

1. Certyfikat EFS używany w NTS zawiera: a,b,d

1. Certyfikat EFS używany w NTFS zawiera:

- o klucz, którym szyfruje się pliki
- o klucz, którym deszyfruje się pliki
- o klucz publiczny użytkownika, używany do odszyfrowywania kluczy FEK
- o klucz publiczny użytkownika, używany do szyfrowania kluczy FEK

2. Które stwierdzenia dotyczące blokady konta użytkownika w systemie Windows są nieprawdziwe: d

4. Które stwierdzenia dotyczące blokady konta użytkownika w systemie Windows są nieprawdziwe:

- o licznik prób logowania jest zerowany po każdym nieudanym logowaniu
- o licznik prób logowania jest zerowany automatycznie po zadanym czasie
- o licznik prób logowania może wyzerować administrator
- o licznik prób logowania jest zerowany po każdym pomyślnym zalogowaniu

3. Zasoby systemu operacyjnego MS Windows udostępnione poprzez SMB: d

6. Zasoby systemu operacyjnego MS Windows udostępnione poprzez SMB:

- o są dostępne zdalnie tylko dla tych użytkowników, którzy posiadają lokalne konto w systemie operacyjnym
- o nazywa się portami
- o zawsze wymagają uwierzytelniania (podania hasła) przy dostępie zdalnym
- o mogą mieć ograniczony dostęp do odczytu i/lub zapisu tylko dla wskazanych użytkowników

4. Użytkownik U systemu Linux należący do grupy G1 nie ma wpisu na liście ACL do zasobu O w systemie plików. Jednak grupie G1 na liście ACL zasobu O nadano prawa r i x, a uprawnienia domyślne tego zasobu wynoszą rwx. Jakie efektywne uprawnienia do O posiada U? (U nie jest właścicielem O i nie należy do grupy zasobu O, mask=rwx) b

7. Użytkownik U systemu Linux należący do grupy G1 nie ma wpisu na liście ACL do zasobu O w systemie plików. Jednak grupie G1 na liście ACL zasobu O nadano prawa r i x, a uprawnienia domyślne tego zasobu wynoszą rwx. Jakie efektywne uprawnienia do O posiada U? (U nie jest właścicielem O i nie należy do grupy zasobu O, mask=rwx)

- o tylko r
- o rx
- o rwx
- o żadne

5. Co użytkownik może zrobić za pomocą komendy ulimit? b,c

8. Co użytkownik może zrobić za pomocą komendy ulimit?

- o zwiększyć swoje uprawnienia dostępu do plików
- o zablokować możliwość dokonywania zrzutu obrazu pamięci procesu do pliku (core dump)
- o ograniczyć liczbę jednocześnie otwartych plików
- o ograniczyć uprawnienia dostępu do swoich plików dla innych użytkowników

6. Jakie mechanizmy kryptograficzne są niezbędne w celu zapewnienia niezaprzecjalności (ang.nonrepudation) w kontekście poczty elektronicznej? b

- o wiadomość musi być podpisana elektronicznie kluczem publicznym nadawcy
- o wiadomość musi być podpisana elektronicznie kluczem prywatnym nadawcy

oczta.student.put.poznan.pl/service/home/~/?auth=co&loc=pl&id=5744&part=2

024, 13:19

poczta.student.put.poznan.pl/service/home/~/?auth=co&loc=pl&id=5744&part=2

- o do wiadomości musi zostać dołączony certyfikat poświadczony przez zaufany urząd CA
- o wiadomość musi zostać zaszyfrowana kluczem symetrycznym znanym jedynie stronom komunikacji

7. Mechanizm wirtualizacji dostępu do newralgicznych komponentów systemu Windows: a,c

10. Mechanizm wirtualizacji dostępu do newralgicznych komponentów systemu Windows:

- o dotyczy niektórych obiektów rejestru systemowego
- o może być włączany/wyłączany przez użytkownika dla jego własnych procesów
- o dotyczy niektórych obiektów systemu plików
- o jest stosowany wyłącznie wobec aplikacji 64-bitowych

8. Których wpisów ACE na liście POSIX ACL dotyczy maska: c,d

11. Których wpisów ACE na liście POSIX ACL dotyczy maska:

- o właściciela obiektu
- o grupy (domyślnej) pliku (z bazowych ACE)
- o każdej jawnie wpisanej grupy
- o wszystkich użytkowników niewpisanych jawnie, ale należących do dowolnej jawnie wpisanej grupy

9. Wskaż wszystkie warunki konieczne do weryfikacji podpisu cyfrowego wiadomości S/MIME: c

12. Wskaż wszystkie warunki konieczne do weryfikacji podpisu cyfrowego wiadomości S/MIME:

- o uprzednie przekazanie do nadawcy klucza publicznego odbiorcy
- o dostęp odbiorcy do certyfikatu klucza publicznego CA, który certyfikował klucz publiczny nadawcy
- o uprzednie przekazanie do odbiorcy klucza publicznego nadawcy
- o poprawna wymiana kluczy między nadawcą a odbiorcą metodą Diffiego-Hellmana

10. Maska: b, c

- 16.

```
$ getfacl skrypt
  user::rw-
  user:jbond:r-x
  group::rwx
  group:agents:rwx
  mask::r-x
  other::-w-
```

Oznacza, że:

- o grupa agents może zmodyfikować skrypt
- o grupa domyślna (owning group) może zmodyfikować skrypt
- o użytkownik jbond może wykonać skrypt
- o pozostali użytkownicy mogą zmodyfikować skrypt

11. TCP Wrapper może korzystać z dwóch plików z regułami polityki, przy czym: d

17. TCP Wrapper może korzystać z dwóch plików z regułami polityki, przy czym:

- ponieważ stosuje zasadę pierwszego dopasowania, plik `/etc/hosts.deny` może nie być w ogóle sprawdzany
- jeśli reguła nie zostaje odnaleziona w żadnym pliku, to dostęp zostaje odrzucony
- najpierw sprawdzane są reguły z pliku `/etc/hosts.deny`, a ewentualnie później reguły z pliku `/etc/hosts.allow`
- najpierw sprawdzane są reguły z pliku `/etc/hosts.allow`, a ewentualnie później reguły z pliku `/etc/hosts.deny`

12. Które stwierdzenia najlepiej opisują mechanizm Bypass Traverse Checking: b

18. Które stwierdzenia najlepiej opisują mechanizm Bypass Traverse Checking:

- pozwala na wyświetlanie zawartości katalogu, do którego użytkownik nie ma przyznanego dostępu, ale ma dostęp do któregokolwiek pliku wewnętrz
- pozwala na ominięcie sprawdzania uprawnień do katalogów na ścieżce do pliku, do którego użytkownik ma przyznaną dostęp
- pozwala na zestawianie tunelu IPsec w sieci wykorzystującej NAT (NAT-T)

<https://poczta.student.put.poznan.pl/service/home/~/?auth=co&loc=pl&id=5744&part=2>

2/3

1.01.2024, 13:19

poczta.student.put.poznan.pl/service/home/~/?auth=co&loc=pl&id=5744&part=2

- pozwala na dostęp do udziałów sieciowych bez konieczności posiadania konta w zdalnym systemie

13. Które z poniższych poleceń pozwolą ustawić bit SGID dla katalogu dir: b

20. Które z poniższych poleceń pozwolą ustawić bit SGID dla katalogu dir:

- set-suid dir
- chmod g+s dir
- sgid --set dir
- setfacl -m group::s

14. Uprawnienia domyślne POSIX ACL oznaczają: d

1. Uprawnienia domyślne POSIX ACL oznaczają:

- uprawnienia obowiązujące użytkowników spoza listy ACL
- minimalne uprawnienia do danego obiektu dla wszystkich użytkowników
- uprawnienia ustawiane po wyczyszczeniu listy ACL (`setfacl -b`)
- uprawnienia nadawane nowym elementom utworzonym w danym katalogu

15. Dany jest plik Tajne.txt w katalogu Jawne. c

2. Dany jest plik Tajne.txt w katalogu Jawne. Założmy, że użytkownik Adaś należy do grupy Users. Katalog Jawne ma przydzielone uprawnienia ACL dla grupy Users: ALLOW na czytanie i DENY na zapis. Plik Tajne.txt ma uprawnienia ALLOW na zapis dla użytkownika Adaś. Jakie uprawnienia ostatecznie ma Adaś do pliku Tajne.txt?

- ma uprawnienia do odczytu, brak uprawnień do zapisu
- brak uprawnień do odczytu i zapisu
- ma uprawnienia do odczytu i zapisu
- ma uprawnienia do zapisu, brak uprawnień do odczytu

16. Użytkownik U systemu Linux. c

3. Użytkownik U systemu Linux należący do grupy G1 otrzymał jawnie na liście ACL prawa r oraz w do zasobu O w systemie plików. Grupie G1 na liście ACL zasobu O nadano prawa w oraz x, a maska zawiera prawa r oraz x. Jakie efektywne uprawnienia do O posiada U? (U nie jest właścicielem O i nie należy do grupy zasobu O)

- tylko r
- tylko w
- rw
- rx

17. Które zdania są prawdziwe w odniesieniu do aktywnego mechanizmu UAC w systemie Windows: a,c,d

7. Które zdania są prawdziwe w odniesieniu do aktywnego mechanizmu UAC w systemie Windows:

- jeśli zwykły użytkownik chce wykonać operację wymagającą uprawnień administratora zostanie zapytany o hasło administratora
- UAC blokuje możliwość instalacji programów przez administratora
- zmiana istotnych gałęzi rejestru systemu wymaga świadomej reakcji uprawnionego użytkownika
- UAC chroni przed przypadkowym uruchomieniem potencjalnie niebezpiecznych programów przez użytkownika

18. Które stwierdzenia dotyczące blokady konta w systemie Windows są prawdziwe: c,d

10. Które stwierdzenia dotyczące blokady konta w systemie Windows są prawdziwe:

- licznik prób logowania jest zerowany po każdej udanej próbie logowania
- w czasie określonym długością okresu zerowania licznika prób logowania, użytkownik nie może podjąć więcej udanych prób logowania niż określa próg blokady
- istnieje ustawienie progu blokady dopuszczające nieblokowanie konta mimo dowolnej liczby niepomyślnych prób logowania
- próg blokady określa ilość kolejnych niepomyślnych prób logowania, po osiągnięciu której dostęp do konta będzie zablokowany trwale (do odwołania przez administratora)

19. Czy pakiet PGP(GPG) używa szyfrowania symetrycznego? b

12. Czy pakiet PGP(GPG) używa szyfrowania symetrycznego?

- tak, treść listu jest zawsze szyfrowana algorytmem symetrycznym
- nie, PGP stosuje tylko kryptografię klucza publicznego
- tak, np. do szyfrowania plików
- tak, nadawca i odbiorca generują metodą DH wspólny klucz sesji na podstawie swoich kluczy publicznych

20. Grupa użytkowników systemie MS Windows o nazwie Użytkownicy uwierzytelnieni:a,c

13. Grupa użytkowników systemie MS Windows o nazwie Użytkownicy uwierzytelnieni:

- nie obejmuje konta Gość
- obejmuje wszystkich użytkowników lokalnych
- jest podziobrem grupy Wszyscy
- jest identyczna z grupą Wszyscy

21. Windows Firewall pozwala tworzyć reguły: a,b,c,d

16. Windows Firewall pozwala tworzyć reguły:

- blokujące wybrany ruch
- blokujące odbieranie ruchu sieciowego przez wskazane programy
- przepuszczające wybrany ruch
- blokujące wysyłanie ruchu sieciowego przez wskazane programy

22. Bezpośrednim efektem operacji eksportu certyfikatu PKCS#12 jest: d

17. Bezpośrednim efektem operacji eksportu certyfikatu do formatu PKCS#12 jest:

- przekazanie klucza publicznego innemu użytkownikowi w celu umożliwienia mu wysłania do nas zaszyfrowanej poczty
- wyodrębnienie z certyfikatu klucza publicznego w celu dołączenia go do kryptogramu przesyłanej wiadomości
- wyodrębnienie z certyfikatu klucza prywatnego w celu dołączenia go do wykonanego podpisu elektronicznego wiadomości
- utworzenie kopii zapasowej klucza prywatnego i publicznego w pliku

23. Mechanizm sudo można tak skonfigurować by: a,b,d

18. Mechanizm sudo można tak skonfigurować by:

- nigdy nie wymagał podania hasła
- wymagał podania hasła użytkownika, w ramach konta którego należy wykonać polecenie
- wykonał polecenie bez pytania o hasło użytkownika o ile plik programu tego polecenia ma ustawiony bit SUID
- wymagał podania hasła bieżącego użytkownika przy każdym poleceniu

24. Maska: b,c

20.

```
$ getfacl skrypt
  user::rw-
  user:jbond:r-x
  group::rwx
  group:agents:rwx
  mask::r-x
  other::-w-
```

Oznacza, że:

- grupa agents może zmodyfikować skrypt
- grupa domyślna (owning group) może zmodyfikować skrypt
- użytkownik jbond może wykonać skrypt
- pozostali użytkownicy mogą zmodyfikować skrypt

25. Mechanizm Lock-and-Key: d

4.

Mechanizm Lock-and-Key:

- służy do translacji reguł filtracji z jednej zapory na inną
- wymaga uwierzytelnienia użytkownika, np. za pomocą RADIUS-a
- automatycznie blokuje stacje nie spełniające wymagań polityki bezpieczeństwa
- może być wykorzystany do tymczasowego uzyskania uprzywilejowanego dostępu do sieci wewnętrznej z zewnątrz

26. W modelu uwierzytelnienia z udziałem zaufanej trzeciej strony, do zadań tej trzeciej strony należy: c,d

5. W modelu uwierzytelniania z udziałem zaufanej trzeciej strony, do zadań tej trzeciej strony należy:

- przekazane danych uwierzytelniających strony uwierzytelnianej docelowemu serwerowi
- przekazane danych uwierzytelniających stronie uwierzytelnianej
- wystawienie poświadczania uwierzytelnienia stronie uwierzytelnianej
- pobranie danych uwierzytelniających od strony uwierzytelnianej

27. Które z poniższych protokołów służą do realizacji kryptograficznych tuneli wirtualnych: a,b

6. Które z poniższych protokołów służą do realizacji kryptograficznych tuneli wirtualnych:

- o **TLS**
- o **ESP**
- o **IKE**
- o **SSO**

28. Jakie restrykcje wprowadza flaga HTTPOnly w definicji ciasteczka WWW? a

8. Jakie restrykcje wprowadza flaga HTTPOnly w definicji ciasteczka WWW?

- o wartości ciasteczka nie można odczytać w skryptach
- o ciasteczko będzie wysyłane do serwera tylko w tunelu kryptograficznym
- o dostęp tylko do ciasteczka ma tylko oryginalna strona, która utworzyła ciasteczko
- o ciasteczka nie wolno przesyłać w sesji SSL/TLS

29. Które z poniższych określeń opisują protokół Radius: a,c

12. Które z poniższych określeń opisują protokół RADIUS:

- o pozwala na scentralizowane przechowywanie danych uwierzytelniających dla wielu punktów dostępowych
- o podnosi dostępność poprzez redundantne rozproszenie danych uwierzytelniających do wielu punktów dostępowych
- o udostępnia informacje niezbędne do kontroli uprawnień zdalnego dostępu (np. restrykcje czasowe)
- o oferuje wymianę kluczy protokołu IPsec przy wykorzystaniu zarówno haseł jak i certyfikatów PKI

30. Jak zachowa się system kontroli ACL standardu POSIX. d

13. Jak zachowa się system kontroli ACL standardu POSIX w przypadku użytkownika U należącego do grupy G i wpisanego na liście ACL obiektu p, jeśli ani U ani G nie mają jawnie przydzielonego prawa r, ale kategoria "wszyscy użytkownicy" (others) takie uprawnienie do obiektu p posiada:

- o prawo r do obiektu p zostanie efektywnie przyznane, o ile U jest właścicielem p
- o prawo r do obiektu p nie zostanie efektywnie przyznane
- o prawo r do obiektu p zostanie efektywnie przyznane bezwarunkowo
- o prawo r do obiektu p zostanie efektywnie przyznane, o ile maska na to pozwala

31. Jakiego typu pakiety są wykorzystywane w atakach sieciowych zalewających ofiarę (flooding)?

b

15. Jakiego typu pakiety są wykorzystywane w atakach sieciowych zalewających ofiarę (flooding)?

- o **ARP**
- o **TCP SYN**
- o **TCP RST**
- o **ICMP**

32. Standard IEEE 802.1X: a,d

1. Standard IEEE 802.1X:

- o realizuje uwierzytelnianie i kontrolę dostępu do lokalnej infrastruktury sieciowej
- o dotyczy zabezpieczenia poufności
- o dotyczy uprawnień dostępu do zasobów plikowych
- o może współpracować z protokołami takimi jak RADIUS lub TACACS+

33. Które z wymienionych technik mogą być wykorzystane do uwierzytelnienia z hasłami jednorazowymi: c,d

3. Które z wymienionych technik mogą być wykorzystane do uwierzytelniania z hasłami jednorazowymi:

- o certyfikacja klucza sesji
- o jednokrotne uwierzytelnianie (single sign-on)
- o metoda zawołanie-odzew (challenge-response)
- o synchronizacja czasu

34. W metodzie uzgadniania klucza Diffiego-Helmana system może zostać skompromitowany poprzez: c,d

5. W metodzie uzgadniania klucza Diffiego-Hellmana system może zostać skompromitowany poprzez:

- o przechwycenie (poznanie) jednego z wymienianych kluczy
- o przechwycenie (poznanie) obu wymienianych kluczy
- o podstawienie fałszywego klucza w miejsce każdego z wymienianych
- o podstawienie fałszywego klucza w miejsce jednego z wymienianych

35. Wskaż operacje niedozwolone w systemie kontroli dostępu MAC: b,d

6. Wskaż operacje niedozwolone w systemie kontroli dostępu MAC:

- o read-down
- o read-up
- o write-up
- o write-down

36. Jakie restrykcje wprowadza flaga Secure w definicji ciasteczka WWW? a

7. Jakie restrykcje wprowadza flaga Secure w definicji ciasteczka WWW?

- o ciasteczko będzie wysyłane do serwera tylko w tunelu kryptograficznym
- o dostęp do ciasteczka ma tylko oryginalna strona, która utworzyła ciasteczko
- o ciasteczko musiało zostać sprawdzone przez filtr SOP
- o do ciasteczka nie można uzyskać dostępu w skryptach

37. Niezaprzecjalność to własność potwierdzająca iż: b

10. Niezaprzecjalność to własność potwierdzająca iż:

- o nadawca wiadomości jest rzeczywiście tym za kogo się podaje
- o nadawca wiadomości faktycznie ją wysłał
- o odbiorca wiadomości faktycznie ją otrzymał
- o odbiorca wiadomości nie sfałszował jej treści

38. Następująca reguła filtracji zapory sieciowej: a

11. Następująca reguła filtracji zapory sieciowej:

od	do	źródłowy	docelowy	port	protokół	flagi	reakcja
..*.*	->	1.1.1.1	*	80	TCP	SYN=1	odrzuć

- o blokuje wszelkie połączenia nawiązywane z serwerem www o adresie 1.1.1.1
- o blokuje wszelkie połączenia nawiązywane z serwera www o dowolnym adresie
- o blokuje wszelkie połączenia nawiązywane z serwerem www o dowolnym adresie
- o blokuje wszelkie połączenia nawiązywane z serwera www o adresie 1.1.1.1

39. Wskaż cechy zapory sieciowej zrealizowanej poprzez Komputer-Twierdzę: a,b,c,d

15. Wskaż cechy zapory sieciowej zrealizowanej poprzez Komputer-Twierdzę (Bastion Host):

- dla ruchu z zewnątrz zapora "przykrywa" sobą całą sieć wewnętrzna
- w systemie operacyjnym nie jest realizowany routing
- dla ruchu od wewnętrz zapora "przykrywa" sobą cały świat zewnętrzny
- komunikacja zachodzi wyłącznie przez usługi proxy

40. Określ prawidłową kolejność: d

41. Systemy NAC: d

16. Określ prawidłową kolejność pełnej sekwencji odwołań klienta do serwerów w przypadku dostępu do usługi SMTP w środowisku Kerberos:

- serwer AS - serwer TGS - serwer SMTP - serwer AS
- serwer TGS - serwer AS - serwer SMTP
- serwer TGS - serwer AS - serwer TGS - serwer SMTP
- serwer AS - serwer TGS - serwer SMTP

17. Systemy NAC (Network Admission Control):

- oferują filtrację poczty elektronicznej
- służą realizacji rozległych korporacyjnych sieci VPN
- to zapory sieciowe stosujące bezstanowe reguły filtracji
- umożliwiają blokowanie ruchu sieciowego ze stacji nie spełniających wymagań polityki bezpieczeństwa

42. Elementem ochrony przed złośliwym wykorzystaniem bufora: a,d

20. Elementem ochrony przed złośliwym wykorzystaniem przepełnienia bufora może być:

- remapowanie (dereferencja) adresu 0
- randomizacja przydziału przestrzeni adresowej procesu
- randomizacja adresu obsługi przerwania/wyjątku
- wstawienie "kanarka" bezpośrednio po adresie powrotu z funkcji

43. Poleceniem ulimit użytym przez użytkownika w powłoce można: c

1. Poleceniem `ulimit` użyтыm przez użytkownika w powłoce można:

- stworzyć ograniczenia zasobów obowiązujące wszystkie procesy tego użytkownika w systemie, ale tylko aż do zakończenia bieżącej sesji (wylogowania użytkownika)
- stworzyć ograniczenia zasobów obowiązujące wszystkie procesy tego użytkownika w systemie (także już te istniejące)
- stworzyć ograniczenia zasobów obowiązujące wszystkie nowe procesy tego użytkownika w systemie
- stworzyć ograniczenia zasobów obowiązujące tylko daną powłokę i jej procesy potomne

44. Maska: d

4.

```
$ getfacl test
  user::rwx
  user:jbond:rwx
  group::r--
  group:agents:r-x
  mask::r-x
  other::---
  default:user::rwx
  default:user:jbond:r-x
  default:group::wx
  default:group:agents:wx
  default:mask::wx
  default:other::r-x
Oznacza, że:
```

- użytkownik jbond może tworzyć pliki w katalogu test
- grupa agents może tworzyć nowe pliki w nowych podkatalogach katalogu test
- grupa agents może modyfikować zawartość obiektu test
- użytkownik jbond może przeglądać listę plików w katalogu test

45. Mechanizm sudo umożliwia: b

11.

Mechanizm sudo umożliwia:

- miękkie (soft) zmniejszenie limitów użytkownika
- uruchamianie polecen z uprawnieniami administratora po podaniu własnego (domyślnie) hasła
- miękkie (soft) zwiększenie limitów użytkownika
- uruchamianie wybranych aplikacji z uprawnieniami innych użytkowników

46. Czym różnią się klauzule drop i reject w akcjach reguły iptables? b

14.

Czym różnią się klauzule DROP i REJECT w akcjach reguły iptables?

- obie odrzucają pakiety, ale REJECT dotyczy tylko łańcucha FORWARD
- obie odrzucają pakiety, ale DROP zawsze robi to "po cichu"
- obie odrzucają pakiety, ale DROP powoduje przerwanie przeglądania reguł, a REJECT nie
- REJECT odrzuca pakiety warunkowo, a DROP bezwarunkowo

47. Autentyczność kluczy publicznych PGP jest weryfikowana: c

15.

Autentyczność kluczy publicznych PGP jest weryfikowana:

- poprzez PKI (infrastrukturę klucza publicznego)
- przez pozyskanie certyfikatu klucza publicznego
- metodą Web of Trust, w której użytkownicy PGP podpisują sobie wzajemnie klucze
- poprzez weryfikację podpisu urzędu CA pod kluczem użytkownika

48. Udział IPC\$ jest to: c

16.

Udział IPC\$ jest to:

- udział domyślny służący do dostępu do dysku C w celu zdalnej administracji
- endpoint kryptograficznej komunikacji IPsec
- udział do zdalnych wywołań procedur RPC
- udział domyślny kontrolera domeny służący do obsługi logowania w sieci

49. Możliwe metody uwierzytelniania użytkownika w protokole SSH to: a,c

3. Możliwe metody uwierzytelniania użytkownika w protokole SSH to:

- hasło użytkownika
- mechanizm TOFU (Trust On First Use)
- asymetryczne klucze kryptograficzne
- symetryczne klucze kryptograficzne

50. Kto może nadawać i modyfikować uprawnienia POSIX ACL danego obiektu w systemie plików:
b,d

4. Kto może nadawać/modyfikować uprawnienia POSIX ACL danego obiektu w systemie plików:

- właściciel obiektu, ale pod warunkiem, że posiada prawo 'w'
- właściciel obiektu, niezależnie od posiadania prawa 'w'
- dowolny użytkownik posiadający prawo 'w'
- administrator (root)

51. Mechanizm impersonation systemu Windows: a,b

5. Mechanizm impersonation systemu Windows:

- jest wykorzystywany do uruchamiania programów przez polecenie runas
- pozwala procesowi użyć chwilowo innego niż bieżący tokenu zabezpieczeń
- pozwala użytkownikowi przejąć na własność wybrane obiekty systemu plików
- pozwala użytkownikowi zdefiniować dla swoich plików innego właściciela (np. grupę)

52. Wskaż prawdziwe stwierdzenia dotyczące szyfrowania treści plików EFS: b

pozwala użytkownikowi zdefiniować dla swoich plików innego właściciela (np. grupę)

6. Wskaż prawdziwe stwierdzenia dotyczące szyfrowania treści plików mechanizmem EFS:

- każdy plik szyfrowany jest kluczem publicznym właściciela pliku
- każdy plik szyfrowany jest innym kluczem
- plik udostępniony przez właściciela 2 innym użytkownikom jest szyfrowany 3 kluczami
- każdy plik szyfrowany jest kluczem prywatnym właściciela pliku

53. Wskaż różnicę między dwoma poleceniami sudo su oraz su: c

8. Wskaż różnicę między dwoma poleceniami: sudo su oraz su.

- nie ma żadnej różnicy, obie komendy zawsze zachowają się tak samo
- sudo su może nie wymagać podania hasła, su natomiast zawsze będzie wymagać (o ile to hasło zostało ustawione)
- sudo su może wymagać podania hasła bieżącego użytkownika, su natomiast hasła administratora
- su będzie wymagać podania hasła bieżącego użytkownika, sudo su natomiast hasła administratora

54. Protokół TLS w usłudze poczty elektronicznej stosuje się do: a

administratora

9. Protokół TLS w usłudze poczty elektronicznej stosuje się do:

- tworzenia bezpiecznego kanalu komunikacji programu klienta z serwerem poczty
- uwierzytelniania nadawcy konkretnej wiadomości
- podpisywania cyfrowego treści listu
- szyfrowania załączników wiadomości

55. Który opis pasuje do poniższej konfiguracji TCP wrappera: a,d

11. Który opis pasuje do poniższej konfiguracji TCP wrappera:

```
ftpd : ALL EXCEPT www : ALLOW  
ALL  : ALL  : twist /bin/echo "OK"
```

- za wyjątkiem komputera www umożliwia każdemu dostęp do każdej usługi
- zabrania dostępu do usługi WWW z komputera ftpd
- umożliwia dostęp do usługi FTP z komputera www
- zabrania dostępu do usługi FTP z komputera www

56. Zaznacz poprawne warunki, których spełnienie w systemie plików NTFS pozwoli: a,b

12. Zaznacz poprawne warunki, których spełnienie w systemie plików NTFS pozwoli by użytkownik U należący do grupy G mógł odczytać zawartość pliku P w katalogu K:

- U lub G dziedziczą dostęp do odczytu z katalogu K
- U lub G mają jawnie nadane prawo odczytu pliku P
- U jawnie odebrano prawo odczytu P, ale U dziedziczy to prawo z katalogu K
- U jawnie odebrano prawo odczytu P, ale G dziedziczy to prawo z katalogu K

57. Pliki zwirtualizowane mechanizmem UAC: a

13. Pliki zwirtualizowane mechanizmem UAC przechowywane są w systemie Windows w:

- katalogu "%WINDIR%\User Access Container\Sandbox"
- katalogu "%SYSTEMDRIVE%\VirtualStore"
- katalogu "VirtualStore" lokalnym dla każdego użytkownika
- alternatywnych strumieniach danych (ADS) systemu NTFS

58. Czego nie można ograniczyć za pomocą komendy ulimit? b

14. Czego nie można ograniczyć za pomocą komendy ulimit?

- wielkości pliku zrzutu pamięci
- sumy zajmowanej przestrzeni dyskowej przez pliki
- ilości otwartych deskryptorów
- ilości tworzonych procesów

59. Jakią właściwość można ustawić w Zasadach haseł? A,c

15. Jakią właściwość można ustawić w Zasadach haseł w systemie Windows?

- złożoność haseł
- włączenie szyfrowania AES haseł użytkowników
- minimalna długość nazwy użytkownika
- maksymalna długość nazwy użytkownika

60. Polecenie d

16. Polecenie

```
netsh advfirewall firewall add rule name="private"  
protocol=icmpv4 action=block dir=out remoteip=10.10.0.2
```

zablokuje możliwość:

- pingowania adresu 10.10.0.2 niezależnie od użycia IPv4 czy IPv6
- pingowania adresu 10.10.0.2 tylko w sieci o profilu prywatnym
- pingowania tylko po IPv4 bieżącego systemu z adresu 10.10.0.2 (bez wpływu na IPv6)
- pingowania tylko po IPv4 adresu 10.10.0.2 z bieżącego systemu (bez wpływu na IPv6)

61. W jaki sposób można jednoznacznie określić, które konto w systemie operacyjnym MS Windows jest wbudowanym kontem administracyjnym? d

17. W jaki sposób można jednoznacznie określić, które konto w systemie operacyjnym MS Windows jest wbudowanym kontem administracyjnym?

- ostatnia część identyfikatora tego konta ma stałą wartość 0
- aktualnie w Windows nie ma wbudowanego konta administracyjnego
- konto takie ma zawsze nazwę "Administrator"
- ostatnia część identyfikatora tego konta ma stałą wartość 500

62. W jaki sposób można udostępnić swój klucz publiczny PGP innemu użytkownikowi: a,b,c,d

19. W jaki sposób można udostępnić swój klucz publiczny PGP innemu użytkownikowi:

- przekazać osobiście na nośniku wymiennym
- umieścić na swojej stronie www
- wysłać pocztą elektroniczną
- umieścić w sieciowym repozytorium kluczy (tzw. serwerze kluczy)

63. Które z poniższych poleceń pozwala ustawić bit SUID dla katalogu dir: c

20. Które z poniższych poleceń pozwala ustawić bit SUID dla katalogu dir:

- suid --set dir
- setfacl -m user::s
- chmod u+s dir
- set-suid dir

64. PGP (GPG) używane jest do: c,d

1 PGP (GPG) używane jest do:

*realizacji tuneli VPN

*podpisywania plików muzycznych celem zachowania praw autorskich DRM

* [X] podpisywania danych

* [X] szyfrowania plików

65. Maska: a

```
2 $getfacl test
owner: jbond
group: agents
user::rw-
user:jbond:r-x
group:agents:--x
mask::r-x
other:---
W takim wypadku użytkownik jbond (będący właścicielem obiektu test), należący do gryu agents, ma efektywne uprawnienia:
*[X]rwx
*[X]r-x
*[X]r
*[X]rwx
```

66. Wybierz prawdziwe stwierdzenie: c,d

3 Wybierz prawdziwe stwierdzenie dotyczące ponieszego polecenia:
ssh -L 9999:neptun:23 pluto
*dane kierowane na port 999 systemu neptun zostaną rzesiane w niezabezpieczonej formie na port 23 systemu pluto
*[X]dane kierowane na port 9999 lokalnego systemu zostaną przesiane w niezabezpieczonej formie na port 23 systemu neptun
*[X]dane kierowane na port 9999 lokalnego systemu zostaną przesiane w zaszyfrowanej formie na port 22 systemu pluto
*w wyniku polecenia zestawiony zostanie tunel kryptograficzny między systemem neptun i systemem pluto

67. Klucz z certyfikatu EFS użytkownika U jest wykorzystywany w systemie NTFS do: a

6 Klucz z certyfikatu EFS użytkownika U jest wykorzystywany w systemie NTFS do:
*[X]szycfrowania jednorazowych kluczy, którymi zaszyfrowane zostały poszczególne pliki do których U ma dostęp
*szycfrowania i deszyfrowania treści plików należących do U
*szycfrowania i deszyfrowania wszelkiej komunikacji z użytkownikiem U (np. poczty elektronicznej)
*szycfrowania i deszyfrowania treści plików należących do użytkowników, którzy udostępnili te pliki użytkownikowi U

68. Mechanizm mandatory (MIC) system Windows: a,b,d

Mała zmiana odpowiedzi:
10 Mechanizm mandatory Integrity Control (MIC) system Windows:
*[X]pozwala ograniczyć swobodę komunikacji między procesami
*[X]pozwala ograniczyć dostęp do zapisu w systemie plików
*pozwala ograniczyć dostęp do odczytu dla wybranych plików
*[X]przypisuje procesowi jeden z kilku poziomów uprawnień uwzględnianych dodatkowo w kontroli dostępu

69. Lokalna zapora sieciowa systemu Windows na stanowisku X: d

2. Lokalna zapora sieciowa systemu Windows na stanowisku X zablokowała możliwość zdalnego odpytywania o dostępność X przy pomocy narzędzia ping, pozostawiając jednak możliwość zdalnego dostępu do serwera www w tym systemie. Mogła to osiągnąć poprzez:
- odrzucanie całego ruchu ICMP
 - zablokowanie komunikacji z siecią dla programu ping
 - wyłączenie ruchu IP na wszystkich interfejsach, ale pozostawienie dostępu do wskazanych portów TCP
 - wyłączenie obsługi przychodzących komunikatów ICMP echo

70. Kto może jako pierwszy dla danego pliku zaszyfrować ten plik mechanizmem EFS: a

3. Kto może jako pierwszy dla danego pliku zaszyfrować ten plik mechanizmem EFS:
- tylko właściciel pliku
 - każdy administrator, niezależnie od praw dostępu do pliku
 - każdy agent DRA, niezależnie od praw dostępu do pliku
 - każdy kto posiada prawo modyfikacji pliku

71. Nowoutworzony katalog w systemie Linux: a

12. Nowoutworzony katalog w systemie Linux:

- na liście ACL otrzymane skopiowane z katalogu nadzorowanego uprawnienia domyślne jako wpisy ACE
- na liście ACL otrzyma skopiowane z katalogu nadzorowanego uprawnienia domyślne jako wpisy DefaultACE
- na liście ACL otrzyma skopiowane wszystkie prawa efektywne oprócz prawa 'x' jako wpisy ACE
- zawsze otrzyma pustą listę ACL

72. W zależności od konfiguracji polityki sudoers program sudo może: a,b,c,d

18. W zależności od konfiguracji polityki **sudoers** program **sudo** może:

- zawsze pytać o hasło administratora
- wykonać polecenie bez pytania o hasło
- zapytać o hasło aktualnie zalogowanego użytkownika
- zapytać o hasło użytkownika, w imieniu którego polecenie ma zostać wykonane

73. Ataki o nazwie phishing:

39. Ataki o nazwie phishing:

- dotyczą wykradzenia zaufanych certyfikatów CA
- realizowane są za pośrednictwem poczty
- polegają na zatrudniania cache przeglądarki www
- realizowane są za pośrednictwem www

74. Które z wymienionych poniżej mechanizmów wspomagają wykrywanie podsłuchu w sieci:

40. Które z wymienionych poniżej mechanizmów wspomagają wykrywanie podsłuchu w sieci:

- 802.1X
- ARP
- 802.11X
- ICMP echo

75. Metoda Diffiego-Hellmana:

41. Metoda Diffiego-Hellmana:

- pozwala stronom komunikacji bezpiecznie ustalić wspólne klucze asymetryczne
- wymaga szyfrowania negocjacji w celu ochrony przed atakami pasywnymi
- pozwala stronom komunikacji bezpiecznie ustalić wspólny klucz symetryczny

-
-
-
- wymaga uwierzytelniania negocjacji w celu ochrony przed atakami aktywnym

76. Wskaż cechy charakteryzujące kontrolę dostępu MAC:

43. Wskaż cechy charakteryzujące kontrolę dostępu MAC

- tylko właściciel zasobu może dysponować prawami dostępu do tego zasobu
- etykiety ochrony danych przypisane do zasobów automatycznie wymuszają uprawnienia
- właściciel zasobu nie może dysponować prawami dostępu do tego zasobu
- tylko wybrany oficer bezpieczeństwa może dysponować prawami dostępu do zasobów

77. Wskaż możliwe sposoby ochrony przed atakami na protokół DHCP:

44. Wskaż możliwe sposoby ochrony przed atakami na protokół DHCP (takimi jak np. DHCP redirection, lease starvation):

- **DHCP Snooping - przełącznik przepuszcza odpowiedzi DHCP tylko z określonego wcześniej portu**
- **DHCP Hoping - zapora zamienia numer VLAN w zadaniach DHCP**
- ICMP redirection - wykorzystanie ICMP do ponownej zmiany trasy pakietów DHCP
- DHCP session hijacking - przejmowanie połączeń TCP sesji DHCP przez proxy

78. Wskaż protokoły wymagające zabezpieczenia autentyczności i integralności danych, ale niekoniecznie poufności:

46. Wskaż protokoły wymagające zabezpieczenia autentyczności i integralności danych, ale niekoniecznie poufności:

- **DNS (Domain Name Service)**
- ARP (Address Resolution Protocol)
- **STP (Spanning Tree Protocol)**
- rlogin (Remote Login)

79. Utworzenie strumienia ADS pliku wpływa na rozmiar samego pliku w systemie operacyjnym:

d

20. Utworzenie strumienia ADS pliku wpływa na rozmiar samego pliku widocznego w systemie operacyjnym:

- tylko jeżeli strumień ADS ma rozmiar większy od rozmiaru samego pliku
- zawsze (zmianę rozmiaru można zobaczyć zwykłym poleceniem `dir`)
- tylko jeśli wymusimy przeliczenie rozmiaru poleceniem `dir /r`
- zupełnie nie wpływa

80. Jeśli proces w systemie Windows jest na poziomie integralności X, to wówczas: b

9. Jeśli proces w systemie Windows jest na poziomie integralności X, to wówczas:

- może czytać i zapisywać wyłącznie pliki o tym samym poziomie integralności (o ile pozwala na to ACL)
- nie może pisać do plików o wyższym poziomie integralności, nawet jeżeli pozwala na to ACL
- może pisać do plików o wyższym poziomie integralności tylko, jeżeli jest ich właścicielem i ma jawnie nadane prawo zapisu w ACL
- nie może pisać do plików o niższym poziomie integralności, nawet jeżeli pozwala na to ACL

81. Który opis pasuje do poniższej konfiguracji TCP wrappera: b

8. Który opis pasuje do poniższej konfiguracji TCP wrappera:

```
ftpd : ALL EXCEPT www  
ALL  : ALL
```

- jeśli znajduje się w pliku `hosts.deny` to nie zabrania dostępu do usługi WWW z komputera `ftpd`
- jeśli znajduje się w pliku `hosts.allow` to zabrania dostępu do usługi FTP z komputera `www`
- jeśli znajduje się w pliku `hosts.allow` to zabrania dostępu do usługi WWW z komputera `ftpd`
- jeśli znajduje się w pliku `hosts.deny` to zabrania dostępu do usługi FTP z komputera `www`

82. Czy w katalogu KAT należącym: c

5. Czy w katalogu KAT należącym do zwykłego użytkownika systemu Linux, inny użytkownik może utworzyć (oczywiście mając do tego niezbędne uprawnienia POSIX ACL) taki obiekt którego później właściciel katalogu KAT nie będzie mógł usunąć?

- tak, jeśli obiektem jest plik
- nie, jeśli obiektem jest plik
- tak, jeśli obiektem jest katalog, który posiada zawartość
- nigdy, jeśli KAT ma ustawioną flagę SGID

83. Czego nie można ograniczyć za pomocą mechanizmu limitów zasobowych w systemie Linux?

d

4. Czego nie można ograniczyć za pomocą mechanizmu limitów zasobowych w systemie Linux?

- wielkości pliku zrzutu pamięci
- ilości wykorzystanej pamięci operacyjnej przez proces
- ilości otwartych deskryptorów
- ilości zalogowanych równocześnie użytkowników

84. Zaznacz poprawne warunki a,c,d

3. Zaznacz poprawne warunki, których spełnienie w systemie plików NTFS pozwoli by użytkownik U należący do grupy G mógł odczytać zawartość pliku P w katalogu K:

- tylko U ma jawnie nadany dostęp do P i K, G nie nadano żadnych praw ani do K, ani do P
- U jawnie odmówiono dostępu do odczytu P, ale G dziedziczy taki dostęp z katalogu nadzielnego
- U lub G mają jawnie nadane prawo odczytu pliku P
- tylko U dziedziczy dostęp do P i K, G nie dziedziczy żadnych praw ani do K, ani do P