System operacyjny Linux

Dystrybucja Arudius

Arudius

- Arudius to Linux live CD bazujący na dystrybucji Slackware Linux, Zenwalk Linux i Linux Live scripts. Zawiera on obszerny zbiór oprogramowania używanego przez profesjonalistów ds. bezpieczeństwa z branży IT, do testowania i wykrywania luk w zabezpieczeniach. Celem twórców jest zawarcie jak najwięcej przydatnych narzędzi gwarantujących wysoki poziom bezpieczeństwa, utrzymując przy tym małe obciążenie komputera.

Użytkownicy

- Najważniejszym użytkownikiem systemu jest root
- Możesz dodać dowolną liczbę użytkowników poleceniem ***useradd*** wydanym z poziomu konsoli

  np. useradd –m uczen
- Każde konto musi być zabezpieczone hasłem, komenda ***passwd*** nazwa_konta

  np. passwd uczen

Wykonaj

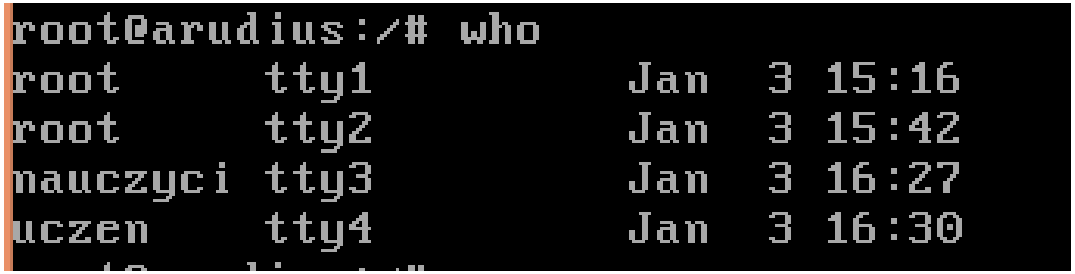
- Zaloguj się jako root
- Utwórz konta użytkownika uczen z hasłem uczen
- Utwórz konto użytkownika gosc z hasłem gosc

Uwaga

- Korzystając z lewego ALT +F2 możesz zmienić konsolę. Zaloguj się na tty2 jako uczen
- ALT+F3 na tty3 zaloguj się jako gosc
- ALT+F1 wracasz na tty1 czyli konto root-a

Polecenia

- who – możesz sprawdzić kto jest zalogowany na Twoim komputerze



Konto konsola data i godzina zalogowania

Pliki i katalogi

- Polecenie ls wyświetla zawartość katalogu

```
root@arudius:~# ls
arudius_list.txt  tools/
root@arudius:~# _
```

- Polecenie ls z nazwą katalogu wyświetli jego zawartoś

ls /tools

```
root@arudius:~# ls tools
aimsniff-1.0alpha/  framework-2.5/  nikto-1.35/  siphon/  therev/
cisco-torch/        httprint_301/   passifist/   smbat/   wmap1.3/
fakeap-0.3.2/       massrooter/     scapy-1.0.2/ snacktime/
root@arudius:~# _
```

Pliki i katalogi

Istnieje możliwość wyświetlenia i odczytania bardziej szczegółowych informacji. Do polecenia ls dodamy *przełącznik –l* (litera)

np. ls /usr –l

```
root@arudius:~# ls /usr -l
total 0
lrwxrwxrwx  1 root root     5 2006-03-15 23:10 X11 -> X11R6/
drwxr-xr-x  4 root root    42 2005-12-30 02:00 X11R6/
lrwxrwxrwx  1 root root     8 2006-03-15 23:10 adm -> /var/adm/
drwxr-xr-x  4 root bin  11758 2006-03-15 22:30 bin/
drwxr-xr-x  4 root root    13 2005-12-31 07:36 com/
drwxr-xr-x  4 root root     0 1993-11-25 22:40 dict/
drwxr-xr-x  4 root root    59 2006-03-15 22:30 doc/
drwxr-xr-x  4 root root    23 2005-11-19 06:20 etc/
drwxr-xr-x  4 root root    16 2005-04-21 15:45 i486-slackware-linux/
drwxr-xr-x  4 root root  4293 2006-03-15 22:30 include/
drwxr-xr-x  4 root root    81 2005-08-05 01:11 info/
drwxr-xr-x  4 root root 14576 2006-03-15 22:30 lib/
drwxr-xr-x  4 root root   259 2006-03-13 07:22 libexec/
```

Odczytujemy

Odczytanie zapisu liczbowego jest jednoznaczne

7=4+2+1	rwx
6=4+2+0	rw-
5=4+0+1	r-x
4=4+0+0	r—
3=0+2+1	-wx
2=	
1=	
0=	

Szczegółowe informacje

Prawa dostępu	Liczba powiązań	Właściciel	Grupa przypisania do pliku	Rozmiar	Data i godzina modyfikacji	Nazwa elementu
drwxr-xr-x	4	Root	Root	42	20014-12-30 02:00	X11R6

Prawa dostępu

Pierwsza kolumna, zawierająca uprawnienia, zawsze ma długość 10-ciu znaków

Pierwszy znak może przyjąć następujące wartości

d – katalog

- - zwykły plik

b – specjalny plik blokowy

c – specjalny plik znakowy

l – link symboliczny

s – gniazdo (ang. Socket)

? – inny, nieznany rodzaj pliku

Atrybuty pliku, katalogu

Kolejne dziewięć znaków tworzy trzy równe grupy. Pierwsza to zbiór praw dla właściciela pliku, druga to prawa grupy, a trzecia dla pozostałych użytkowników.
Literki w każdej grupie mają przypisane znaczenia np. ***rwx***
r – read prawo odczytu
w – write prawo zapisu
x – execute atrybut wykonywalności
Zapis ***r-x*** oznacza prawo odczytu, bez prawa zapisu oraz x oznacza możliwość otwarcia katalogu.

Zapis liczbowy

Oprócz notacji literowej (zwanym zapisem flagi) istnieje zapis liczbowy. Jego podstawą są cztery liczby, które mają odzwierciedlenie w zapisie literowym.

Atrybut pliku(prawa)	Symbol	Liczba
Wykonywanie	x	1
Zapis	w	2
Odczyt	r	4
Brak uprawnień	-	0

Uprawnienia zapisane w postaci symbolicznej

rwxr-xr-x

Uprawnienia dla właściciela	rwx	4+2+1=7
Uprawnienia dla grupy	r-x	4+0+1=5
Uprawnienia dla innych	r-x	4+0+1=5

- Uprawnienia, które w zapisie literowym oznaczone zostały rwxr-xr-x, w zapisie liczbowym przyjmują wartość 755

Ćwiczenia

Zapis symboliczny	Zapis liczbowy	Opis
	600	
	644	
	666	
	700	
	777	
-rwx- -x - x		
-rwxr – xr – x		
drwxr - - r - -		

Co ukrywa Linux ?

Wpisz polecenie ls z przełącznikiem –a

ls -a

```
root@arudius:~# ls -a
./              .ethereal/     .gnome2/          .msf/           .siegerc
../             .fluxbox/      .gnome2_private/  .nessusrc       .ssh/
.Xauthority     .fullcircle/   .gnupg/           .nessusrc.cert  .xinitrc
.airsnortrc     .gconf/        .icons/           .qt/            arudius_list.txt
.bash_history   .gconfd/       .links/           .rnd            tools/
.esd_auth       .gnome/        .mozilla/         .scapy_history
root@arudius:~# ls
arudius_list.txt  tools/
root@arudius:~# _
```

Kropka przed nazwą oznacza atrybut ***ukryty***

Prawa dostępu

Można zmieniać prawa dostępu do plików i katalogów poleceniem ***chmod***

Składnia: chmod kategoria operatory[+/-/=] uprawnienia nazwa_pliku

Opis kategorii użytkowników

u – użytkownik (user)
g – grupa (group)
o – inni (other)
a – wszyscy (all)

Operatory

+ - dodajemy uprawnienie
- - odbieramy uprawnienia
= - zmieniamy uprawnienia

Przykład:

chmod u=rwx,g+rw,o-r plik.txt

Właściciel ma prawo odczytu, zapisu i wykonania, grupie doda prawo zapisu i odczytu a innym odbierze prawo odczytu.

Ćwiczenia

- Zaloguj się jako root i w katalogu home utwórz katalog nowy
- Sprawdź jakie ma prawa poleceniem ls –l
- Zmień prawa tak by tylko właściciel miał prawo otwierania tego folderu (odbierz x grupie i wszystkim)
- Sprawdź zmianę

```
-rw-r--r--  1 root root 6684 2005-12-29 05:57 arudius_list.txt
drwxr-xr-x  2 root root   60 2015-01-04 15:08 nowy/
root@arudius:/home#
root@arudius:/home#
root@arudius:/home#
root@arudius:/home# chmod u=rwx,g+w,o-x nowy
root@arudius:/home# ls -l
total 7
-rw-r--r--  1 root root 6684 2005-12-29 05:57 arudius_list.txt
drwxrwxr--  2 root root   60 2015-01-04 15:08 nowy/
```

Zaloguj się na konsoli tty2 jako uczeń i spróbuj otworzyć katalog nowy

```
uczen@arudius:/home$ cd nowy
-sh: cd: nowy: Permission denied
uczen@arudius:/home$ ls -l
total 7
-rw-r--r--  1 root  root  6684 2005-12-29 05:57 arudius_
drwxrwxr--  2 root  root    60 2015-01-04 15:08 nowy/
drwxr-xr-x  2 uczen users   60 2015-01-04 15:12 uczen/
uczen@arudius:/home$ _
```

Prawa dostępu

Możemy zmieniać prawa w postaci liczbowej np. zapis praw drwxrwxr – x rozbijemy na grupy

	u	g	o
d	rwx	rwx	r - x
	421	421	401
	7	7	5

Polecenie zamiany będzie zatem wyglądało następująco :

chmod 755 nowy

Inne komendy

- mkdir – tworzy nowy katalog
- rmdir – usuwa katalogi
- cd – zmienia katalog bieżący
- pwd informacja o bieżącym katalogu
- tree – wyświetla drzewo katalogu

Edytor tekstu vi

- Edytor ma dwa tryby pracy tryb poleceń i tryb edycji. W trybie poleceń wydajesz polecenia co chcesz zrobić, w trybie edycji piszesz tekst.
- Przełącznikiem jest dla trybu edycji jest INS, natomiast tryb poleceń klawisz ESC
- Polecenie vi nazwa_pliku.txt tworzy nowy plik, lub otwiera istniejący
- Polecenie :w zapisuje plik w trybie poleceń
- Polecenie :q zamyka edytor

Zadania

- Utwórz katalog informatyka i nadaj mu pełne prawa dla wszystkich
- Utwórz plik podanie.txt każdy z grupy może go czytać, właściciel może czytać i pisać
- Utwórz plik list.txt gdzie nikt nie może pisać
- Utwórz plik cw2 i odbierz wszystkim prawa wykonywania