1. **Jaká je maximální délka IPv4 adresy?**
   a) 32 bitů
   b) 64 bitů
   c) 128 bitů
   d) 256 bitů

2. **Jaký typ IPv4 adresy je používán pro vnitřní sítě?**
   a) Veřejná adresa
   b) Privátní adresa
   c) Linková adresa
   d) Broadcast adresa

3. **Co znamená zkratka DNS v kontextu IPv4 sítí?**
   a) Data Network System
   b) Domain Name System
   c) Dynamic Network Services
   d) Digital Network Security

4. **Co je autentifikace uživatele?**
   a) Proces ověření totožnosti uživatele
   b) Proces šifrování dat uživatele
   c) Proces zabezpečení sítě
   d) Proces zrychlení přenosu dat

5. **Jaké jsou základní faktory autentizace uživatele?**
   a) Něco, co vím, něco, co mám, něco, co jsem
   b) Něco, co jím, něco, co mám, něco, co vidím
   c) Něco, co slyším, něco, co vím, něco, co cítím
   d) Něco, co píši, něco, co vidím, něco, co mám

6. **Jaké jsou základní metody autentizace uživatele?**
   a) Heslo, biometrická autentizace, tokeny
   b) Heslo, čárový kód, kryptografické klíče
   c) Kryptografické klíče, biometrická autentizace, tokeny
   d) Čárový kód, biometrická autentizace, heslo

7. **Jakou roli hraje autentizace uživatele v kyberbezpečnosti?**
   a) Zabezpečuje, že se uživatelé skutečně identifikují před vstupem do systému
   b) Zabraňuje neoprávněnému přístupu k citlivým informacím
   c) Zvyšuje ochranu proti kybernetickým útokům
   d) Všechny výše uvedené odpovědi jsou správné

8. **Co je to DNS?**
   a) Systém pro ukládání a převádění IP adres na doménová jména.
   b) Systém pro ukládání a převádění doménových jmen na IP adresy.
   c) Systém pro ukládání a převádění číselných adres na textové jméno serverů.
   d) Systém pro ukládání a převádění textových jmen na číselné adresy serverů.

9. **Co se stane, když se DNS server zeptá jiného DNS serveru o doménové jméno, které není v jeho vlastní databázi?**
   a) DNS server pošle dotaz zpět k počítači, který se na něj původně zeptal.
   b) DNS server pošle dotaz na kořenový server DNS.
   c) DNS server si uloží dotaz do mezipaměti a bude na něj čekat, dokud se neaktualizuje.
   d) DNS server vrátí chybovou hlášku a počítač, který se na něj zeptal, se musí zeptat jiného DNS serveru.

10. **Co je Zero Trust princip?**
    a) Bezpečnostní koncept, který předpokládá, že každý uživatel nebo zařízení musí být ověřen a autorizován před přístupem k síti nebo aplikaci.
    b) Bezpečnostní koncept, který předpokládá, že lze důvěřovat pouze uživatelům se správnými oprávněními.
    c) Bezpečnostní koncept, který předpokládá, že každý uživatel nebo zařízení může být automaticky autorizován při přístupu k síti nebo aplikaci.

11. **Co je cílem Zero Trust principu?**
    a) Ochrana firemních dat a sítě před neoprávněným přístupem.
    b) Umožnit uživatelům přístup k síti a aplikacím bez nutnosti opakované autentifikace.
    c) Umožnit neoprávněným uživatelům přístup k citlivým datům.

12. **Jaký je rozdíl mezi Zero Trust principem a tradičním síťovým zabezpečením?**
    a) Tradiční síťové zabezpečení předpokládá, že interní síť je důvěryhodná a externí síť ne, zatímco Zero Trust princip nepředpokládá důvěryhodnost žádné sítě.
    b) Tradiční síťové zabezpečení nepoužívá firewally, zatímco Zero Trust princip naopak.
    c) Tradiční síťové zabezpečení je založeno na tom, že každý uživatel má automaticky přístup k síti a aplikacím, zatímco Zero Trust princip naopak vyžaduje ověření a autorizaci před každým přístupem.

13. **Co je phishing?**
    a) Typ útoku, při kterém útočník získává citlivé informace pomocí falšovaných webových stránek nebo e-mailů. (správná odpověď)
    b) Typ útoku, kdy útočník získává neoprávněný přístup do sítě firem.
    c) Typ útoku, kdy útočník vysílá spamové e-maily s nežádoucím obsahem.
    d) Typ útoku, kdy útočník používá šifrovanou komunikaci k získání citlivých informací.

14. Jaký je hlavní cíl phishingového útoku?

a) Získat citlivé informace od uživatele, jako jsou hesla, bankovní údaje, čísla platebních karet atd.
b) Zpomalit počítačový systém.
c) Odeslat spamové e-maily s nežádoucím obsahem.
d) Ovládnout webovou stránku pro zobrazení nelegálního obsahu.

15. Co je spear phishing?

a) Typ phishingového útoku, který se zaměřuje na specifickou skupinu lidí nebo organizaci.
b) Typ phishingového útoku, kdy útočník získává neoprávněný přístup do sítě firem.
c) Typ phishingového útoku, kdy útočník používá šifrovanou komunikaci k získání citlivých informací.
d) Typ phishingového útoku, kdy útočník vysílá spamové e-maily s nežádoucím obsahem.

16. Jak se lze chránit proti phishingovým útokům?

a) Neposkytovat citlivé informace prostřednictvím e-mailů ani webových stránek, které nejsou důvěryhodné.
b) Používat veřejné Wi-Fi sítě pro odesílání citlivých informací.
c) Používat jednoduchá hesla pro snadnou paměť.
d) Stáhnout a spustit jakýkoli přílohu v e-mailu.

17. Co je phishingový e-mail?

a) E-mail, který se snaží získat citlivé informace od uživatele.
b) E-mail s nežádoucím obsahem.
c) E-mail, který obsahuje nebezpečné viry

18. Co je ransomware?

a) Antivirový program
b) Malware, který šifruje uživatelská data a požaduje výkupné
c) Typ počítačového hardwaru

19. Jak se ransomware nejčastěji šíří?

a) Přes neaktualizovaný software
b) Skrze phishingové e-maily
c) Přes sociální sítě

20. Jak se můžete chránit před ransomwarem?

a) Pravidelně aktualizovat software
b) Nesdílet hesla
c) Otevírat e-maily od neznámých odesílatelů

21. Co je síťový adresní prostor (network address space)?

a) Množina IP adres používaných v rámci jedné sítě
b) Soubor protokolů pro řízení přenosu dat v síti
c) Fyzický prostor, kde jsou umístěny síťové prvky

22. Jaká je maximální velikost síťového adresního prostoru v IPv4?

a) 2^8 (256)
b) 2^16 (65 536)
c) 2^32 (4 294 967 296)

23. Jaký je rozdíl mezi veřejnou a privátní IP adresou?

a) Veřejná IP adresa je používána v lokální síti, privátní IP adresa je přiřazena k zařízení připojenému k internetu
b) Veřejná IP adresa je globálně jedinečná a používá se pro komunikaci v rámci internetu, privátní IP adresa se používá v lokální síti
c) Rozdíl mezi veřejnou a privátní IP adresou neexistuje, jsou to synonyma

24. Co je síťový adresní prostor?

a) Fyzická adresa počítače v síti
b) Jednoznačná identifikace zařízení v síti pomocí IP adresy
c) Počet sítí, které mohou být vytvořeny v dané síťové infrastruktuře

25. Jaká je maximální délka IPv4 adresy?

a) 32 bitů
b) 64 bitů
c) 128 bitů

26. Jak se dělí IPv4 adresa?

a) Na 2 oktety
b) Na 4 oktety
c) Na 8 oktetů

27. Co je sociální inženýrství?

a) Technika pro vytváření sociálních sítí na internetu
b) Způsob, jak získat citlivé informace od lidí prostřednictvím manipulace
c) Způsob, jak efektivně využívat sociální média pro marketing

28. Jakou formu může mít sociální inženýrství?

a) Hacking webových stránek

b) Získávání informací pomocí sociálních médií
c) Ovlivňování rozhodnutí pomocí emocionální manipulace

29. Co je to "tailgating" ?
a) Technika, při které útočník získává přístup do chráněného prostoru tím, že se podstrčí za legitimního uživatele
b) Technika, která slouží k rozšíření bezdrátové sítě
c) Technika, která zabezpečuje zvýšenou bezpečnost pro připojení k VPN síti

30. Jak může být použito sociální inženýrství k útoku na firemní síť?
a) Získání přístupových údajů pomocí e-mailového phishingu
b) Využití slabých hesel zaměstnanců
c) Fyzické proniknutí do budovy a instalace malware na počítači

31. Jak může být organizace chráněna před sociálním inženýrstvím?
a) Vzděláváním zaměstnanců o bezpečnosti
b) Používáním silných hesel
c) Instalací nejnovějšího antivirového softwaru

32. Co je to sociální inženýrství?
a) Útok na síťovou infrastrukturu pomocí sociálních sítí.
b) Manipulace s lidmi, aby sdělili citlivé informace.
c) Hacking pomocí softwarových nástrojů.
d) Zabezpečování sítě proti ztrátě dat.

33. Která z následujících praktik sociálního inženýrství je nejčastější?
a) Phishing
b) Shoulder surfing
c) Dumpster diving
d) Baiting

34. Co znamená termín "pretexting" v kontextu sociálního inženýrství?
a) Použití falešné identity nebo záminky k získání informací.
b) Získávání informací z veřejně dostupných zdrojů.
c) Získávání hesel a přihlašovacích údajů pomocí softwarových nástrojů.
d) Hacking síťových zařízení pomocí úniků v softwaru.

35. Co zahrnuje pojem informační bezpečnost?
a) Ochrana proti fyzickému napadení zařízení
b) Ochrana proti ztrátě dat

c) Ochrana proti neoprávněnému přístupu k datům a informacím
d) Ochrana proti škodlivému softwaru

36. Co znamená zkratka CIA v kontextu informační bezpečnosti?
a) Centrální informační agentura
b) Confidentiality, Integrity, Availability (tj. Ochrana důvěrnosti, integrity a dostupnosti dat)
c) Computer Incident Alert
d) Cyber Intelligence Agency

37. Jaké jsou základní kategorie bezpečnostních hrozeb v oblasti informační bezpečnosti?
a) Fyzické hrozby, sociální hrozby a kybernetické hrozby
b) Přírodní katastrofy, technické selhání a lidská chyba
c) Hackeři, viry a spam
d) Záplavy, požáry a vichřice

38. Co je to přístupový bod v kontextu informační bezpečnosti?
a) Bod, kudy vstupuje do systému uživatel nebo zařízení
b) Bod, kudy vstupují do systému síťové útoky
c) Bod, kudy vstupuje do systému škodlivý software
d) Bod, kudy vstupuje do systému neoprávněný uživatel

39. Jaké jsou základní prvky bezpečnostní politiky v oblasti informační bezpečnosti?
a) Identifikace hrozeb, zajištění bezpečnosti, ochrana dat a pravidla pro uživatele
b) Pravidla pro uživatele, šifrování dat, kontrola přístupu a zálohování dat
c) Detekce hrozeb, zálohování dat, šifrování komunikace a firewall
d) Zálohování dat, aktualizace softwaru, šifrování disku a bezpečná síťová konfigurace

40. Co znamená termín "cyber kill chain"?
a) Proces, který popisuje kroky útočníka při plánování a provádění kybernetického útoku.
b) Ochrana před kybernetickými útoky pomocí protivirového software.
c) Bezpečnostní opatření k minimalizaci počtu kybernetických útoků na organizaci.

41. Kolik fází obsahuje cyber kill chain?
a) 5
b) 7
c) 10

42. Jakým způsobem může organizace minimalizovat dopad útoku na základě cyber kill chain?
a) Snížením úrovně oprávnění zaměstnanců.
b) Využitím multifaktorové autentifikace.

c) Monitorováním a zamezením útočníkům v každé fázi cyklu útoku.

43. Jaká fáze cyber kill chain zahrnuje sběr informací o cíli?

a) Výzkum a průzkum.
b) Exploatace.
c) Dodání.

44. Jakou technologii může organizace využít k rychlému odhalení útoku v rané fázi cyber kill chain?

a) Antivirový software.
b) Firewall.
c) SIEM (Security Information and Event Management).

45. Co je internet?

a) Fyzická síť, která propojuje počítače po celém světě.
b) Globální systém sítí, které umožňují komunikaci a přenos dat po celém světě.
c) Program, který umožňuje prohlížení webových stránek.

46. Co jsou data?

a) Fyzické předměty, které se dají hmatat.
b) Informace, které jsou reprezentovány symboly nebo čísly.
c) Softwarové aplikace.

47. Co znamená označení "http" v adrese webové stránky?

a) Http je protokol pro přenos dat přes internet.
b) Http je označení pro webové stránky s bezpečným připojením (HTTPS).
c) Http je zkratka pro "hyper text markup language" - značkovací jazyk pro tvorbu webových stránek.

48. Co je to "cloud storage"?

a) Forma datového úložiště, kde jsou data uložena na vzdáleném serveru a lze k nim přistupovat z jakéhokoli zařízení připojeného k internetu.
b) Fyzické úložiště na pevném disku počítače.
c) Forma šifrování dat pro zvýšení jejich bezpečnosti.

49. Jakým způsobem mohou být data přenášena přes internet?

a) Pomocí kabelů, které propojují počítače po celém světě.
b) Pomocí bezdrátového připojení, jako je například WiFi.
c) Pouze přenosem dat mezi počítači připojenými k jedné lokální síti.

50. Co je cyberstalking?

a) Typ kybernetického útoku
b) Elektronické obtěžování nebo pronásledování člověka
c) Online nákupový systém
d) Metoda úniku osobních údajů

51. Jaké jsou příklady aktivit, které by mohly být považovány za cyberstalkování?

a) Následování někoho na sociálních médiích
b) Posílání hromadného spamu e-mailů
c) Neustálé telefonování a posílání zpráv bez souhlasu druhé osoby
d) Použití VPN pro ochranu identity online

52. Který z následujících faktorů může zvyšovat riziko cyberstalkingového útoku?

a) Mít veřejné profily na sociálních médiích
b) Mít silné heslo k e-mailovému účtu
c) Používání firewallu na počítači
d) Pravidelné mazání cookies z webového prohlížeče

53. Co byste měli udělat, pokud se stáváte obětí cyberstalkingového útoku?

a) Ignorovat to a doufat, že to přejde
b) Nahlásit to správci sociální sítě
c) Kontaktovat policii
d) Vyřešit to sám tím, že se stanete kyberdetektivem

54. Jak můžete zabránit cyberstalkingovému útoku?

a) Mít silné hesla a pravidelně je měnit
b) Omezit informace, které sdílíte online
c) Pravidelně kontrolovat své online profily
d) Všechny výše uvedené varianty jsou správné

55. Co je Pharming?

a) Typ útoku, kde útočník získává citlivé informace prostřednictvím phishingových e-mailů.
b) Typ útoku, kde útočník využívá softwaru, který modifikuje DNS záznamy, aby přesměroval uživatele na škodlivé webové stránky.
c) Typ útoku, kde útočník podvrhne identity ostatních uživatelů a získá přístup k jejich citlivým datům.
d) Typ útoku, kde útočník využívá škodlivého kódu, který se šíří pomocí sociálních sítí.

56. Jakým způsobem může útočník provádět Pharming útoky?

a) Pomocí modifikace DNS záznamů.
b) Pomocí získání hesla k cílovému účtu.

c) Pomocí phishingových e-mailů s malwarem.
d) Pomocí sociálního inženýrství a získání citlivých dat.

57. Jak se může uživatel bránit proti Pharming útokům?
a) Používáním silných hesel.
b) Aktualizací antivirového softwaru.
c) Používáním více faktorové autentizace.
d) Zabezpečením Wi-Fi sítě.

58. Co je Captcha?
a) Bezpečnostní protokol pro ochranu před útoky DDoS
b) Bezpečnostní protokol pro ochranu před robotickými útoky
c) Obrázek s textem, který slouží k ověření, že na stránku přistupuje skutečný uživatel
d) Způsob ověření identity uživatele pomocí biometrických údajů

59. Jak funguje Captcha?
a) Uživatel musí zadat své jméno a heslo pro ověření identity
b) Uživatel musí vyplnit formulář s otázkami pro ověření identity
c) Uživatel musí zadat kód z obrázku generovaného Captcha protokolem
d) Uživatel musí dokončit sérii výzev a odpovědí pro ověření identity

60. Proč se Captcha používá?
a) K ochraně před phishingovými útoky
b) K ochraně před robotickými útoky
c) K ochraně před útoky DDoS
d) K ověření identity uživatele pomocí biometrických údajů

61. Jaký je hlavní problém s Captcha?
a) Náklady na implementaci jsou příliš vysoké
b) Uživatelé ji často neumí správně vyplnit
c) Může být snadno obejitelná pomocí robotických útoků
d) Je příliš komplikovaná pro průměrného uživatele

62. Jaké jsou alternativy k Captcha?
a) Biometrická ověření
b) Tokeny a certifikáty
c) Sociální ověřování
d) Všechny výše uvedené

63. Jaký typ hesla je nejsilnější?

a) Jednoduché heslo, jako je "123456"
b) Krátké heslo s čísly, písmeny a symboly
c) Heslo složené z náhodných slov
d) Všechny výše uvedené typy hesel jsou stejně silné

64. Jaké jsou doporučené minimální požadavky na délku hesla?
a) 4 znaky
b) 6 znaků
c) 8 znaků
d) 10 znaků

65. Jakým způsobem lze zvýšit bezpečnost hesla?
a) Časté změny hesla
b) Použití kombinace písmen, čísel a symbolů
c) Použití osobních údajů jako součásti hesla
d) Všechny výše uvedené způsoby jsou správné

66. Jaký je problém s používáním jednoduchých hesel?
a) Jsou snadno odhadnutelné
b) Mají tendenci být zapomenuty
c) Zvyšuje se riziko útoku hrubou silou
d) Všechny výše uvedené odpovědi jsou správné

67. Jaké jsou některé doporučené praktiky pro vytváření silného hesla?
a) Použijte kombinaci písmen, čísel a symbolů
b) Použijte dlouhé heslo
c) Použijte unikátní heslo pro každou službu
d) Všechny výše uvedené praktiky jsou správné

68. Co je to kryptografie?
a) Studie o kryptických animacích
b) Studie o matematických technikách pro zabezpečení informací
c) Studie o tvorbě animovaných filmů
d) Studie o zabezpečení fyzických objektů

69. Co je asymetrická kryptografie?
a) Typ kryptografie, který používá stejné klíče pro šifrování a dešifrování
b) Typ kryptografie, který používá různé klíče pro šifrování a dešifrování
c) Typ kryptografie, který používá klíče založené na biometrických datech
d) Typ kryptografie, který se používá pouze pro šifrování souborů

70. Co je to šifrování?

a) Proces, kdy se text převádí do čitelného tvaru
b) Proces, kdy se text převádí do nečitelného tvaru
c) Proces, kdy se text ukládá na bezpečné místo
d) Proces, kdy se text přepisuje z jednoho jazyka do druhého

71. Jaký je účel kryptografie?

a) Umožnit přenos informací bezpečně mezi komunikujícími stranami
b) Umožnit přístup k nechráněným datům
c) Umožnit monitorování komunikace mezi stranami
d) Umožnit změnu dat bez vědomí uživatele

72. Co znamená termín "symetrická kryptografie"?

a) Typ kryptografie, který používá různé klíče pro šifrování a dešifrování
b) Typ kryptografie, který používá stejné klíče pro šifrování a dešifrování
c) Typ kryptografie, který používá klíče založené na biometrických datech
d) Typ kryptografie, který se používá pouze pro šifrování souborů

73. Co je hacking?

a) Legální a etické způsoby testování zabezpečení počítačů a sítí
b) Nelegální činnost spočívající v neoprávněném pronikání do počítačových systémů
c) Ochranný mechanismus chránící před neoprávněným přístupem do počítačových systémů
d) Software určený k ochraně počítačů proti hackingu

74. Co je white hat hacker?

a) Hacker, který se zaměřuje na nelegální činnosti
b) Hacker, který se zaměřuje na zabezpečení a testování systémů
c) Hacker, který se specializuje na sociální inženýrství
d) Hacker, který pracuje pro státní organizace

75. Co znamená termín "exploit" v kontextu hackingu?

a) Software, který umožňuje hackerovi získat přístup do cílového systému
b) Hacking nástroj, který umožňuje monitorovat síťovou komunikaci
c) Počítačový program určený k blokování útoků hackerů
d) Technika, která umožňuje ochránit přístupové údaje pomocí biometrických prvků

76. Co znamená termín "penetration testing"?

a) Hacking technika, která využívá nejnovější zranitelnosti operačního systému
b) Etické testování zabezpečení, které má za cíl nalézt chyby v počítačových systémech
c) Ochranný mechanismus proti neoprávněnému přístupu do počítačových systémů

d) Software určený k analýze síťového provozu

77. Co znamená termín "social engineering" v kontextu hackingu?

a) Technika, která umožňuje hackerovi vniknout do počítačového systému prostřednictvím sociálních sítí
b) Způsob, jak přemluvit uživatele, aby poskytl citlivé informace nebo umožnil přístup do systému
c) Hacking technika, která umožňuje získat přístup do sítě bez potřeby hesla
d) Softwarový nástroj určený k odstraňování virů a škodlivého kódu