	Państwowa Wyższa Szkoła Zawodowa w Nysie		Wydział Nauk Technicznych		
	Laboratorium Podstaw Systemów Komputerowych				
Kierunek:	Informatyka	Rok studiów nr:	1	Semestr nr:	2
Rok akademicki:	2020/2021	Grupa administracyjna:	L5	Grupa ćwiczeniowa:	L5g1

SPRAWOZDANIE

Nr ćwiczenia	Temat ćwiczenia			
4	Zabezpieczanie konta root-a			
Termin złożenia sprawozdania				
Termin wg listy				
Data faktycznego złożenia sprawozdania				
(nie wypełniaj)				
Wykonawcy	Nazwisko	Imię	Nr indeksu	Ocena
	Roszak	Damian		(Nie wypełniane w trybie online)
				(Nie wypełniane w trybie online)

Uwaga: Umieszczenie danych osobowych wykonawców stanowi grupowe i nieodwołalne oświadczenie, że są oni/one (i tylko oni/one) współautorami przedstawionego sprawozdania. Późniejsza zmiana składu zespołu wykonawców nie będzie możliwa.

Nie wypełniać przy składaniu online

Data i podpis prowadzącego
ćwiczenia

Wymagania typograficzne

- Tekst główny (w ramach) należy składać czcionką normalną typu **Times 12 pkt.**
- Zawartość plików, nazwy ścieżek w systemie plików, polecenia wydawane z konsoli i używane odpowiedzi systemu/aplikacji oraz kopie tabulogramów interakcji z powłoką należy składać czcionką normalną typu **Courier 11 pkt.** Należy zachować wygląd, w tym pozycjonowanie tekstu.
- Nazwy pozycji menu w programach i nazwy przycisków ekranowych należy składać czcionką pogrubioną typu **Arial 11 pkt.**
- Wykluczone jest zamieszczanie ilustracji graficznych z ciemnym tłem. Tekst powinien z tłem wyraźnie kontrastować.

1. Temat ćwiczenia

(kopia tematu instrukcji, identyczna jak tytuł sprawozdania)

Zabezpieczanie konta root-a.

2. Zakres ćwiczenia

Streszczenie treści ćwiczenia oraz ustalenia prowadzącego zajęcia dotyczące wyboru funkcji badanego programu, zastosowanego algorytmu, zbioru przetwarzanych danych, precyzji przedstawienia liczb, liczby wątków i cykli obliczeń, sposobu prezentacji wyników, itp.)

Przedmiotem ćwiczenia jest zaprezentowanie sposobów zwiększania bezpieczeństwa konta superużytkownika systemu *N*X, polegającego na uniemożliwieniu mu bezpośredniego logowania się do systemu. Zamiast tego, wykonuje się logowanie na konto specjalnego użytkownika, który po zalogowaniu wchodzi w prawa użytkownika root. Grono specjalnych użytkowników stanowi grupę wheel (CentOS) lub sudo (Ubuntu).

3. Środowisko realizacji ćwiczenia

(architektura logiczna systemu – sprzęt, elementy składowe, ich cechy i sposób wzajemnego połączenia, schematy; wykorzystywane języki, oprogramowanie, biblioteki, skrypty powłokowe, zasoby sieciowe i dokumentacja)

CentOS Linux 7.5-2G jako maszyna wirtualna stworzona z pomocą oprogramowania wirtualizującego VMware Workstation 16 Player uruchomioną w środowisku Windows 10.

4. Przebieg ćwiczenia i uzyskane wyniki

(przedstawienie czynności wykonanych w ramach realizacji ćwiczenia, w kolejności określonej treścią instrukcji.

Dla każdego punktu instrukcji należy przedstawić: nr i tytuł tego punktu, cel działania, sposób wykonania, otrzymany rezultat i jego ocenę). Wymagana jest 100% chronologia zadań, czynności i uzyskanych rezultatów.

4.1 Zadanie nr 1

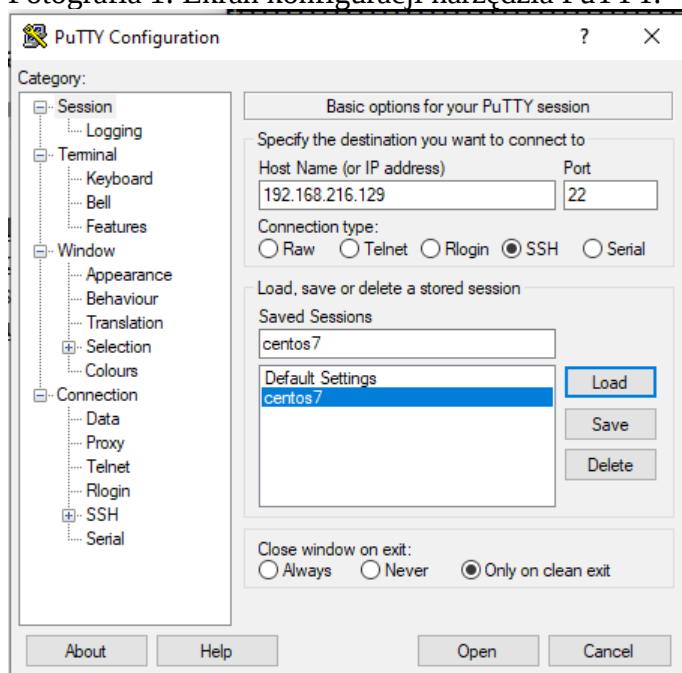
4.1.1 Nr i treść polecenia wg instrukcji: 2.1 Połączenie się z systemem docelowym przez SSH

4.1.2 Cel czynności: Korzystając z terminala putty, połączyć się jako superużytkownik z systemem Linux w maszynie wirtualnej.

4.1.3 Sposób i rezultat:

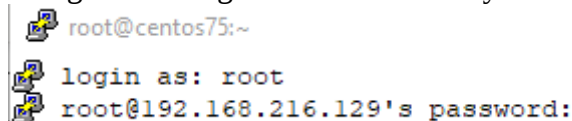
Rozpoczynam od uruchomienia programu VMware Workstation 16 Player. Następnie uruchamiam w nim maszynę wirtualną CentOS Linux 7.5-2G, po jej uruchomieniu program PuTTY (fot. 1) i dokonuję jego konfiguracji w zakresie niezbędnym do nawiązania połączenia z maszyną wirtualną.

Fotografia 1: Ekran konfiguracji narzędzia PuTTY.



Po skonfigurowaniu, nawiązuję połączenie z maszyną wirtualną oraz loguję się na konto użytkownika root, fot. 2.:

Fotografia 2. Logowanie na konto użytkownika root w terminalu putty.



```
root@centos75:~  
login as: root  
root@192.168.216.129's password:
```

Po poprawnym zalogowaniu terminal wyświetla ekran startowy CentOS'a dla użytkownika root, który przedstawiam wycinkiem z logu terminala.:

```
==~==~==~==~==~==~==~==~==~== PuTTY log 2021.04.16 10:48:44 ==~==~==~==~==~==~==~==  
login as: root  
root@192.168.216.129's password:  
Last login: Fri Apr 16 10:11:50 2021 from 192.168.216.1
```

```
+-----+  
|                               Wita Cie maszyna CentOS 7.5                               1.1|  
|-----+  
|   Konfiguracja: VCPU 2, RAM 1 GB, HDD 2,0 GB, polaczenie sieciowe NAT   |  
+-----+  
| * Minimalna konfiguracja Centos-7.5 oraz dodatkowo zainstalowane pakiety: |  
|   gcc, gpm, nano, mc, net-tools, htop, openmpi, openmpi-devel           |  
+-----+  
|   Przed przystapieniem do korzystania z Open MPI wykonaj dzialania opisane |  
|   w pliku /root/dotyczy_OpenMPI/_CZYTAJ_TO.                             |  
+-----+  
|   W sieci LAN można polaczyc sie z serwerami 172.30.205.20x, np. za pomoca |  
|   aplikacji mc: Prawy/Lewy panel -> Polaczenie po powloce               |  
+-----+  
| * Sprawdzenie adresu IP maszyny poleceniem ifconfig.                   |  
+-----+  
|   Zatrzymanie maszyny: shutdown now                                     |  
+-----+
```

Jeśli chcesz ponownie odczytać ten komunikat, wpisz polecenie `cat /etc/motd`.

[root@centos75 ~]#

4.1.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

Zadanie niezwykle proste do wykonania, nie zajmuje więcej niż kilka chwil.

4.2 Zadanie nr 2

4.2.1 Nr i treść polecenia wg instrukcji: 2.2 Utworzenie konta użytkownika specjalnego i przypisanie mu mocnego hasła.

4.2.2 Cel czynności: Zmylenie potencjalnych atakujących, nowe konto nie wyróżniające się nazwą nie będzie brane pod uwagę przy próbie przejęcia kontroli nad systemem poprzez konto użytkownika root. Jednocześnie nowe konto zabezpieczone silnym hasłem będzie zapewniało pełną funkcjonalność konta użytkownika root.

4.2.3 Sposób i rezultat wykonania polecenia (np. polecenia wydane na konsoli i odpowiedź systemu/aplikacji, w postaci wycinka zarejestrowanego logu konwersacji terminalowej w formie tekstowym). Dopuszcza się zamieszczenie fragmentu zrzutu ekranowego. W każdym przypadku obraz rezultatu ma obejmować wykonania wyłącznie danego punktu (a nie wszystko, co widać w oknie terminala lub konsoli). Log konwersacji musi zawierać następujące bezpośrednio po niej zaproszenie (tzw. *prompt*) powłoki.

Na początek dokonuję wyboru nazwy konta nowego użytkownika, wg zasady, że nazwa powinna być banalna i nie sugerująca prawdziwego przeznaczenia konta: szarik102

Następnie wybieram hasło, wg zasady minimum 10 znaków, duże i małe litery, cyfry i znaki specjalne, a dodatkowo uwzględniam zasadę, że jeśli to możliwe znaki nie powtarzały się oraz by taki ciąg coś mi sugerował aby łatwiej mi było zapamiętać hasło.: *****

Po czym w terminalu jako root wykonuję kolejno polecenia:

```
useradd szarik102
passwd *****
```

a następnie podaję nowe hasło:

Poniżej zamieszczam efekt działania poleceń z logu terminala:

```
[root@centos75 ~]# useradd szarik102
```

```
[root@centos75 ~]# passwd *****
```

Zmianie hasła użytkownika szarik102.

Nowe hasło :

Proszę ponownie podać nowe hasło :

passwd: zaktualizowanie wszystkich tokenów uwierzytelniania się powiodło.

4.2.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

Przy zmianie hasła należy zwrócić szczególną uwagę czy polecenie passwd podaje się z parametrem czy bez i czy ten parametr jest nazwą użytkownika czy faktycznym parametrem. W przypadku nie podania parametru, będąc zalogowanym jako użytkownik root, polecenie przejdzie do zmiany jego hasła, gdyż polecenie to bezparametru i bez nazwy użytkownika, zmienia hasło użytkownika, który je wywołał – stąd wzmiankowana ostrożność, dotycząca również podawanych parametrów, gdyż poleceniem dokonuje się znaczących zmian w systemie i lepiej być ich świadomym. Użyta w zadaniu wersja polecenia jest bez parametru, natomiast zawiera nazwę użytkownika, którego hasło zostaje zmienione.

4.3 Zadanie nr 3

4.3.1 Nr i treść polecenia wg instrukcji: 2.3 Włączenie użytkownika specjalnego do grupy zaufanej o nazwie wheel.

4.3.2 Cel czynności: Dodanie nowego konta użytkownika do grupy wheel, czyli umożliwienie korzystania z uprawnień root-a.

4.3.3 Sposób i rezultat wykonania polecenia (np. polecenia wydane na konsoli i odpowiedź systemu/aplikacji, w postaci wycinka zarejestrowanego logu konwersacji terminalowej w formacie tekstowym). Dopuszcza się zamieszczenie fragmentu zrzutu ekranowego. W każdym przypadku obraz rezultatu ma obejmować wykonania wyłącznie danego punktu (a nie wszystko, co widać w oknie terminala lub konsoli). Log konwersacji musi zawierać następujące bezpośrednio po niej zaproszenie (tzw. *prompt*) powłoki.

Zadanie realizuję wpisując w terminalu polecenie:

```
usermod -aG wheel szarik102
```

Następnie sprawdzam przynależność konta do grupy wheel poleceniem:

```
id szarik102
```

Wpisane polecenia dały następujący wynik w terminalu:

```
[root@centos75 ~]# usermod -aG wheel szarik102
```

```
[root@centos75 ~]# id szarik102
```

```
uid=1001(szarik102) gid=1001(szarik102) grupy=1001(szarik102),10(wheel)
```

```
[root@centos75 ~]#
```

4.3.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

Jak widać na załączonym fragmencie logu, konto użytkownika szarik102 zostało pomyślnie dodane do grupy wheel.

4.4 Zadanie nr 4

4.4.1 2.4 Sprawdzenie/aktualizacja pliku `/etc/sudoers` za pomocą edytora visudo

4.4.2 Cel: Sprawdzenie czy plik `/etc/sudoers` zawiera niezakomentowany wpis dotyczący grupy wheel, jeśli tak odkomentowanie go, czyli potwierdzenie, że grupa wheel ma prawo korzystać z polecenia sudo.

4.4.3 Sposób i rezultat:

Po wpisaniu polecenia:

```
visudo -f /etc/sudoers
```

terminal za pomocą programu visudo wyświetlił plik `/etc/sudoers` i umożliwił jego przejrzenie. Odnalazłem linijkę dotyczącą grupy wheel, tj.: zaczynającą się od `%wheel`, i potwierdziłem, że nie zaczyna się ona znakiem „#”, co jest celem zadania, na potwierdzenie zamieszczam właściwy fragment logu.:

```
## Allows people in group wheel to run all commands
%wheel    ALL=(ALL)        ALL
```

4.4.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

Plik `/etc/sudoers` kontroluje dostęp do narzędzia sudo, dlatego należało zadbać o właściwy wpis dla grupy wheel.

4.5 Zadanie nr 5

4.5.1 Nr i treść polecenia wg instrukcji: 2.5 Sprawdzenie poprawności logowania użytkownika specjalnego

4.5.2 Cel czynności: Kontrola poprawności dotychczas wykonanych czynności.

4.5.3 Sposób i rezultat

Sposobem na sprawdzenie poprawności logowania użytkownika specjalnego jest wpisanie następujących komend `su - szarik102` oraz `ls /root`:

```
[root@centos75 ~]# su - szarik102
Ostatnie logowanie: pią kwi 16 18:10:49 CEST 2021 na pts/0
[szarik102@centos75 ~]$ ls /root
ls: nie można otworzyć katalogu /root: Brak dostępu
[szarik102@centos75 ~]$
```

Jak widać drugie polecenie nie zadziałało, gdyż konto użytkownika, nie posiada uprawnień root-a. Do tego celu skorzystam z polecenia:

```
sudo ls /root
```

To polecenie zadziałało i terminal zwrócił następujący efekt.:

```
[szarik102@centos75 ~]$ sudo ls /root
```

Ufamy, że lokalny administrator udzielił odpowiedniego szkolenia.

Zwykle sprowadza się ono do tych trzech rzeczy:

- 1) należy respektować prywatność innych,
- 2) należy myśleć przed pisanie,
- 3) z dużą władzą wiąże się duża odpowiedzialność

[sudo] hasło użytkownika szarik102:

```
cat          head          klscpu.txt      stary
\n           cpu.txt       --help          k.cppmes.kopia  tail
anaconda-ks.cfg CPU.txt      ifc             log.bootplik    wc
boot.log     dotyczy_MPI  ipc            ls              plik2
[szarik102@centos75 ~]$
```

Jak widać po zaakceptowaniu wpisanego hasła system wyświetlił zawartość katalogu /root.

4.5.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

Polecenie `su` służy do zmiany użytkownika (z ang. switch user), bez podania nazwy użytkownika przechodzi do użytkownika `root`. Kreska w poleceniu `su` – umożliwia po zalogowaniu być w katalogu domowym użytkownika, na którego następuje przełączenie. Polecenie `sudo` uruchamia pojedyncze polecenie z uprawnieniami `roota`. Jest to kluczowa różnica między `su` i `sudo`. Polecenie `su` przełącza użytkownika na konto użytkownika `root` i wymaga hasła do konta `root`. Polecenie `sudo` uruchamia pojedyncze polecenie z uprawnieniami `roota` - nie przełącza do konta użytkownika `root` i też wymaga hasła z tym, że do konta wywołującego je użytkownika.

Aby nie trzeba było każdego polecenia poprzedzać przez `sudo`, w otwartej sesji będę używał kombinacji poleceń.: `sudo su -`

4.6 Zadanie nr 6

- 4.6.1 2.6 Sprawdzenie możliwości logowania użytkownika specjalnego z zewnątrz
- 4.6.2 Cel: Upewnienie się, że nowe konto jest w stanie zastąpić zdalnie konto `root-a`.
- 4.6.3 Sposób i rezultat wykonania:

Do wykonania zadania wykonuję połączenie z użyciem narzędzia `putty`, logując się na nowo utworzone konto `szarik102`. Po wpisaniu loginu i hasła terminal wyświetlił ekran startowy jak wcześniej dla konta użytkownika `root`, z tą różnicą, że teraz prompt ma postać.: `[szarik102@centos75 ~]$`

Efekt logowania jest następujący.:

```
==~==~==~==~==~==~==~==~==~== PuTTY log 2021.04.16 18:46:41 ==~==~==~==~==~==~==~==
login as: szarik102
szarik102@192.168.216.129's password:
Last login: Fri Apr 16 18:19:03 2021
```

```
+-----+
|                               Wita Cie maszyna CentOS 7.5                               1.1|
|-----+
|  Konfiguracja: VCPU 2, RAM 1 GB, HDD 2,0 GB, polaczenie sieciowe NAT                    |
+-----+
| * Minimalna konfiguracja Centos-7.5 oraz dodatkowo zainstalowane pakiety:            |
|  gcc, gpm, nano, mc, net-tools, htop, openmpi, openmpi-devel                          |
+-----+
|  Przed przystąpieniem do korzystania z Open MPI wykonaj działania opisane           |
```

```
| w pliku /root/dotyczy_OpenMPI/_CZYTAJ_TO. |
+-----+
| W sieci LAN można połączyć się z serwerami 172.30.205.20x, np. za pomocą |
| aplikacji mc: Prawy/Lewy panel -> Połączenie po powłoce |
+-----+
| * Sprawdzenie adresu IP maszyny poleceniem ifconfig. |
+-----+
| Zatrzymanie maszyny: shutdown now |
+-----+
```

Jeśli chcesz ponownie odczytać ten komunikat, wpisz polecenie `cat /etc/motd`.

```
[szarik102@centos75 ~]$
```

Po zalogowaniu się wydaję komendę „`sudo su -`”, której log jest następujący:

```
[szarik102@centos75 ~]$ sudo su -
[sudo] hasło użytkownika szarik102:
Ostatnie logowanie: pią kwi 16 18:17:25 CEST 2021 z 192.168.216.1 na pts/0
[root@centos75 ~]#
```

Jak widać wydanie komendy „`sudo su -`” spowodowało zmianę promptu na `[root@centos75 ~]#` w tym znaku zachęty z dolara \$ na hasz #, co informuje, że użytkownik root zalogował się na swoje konto i do swojego folderu domowego – o czym informuje tylda.

4.6.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

Po wykonaniu wszystkich powyższych czynności zdalne logowanie się na konto użytkownika specjalnego jest możliwe. Jak również za jego pomocą, na konto root.

4.7 Zadanie nr 7

4.7.1 Nr i treść polecenia wg instrukcji: 2.7 Zablokowanie możliwości logowania się root-a przez SSH.

4.7.2 Cel czynności: Zabezpieczenie systemu przed zdalnym nie powołanym dostępem do konta root-a.

4.7.3 Sposób i rezultat:

Najpierw upewniam się, że mam możliwość pracy zdalnej z prawami superużytkownika przy wykorzystaniu utworzonego konta użytkownika specjalnego. Robię to w sposób opisany w poprzednim zadaniu. Następnie w pliku `/etc/ssh/sshd_config` odszukuję zapis `PermitRootLogin yes` i zamieniam go na `PermitRootLogin no`, efekt:

- znaleziony fragment posiada następującą postać: `#PermitRootLogin yes`, zauważam, że jest objęty komentarzem poprzez znak „#”, który usuwam i zmieniam wpis na „`PermitRootLogin no`”.

Teraz restartuję serwer SSH poleceniem: `systemctl restart sshd` i wylogowuję się oraz zamykam sesję putty. Po tych czynnościach na powrót nawiązuje połączenie z pomocą putty i zaczynam od próby zalogowania się na konto użytkownika root, która kończy się odmową dostępu mimo kilkukrotnego wpisania prawidłowego hasła, co widać na tym fragmencie logu.:

```
===== PuTTY log 2021.04.16 20:51:40 =====
login as: root
root@192.168.216.129's password:
Access denied
root@192.168.216.129's password:
Access denied
root@192.168.216.129's password:
Access denied
```

```
root@192.168.216.129's password:
Access denied
root@192.168.216.129's password:
Access denied
root@192.168.216.129's password:
```

Natomiast próba logowania się na nowoutworzone konto użytkownika specjalnego wraz z wydaniem komendy „sudo su -” zakończyła się pełnym sukcesem, co pokazuje następujący fragment logu.:

```
[szarik102@centos75 ~]$ sudo su -
[sudo] hasło użytkownika szarik102:
Ostatnie logowanie: pią kwi 16 20:50:26 CEST 2021 z 192.168.216.1 na pts/0
Ostatnie nieudane logowanie: pią kwi 16 20:52:06 CEST 2021 z 192.168.216.1 na
ssh:notty
Nastąpiło 6 nieudanych prób zalogowania od ostatniego udanego logowania.
[root@centos75 ~]#
```

4.7.4 Ocena/wnioski/komentarze dotyczące wykonania danego zadania.

Zmiana wpisu #PermitRootLogin yes w pliku /etc/ssh/sshd_config na PermitRootLogin no skutecznie zablokowała możliwość zdalnego logowania się na konto root-a. Od teraz aby móc zdalnie zarządzać systemem będę używał konta szarik102, które posiada już stosowne funkcjonalności.

Praca zdalna jest jak najbardziej możliwa, pierwsza różnica między kontami root-a i użytkownika specjalnego to oczywiście konieczność uzyskania uprawnień root-a do pracy na dotychczasowych zasadach, natomiast kolejna, to wynikająca z pierwszej, że konto użytkownika specjalnego to nie konto root-a i na odwrót.

O czym należy pamiętać, by nie dokonać zmian, których się nie chce (o czym informował sam system podczas zastosowania polecenia sudo wylistowania zawartości katalogu /root w pkt. 4.5) oraz, by nie oczekiwać, że system coś zrobi kiedy brakuje uprawnień lub gdy jest potrzebna dodatkowa autentykacja, jak w przypadku zamykania systemu zdalnie, co obrazuje następujący fragment logu.:

```
[root@centos75 ~]# logout
[szarik102@centos75 ~]$ shutdown now
==== AUTHENTICATING FOR org.freedesktop.login1.power-off ====
Wymagane jest uwierzytelnienie, aby wyłączyć system.
Multiple identities can be used for authentication:
 1. les
 2. szarik102
Choose identity to authenticate as (1-2): Failed to execute operation: Method call timed out
Must be root.
[szarik102@centos75 ~]$ shutdown now
==== AUTHENTICATING FOR org.freedesktop.login1.power-off ====
Wymagane jest uwierzytelnienie, aby wyłączyć system.
Multiple identities can be used for authentication:
 1. les
 2. szarik102
Choose identity to authenticate as (1-2): 2
Password:
==== AUTHENTICATION COMPLETE ====
```

Jak widać bez stosownego uwierzytelnienia nie można zamknąć CentOS-a. Nowo utworzone konto użytkownika specjalnego posiada taką możliwość, co wskazał sam system operacyjny zgłaszając potrzebę uwierzytelnienia przed wyłączeniem się. Dotychczas, tzn. podczas pracy na koncie root, zamknięcie systemu

następowało bezzwłocznie po wydaniu komendy `shutdown now`, w przypadku korzystania z konta użytkownika specjalnego należy ponadto dokonać uwierzytelnienia, aby wyłączyć system.

5. Wnioski z przeprowadzonych prac

(podsumowanie celu ćwiczenia i osiągniętych wyników, wnioski dotyczące zastosowanych środków programowych i uzyskanych wyników, samoocena stopnia osiągnięcia celu ćwiczenia)

Wykonane czynności płynnie doprowadziły mnie do zastąpienia pracy zdalnej na koncie `root`, na pracę zdalną na koncie użytkownika specjalnego, zachowując możliwości i funkcjonalność konta `root`. Poprzez stworzenie dodatkowego nie rzucającego się w oczy konta użytkownika specjalnego oraz nadając mu możliwość korzystania z polecenia `sudo`, dodanie go do grupy `wheel` będącej w pliku `/etc/sudoers` i posiadającej odpowiednie prawa, mogłem wyłączyć możliwość logowania się zdalnego na konto `root-a`.

Dzięki tak skonfigurowanemu kontu użytkownika `root`, potencjalny napastnik nie będzie mógł połączyć się z systemem zdalnie bezpośrednio poprzez to konto, a co za tym idzie zmniejsza się szansa na dokonanie skutecznego cyberataku. Ta możliwość nadal istnieje, gdyż system posiada konto pozwalające na prace w trybie konta `root` z jednoczesną możliwością zdalnego połączenia. Dlatego też, tworząc nowe przeznaczone do takiej pracy konto, zadbałem o to by jego nazwa była banalna i niesugerująca, że ma jakiś związek z kontem `root` oraz by jego hasło było skomplikowane i niedające się łatwo odgadnąć.

Taka konfiguracja kont utrudnia rozeznanie się w sytuacji napastnikowi oraz zwiększa poziom bezpieczeństwa pracy na tak skonfigurowanym systemie operacyjnym. Jest również niezbędna w dzisiejszej rzeczywistości cyberbezpieczeństwa.

6. Inne uwagi

Bardzo fajne zadanie, to właśnie dzięki takim zadaniom chcę studiować informatykę.