**Labo 6 - Gebruikersaccounts**

# **Doelstelling**

* Aanmaken, testen en verwijderen van gebruikersaccounts en groepen

# **Richtlijnen**

* Log in bij virtuele PC in als student
* Om administratieve taken te kunnen verrichten moeten we dit telkens als een gebruiker doen met voldoende rechten. Tot nu toe voerden jullie deze administratieve taken uit als gebruiker “student” met telkens sudo voorafgaand aan de commando’s. Omdat dit labo continu gebruik maakt van commando’s die enkel met voldoende rechten kunnen uitgevoerd worden, mogen jullie deze als de gebruiker “root” uitvoeren. Wisselen van account (gebruiker) kan je makkelijk doen met su -
* Log nooit graﬁsch in als root-gebruiker, dit brengt uw systeem onnodig in gevaar

# **Gebruikers**

1. Maak als root gebruiker een kopie van **/etc/passwd**, **/etc/shadow** en **/etc/group**
2. Maak gebruik van het commando adduser om een nieuwe gebruiker “testuser” aan te maken. Ga na welke veranderingen er allemaal gebeurd zijn in passwd, shadow en group. Welke mappen werden er op het systeem gecreëerd?
3. Test de gebruiker: open een terminal als student, gebruik het commando su - <gebruikersnaam> om de nieuwe gebruiker te worden en probeer een bestand aan te maken. Geef ook de commando’s **pwd** en **whoami** in. Als alles lukt en een verwacht resultaat oplevert, keer je terug met exit
4. Maak nu handmatig een nieuwe gebruiker “directeur” en zijn bijhorende groep aan door de aanpassingen die je in punt 2 opmerkte, handmatig aan te brengen.

Het grootste probleem hierbij is het toekennen van een wachtwoord. Hiervoor heb je twee opties:

* ofwel kopieer je bij het editeren van /etc/shadow de hash van het wachtwoord van student of root. Dit wachtwoord ken je. Merk op dat de hashes voor root en student verschillend zijn, hoewel het wachtwoord identiek is. Hoe komt dit?
* ofwel ken je als root gebruiker een wachtwoord toe met het **passwd** commando. Als je dit als root gebruiker doet, moet je het oude wachtwoord niet opgeven.

1. Test opnieuw de gebruiker uit via je account “student”. Dit moet even goed werken als bij de vorige test.
2. Installeer de C-shell (csh) en pas de shell voor de “directeur” aan in het wachtwoordbestand. Test dit uit door opnieuw deze gebruiker te worden en keer terug met exit.
3. Verwijder de account “testuser” met een tool, en verwijder “directeur” handmatig.

# **Groepen**

1. Maak drie groepen (“linuxfans”, “windowsfans” en “macfans”) aan met een commando:
2. Verwijder de groep macfans
3. Bekijk de inhoud van /etc/group en verifieer of de aangemaakte groepen daar voorkomen.
4. Maak twee gewone gebruikers aan: gates en torvalds
5. Maak gebruik van het commando usermod of adduser om gates lid te maken van de groepen “windowsfans” en “linuxfans”. Zijn hoofdgroep moet wel gates blijven. **Verifieer in /etc/passwd** en **/etc/group** (of maak gebruik van het commando **id**)
6. Gebruik usermod om de hoofdgroep van torvalds aan te passen naar linuxfans
7. Maak als torvalds een nieuw bestand aan. Stel de rechten in op 640. Probeer het bestand te lezen als gebruiker torvalds, gates en student. Verklaar wie er wel en niet kan lezen.
8. Maak als gates een bestand aan, stel de rechten weer in op 640 en probeer te lezen als torvalds. Waarom lukt dit niet?
9. Pas de groepseigenaar van het bestand aan naar linuxfans (met chgrp of chown). Probeer opnieuw of torvalds nu kan lezen.

# **Extra**

Op linux worden de wachtwoorden opgeslagen als hashes. Alvorens te hashen wordt aan de wachtwoorden ook nog een salt toegevoegd.

Dit betekent dat je de wachtwoorden niet kan berekenen uit de opgeslagen waarde, maar je kan wel een dictionary attack uitvoeren.

Eén zo’n tool is John the Ripper.

* Installeer met apt-get install john.
* Maak een password file die john kan aanvallen

unshadow /etc/passwd /etc/shadow > toCrack

* Val de paswoorden aan met het standaard wachtwoordenboek:

john toCrack

Deze aanval kan een hele tijd duren, omdat alle wachtwoorden in het woordenboek gehashed worden (met gebruik van de salt) om dan te kijken of het resultaat overeen komt met de hash die aan die gebruiker is gekoppeld. Aangezien aan de wachtwoorden een salt werd toegevoegd voor het hashen en elke gebruiker een eigen salt heeft, moet dit proces uitgevoerd worden voor elke gebruiker voor alle wachtwoorden in de dictionary.

Gevonden wachtwoorden worden weergegeven op de commandolijn en kan je achteraf terugvinden in een bestand john.pot in de folder .john.

Of de aanval succes oplevert is afhankelijk van het feit of het wachtwoord al dan niet voorkomt in de dictionary waarmee de aanval wordt uitgevoerd.

Als de aanval niet meteen succes oplevert of je weinig tijd hebt, kan je een aangepaste lijst maken die snel resultaat oplevert. Maak daarvoor een bestand “words” aan en steek daarin alle wachtwoorden van de gebruikers. Voer nu john uit met de optie wordlist:

john toCrack -wordlist=words

Eventueel kan je eerst de .john directory wissen om van voor af aan te beginnen.

Het succes van een dergelijke aanval is dus afhankelijk van de woordenlijst. Op het (automatisch) opbouwen van een geschikte lijst wordt later in het curriculum teruggekomen.