Analiza Hasła

Dobre hasła stanowią pierwszą linię obrony przed nieautoryzowanym dostępem do systemu. Zarówno systemy operacyjne Linux, jak i systemy podobne do UNIX używają polecenia `passwd` do zmiany hasła użytkownika.

- Zwykły użytkownik może zmienić hasło tylko do swojego konta.
- Superużytkownik (lub root) może zmienić hasło do dowolnego konta.

PLIK `/etc/passwd`

Podczas logowania system odwołuje się do pliku `/etc/passwd`, aby określić m.in. identyfikator użytkownika (UID) i jego katalog domowy. Każdy wiersz w tym pliku reprezentuje jednego użytkownika i zawiera siedem pól rozdzielonych dwukropkami:

- username – identyfikator użytkownika (małe litery i cyfry, pierwsza litera, do 8 znaków)
- password – zaszyfrowane hasło użytkownika (x - shadow, * - blokada)
- uid – numeryczny identyfikator użytkownika (0..32767)
- gid – numeryczny identyfikator grupy (0..32767)
- gcos-field – imie i nazwisko użytkownika + ew. telefon, nr pokoju itp.
- home-dir – katalog prywatny użytkownika
- login-shell – interpreter komend (musi figurować w /etc/shells)

Wyświetlisz zawartość pliku komendą:

```
cat /etc/passwd
```

PLIK `/etc/shadow`

Plik shadow nie jest nadzbiorem pliku passwd, a plik passwd nie jest generowany na jego podstawie. Musisz utrzymywać oba te pliki lub skorzystać z takich narzędzi jak useradd, które będą to robić za Ciebie. Podobnie jak /etc/passwd, plik /etc/shadow zawiera jeden wiersz dla każdego użytkownika. Każdy wiersz to dziewięć pól rozdzielonych dwukropkami, a przeznaczonych na:

- username – identyfikator użytkownika
- password – zaszyfrowane hasło (13 znaków)
- lastchg – data ostaniej zmiany hasła
- min – minimalny okres pomiędzy zmianami hasła (dni)
- max – maksymalny okres pomiędzy zmaianami hasła (dni)
- warn – na ile dni przed upływem terminu przypominać o zmianie hasła
- inactive – maksymalny okres nieaktywności użytkownika
- expire – termin ważności konta
- flag – 0 (zarezerwowoane na przyszłość) Wyświetlisz zawartość pliku komendą:

```
sudo cat /etc/shadow
```

Zarządzanie czasem haseł systemu Linux, polecenie chage

Jednym z wielu zadań, które musimy wykonać, jest nie tylko ochrona haseł, ale także wygaśnięcie haseł użytkowników, którymi zarządzamy i należą do naszej domeny, ponieważ ten aspekt pomaga poprawić bezpieczeństwo systemu oraz informacji każdego użytkownika, ponieważ jedną z zalecanych praktyk jest regularna modyfikacja hasła w celu zwiększenia bezpieczeństwa na poziomie dostępu i uwierzytelnienia (w rozsądnym czasie).

Polecenie `chage` pozwala nam ustawić datę ważności haseł użytkowników w naszej organizacji, dzięki czemu możemy wykonać następujące czynności:

- Określ liczbę dni, w których hasło musi zostać odnowione
- Ustaw datę ważności ręcznie
- Lista kont informacyjnych, wśród innych zadań.

Podstawowa składnia użycia chage jest następująca:

```
chage [Opcje] Użytkownik
# Aby zobaczyć opcje dostępne w poleceniu chage, możemy użyć:
chage --help

chage -l student
# Sprawdza datę ważności użytkownika student

sudo chage -E [data] [user]
# Zmiana terminu ważności hasła.

sudo chage -E 2021-12-30 student
# Zmiana terminu ważności hasła użytkownika student na 30 grudnia 2021 roku

sudo chage -W [liczba_dni] [login]
# Aby wskazać użytkownikowi za pomocą wiadomości, że musi zmodyfikować hasło w ciągu X
[liczba_dni], należy użyć opcji W

sudo chage –W 2 student
# Użytkownik otrzyma informację, iż musi zmienić hasło w ciągu 2 dni.

sudo chage –I [dni] [uzytkownik]
# Opcja ta służy do ustawiania czasu nieaktywności konta po wygaśnięciu ważności
hasła, po którym to czasie konto jest blokowane

sudo chage –I 5 student2
# konto użytkownika student2 zostnanie zablokowane w ciągu 5-ciu dni po wygaśnięciu
ważności hasła
```

Resetowanie hasła roota

By zresetować hasło roota, będziemy potrzebować:

1. Dostępu do konsoli maszyny, oczywiście dostęp ten może być zarówno fizyczny, jak i zwirtualizowany (np. przez klienta przeglądarkowego).
2. Jeśli dysk jest zaszyfrowany, to hasła do dysku.
3. Jeśli bootloader jest chroniony hasłem, będziemy potrzebować hasła lub użycia innego źródła, z którego uruchomimy system. Może to być płytka instalacyjna, na której wybieramy tryb ratowania systemu.

Reset hasła w nowszych dystrybucjach Enterprise Linux 7 i 8:

1. Jeśli mamy dostęp do bootloadera `GRUB`, przed startem systemu możemy przerwać sekwencję jego uruchamiania, wciskając dowolny klawisz.
2. Następnie przy pomocy klawisza `e` należy wejść w edycję wpisu GRUB.
3. Następnie poruszając się przy pomocy strzałek, wybieramy linię, na której znajdują się parametry jądra.

- Linia ta zaczyna się od „kernel” i w zależności systemu i jego konfiguracji, może to być między innymi: „kernel”, „kernel16” lub „kernelefi”.
- W pewnych przypadkach należy skasować niektóre parametry, z reguły „console=”.

4. Na sam koniec linii dopisujemy `rd.break`.
5. Następnie przy pomocy kombinacji klawiszy `ctlr-x` startujemy system

Od tego momentu na konsoli należy wykonać następujące kroki 6. `mount -o rw,remount /sysroot` – krok ten jest odpowiedzialny za ponowne zamontowanie głównej partycji systemu w trybie do odczytu. 7. `chroot /sysroot` – uruchamia powłokę w nowym katalogu głównym. 8. `passwd` – zmienia hasło superużytkownika. 9. Przy pomocy `load_policy -i` ładujemy do jądra polityki SELinuxa. Przełącznik `-i` jest opcją informującą program `load_policy`, że ma do czynienia z pierwszym załadowaniem reguł SELinuxa i tylko w takim wypadku należy go używać. 10. Przy pomocy `restorecon -Rv /etc/` lub `restorecon -v /etc/shadow` przywracamy konteksty plikom. Opcja `-v` odpowiada za bardziej informacyjne wyjście, czasem nazywane gadatliwym (wprost z tłumaczenia słowa verbose). Z kolei opcja `-R` przywraca rekursywnie konteksty. 11. Wyjść z `chroot` poprzez `exit` i wykonać `reboot`.

Narzędzia – ataki offline

Atak offline jest atakiem kryptograficznym na hashe haseł, a jego celem jest znalezienie oryginału hasła lub jego kolizji. Atak ten jest o wiele wydajniejszy od brutalnego ataku online, ponieważ mamy do dyspozycji nie tylko całą moc obliczeniową swojej maszyny, ale do obliczeń możemy też wykorzystać inne komputery.

1. `hashcat` - zapewnia kilka różnych metod łamania hashy oraz wspiera ponad 200 algorytmów hashujących.

```
sudo apt install hashcat
man hashcat
```

2. `Hashid` - obsługuje identyfikację ponad 220 unikalnych typów skrótów za pomocą wyrażeń regularnych

```
sudo apt install hashid
man hashid
```

3. `John` - program służący do łamania haseł.

```
sudo apt install john
man john
```

Narzędzia – ataki online

Atak online na hasła polega na wysyłaniu do danej usługi wielu zapytań wraz z danymi uwierzytelniającymi. Nie jest to atak kryptograficzny – siłowo próbujemy znaleźć hasło do serwisu lub usługi.

4. Hydra - jest jednym z najpopularniejszych narzędzi służących do ataków online na hasła statyczne. Nie bez powodu program zyskał sobie przydomek THC (The Hackers Choise).
5. Patator - wielowątkowe narzędzie napisane w Pythonie do odgadywania haseł online

Narzędzia – passing the hash

Umożliwia atakującemu uwierzytelnienie się na zdalnym serwerze lub usłudze przy użyciu bazowego skrótu NTLM [_NT (New Technology) LAN Manager (NTLM)_].

1. pth-net: wykonuje polecenia sieciowe na zdalnych hostach
2. pth-rpcclient: otwiera sesję interaktywną w celu wykonania poleceń RPC
3. pth-smbclient: przegląda dostępne zasoby na zdalnych komputerach
4. pth-winexe: wykonuje interaktywnie polecenie na zdalnych hostach
5. pth-wmic: wykonuje zapytania WMI na komputerach zdalnych
6. pth-wmis: wykonuje polecenie za pomocą WMI na zdalnych hostach

Narzędzia – profilowanie haseł

1. Cewl - przeczesuje dany adres URL na określoną głębokość, opcjonalnie podążając za zewnętrznymi linkami i zwraca listę słów, które można następnie wykorzystać do łamania haseł
2. Crunch – służy do generowania listy haseł
3. Rsmangler - służy do mutacji haseł z wordlisty
4. SecLists – repozytorium zawierające profilowane listy haseł

Ćwiczenie: Łamanie haseł z użyciem narzędzia John The Ripper metodą siłową

Podstawowym programem Linuxowym służącym do łamania haseł jest **John The Ripper**. W wielu dystrybucjach (np. Debian, Red Hat, Arch) znajduje się on w pakietach. Pozwoli on nam znaleźć słabe hasła użytkowników.

W celu złamania haseł Linuxowych przy użyciu komendy `john` należy najpierw użyć narzędzia `unshadow` w celu przekazania plików `/etc/passwd` oraz `/etc/shadow` jako argumenty wejścia do programu `john`.

Kopiujemy oba pliki (tworzymy kopię zapasową):

```
cd
cat /etc/passwd > password-file
sudo cat /etc/shadow > shadow-file
```

Tworzymy plik `wordlist.txt` o następującej, przykładowej treści

```
touch wordlist.txt
echo '1234' >> wordlist.txt
echo 'test1234' >> wordlist.txt
echo 'haslo' >> wordlist.txt
echo 'hasło' >> wordlist.txt
echo 'qwe' >> wordlist.txt
echo 'qwerty' >> wordlist.txt
echo 'qwe123' >> wordlist.txt
echo 'haslo1!' >> wordlist.txt
echo 'asdqwe' >> wordlist.txt
echo 'asdqwe123' >> wordlist.txt
echo '123qweasd' >> wordlist.txt
```

Uwaga: W celu sprawdzenia efektów działania programu `john`, przed wykonaniem ćwiczenia, warto wpisać hasło wybranego użytkownika (np. własnego) do ww. pliku, lub stworzyć nowego użytkownika i nadać mu jedno z ww. haseł lub zmienić wybranemu użytkonikowi hasło

```
sudo passwd
# zmiana własnego hasła
```

```
sudo useradd [nazwa_uzytkownika] # stworzenie nowego użytkownika
sudo passwd [nazwa_uzytkownika] # nadanie hasła nowemu użytkownikowi

sudo passwd [nazwa_uzytkownika]
# zmiana hasła użytkownika
```

Oczywiście po zmianie haseł musimy ponownie skopiować oba pliki:

```
cat /etc/passwd > password-file
sudo cat /etc/shadow > shadow-file
```

Następnie sprawdzamy zawartość katalogu oraz przygotowanych plików

```
ls
cat shadow-file
cat password-file
```

Wykorzystujemy `unshadow`, aby przygotować zawartość plików `/etc/passwd` oraz `/etc/shadow` dla programu `john`

```
unshadow password-file shadow-file > for_john
cat for_john
```

Ostatecznie, crackujemy hasło

```
john for_john --wordlist=wordlist.txt
cat wordlist.txt | grep -c ""
```

Crack the hash

```
echo '48bb6e862e54f2a795ffc4e541caed4d' > hash_to_crack
# Wprowadzamy hash do pliku

hashid hash_to_crack
# sprawdzamy, potencjalny typ hashu

john -format=raw-md5 hash_to_crack
# staramy się złamać hash o formacie raw-md5, znajdujący się w pliku hash_to_crack
```

Więcej ćwiczeń:

- tryhackme.com - Cracking hashes challenges
- tryhackme - crack the hash