Examen pràctic del primer trimestre (RA1 i RA2)

En primer lloc, baixem la imatge Docker que utilitzarem per a l'examen:

```
docker pull br3baj3/examen_practic_1er:latest
```

I una vegada fet això, executem el contenidor amb el nom **examen_container**, en *background* i mapejant el port **8888** de la nostra pròpia màquina al 2222 del contenidor. Després comprovarem que el contenidor està corrent sense problemes:

```
docker run --name examen_container -d -p 8888:2222
br3baj3/examen_practic_1er:latest

docker ps
```

Història de dos ciutats

Per a esta pràctica/examen, assumirem primer el paper d'un atacant/ciberdelincuent i despŕes el de l'administrador de sistemes que vol solucionar el problema.

Atacant

Suposem que el atacant ha aconseguit unes credencials d'alguna forma no molt ética i les fa servir.

Haurem d'esperar 1 ó 2 minuts per a que finalitze la provisió del contenidor. Passat este temps podrem conectar-nos per SSH:

```
ssh examen_practic@localhost -p8888
```

> **Info**
>
> - **usuari**: examen_practic
> - **contrasenya**: examensad

En primer lloc, l'atacant vol facilitar-se la vida a l'hora de fer servir las credencials i conectar-se a la màquina d'una forma més còmoda.

Tasca 1 - Conexió SSH amb claus

Crea un parell de claus de 2048 bits amb l'algorisme RSA i copia-les al server per a conectarte mitjançant clau pública. Comprova que funciona correctament.

Després d'una intensa auditoria, el ciberdelincuent ha descobert que la màquina té una vulnerabilitat del paquet pkexec molt crítica anomenada *Pwnkit* que permet a un usuari escalar privilegis i convertir-se en root.

Tasca 2 - Explotació de la vulnerabilitat

Busca un exploit en python per a **pwnkit** i fes-lo servir a la màquina per a convertir-te en root. Després d'executar-lo introdueix el comandament `id` com a prova.

El ciberdelincuent, aprofitant els seus poders de root, vol cobrir les seues empremtes i per tant, procurarà esborrar dels logs les línies que facin referència al login amb claus (el login original estava amb usuari/contrasenya i una altra cosa alçaría sospites). Per a fer això utilitzarà l'eina **vi** i no **nano**.

Consell

Una vegada aconseguida una *shell* de root pots obtenir una shell més amigable amb el comadament `/bin/bash`

Tasca 3 - Ocultació d'evidències

Busca entre els arxius del directori a on s'ubiquen tots els logs del sistema totes les línies que facin referència a l'usuari *examen_practic*. Entre eixes línies hi haurà algunes que facin referència al login *ssh* amb clau pública, que també pots filtrar si vols.

Ara, amb l'eina *vi* obri l'arxiu d'on hagis d'esborrar les línies i esborra només les que mostren un login amb clau pública.

Consells

Vi és una eina un poc especial, alguns consells per a fer-lo servir:

- Per pasar al mode d'inserció de text heu de prémer primer la tecla **i**
  - En este mode podeu escriure i esborar
- Després d'escriure lo desitjat, heu d'eixir del mode d'inserció prement la tecla *ESC*
- Fora del mode d'inserció de text podeu buscar paraules escrivint **/terme_a_buscar** (important la barra)
  - Per a buscar la següent coincidència, premeu **n**
- Per a esborrar una línea sencera d'una vegada, fora del mode d'inserció de text, vos coloqueu en la línia y premeu **dd**
- Per a guardar i eixir, eixiu del mode d'inserció de text (tecla **ESC**) i escriviu **:wq** (important els dos punts)

Després d'esborrar les pistes que el delaten, l'atacant decidix que utilitzar aquest usuari es perillós pel risc que té de que el pugen descobrir. Es per això que ha decidit fer servir un altre usuari. Consultant l'arxiu `/etc/passwd` ha vist que el mes indicat és un anomenat **altre_usuari**.

Tasca 4 - Desxifrat de contrasenya

1. Treu la línia que et fa falta de l'arxiu `/etc/shadow`
2. En la teua màquina fes servir `johntheripper` per a desxifrar la contrasenya. Utilitza el diccionari que trobaràs en Aules.
3. Comprova que, efectivament, pots conectar-te per SSH amb el nou usuari

Una vegada l'atacant ha fet login amb el nou usuari pren vol procedir a exfiltrar certa informació en un arxiu de text. L'atacant ha decidit aprofitar-se de que la màquina té instal·lada la utilitat ***rsync***.

Tasca 5 - Exfiltració amb rsync

Fes servir *rsync* per a enviar l'arxiu **dades_interessants.txt** a la teua màquina amfitriona. Recorda que has de poder conectar-te per SSH a la teua màquina amfitrió.

L'arxiu ha de contindre dos dades:

- Hash SHA256 de la contrasenya de l'usuari
- Hash SHA256 de l'exida del comandament `date`

Atenció!

Recorda que *rsync* ha d'estar instal·lat tant en la màquina origen com en la de destí.

Administrador de sistemes

Després d'una àrdua tasca d'investigació, el administrador de sistemes ha descobert quina es la vulnerabilitat que ha fet servir l'atacant i ha de procedir a solucionar-la.

L'administrador té un usuari propi:

Info

- **usuari**: ubuntu
- **contrasenya**: iessevero

Tasca 6 - Mitigació

1. Busca informació de com **mitigar** la vulnerabilitat i posa-lo en pràctica.
2. Busca informació sobre com **solucionar-lo** i indica el comandament que sería necessari introduïr per a fer-lo.
3. Comprova que l'exploit ja no funciona

Atenció!

La tasca es considera correcta amb la mitigació i la indicació de com solucionar-lo. En cas de que vulgues fer-lo més real, pots fet l'actualització necessària però **pot trigar molt de temps**. Tens dos opcions, o deixar indicat el comandament o executar-lo i deixar-lo funcionar mentres continues amb l'examen.

Per a augmentar un poc la seguretat, l'administrador decideix aplicar una nova **política de contrasenyes**. Concretament aplicarà els següents paràmetres:

- Al ficar el nou password, si no compleix la política, només deixarà 3 intents abans de tornar un error
- La longitud mínima del password ha de ser 12 caràcters
- Només deixa que la contrasenya continga el mateix carácter consecutiu 3 vegades
- El password ha de contindre al menys 2 lletres mayúscules

- Al menys una lletra minúscula és necessària
- Ha de contindre com a mínim 2 dígits
- La política ha d'aplicar-se també a l'usuari root

En quant a **la vida útil de la contrasenya**:

- La contrasenya caducarà als 6 mesos
- No fa falta esperar cap temps o día per a canviar la contrasenya
- Avisarà l'usuari de que la contrasenya caduca als 5 mesos

Per a comprovar la política, des-de l'usuari **ubuntu** per a canviar la contrasenya de l'usuari **examen_practic** pels següents valors:

1. aBC24
2. AAAAbecedari24
3. Contrasenya.forta.2024
4. CONTRASENYA.FORTA.2024
5. HoAproveSegur1
6. examenSAD2024

Tasca 7 - Política de contrasenyes

- Configura la política demanada
- Mostra com cada 3 intents infructuosos, et dona un error.
- Mostra en els logs on es puguen vore els intents i l'éxit final, utilitzant el comandament: `sudo journalctl | grep passwd`

Per últim, l'administrador configurarà que cada 3 intents erronis de login per SSH a la màquina, eixe compte quedarà bloquejat un temps abans de poder tornar a fer login.

Tasca 8 - Bloqueig de comptes amb logins erronis

- Un amic de l'*admin* li ha parlat de la eina ***tally2*** per a poder configurar estos bloquejos ja que està utilitzant una versió molt antiga d'Ubuntu
- Per tal de provar primer i no bloquejar usuaris a *tutiplen*, ha decidit configurar que als **3 intents de login erronis**, es bloqueje el compte durant **15 segons**
- Per a demostrar que està funcionant, mostra la part del log `/var/log/auth` on es puga vore, una cosa a continuació d'una altra, com tally bloqueja el compte i 15 i no deixa fer login però 15 segons més tard sí que deixa. Indica cadascuna de les accions en la captura de pantalla.