1. **Které z následujících bodů lze zařadit mezi obecné principy pro bezpečnost IT?**
*Usilujte o jednoduchost.
*Externí zdroje pokládejte za nebezpečné.
Nepoužívejte klíče s délkou < 128 bitů.
Nikdy nezveřejňujte kritické bezpečnostní algoritmy.
*Fyzicky nebo logicky oddělte kritické zdroje.

2. **Základní metody autentizace uživatelů jsou založeny na něčem, co**
*vím
smím
*mám

3. **Protokoly SSL/TLS umožňují**
*kontrolu integrity přenášených dat
autentizaci jen a pouze jedné strany
komunikovat anonymně
zajistit nepopiratelnost
*autentizaci komunikujících stran (klient i server)

4. **Jakým způsobem je počítána analýza rizik metodou ALE (Annual Loss Expentancy)**
ALE=SLOxARE, kde SLO=Single Loss of Opportunity a ARE=Annualized Rate of Executions
ALE=SLO/ARE, kde SLO=Single Loss of Opportunity a ARE=Annualized Rate of Executions
ALE=SLO+ARE, kde SLO=Single Loss of Opportunity a ARE=Annualized Rate of Executions
ALE=SLE/ARO, kde SLE=Single Loss Expentancy a ARO=Annualized Rate of Occurence
ALE=SLExARO, kde SLE=Single Loss Expentancy a ARO=Annualized Rate of Occurence
ALE=SLE+ARO, kde SLE=Single Loss Expentancy a ARO=Annualized Rate of Occurence

5. **Chybovost biometrických systémů vyjádřená pomocí FRR (False Rejection Rate) je:**
Podíl počtu všech pokusů o přihlášení legitimních i nelegitimních uživatelů ku počtu všech pokusů o přihlášení legitimních uživatelů.
Podíl počtu akceptovaných pokusů o přihlášení legitimních uživatelů ku počtu všech pokusů o verifikaci legitimních uživatelů.
*Podíl počtu odmítnutých pokusů o přihlášení legitimních uživatelů ku počtu všech pokusů o přihlášení.
Podíl počtu akceptovaných pokusů o legitimních legitimních uživatelů ku počtu odmítnutých pokusů o přihlášení legitimních uživatelů.

6. **Poskytuje TOR testování integrity přenášených dat?**
Ano, je to obrana proti mig-in-the-middle útokům.
*Ano, je to vylepšení oproti původnímu návrhu Onion Routing systémů.
Ne, proč bychom něco takového potřebovali, stačí zaručená anonymita.
*Ano, je to obrana proti tagging útokům.

7. **Pokud má hašovací funkce vlastnost silné bezkoliznosti, znamená to, že:**
Nelze nalézt dva navzájem různé vstupy takové, aby byly výsledné haše pro oba vstupy stejné na alespoň 1/2 pozic.
*Je výpočetně neproveditelné nalézt dva libovolné navzájem různé vstupy takové, aby byly výsledné haše pro oba vstupy stejné.
Je výpočetně neproveditelné nalézt k danému vstupu jiný vstup tak, aby byly výsledné haše pro oba vstupy stejné.
Nelze nalézt dva navzájem různé vstupy takové, aby byly výsledné haše pro oba vstupy stejné.

8. **Bezpečnostní politika zahrnuje**
Seznam konkrétních osob, které mají povoleno přistupovat k citlivým datům společnosti
Specifikaci technologických opatření kterými budou prosazovány bezpečnostní požadavky společnosti
*Požadavky, pravidla a postupy určující způsob ochrany a zacházení s hodnotami společnosti

9. **V případě nepozorovatelnosti (unobservability) je ochraňovanou hodnotou?**
Informace o aplikovaných bezpečnostních opatřeních systému (např. nastavení pravidel firewallu)
Informace o přihlášených uživatelích
Informace o překročení přiděleného procesorového času pro použití nabízených zdrojů a služeb
*Informace o použití zdrojů a služeb

10. **Existuje nějaký útok na službu TOR, který sníží anonymitu uživatelů?**
Ano, existuje útok, který stoprocentně "odanonymizuje" všechny uživatele.
Ne, TOR je navržen tak, aby odolal všem známým i neznámým typům útoků.
*Ano, existuje útok, který může snížit anonymitu uživatelů.
Ne, žádný takový útok zatím není znám.

11. **Co je to perturbační technika používaná ve statistických databázích?**
Žádná taková technika neexistuje.
Pro vyhodnocení dotazu nesmí být použito více záznamu než je stanovená maximální (perturbační) mez.
Pro vyhodnocení dotazu může být použito pouze menší množství záznamů než je stanovená maximální (perturbační) mez.
*Technika stavějící např. na zaokrouhlování mezivýsledků dotazů.
*Technika umožňující zjistit konzistentní, ale ne spolehlivé odpovědi na sérii podobných dotazů.
*Přidávání pseudonáhodného "šumu" k množině záznamů, na jejichž základě se vyhodnotí dotaz.

12. **Anonymita (podle Společných kritérií) zajišťuje možnost použití zdrojů nebo služeb systému tak, že:**
*identita uživatele zůstane skryta
identita uživatele zůstane skryta, ale v případě potřeby ji lze zpětně zjistit
*identita uživatele zůstane skryta specifickým uživatelům, pro specifické operace
specifikované entity jsou schopny určit skutečné uživatelské jméno spojené se specifikovanými subjekty, operacemi, objekty

13. **Autentizace protokolem s nulovým rozšířením znalostí (zero-knowledge)**
zabrání prokazující se straně, aby se dozvěděla, jak zní tajemství, které vlastní ověřovatel
zabrání ověřovateli, aby se zároveň autentizoval prokazující se straně
sdělí ověřovateli pouze počet nul v tajném klíči prokazující se strany
*zabrání ověřovateli, aby se mohl později neoprávněně vydávat za prokazující se stranu
*zabrání ověřovateli, aby se dozvěděl tajemství, které vlastní prokazující se strana

14. **Která z následujících tvrzení platí:**
silná integrita zaručuje důvěrnost.
prokazatelná zodpovědnost vyžaduje důvěrnost.
důvěrnost zaručuje integritu.
*neplatí ani jedno tvrzení.
integrita zaručuje důvěrnost.

15. **Která z těchto tvrzení jsou správná?**
Se zvýšením FAR se zvyšuje FRR.
Se snížením FAR se snižuje FRR.
*Se zvýšením FAR (False Acceptance Rate) se snižuje FRR (False Reject Rate).
*Se snížením FAR se zvyšuje FRR.

16. **Autentizace je**
proces nezbytný pro ustavení šifrované komunikace u bezdrátového spojení
*všechny ostatní možnosti jsou nepravdivé
překlep - správně je "autorizace"
volitelná (ale obvykle přítomná) fáze procesu prokazování identity

17. **Systém detekce průniku (IDS)**
poskytuje lepší ochranu než firewall
je možné použít buď v síti nebo na počítači
*je možné použít v síti i na počítači
má smysl používat pouze jako síťový prvek, kdy detekuje a informuje o probíhajícím útoku

18. **PGP umožňuje nastavit úroveň důvěry pro konkrétní veřejný klíč. Toto nastavení se používá pro:**
indikaci důvěry v původ dat podepsaných daným veřeným klíčem.
*indikaci důvěry v původ dat podepsaných vlastníkem odpovídajícího privátního klíče.
kontrolu skupiny lidí, které může být distribuován náš veřejný klíč.
indikaci důvěry v klíč na základě jeho bitové velikosti.
filtrování zpráv, které mohou být poslány danému uživateli.

19. **Pokud neautorizovaná osoba zjistí sémantický obsahu chráněných dat, jedná se o narušení**
*důvěrnosti
integrity
dostupnosti
prokazatelné zodpovědnosti