**MDfeOrganisation DS SSI**

Règles du drive :

* Première colonne : intitulé de la question. Premiers mots + un screen.
* Deuxième colonne : la/ les réponses probables (vert si sûr, jaune si doute)
* Troisième colonne : commentaire
* 4 eme colonne : mettez un I si vous êtes d’accord. Une barre par personne.

**En cas de questions successives (genre on peut pas revenir en arrière):**

* Ne pas paniquer
* Rentrer sa question, chercher la réponse.
* Une fois que l’on a trouvé la réponse, on travail sur les questions des autres pour les aider.
* On avance petit à petit avec les autres afin de construire la correction ensemble.
* La discipline et l’organisation aideront tout le monde, y compris les meilleurs.

NE PAS OUBLIER :

* si on a 25-30% de fausses réponses, on a encore entre entre 14 et 15. Donc pas de stresse. L’entraide nous sauvera.
* On est une équipe avant tout.
* Il n’y a d’enjeux que de valider l’année, pas de compétition.
* **DOCUMENT DE SECOURS :** [Cliques ici](https://docs.google.com/document/d/1no0_Vv-n1KZjbBDPn_GFYBj2LOMkyYrdhfFpSfhb2a0/edit) **Si qq copie les questions on peut chercher (pour les gens qui ont pas encore commencer)**

C’EST à REPONSES MULTIPLES

robustessepremier

|  |  |  |  |
| --- | --- | --- | --- |
| Question | Réponse(s)  <= L'icône tout à droite | Commentaire | Vote de validation |
| Question ouverte - Dans le cadre de l’analyse de la robustesse de mot de passe (de leur hash) quel est la  méthodologie à suivre ?  Décrivez les différents types d’attaques et dans quel ordre les utiliser. | La méthodologie à suivre consiste en des audits afin de verifier la robustesse du mot de passe  Les différents types d'attaque sont  -Bruteforcebr  -Dictionnary  -Rules attack + dictionnary attack  -Rainbow tables  -Mask Attacks |  |  |
| Réponse unique - Parmi les fichiers suivants, quels est le fichier à récupérer pour casser les mots de passe locaux  d’un poste de travail Windows ?  Veuillez choisir au moins une réponse :  a. PASSWD  b. HKLM  c. LSASS  d. SAM | B ?  PASSWD  SAM d’  apres googlpe  SAM d’après google pour moi aussi  SAM aussi | LSASS?  (c’est etc/passwd en principe) => ça c’est pour Linux !  Oui pardon c SAM ducoup |  |
| Vous souhaitez scanner les 2500 ports UDP les plus fréquemment utilisé sur le serveur cible | Le dernier sur  C’est C, -sU scan les ports UDP, -sS scan TCP SYN | Nmap le dernier ? lequel?  C’est C je suis d’accord |  |
| *Question ouverte -* Via le moteur de recherche Google, vous souhaitez trouver dans des répertoires  nommés "ECE", des documents PDF, dont le titre contient "Confidentiel". Quelle requête effectuez-  vous | site:ece.fr  allintitle: Confidentiel filetype:pdf  [confidentiel site:ece.fr] filtetype:pdf | C faux ptn  C tendu |  |
| Réponse unique - Vous êtes l’utilisateur "user1" d’un système GNU/Linux récent. Vous souhaitez iden- tifier les fichiers présents dans le répertoire "/etc" qui appartiennent à l’utilisateur "root" et sur lesquels vous disposez de droits d’écriture. Quelle commande pouvez-vous utiliser ?  Veuillez choisir au moins une réponse :  a. find /etc -type d -user root -perm -o=w  b. find /etc -name root -perm=write  c. find /etc -type f -user root -perm -o=w  d. find /etc -name root -perm=0666 | find /etc -type f -user root -perm -o=w  C bien celui avec f, car il va chercher les FICHIERS et pas le DIRECTORY  net | Sur? | +1 |
| *Réponses multiples* – Sur un réseau interne sans accès à Internet, quels outils peuvent être utilisés  pour analyser la configuration TLS d’un service web ? | a. ssllabs  b. openssl  c. sslconf  d. nmap | Sslconf aussi  Non c nmap et ssllabs |  |
| Réponse unique - Sur quoi se base la cryptographie asymétrique (public key algorithm) ? | Veuillez choisir au moins une réponse :  a. Des problèmes mathématiques complexes (factorisation, courbes elliptiques, etc.)  b. Des autorités de certification  c. Des certificats publiques  d. Un secret commun | Il ,y a pas le secret commun aussi?  Non ça c’est symétrique |  |
| Réponse unique - Sur un système GNU/Linux récent, vous êtes parvenus à extraire un fichier contenant  ces mots de passe dans un format "sécurisé". Quelle est le premier type d’attaque que vous lancez ? | a. exhaustive (bruteforce complet)  b. dictionnaire  c. canal auxiliaireha1  d. rainbow table |  |  |
| *Réponses multiples* - Vous avez tenté d’exploiter une vulnérabilité de type Injection SQL sur la fonc-  tionnalité de recherche de jaipasdidee.com. Quel comportement peut vous indiquer la présence d’une  potentielle injection SQL ? | d. un temps de réponse important  a. l’apparition du logo du système de gestion de base de données sur la page requêtée | J’aurais dit apparition erreur string not terminated car la string n’est pas finie  Les deux en jaune sont fausses je pense |  |
| *Réponses multiples* - L’utilisation d’une injection tautologique pour exploiter une injection SQL. . . | a. tente d’injecter des données erronées dans le but d’obtenir des informations sur le type des variables, le nom des tables, etc.  b. tente de forcer la requête à retourner plusieurs résultats dans l’évaluation d’une clause WHERE  c. peut permettre de valider un formulaire d’authentification sans connaissance du mot de passe légitime  d. consiste en l’utilisation d’une assertion toujours vraie | Sure ?  Je pense que c’est les deux autres perso  Pareil je dirai c et d Tautologique c’est toujours vrai, “qui n’apporte aucune information”  Pareil je pe  C et D |  |
|  | Sure  Déjà en haut |  |  |
| Question ouverte – Dans le cadre des permissions Unix, que signifie le bit de contrôle SETUID ? Dans  le cas d’un exécutable apparte"sénant à l’utilisateur « root » et rendu setuid par l’administrateur système,  quel est le risque de sécurité associé exploitable par un attaquant possédant un compte utilisateur sur  le système ? |  |  |  |
| Question ouverte – Dans le cadre des permissions Unix, que signifie le bit de contrôle SETUID ? Dans  le cas d’un exécutable appartenant à l’utilisateur « root » et rendu setuid par l’administrateur système,Li  quel est le risque de sécurité associé exploitable par un attaquant possédant un compte utilisateur sur  le système ? | Si un fichier avec ce bit est exécuté, l'uid (gid) sera modifié par le propriétaire.  Le risque de sécurité associé est le fait qu'un attaquant avec un compte utilisateur puisse devenir root à son tour.  (no copy paste pls) |  |  |
| Réponse unique - Sur un système GNU/Linux récent, vous êtes parvenus à extraire un fichier contenant  ces mots de passe dans un format "sécurisé". Quelle est le premier type d’attaque que vous lancez ? | Veuillez choisir au moins une réponse :  a. dictionnaire  b. canal auxiliaire  c. exhaustive (bruteforce complet)  d. rainbow table | Franchement j’ai mis dictionnaire |  |
| Réponse unique - Sur un système GNU/Linux récent, les mots de passe sont stockés. . . | a. cryptés dans /serieusement/n/utilisez/pas/ce/terme/il/est/tres/moche  b. chiffrés dans /etc/passwd  c. chiffrés dans /etc/security/password  d. hachés dans /etc/shadow |  |  |
| **Autorité de certification** | Je valide les réponses |  | l |
| *Réponses multiples* - L’attribut Content-Type. . . | a. est modifiable par l’utilisateur  b. permet d’apporter des informations sur le format de fichier envoyé  c. est défini côté serveur  d. est envoyé en HTTP GET  e. est défini côté client | B  Pour moi il est définit cote client  Modifiable apr l’utilisateur  Defini cote client |  |
| éponses multiples - Quels sont les propriétés d’une « bonne » fonction de hashage ? | a. Éviter les collisions  b. Deux entrées semblables (quelques bits de différence) auront une sortie très différente  c. La fonction est à sens unique  d. La taille de sortie dépend de la taille de l’entrée |  |  |
| Réponse unique - Sur un système GNU/Linux récent, qu’est ce que les capabilités ? | 1. *Une manière de lancer des processus privilégiés sans les privilèges root* 2. Un ensemble d’outils pour l’analyse réseau 3. Une manière d’obtenir directement des droits root 4. Un algorithme de hashtage pour le stockage des mot de passe |  |  |
| Sur un système GNU/Linux récent les mots de passes sont stokés ... | A- chiffré dans /etc/passwd  B- chiffré /etc/security/password  C - haché dans /etc/security/password  B- haché dans /etc/shadow | SHADOW SÛR 100% |  |
| Les caractères suivant peuvent être utilisés pour commenter la fin d’une requête SQL : (rep multiples) | #  --  Sûr pour ces 2 là |  |  |
| Réponse unique- Bob possède la clé RSA suivante : clé publique RSA(143,7) et clé privée RSA(142,103) quelle est la formule mathématique permettant de chiffrer un message C à destination de Bob ?  Note: le symbole “^” est utilisé comme exposant. | 1. C^7 mod 143 2. C^143 mod 7 3. C^103 mod 143 4. C^143 mod 103 | Réponse B  J’aurais dis c  Qulequ’un a dit la A plus haut  DU coup? Les inters disent A | Le cours :  RSA by example Public key is RSA(143,7) Private key is RSA(143,103) Bob publish his public key RSA(143, 7) to the world.  Alice want to send a message to Bob: C = Me mod n: C = 467 mod 143 = 84  Bob can read Alice message: D = Cd mod n: D = 84103 mod 143 = 46 |
| Question ouverte - Décrivez la méthodologie permettant de décrypter un chiffrement de Vigenere ? | 1) analisée le le text et retrouver les bigramme/trigramme revenant souvant.  2) clalculer la distance entre chaque meme bigramme/trigramme.  3) decomposer les distance en facteur premier et en deduire la longueur de la clé (m)  loop :  4) extraire toute les lettre module m  5) analyser la frequence des lettre  6) comparer les frequence avec les frequence de lettre dans le language courant  7) continuer en changeant de première lettre a extraire jusqua avoir trouver la clé | Chaque meme?? |  |
| Modifier les permissions du fichier /var/log/ideabox | chmod u+w-r /var/log/ideabox  Chmod -R +w /var/log/ideabox  Chmod 622 /var/log/ideabox | Non u cest que pour le propriètaire  1ère ou 2ème ?  C’est laquelle des deux? |  |
| Vous souhaitez modifier les permissions du fichier /var/log/ideabox |  | PAS DE SCREENS, COPIE COLLE  Ok |  |
| Réponse multiple - Vous venez d’obtenir un accès à faibles privilèges sur un système GNU/Linux. Vous cherchez à identifier des mots de passe présents sur le système pour, éventuellement, élever vos privilèges. Quels binaires pouvez-vous utiliser pour faire cette recherche ? | Grep  Locate je dirai |  |  |
| Question ouverte - Lors d'un test d'intrusion sur une application web developpee en PHP, vous identifiez un formulaire permettant de deposer un commentaire. Cote serveur, la verification est realisee par le code ci-dessous. Quel principe et quelle payload utilisez-vous pour contourner le mecanisme de securite ?  <?php  header ("X-XSS-Protection: 0");  // Is there any input? if( array\_key\_exists( "name", $\_GET ) && $\_GET[ 'name' ] != NULL )1 II Get input $name = str\_replace( '<script>', ", S\_GET[ 'name' ] );  /I Feedback for end user $html .= "<pre>Hello $InameWpre>"; 1  ?> | Injection SQL |  |  |
| Vous souhaitez savoir si vous pouvez communiquer au travers du protocole SMTP avec le serveur $CIBLE. Vous pouvez utiliser la commande. . . | d. nmap -sS -p 25 $CIBLE  ? rien de s ur | 25 car port SMTP |  |
| *Réponses multiples* - Une application web cherche à se protéger contre l’envoi de fichiers malveillants en réalisant une liste noire d’extensions interdites. Vous parvenez à identifier que les extensions suivantes sont interdites : html, php, php3, php4, php5. Parmis les propositions ci-dessous, quelles tentatives supplémentaires pourraient vous permettre d’envoyer un webshell que vous pourrez ensuite invoquer pour compromettre le serveur ? | a. webshell.php%00.jpg d. webshell.php.jpg |  |  |
| Réponses multiples - Une autorité de certification. . . | Tout sauf “partage sa clef privée” |  |  |
| Sur un système GNU/Linux récent,les mots de passe sont stockés… (réponse unique)  a. chiffrés dans /etc/passwd  b. hachés dans /etc/shadow  c. hachés dans /etc/security/password  d. cryptés dans /serieusement/n/utilisez/pas/ce/terme/il/est/tres/moche  e. chiffrés dans /etc/security/password | Hachés dans etc shadow |  |  |
|  |  |  |  |
| Réponse unique - La procédure xp\_cmdshell… | Veuillez choisir au moins une réponse :  a. peut permettre d’exécuter des commandes sur le système d’exploitation hébergeant le système de gestion de bases de données  b. offre un moyen sécurisé d’exécuter des commandes sur le système de gestion de bases de données  c. doit être activée pour assurer la sécurité du système  d. est spécifique au SGBD Oracle | A (très dangereux/non sécurisé)  ou b | | |
|  | SAM |  |  |
| Réponse multiples - Parmi les fonctions de hashage suivantes lesquels sont recommandées pour le stockage  de mot de passe ? | SHA1 MD5  Faux c’est bcrypt et MD5 et argon2 | MD5 non | I |
| Reponse unique - Quelles sont les communautés SNMP par défaut ? | public / private |  | I |
| Réponse unique - Bob possède la clé RSA suivante : clé publique RSA(143,7) et clé privée RSA (143,103)  quelle est la formule mathématique permettant de chiffrer un message C à destination de Bob ? | C^7 mod 143 |  |  |
| Parmi les fonctions de hashage suivantes lesquels sont recommandées pour le stockage  de mot de passe ? | a. bcrypt  b. SHA1  c. MD5  d. argon2 |  |  |
| Quels outils peuvent être utilisés scan vulnérabilité | Nmapsql  Nessus  (on valide) |  | +1 +1 1 |
| *Question ouverte* — Nous nous plaçons dans le cadre d’une exploitation d’une vulnérabilité de type  injection SQL. L’attaquant à la possibilité d’exécuter la requête suivante :  Select \* from comments where name = ‘’UNION select users, password from logins ;  Le message d’erreur suivant est renvoyé par le système :  Mysql : Column count doesn ’ t match value  L’attaquant n’ayant la possibilité de modifier uniquement la partie en gras de la requête, comment  peut-il modifier sa requête afin de la rendre valide ? | Afin que la requête soit valide, il doit modifier sa requête tq il retire le signe "="  Sur ?  Le = n’est pas en gras  Il ne peut y avoir qu’un résultat après le = ? La il en envoie plusieurs | QL |  |
| Réponses multiples - Les caractères suivants peuvent être utilisés pour commenter la fin d’une requête  SQL | # et -- |  |  |
| Les mots de passes au format LM sont ils vulnerables au rainbow table pourquoi | Oui les mot de passes au format LM sont vulnérable aux attaques par rainbow table.  En effet le hash LM n'est pas tres sécurisé et est vite cracké par les rainbow table |  |  |
| Réponse unique - Sur un système GNU/Linux récent, qu’est ce que les capabilities ? |  |  |  |
| Question ouverte - Vous obtenez une capture réseau et souhaitez, dans Wireshark, mettre en évidence  le trafic FTP échangé par 10.0.0.1 et 10.0.0.2. Quel filtre de recherche pouvez-vous utiliser ? | IP.src = 10.0.0.1 & IP.dst = 10.0.0.2 | ??  Follow TCP-stream |  |
| *Question ouverte* - Lors d’un test d’intrusion sur une application web développée en PHP, vous identifiez un formulaire permettant l’envoi de fichiers. Côté serveur, la vérification est réalisée par le code ci-dessous. Quel principe utilisez-vous pour contourner le mécanisme de sécurité ?    if( isset( $\_POST[ 'Upload' ] ) ) {  // Where are we going to be writing to?  $target\_path = DVWA\_WEB\_PAGE\_TO\_ROOT . "hackable/uploads/";  $target\_path .= basename( $\_FILES[ 'uploaded' ][ 'name' ] );  // File information  $uploaded\_name = $\_FILES[ 'uploaded' ][ 'name' ];  $uploaded\_type = $\_FILES[ 'uploaded' ][ 'type' ];  $uploaded\_size = $\_FILES[ 'uploaded' ][ 'size' ];  // Is it an image?  if( ( $uploaded\_type == "image/jpeg" || $uploaded\_type == "image/png" ) &&  ( $uploaded\_size < 100000 ) ) {  // Can we move the file to the upload folder?  if( !move\_uploaded\_file( $\_FILES[ 'uploaded' ][ 'tmp\_name' ], $target\_path ) ) {  // No  $html .= '<pre>Your image was not uploaded.</pre>';  }  else {  // Yes!  $html .= "<pre>{$target\_path} succesfully uploaded!</pre>";  }  }  else {  // Invalid file  $html .= '<pre>Your image was not uploaded.  We can only accept JPEG or PNG images.</pre>';  }  }  ?> | Afin de contourner le mécanisme, on peut réaliser un Cross-Site Scripting qui équivaut à <img src="URL = document.cookie" /> (en HTML)  Pas plutôt insertion d’un fichier.php.jpeg …? |  |  |
| Quelle approche apporte à elle seule le meilleur niveau de protection contre les injections sql? | ?? |  |  |
|  |  |  |  |
| Quels sont les propriétés d’une « bonne » fonction de hashage ?  Veuillez choisir au moins une réponse :  a. Éviter les collisions  b. Deux entrées semblables (quelques bits de différence) auront une sortie très différente  c. La taille de sortie dépend de la taille de l’entrée  d. La fonction est à sens unique | Éviter les collisions  Éviter les collisions  La fonction est à sens unique  Deux entrées semblables (quelques bits de différence) auront une sortie très différente  La derniere aussi non? |  |  |
|  |  |  |  |
| Réponse multiples - Parmi les fonctions de hashage suivantes lesquels sont recommandées pour le stockage  de mot de passe ? | argon 2 + bcrypt |  |  |
|  |  |  |  |
| Quels outils peuvent etre utilises pour realiser un scan de vulnerabilite | Nmap  Nessus |  | inject |
| gnu/liinux qu’est ce que le path | Le path correspond au chemin vers les fichier/programmes. Ces chemins nous permettent d'executer une commande sur le terminal. |  |  |
| *Réponse unique -* Quelle approche apporte, à elle seule, le meilleur niveau de protection contre les  injections SQL ? (NdA : ne pas considérer pour autant qu’une de ces solutions est suffisante pour protéger  une application contre les injections SQL) |  |  |  |
|  |  |  |  |
| Réponse unique - Vous souhaitez savoir si vous pouvez communiquer au travers du protocole SMTP avec le serveur $CIBLE. Vous pouvez utiliser la commande. . . | (pas sur du tout) |  | I |
| Question ouverte - Vous souhaitez modifier les permissions du fichier /var/log/ideabox afin que tous les  utilisateurs puissent y écrire, mais que seul le propriétaire puisse en lire le contenu. Quelle commande  chmod utilisez-vous ? |  |  |  |
| Sur un réseau interne sans accès à Internet, quels outils peuvent être utilisés  pour analyser la configuration TLS d’un service web ? |  |  |  |
| Sur un sustème GNU/Linux, qu’est ce que le PATH? Détaillez ses fonctions et comment le PATH peut être exploité |  |  |  |
| Question ouverte - Décrivez la méthodologie permettant de décrypter un chiffrement de Vigenere ? | Cela nécessite une clef  On déchiffre par soustraction des lettres. On soustrait la première lettre du message à la première de la clef (modulo 26 si il y a uniquement des lettres). Le résultat est la lettre correspondante (également fesable via un tableau) |  |  |
| Parmi les fonctions de hashage suivantes llesquels sont recommandées pour le stockage de mot de passe | Sha1 md5 |  |  |