Zebrane pytania z lat poprzednich by RD 2022/2023
Zielony marker - pewne odpowiedzi, potwierdzone przez ekursy.
Żółty marker - strzały roczników wyżej.
Czerwony marker - na pewno błędne.

1. Sieci VPN można zbudować wykorzystując: [1/1]

a) IDS
b) Wireguard
c) TLS
d) SIEM

2. Użytkownik Windows, będący administratorem, po zalogowaniu się do systemu: [1/1]

a) otrzyma pełny token uprawnień i zawsze będzie korzystał z pełnego tokenu
b) otrzyma token pełny i ograniczony, zawsze będzie korzystał z pełnego tokenu
c) otrzyma token pełny i ograniczony, będzie mógł korzystać z jednego lub drugiego
d) otrzyma tylko token ograniczony, ale będzie mógł wykorzystać pełny token przy użyciu mechanizmu impersonation

3. Metoda Diffiego-Hellmana:

a) pozwala bezpiecznie składować klucze prywatne użytkowników
b) jest odporna na ataki pasywne
c) jest odporna na ataki aktywne
d) pozwala bezpiecznie dystrybuować klucze publiczne użytkowników
e) wykorzystuje ideę asymetrycznej pary kluczy (prywatny-publiczny)
f) generuje programowo hasła SSO
g) pozwala wygenerować symetryczny klucz sesji
h) realizuje uwierzytelnianie metodą haseł jednorazowych

4. Usługa DNSsec: [1/1]

a) wykorzystuje IPsec do tunelowania zapytań i odpowiedzi DNS
b) wykorzystuje SSL do tunelowania zapytań i odpowiedzi DNS
c) wymaga podpisanych cyfrowo zapytań DNS
d) stosuje podpisy cyfrowe odpowiedzi DNS

5. Które metody uwierzytelniania stosuje protokół HTTP/1.1 [1/1]

a) tylko użycie jednokierunkowej funkcji skrótu
b) tylko username-password
c) zarówno username-password jak i użycie funkcji skrótu, ale nie certyfikaty X.509
d) zarówno username-password, funkcją skrótu, jak i certyfikaty X.509

6. Które komponenty systemu operacyjnego Windows mogą korzystać ze sprzętowej wirtualizacji celem podniesienia bezpieczeństwa systemu: [1/1]

a) Alpine docker containers
b) Defender Application Guard
c) AppContainer
d) Ring - 1 compartmentalization

7. Wskaż mechanizmy chroniące m.in. przed atakami przepełnienia bufora: [1/1]

a) wykorzystanie Structured Exception Handling i Vectored Exception Handling
b) zapewnienie by segment pamięci z prawem zapisu nie posiadał jednocześnie prawa wykonywania
c) randomizacja alokacji wirtualnej przestrzeni adresowej procesu - aslr
d) alokowanie na stosie dodatkowego elementu ramki funkcji wykrywającego modyfikację adresu powrotu - stack cookie (kanarek)

8. Mechanizm two-factor authentication (2FA): [1/1]

a) wymaga użycia 2 oddzielnych operacji (oraz danych) uwierzytelniających
b) dotyczy złożoności hasła i wymaga by nowe hasło różniło się od dotychczasowego na 2 pozycjach
c) to uwierzytelnianie z zaufaną stroną trzecią
d) to uwierzytelnianie metodą zawołanie-odzew

9. System Kerberos oferuje (wybierz wszystkie poprawne możliwości): [1/1]

a) kryptograficzne uwierzytelnianie użytkowników w ramach domeny
b) delegowanie uprawnień jednego podmiotu innym podmiotom
c) zastosowanie kryptograficznego weryfikatora w celu ochrony przed atakiem Golden Ticket
d) uwierzytelnianie użytkowników pomiędzy domenami

10. Komputer-Twierdza: [1/1]

a) dopuszcza komunikację przechodzącą tylko przez usługi proxy
b) to rodzaj zapory sieciowej z filtracją pakietów i modułem IDS
c) jest implementacją zapory typu Application Layer Gateway
d) pełni rolę zaufanej strony trzeciej w domenie Kerberos

11. Które komponenty sprzętowe służą (między innymi) do bezpiecznego przechowywania materiału kryptograficznego: [1/1]

a) IEEE 1609.2
b) X.509
c) EFS
d) Trusted Platform Module

12. Model CAP kontroli dostępu: [1/1]

a) jest stosowany w systemach MIC (Mandatory Integrity Control)
b) jest stosowany w systemach RBAC (Role-Based Access Control)
c) uprawnienia dostępu wiąże z podmiotami
d) uprawnienia dostępu wiąże z zasobami

13. Model kontroli dostępu MAC zabrania podmiotowi o etykiecie P: [1/1]

a) odczytu obiektu o niższej etykiecie niż P
b) zapisu obiektu o wyższej etykiecie niż P
c) odczytu obiektu o wyższej etykiecie niż P

14. Wskaż protokoły i standardy dokonujące uwierzytelniania dostępu do sieci, działające między klientem sieci (komputerem) a punktem (serwerem) dostępowym: [1/1]

a) IEEE 802.1X
b) TACACS
c) RADIUS
d) EAP

15. Protokół Kerberos: [1/1]

a) pozwala osiągnąć obustronne uwierzytelnienie klienta usługi sieciowej i serwera tej usługi
b) realizuje uwierzytelnianie w modelu z zaufaną stroną trzecią
c) realizuje uwierzytelnianie kryptograficzne z wykorzystaniem kluczy symetrycznych
d) realizuje uwierzytelnianie SSO w środowisku domenowym
e) realizuje uwierzytelnianie SSO w środowisku między-domenowym
f) umożliwia uwierzytelnianie i autoryzację klientów usług sieciowych przez scentralizowany mechanizm (serwer KDC)
g) nie wymaga znajomości po stronie uwierzytelniającej żadnych danych wrażliwych klienta (Zero-Proof Knowledge)

16. Wskaż możliwe prawidłowe reakcje na wykrycie faktu przepełnienia bufora (w segmencie stosu) umożliwiające zachowanie bezpieczeństwa systemu: [1/1]

a) ponowne zainicjowanie bufora domyślną wartością
b) usunięcie danych wykraczających poza bufor, zanim zostaną odczytane
c) natychmiastowe przerwanie działania procesu
d) zapisanie zaraz za nadmiernymi danymi “kanarka” ostrzegającego o wystąpieniu przepełniania przy próbie odczytu bufora

17. Systemy nadzoru NAC (Network Access Control): [0.5/1]

a) dokonują uwierzytelniania stanowisk sieciowych przed dopuszczeniem ich do sieci lokalnej
b) wykrywają pakiety na podstawie analizy behawioralnej i uczenia maszynowego
c) dopuszczają stanowiska do sieci lokalnej po weryfikacji zgodności ich konfiguracji z polityką bezpieczeństwa
d) wykrywają podejrzane pakiety na podstawie sygnatur ataków sieciowych

18. Protokół SSL/TLS: [1/1]

a) pozwala uwierzytelniać kryptograficznie zarówno klienta, jak i serwer
b) nigdy nie uwierzytelnia klienta, to zadanie wyłącznie protokołu aplikacyjnego, np. HTTP
c) nigdy nie dokonuje uwierzytelniania, zostawiając to zadanie innym protokołom, np. ISAKMP
d) kryptograficznie uwierzytelnia tylko serwer, klienta tylko hasłem
e) uwierzytelnianie obustronne uczestników komunikacji
f) szyfrowanie transmisji na poziomie warstwy sesji OSI
g) uwierzytelnianie SSO

h) szyfrowanie transmisji na poziomie warstwy transportowej OSI

19. Wskaż prawdziwe stwierdzenia dotyczące bramy aplikacyjnej Application Layer Gateway: [1/1]

a) pośredniczy w komunikacji wyłącznie na poziomie warstwy aplikacyjnej
b) optymalizuje ruch stosując filtrację kontekstową na podstawie tablicy aktywnych połączeń
c) wymaga działającego poprawnie routingu między interfejsami sieciowymi
d) filtruje pakiety na poziomie wszystkich 3 warstw: sieciowej, transportowej i aplikacyjnej

20. Które z poniższych algorytmów kryptograficznych mogą w praktyce zostać wykorzystane do zaszyfrowania treści listu e-mail: [1/1]

a) AES
b) RSA
c) Twofish
d) Blowfish

21. Technologie umożliwiające ochronę integralności transmitowanych danych to m.in:

a) protokół TLS
b) protokół AH
c) protokół ESP
d) SYN cookies

22. Szyfrowanie asymetryczne zapewnia:

a) autentyczność pod warunkiem zachowania tajności klucza prywatnego odbiorcy
b) poufność pod warunkiem zachowania tajności klucza prywatnego nadawcy
c) poufność pod warunkiem zachowania tajności klucza prywatnego odbiorcy
d) autentyczność pod warunkiem zachowania tajności klucza prywatnego nadawcy

23. Algorytm Lamporta, leżący u podstaw koncepcji programowej generacji haseł jednorazowych:

a) wymaga użycia funkcji jednokierunkowej
b) wymaga rozwiązania problemu rozproszonego konsensusu
c) wymaga wykorzystania kryptografii asymetrycznej
d) wymaga rozwiązania problemu rozproszonego wzajemnego wykluczania

24. Wskaż mechanizmy systemu operacyjnego będące realizacją (choćby częściową) koncepcji piaskownicy:

a) Windows AppContainer
b) SSL/TLS
c) click-jacking
d) wirtualizacja systemu operacyjnego

25. Pewna zapora sieciowa filtrująca pakiety realizuje jednocześnie funkcje NAT. Które opisy pasują do takiej zapory:

a) filtracja DNAT może być dokonywana dla pakietów przechodzących przez zaporę niezależnie od kierunku

b) translacja DNAT musi być dokonana przed routingiem pakietu aby pozycje tablicy routingu mogły być prawidłowo dopasowane
c) translacja DNAT musi być dokonana przed filtracją pakietu na interfejsie wejściowym, aby reguły łańcucha wejściowego mogły być prawidłowo dopasowane
d) translacja SNAT musi być dokonana przed filtracją kontekstową na interfejsie wyjściowym, aby pakiet znalazł prawidłowe dopasowanie do tablicy aktywnych połączeń

26. Jakie cechy wirtualizacji są istotne dla bezpieczeństwa systemu?
a) procesor utrudnia ucieczkę ze środowiska zwirtualizowanego poprzez ochronę komend hipervisora na poziomie Ring -1
b) wirtualizacja systemu operacyjnego daje efekt piaskownicy dla uruchomionych w tym systemie aplikacji
c) hypervisor pośredniczy w wywołaniach funkcji jąda systemu operacyjnego, więc może wychwytywać potencjalnie niebezpieczne zachowania
d) w systemie wirtualnym bezpośredni dostęp do pamięci fizycznej (w tym pamięci urządzeń I/O) nie jest możliwy nawet dla rozkazów Ring 0, co ułatwia izolację maszyn wirtualnych nawet w przypadku przejęcia uprawnień administracyjnych wewnątrz dowolnej z nich

27. Które z poniższych cech dotyczą szyfrowania asymetrycznego: [1/1]
a) odporność na kolizje
b) gwarancja autentyczności i niezaprzeczalności komunikacji
c) większa niż dla algorytmów symetrycznych efektywność

28. Które z poniższych cech dotyczą szyfrowania symetrycznego: [1/1]
a) odporność na kolizje
b) gwarancja autentyczności i niezaprzeczalności komunikacji
c) większa niż dla algorytmów asymetrycznych efektywność

29. Które z poniższych mechanizmów pozwalają w systemie operacyjnym na chwilowe uzyskanie innych uprawnień dostępu niż posiadane aktualnie przez użytkownika: [0.7/1]
a) Windows UAC
b) POSIX ACL
c) sudo
d) POSIX CAP

30. Wskaż cechy mechanizmu AppContainer:
a) kontroluje wywołania funkcji jądra systemu operacyjnego
b) jest “lekkim” odpowiednikiem maszyny wirtualnej, z tą różnicą, że nie zawiera zwirtualizowanego systemu operacyjnego, tylko aplikację i potrzebne biblioteki
c) wykorzystuje wirtualizację systemu plików i rejestru systemu Windows
d) jest rodzajem kwarantanny dla potencjalnie zainfekowanych aplikacji, przetrzymywanych tam zanim antywirus otrzyma z chmury ostateczny rezultat analizy behawioralnej podejrzanego kodu

31. Wskaż cechy charakterystyczne ataku przez przepełnienie bufora (w segmencie stosu): [1/1]

a) celem przepełnienia jest nadpisanie adresu powrotu w ramce funkcji odłożonej aktualnie na stosie
b) architektura pamięci musi być taka by adresy rosły zgodnie z kierunkiem przyrostu stosu
c) celem przepełnienia jest nadpisanie pamięci jądra i wywołanie błędu obsłużonego przez złośliwy kod
d) przepełnienie bufora można wykryć i odpowiednio zareagować'

32. Zaznacz cechy charakterystyczne metody ARP detekcji podsłuchu w sieci:

a) ogłoszenie ARP skierowane pod fałszywy adres IP
b) zapytanie ARP skierowane pod właściwy adres MAC odpytywanej stacji
c) zapytanie ARP skierowane pod rozgłoszeniowy adres MAC
d) zapytanie ARP skierowane pod nierozgłoszeniowy adres MAC

33. Wskaż problemy bezpieczeństwa wynikające z fragmentacji IP:

a) fragmentacja jest przyczyną skuteczności ataku SYN flood
b) potencjalna możliwość przepełnienia bufora pamięci przy scalaniu fragmentów
c) utrudniona możliwość filtracji fragmentów przez zapory sieciowe
d) kontrola fragmentacji wymaga użycia ciasteczek SYN cookies

34. Zaznacz prawdziwe stwierdzenia dotyczące protokołu HTTP: [0.5/1]

a) HTTP od wersji 1.1 uwierzytelnia nie tylko klienta, ale i serwer
b) Digest Authentication HTTP 1.1 realizuje metodę challenge-response
c) Basic Authentication w HTTP 1.0 przesyła nazwę użytkownika i hasło w postaci niezaszyfrowanej
d) Basic Authentication w HTTP 1.1 przesyła nazwę użytkownika i hasło w postaci zaszyfrowanej

36. Które z poniższych cech prawidłowo opisują protokół IPsec?

a) może działać z uwierzytelnianiem stron dokumentowanym tylko przez ESP
b) może działać w trybie tylko z ochroną integralności przez ESP
c) może działać z uwierzytelnianiem stron dokumentowanym tylko przez AH
d) może działać w trybie tylko z ochroną integralności przez AH

37**. Wskaż cechy uprawnień POSIX CAP: [1/1]**

a) mogą być przypisywane do użytkowników
b) mogą być przypisywane do procesów
c) podlegają dziedziczeniu przez procesy potomne
d) pozwalają na delegowanie podmiotom wybranych elementarnych uprawnień administracyjnych

38. Które z poniższych algorytmów kryptograficznych mogą zostać wykorzystane w sieci VPN do szyfrowania transmisji przez protokół SSL/TLS lub IPsec:

a) RSA
b) ECDH
c) AES
d) DH

39. Które z poniższych cech prawidłowo opisują protokół IKE? [1/1]

a) umożliwia zmianę kluczy szyfrowania protokołu IPsec ESP
b) uwierzytelnia sesje SA protokołu IPsec
c) negocjuje parametry sesji SA protokołu IPsec
d) umożliwia zmianę kluczy szyfrowania protokołu IPsec AH
e) oferuje uwierzytelnianie stron
f) korzysta z ICMP
g) korzysta z UDP
h) oferuje negocjację algorytmów szyfrujących

40. Tunele OpenVPN: [1/1]

a) stosują protokół ESP do szyfrowania ruchu
b) stosują protokół AH do szyfrowania ruchu
c) stosują protokół TLS do szyfrowania ruchu
d) stosują protokół ISAKMP do uwierzytelniania ruchu

41. Które z poniższych słów kluczowych mogą być prawidłowym “celem” w regule iptables dla łańcucha OUTPUT?

a) DROP
b) FORWARD
c) XOR
d) ACCEPT

42. Polecenie ulimit: [1/1]

a) decyduje o tym czy mogą być tworzone zrzuty przestrzeni adresowej (obrazy) procesów
b) podaje bieżące ograniczenia hard i soft, ale pozwala zmienić tylko soft
c) podaje bieżące ograniczenia hard i soft, ale nie pozwala ich zmieniać
d) pozwala zmienić oba rodzaje limitów: i hard, i soft

43. Czym się różni twist od spawn w polityce tcp wrappera (np. w pliku hosts.allow)? [1/1]

a) spawn służy do zapisywania wiadomości w logu lub wysyłania poczty, natomiast twist wysyła wiadomość i odmawia dostępu do usługi
b) oba polecenia użyte w hosts.allow kończą się odmową polecenia, ale twist dodatkowo zapisuje informację o tym w logu systemowym
c) twist przekierowuje połączenie do innej, określonej opcją usługi, podczas gdy spawn tworzy nowy proces wykonujący dowolne polecenie
d) spawn tworzy nowy proces wykonujący dane polecenie, natomiast twist wykonuje polecenie w ramach bieżącego procesu

44. Co oznacza udział IPC$ i do czego jest wykorzystywany? [1/1]

a) to udział służący w systemie Windows do zdalnego wywołania procedur (RPC)
b) to udział domyślny służący do zdalnej administracji systemem Windows
c) to udział administracyjny obejmujący wszystkie istniejące lokalne dyski

d) to udział kolejek POSIX IPC służący do lokalnej komunikacji między procesami

45. SSH pozwala:
a) uwierzytelniać użytkowników z wykorzystaniem kluczy kryptograficznych
b) uwierzytelniać użytkowników z wykorzystaniem haseł
c) uwierzytelniać komputery (systemy operacyjne) z wykorzystaniem kluczy kryptograficznych
d) udostępnić zasoby serwera lokalnego przez przekierowanie portów z serwera zdalnego

47. W których z poniższych przypadków rekalkulowana jest maska uprawnień ACL w systemie Linux:
a) gdy podamy opcję -m dla polecenia setfacl
b) przy zmianie uprawnień właściciela przy pomocy polecenia chmod
c) przy każdej zmianie uprawnień poleceniem setfacl, chyba że użyjemy opcji -n
d) przy dowolnej zmianie uprawnień danej kategorii praw (np. maska dla grupy modyfikowana jest przy modyfikacji praw dotyczących grupy)

48. Domyślne udziały administracyjne w systemie Windows:
a) dostępne są tylko dla administratora
b) są tworzone automatycznie przy instalacji systemu
c) nie mogą być usunięte
d) mogą być usunięte

49. Aby użytkownik L na komputerze HL mógł logować się bez podawania hasła na komputer HR na konto R należy:
a) skopiować klucz prywatny użytkownika R z komputera HR do pliku ~/.ssh/authorized_keys na koncie L na komputerze HL
b) skopiować klucz publiczny użytkownika L z komputera HL do pliku ~/.ssh/authorized_keys na koncie R na komputerze HR
c) skopiować klucz publiczny użytkownika R z komputera HR do pliku ~/.ssh/authorized_keys na koncie L na komputerze HL
d) skopiować klucz prywatny użytkownika L z komputera HL do pliku ~/.ssh/authorized_keys na koncie R na komputerze HR

50. Model kontroli dostępu MIC **zabrania** podmiotowi o etykiecie P:
a) zapisu obiektu o wyższej etykiecie niż P
b) odczytu obiektu o niższej etykiecie niż P
c) zapisu obiektu o niższej etykiecie niż P

51. Wykorzystanie TCP Wrappera do ochrony określonej usługi jest możliwe:
   a) jeśli program serwera usługi korzysta z biblioteki libwrap.so i sam czyta politykę TCP Wrappera
   b) automatycznie po definicji polityki (host_access), bowiem TCP Wrapper jest zintegrowany z systemem operacyjnym
   c) w przypadku przekazania nawiązywanego przez klienta usługi połączenia do demona TCP Wrappera zamiast do serwera obsługującego tę usługę
   d) dopiero po skonfigurowaniu iptables do przekierowania ruchu na port nasłuchującego superserwera xinetd?

52. Strumień ADS:
   a) jest częścią nagłówka pliku dołączaną zawsze przez system Windows podczas operacji pakowania do archiwum lub udostępniania w sieci
   b) jest wykorzystywany przez mechanizm informujący o stopniu zaufania do pliku (określający jego pochodzenie przez wpis ZoneId)
   c) pozwala związać z dowolnym plikiem lub katalogiem dowolne (zarówno tekstowe, jak i binarne) dane
   d) jest wykorzystywany przez procesy w systemie Windows do informowania o błędach wykonania (tzw. metainformacje)

52. Mechanizm EFS:
   a) zabezpiecza dostęp do treści poszczególnych plików zarówno w czasie działania systemu, jak i po jego wyłączeniu (at rest)
   b) stosuje kryptografię asymetryczną do szyfrowania treści plików
   c) realizuje full disc encyption w celu zabezpieczenia systemu operacyjnego przed niepowołanym uruchomieniem i dostępem
   d) wymaga do swojego działania konta DRA

53. Jakie hasło jest domyślnie wymagane przez polecenie sudo, jeżeli w konfiguracji nie będzie ustawione inaczej (czyli jeżeli wszystkie ustawienia będą miały wartości domyślne)?
   a) administratora systemu
   b) właściciela programu (SUID) uruchamianego tym poleceniem
   c) hasło puste (domyślnie sudo nie pyta o hasło)
   d) użytkownika wywołującego polecenie sudo

54. Gdy w poleceniu iptables nie podamy celu reguły, przy pomocy opcji -j (np. -j REJECT), wówczas:
   a) po dopasowaniu reguły iptables przerywa przetwarzanie, ale pakiet jest przepuszczany
   b) po dopasowaniu reguły iptables przetwarza kolejne reguły?
   c) używany jest cel domyślny dla danego łańcucha, tzw. polityka (ustawiana przy pomocy -P)

d) reguła zostanie odrzucona jako błędna, chyba że jest to modyfikacja wcześniej istniejącej reguły (przy pomocy opcji -R), kiedy to zostanie zastosowany taki cel, jaki był ustawiony dotychczas w tej regule

55. Impersonation w systemie Windows to:
a) przypisanie tokenu bezpieczeństwa ogólnego przeznaczenia do konkretnego użytkownika stanowiącego instancję pewnego SID
b) rodzaj zdalnego ataku na system, w którym napastnik podszywa się pod jednego z użytkowników
c) przechwycenie tokenu bezpieczeństwa SID przez nieuprawnionego użytkownika
d) czasowe przejęcie przez proces (wątek) uprawnień innego podmiotu

56. Hasła użytkowników systemu Windows są przechowywane: [0.7/1]
a) w rejestrze systemowym
b) w bazie SAM na dysku
c) w formie nieodwracalnego wyniku funkcji mieszającej
d) w pliku shadow zaszyfrowanym kluczem RSA (SYSKEY), do którego dostęp ma tylko administrator systemu

57. W poleceniu: iptables -I INPUT -p icmp –icmp-type echo-request -m recent –name “ping” –set nazwa “ping”:
a) jest to komentarz, pozwalający na szybką identyfikację reguły w przyszłości (np. w celu modyfikacji lub skasowania)
b) określa ten z ostatnio inicjowanych modułów filtracji (łańcuchów), który teraz będzie przechwytywał wskazane pakiety
c) identyfikuje konkretne statystyki, które później można wykorzystać do dalszej selekcji ruchu
d) definiuje nazwę pliku, który zawierać będzie informacje o ruchu pakietów do bieżącej reguły zapory

58. Serwer OpenVPN umożliwia uwierzytelnianie klientów poprzez:
a) klucze kryptograficzne
b) hasła użytkowników
c) certyfikaty X.509
d) protokół Kerberos
e) biometrycznie, poprzez analizę długości rzutu beretem

59. Po uruchomieniu Notatnika na niskim poziomie integralności, może on zapisywać pliki:
a) tylko w katalogach o przypisanym poziomie integralności co najwyżej niskim, np. %userprofile&/AppData/LocalLow
b) tylko w katalogach o przypisanym poziomie integralności co najmniej niskim, np. %userprofile&/Documents
c) nigdzie
d) tylko w katalogu z danymi tymczasowymi, np. %systemroot%/Temp

60. Wykorzystanie kryptograficznego podpisu wiadomości pozwala odbiorcy zweryfikować: [1/1]

a) autentyczność wiadomości przy użyciu klucza prywatnego odbiorcy
b) autentyczność wiadomości przy użyciu klucza publicznego nadawcy
c) autentyczność wiadomości przy użyciu klucza prywatnego nadawcy
d) autentyczność wiadomości przy użyciu klucza publicznego odbiorcy
e) pochodzenie wiadomości przy użyciu klucza prywatnego odbiorcy
f) pochodzenie wiadomości przy użyciu klucza publicznego odbiorcy
g) pochodzenie wiadomości przy użyciu klucza prywatnego nadawcy
h) pochodzenie wiadomości przy użyciu klucza publicznego nadawcy

62. Dodanie klucza wygenerowanego dla nowego agenta DRA, do istniejącego wcześniej zaszyfrowanego pliku, można uzyskać:

a) automatycznie, poprzez otwarcie tego pliku przez nowego agenta DRA
b) automatycznie, przy pierwszym otwarciu tego pliku przez dowolnego administratora
c) samoczynnie, przy okazji pierwszego dostępu do pliku kogoś mogącego odszyfrować ten plik
d) wydając polecenie cipher /u

63. Program SSH można wykorzystać m.in. do: [0.7/1]

a) stworzenia dynamicznego proxy aplikacyjnego
b) przekierowywania portów zdalnego serwera do maszyny lokalnej (klienta)
c) stworzenia proxy www wyłącznie dla protokołu HTTPS
d) przekierowywania portów maszyny lokalnej (klienta) do zdalnego serwera

64. Uprawnienia domyślne na liście POSIX ACL nadawane są:

a) jedynie plikom wykonywalnym w celu uściślenia jakie uprawnienia mają mieć pliki tworzone w czasie działania tych programów
b) jedynie katalogom w celu inicjowania list ACL nowo tworzonym plikom
c) plikom i katalogom w celu określenia uprawnień w przypadku braku pasującego wpisu ACE
d) plikom i katalogom w celu określenia ACL w przypadku ich kopiowania lub przenoszenia do innego katalogu

65. Które z poniższych zdarzeń są efektami braku wirtualizacji danego klucza rejestru systemu Windows?

a) operacja zapisu wartości parametrów tego klucza przez proces nie posiadający uprawnienia zapisu kończy się powodzeniem
b) operacja zapisu wartości parametrów tego klucza przez proces posiadający uprawnienie zapisu kończy się błędem
c) operacja zapisu wartości parametrów tego klucza przez proces posiadający uprawnienia zapisu kończy się powodzeniem
d) operacja zapisu wartości parametrów tego klucza przez proces nie posiadający uprawnienia zapisu kończy się błędem

66. Z jaką inną opcją polityki silnych haseł ma bezpośredni związek ilość haseł pamiętanych w historii?

a) maksymalny okres ważności hasła

b) minimalny okres ważności
c) minimalna długość hasła

67. Jak modyfikowana jest maska uprawnień POSIX ACL przy zmianie uprawnień do danego pliku:
a) nowa maska jest alternatywą bitową uprawnień nazwanych użytkowników, grupy i nazwanych grup
b) nowa maska jest alternatywą bitową starej maski i wszystkich uprawnień nowo nadanych przez setfacl
c) nowa maska jest iloczynem logicznym starej maski i wszystkich uprawnień nowo nadanych przez setfacl
d) nowa maska jest alternatywą bitową wszystkich uprawnień danego pliku (właściciela, grupy, pozostałych, nazwanych użytkowników, nazwanych grup)

68. Czyje hasło wymagane jest przy uruchomieniu polecenia sudo?
a) zawsze administratora systemu
b) zawsze użytkownika wywołujacego dane polecenie
c) w zależności od ustawień w polityce sudoers
d) zawsze użytkownika z uprawnieniami którego chcemy wykonać dane polecenie

69. Kolejność sprawdzania reguł polityki przez TCP Wrappera (pomijajac opcje only_from oraz no_access) jest następująca:
a) najpierw hosts.allow, potem hosts.deny, do odnalezienia pasującej reguły
b) sprawdzane są wszystkie reguły i jeżeli żadna z nich nie kończy się DENY, przyznawany jest dostęp
c) najpierw hosts.deny, potem hosts.allow, do odnalezienia pierwszej pasującej reguły
d) sprawdzane są wszystkie reguły i jeżeli żadna z nich nie kończy się DENY, a chociaż jedna kończy się ALLOW, przyznawany jest dostęp

70. UStawienia protokołu ESP w systemie Windows umożliwiają:
a) przesyłanie niezaszyfrowanego pakietu zabezpieczonego przed modyfikacją przy pomocy kryptograficznych funkcji mieszających
b) komunikację w trybie transportowym (bezpośrednim, host-to-host)
c) komunikację w trybie tunelowym (net-to-net)
d) ustanowienie bezpiecznego kanału do zarządzania asocjacją IPsec

71. Mechanizm iptables może dokonywać wyboru reguł filtracji dla danego pakietu przez:
a) zasadę pierwszego dopasowania i zawsze przerywa szukanie przy pierwszym dopasowaniu
b) zasadę najlepszego dopasowania (najbardziej szczegółowa reguła)
c) zasadę pierwszego dopasowania, ale niekoniecznie przerywa szukanie przy pierwszym dopasowaniu
d) zasadę określoną w polityce danego łańcucha (np. BESTMATCH, FIRSTMATCH)

72. Wirtualizacja rejestru w systemie Windows: [1/1]

a) chroni konfigurację systemu przed niepożądanymi zmianami
b) pozwala aplikacji 32-bitowej na modyfikację obszarów rejestru, do których aplikacja nie ma prawa zapisu
c) dotyczy wszystkich gałęzi rejestru
d) jest mechanizmem koniecznym do uruchomienia wirtualnych systemów Windows

73. Tunele IPsec: [1/1]

a) stosują protokół TLS do szyfrowania ruchu
b) stosują protokół AH do szyfrowania ruchu
c) stosują protokół ESP do szyfrowania ruchu
d) stosują protokół AH do uwierzytelniania stron tunelu

74. Które z poniższych twierdzeń jest prawdziwe? [1/1]

a) program SSH na komputerze A może połączyć się z komputerem B, tak by B nasłuchiwał na połączenia na porcie X. Metoda ta nazywa się local port forwarding (-L)
b) program SSH do uwierzytelniania oraz szyfrowania komunikacji pomiędzy komputerem A i B wykorzystuje algorytm RSA
c) program SSH na komputerze A wykorzystuje klucz publiczny komputera B w celu weryfikacji czy tożsamość B się nie zmieniła
d) program SSH na komputerze A może połączyć się z komputerem B, tak by B nasłuchiwał na połączenia na porcie X. Metoda ta nazywa się remote port forwarding (-R)

75. Agent DRA w systemie Windows to:

a) administrator systemu Windows, któremy przypisano prawo tworzenia strumieni ADS
b) lokalny administrator stacji roboczej w środowisku domenowym mogący robić kopie zapasowe
c) główny administrator domeny (serwera AD)
d) konto pozwalające na dostęp do plików zaszyfrowanych przez EFS

76. Które z poniższych twierdzeń dotyczących POSIX ACL są prawdziwe? [1/1]

a) w momencie tworzenia katalogu jego uprawnienia ACL kopiowane są z domyślnych uprawnień (Default ACL) folderu nadrzędnego z wykluczeniem uprawnienia do wykonywania
b) w momencie tworzenia pliku jego uprawnienia domyślne (Default ACL) zostają odziedziczone z folderu nadrzędnego
c) w momencie tworzenia pliku jego uprawnienia ACL kopiowane są z domyślnych uprawnień (Default ACL) folderu nadrzędnego z wykluczeniem uprawnienia do wykonywania
d) w momencie tworzenia katalogu jego uprawnienia domyślne (Default ACL) zostają odziedziczone z folderu nadrzędnego

77. Standard IEEE 802.1ae:
a) to odpowiednik IPsec na poziomie warstwy transportowej
b) oferuje uwierzytelnianie na poziomie warstwy sieciowej OSI
c) oferuje ochronę poufności i integralności komunikacji na poziomie warstwy MAC
d) oferuje ochronę poufności i integralności komunikacji na poziomie warstwy OSI

78. Wskaż, które z wymienionych operacji obsługiwane są przez mechanizm POSIX CAP (capabilities):
a) administrowanie siecią
b) administrowanie modułami jądra
c) omijanie limitów zasobowych
d) omijanie ograniczeń dotyczących kontroli dostępu do plików
e) dowiązanie do gniazd numerów portów systemowych
f) realizacja komunikacji grupowej rozgłoszeniowej w sieci

79. Cechą single-sign-on jest:
a) stosowanie funkcji skrótu w celu uzyskania podpisu cyfrowego
b) jednokrotne uwierzytelnianie użytkownika sieci
c) podpisywanie każdego pliku innym kluczem
d) szyfrowanie sesji przy pomocy jednorazowego klucza

80. Który z wymienionych protokołów pozwala w procesie uwierzytelniania całkowicie uniknąć przesyłania hasła podmiotu uwierzytelnianego (w jakiejkolwiek postaci):
a) SSH
b) SSL
c) CHAP
d) PAP
e) SPAP

81. Metoda programowego generowania haseł jednorazowych opracowana przez L.Lamporta polega m.in. na:
a) wygenerowaniu losowe listy N haseł wykorzystywanych wyrywkowo przez system
b) wygenerowaniu N-elementowej sekwencji wywierdoznej deterministycznie z zadanego hasła
c) wykorzystywaniu silnej kryptografii z kluczem równym początkowemu hasłu do ochrony kolejnych haseł
d) wykorzystywaniu wygenerowanych haseł w kolejności odwrotnej (od ostatniego począwszy)

82. Które narzędzia wykorzystywane są do ochrony antyspamowej w systemie pocztowym?
a) open proxy
b) open relay
c) szare listy
d) filtry Bayesa

83. Spośród podanych mechanizmów wskaż te wykorzystujące kryptografię:
a) X.509
b) podpis cyfrowy
c) ROT13
d) UUencoding

84. Wskaż cechy SNAT:
a) wymaga utrzymywania listy aktywnych translacji
b) ukrywa rzeczywisty adres nadawcy pakietu
c) może być pomyślnie wykonane pośrodku tunelu VPN zarówno w trybie tunelowym jak i transportowym
d) może być pomyślnie wykonane pośrodku tunelu VPN tylko w trybie transportowym
e) wymaga uwierzytelnienia stron przed zestawieniem połączenia
f) pozwala uniknąć powtórnego sprawdzania reguł filtracji dla ruchu zweryfikowanego uprzednio
g) dokonuje podmiany zarówno adresu jak i numeru portu

85. Komputery kwantowe i obliczenia kwantowe mogą stanowić poważne zagrożenie dla:
a) steganografii
b) aktualnych mechanizmów detekcji anomalii w systemach IDS
c) współczesnych algorytmów kryptografii asymetrycznej, takich jak RSA
d) zapór sieciowych typu proxy

86. 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:
a) prawo do obiektu p nie zostanie efektywnie przyznane, ale U odziedziczy je w głąb, jeśli p jest katalogiem
b) prawo r do obiektu p zostanie efektywnie przyznane bezwarunkowo
c) prawo r do obiektu p zostanie efektywnie przyznane, o ile U jest właścicielem p
d) prawo r do obiektu p nie zostanie efektywnie przyznane
e) prawo r do obiektu p zostanie efektywnie przyznane, o ile U jest wlascicielem p
f) prawo r do obiektu p nie zostanie efektywnie przyznane

87. Funkcja skrótu SHA-3 różni się od SHA-2:
a) ograniczeniami eksportowymi
b) posiadaniem strumieniowego trybu pracy
c) odpornością na ataki Length extension
d) użyciem asymetrycznego schematu szyfrowania

88. Wersja 3DES-EDE jest wzmocnieniem algorytmu kryptograficznego DES osiągniętym poprzez:

a) trzystopniowe sprawdzenie losowości doboru klucza
b) trzykrotne użycie algorytmu DES w trybie szyfrowania, deszyfrowania i ponownie szyfrowania
c) trzykrotne zastosowanie konwencji jednokierunkowej Electronic Data Exchange
d) podział wyniku szyfrowania na 3 porcje różnej długości wg standardu electronic Data Exchange

89. Własność Perfect Forward Secrecy w przypadku generowania kluczy kryptograficznych:

a) wymaga stosowania każdego klucza głównego (master) tylko jeden raz
b) ogranicza skutki znalezienia klucza sesji jedynie do części komunikacji
c) każdy klucz sesji generowany jest z innego klucza głównego (master)
d) stosuje różne klucze sesji do szyfrowania komunikacji w przeciwnych kierunkach

90. Separację środowiska wykonania poprzez wirtualizację (jądra) systemu operacyjnego oferuje:

a) Trusted Execution Environment (TEE)
b) funkcja systemowa chroot()
c) Address Space Layout Randomization (ASLR)
d) Windows Virtualization-Based Security (VBS)

91. Tryb strumieniowy szyfrowania:

a) umożliwia szyfrowanie komunikacji asynchronicznej
b) wymaga klucza prywatnego i publicznego
c) polega na szyfrowaniu każdorazowego po jednym znaku
d) wykorzystuje wektor inicjujący rejestr szyfrowania

92. Określ jakie potencjalne zagrożenia dla bezpieczeństwa niesie funkcja CreateRemotethread():

a) wywołanie zdalnych procedur (RPC) bez kontroli jądra zdalnego systemu operacyjnego
b) wykonanie nieautoryzowanych operacji podszywając się pod autoryzowany proces (obejście autoryzacji)
c) wstrzyknięcie złośliwego kodu do przestrzeni adresowej innego procesu w systemie operacyjnym
d) nie uwierzytelniony dostęp do komunikacji sieciowej poniżej warstwy transportowej

93. Koncepcja „zamkniętych grup użytkowników” dotyczy odseparowania danych przetwarzanych przez odrębne grupy użytkowników tego samego środowiska sieciowego. Które z poniższych mechanizmów są realizacją tej koncepcji:

a) sandbox net jail
b) Trusted Execution Environment (TEE)
c) Virtualization-Based Security (VBS)
d) sieci wirtualne VLAN
e) uwięzienie (jail)
f) protokół rezerwacji zasobów (RSVP)
g) transmisja grupowa (multicast) w sieci Ethernet

94. Które z poniższych protokołów służą realizacji kryptograficznych tuneli wirtualnych z ochroną poufności:

a) PEM
b) ESP
c) TLS
d) S/MIME
e) IPsec
f) SSL

140. Które z poniższych protokołów służą realizacji kryptograficznych tuneli wirtualnych:

a) TLS
b) LDAP
c) X.400
d) L2TP
e) IPsec
f) SSL

125. Które z poniższych protokołów służą realizacji kryptograficznych tuneli wirtualnych z ochroną integralności?

a) TLS
b) S/MIME
c) AH
d) ESP
e) PGP
f) X.400

95. Wskaż cechy filtracji kontekstowej (SPF) realizowanej przez zapory sieciowe:

a) pozwala uniknąć niepotrzebnego sprawdzania reguł dla pakietów powracających w ruchu zweryfikowanym w stronę przeciwną
b) zapora utrzymuje listę aktywnych połączeń
c) dopasowuje pakiety do zapamiętanej historii komunikacji
d) historia komunikacji nie ma wpływu na decyzje zapory
e) pozwala na dynamiczne modyfikacje reguł filtracji

96. Które stwierdzenie poprawnie opisują protokół IKE w IPsec:

a) realizuje uwierzytelnianie stron
b) realizuje podpis cyfrowy pakietów IP
c) korzysta z UDP

d) korzysta z ICMP
e) realizuje negocjację algorytmów szyfrujących
f) realizuje wymianę kluczy metodą Diffiego-Hellmana

98. Firewalking to:
a) połączenia zapór filtrujących ruch sieciowy z usługami proxy
b) technika odkrywania istnienia zapory sieciowej i otwartych na niej portów
c) szeregowe połączenia zapór sieciowych typu proxy
d) kaskadowe połączenia zapór sieciowych filtrujących pakiety

99. Które z poniższych podatności mogą potencjalnie pozwolić na wykonanie nieuprawnionego (złośliwego) kodu w aplikacji:
a) remapowanie adresu 0 (dereferencja)
b) randomizacja przydziału przestrzeni adresowej procesu
c) przepełnienie bufora
d) nadpisanie adresu obsługi przerwania/wyjątku

100. Ataki o nazwie phishing:
a) dotyczą wykradzenia zaufanych certyfikatów użytkownika
b) pozwalają w efekcie podszyć się pod atakowanego
c) mogą być w pewnym stopniu udaremnianie przy pomocy „czarnych list”
d) zmierzają do fałszowania ciasteczek www

101. Mechanizm umożliwiający przydzielenie poszczególnych uprawnień administracyjnych (uprzywilejowanych operacji jądra systemy operacyjnego) użytkownikom to:
a) capabilities
b) sandbox
c) remote administration
d) switch root

102. Jakie restrykcje wprowadza flaga Secure w definicji ciasteczka WWW?
a) do ciasteczka nie można uzyskać dostępu w skryptach
b) dostęp do ciasteczka ma tylko oryginalna strona, która utworzyła ciasteczko
c) ciasteczko będzie wysyłane do serwera tylko w tunelach kryptograficznych
d) ciasteczko musiało zostać sprawdzone przez filtr SOP

103. Użycie IPsec + IKE wprost chroni przed atakiem:
a) name spoofing
b) ARP cache spoofing
c) TCP spoofing
d) session hijacking
e) network sniffing
f) ARP spoofing

104. Mechanizm single-sign-on cechuje: // Mechanizm SSO cechuje:
a) uwierzytelnianie użytkownika wobec wielu serwerów jednorazową procedurą
b) podpisywanie każdego pakietu danych VPN innym kluczem
c) uwierzytelnianie użytkownika za każdym razem innym hasłem
d) uwierzytelnianie użytkownika innym hasłem wobec każdego serwera

e) autoryzacja podmiotu zgodnie z modelem MAC
f) uwierzytelnianie podmiotu za każdym razem innych hasłem jednorazowym
g) zastosowanie mechanizmu szyfrowania asymetrycznego w procesie autoryzacji
h) zastosowanie pojedynczego uwierzytelniania podmiotu w dostępie do wielu różnych zasobów

105. Proszę wskazać algorytmy podpisu cyfrowego:
a) ElGamal
b) Blowfish
c) Rijndael
d) SHA-1
e) MD5
f) żadne z powyższych

106. Wskaż prawidłowe stwierdzenia dotyczące metod uwierzytelniania systemów operacyjnych MS Windows w środowisku sieciowym:
a) NTLM jest bezpieczniejszy niż LM
b) Kerberos jest bezpieczniejszy niż LM
c) Kerberos jest dostępny tylko w środowisku domenowym
d) LM jest bezpieczniejszy niż NTLM

107. Wskaż własności protokołu RADIUS:
a) zabezpiecza pocztę elektroniczną wraz z załącznikami
b) mogą go wykorzystywać np. serwery dostępowe
c) jest realizacją koncepcji AAA
d) pozwala na centralizację zarządzania danymi, które dystrybuuje
e) wspomaga uwierzytelnianie (rozproszone)
f) pracuje w architekturze klient-serwer
g) Umożliwia rejestrowanie dostępu do zasobów

108. Następująca reguła filtracji zapory sieciowej:

od	do	port źródłowy	port docelowy	protokół	flagi	reakcja
1.1.1.1 ->	*.*.*.*	80	*	TCP	ACK=0	odrzuć

a) blokuje wszelkie połączenia nawiązywane z serwera www o dowolnym adresie
b) blokuje wszelkie połączenia nawiązywane z serwera www o adresie 1.1.1.1
c) blokuje wszelkie połączenia nawiązywane z serwerem www o adresie 1.1.1.1
d) blokuje wszelkie połączenia nawiązywane z serwerem www o dowolnym adresie

110. Wskaż protokoły wymagające zabezpieczenia autentyczności i integralności danych, ale niekoniecznie poufności:
a) DNS (Domain Name Service)
b) ARP (Address Resolution Protocol)
c) STP (Spanning Tree Protocol)
d) rlogin (Remote Login)

111. Które nazwy ataków dotyczą zalewania użytkowników niepożądaną informacją:

a) spam
b) pharming
c) scam
d) spim

112. Do szyfrów asymetrycznych zaliczamy:
a) SHA
b) SSH
c) AES
d) żadne z powyższych

113. W metodzie uzgadniania klucza Diffiego-Hellmana system może zostać skompromitowany poprzez:
a) przechwycenie jednego z wymienianych kluczy
b) przechwycenie obu wymienianych klucz
c) postawienie fałszywego klucza w miejsce każdego z wymienianych
d) postawienie fałszywego klucza w miejsce dowolnego z wymienianych

114. Algorytm SHA-256 i SHA-512 różnią się wzajemnie:
a) odpornością na ataki Length extension
b) podatnością na kolizje
c) wielkości wynikowego skrótu
d) żadne z powyższych

115. Wskaż cechy zapory sieciowej zrealizowanej poprzez Komputer-Twierdzę (Bastion Host):
a) dla ruchu z zewnątrz zapora „przykrywa" sobą całą sieć wewnętrzną
b) dla ruchu od wewnątrz zapora „przykrywa" sobą cały świat zewnętrzny
c) w zaporze nie jest realizowany routing
d) komunikacja zachodzi wyłącznie przez usługi proxy

116. Funkcja systemowa chroot()
a) oferuje kontrolę nad komunikacją sieciową
b) nie oferuje kontroli nad komunikacją sieciową
c) jest wykorzystywana przez narzędzie sudo do zmiany aktualnych uprawnień procesu
d) służy do chwilowego przeniesienia administratora na wybranego użytkownika
e) ogranicza aplikacji dostęp do systemu plików
f) chroni system przed atakami DoS
g) jest jednym z mechanizmów tworzenia piaskownicy
h) pozwala wykonać pojedyncze polecenia administracyjne administracyjne bez weryfikacji hasła
i) wymaga powielania plików niezbędnych dla poprawnego działania aplikacji
j) pozwala wielokrotnie skorzystać z uprawnień administratora bez weryfikacji hasła przez ustalony czas
k) ogranicza procesom dostępność systemu plików

117. Które z poniższych technologii sprzętowych umożliwiają separację środowiska wykonawczego aplikacja poprzez wirtualizację całości bądź części systemu operacyjnego (np. jądra systemu):
a) TEE (Trusted Execution Environment)
b) VBS (Virtualization-Based Security)

c) ARM TrustZone
d) SSL (Secure Socket Layer)

118. Który z wymienionych protokołów chroni klienta przed przypadkiem podszywania się pod zaufany serwer?
a) IPsec + PSK(Pre shared key)
b) HTTP/1.1
c) SSH
d) HTTP/1.0

119. Który angielski termin określa wykorzystanie do ataku znanych luk w systemie atakowanym:
a) exploiting
b) eavesdropping
c) masquerading
d) tampering

120. Metoda Diffiego-Hellmana:
a) generuje programowo hasła SSO
b) realizuje uwierzytelnianie metodą haseł jednorazowych
c) wykorzystuje ideę asymetrycznej pary kluczy (prywatny – publiczny)
d) pozwala wygenerować symetryczny klucz sesji

121. Które ataki sieciowe można wyeliminować stosując ochronę autentyczności komunikacji?
a) ARP cache poisoning
b) DNS cache poisoning
c) ARP spoofing
d) DNS spoofing

122. Wskaż cechy PKI:
a) certyfikaty kluczy prywatnych są składowane w repozytoriach takich jak np. DNSsec
b) certyfikaty kluczy są wzajemnie wystawiane przez innych użytkowników
c) unieważnienia certyfikatu klucza ma również postać certyfikatu /+1
d) do zweryfikowania certyfikatu klucza publicznego użytkownika potrzebny jest certyfikat głównego urzędu (RootCA)

123. Atak typu TCP spoofing wymaga:
a) intensywnego zalewania segmentami SYN
b) odgadnięcia numeru ISN strony odbierającej żądanie nawiązania połączenia
c) odgadnięcia numeru sekwencyjnego pierwszego segmentu strony żądającej nawiązania połączenia
d) zalewania żądaniami nawiązania połączenia TCP w trybie rozgłoszeniowym

124. W protokole HTTP/2:
a) uwierzytelnianie klienta jest obowiązkowe
b) uwierzytelnianie serwera jest opcjonalne
c) uwierzytelnianie serwera jest obowiązkowe
d) szyfrowanie całej komunikacji jest obowiązkowe

126. Standard IEEE 802.1X:
a) pozwala na wykorzystanie certyfikatów X.509 do realizacji swoich zadań

b) pozwala uwierzytelniać stanowiska sieciowe przy dostępie do sieci lokalnej
c) oferuje wymianę kluczy w sieci WiFi przy wykorzystaniu zarówno haseł jak i certyfikatów
d) umożliwia scentralizowane uwierzytelnianie wielu punktów zdalnego dostępu
e) podnosi dostępność poprzez redundantne rozproszenie danych uwierzytelniających do wielu punktów dostępowych

127. Wskaż rodzaje adresów, które zapora sieciowa dokonująca translacji NAT powinna filtrować w pakietach przychodzących od strony zewnętrznej sieci publicznej:
a) dowolne prywatne IP, w polu źródłowym
b) dowolne prywatne IP, w polu docelowym
c) adresy wykorzystywane wewnątrz, w polu źródłowym
d) adresy wykorzystywane wewnątrz, w polu docelowym

128. Do przechowywania danych uwierzytelniających w systemie MS Windows aplikacje mogą skorzystać z:
a) Winlog API
b) Data Protection API (DPAPI)
c) Credential Manager API
d) Generic Security Service API (GSSAPI)

129. Następująca reguła filtracji zapory sieciowej:

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

a) blokuje wszelkie połączenia nawiązywane z serwera www o dowolnym adresie
b) blokuje wszelkie połączenia nawiązywane z serwerem www o dowolnym adresie
c) blokuje wszelkie połączenia nawiązywane z serwerem www o adresie 1.1.1.1
d) blokuje wszelkie połączenia nawiązywane z serwera www o adresie 1.1.1.1

130. Które operacje mogą być wykorzystywane do realizacji ataku DoS (Denial of Service):
a) intensywny strumień segmentów FIN z adresem docelowym ofiary
b) fragmentacja datagramu o sumarycznej wielkości ponad 64kB
c) intensywny strumień pakietów UDP echo z adresem docelowym ofiary
d) intensywny strumień rozgłoszeniowym segmentów SYN z adresem źródłowym ofiary
e) intensywny strumień segmentów SYN z adresem docelowym ofiary
f) intensywny strumień rozgłoszeniowych pakietów ICMP echo z adresem źródłowym ofiary
g) fragmentacja datagramu o sumarycznej wielkości ponad 16 kB

131. Elementem ochrony przed złośliwym wykorzystaniem przepełnienia bufora może być:
a) remapowanie adresu 0 (dereferencja stała)

b) randomizacja przydziału przestrzeni adresowej procesu
c) remapowanie adresu obsługi przerwania/wyjątku (dereferencja zmienna)
d) wstawienie „kanarka” bezpośrednio po wskaźniku poprzedniej ramki

132. Wskaż cechy DNAT:
a) pozwala uniknąć powtórnego sprawdzania reguł filtracji dla ruchu zweryfikowanego uprzednio
b) ukrywa rzeczywisty adres odbiorcy pakietu
c) może być pomyślnie wykonanie pośrodku tunelu VPN tylko w trybie transportowym // w tunelowym
d) ukrywa rzeczywisty adres nadawcy pakietu

133. Wskaż cechy filtracji bezstanowej realizowanej przez zapory sieciowe:
a) zapora utrzymuje listę aktywnych połączeń
b) pozwala uniknąć niepotrzebnego sprawdzania reguł dla pakietów powracających w ruchu zweryfikowanym w stronę przeciwną
c) dopasowuje pakiety do zapamiętanej historii komunikacji
d) historia komunikacja nie ma wpływu na decyzje zapory
e) wymaga sprawdzania regul dla kazdego pakietu

134. Jakie metody uwierzytelniania oferuje protokół HTTP?
a) obustronne uwierzytelnianie metodą Diffiego-Hellmana
b) uwierzytelnianie serwera poprzez certyfikat X.509
c) uwierzytelnianie klienta poprzez username token (username + password)
d) uwierzytelnianie klienta metodą digest (z użyciem funkcji skrótu)

135. Wskaż funkcje biblioteczne odpowiedzialne za podatność na atak przepełnienia bufora
a) strcpy()
b) strncpy()
c) execv()
d) shellcode()
e) gets()

136. Niezaprzeczalność to własność potwierdzająca iż:
a) odbiorca wiadomości nie sfałszował jej treści po odebraniu
b) nadawca wiadomości jest rzeczywiście tym za kogo się podaje
c) nadawca wiadomości faktycznie ją wysłał
d) doszło do ataku aktywnego MiM
e) odbiorca wiadomości faktycznie ją odebrał

137. Termin two-factor authentication (2FA) dotyczy:
a) procesu potwierdzania tożsamości przy użyciu dwóch oddzielnych procedur lub składników sprzętowychszare
b) użycia w protokole HTTP/2 obustronnego uwierzytelniania
c) wykorzystania do kontroli integralności danych algorytmów kryptografii asymetrycznej bazujących na złożoności rozkładu dużych liczb na czynniki (faktoryzacji)
d) uwierzytelniania metodą zawołanie-odzew

138. Wskaż cechy poprawnie opisujące DNSsec:
a) umożliwia przechowywanie kluczy publicznych podmiotów z domeny
b) stosuje kryptografię asymetryczną do podpisywania rekordów
c) przesyła zapytania i odpowiedzi w tunelu IPsec
d) stosuje kryptografię symetryczna do szyfrowania rekordów

139. Klucze w szyfrowaniu symetrycznym:
a) mogą być publicznie dostępne pod warunkiem certyfikacji
b) zapewniają autentyczność i niezaprzeczalność pod warunkiem zachowania tajności klucza
c) zawsze powinny być znane tylko komunikującym się stronom
d) wymagają losowego wyboru dużych liczb pierwszych

141. Mechanizm ochrony antyspamowej o nazwie „szare listy” opera się na:
a) automatycznym weryfikowaniu listy zabronionych adresów nadawców przez MTA
b) odesłaniu komunikatu SMTP o czasowej niedostępności usługi
c) analizie heurystycznej nagłówka SMTP przez MUA
d) dynamicznym weryfikowaniu listy podejrzanych adresów nadawców przez użytkownika

142. Wskaż zagrożenie bezpieczeństwa związane z fragmentacją datagramów w protokole IP?
a) scalanie fragmentów perfidnie przygotowanych może powodować nieprzewidziane efekty
b) fragmentacja uniemożliwia stosowanie AH IPsec
c) fragmentacja uniemożliwia stosowanie ESP IPsec
d) fragmentacja utrudnia skuteczną filtrację pakietów

143. Atak na usługę www realizowany poprzez wymuszenie wykonania w przeglądarce kodu pochodzącego z lokalizacji innej niż pobrana strona to:
a) same origin forgery
b) command injection
c) SQL injection
d) cross site scripting

144. Wskaż wśród wymienionych jeden standard bezpieczeństwa, którego należy najbardziej unikać w zabezpieczaniu sieci WiFi:
a) WEP
b) WPA2
c) WPA
d) 802.11i

145. Wskaż które z poniższych technik mogą być wykorzystywane do tzw. wzmacniania DDoS:
a) SYN cookies
b) protokół DNSsec
c) rozgłoszenie
d) protokół DNS

147. Mechanizm ACL:
a) oferuje niezaprzeczalność nadania wiadomości
b) jest narzędziem kontroli dostępu do zasobów
c) oferuje niezaprzeczalność odbioru wiadomości
d) wyróżnia systemy MAC od DAC

148. Wskaż cechy ścisłej kontroli dostępu (MAC):
a) podatna na błędy samodzielnej konfiguracji przez użytkownika
b) wymaga kosztownej globalne konfiguracji systemu
c) nie pozwala użytkownikowi sterować uprawnieniami do jego własnych zasobów
d) trudna do nadzorowania przez system

149. Jaki rodzaj filtracji umożliwia podejmowanie decyzji o filtracji pakietów z uwzględnieniem stanu sesji do której przynależą?
a) filtry bezstanowe
b) filtry statyczne
c) filtry kontekstowe
d) Stateful Packet Filtering

150. Które z poniższych cech poprawnie opisują standard IEEE 802.1X:
a) umożliwia scentralizowane zarządzanie kluczami publicznymi użytkowników PKI/X
b) może wykorzystywać certyfikaty X.509 do kontroli dostępu w sieciach WiFi
c) chroni przed atakami IP spoofing
d) umożliwia uwierzytelnianie stanowisk sieci LAN

151. Algorytm 3DES to:
a) zastosowanie skrótu qubicznego Extended Signature
b) pseudolosowy generator 3D cube
c) trzykrotne użycie algorytmu DES
d) podział szyfrogramu na 3 porcje różnej długości wg Disturb-Extraction Split

152. Która z poniższych cech poprawnie opisuje protokół RADIUS:
a) wspiera realizację kontroli dostępu do zasobów sieciowych
b) umożliwia rejestrowanie dostępu do zasobów sieciowych
c) chroni przed atakami DNS spoofing
d) umożliwia scentralizowane uwierzytelnianie podmiotów
e) oferuje wymiane kluczy protokołu IPsec przy wykorzystaniu zarówno haseł jak i certyfikatów PKI
f) podnosi dostępność poprzez redundantne rozproszenie danych uwierzytelniających do wielu punktów dostępowych
g) udostępnia informacje niezbędne do kontroli uprawnień zdalnego dostępu (np. restrykcje czasowe)
h) pozwala na scentralizowane przechowywanie danych uwierzytelniających dla wielu punktów dostępowych
i) podnosi dostepnosc poprzez redundantne rozproszenie danych uwierzytelniajacych do wielu punktow dostepowych

154. Przed którymi atakami chroni poprawnie nawiązana sesja VPN (IPsec lub TLS):
a) TCP spoofing
b) SQLi

c) DNS spoofing
d) ARP spoofing

155. Do zrealizowania zamaskowanego kanału komunikacyjnego może potencjalnie posłużyć:
a) metoda challenge-response na poziomie warstwy 2 OSI
b) port szeregowy
c) obciążenie systemu
d) kolejka wydruku

156. Wskaż kto może rozszyfrować plik zaszyfrowany mechanizmem EFS:
a) każdy agent DRA istniejący w momencie deszyfrowania pliku
b) właściciel pliku
c) administrator
d) każdy DRA istniejący w momencie szyfrowania pliku

157. Mechanizm Lock-and-Key:
a) wymaga uwierzytelnienia użytkownika, np. za pomocą RADIUS-a
b) automatycznie blokuje stacje niespełniające wymagań polityki bezpieczeństwa
c) może być wykorzystywany do tymczasowego uzyskania uprzywilejowanego dostępu do sieci wewnętrznej z zewnątrz
d) służy do translacji reguł filtracji z jednej zapory na inną
e) jest podatny na IP spoofing

159. Wyobraźmy sobie serwer udostępniający wybranym podsieciom dwie usługi: www i ftp. Zapewnienie kontroli dostępu, np. za pomocą narzędzia personal firewall (lub wrappera połączeń) tylko do jednej z tych usług stanowi:
a) realizację predykatu ograniczonej kontroli dostępu (MAC)
b) naruszenie warunku spójności pionowej zabezpieczeń
c) naruszenie warunku spójności poziomej zabezpieczeń
d) naruszenie zasad poziomu B1/TCSEC i EAL4/CC

160. Który termin określa ochronę informacji przed nieautoryzowanym jej zmodyfikowaniem:
a) autoryzacja
b) niezaprzeczalność
c) spójność
d) integralność

161. Ktore z ponizszych okreslen opisuja mechanizm CAP (capabilities):
a) opisuje prawa uwierzytelnionego użytkownika w bilecie systemu Kerberos
b) specyfikuje w certyfikacie klucza publicznego możliwości wykorzystania danego klucza
c) pozwala na rozdzielenie uprawnień ogólno administracyjnych na szczegółowe podzbiory
d) przydziela użytkownikowi pewne informacje uwierzytelniające przedstawiane następnie podczas dostępu do poszczególnych usług

162. Którego typu ataku dotyczy następujący opis: Atak ten przeprowadza osoba, która wobec każdej z dwóch uprawnionych stron komunikacji podszywa się za przeciwna strone, pośrednicząc w przesyłaniu danych:
a) aktywny
b) zdalny
c) pasywny
d) lokalny

163. Co zapewnia uwierzytelnianie przez posiadanie?
a) poufność
b) integralność poufność i integralność
c) integralność
d) żadne z powyższych

164. Bezpośrednim celem ataku metodą przepełnienia bufora jest:
a) wypchnięcie wartości zmiennych globalnych programu poza chroniony segment danych
b) uszkodzenie zawartości segmentu danych i w efekcie zawieszenie procesu
c) uszkodzenie zawartości segmentu kodu i w efekcie zawieszenie procesu
d) nadpisanie adresu powrotu na stosie

165. Mechanizm haseł jednorazowych można zrealizować poprzez:
a) listy haseł jednorazowych
b) generowanie hasła jednorazowego co stały czas
c) generowanie hasła jednorazowego w odpowiedzi na żądany kod
d) generowanie hasła jednorazowego na podstawie czasu i kodu

166. W RSBAC, czy każdy program może zmienić uprawnienia na inne niż te, na których został uruchomiony?
a) zgodę wydaje oficer bezpieczeństwa modyfikując odpowiednio politykę bezpieczeństwa
b) tak
c) każdorazowo musi otrzymać zgodę oficera bezpieczeństwa
d) bezwzględnie nie

167. Skrót ACL oznacza:
a) Added Control List
b) Access Control List
c) Lista uprawnień nadanych
d) Lista kontroli dostępu

168. Czy RSBAC zapewnia:
a) wymuszanie stosowania skomplikowanych haseł
b) aktualizacje oprogramowania
c) stosowanie polityki MAC
d) system trudny do przechwycenia przez osobę niepowołaną
e) poufność przechowywanych danych
f) stosowanie polityki DAC

169. Szyfrowanie asymetryczne:
a) to używanie dwóch matematycznie zależnych kluczy
b) jest wykorzystane przy podpisywaniu wiadomości
c) to używanie dwóch niezależnych kluczy: jednego do szyfrowania, drugiego do deszyfrowania
d) nie jest wykorzystywane przez SSH

170. TUN/TAP to:
a) rozszerzenie programu OpenVPN
b) sterownik działający tylko na systemach Windows
c) sterownik działający tylko na systemach Linux
d) coś takiego nie istnieje
e) komponent pozwalający tworzyć wirtualne interfejsy sieciowe

171. Możliwości uwierzytelniania przy użyciu SSH to:
a) certyfikaty SSL X.509
b) para login, hasło naszego konta na zdalnym hoście
c) samo hasło naszego konta na zdalnym hoście
d) klucz publiczny, używany przy szyfrowaniu symetrycznym
e) trójka login, klucz publiczny i klucz prywatny

172. Protokół SSH umożliwia:
a) pobieranie plików
b) bezpołączeniową komunikację ze zdalnym hostem, na którym uruchomiony jest serwer ssh
c) nawiązywanie połączeń ze zdalnymi terminalami

173. Jakie restrykcje wprowadza tryb Safe w konfiguracji modułu PHP serwera WWW?
a) blokowanie wybranych funkcji
b) ograniczenie dostępu do fragmentu systemu plików SSL
c) dostęp tylko do plików o tym samym właścicielu co skrypt
d) ograniczenie zakresu zmiennych modyfikowanych

174. Serwer KDC:
a) jest bardzo dobrze zabezpieczony
b) może zapewnić bardzo dobre bezpieczeństwo w sieci
c) stosuje proste mechanizmy kryptograficzne, które są proste do złamania
d) można prosto oszukać podszywając się pod niego
e) ufa każdej usłudze
f) ufa uwiarygodnionym użytkownikom
g) ufa każdemu komputerowi w domenie
h) działa jedynie w obrębie jednej sieci lokalnej

175. Wektor inicjujący w szyfrowaniu:
a) musi być tajny i znany tylko odbiorcy
b) musi być tajny i znany obu stronom komunikacji
c) powinien mieć losową wartość, za każdym razem inną
d) wykorzystywany jest wyłącznie w szyfrowaniu asymetrycznym

176. W uwierzytelnianiu z udziałem zaufanej trzeciej strony, do zadań tej trzeciej strony należy:
a) poświadczenie uwierzytelnienia
b) pobranie listu uwierzytelniającego od jednej ze stron
c) pobranie listu uwierzytelniającego od obu stron
d) uwierzytelnienie jednej ze stron

177. W uwierzytelnianiu z udziałem zaufanej trzeciej strony, do zadań strony uwierzytelnianej należy:
a) przekazanie poświadczenia uwierzytelnienia drugiej ze stron
b) pobranie poświadczenie uwierzytelnienia od drugiej ze stron
c) przekazanie danych uwierzytelniających drugiej ze stron
d) przekazanie danych uwierzytelniających stronie trzeciej

178. Zastosowanie rozszerzenia Enigmail w kliencie poczty Thunderbird pozwala na:
a) używanie mechanizmu SSL do zapewniania bezpiecznych szyfrowanych kanałów komunikacyjnych z serwerem poczty POP
b) wykorzystywanie PGP do szyfrowania i podpisywania wiadomości
c) ochronę przed atakami man-in-the-middle
d) używanie mechanizm SSL do zapewniania bezpiecznych szyfrowanych kanałów komunikacyjnych z serwerem poczty SMTP

179. Szyfr, w którym poddawana szyfrowaniu zostaje tej samej wielkości jednobajtowa porcja nieregularnie pojawiających się danych, nazywamy:
a) strumieniowym
b) symetrycznym
c) blokowym
d) niesymetrycznym

180. Istotna przewaga podpisu elektronicznego nad odręcznym polega m. in. na:
a) jest ściśle powiązany z treścią podpisywanego dokumentu
b) weryfikacja podpisu wymaga tylko dostępu do certyfikatu klucza prywatnego podpisującego, co wystarcza do sądowego uznania podpisu za autentyczny
c) autentyczność podpisu można zweryfikować poprzez prosta weryfikacje certyfikatu klucza publicznego podpisującego
d) samo złożenie podpisu umożliwia wyparcie się tego przez podpisującego

181. Prosze wskazać algorytmy wykorzystywane w HMAC:
a) AES
b) SHA-4
c) SSH
d) ElGamal
e) Blowfish
f) Rijndael
g) MD5
h) żadne z powyższych

182. System NAC (Network Admission Control):
   a) oferują filtracje poczty elektronicznej
   b) służą realizacji rozległych korporacyjnych sieci VPN
   c) to zapory sieciowe stosujące bezstanowe reguły filtracji
   d) umożliwiają blokowanie ruchu sieciowego ze stacji nie spełniających wymagań polityki bezpieczeństwa

183. Metoda PING stosowana przez systemy IDS polega na wysłaniu:
   a) zapytania ICMP echo request pod adres MAC niezgodny z odpytywanym IP i oczekiwaniu na odpowiedź
   b) pakietów ICMP ping i porównaniu różnic w czasach odpowiedzi pomiędzy różnymi stanowiskami
   c) zapytania ICMP echo request pod adres rozgłoszeniowy i oczekiwaniu na odpowiedź
   d) zapytania ICMP echo request pod adres MAC podejrzanej stacji i oczekiwaniu na odpowiedź

184. Cechy charakterystyczne ataku SYN flood to:
   a) intensywny strumień segmentów SYN skierowany na adres ofiary
   b) intensywny strumień segmentów SYN/ACK skierowany na adres ofiary
   c) brak segmentów SYN/ACK
   d) brak segmentów ACK

185. Do szyfrów symetrycznych zaliczamy:
   a) IDEA
   b) RSA
   c) Rijndael
   d) Blowfish
   e) ElGamal
   f) MD4
   g) MD5
   h) DES
   i) RC4
   j) RC2
   k) AES
   l) żadne z powyższych

186. Do szyfrów niesymetrycznych zaliczamy:
   a) MD4
   b) Rijnadael
   c) Blowfish
   d) ElGamal
   e) MD5
   f) DES
   g) żadne z powyższych

187. IPsec ESP umożliwia zapewnienie:
a) autentyczności treści datagramu przy wykorzystaniu algorytmu MD5
b) autentyczności treści datagramu przy wykorzystaniu algorytmu 3DES
c) poufności treści datagramu w trybie tunelowym
d) poufności treści datagramu w trybie transportowym
e) tylko autentyczności treści datagramu, nie poufności
f) tylko poufności treści datagramu, nie autentyczności
g) poufności i/lub autentyczności treści datagramu, w trybie synchronicznym
h) poufności i/lub autentyczności treści datagramu, w trybie tunelowym

188. Jaki mechanizm może wykorzystać administrator do dynamicznego uaktywnienia specjalnie przygotowanych reguł filtracji umożliwiających obejście ograniczeń narzuconych na normalny ruch sieciowy?
a) zamek-i-klucz
b) dynamiczny skaner portów
c) sniffer dynamiczny
d) NIDS lub HIPS

189. Do czego służy protokół SMTP?
a) pozwala na szyfrowania załączników wiadomości
b) pozwala na przesyłanie grupowych wiadomości w trybie multicast
c) pozwala na przeszukiwanie bazy użytkowników na serwerze smtp w celu określenia adresata wiadomości
d) pozwala na wysyłanie wiadomości do innych użytkowników

190. Do czego służy komenda rlogin?
a) pozwala tylko systemowym użytkownikom zalogowac sie na lokalna maszyne
b) pozwala na zdalny dostęp do hosta
c) pozwala zalogowac sie lokalnym uzytkownikom na zdalna maszyne tylko na konto o takiej samej nazwie
d) dostarcza zaawansowanego mechanizmu uwierzytelniania użytkowników logujących się na lokalna maszyne

191. Co ma na celu publikowanie swojego klucza publicznego PGP?
a) nic nie daje, publikowanie klucza ma na celu tylko usprawnienie mechanizmu wymiany kluczy między użytkownikami
b) uniemożliwienie intruzowi podszycie się pod nasz e-mail
c) umożliwienie zaszyfrowania wiadomości adresowanej do właściciela klucza
d) umożliwienie sprawdzenia autentyczności listu wysłanego przez właściciela klucza
e) umożliwienie odszyfrowania zawartości email wysłanej przez właściciela klucza

192. Czy w systemie Ms Windows można skorzystać z szyfrowania PGP?
a) niestety system ten nie wspiera szyfrowania PGP
b) tak, ale tylko przy wykorzystaniu komercyjnych, płatnych programów
c) tylko przy wykorzystaniu programu Ms Outlook
d) tak, jeżeli wykorzysta się odpowiednie oprogramowanie

193. Szyfrowanie plików w systemie Ms Windows:
a) jest dostępne dla każdego pod warunkiem korzystania z partycji typu NTFS
b) jest dostępne wyłącznie dla administratora systemu
c) jest niemożliwe
d) jest dostępna dla administratora systemu i operatora kopii bezpieczeństwa
194. Wykorzystując stanowość zapory sieciowej możemy określić:
a) odrzucić pakiety próbujące podszywać się pod rzekomo istniejące połączenia
b) czy pakiet próbuje obejść nasz system bezpieczeństwa
c) czy połączenie jest już ustanowione
d) czy pakiet zawiera flagę ACK
195. LMhash to:
a) hasło administratora systemu zapisane w sposób jawny
b) hasła użytkowników w postaci skrótów (hashy) wykorzystywane przez Lan Managera
c) Lan Manager hash służący do identyfikacji systemu w sieci lokalnej
d) hash numeru seryjnego systemu Ms Windows
196. Dziedziczenie uprawnień w systemie plików NTFS:
a) uprawnienia sa pobierane bezpośrednio z uprawnień obiektu wyższego
b) może przenieść również na system plików FAT64
c) jest identycznie z systemem plików ext3
d) nie istnieje w tym systemie plików
197. Wadą single-sign-on jest:
a) relacja zaufania między parami hostów w domenie zaufania z wyłączeniem hosta zapewniającego uwierzytelnianie
b) możliwość logowania się tylko na konta systemowe
c) zależność od poprawnego działania uwierzytelniającej maszyny
d) brak relacji zaufania między hostem uwierzytelniającym a hostem usługowym w domenie zaufania
198. Aby serwer usług w domenie kerberos mogl dzialac wykorzystując uwierzytelniania Single-Sign-On, musi:
a) używać odpowiednio zmodyfikowanych demonów usług, które potrafią rozmawiać z serwerem Kerberos
b) używa zmodyfikowanego stosu IP, który współpracuje z serwerem KDC
c) zapewnia sprzętowe szyfrowanie i generowanie liczb losowych
d) używa specjalnego jądra systemu operacyjnego, wspierającego współpracę z serwerem KDC
199. Nazwa domenowa komputera a nazwa domeny kerberos:
a) musi być różna
b) musi być identyczna
c) zaleca się, aby była identyczna
d) zaleca się, aby byla rozna
200. Mechanizm TCP Wrapper:
a) pozwala ograniczać dostęp do usług uruchamianych przez xinetd
b) pozwala blokować spam przychodzący do serwera SMTP
c) pozwala szyfrować ruch TCP z użyciem protokołów TLS/SSL
d) powstał, aby wprowadzić silne uwierzytelnianie dla tzw. small services

201. Tunel Net-to-Net to:
a) koncepcja połączenia dwóch lub więcej sieci, w której istnieją zestawione tunele między bramami dla każdej z sieci w sieci Internet
b) bezpośrednie połączenie typu proxy dwóch sieci przez Internet
c) tunel zestawiany między systemami autonomicznymi w celu wymiany informacji o trasach routingu
d) bezpośrednie połączenie dwóch lub więcej sieci przez Internet

202. Klucz FEK to:
a) klucz asymetryczny
b) klucz prywatny użytkownika
c) klucz publiczny użytkownika
d) klucz symetryczny

203. Połączenie pasywne ftp to:
a) jeden z czterech rodzajów połączeń jakie moze nawiazac klient tj. połączenie danych, połączenie sterujące, połączenie aktywne, połączenie pasywne
b) specjalny rodzaj szybkich połączeń przeznaczony do wysyłania dużych porcji danych do klientów
c) połączenie, w którym klient informuje serwer, aby to on określił port a klient połączy się z tym portem i pobierze dane
d) specjalny rodzaj połączeń dzięki którym możliwe jest połączenie w sytuacji gdy klient i serwer znajduja sie za firewallem realizujacym SNAT

204. Połączenie aktywne ftp to:
a) jeden z czterech rodzajów połączeń jakie moze nawiazac klient tj. połączenie danych, połączenie sterujące, połączenie aktywne, połączenie pasywne
b) sytuacja, w której serwer ftp tworzy połączenie do klienta na losowy wybrany port przez klienta, aby przesłać żądany plik
c) sytuacja w której specjalnie skonfigurowany serwer ftp potrafi przyjmować połączenia gdy sam znajduje się za firewallem realizującym usługę SNAT
d) sytuacja w której przychodzące połączenie od serwera ftp do klienta ftp jest przekierowywane na firewallu do klienta znajdującego się w sieci lokalnej

205. Skrót IKE oznacza:
a) rodzaj algorytmów wymiany kluczy w FreeS/Wan
b) bardzo ważny element pakietu FreeS/Wan pozwalający tworzyć bezpieczne połączenie sterujące tunelami VPN
c) Information Key Exchange
d) jeden z algorytmów szyfrowania w pakiecie FreeS/Wan

206. Pakiet FreeS/Wan składa się z:
a) z trzech komponentów: łata na jądro KLIPS, demon PLUTO, zestaw skryptów
b) z dwóch protokołów: AH i ESP
c) z kilkunastu różnych algorytmów szyfrowania m.in. DES i 3DES oraz protokołu wymiany kluczy: ISAKMP

207. Kryptografia oportunistyczna to:
a) nowy rodzaj szyfrowania, bardzo wydajny i nie do złamania w dzisiejszych czasach z użyciem obecnych maszyn obliczeniowych
b) automatyczny sposób negocjowania parametrów połączenia zaimplementowany w pakiecie FreeS/Wan
c) eksperymentalny projekt nowego rodzaju szyfrowania rozwijany na potrzeby amerykańskiej Agencji Bezpieczeństwa Narodowego
d) prosty rodzaj szyfrowania, nazwa "oportunistyczna" zaczerpnięta od francuskiego słowa: opportunisme oznaczającego "sprzyjający, dogodny"

208. Narzędzie FreeS/Wan to:
a) łata na jądro implementująca funkcjonalność ISec plus zestaw skryptów do zarządzania tym narzędziem
b) program działający w przestrzeni użytkownika który posiada jeden plik konfiguracyjny zlokalizowany domyślnie: /etc/spiec
c) narzędzie w formie łaty na jądro systemu Linux wraz z zestawem skryptów zarządzających oraz demon pozwalający wymieniać klucze
d) narzędzie bardzo podobne do narzędzia Vtun służące do zestawiania połączeń VPN

209. Tunel Host-to-host to:
a) połączenie punkt - punkt między dwoma hostami, ale tylko na czas transmisji zaszyfrowanej
b) połaczenie peer-to-peer z rezerwacja pasma na calej
c) połączenie wykorzystujące już zestawione połączenie punkt-punkt dodające tylko szyfrowanie i uwierzytelnianie

210. W jakich trybach może działać VPN:
a) ruch sieciowy tunelowy i uwierzytelniany
b) ruch sieciowy nieszyfrowany ale uwierzytelniany
c) ruch sieciowy szyfrowany ale nie uwierzytelniany
d) ruch sieciowy tunelowany/transportowany
e) ruch sieciowy transportowany, szyfrowany i uwierzytelniany

211. Skrót VPN to:
a) szczególny rodzaj sieci vlan ale rozciągającej się na kilka sieci lokalnych rozdzielonych Internetem
b) wirtualna sieć prywatna
c) dodatkowy model komunikacji wykorzystywany przez IPSec do zaufanych połączeń między urządzeniami sieciowymi takimi jak routery i switche, hosty
d) szkieletowa sieć w Internecie przeznaczona dla zastosowań korporacyjnych zapewniająca wysoki stopień bezpieczeństwa np. w przypadku transakcji między bankami albo filiami tego samego banku połączonych Internetem
e) eksperymentalny projekt bezpiecznej sieci następnej generacji w której będzie można łączyć dowolną ilość sieci lokalnych rozdzielonych Internetem w jedna calosc, dzięki czemu będzie możliwy swobodny dostep do zasobow jednej sieci lokalnej przez inna np. dostep do intranetu centrali firmy przez pracowników firmy z oddziałów firmy w innym mieście

212. Translacja typu DNAT charakteryzuje się:
a) zamiana adresów źródłowych na inne (możliwe do wykorzystania na danym urządzeniu)
b) nie ma translacji typu DNAT
c) zamiana adresów docelowych na inne
d) zamiana adresu źródłowego z adresem docelowym w konkretnym pakiecie

213. Mechanizm SSO pozwala na
a) zapobieganie atakom typu XSS
b) zapobieganie atakom typu IP spoofing poprzez jawne podanie adresów IP w konfiguracji tego mechanizmu
c) szyfrowanie ruchu sieciowego między zaufanymi hostami
d) tworzenie relacji zaufania między hostami

214. Ukrycie widoczności systemu Ms Win spowoduje:
a) niedziałanie zdalnego logowania do systemu
b) niedziałanie udostępniania zasobów
c) ukrycie systemu przed innymi systemami
d) ukrycie systemu tylko przed systemami typu Unix

215. Wskaż cechy metody uwierzytelniania klienta wobec serwera z udziałem zaufanej trzeciej strony:
a) serwer uwierzytelnia klienta na podstawie poświadczenia wystawionego przez trzecią stronę
b) opłaca się stosować szczególnie wobec większej ilości serwerów
c) serwer uwierzytelnia klienta poprzez hasło (np. jednorazowe)
d) serwer uwierzytelnia klienta metoda challenge-response

216. Flaga suid wg standardu POSIX 1003.1
a) oznacza przejęcie przez proces uprawnień właściciela pliku, z którego proces został uruchomiony
b) oznacza, że usunięcie i zmiana nazwy pliku są możliwe tylko przez właściciela samego pliku (lub właściciela katalogu)
c) może być nadawana dla plików wykonywalnych
d) ma sens tylko w przypadku katalogów

219. Wskaż cechy protokołu Hot Standby Routing Protocol:
a) oferuje transparentne zasilanie z kilku redundantnych torów energetycznych
b) jest wykorzystywany w LAN Emulation
c) chroni przed atakami DoS poprzez czasowe wyłączenie routingu po wykryciu próby ataku
d) oferuje transparentna redundancje urządzeń sieciowych

220. Wskaż kiedy system kontroli dostępu MAC może zezwolić podmiotowi P na dopisanie danych do zasobu Z:
a) gdy zbiór kategorii przynależności danych Z zawiera się w zbiorze kategorii P
b) gdy poziom zaufania P jest niższy niż Z
c) gdy poziom zaufania P jest wyższy niż Z
d) gdy poziom zaufania P jest wyższy niż Z

221. Wskaż kiedy system kontroli dostępu MAC nie zezwoli podmiotowi P na dopisanie danych do zasobu Z:
a) gdy zbiory kategorii przynależności danych P i Z są rozłączne

b) gdy zbiór kategorii przynależności danych Z zawiera się w zbiorze kategorii P
c) gdy poziom zaufania Z jest niższy niż P
d) gdy poziom zaufania Z jest wyższy niż P

222. Mechanizm SSO (single-sign-on):
a) służy ochronie danych uwierzytelniających użytkownika
b) pozwala jednolicie chronić podpisem cyfrowym poufność całej komunikacji
c) służy ochronie niezaprzeczalności danych składowanych w repozytorium
d) pozwala jednolicie chronić podpisem cyfrowym integralność całej komunikacji

223. Statyczne reguły filtracji (filtracja bezstanowa) nie radzą sobie z precyzyjna filtracja ruchu:
a) HTTP, gdy serwer pracuje w trybie bezstanowym
b) HTTP, gdy serwer pracuje w trybie stanowym
c) FTP, gdy serwer pracuje w trybie aktywnym
d) FTP, gdy serwer pracuje w trybie pasywnym

224. Standard IEEE 802.1x:
a) realizuje autoryzację i kontrolę dostępu do lokalnej infrastruktury sieciowej
b) współpracuje z protokołami takimi jak RADIUS lub TACACS+
c) dotyczy zabezpieczenia poufności
d) dotyczy uprawnień dostępu do zasobów plikowych

225. Algorytm 3DES w trybie EDE wykorzystuje klucze o długości:
a) 256b
b) 116b
c) 64b
d) 192b

226. Wskaż cechy charakteryzujące kontrole dostępu MAC:

a) właściciel zasobu nie może przekazać możliwość decydowania o uprawnieniach dostępu do tego zasobu
b) właściciel zasobu może przekazać możliwość decydowania o uprawnieniach dostępu do tego zasobu
c) właściciel zasobu nie może decydować o uprawnieniach dostępu do tego zasobu
d) właściciel zasobu może decydować o uprawnieniach dostępu do tego zasobu
e) tylko właściciel zasobu może dysponować prawami dostępu do tego zasobu
f) tylko wyróżniony oficer bezpieczeństwa może dysponować prawami dostępu do zasobów
g) etykiety ochrony danych przypisane do zasobów automatycznie wymuszają uprawnienia

227. Który z wymienionych protokołów nie chroni przed podszywaniem się pod podmiot uwierzytelniający:

a) SSL v3
b) SSL v2
c) TLS v1
d) PAP

228. Który z wymienionych protokołów nie chroni przed podszywaniem się pod podmiot uwierzytelniający:

a) IPsec/IKE
b) IPsec/ISAKMP
c) PAP
d) SSL

229. Wskaż przykłady zamaskowanych kanałów komunikacyjnych:

a) system plików (tworzenie / usuwanie pliku)
b) obciążenie procesora
c) SSL
d) VPN

231. Który protokół umożliwia transparentna dla stacji sieciowej obsługę uszkodzenia jej routera domyślnego?

a) RIP (Routing Information Protocol)
b) TRP (Transparent Router Protocol)
c) LSP (Link State Protocol)
d) HSRP (Hot Standby Routing Protocol)

232. Wskaż własności protokołu HSRP (Hot Standby Router Protocol):
a) służy do tworzenia tuneli VPN
b) zabezpiecza poczte elektroniczna
c) pozwala uzyskać redundancje routerów
d) wspomaga uwierzytelnianie

233. Wskaż najbezpieczniejszy standard zabezpieczeń komunikacji w sieciach bezprzewodowych Wi-Fi:
a) IEEE 802.11 WEP
b) IEEE 802.11i WPA
c) WPA-Enterprise
d) WPA-PSK

234. Które z poniższych standardów nie oferują żadnej redundancji:
a) RAID 0
b) RAID 5
c) RAID 3
d) RAID 1

235. Ktora klasa RAID zapewnia odpornosc na jednoczesna awarie 2 dyskow w 5-dyskowej macierzy?
a) RAID 2
b) RAID 1
c) RAID 6
d) żadna z powyższych

236. Program xinetd to:
a) ważny element systemu operacyjnego Linux, odpowiedzialny za uruchamianie innych programów
b) krytyczny program w systemie operacyjnym Linux, który zawsze musi być uruchomiony
c) krytyczny program w systemie operacyjnym Linux, który zawsze musi być uruchomiony, jest rodzicem dla wszystkich nowo powstałych procesów
d) bardzo ważny komponent systemu Linux, bez którego system operacyjny nie będzie działał prawidłowo z uwagi na niemoznosc uruchamiania dodatkowych programów

237. Relacja zaufania w uwierzytelnianiu w środowisku sieciowym
a) jest wykorzystywana zarówno przez systemy Unix, jak i MS Windows
b) może być jednostronna lub dwustronna
c) nie jest przechodnia
d) jest realizacją koncepcji SSO

238. Mechanizm ACL umożliwia
a) nadawanie praw (rwx) wielu użytkownikom i grupom
b) odtwarzanie zniszczonych plików
c) nadawanie nowych praw (np. dopisywania) wielu użytkownikom
d) ustanowienie szyfrowania plików

239. Jakie restrykcje pozwala narzucić systemowa funkcja chroot() systemu Unix?
a) ograniczenie odczytu do określonego poddrzewa systemu plików
b) ograniczenie komunikacji sieciowej do wybranych portów
c) niedostępność odziedziczonych deskryptorów
d) ograniczenie zapisu do określonego poddrzewa systemu plików

240. Które z poniższych mechanizmów stosują programy malware w celu kamuflażu swojej obecności
a) opancerzenie (armor)
b) zamaskowane węzły (shadow i-node)
c) fingerprinting
d) polimorfizm

241. SFTP to
a) klient protokołu FTP będący częścią pakietu SSH
b) niezależna implementacja protokołu Secure FTP
c) SSL FTP , czyli wersja protokołu FTP wykorzystująca mechanizm certyfikatów SSL
d) podsystem SSH służący do przesyłania plików
e) podsystem raportowania o błędach w SSH

242. Które zdania poprawnie opisują nawiązywanie sesji SSL?
a) serwer przesyła komunikat ServerHello ze swoim certyfikatem
b) klient uwierzytelnia serwer na podstawie odebranego certyfikatu
c) serwer przesyła komunikat ServerHello z opcjonalnym losowym zawołaniem
d) klient odsyła podpisane zawołanie do serwera tylko jeśli serwer zadał uwierzytelnienia klienta

243. Które z wymienionych protokołów i standardów oferują szyfrowaną transmisję wiadomości pocztowych?
a) X.400
b) S/MIME
c) PGP
d) SMTP

244. Wskaż możliwe środki ochronne przed atakami przepełnienia bufora
a) niewykonywany segment kodu
b) niewykonywany segment stosu
c) kontrola zakresu danych globalnych programu na etapie wykonania
d) kontrola zakresu danych lokalnych funkcji na etapie kompilacji

245. Wskaż szyfry symetryczne
a) Blowfish
b) DES
c) ElGamal
d) żadne z powyższych

246. Protokół IPv6
a) oferuje mechanizm AH w celu zapewnienia autentyczności
b) oferuje mechanizm ESP w celu zapewnienia poufności
c) nie oferuje AH, jako że jego zadania powiela ESP
d) nie oferuje żadnych mechanizmów bezpieczeństwa (wymaga dodatkowej implementacji IPsec)

247. Która zasada realizacji zabezpieczeń wymaga konsekwentnego zastosowania odpowiedniego mechanizmu ochrony wobec wszystkich wykorzystywanych protokołów aplikacyjnych

a) spójności poziomej
b) spójności pionowej
c) naturalnego styku
d) obligatoryjnej kontroli dostępu

248. Moduły PAM (Pluggable Authentication Modules) umożliwiają

a) oddzielenie konfiguracji procesu uwierzytelniania od kodu aplikacji
b) integrację uwierzytelniania użytkowników sieci pomiędzy systemami Windows i Linux
c) dostęp serwera usługi www (np. z systemu operacyjnego MS Windows w środowisku domenowym) do zewnętrznych źródeł danych uwierzytelniających, np. bazy danych
d) implementuje filtry Bayesa do ochrony poczty przed niepożądanymi przesyłkami

249. Okresl prawidlowa kolejnosc pelnej sekwencji odwolan klienta do serwerow w przypadku dostepu do uslugi SMTP w środowisku Kerberos

a) serwer TGS - serwer AS - serwer TGS - serwer SMTP
b) serwer AS - serwer TGS - serwer SMTP - serwer AS
c) serwer AS - serwer TGS - serwer SMTP
d) serwer TGS - serwer AS - serwer SMTP

250. Które protokoły umożliwiają propagacje portów w tunelu kryptograficznym?

a) ESP
b) SSH
c) SSL
d) AH

251. Standard SASL (Simple Authentication and Security Layer) umożliwia

a) rozszerzenie mechanizmu uwierzytelniania protokołu SMTP o mechanizm haseł jednorazowych
b) rozszerzenie mechanizmu uwierzytelniania protokołu IMAP o współpracę z systemem Kerberos
c) rozszerzenie mechanizmu kontroli dostępu do katalogu domowego o listy ACL
d) redukcje mechanizmu kontroli dostępu do plików w Windows do postaci rwx

252. Które zdania poprawnie opisują proces uwierzytelniania w usłudze pocztowej?

a) standard ESMTP umozliwia uwierzytelnianie metoda zawolanie-odzew
b) standard SMTP umozliwia uwierzytelnianie metoda zawolanie-odzew
c) w standardzie SMTP serwery uwierzytelniane są na podstawie adresów
d) standard ESMTP oferuje mechanizmy uwierzytelniania SASL i TLS

253. Ochronę SYSKEY wprowadzono w systemie MS Windows w celu

a) szyfrowania plików użytkowników w systemie NTFS
b) wzmocnionego szyfrowania postaci hash haseł użytkowników
c) odszyfrowania plików przez systemowa usługę odzyskiwania plików
d) szyfrowania plików systemowych w systemie NTFS

254. Skrót KDC w systemie Kerberos oznacza
a) Key Distribution Center
b) Kerberos Domain Controller
c) Kerberos Directory Center
d) Kerberos Designated Certificate

255. Funkcja skrótu dająca wynik 512-bitowy
a) ma teoretyczna odpornosc na kolizje = 2^256
b) wymaga klucza 512b
c) wymaga klucza 256b
d) ma teoretyczna odpornosc na atak urodzinowy = 2^256

256. Jakie komponenty tworzą każdą zaporę sieciowa?
a) dekoder ramek PDU
b) filtr pakietów
c) sniffer pakietów
d) skaner portów

257. Wskaż operacje stosowane w metodzie ARP cache detekcji snifferów
a) wysłanie zapytania ICMP echo request z fałszywym adresem źródłowym IP na adres podejrzewanej stacji
b) wysłanie ogłoszenia ARP o fałszywym adresie IP
c) wysłanie zapytania ICMP echo request z fałszywym adresem docelowym IP i oczekiwaniu na odpowiedź
d) odpytanie podejrzewanej stacji o wszystkie adresy MAC sieci lokalnej

258. Jaka usługa jest szczególnie narażona na atak TCP spoofing?
a) FTP, ponieważ domyślnie serwery działają w trybie pasywnym
b) FTP, ponieważ domyślnie serwery działają w trybie aktywnym
c) RCP, ponieważ używa adresu klienta do uwierzytelnienia
d) RCP, ponieważ nie używa adresu klienta do uwierzytelnienia

259. Przykładem realizacji mechanizmu uwierzytelniania z udziałem zaufanej trzeciej strony jest
a) protokół Kerberos
b) urząd CA
c) system PKI
d) protokół Diffiego-Hellmana

260. Mechanizm OTP (one-time passwords)
a) uniemożliwia atak poprzez odtwarzanie (replaying)
b) weryfikuje nietrywialność hasła podczas jego zmiany
c) jest niewrażliwy na podsłuch
d) uniemożliwia zdobycie hasła metodą przeszukiwania wyczerpującego

261. Które z wymienionych technik mogą być wykorzystane do uwierzytelniania z hasłami jednorazowymi
a) jednokrotne uwierzytelniane (single sign-on)
b) certyfikacja klucza sesji
c) metoda zawołanie-odzew (challenge-response)
d) synchronizacja czasu

262. Które z poniższych reguł są prawdziwe w przypadku mechanizmu Mandatory Access Control (MAC). Podmiot nie może …

a) zapisać danych o etykiecie niższej niż jego aktualna
b) uruchomić procesu o etykiecie wyższej niż jego aktualna
c) zapisać danych o etykiecie wyższej niż jego aktualna
d) czytaj danych o etykiecie niższej niż jego aktualna

263. Jakie funkcje moga pelnic systemy HIPS?

a) sondowanie usług (port enumeration)
b) zamek-i-klucz
c) monitor antywirusowy
d) ochrona przed atakami DoS

264. Do zrealizowania zamaskowanego kanału komunikacyjnego może potencjalnie posłużyć

a) port szeregowy
b) kolejka drukowania
c) system plików
d) obciążenie systemu

265. Wskaż warunek wystarczający do weryfikacji podpisu cyfrowego wiadomości S/MIME:

a) uprzednie przesłanie do nadawcy klucza publicznego odbiorcy
b) uprzednie przesłanie do odbiorcy klucza publicznego nadawcy
c) dostęp do centrum CA w celu pobrania certyfikatu wskazanego w podpisie (i innych certyfikatów na ścieżce certyfikacji)
d) wymiana kluczy między nadawcą a odbiorcą metodą Diffiego-Hellmana

266. Jakie właściwości można ustawić w Zasadach haseł w systemie Windows?

a) złożoność haseł
b) maksymalna długość nazwy użytkownika
c) minimalna długość nazwy użytkownika
d) włączenie szyfrowania AES haseł użytkowników
e) minimalna długość hasła użytkownika

267. Systemowa zapora sieciowa w systemie Windows:

a) pozwala zestawiać tunel IPsec domyślnie szyfrując dane algorytmem 3DES
b) może monitorować parametry asocjacji IPsec
c) pozwala zestawiać tunel IPsec domyślnie szyfrując dane algorytmem AES
d) może monitorować parametry asocjacji ISAKMP

268. 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:

a) wyłączenie obsługi przychodzących komunikatów ICMP echo
b) odrzucanie całego ruchu ICMP
c) zablokowanie komunikacji z siecią dla programu ping
d) wyłączenie ruchu IP na wszystkich interfejsach, ale pozostawienie dostępu do wskazanych portów TCP

269. Użytkownik U systemu Unix należący do grupy G1 nie ma wpisu na liście ACL do zasobu O w systemie plików. Jednak grupie G1 na liście ACL tego zasobu nadano prawa r i w, natomiast wszystkim pozostałym (others) - prawa r oraz x. Które efektywne uprawnienia do O posiada U? (U nie jest właścicielem O i nie należy do grupy zasobu O):

a) r
b) w
c) x
d) żadne

270. Zasoby systemu operacyjnego MS Windows udostępnione poprzez SMB:

a) mogą mieć ograniczony dostęp do odczytu i/lub zapisu tylko dla wskazanych użytkowników
b) nazywa się udziałami
c) nazywa się portami
d) przy dostępie zdalnym zawsze wymagane jest logowanie (podawanie hasła)
e) tylko użytkownicy, którzy posiadają lokalne konto w systemie operacyjnym mogą uzyskać zdalny dostęp do zasobu

271. ssh -L 9999:cerber:23 polluks Wybierz prawdziwe stwierdzenia dotyczące powyższego polecenia:

a) ruch między między lokalnym komputerem a polluksem będzie szyfrowany
b) dane kierowane na port 9999 systemu cerber zostaną przesłane w zaszyfrowanej formie na port 23 systemu polluks
c) dane kierowane na port 9999 systemu cerber zostaną przesłane w niezabezpieczonej formie na port 23 systemu polluks
d) w wyniku polecenia zestawiony zostanie zabezpieczony tunel między systemem cerberem a polluksem

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

a) właściciel obiektu, ale pod warunkiem, że posiada prawo 'w'
b) właściciel obiektu, niezależnie od posiadania prawa 'w'
c) dowolny użytkownik posiadający prawo modyfikacji pliku
d) administrator (root)

273. Mechanizm SUID/SGID:

a) SUID zawsze powoduje wykonanie aplikacji z uprawnieniami grupy właściciela aplikacji
b) SUID zawsze powoduje wykonanie aplikacji z uprawnieniami administratorskimi
c) SGID zawsze powoduje wykonanie aplikacji z uprawnieniami administratorskimi
d) SGID zawsze powoduje wykonanie aplikacji z uprawnieniami grupy właściciela aplikacji

274. Wpisy ACE (na liście ACL) zabraniające dostępu:

a) występują tylko w przypadku zwirtualizowanych aplikacji w MS Windows
b) nie są dziedziczone wgłąb katalogu
c) występują tylko w POSIX ACL
d) mają priorytet nad wpisami ACE przyznającymi dostęp

275. Jakie metody uwierzytelniania oferuje protokół HTTP:
a) obustronne uwierzytelnianie metodą Diffiego-Hellmana
b) uwierzytelnianie serwera poprzez certyfikat X.509
c) uwierzytelnianie klienta poprzez userame token (username+password)
d) uwierzytelnianie klienta metodą digest (z użyciem funkcji skrótu)

276. Trusted Platform Module (TPM) może być wykorzystywany do:
a) przechowywania kluczy kryptograficznych używanych przez aplikacje w systemie operacyjnym
b) uwierzytelniania podmiotu przy wystawianiu certyfikatu przez urząd CA w systemie PKI
c) podejmowania decyzji o autoryzacji w systemie kontroli dostępu MAC
d) wykonywania operacji kryptograficznych zlecanych przez aplikacje w systemie operacyjnym

277. Czy zaszyfrowany plik w systemie MS Windows możemy współdzielić z innym użytkownikiem?
a) tylko pod warunkiem przekazania temu użytkownikowi swojego klucza prywatnego
b) tylko pod warunkiem przekazania temu użytkownikowi swojego klucza publicznego
c) nie jest to możliwe
d) pod warunkiem posiadania certyfikatu EFS tego użytkownika

278. W jaki sposób można jednoznacznie określić, które konto w systemie operacyjnym MS Windows jest wbudowanym kontem administracyjnym?
a) Aktualnie nie ma jednego wbudowanego konta administracyjnego- każde konto użytkownika może posiadać takie uprawnienia po odpowiedniej konfiguracji
b) konto takie ma zawsze nazwę “Administrator”
c) część względna identyfikatora tego konta ma stałą wartość 500
d) część względna identyfikatora tego konta ma stałą wartość 0

279. Co oznacza termin “asocjacja bezpieczeństwa” (ang.Security Association)?
a) Nazwa jednokierunkowego protokołu uwierzytelniania tuneli IPSec
b) Jest to zestaw parametrów zabezpieczonego połączenia niezbędny do poprawnej interpretacji danych płynących w tunelu VPN
c) Jest to wstępny proces zestawiania tunelu VPN, w którym negocjowane są parametry połączenia
d) Jest to nazwa polityki IPsec określające filtry pakietów poddawanych zabezpieczaniu

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

a) próg blokady określa ilość kolejnych niepomyślnych prób logowania, po osiągnięciu której dostęp do konta będzie czasowo zablokowany
b) licznik prób logowania jest zerowany automatycznie po upływie czasu blokady konta
c) podczas blokady konta, kolejne logowanie będzie możliwe dopiero po wyzerowaniu licznika prób (np. przez administratora)
d) w czasie określonym długością okresu zerowania licznika prób logowania, użytkownik nie może podjąć więcej udanych prób logowania niż określa próg blokady

281. Zapora sieciowa lokalnego systemu na stanowisku X zablokowała możliwość zdalnego odpytywania o dostępności X przy pomocy narzędzia ping, pozostawiając jednak możliwość zdalnego dostępu do serwera www w tym systemie. Mogła to osiągnąć poprzez

a) wyłączenie ruchu IP na wszystkich interfejsach, ale pozostawienie dostępu do wskazanych portów TCP
b) zablokowanie komunikacji z siecią dla programu ping
c) wyłączenie obsługi przychodzących komunikatów ICMP echo
d) odrzucenie całego ruchu ICMP

282. Która z poniższych usług aplikacyjnych wykorzystuje mechanizm SSO

a) rlogin
b) telnet
c) tcpd
d) xinetd
e) ssh
f) rsh

283. Mechanizm sudo umożliwia

a) wskazanie konta, z którego można wykonać polecenie bez pytania o hasło użytkownika przypisanego do pliku programu tego polecenia, pod warunkiem przynależności do grupy przypisanego do tego pliku
b) określenie jaki użytkownik może wykonywać konkretne programy z innymi uprawnieniami
c) wykonywanie tylko programów należących do użytkownika root z uprawnieniami bieżącego użytkownika
d) uruchamianie innych aplikacji wyłącznie z uprawnieniami administratora

284. Mechanizmem PAM można skonfigurować

a) ograniczenia czasowe dostępu do systemu operacyjnego
b) ograniczenie maksymalnego ilości procesów jakie może uruchomić użytkownik
c) sposób uwierzytelniania aplikacji
d) procedurę zmiany danych uwierzytelniających

285. Preshared key to
a) (wstępny) klucz symetryczny
b) mechanizm pozwalający uwierzytelniać i szyfrować za pomocą jednego klucza
c) silny mechanizm uwierzytelniania wykorzystujący generowany losowo po obu stronach klucz
d) silny mechanizm szyfrowania wykorzystujący certyfikaty SSL do generacji losowego klucza sesyjnego

286. Mechanizm User Account Control (UAC) systemu Windows:
a) blokuje konto po zdefiniowanej wcześniej ilości nieudanych prób logowania
b) wprowadza dodatkową formę ochrony konta administracyjnego m.in. przed koniami trojańskimi i złośliwym oprogramowaniem
c) pozwala administratorowi chwilowo skorzystać z pełnego tokenu administracyjnego
d) wirtualizuje dostęp do newralgicznych komponentów systemu plików

287. Klucz szyfrowania, którym zaszyfrowana została treść pliku (standardowym mechanizmem EFS z systemu NTFS)
a) znajduje się w certyfikacie właściciela pliku
b) znajduje się w certyfikacie każdego agenta DRA w systemie operacyjnym
c) jest zapisany wewnątrz zaszyfrowanego pliku
d) znajduje się w certyfikacie administratora systemu operacyjnego
e) jest przechowywany wraz z zaszyfrowanym plikiem

288. Skuteczna weryfikacja w systemie PGP podpisanego cyfrowo listu przesłanego od użytkownika A do użytkownika B wymaga:
a) wykonania podpisu kluczem prywatnym B
b) wykonania podpisu kluczem prywatnym A
c) wykonania podpisu kluczem publicznym B
d) wykonania podpisu kluczem publicznym A

289. xinetd to:
a) moduł jądra Linux, który implementuje kontekstową filtrację pakietów
b) prosty mechanizm szyfrowania używany przez zaporę sieciową w systemie Linux
c) element systemu operacyjnego Linux, odpowiedzialny za dynamiczne uruchamianie usług sieciowych
d) moduł jądra Linux, który limity zasobowe w stosie TCP/IP

290. Przy kopiowaniu zaszyfrowanego pliku z NTFS na partycję FAT:
a) plik będzie możliwy do odczytu tylko na systemie, na którym został zaszyfrowany
b) plik zostaje odszyfrowany
c) plik będzie później wymagał ręcznego odszyfrowania
d) plik może być skopiowany tylko przez użytkownika "Data Recovery Agent"

291. 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:

a) U lub G dziedziczą dostęp do odczytu z katalogu K
b) U jawnie odebrano prawo odczytu P, ale U dziedziczy to prawo z katalogu K
c) U jawnie odebrano prawo odczytu P, ale G dziedziczy to prawo z katalogu K
d) U lub G mają jawnie nadane prawo odczytu pliku P
e) tylko U ma jawnie nadany dostęp do P i K, G nie nadano żadnych praw ani do K, ani do P
f) tylko U dziedziczy dostęp do P i K, G nie dziedziczy żadnych praw ani do K, ani do P

292. Wskaż to z ustawień parametrów haseł (tylko jedno), które jest najkorzystniejsze dla bezpieczeństwa konta:

a) okres ważności hasła: nieskończony
b) maksymalna długość: 14 znaków
c) minimalna długość: 10 znaków
d) odwracalne szyfrowanie haseł: włączone

293. getfacl --omit-header 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::--x
default:other::r-x
```

Oznacza, że:

a) grupa "agents" może modyfikować zawartość obiektu test
b) właściciel może tworzyć pliki w katalogu test
c) użytkownik "jbond" może modyfikować zawartość obiektu test
d) użytkownik "jbond" może przeglądać listę plików w katalogu test

294. Stosowany w sieciach VPN preshared key to:

a) klucz publiczny z predefiniowanego certyfikatu SSL służący do generacji asymetrycznego klucza szyfrowania danych
b) statycznie ustalony po obu stronach tunelu klucz symetryczny
c) mechanizm uwierzytelniania wykorzystujący generowane losowo po obu stronach wstępne klucze asymetryczne D-H
d) mechanizm pozwalający uwierzytelniać strony tunelu

295. Czego nie można ograniczyć za pomocą komendy ulimit (mechanizmu limitów zasobowych)?
a) wielkości pliku zrzutu pamięci
b) ilości otwartych deskryptorów
c) ilości tworzonych procesów
d) sumy zajmowanej przestrzeni dyskowej przez pliki
e) ilości zalogowanych równocześnie użytkowników
f) ilości wykorzystanej pamięci operacyjnej przez proces

296. Asocjacja bezpieczeństwa (ang. Security Association) IPsec w systemie Windows:
a) to protokół zestawiania tunelu IPsec, w którym negocjowane są parametry tunelu
b) może być monitorowana przez systemową zaporę sieciową
c) obejmuje zestaw parametrów niezbędnych do komunikacji w tunelu IPsec
d) to polityka IPsec określająca filtry pakietów poddawanych tunelowaniu

297. Mechanizm sudo:
a) zawsze wymaga podania hasła docelowego użytkownika
b) można tak skonfigurować by wymagał podania hasła bieżącego użytkownika
c) można tak skonfigurować by nie wymagał podania hasła docelowego użytkownika
d) nigdy nie wymaga podania hasła docelowego użytkownika

298. Szyfrowanie asymetryczne w PGP:
a) jest wykorzystywane do zaszyfrowania treści wiadomości
b) jest wykorzystywane przy podpisywaniu wiadomości
c) to uzywanie dwoch matematycznie zaleznych kluczy
d) wymaga użycia klucza publicznego nadawcy do rozszyfrowania listu
e) wymaga użycia klucza publicznego odbiorcy do zaszyfrowania listu

299. Wskaż możliwe sposoby uwierzytelniania tunelu IPsec w systemie Windows:
a) Wskaż możliwe sposoby uwierzytelniania tunelu IPsec w systemie Windows:
b) certyfikat X.509
c) hasło
d) klucz RSA

300. Jak często sudo będzie pytać użytkownika o hasło?
a) co określony czas od ostatniego użycia
b) nigdy, jeśli sudo wykorzystuje SSO
c) tylko przy pierwszym użyciu po zalogowaniu
d) za każdym razem, kiedy zostanie wywołane

301. Mechanizm POSIX ACL umożliwia:
a) nadawanie praw do zasobów plikowych poszczególnych użytkownikom i grupom
b) odtwarzanie skasowanych plików pod warunkiem posiadania praca C
c) szyfrowania plików metodą symetryczną
d) automatyczne sumowanie uprawnień użytkownika ze wszystkich grup, do których należy

302. Historia haseł jest przechowywana przez system operacyjny:
a) aby wykluczyć ponowne użycie tego samego hasła jednorazowego
b) aby wykluczyć ustawienie nowego hasła identycznego z jakimkolwiek wcześniej wybranych przez tego samego użytkownika od początku
c) w połączeniu z minimalnym okresem ważności hasła, aby wykluczyć zbyt częste wybieranie przez użytkownika tego samego nowego hasła
d) aby umożliwić tzw. przypomnienie haseł użytkowników (szczególnie użyteczne w przypadku aplikacji nieobsługujących funkcji jednokierunkowych)

303. Pojedyncza reguła zapory sieciowej Windows:
a) może dotyczyć jednocześnie ruchu przychodzącego i wychodzącego
b) może dotyczyć wszystkich 3 profili sieciowych jednocześnie
c) może być ustawiona z użyciem polecenia netsh
d) może dotyczyć tylko wskazanego programu

304. Grupa użytkowników w systemie MS Windows o nazwie Użytkownicy uwierzytelnieni:
a) jest identyczna z grupą Wszyscy
b) jest podzbiorem grupy Wszyscy
c) obejmuje wszystkich użytkowników lokalnych
d) nie obejmuje konta Gość

305. Mechanizm mandatory Integrity Control (MIC) system Windows:
a) przypisuje procesowi jeden z 5 poziomów uprawnień uwzględnianych dodatkowo w kontroli dostępu
b) pozwala ograniczyć dostęp do odczytu dla wybranych plików
c) pozwala ograniczyć dostęp do zapisu w systemie plików
d) pozwala ograniczyć swobodę komunikacji między procesami

306. Wskaż pliki zaangażowane w konfigurację TCP wrappera w systemie Unix:
a) /etc/hosts.allow
b) /etc/hosts
c) /etc/hosts.deny
d) /etc/hosts.equiv

307. Wybierz prawdziwą kolejność operacji NAT:
a) PREROUTING(mangle) PREROUTING(nat) FILTERING POSTROUTING(nat) POSTROUTING(mangle)
b) PREROUTING(nat) PREROUTING(mangle) FILTERING POSTROUTING(nat) POSTROUTING(mangle)
c) PREROUTING(nat) PREROUTING(mangle) FILTERING POSTROUTING(mangle) POSTROUTING(nat)
d) PREROUTING(mangle) PREROUTING(nat) FILTERING POSTROUTING(mangle) POSTROUTING(nat)

308. Wskaż różnicę między dwoma komendami sudo su oraz su:
a) jedyną różnicą jest to, że aby wykonać polecenie sudo su użytkownik musi należeć do grupy whels
b) sudo su może wymagać podania hasła bieżącego użytkownika, su natomiast root'a
c) su będzie wymagać podania hasła bieżącego użytkownika, sudo su natomiast root'a
d) nie ma żadnej różnicy, sudo su jest aliasem na su OpenVPN

309. Które konfiguracje tuneli obsługuje system OpenVPN:
a) 1 do wielu przy uwierzytelnianiu poprzez wspólny klucz
b) 1 do 1 przy uwierzytelnianiu poprzez certyfikaty X.509
c) 1 do 1 przy uwierzytelnianiu poprzez wspólny klucz
d) 1 do wielu przy uwierzytelnianiu poprzez certyfikaty X.509

310. Wskaż elementy konfiguracji klienta ssh niezbędne do uwierzytelnienia bez konieczności interakcji z użytkownikiem:
a) klucz publiczny użytkownika musi zostać dopisany do pliku authorized_keys w węźle docelowym
b) klucz prywatny użytkownika musi zostać dopisany do pliku authorized_keys w węźle docelowym
c) w lokalnym pliku known_hosts zapisany musi być klucz publiczny docelowego węzła
d) w lokalnym katalogu .ssh znajdować się musi klucz prywatny docelowego węzła

311. Definicji zaufania (single-sign-on) dla usług r* można dokonywać w:
a) ~/.rhosts
b) /etc/rhosts
c) ~/.sso_hosts
d) /etc/hosts.allow
e) /etc/hosts.equiv
f) /etc/hosts

312. W jaki sposób przebiega uwierzytelnianie w usłudze rlogin
a) uwierzytelnienie obu stron połączenia następuje mechanizmem Challenge-Response
b) zawsze wymagane jest uwierzytelnianie bez hasła
c) możliwe jest wykorzystanie SSO by nie podawać hasła
d) zawsze wymagane jest hasło

313. Udział C$ jest to:
a) udział domyślny kontrolera domeny służący do obsługi logowania w sieci
b) udział służący do dostępu do dysku C w celach zdalnej administracji
c) udział komunikacji międzyprocesowej w systemie operacyjnym
d) udział do komunikacji IPsec

314. Jaka jest kolejność sprawdzania reguł w plikach hosts.deny hosts.allow
   a) jeśli znajdzie się najpierw dopasowanie w deny to allow w ogóle nie jest sprawdzane
   b) najpierw deny do pierwszego dopasowania
   c) najpierw allow do pierwszego dopasowania
   d) jeśli znajdzie się najpierw dopasowanie w allow to deny w ogóle nie jest sprawdzane
315. Co można ustawić w zasadach kont w MS Windows
   a) minimalną długość nazwy użytkownika
   b) maksymalną długość nazwy użytkownika
   c) minimalną długość hasła
   d) maksymalną długość hasła
   e) złożoność hasła
   f) szyfrowanie AES
   g) Minimalny czas ważności hasła
316. Czy maska uprawnień POSIX ACL jest definiowana dla każdego użytkownika osobno?
   a) tak, z priorytetem maski domyślnej (logiczny AND)
   b) nie, maskę można zdefiniować tylko dla grup użytkowników
   c) tak, jeśli jawnie wskażemy nazwę użytkownika
   d) nie, istnieje tylko jedna obowiązująca maska
317. Przesłanie i zweryfikowanie podpisanego cyfrowo listu w standardzie S/MIME od użytkownika A do użytkownika B wymaga:
   a) pozyskania przez użytkownika B tajnego klucza symetrycznego od A
   b) pozyskania przez B certyfikatu klucza publicznego A
   c) pozyskania certyfikatów kluczy publicznych wzajemnie przez obu użytkowników
   d) pozyskania przez A certyfikatu klucza publicznego B
318. Szyfrowanie symetryczne plików mechanizmem EFS systemu NTFS
   a) może być realizowane po zainstalowaniu dodatkowego oprogramowania DRA
   b) może być realizowane pod warunkiem posiadania przez użytkownika certyfikatu klucza publicznego
   c) szyfruje pliki użytkownika jego kluczem prywatnym
   d) nie jest realizowane przez system operacyjny starszy niż Windows 10
319. Mechanizm impersonation systemu Windows:
   a) jest wykorzystywany przez polecenie <code>runas</code>
   b) pozwala zdefiniować dla użytkownika inną nazwę wyświetlaną (np. imię i nazwisko) niż nazwę konta
   c) definiuje 5 dodatkowych poziomów kontroli dostępu do danych i procesów
   d) pozwala procesowi użyć chwilowo innego niż bieżący tokenu zabezpieczeń
320. Możliwości uwierzytelniania się przy użyciu SSH2 to:
   a) mechanizm zaufania (.rhosts) // to odpada, SSH2 zrezygnowało z mechanizmu zaufania
   b) symetryczne klucze użytkownika
   c) hasło użytkownika
   d) asymetryczne klucze użytkownika

321. W jakim celu można weksportować certyfikat do formatu PKCS #12:
a) W celu wyekstraktowania klucza do szyfrowania wiadomości
b) W celu wyekstraktowania klucza aby przekazać go drugiej stronie
c) W celu stworzenia kopii zapasowej certyfikatu
d) zaimportować w kliencie pocztowym - ze skryptu z labów

322. Który mechanizm pozwala na wirtualizację jądra systemu:
a) VBS
b) ARM TrustZone
c) TEE
d) SSL

323. Aby zweryfikować podpis cyfrowy w systeme PGP wiadomości od nadawcy A do odbiorcy B potrzeba:
a) klucz prywatny nadawcy A, przecież B nie posiada klucza prywatnego A, a A podpisuje swoim prywatnym
b) klucz publiczny nadawcy A
c) klucz prywatny odbiorcy B
d) klucz publiczny odbiorcy B

324. Kiedy w Windowsie następuje zerowanie licznika prób wpisania hasła:
a) Po pomyślnym zalogowaniu
b) Po upływie określonego czasu
c) Administrator może ręcznie wyzerować
d) nie pamiętam, ale nie powinno być zaznaczone

325. Czy iptables umożliwia określenie domyślnej polityki w łańcuchu?
a) Tylko w łańcuchach tablicy filter
b) Tylko w predefiniowanych łańcuchach
c) Tak, w każdym łańcuchu
d) tylko w nowo utworzonych lancuchach
e) tak
f) tylko w standardowych lancuchach
g) Nie

326. W metodzie uzgadniania klucza Diffiego-Hellmana system kompromituje (narusza bezpieczenstwo)
a) przechwycenia jednego z wymienianych kluczy
b) przechwycenia obu wymienianych kluczy
c) podstawienie falszywego klucza w miejsce kazdego z wymienianych
d) podstawienie falszywego klucza w miejsce dowolnego z wymienianych

327. Klasa B1 wg TCSEC („Orange Book”) lub rownowazna jej klasa EAL4 wg Common Criteria wymaga m. in.
a) ochrony systemowych obszarow pamieci
b) uwierzytelniania uzytkownikow
c) scislej kontroli dostepu do danych (MAC)
d) szyfrowania plikow

328. Czy certyfikaty SSL dla obu stron polaczenia vpn nawiazanego przy pomocy programu OpenVPN musza by podpisane przez ta sam zaufana strone trzecia?
a) nie, poniewaz nie ma takiej opcji w OpenVPN
b) nie, poniewaz nie ma znaczenia czy to jest to samo CA, wazne aby zaufanie strony trzeciej bylo ogolnie znane CA, np. Thawte, VeriSign, Unizeto

c) nie trzeba podawac parametru wskazujacego na CA, jest to opcjonalne
d) tak

329. Ktore funkcje i parametry konfiguracyjne PHP moga byc wykorzystane do ochrony przed atakami typu command injection?

a) magic_quotes_gpc
b) addslashes()
c) mysql_escape_string()
d) strip_tags()

330. Wskaz prawidlowe stwierdzenia dotyczace metod uwierzytelniania systemow operacyjnych MS Windows w srodowisku sieciowym:

a) Kerberos jest bezpieczniejszy niz LM i NTLM
b) LM jest bezpieczniejszy niz NTLM
c) Kerberos jest bezpieczniejszy niz NTLM, ale jest dostepny tylko w srodowisku domenowym
d) NTLM jest bezpieczniejszy niz LM

331. Program inetd to:

a) wazny element systemu operacyjnego Linux, odpowiedzialny za uruchamianie innych programow
b) krytyczny program w systemie operacyjnym Linux, ktory zawsze musi byc uruchomiony
c) krytyczny program w systemie operacyjnym Linux, ktory zawsze musi byc uruchomiony, jest rodzicem dla wszystkich nowo powstalych procesow
d) bardzo wazny komponent systemu Linux, bez ktorego system operacyjny nie bedzie dzialal prawidlowo z uwagi na niemoznosc uruchamiania dodatkowych programow

332. Wskaz cechy mechanizmu SYN cookies:

a) pozwala przegladarce na bezpieczna aktualizacje ciasteczek
b) minimalizuje ilosc informacji potrzebnych przegladarce do uwierzytelniania zdalnego dostepu
c) identyfikuje polaczenie wartoscia wpisywana do pola ACK
d) minimalizuje wielkosc zasobow przydzielanych przy odbiorze zadania nawiazania polaczenia

97. Mechanizm SYN cookies:

a) odpowiada na wcześniej odebrany pakiet SYN po zadanym czasie oczekiwania
b) pozwala przeglądarce na bezpieczną aktualizację ciasteczek
c) minimalizuje ilość informacji potrzebnych przeglądarce do uwierzytelniania zdalnego dostępu
d) odpowiada na właśnie odebrany pakiet SYN, tylko jeśli spełnia zadane kryteria poprawności
e) nie rozpoczyna zestawienia połączenia po odebraniu segmentu SYN
f) jest wykorzystywany do przeprowadzania rozproszonego ataku DoS
g) ogranicza zasoby przydzielane przez system przy odbiorze żądania nawiązania połączenia
h) identyfikuje połączenie wartością pola ACK

146. Która z poniższych cech poprawnie opisuje mechanizm SYN cookies:

a) chroni przed atakami buffer overflow
b) jest jedną z technik wzmacniania ataków DDos
c) chroni przed atakami SYN flood

d) po wysłaniu segmentu SYN/ACK nadawca zapomina o połączeniu

333. Jesli ls -l plik.txt wyglada nastepujaco -rwx r-x r-x+ 1 user group 1000 2005-01-10 09:00 plik.txt to chmod 715 plik.txt" spowoduje:

a) zwiekszenie uprawnien wpisom ACL'owym
b) zmiane uprawnien grupie "group" dla tego pliku
c) zmniejszenie uprawnien wpisom ACL'owym
d) rozszerzenie uprawnien dla innych

334. Zapora sieciowa wbudowana w Ms Win XP sp2:

a) jest typu stateless
b) jest jedyna mozliwa do zastosowania zapora sieciowa w systemie
c) pozwala powiadamiac uzytkownika droga mailowa o zagrozeniach
d) jest zapora typu stateful

335. W jaki sposob mozna utworzyc wiele polaczen z danego hosta za pomoca programu OpenVPN?

a) nalezy powtorzyc wpisanie opcji: remote tyle razy ile polaczen VPN mamy utworzyc
b) nalezy uruchomic program OpenVPN z przelacznikiem: --force-multi-instance, wymuszajac w ten sposob uruchomienie wielu procesow programu OpenVPN do obslugi wielu jednoczesnych polaczen vpn
c) nie ma takiej mozliwosci
d) nalezy uruchomic program OpenVPN z wieloma plikami konfiguracyjnymi, kazdy plik definiuje jedno polaczenie
e) nalezy wykorzystac opcje --mode server ale tylko dla polaczen z zastosowaniem certyfikatow SSL
f) nalezy uruchomic kolejne instancje programu OpenVPN wraz z osobnymi plikami konfiguracyjnymi

336. Ktore polecenie bedzie poprawne, dla ustalenia DNAT (wybierz 2 odpowiedzi)?

a) iptables -t nat -A FORWARD -d 150.254.17.3 -i eth- -j DNAT --to 192.168.1.1
b) iptables -t nat -A PREROUTING -d 150.254.17.3 -i eth0 -j NAT --to 192.168.1.1
c) iptables -t nat -A PREROUTING -i eth0 -j SAME --to 150.254.17.2
d) iptables -t nat -A PREROUTING -d 150.254.17.3 -i eth0 -j DNAT --to 192.168.1.1
e) iptables -t nat -A POSTROUTING -d 150.254.17.3 -i eth0 -j DNAT --to 192.168.1.1
f) iptables -t nat -A POSTROUTING -o eth0 -j SAME --to 150.254.17.2

337. Ponizsza regula zostala wpisana na komputerze pelniacym role routera: iptables -t filter -A INPUT -m state --state NEW -j DROP

a) odrzuca nowe polaczenia do tego komputera
b) odrzuca nowe polaczenia inicjalizowane przez ten komputer
c) odrzuca nowe polaczenia przechodzace przez ten komputer
d) DROP znaczy nie przeszukuj dalej zapory, przepusc pakiet

338. Narzedzie OpenVPN

a) dziala tylko na protokole TCP
b) wykorzystuje mechanizm pre-shared key do losowego generowania kluczy
c) nie ma wyroznionego programu serwerowego i klienckiego
d) jest przykladem SSL-VPN
e) wykorzystuje certyfikaty MD5 i funkcje skrotu SHA-1 do uwierzytelniania stron i szyfrowania ruchu sieciowego
f) wykorzystuje mechanizm SSL-VPN do laczenia sie z serwerami wspierajacymi protokol https np. Apache

339. Narzedzie Vtun to:
a) samodzielny pakiet niskopoziomowego(dzialajacego na poziomie jadra) oprogramowania do tworzenia podsieci VPN
b) proste narzedzie do tworzenia polaczen VPN korzystajace tylko z jednego pliku konfiguracyjnego i zestawu narzedzi obecnych w systemie
c) narzedzie dzialajace na poziomie warstwy uzytkownika (tzw. userland) pozwalajace tworzyc tylko pojedyncze polaczenia VPN przy uzyciu prostego pliku konfiguracyjnego vtund.

340. Program Vtun dziala w architekturze:
a) punkt – punkt
b) klient – serwer
c) polaczenia peer-to-peer dla kazdego polaczenia
d) w zadnej z powyzszych poniewaz Vtun jest bardzo prosty i nie zawiera w sobie zadnej skomplikowanej architektury

341. Program Vtun dziala:
a) na porcie domyslnym 1045 ale mozna to zmienic
b) na porcie domyslnym 5000 i mozna to zmienic ale trzeba przekompilowac kod programu
c) na domyslnym porcie 5000
d) na porcie domyslnym 1001 mozna to zmienic w pliku konfiguracyjnym vtund.conf
e) na porcie domyslnym 1045 ale mozna to bez problemu zmienic w pliku konfiguracyjnym vtund.conf

342. Polaczenie w Vtun przebiega nastepujaco:
a) w momencie tworzenia polaczenia wykonywane sa odpowiednie podsekcje up w definicji danego polaczenia ktore ma zostac utworzone, w momencie zakonczenia polaczenia wykonywana jest podsekcja down w definicji polaczenia
b) po nawiazaniu polaczenia obie strony uzgadniaja parametry polaczenia takie jak np. haslo i rodzaj transmisji danych, w momencie zakonczenia polaczenia nastepuje specjalna procedura rozpoczynana przez strone, ktora chce zakonczyc polaczenie
c) w zaden z wymienionych, na poczatku sposobow, obie strony musza wymienic sie ustalonym haslem, potwierdzic jego prawdziwosc, wynegocjowac parametry transmisji i dopiero tworzone jest polaczenie do przesylania danych, zakonczenie rozpoczynane jest przez dowolna strone

343. Czy polecenie jest poprawne? iptables -t mangle -A PREROUTING -s localnet -d ! localnet -m ipp2p --dc -m comment --comment "zla regulka" -j TTL --ttl-set 1
a) tak, ale system bedzie usuwal te pakiety
b) tak, lecz taka regula niczego nie zmieni, gdyz nie ma celu ACCEPT lub DROP
c) nie, gdyz nie mozna uzywac wielu argumentow "-m"
d) nie, gdyz cel TTL moze byc uzywany tylko w lancuchu POSTROUTING

344. Idea polaczen typu VPN jest
a) zmiana routingu pakietow, aby z jednej sieci pakiety trafialy bezposrednio do sieci docelowej
b) wsparcie polaczen p2p, aby hosty mogly bezposrednio komunikowal sie
c) obejscie problemow z polaczeniami z sieciami zlokalizowanymi za NAT
d) mozliwosc zapewnienia bardziej niezawodnych, w sensie polaczeniowym, niz TCP polaczen miedzy hostami
e) utworzenie sieci laczacej odseparowane, odlegle sieci lokalne

345. Opcja PARANOID w pliku hosts.deny

a) blokuje zdalne zarzadzanie mechanizmem TCP wrappers, pozostawiajac dostep tylko z lokalnego hosta
b) wymusza sprawdzanie segmentow TCP czy sa poprawne w stosunku do norm RFC
c) pozwala ograniczyc ilosc pakietow/s przychodzacych do danej uslugi
d) blokuje pakiety pochodzace od hosta, ktorego ip nie posiada nazwy domenowej

346. getfacl --omit-header acl-test5 user::r-x user:inf44444:r-- group::rw- group:student:r-x mask::rwx other::--x Oznacza:
a) uzytkownik "inf44444" nie moze czytac pliku acl-test5
b) wlasciciel ma prawo zmodyfikowac zawartosc katalogu acl-test5
c) uzytkownik "inf44444" moze czytac plik acl-test5
d) maska blokuje wszystkie uprawnienia do pliku acl-test5
e) grupa wlasciciela moze zmodyfikowac plik acl-test5
f) grupa "student" moze zmodyfikowac plik acl-test5

347. Zaleta single-sign-on jest:
a) jednokrotne uwierzytelnianie
b) stosowanie funkcji skrotu w celu uwierzytelniania
c) jednokrotne szyfrowanie
d) jednokrotna autoryzacja

348. $ssh host Enter passphrase for key '/home/junior/.ssh/id_dsa': Wpis passphrase to:
a) Haslo, ktorym jest zaszyfrowany klucz publiczny
b) haslo, ktorym jest zaszyfrowany klucz prywatny
c) klucz, ktorym bedzie szyfrowana transmisja
d) haslo wymagane przez zdalny host, aby zostac zalogowanym

349. getfacl --omit-header acl-test1 user::rw- user:junior:rwx group::r-- group:student:r-x mask::r-- other::--- Oznacza, ze:
a) wlasciciel moze wykonac plik
b) grupa domyslna/wlasciciela moze odczytac plik
c) uzytkownik "junior" moze wykonac plik
d) wlasciciel moze modyfikowac plik
e) grupa "student" moze wykonac plik
f) inni moga zmodyfikowac plik

351. Szyfr, w ktorym poddawana szyfrowaniu zostaje tej samej wielkosci jednobajtowa porcja nieregularnie pojawiajacych sie danych, nazywamy:
a) strumieniowym
b) symetrycznym
c) blokowym
d) niesymetrycznym

352. SUID to:
a) uproszczona wersji limitow
b) bit uprawnien
c) odpowiednik SGID dla katalogow
d) rozszerzenie mechanizmu SUDO

353. W jaki sposob administrator moze narzucic ograniczenia uzytkownikom (limity)?
a) korzystajac z mechanizmu PAM
b) korzystajac z mechanizmu Kerberos
c) wykorzystujac skrypt "hosts.equiv"
d) wykorzystujac skrypty startowe systemu

354. Problem przepelnienia bufora dotyczy potencjalnie aplikacji:
a) napisanych w jezyku C
b) napisanych w jezyku Java
c) uruchamianych w systemie z rodziny Windows
d) uruchamianych w systemie z rodziny Unix/Linux

355. Czy istnieje mozliwosc zmiany portu docelowego i adresu docelowego na adres localhost i dowolny inny port?

a) tak
b) tylko, jesli okreslimy protokol oraz oryginalny port docelowy
c) tylko poprzez dodatkowy modul
d) nie

356. W jaki sposob program OpenVPN bedzie wiedzial, gdzie znajduje sie drugi koniec tunelu VPN

a) OpenVPN w sposob interaktywny poprosi uzytkownika o podanie adresu IP i numeru portu
b) nalezy wpisac odpowiednia opcje w pliku konfiguracyjnym
c) OpenVPN wysle zapytanie do najblizszego serwera VPN
d) OpenVPN odczytuje zawartosc zdalnej tablicy routingu i pobiera ta informacje

357. Dyrektywa "mask" w ACL okresla:

a) mozna ja modyfikowac jedynie raz
b) jest utozsamiana z uprawnieniami grupy
c) ukrywanie nadanych uprawnien dodatkowych uzytkownikow
d) nie ma zadnego znaczenia

358. Opcja spawn w pliku hosts.deny:

a) pozwala tworzyc kolejne procesy TCP wrapper
b) jest wykorzystywana tylko w pliku hosts.allow
c) nie jest wykorzystywana
d) pozwala odeslac do nadawcy specjalnie spreparowana wiadomosc w odpowiedzi na zadanie

359. Ktore polecenie bedzie poprawne, dla ustalenia SNAT

a) iptables -t nat -A FORWARD -o eth0 -j SNAT --to 150.254.17.2
b) iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 150.254.17.2
c) iptables -t nat -A PREROUTING -o eth0 -j SAME --to 150.254.17.2
d) iptables -t nat -A POSTROUTING -o eth0 -j NAT --to 150.254.17.2
e) iptables -t fnat -A PREROUTING -o eth0 -j SNAT --to 150.254.17.2
f) iptables -t nat -A POSTROUTING -o eth0 -j SAME --to 150.254.17.2

360. Czy iptables umozliwia ograniczenie dostepu do uslugi w jednym poleceniu?

a) jesli okreslamy protokol
b) jesli nie okreslimy protokolu
c) nie
d) tak

361. Oprogramowanie OpenVPN wykorzystuje tablice routingu w Linuxie:

a) do sprawdzenia kosztu trasy prowadzacej do sieci po drugiej stronie polaczenia VPN
b) aby dowiedziec sie jak nawiazac polaczenie z siecia po drugiej stronie tunelu VPN
c) do przechowywania trasy do sieci dostepnej po drugiej stronie polaczenia VPN
d) jako bufor przechowujacy nadchodzace informacje o zmianie trasy do odleglej sieci po drugiej stronie polaczenia VPN

362. Nazwa konta "administrator" w systemie Ms Windows XP:

a) mozna ja zmienic w kazdej chwili
b) jest definiowana przy instalacji systemu
c) mozna ja zmienic tylko przy wykorzystaniu dodatkowego oprogramowania
d) jest stala i nie moze byc zmieniona

363. Jaki uzytkownik zostanie wybrany w momencie logowania sie na zdalna maszyne przez rsh, gdy w poleceniu rsh nie podano nazwy uzytkownika?:

a) wystapi blad podczas uwierzytelniania poniewaz nie podano nazwy uzytkownika
b) lokalny uzytkownik nobody
c) zawsze root z uwagi na mozliwosc wykonania niektorych komend systemowych
d) lokalny uzytkownik rshd
e) zdalny uzytkownik rshd
f) lokalny uzytkownik operator
g) lokalny biezacy uzytkownik

364. Do czego sluzy komenda rsh?

a) pozwala wykonac zdalne polecenie na lokalnym hoscie
b) pozwala wykonac polecenie na zdalnym hoscie
c) pozwala nawiazac szyfrowane polaczenie ze zdalnym hostem

365. user::rw- user:inf44444:r-x group::rwx group:student:rwx mask::rwx other::--- Oznacza:

a) grupa "student" nie moze skasowac pliku
b) uzytkownik "inf44444" moze wykonac plik
c) grupa "student" moze skasowac katalog
d) wlasciciel moze wykonac plik
e) maska blokuje wszystkie uprawnienia
f) grupa domyslna (wlasciciela) nie moze zmodyfikowac pliku

366. Czy system MS Windows korzysta z serwera Kerberos?

a) nigdy
b) tylko w starszych systemach (95, 98)
c) zawsze
d) jesli zostanie odpowiednio skonfigurowany

367. Algorytmy SHA-256 i SHA-512 roznia sie wzajemnie:

a) ograniczeniami eksportowymi
b) dlugoscia kluczy
c) wielkoscia wynikowego skrotu
d) zadne z powyzszych

368. Ktorym z ponizszych terminow okresla sie ograniczone srodowisko wykonawcze aplikacji lub jej komponentu:

a) komnata (room)
b) komora (chamber)
c) karcer (jailbox)
d) piaskownica (sandbox)

369. Kontrola dostepu do zasobow jest zwiazana z zachowaniem wlasnosci:

a) poufnosci i integralnosci
b) tylko poufnosci
c) tylko integralnosci
d) zadnej z powyzszych

370. Czy RSBAC to:

a) poprawnie skonfigurowana polityka bezpieczenstwa
b) domyslne uprawnienia systemowe
c) zestaw rozszerzajacy kontrole uprawnien
d) zestaw łat na jadro systemu Linux

371. Pre-shared key to
a) przestarzaly mechanizm sluzacy do logowania sie na zdalnego hosta bez podawania hasla
b) cos takiego nie istnieje
c) prosty mechanizm pozwalajacy szyfrowac i uwierzytelniac strony za pomoca jednego klucza
d) silny mechanizm uwierzytelniania wykorzystujacy generowany losowo po obu stronach klucz
e) silny mechanizm szyfrowania wykorzystujacy certyfikaty SSL do generacji losowego klucza sesyjnego
f) jest to przyklad kryptografii symetrycznej

372. Co to jest challenge-response?
a) mechanizm pozwalajacy uwierzytelniac sie bez potrzeby przesylania tajnego klucza
b) przestarzala forma uwierzytelniania stosowana w ssh
c) nie istnieje cos takiego
d) mechanizm wykorzystywany w kryptografii dyskretnej
e) silny mechanizm szyfrowania wykorzystujacy kryptografie klucza publicznego

373. Czy serwer KDC w systemie Kerberos przechowuje konta uzytkownikow?
a) tak
b) tylko lokalne konta
c) nie
d) tylko konta administratorow

374. W jaki sposob polaczenie nawiazane przez rsh jest zabezpieczone?
a) kodowana komunikacja przy uzyciu funkcji XOR
b) szyfrowana komunikacja po podaniu hasla i loginu
c) komunikacja uwierzytelniana w kryptograficznie bezpieczny sposob
d) komunikacja nie jest chroniona

375. W RSBAC, czy mozna zmienic uprawnienia do katalogu dla programu podczas jego dzialania?
a) jesli program posiada taka mozliwosc (programista uwzglednil taka opcje)
b) nie jest to okreslone
c) istnieja takie mozliwosci
d) nie

376. Czy TCP wrapper to
a) samodzielny program analizujacy tylko polaczenia tcp
b) lata (ang. patch) rozszerzajaca funkcjonalnosc programu xinetd
c) program analizujacy tylko przychodzace polaczenia tcp, ale dla numerow portow na ktorych uruchomione sa uslugi zarzadzane przez xinetd
d) program w postaci prostego firewalla za pomoca ktorego mozna blokowac wychodzace polaczenia, odpowiednie reguly zapisywane sa w plikach /etc/hosts.allow i /etc/hosts.deny
e) dodatkowy podsystem sieciowy dla systemu operacyjnego Linux pozwalajacy na nakladanie ograniczen dla polaczen przychodzacych

377. user::r-x user:inf44444:r-- group::rw- group:student:r-x mask::rwx other::--x Oznacza
   a) wszyscy moga wykonac plik
   b) grupa "student" moze zmodyfikowac plik
   c) uzytkownik "inf44444" nie moze czytac plik
   d) uzytkownik "inf44444" moze czytac plik
   e) grupa wlasciciela moze zmodyfikowac plik
   f) maska blokuje wszystkie uprawnienia
378. Jaka usluga jest szczegolnie trudna do filtrowania statycznego?
   a) ftp, poniewaz domyslnie serwery dzialaja w trybie pasywnym,
   b) ftp, poniewaz domyslnie serwery dzialaja w trybie aktywnym,
   c) rlogin, bo costam
   d) rlogin, bo drugie costam
379. To koniec ponieważ:
   e) Mam wysoką ziemię
   f) nie ma już nic,
   g) słodzimy herbatę żeby mieć po co mieszać