**Organisation 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 stress. L’entraide nous sauvera.
* On est une équip e avant tout.
* Il n’y a d’enjeux que de valider l’année, pas de compétfition.

|  |  |  |  |
| --- | --- | --- | --- |
| Question | Réponse(s)  <= L'icône tout à droite | Commentaire | Vote de validation |
| You tried to exploit a SQL injection vulnerability on the search functionality of noidea.com Which behavior my indicate the presence of the potQL injection ?  Veuillez choisir au moins une réponse :  a. The appearance of an error like « ORA-01756: quoted string not properly terminated »  b. The appearance of the SQL database’s logo on the requested page  c. The appearance of an error like « UPLOAD\_ERR\_NO\_TMP\_DIR » on the page  d. A long response timen | A & C |  | I |
| Which solutions brings, by herself, the best protection against sql injections ? | Use prepared statement |  |  |
| Bob RSA(143,7) , (143,103), how to encrypt ? | C⁷ mod 143 |  |  |
|  |  | manque un morceau mais j’ai envie de dire :  Je crois :  [confidential site:ece.fr] filtetype:pdf |  |
| On a GNU/Linux operating system, you managed to extract the passwords hashes | Bruteforce ,not sure  Moi je pense la a | Moi je dirai dictionary (tu testes les mdp les plus connu, avant de tester CHAQUE combinaison)  bruteforce c’est tres tres long contrairement a bruteforce donc d’abord dictionnary |  |
| Open question - Are the passwords in the LM format vulnerable to rainbow table attacks ? Why ? | LM is vulnerable to the rainbow tables crack hashes because it uses a dictionary tables | Yes for lengh password <= 14  **Oubliez pas de reformuler un peu** |  |
|  | Common secret il parait |  |  |
| *One answer only* - On GNU/Linux system, the passwords are stored in  Veuillez choisir au moins une réponse :  a. /etc/security/password  b. /etc/security/password  c. /etc/shadow  d. /etc/passwd | Non juste la c  Juste la c | The [/etc/passwd](https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/) is the password file that stores each user account. The [/etc/shadow](https://www.cyberciti.biz/faq/understanding-etcshadow-file/) file stores contain the password information for the user account and optional aging information | I |
| What are the properties of a good hash function?   1. Avoid collision   b.Outputd depends of input size  c.2 similar inputs will have diff outputs  d.Function is one way only | a,c,d |  |  |
| *Multiple answers* - A certification authority. . .  Veuillez choisir au moins une réponse :  a. is a trusted organization  b. signs digital certificates  c. is trusted by the web browsers  d. share its private key with everyone | A trusted organization  Signs digital certificated  Is trusted by the web browers  (tous sauf “share ..”) |  | hashes |
| *Open question -* You wish to modify the permission of the /var/log/ideabox file so that every user may  write in it by only its owner might be able to read the file’s content. Which chmod command do you use ? | chmod u+w-r  /var/log/ideabox |  |  |
| Open question — In the case of the exploitation of an SQL injection. You have the possibility to exploit  the following request :  Select \* from comments where name = **‘’UNION select users, password from logins** ;  The following error message is send back by the application :  Mysql : Column count doesn ’ t match value  You can only change the bold part of the request. How can you modify it in order to discard the  error ? | Alors ?  #  -- |  |  |
|  | B,c  J’aurais dit c & d |  |  |
| The statement xp\_cmdshell: | May allow to execute commands on the OS hosting the database | Je suis ok  La mm |  |
| The following characters might be use to comment the end of an SQL request   1. || 2. -- 3. “ 4. # | B and D |  |  |
|  |  |  |  |
| On a GNU/Linux system, what is the PATH ? Detailed its functions and how the path  might be exploited ? | The PATH corresponds to the path to the files or programs. These paths allow us to execute an order on the terminal. |  |  |
| *Multiple answers* - The Content-Type attribute. . .  Veuillez choisir au moins une réponse :  a. can be modified by the user  b. allow to send more information about the uploaded file format  c. is send in HTTP GET  d. is defined server sideWire/log  e. is defined client side | Dans le body donc HTTP GET ? client side ?  Je pense c’est a, b, e (voir screen à droite)  Http post non d’apres screen ? |  |  |
| Vulerability scan tools ? | Nessus, Wireshark, nmap |  |  |
| A web APPLICATION is protection itself agains malicious file upload using a black list of forbidden extension. You are able to identify forbidden extnetion html php,php3,pp4 ,php5 among proposition, which one could allow you tu upload a webshell that you will be able to invocate in order to compromise the serve?  a.webshell.php%00.jpg  B.webshell.php.jpg  C.webshell.html5  d.webshell.jpg.php | a. webshell.php%00.jpg  d. webshell.php.jpg  Ils ont mis ca en FR mdrr |  |  |
| *One answer only* - You wish to scan the top 2 500 UDP ports used on the $TARGET server. You  use. . .  Veuillez choisir au moins une réponse :  a. nmap -sVC –top-ports=2500 $TARGET  b. nmap -Pn -PP -PE –top-ports=2500 $TARGET  c. nmap -sS –top-ports=2500 $TARGET  d. nmap -sU –top-ports=2500 $TARGET | d |  |  |
| One answer only - You are the user “user1” of a GNU/Linux system. You want to identify the file in the /etc/ directory that belong to the root user on which you have the write permissions. Which command do you use?   1. find /etc -name root -perm=0666 2. find /etc -name root -perm=write 3. find /etc -type d -user root -perm -o=w 4. find /etc -type f -user root -perm -o=w | D  Find /etc -type f -user root -perm -o=w |  |  |
| One answer only - What are the foundation of the asymetric cryptography (public key algorithm) ?  a. complex mathematical problems (factorisation, elleptic curve. . . )  b. a common secret  c. certification authorities  d. public certificates | Public certificates ? | A verifier ca se contredit  I think it is D  Looked on Wikipedia  A) parce que c'est hyper long à trouver la clé privée à partir de la clé publique | I |
| Multiple answers - You just obtain a low privilege access on a GNU/Linux System. You wish to identify  the passwords on the filesystem in order to eventually escalate your privileges. Which binaries can you  use to realize this research | Grep  Find --> | Findstr c’est pour Windows  <https://doc.ubuntu-fr.org/locate> | I |
| Open question - In the case of the exploitation of an SQL injection. You have the possibility to exploit the following request:  Select \* from comments where name = **Union select users, password from logins”**  The following error message is send back by the application:  Mysql: collumn count doesnt match value  Change the bold part to discard the error | ? |  |  |
| os*Multiple answers* - The usage of a tautology injection to exploit an SQL injection. . .  Veuillez choisir au moins une réponse :  a. try to inject faulty data in order to obtain information on the variable type, the table name, etc.  b. try to force the request to return more than one result in the evaluation of a WHERE request  c. may allow to validate an authentication form without knowing the legitimate password  d. is the usage of a always true assertion | C et D | D  ”tautology is a formula or assertion that is true in every possible interpretation. An example is "x=y or x≠y".”  En vrai on s’en fiche que ça retourne plusieurs resultats dans le WHERE donc C ET D  okey |  |
| You want to know if you can communicate using SMTP protocol with the TARGET server. You can use command…  a )Nmap -sS p25  b) nmap -sV-p 123  c) nmap -sU -p 53  d) nmap -PS53.. | a |  |  |
|  |  |  |  |
| Multiple Answers - Among the following hashes function which one are advised to be use to store passwords  a. SHA1  b. bcrypt  c. argon2  d. MD5 | SHA1 MD5 |  |  |
| On an internal network without access to internet which tools can be used to analyze the TLS config of a web application?  A.nmap  B.openssl  C.sslconf  d.ssllabs |  | Nmap  Ssl conf |  |
| Identify the file in the /etc/directory that belong to root user | A |  |  |
| Which are the default SNMP community ? | public / private |  |  |
|  |  |  |  |
| Open question - Dunging a penetration test on a web application written in PHP, you identify a form  allowing to share a comment. The check function is realized server side by the following code. Which  principle and which payload do you use to bypass the security mechanism ?    <?php  header ("X-XSS-Protection: 0");  // Is there any input?  if( array\_key\_exists( "name", $\_GET ) && $\_GET[ 'name' ] != NULL ) {  // Get input  $name = str\_replace( '<script>', '', $\_GET[ 'name' ] );  // Feedback for end user  $html .= "<pre>Hello ${name}</pre>";  }  ?> | We can use this kind of injection : "or" 1 = 1 --  "or" 1 = 1 -- |  |  |
| You obtain a network capture(pcap) and using Wireshark, yopu want to highlight the FTP traffic between 10.0.0.1 and 10.0.0.2. Which research filter do you use? | ftp and ip.addr==10.0.0.1 && ip.addr==10.0.0.2 |  |  |
| Open question - With the Google search engine, you want to find, in directory named "ECE", PDF  documents with the keyword "Confidential" in their title. Which request do you use ? | allintitle: Confidential filetype:pdf  [confidential site:ece.fr] filtetype:pdf  Intitle plutot que allintitle, je pense |  |  |
|  | A B |  |  |
| One answer only - On a GNU/Linux system what are capabilities?   1. Tools for network analysis 2. A way to launch privileged process without the root privileges 3. A way to directly obtain the root permissions on the system 4. A hash algorithm to store passwords | B  source in the script: |  | I |
|  |  |  |  |
| SNMP Communities | Public and private |  |  |
|  |  | <https://www.wordfence.com/learn/how-to-prevent-file-upload-vulnerabilities/> |  |
| *Open question* - Describe the methodology for the Vigenere cipher cryptanalysis | It uses a polyalphabetic substitution.  Instead of monoalphabetic substitition (Ceasar cipher cryptanalysis), it codes a message with a key.  And the final message is chiphered.  If we don't know the key, try to find the lenght of the key by calculating the index of coincidence.  Otherwise, use the Vigenere table |  |  |
| What is SETUID bit ? if a binary belong to the root user the setuid bit, what is the associated security risk that maybe exploited by the attacker with auser account on the system? | Allows user to have rights like the owner in a program |  |  |
| *Multiple answers* - Which tools might be use to execute a vulnerability scan ?  Veuillez choisir au moins une réponse :  a. Wireshark  b. John the ripper  c. nmap  d. Nessus | Wireshark  Nessus | NMAP - saw that in the script  So it is NESSUS AND NMAP - C and D |  |
| *One answer only -* You want to know if you can communicate using the SMTP protocol with the  $TARGET server. You can use the command. . .  Veuillez choisir au moins une réponse :  a. nmap -sV -p 123 $TARGET  b. nmap -sU -p 53 $TARGET  c. nmap -sS -p 25 $TARGET  d. nmap -PS53,123,161 -PU80,443 -PP -PE $TARGET | c |  |  |
| Properties of a good hashes function |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| *One answer only* - Which file, among the followings, is necessary to retrieve in order to crack local  passwords on a MS Windows workstations ?  Veuillez choisir au moins une réponse :  a. SAM  b. HKLM  c. LSASS  d. PASSWD | SAM |  |  |
| *Multiple answers* - A web application is protection itself against malicious file upload using a black list  of forbidden extensions. You are able to identify that the following extensions are forbidden : html, php,  php3, php4, php5.  Among the propositions bellow, which one could allow you to upload a webshell that you will be able to  invocate in order to compromise the server ? | c. webshell.php%00.jpg  d. webshell.php.jpg |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |