Kierunek: ***Informatyka***

Specjalność: ***Cyberbezpieczeństwo***

Stopień: ***drugi***

Zagadnienia zakresowe (specjalnościowe)

1. Omów wirtualizację oraz korzyści płynące z jej zastosowania.
2. Omów różnice pomiędzy konteneryzacją a wirtualizacją.
3. Scharakteryzuj system plików ZFS oraz korzyści płynące z jego użycia.
4. Omów pojęcia funkcji jednokierunkowej oraz kryptografii asymetrycznej. Przedstaw znane Ci algorytmy kryptografii asymetrycznej.
5. Opisz zagadnienie podpisu cyfrowego.
6. Co wiesz na temat protokołów dzielenia sekretów oraz protokołów wielostronnych obliczeń.
7. Omów działanie i realizowane zadania NOC (ang. Network Operation Center).
8. Omów działanie i realizowane zadania SOC (ang. Security Operation Center).
9. Scharakteryzuj poznane metody kryptoanalizy algorytmu RSA.
10. Przedstaw zagadnienie kryptoanalizy algorytmów opartych na trudności obliczeniowej logarytmu dyskretnego.
11. Omów pojęcia: współczynnik koincydencji, entropia, atak siłowy oraz paradoks dnia urodzin.
12. Wymień sposoby weryfikacji tożsamości i omów jeden z nich.
13. Wyjaśnij różnicę pomiędzy błędnym dopasowaniem oraz błędnym niedopasowaniem, sposoby ich określania i interpretowania.
14. Na czym polega identyfikacja DNA, opisz możliwości stosowania tej techniki we współczesnych rozwiązaniach systemowych.
15. Wymień i omów zagrożenia w sieciach bezprzewodowych.

16. Wymień i omów trzy metodyki przeprowadzania audytów systemów informatycznych.
17. Jaka jest różnica pomiędzy audytem bezpieczeństwa a testem penetracyjnym? Dlaczego należy testować aplikacje sieciowe?
18. Wymień i krótko opisz formaty plików zawierających kopie binarne dysków.
19. W jaki sposób zapisać i odczytać alternatywny strumień danych z pliku.
20. Co to jest IMEI, ICCID i IMSI?
21. Opisz podstawową funkcję zapór ogniowych, opisz funkcje dostarczane przez zapory ogniowe klasy UTM.
22. Opisz podstawowe strategie zwiększające bezpieczeństwo sieci komputerowych.
23. Omów podstawowe zagrożenia związane z usługami DNS, DHCP oraz sposobami ich niwelowania.
24. Opisz podstawowe rodzaje połączeń VPN dostępne na zaporze sieciowej konfigurowanej na zajęciach laboratoryjnych.
25. Opisz podstawowe funkcje systemów IPS oraz IDS. Opisz podstawowe różnice między nimi.
26. Opisz co to są HoneyPots oraz HoneyNets. Jakie jest ich zastosowanie.
27. Przedstaw wybrane metody uczenia maszynowego, które można wykorzystać do wykrywania spamu w poczcie elektronicznej.
28. Opisz metody ataków na systemy sztucznej inteligencji.
29. Proszę omówić klucze szyfrujące PMK i PTK wykorzystywane w sieciach bezprzewodowych 802.11 z WPA.
30. Proszę scharakteryzować ataki pasywne i aktywne na sieci bezprzewodowe 802.11.
31. Proszę omówić mechanizmy bezpieczeństwa stosowane w Bluetooth, podać przykłady ataków.
32. Proszę omówić architekturę i zagrożenia sieci komórkowych 5G.