitation (Jon Erickson)	Programmation (du C), Réseau (TCP/IP), failles logicielles, défense, Shellcode, cryptographie (un peu)	Vraiment bien de le lire avant d'arriver (en préparation aux cours de V. Nicomette et S. Duverger). Reprend rapidement le C depuis quasi zéro puis des notions d'OS pour aller vers les exploitations de buffers overflows etc. La VM "fournie" avec le livre ne marche plus.
Metasploit, sécurité et hacking	Framework Metasploit décrit par ses créateurs.	Beaucoup de choses illustrées sur Metasploit. Très sympa à lire, mais plutôt pour la culture perso (pas forcément à lire avant la rentrée pour se préparer).
Black Hat Python, Justin Seitz	Scripting python pour le réseau et le système (Voir sommaire).	Cool pour approfondir / découvrir Scapy. Dans l'ensemble accessible même en ayant fait peu de python, le code est toujours bien commenté. Peu de python à TLS-SEC, ou de programmation réseau donc sympa à lire pour la culture perso. Exemple de début : comment (et pourquoi) se faire un client netcat en python, un traceroute,...
Security Power Tools	Sécurité réseau	Assez long (800 pages) mais couvre énormément de sujets (et peut être lu de façon non linéaire). Grands axes = Reconnaissance, Monitoring, Discovery, Penetration, Control & Defense. Il couvre et approfondi des notions vues en TP à l'ENAC à tls-sec (ou d'autres vues en 2A TR N7 par ex et en modapp). Contenu "mixte" entre théorie et pratique, l'avantage c'est que beaucoup de choses théoriques sont illustrées (fonctionnement de certains logiciels et API etc…) par contre, certains (peu) sont obsolètes (edition en 2007). Il peut aussi bien être lu en parallèle de beaucoup de cours que pour tester / approfondir / élargir chez soi. Aspects réseau, info, système,…
Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation	Reverse engineering	Livre de référence en matière de reverse engineering.

Challenges

Root-me

Catégorie	Nom des challenges	Commentaire
App - Système	Tous les ELF32 (buffer overflow, BSS overflow, format string) → Vont de paire avec le cours de V. Nicomette (et le TP concernant tout ça).	Possible de commencer après avoir lu Hacking the art of exploitation par exemple et sinon dans l'année (cf cours V. Nicomette).
Programmation	Les premiers puis jusqu'à ce qu'il se fasse tard… Principe : Donner des (bonnes) réponses automatiques à un bot IRC.	Pratique pour se remettre à la programmation réseau, en particulier le premier, les suivants se ressemblent. Permet de se remettre au choix au python, C,...
Web - Serveur	Intéressant à regarder, challenges / vulnérabilités assez "connues" dans l'ensemble, difficulté croissante. Peu d'aspect web à tls-sec donc surement bien de (re)regarder sur des challenges comment ça marche. Exemple : parameter tampering, injection SQL, injection LDAP, local / remote file inclusion...	Pas mal quand on a déjà fait du développement web, pourquoi pas en complément avec CodeSafe (voir plus bas). Permet de découvrir / revoir des pratiques à éviter en développement web.
Web - Client	De paire avec web - serveur, vulnérabilités "classiques" côté client. Peu de challenges dans cette catégorie donc peut-être pas mal de regarder du côté d'autres sites de challenge ex : xss-game.	Bien pour apprendre / revoir des "trucs et astuce" web.
Réalistes	Majoritairement des challenges web qui reprennent des principes de challenges web - serveur notamment. Truc super : des challenges sur VM pour rendre le challenge plus "réaliste" (voir section CTF). Exemple de démarche : exploiter une vulnérabilité d'un cms + LFI + bruteforce ssh + escalade de privilège → flag.	Peut être un peu laborieux si on a jamais fait de web, mais en s'entraînant on se prend pas mal au jeu. +++ pour les VM.
Réseau	Les 5 premiers : Analyse de trames Wireshark pour mettre en avant les faiblesses de certains protocoles. La suite : Soit besoin "d'outils" réseau différents de wireshark, soit casse-têtes liés à des protocoles ou "tricks" réseaux (un peu) plus compliqués.	

Autres

OverTheWire	Fonctionnement différent de root-me, pas d'inscription requise et pas de score. Les challenges sont regroupés par "branche". Chaque branche contient des challenges autour d'un thème de difficulté croissante, qu'on doit résoudre dans l'ordre (le flag du challenge 1 donne accès au challenge 2). L'avancée est plus progressive que sur root-me.	Les branches bandit et leviathan par exemple sont bien pour se familiariser avec les commandes bash et le fonctionnement de Linux, facile et progressif. La branche narnia contient des challenges du genre buffer overflow. Beaucoup d'autres "branches" existent.
SSTIC		
Volatility Plugin Contest		

Cours

Intitulé / Lien	Aperçu	Commentaire
Coursera cryptography Stanford	Cours vidéo par un prof de Stanford très complet, allant des bases jusqu'à des choses poussées (concepts, maths, …). NB : Un module (ex : RSA) = ~2h de vidéo pour une semaine divisées en bout de 10 à 20 min environ.	Bien à regarder en parallèle du cours de cryptographie de début d'année, permet de revenir sur certains trucs chez soi.
Coursera cryptography maryland university		Bien à regarder en parallèle du cours de cryptographie de début d'année, permet de revenir sur certains trucs chez soi.
Coursera programming for everybody	Cours sur la programmation, permet de connaitre qq bases de python	Bien pour compléter ses connaissances sur le dev logiciel.
SafeCode https://training.safecode.org/courses	Accès gratuit et sans inscription à quelques cours vidéos de 40min~. Exemple de thème de vidéo : "Secure Memory Handling in C 101", "Product Penetration Testing 101", "Permissions 101: Linux and OS X"	Les vidéos sont de "grosses" introductions à des thèmes assez variés. SafeCode (membres : Adobe, Intel, Symantec...) produit des vidéos à titre d'info et de sensibilisation. Peu de vidéos pour l'instant.
A security Site : www.asecuritysite.com	Cours : Beaucoup, beaucoup de cours, très complet, beaucoup de thèmes -> Crypto, réseau, analyse de formats de fichiers, forensics. Liens vers beaucoup de ressources sur chaque thème (vidéos, soft…) Autres : Des trucs sûrement utiles pour la certification Cisco, des challenges, des guides...	Site d'un prof d'info / sécu à l'université d'Édimbourg, cours en lignes et pas juste des introductions. Bien en parallèle de certains cours (crypto, réseau…).

Autres

Hacker's manifesto	http://phrack.org/issues/7/3.html
Hacking team (news intéressante)	Intro : http://www.zataz.com/piratage-de-hacking-team-explique Source : http://www.pastebin.com/raw/0SNSvyjJ