Tema 3

Ce trebuie să știu? Studiați secțiunea de Cunoștințe evaluate și suportul agregat necesar temei. Nu contactaţi responsabilii de temă pe mail privat decât dacă aceştia vă cer explicit (e.g. pentru debugging local, vizualizarea unor comenzi din rezolvare) Pentru orice fel de întrebare **vă rugăm folositi forumul**!

Thread nou? Nu. Pentru o ușoară parcurgere a mesajelor, folosiți thread-urile de discuții existente în cadrul forumului, fără a crea altele. În consecință, thread-urile (subiectele de discuții) nou create vor fi șterse.

Căutare. Căutați pe forum informația pe care doriți să o obțineți, înainte să puneți o întrebare. De cele mai multe ori, cineva a mai întrebat același lucru. În fiecare thread al forumului aveți informații despre cum puteți căuta în forum.

Printscreen/poză? Nu. În cazul în care doriți să publicați un printscreen pe forum, recomandăm folosirea site-urilor pentru partajarea gratuită a imaginilor, precum imgur [http://imgur.com/] sau alternativele [http://www.makeuseof.com/tag/4-imgur-alternatives-for-uploading-sharing-images/] sale, publicând pe forum doar link către printscreen. Pozele inserate în răspunsuri, vor fi șterse. **NU SE ACCEPTA POZE FACUTE CU TELEFONUL** (se poate recurge la depunctări, sunt imposibil de urmărit).

Actualizări. Urmăriți în special forumul, în topic-urile dedicate taskurilor respective. Urmăriţi şi modificările aduse enunțului/checker-ului, modificări ce sunt publicate și explicate în paragrafele de mai jos.

Regulament. Înainte și în timpul realizării temei, vă rugăm să parcurgeți indicațiile legate de realizarea temelor, încluzând ce înseamnă o temă copiată și cum penalizăm temele copiate. Folosiți cu încredere forumurile de pe cs.curs.pub.ro [http://cs.curs.pub.ro/] pentru întrebări și neclarități legate de teme.

Întrebări frecvente. În timpul realizării temei, când vă loviți de probleme și aveți nevoie de suportul echipei de USO, parcurgeți și lista de întrebări frecvente întâlnite în cadrul temelor. Să țineți cont, va rugăm, și de recomandările de comunicare electronică.

Ajutor reciproc. Vă încurajăm ca atunci când găsiți soluția la o problemă pe care ați postat-o anterior pe forum să postați și soluția găsită. De asemenea dacă știți răspunsul la întrebările colegilor sunteți încurajați să le răspundeți. Studenţii cu o atitudine pozitivă, activă şi care îşi ajută colegii pot fi răsplătiţi cu puncte karma sau un PIN USO.

Înainte și în timpul realizării temei, vă rugăm să parcurgeți indicațiile legate de realizarea temelor, încluzând ce înseamnă o temă copiată și cum penalizăm temele copiate. Folosiți cu încredere forumurile de pe acs.curs.pub.ro [http://acs.curs.pub.ro/] pentru întrebări și neclarități legate de teme.

În timpul realizării temei, când vă loviți de probleme și aveți nevoie de suportul echipei de USO, parcurgeți și lista de întrebări frecvente întâlnite în cadrul temelor. Să țineți cont, va rugăm, și de recomandările de comunicare electronică.

Informații generale

Deadline: **23 Decembrie, ora 23:55**
Punctaj: **1.0 puncte** din nota finală

Actualizări enunț:

- s-a lansat versiunea inițială

Actualizări checker: versiunea 1.0.0

- s-a lansat versiunea inițială

Suportul necesar pentru realizarea temei

- Pe parcusul acestei teme vom folosi cunoștințe generale legate de scripting și securitate (mai precis spargerea parolelor, decriptare vs. decodificare, hashing), dar și comenzi uzuale de lucru în linia de comandă, așa că verificați laboratoarele aferente înainte să vă apucați de această temă.

Testarea temei. Finalizarea temei. Mașină virtuală.

La task-ul 2, pentru a primi toate punctele, trebuie salvate parolele *decodificate* (nu decriptate) în wordlist_decoded.txt (atenție la trailing whitespaces).

Este interzisă publicarea pe forum a comenzilor sau pozelor care fac parte din rezolvarea parțială sau integrală a temei ori a unui task. Dacă e necesar acest lucru vă rog să contactaţi în privat responsabilii de temă, la specificarea explicită a acestora pe forum!

Aveţi voie, însă, să sugeraţi diferite abordări pe care mergeţi sau să daţi idei generale (dar nu comenzi sau fişiere shell script) celorlalţi chiar direct pe forum. Încurajăm clarificarea lucrurilor între studenţi atât timp cât nu sunt rezolvate cerinţele în mod direct.

Urmăriți indicațiile legate de realizarea temelor. La prima abatere studentul primește un avertisment, iar punctajul obținut pe temă îi este redus cu valoarea punctajului pe task-ul respectiv. Începând cu a doua abatere, se va anula întregul punctaj pe tema curentă. Temele anterioare sau cele viitoare nu vor fi afectate. Abaterile se păstrează pe parcursul semestrului. Ori de câte ori se încalcă această regulă, se va ține cont de istoricul abaterilor. Abaterile vor fi actualizate în catalog.

Este interzis studenților să modifice parametrii de rulare ai mașinii virtuale. Orice tentativă malițioasă de modificare a fișierelor și executabilelor care fac mașina virtuală sa ruleze in parametrii optimi (fișierele si folderele ce nu țin de enunțul temei curente), ne conferă dreptul de a oferi 0 puncte pe temele respectivului student.

Task 01 (10p)

Task-urile 2 și 3 sunt dependende de rezolvarea corectă și completă a Task-ului 1. În primele 3 task-uri vom simula trecerea prin mai multe filtre de securitate - de cele mai multe ori, pentru a ajunge la informația pe care o dorește, un atacator va avea de trecut mai multe bariere (firewalls, parole, drepturi limitate ale utilizatorului compromis etc.). În cele ce vor urma, vom încerca să ajungem la un fișier ascuns în 3 arhive protejate de parole.

- În directorul `/home/student/tema3-sec` se află `arhiva1.zip`, protejată de o parolă simplă. Folosiți un utilitar precum fcrackzip sau john the ripper pentru a extrage fișierele din aceasta. Lungimea parolei căutate este de 6 litere.

Task 02 (15p)

- În interiorul arhivei se află un fișier, `wordlist.txt`, și `arhiva2.zip`, pe care trebuie să o dezarhivați la rândul ei. Pentru aceasta, trebuie să vă folosiți de fișierul wordlist.txt, singura problemă este că parolele din el sunt criptate cu OTP/XOR [https://en.wikipedia.org/wiki/XOR_cipher], cu cheia `usostrongkey`. Criptarea cu xor este foarte simplă, presupune realizarea operației xor între textul în clar și cheie, decriptarea realizându-se prin aplicarea xor între textul cifrat și cheie.
- Mai mult, după criptare, cifrurile au fost codificate în base64 [https://en.wikipedia.org/wiki/Base64]. Codificarea este diferită de criptare, neascunzând datele, ci doar trecându-le într-un alt format (baza 64 în acest caz fiind formată din caracterele A-Z, a-z, 0-9 și +/) pentru a fi mai ușoară prelucrarea sau afișarea lor. Scopul acestui task este să decodificați și să decriptați parolele din wordlist pentru a le folosi în spargerea arhivei 2.
- Dacă vă este mai ușor, puteți realiza un script care să facă aceste operații. Aveți însă grijă **SĂ NU MODIFICAȚI** wordlist.txt. Salvați decodificările în **wordlist_decoded.txt** pentru punctajul intermediar aferent acestei operații.

Hint: man base64.

După decodificare, parolele criptate pe care le veți descoperi sunt sub forma unor bitstrings pentru o mai ușoară prelucrare. Folosiți scriptul python `otp_decrypt.py` pentru decriptarea unui bitstring (string format din biți, ex: “0100111”), pasându-i în linia de comandă, în ordine, bitstring-ul de decriptat și cheia (usostrongkey):

`$ python3 otp_decrypt.py <bitstring> <key>`.

(

```
$ wget https://pastebin.com/raw/4mhCcJmv
```

)

Task 03 (15p)

- La finalul punctului anterior ar fi trebuit să obțineți o ultimă arhivă, `arhiva3.zip`, și trei fișiere `user[1..3].txt` cu câte un nume de utilizator și mai multe parole (fictive) pentru diverse site-uri. Doar una dintre ele este parola pentru arhiva3. Pentru a nu face brute-force, încercând fiecare parolă, mai aveți în arhiva2 și fișierul `hashes.txt`, care conține hash-urile celor trei fișiere menționate.
- Verificați care hash-uri sunt corecte, pentru a vă reduce căutarea (unele fișiere au fost modificate și nu mai sunt integre).
- Redenumiți fișierele corupte în user_corrupted_{i}.txt, unde {i} se va înlocui cu numărul prezent în denumirea fișierului inițial.
- Numele de utilizator rămase pot fi căutate cu o unealtă precum Sherlock (https://github.com/sherlock-project/sherlock [https://github.com/sherlock-project/sherlock]) pentru a descoperi care cont dintre cele listate în fișier există cu adevărat (parola rămâne una fictivă totuși). Sherlock primește un nume de utilizator și realizează o căutare extensivă pe o multitudine de site-uri (în special de social media) pentru a găsi conturi asociate cu acel nume de utilizator. Acest gen de activitate poartă numele de OSINT și reprezintă un pas important într-un potențial atac, atunci când dorești să afli cât mai multe informații despre țintă (fie ea sistem sau persoană).
- Odată găsită parola, dezarhivați ultima barieră între voi și mesajul ascuns.

Task 04 (10p)

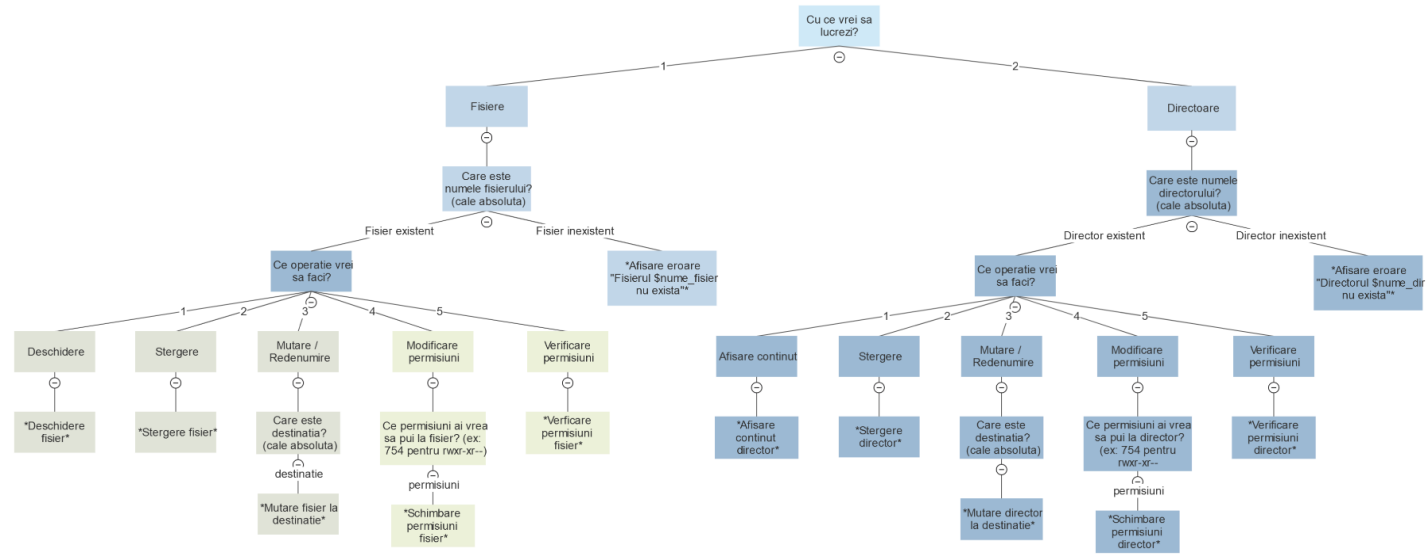
```
Pentru acest task se va lucra exclusiv în directorul /home/student/tema3-task4
Înainte de a vă apuca, intrați in directorul acesta.
```

- În directorul curent se află `64based.txt`. Acest fișier a fost codificat de 20 de ori cu `base64`.
- Creați un script numit `unbase.sh` care să decodifice conținutul acestuia și să scrie noul conținut în `64unbased.txt`.

Task 05 (20p)

```
Pentru acest task se va lucra exclusiv în directorul /home/student/tema3-task5
Înainte de a vă apuca, intrați in directorul acesta.
```

- Creați un script numit `my_menu.sh` care creează un meniu de bază pentru realizarea operațiilor pe fisiere si directoare într-un sistem cu Linux, conform diagramei:



- Un exemplu de rulare a scriptului ar putea fi:

```
❯ bash my_menu.sh
Cu ce vrei sa lucrezi?
1. Fisiere
2. Directoare
3. Iesire
Alege: 1
Care este numele fisierului? (cale absoluta)
Nume fisier: /Users/ry/test_deschidere.txt
Ce operatie vrei sa faci?
1. Deschidere
2. Stergere
3. Mutare/Redenumire
4. Modificare permisiuni
5. Verificare permisiuni
6. Iesire
Alege: 1
Acesta este un fisier
```

- După cum puteți observa în exemplu, puteți implementa în meniu și opțiunea de `Ieșire` la fiecare pas, pentru a va facilita testarea. Acest pas nu are însă niciun efect asupra puncajului obținut la acest task.
- Folosirea diacriticelor în cadrul scriptului nu este necesară și nici recomandată.

Task 06 (30p)

```
Pentru acest task se va lucra exclusiv în directorul /home/student/tema3-task6
Înainte de a vă apuca, intrați in directorul acesta.
```

```
Pentru cerințele a și b veți reține output-ul în log_fixed.txt.
Celelalte linii le veți afișa exact așa cum apar în fișierul log.txt.
```

```
Toate scrierile către fișiere vor fi făcute direct din scripturi, ci nu la momentul execuției.
Exemplu: `./fix_requests.sh > log_fixed.txt` nu va fi acceptat ca soluție.
```

```
De fiecare dată când veți rula `sudo uso start 3` se va genera un nou log.txt.
```

- [5p] a. Creați un script numit `fix_requests.sh` care afișează în `log_fixed.txt` conținutul din `log.txt`, dar modificând liniile care au ca tip de cerere HEAD, astfel încât să fie afișate invers.
- **Exemplu:)46x ;46niW ;0.01 TN swodniW(17.2964.0.79/emorhC :tnegA-resU 1.1/PTTH tuoba/ DAEH**
- [5p] b. Modificați scriptul `fix_requests.sh` astfel încat toate liniile care au ca tip de cerere OPTIONS să fie afișate cu majuscule.
- **Exemplu: OPTIONS /SOME_OTHER_PATH HTTP/1.1 USER-AGENT: CHROME/97.0.4692.71 (WINDOWS NT 6.1; WOW64)**
- [10p] c. Creați un script numit `get_users.sh`. În cadrul acestuia, cu ajutorul cererilor de tip POST (din fișierul `log.txt`) făcute către `/login`, rețineți în fișierul `users_db.txt` toți utilizatorii și parola lor respectivă (ca hash de tipul sha256), sortați alfabetic după utilizatori.
- **Exemplu: adelin:1bc9414dc185b89669dba035340c4684a6733bbf1cdac568dadcfd2eef731054**
- [10p] d. Creați un script numit `get_browsers.sh` în care identificați ce browsere folosesc utilizatorii de iPhone (din fișierul `log.txt`) și le rețineți în fișierul `iphone_users_browsers.txt` alături de numărul de apariții, sortate de la cel mai folosit browser pana la cel mai puțin folosit.
- **Exemplu: Safari - 120**