

بسم الله نبدأ... رب اشرح لي صدري ويسر لي أمري.

Chapter 8

ليه اهلًا عندي فكرة ال Users and groups ؟

- اول حاجة امدد ال Ownership بتاعت ال System resources
- تاني حاجة اعمل Permissions ال resources دي اوله Users
- تقسم يعني مثلاً كل File ليه permission وكذا ال Processes
- نفسها ليه permission ... ليه طبعا مكان فيه ال ال ال ال مثلاً
- Open , read , write وهكذا ال Files دي

طيب عايزين نعرف أهم ال Files عندينا ...

① /etc/passwd

ده بيحتوي على ايه ؟

- login name : - unique
- encrypted password : - empty means no

Pass Word

لجزيه الكلام ده عندي مثلاً لو فتحت ال /etc/passwd

هلاقي منظر زي ده مثلاً

root : (X) : 0 : 0 : root : /root : /bin/bash

هنا دي لو فاضيه مثلاً مفي Password طب لو متي char

زي دي كدة ؟ ال password هتكون موجودة

encrypted ومنه ال Shadow file

- User ID (UID) : 32 bit , 0 → root

- Group ID (GID): 32 bit

- Comment : -extra info about the user

- login shell :

ال Shell الى يعمل منها login ولو فاضيه هيد امن
/bin/sh هو الى هتكون ال Shell بيتا من اول Shell
بتفتح لما ال User يعمل login ال Shell login دي

- home directory :

ال Process ليها CWD بتاعها ودة ال directory
الى بحسب من عنده ال relative path
طب لما ال User يعمل login دة امكن الى ك ال User
يعمل login هتبدأ ال login shell تشتغل عنده

طب بيتفتح لما بتا بتدي home directory في file
User موجود في وفي الجاهات بتاعه ومتقال ال login shell
هتشتغل ودة يكون ظاهر عندي في ال prompt الى هو
الجزء بتاع : \$ دة المفروض أنا ب home refer
بتاع ال user الى أنا عنه عنوان كدة لو طفت بـ ا خالص
عند ال root هتلاقه هو نفسه file بـ ا جواه
ال Users الى عندي وجواه طابات ال User دة وهو دة
ال امكن الى ال login shell بتا operate من عنده زيما زي
ال process

* لا يعمل Users لاجابات زي man و apt
كل الـ pages دي في اواخر هي بتشغل processes
تكون عند Control للـ pages التي هي بتشغلها
اشغلها بـ user معين عشان اديها permissions معينة

يعني مثلاً لو بعمل user لـ man في أنا هي Program
الـ man يقرأ مثلاً الـ man of pages بـر مش
بيعدل فيها في هي User والـ User ده هيكون
no login user هو ده التي هي يقوم الـ
man process no login وهيكون

* /etc/group

كا الـ Unix اتقل كان كل User له هروب واحد بـر عشان
كدة في etc/passwd في GID واحد بـر ويحدد
قالوا لا عايزين الـ user يكون موجود في كذا هروب
في قالوا هتعمل File اسمه etc/group وده هيكون
الـ Files التي هي موجودة في الـ System وده فيه

- group name : unique

- encrypted passwd : زي الـ etc/passwd بـر هي
نادر ما يستعمل ودي موجودة في /etc/shadow

- group ID
- user list

* /etc/shadow

ده ده ربط مشترك security عنوان بعد ما كنت
ال Password مودورة encrypted فرا ال Password etc
واي مد يقدر يشوفها وممكن يعطي decryption ويغير
كدة سهل اعمل اي حاجة قالوا لا افاضات طرقي
File ثاني محدش يقدر يفتحه غير ال root
وردة قمع

- login name : unique , matching name in
etc password

- encrypted password

- aging information :

سوية معلومات عن ال Password ممكن نجيبها من ال man

طيب السؤال المهم ازاى ال Password بيحفظ encryption

عشان نحرف دة لازم نعرف ايه هي ال hash function ؟

هي زي mathematical function او algorithm

Variable number of characters "message"

fixed length string

hash

ويتحول لها اسم

Collision

طيب هو بصير السهولة ممكن يحصل

2 bytes

عبارة عن

Fixed length string

ملا

ال

2 bytes اتصال

في

output

ياي

في

input

في

اتصال

في

input

في

ف باتای ممکن Hash نقش ال
two different strings وکتد مایکون Collision
امتناعیه اقل ک مایکون افضل

ال Hashing دی علیه one way یعنی مینفش ارجع
ال Hash ر String تان

Hash function properties :-

① Pre-image resistance : means it's one way

② Collision resistance :
مینفش اوکازم نقل اصطلاحه ان two messages بطوری
نقش ال Hash

ال قیما الحضاة دی بتسی Crypto graphic hash function

طبیب مال هو ال Authentication : هر علیه انی اعرف
من ال User الی داخل ال System عسی وغالباً بتتعل
ب Password & user name

طبیب آزای یعرف ال Password بتای ال User انها
الصح ؟

مش الصح طبیب انی اسیفها ال ال System عسی والا
ای ص لعیل login صیغ ال Password دی
ف ان مش هسیفها ولا encrypted Value بتای
شان ممکن تیعلها decryption ف ان هسیف ال hash
بتای ال Password دی ویا اجه ادخل انال Password هر
اعلیا hashing و اقرن ال hash ب ال hash

طبي ايه الفرق بين ال Hashing وال Encryption

الكلام ده بعد شوية يمت
أول حاجة ال encryption
هو عليه تشفير ال data
التشفير ده يقدر يقرأها
ودة ايه نوعين
Symmetric Asymmetric

أول حاجة ال Symmetric ده يشفر ال data وسوكتيا Key
بيلغي التشفير ده طبي وال Key ؟ ارجع اشعة
واقفل كدقسي Closed loop يقدر عشان ال data
يقفل ال Safe

في عشان اكد ان ال Asymmetric

مثلا لو عندي mail box من الشارع لو غايروا عندي
هخط فيه ال mail ده طبي لو غايروا اقرأ اللي فيه ؟
لازم يكون معايا مفتاحه في عشان كدة اضربنا فكرة
ال RSA Algorithm

وده مني على فكرة ان يكون في لي مفتاحين واحد public
واحد private ال public ده مع اي حد وده مستخدم
فوال encryption يعني مثلا لو عندي message كايرو
اعلي encryption مستخدم ال Public Key ده
وال private هو اللي يقدر يقرأ ال decryption
ف بالتالي لو غايروا اعمل encryption ل data هاف
ال public key نتاج ال خفة اللي كدقسي ال data
واروع اعلي encryption ووقتها اننا نفسي معرف
اعلي decryption طاعا من معايا ال private key

- آزای بقی البرامج بتعل الموضوع ده ؟
من library routine تايه اسمها crypt ودي فينا
ال encryption methods افتح ال man بتاعتها
هي بتافد ال password وشويه settings كدة تعرفين
استخدم انهم function for hashing

ف لو عاينو ا Check ال password مستخدم ال Crypt
دي طيب انا بيله وأنا ب login ال password بس
هو يعرف مين ال settings وكا ال hash function
دي ؟ يكون فيه Prefix كدة فر أول ال password
يعرف منه انا استخدمت انهم hash function انا
ا hash بها ال password واشوف هل ال اثنين نفس
ال حاجة ولا لا ؟

فري شويه library routines كدة هنتاول تعرف عنهم شويه
طابات وننقر نقرأ ال man بترضو

- getpwnam()
دي هتخرج تفتح ال /etc/passwd وتبي ال entry
بتاعت ال user كدة منه

- getspnam()
دي هتافد معلومات ال user من ال /etc/shadow

- getpass()
دي بتظهر ال password بتتكتب كذا اكتبها ب انا اقول
ال echo بتاعت ال terminal فيش هي عمل echo وبقا
وبعد ما عمل enter زفتها تاف

طبيب لو اننا علمت Program في Check على ال Password
هو كلمة من مواه لازم نفتح ال Shadow عنان يافه منها
ال hash بناتي ويقارنهاب ال Password الى هيبوله
بعد نايعلها hashing

طبيب ايضا كنا قولنا ان ال Shadow دة مصدر يقدريفتحه
غير ال root و ازاي ال Program بناتي هيا كسبه ؟

زمان كنا قولنا ان من حاجة اسمها ال ID وال effective ID
ال ID هو ال ال Process بت inherit من ال Parent
على صول وال effective دة ID قراول وغالبالكو نشه
ال ID الكساح الى بافده من ال Parent بن ميره
أني اقدر اغيره عنان ادي ال Process بناتي Permissions
بناتي غير بناتي ال Parent دي

و هروغ اغيرها - طبيب دة بيحصل ازاي
همل bit ID - user - set ودي لو علمنا
set مستعمل ال Permissions بناتي ال owner
بناتي ال Process دي اكن لو مني مفعولها set هتاه
ال Permissions بناتي ال مستعمل ال Process الى عليها
exec اصل

memory allocation

اول حاجة انا لو عملت Program مثلا بيطلع dynamic allocation
وينطبع ال Program break, end, data, text

اول حاجة لعمل extern لا end, edata, etext
عشان اعرف اشي ففهم

* اول ملاحظه مع كل execution هلاقي ال addresses بتختلف
كل مرة وهنقول ليه ده بيحصل

* بس تاني ملاحظه هلاقي ال Program break
بيتحرك في البداية خالص مع انا كذا قولنا انه المفروض هو من
بداية البرنامج هيكو عند ال end ليه ده حصل
عشان ممكن ال libc و glibc نقل هي malloc اهل لحاجات
حوالها مش انا لوصي اللي يعمل malloc

طيب لو انا عايزة اعرف ال Virtual memory دي مقولة
ازاي او متعة ازاي لعمل ايه هي

/proc / 'pid of process' / maps

موجودة في ال File ده وال
تفعل ال Command اللي فيها اكلول بعدها نقل replace
وتفعل ال Command كذا

1000 hex = 4096 decimal

address - address + 1000 H

الصفحة

Page

Page هذا يبدأ ال

Permissions

read - write - execute

File offset يتبع ال File الى يقرأ منه

File الاسم ال او اسم المكان دة في الميموري في مثلا

1- شوية حاجات بيت allocate لها ال C library في بداية البرنامج خالص قبل ان text يتبع ال Program

2- text segment
وهو هذا ان من ال permissions يتبع ال execute

3- data segment

4- bss segment

5- heap

6- shared libs

7. stack

/ /

12/2/2000

Store

Share

Linus

طبيب من ملاحظة مهمة جداً، أني لو عدت run هلاقي كل مرة
الماكن بتتغير وده عن مفهوم ال Virtual memory
اللى هو مبنى من اصفار ال FFFs عشان أول حاجة تخلى
كل Process لها ال ميموري كلها وتاني حاجة تخلى البرنامج
كل مرة يروح لنفس المكان و ال run ميموريه
فليه ده بيحصل ؟

من حاجة اسمها Address space layout Randomization (ASLR)

عنا كانت ال sections بتاعت البرنامج ثابتة من مكان معين كان
بيحصل حاجة اسمها ال buffer overflow دي بتوع من ال attacks
وطريقة ما بيخلي البرنامج يروح من صفة نيمو bug مثلاً أو اوصل
ليه قبحاً مثلاً ال password في طريقة تخزينه غير
من ال behaviour بتاع البرنامج أو اوصل ال sensitive data

و بالتالي انا فضل اني احط ال program sections من ميموريه
كل مرة بحيث ميقدريش ال attacker يتنبأ بال address
الى جاي لاي حاجة من ال program

ودي حاجة اقدر اعلمها disable
(man proc → search for randomization)

طبیعاً در ملاحظه مهمه مدأ، آنی نوعات run هلاقر کلمره
اکامان بستنر وده فکرم مفهوم در Virtual memory
الان هلاقر مهووه من اصفار ل FFFs عسکان اول حاجه تغلی
کأن کلمه Process لهما المیسوری کلمه وانی حاجه تغلی البرنامج
کلمره یروج لنفسه اعکان و run مهووه
فایه ده یحصل ؟

فحاجه اسمها Address space layout Randomization (ASLR)

کما کانت ال Sections بتات البرنامج ثابتة فمکان معین کان
یحصل حاجه اسمها ال buffer overflow دی نوع من ال attacks
طریقه ما یغلی البرنامج یروج فحاجه نیرا bug مثلاً أو اوصول
لیه قیام مثلاً ال password فدی طریقه تغلی غیر
من ال Behaviour بتاع البرنامج أو اوصول ال Sensitive data

و بالتالی اکامان فی الحظ ال program sections فحاجه معینه
کلمره یصیت میقد رستی ال attacker یتنبا بال address
الی جای لای حاجه فحال Program

ودی حاجه اقدر اعلا disable
(man proc → search for randomization)

طبيب بعد ما اعلمها disable هلاقم ال addresses مش بادعه
من صفر مثلاً لا هه بادعه من بعد كده بتكثير طب ليه الكلام ده؟

ده بسبب ال dynamic linking طب ايه الموضوع ده

اضافه فنانا من ال dynamic linking لما اصبر اعل Shared library
بعلها بـ ELF PIC الى كان بيخليه Position Independent Code
ف بالتي يكون اكل حاجه مكان كذا مرة من المصوري وهه مش بتشتغل
بناد اكل مكانها من ... فلا بعل Program بخله dynamic linked
لو محتاج كانه يكون position independent وبالتي الامكان
مش هه نفسها اللي فر ال elf بتاخره يعني ال map file
وال elf اما كنهم مش واصله ويرض على حسب فهمه انه
ال dynamic linker بيخه مكان ما الارل يعني

ف لو خليت البرنامج بتاعي linked statically هلاقم ان
الامكان اللي فر ال map file هه تنسب ال فر ال elf
طب ما كنا قولنا ان ال Randomization هو اللي بيدل الكلام
ده

الفكرة ان اللي هيشيت الاحاط الي هتكون محتاجها statically
يعني مثلاً ال .bss و .data و .text هيفضلوا مكانهم مش
هيتغيروا والي هيتغير ال heap وال stack مثلاً كوفنت
ال Randomization بتاتي الحاجه الي ممكن اغير مكانها
هه الي هتغير ف انا محتاج ال dynamic linking
وال Randomization الاثنين حوا عشان اغير مكان الحاجه
عندى بالكل وتكون الدنيا Safe ومحصنة attacks