SEGURETAT DE COMPTES D'USUARIS

Ara que ja tenim coneixements sobre la gestió d'usuaris i grups, podem veure mètodes per intentar reduir, en mesura del possible, uns dels forats de seguretat més importants de tots els equips informàtics, les contrasenyes dels usuaris del sistema.

Aquestes contrasenyes, si no posem normes, son normalment massa "dèbils" i fàcils d'esbrinar a través d'un atac de diccionari. A més, molts cops, son capturades en altres equips de l'usuari, o en altres aplicacions, i com que molts cops els usuaris les utilitzen per a tot, proporcionen un gran nivell d'accés.

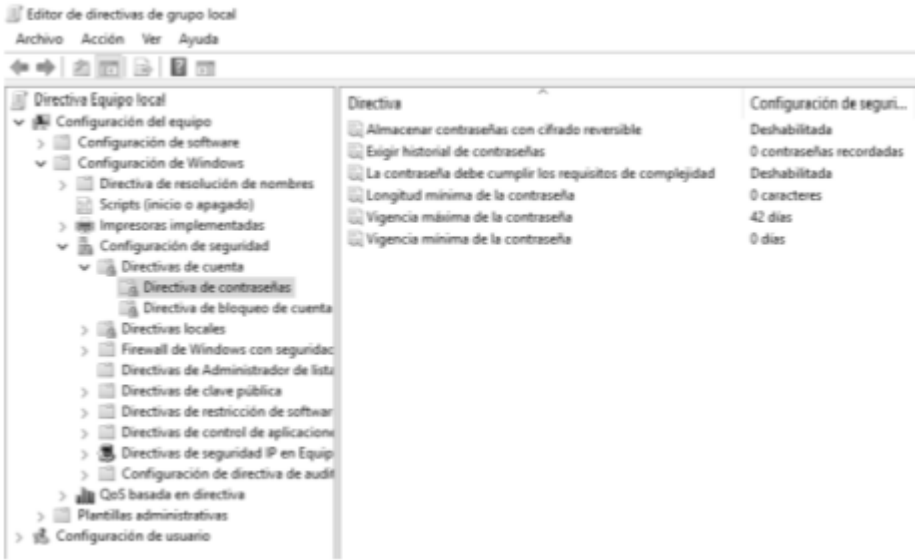
Abans de començar, doncs, insistir que una bona consciència d'un ús responsable de credencials als nostres usuaris, serà la millor eina per aconseguir un entorn de treball més segur.

1. DIRECTIVES DE CONTRASENYA A WINDOWS

Les directives de contrasenya als equips amb sistemes operatius de la família Windows és controlen com una política de configuració del sistema. Recordeu que per tal d'accedir al panell de control de la consola de polítiques em d'executar **gpedit.msc**.

Dins d'aquest consola de Microsoft la configuració de les directives de seguretat estaran associades a la branca de configuració del equip. Dins d'aquesta accedirem a la **configuració de seguretat** on podrem trobar les configuracions relatives a les directives de comptes d'usuari.

A la seguent imatge veiem les sis configuracions que podem editar per forçar l'ús de contrasenyes fortes:



Una de les primeres coses recomanables a habilitar la directiva anomenada **"La contraseña debe complir los requisitos de complejidad"**. Amb això aconseguirem

directament que l'usuari no pugui utilitzar contrasenyes febles ja que imposa els següents requeriments:

- No pot contenir el nom d'usuari o parts del nom complert de l'usuari en més de dos caràcters consecutius.
- Ha de tenir una longitud mínima de 6 caràcters. És recomanable habilitar la directiva **"Longuitud mínima de la contraseña**" i augmentar aquest valor fins als 8 o 10 caràcters.
- Incloure al menys caràcters de 3 d'aquests 4 grups de caràcters:
    - o Majúscules (A-Z)
    - o Minúscules (a-z)
    - o Dígits de base 10 (0-9)
    - o Caràcters no alfanumèrics (#,$,%,@,etc.)

Cal tenir en compte que aquests requisits s'hauran de complir a partir d'ara quan creem qualsevol nova contrasenya o en qualsevol canvi que és realitzi, però que no afectarà a contrasenyes febles que ja puguin tenir els usuaris.

Amb l'acció d'exigir contrasenyes fortes haurem guanyat molt en seguretat, tot i això, podem anar un pas més enllà fent que les contrasenyes fortes escollides no siguin estàtiques i permanents, sinó que tinguin un caràcter temporal. Per aquest fi tenim les directives **"Vigencia màxima de la contraseña"** i **"Vigencia mínima de la contraseña"**, que ens permetran establir un període de vigor de la contrasenya. Així, per exemple, podrem imposar que una contrasenya introduïda per l'usuari s'hagi de canviar en un termini de 3 mesos, i al mateix temps, si volem, que no la pugui canviar durant el primer mes d'aquests 3 mesos.

Per últim, podem evitar que els usuaris estiguin reutilitzant antigues contrasenyes en cada canvi forçat per temps. A la directiva **"Exigir historial de contraseña"** podrem establir el número de contrasenyes que el sistema recordarà com utilitzades per un usuari i que no podrà reutilitzar fins que quedin alliberades.

ACTIVITAT | Directiva de bloqueig de compte a Windows

Un altre aspecte que pot millorar el nostre nivell de seguretat pel que fa a les contrasenyes del comptes d'usuari és aplicar directives per a bloquejar els usuaris que facin un número d'intents erronis en l'accés al equip.

Accedeix a les directives de comptes d'usuari i explica les 3 directives relacionades amb el bloqueig de comptes d'usuari. Fes algunes proves amb un usuari per veure els missatges que envia el sistema quan es bloqueja un usuari. Com es pot desbloquejar posteriorment?

2. DIRECTIVES DE CONTRASENYA A UBUNTU

Els sistemes operatius basats en Ubuntu permeten configurar una política de contrasenyes de forma fàcil i ràpida editant un document de text. Això sí, per poder establir alguns dels paràmetres més avançats, relacionats amb la complexitat i/o evitar els atacs de diccionari, caldrà instal·lar alguna llibreria "extra" que ens faciliti la tasca.

Així doncs, el primer que farem serà executar **sudo apt install libpam-cracklib**. Un cop instal·lada la nova llibreria per a PAM, podrem configurar una política de contrasenyes que eviti l'ús de paraules del diccionari, la no reutilització de contrasenyes (historial), la complexitat d'aquesta, etc.

El fitxer per configurar la nostra política de contrasenyes s'anomena **common-password** i, com tots els fitxers de configuració del sistema, penja del directori /etc (/etc/pam.d/common-password). Dintre d'aquest fitxer haurem de trobar la línia **password required** i afegir just darrera que utilitzi la nova llibreria instal·lada (pam_cracklib.so). Només amb això aconseguirem que les contrasenyes no difereixin només d'un caràcter (per exemple de password a Password) o que no siguin al revés (de password a drowssap). També preveu contra atacs de diccionaris. A partir d'aquí podrem establir més opcions que considerem a la nostra política:

- **retry**: número d'intents de login abans de tornar un error.
- **minlen**: longitud mínima de la contrasenya.
- **difok**: nombre de caràcters que han de canviar entre una nova contrasenya i l'anterior.
- **ucredit41**: nombre de caràcters en majúscules que ha de contenir la contrasenya.
- **lcredit**: nombre de caràcters en minúscules que ha de contenir la contrasenya.
- **dcredit**: nombre de números que ha de contenir la contrasenya.
- **ocretid**: nombre de caràcters no alfanumèrics que ha de contenir la contrasenya.

Altres consideracions que hauríem de fer es si volem conservar un **historial de contrasenyes** o establir una **durada mínima i màxima** de cada canvi de contrasenya. Pel primer supòsit, la llibreria pam_cracklib consulta el historial a través del mòdul **pam_unix**. Per poder fer-ho primer hauríem de crear un fitxer anomenat **opasswd** per poder emmagatzemar les antigues contrasenyes dels usuaris. Per que sigui segur hauria de tenir uns privilegis iguals als de /etc/shadow (on es guarden les contrasenyes actuals), és a dir, amb permisos de lectura/escriptura només per al root .

Un cop disposem d'un magatzem de contrasenyes cal indicar una nova línia de password required afegint ara darrera el mòdul pam_unix.so. A continuació indicarem opcions:

- **"tipus de xifrat"**: si no s'especifica el fitxer contindrà contrasenya en text pla. Habitualment utilitzarem **md5** per indicar que es guardin amb un hash (xifrat).
- **rembember**: indicarà el nombre de contrasenyes a recordar.
- **use_authtok**: si afegim aquest forcem que es consulti l'historial al fer canvi de contrasenya. Paràmetre requerit, per tant.

Pel segon supòsit, establir una durada mínima i màxima per les contrasenyes, veurem que no és una funció actual de la nostra llibreria pam_cracklib, sinó que s'estableix com una condició a editar a **/etc/login.defs**. Dintre d'aquest fitxer trobarem les variables del sistema PASS_MAX_DAY, PASS_MIN_DAY i PASS_WARN_AGE, que estableixen el màxims dies que pot durar una contrasenya, els mínims dies abans de poder tornar a canviar la contrasenya, i els dies abans que s'avisarà a l'usuari de que ha de canviar la contrasenya, respectivament. Aquestes configuracions només tindran efecte per als nous usuaris creats a traves de *useradd*. Per a usuaris que ja estan al sistema caldrà utilitzar un canvi de contrasenya a través de la comanda *passwd* amb els modificadors *-x#,-n# i -w#* (# serà el número que volem) per establir el màxim temps, mínim temps i avis abans que no caduqui, per la nova contrasenya de l'usuari.

ACTIVITAT | **Política de contrasenyes a Ubuntu**

Anem a treballar amb l'exposat anteriorment dissenyant una política de contrasenyes pel nostre sistema Ubuntu que compleixi les següents condicions:

- Ha d'utilitzar els paràmetres de seguretat que proporcional la llibreria pam_cracklib per defecte.
- Un usuari tindrà 3 opcions per ficar correctament la seva contrasenya.
- Aquesta tindrà una longitud mínima de 10 caràcters, dels quals només un ha de ser en majúscules i com a mínim 2 han de ser números.
- A més, s'ha de conservar un historial de les últimes 2 contrasenyes que no es podran reutilitzar.
- A més, la contrasenya caducarà cada mes, i s'avisarà 3 dies abans a l'usuari de que cal canviar-la.

Un cop fetes aquestes configuracions, crea un nou usuari i comprova que la teva política de contrasenyes funciona correctament. Afegim un punt extra per tal de que investiguis:

- Com puc aconseguir que en el meu sistema no estigués permesa específicament una contrasenya concreta, per exemple: asWd345jku, que tindria que ser vàlida segons la política de contrasenyes anteriors?