Záróvizsga tematika

Mérnökinformatikus alapképzési szak BSc F tanterv

Specializáció: **Felhő szolgáltatási és IT biztonság** *(Hálózati technológiák, Számítógéphálózatok és felhők biztonsága, Informatikai rendszerek és szolgáltatások biztonsága, Felhő szolgáltatások, Virtuális hálózatok és adatközpontok technológiái)*

1. **Fizikai közeg kiválasztása:** Hasonlítsa össze a sodrott réz érpár és az optikai szál alkalmazását! Mutassa be a csillapítás, az áthallás és az optikai veszteség gyakorlati jelentőségét! Indokolja a közegválasztást a távolság, a kapacitás és a környezet alapján! *Fő technológiák és fogalmak: Twisted pair, optical fiber, attenuation, crosstalk*
   A felhő működési modellje és alkalmazhatósága: Ismertesse a felhő öt alapvető jellemzőjét: az igény szerinti önkiszolgálást, a széles körű hálózati hozzáférést, az erőforrás-megosztást, a gyors rugalmasságot és a mért szolgáltatást! Különítse el a felhőt a puszta virtualizációtól vagy távoli szerverüzemeltetéstől! Mutassa be, milyen igények mellett jelent előnyt vagy hátrányt a felhő alkalmazása! *Fő technológiák és fogalmak: On-demand self-service, broad network access, resource pooling, rapid elasticity, measured service*
2. **Jelátvitel és hibadetektálás:** Különítse el a vonalkódolás, a moduláció és a hibadetektálás feladatát! A Manchester vagy PAM példáján ismertesse a bitek fizikai jelekké alakításának elvét! Mutassa be az Ethernet FCS szerepét, és különítse el a véletlen hibák felismerését a biztonsági integritásvédelemtől! *Fő technológiák és fogalmak: Line coding, modulation, Manchester/PAM, FCS*
   Virtuális gépek és konténerek összehasonlítása: Mutassa be a virtuális gépek és konténerek felépítését, izolációját és erőforrás-kezelését! Hasonlítsa össze a hypervisorra és a közös kernelre épülő működést! Indokolja a futtatási környezet kiválasztását az alkalmazás követelményei és az üzemeltetési ráfordítás alapján! *Fő technológiák és fogalmak: VM, hypervisor, guest OS, container*
3. **Címek szerepe a hálózati kommunikációban:** Mutassa be az adatkapcsolati címzés (MAC), az IP-címzés és a portszámok eltérő feladatát! Egy távoli szolgáltatás elérésénél szemléltesse, hogyan kapcsolódnak ezek a címek a beágyazáshoz, és melyek változnak a továbbítás során! *Fő technológiák és fogalmak: Ethernet, MAC, IP, ports, encapsulation*
   Identitás és hozzáférés-kezelés: Különítse el az azonosítást, a hitelesítést és a jogosultságellenőrzést! Mutassa be az MFA, a szerepkörök és a legkisebb jogosultság elvének szerepét az IAM-ban! Egy felhőszolgáltatás példáján ismertesse a felhasználói és szolgáltatásidentitás különbségét! *Fő technológiák és fogalmak: IAM, authentication, authorization, MFA, RBAC*
4. **Ethernet-keretek és kapcsolási technikák:** Mutassa be az Ethernet-keret fő mezőit és a MAC-cím felépítését! Hasonlítsa össze a store-and-forward és a cut-through továbbítást az FCS-ellenőrzés és a késleltetés szempontjából! Különítse el a keret hibadetektálását a hibás adat újraküldésétől! *Fő technológiák és fogalmak: Ethernet frame, MAC address, FCS, store-and-forward, cut-through*
   Felhőalapú tárolási megoldások kiválasztása: Hasonlítsa össze a blokk-, fájl- és objektumtárolás hozzáférési módját és felhasználási területeit! Mutassa be, hogyan befolyásolja a választást a teljesítményigény, a hozzáférési gyakoriság és a költség! Indokoljon tárolási megoldást egy választott alkalmazási példára! *Fő technológiák és fogalmak: Block/file/object storage, performance, access frequency, cost*

5. **Kapcsolók tanulása és kerettovábbítása:** Mutassa be a kapcsoló MAC-címtanulását és a kapcsolási tábla használatát! Egyszerű példán hasonlítsa össze az ismert és ismeretlen unicast, valamint a broadcast továbbítását! Ismertesse egy állomás áthelyezésének hatását a tanult címekre! *Fő technológiák és fogalmak: MAC address table, learning, forwarding, flooding, aging*
   Felhőszolgáltatási modellek és felelősségi határok: Hasonlítsa össze az IaaS, a PaaS és a SaaS modellt a szolgáltató és az ügyfél feladatai alapján! Mutassa be a szükséges kontroll, a rendelkezésre álló szakértelem és az üzemeltetési teher hatását a választásra! Ismertesse a megosztott felelősség elvét egy választott szolgáltatás példáján! *Fő technológiák és fogalmak: IaaS, PaaS, SaaS, shared responsibility model*
6. **VLAN-ok és hálózati elkülönítés:** Mutassa be a VLAN-ok szerepét, az access és trunk kapcsolatok, valamint a tagging és a native VLAN működését az IEEE 802.1Q példáján! Egyszerű ábrán szemléltesse a VLAN-ok közötti routingot! Különítse el a VLAN-elkülönítést a hozzáférési jogosultságtól! *Fő technológiák és fogalmak: VLAN, access/trunk, IEEE 802.1Q, tagging, native VLAN, inter-VLAN routing*
   Virtuális hálózatok és alhálózatok a felhőben: Mutassa be a virtuális hálózatok, alhálózatok és útvonaltáblák szerepét! Különítse el a publikus és privát elérhetőséget, és ismertesse a kimenő internetelérés lehetőségeit! Egyszerű ábrán mutassa be egy publikus alkalmazáskomponens és egy privát adatbázis hálózati kapcsolatát! *Fő technológiák és fogalmak: Virtual network, subnet, route table, public/private reachability*
7. **Redundáns kapcsolt hálózatok:** Mutassa be a redundáns Ethernet-kapcsolatok hurokproblémáját és az STP hurokmentes aktív topológiáját! Egyszerű ábrán szemléltesse egy kapcsolat kiesésének hatását és az RSTP célját! Különítse el az L2 hurokmegelőzést az L3 csomagok TTL/Hop Limit szerinti korlátozásától! *Fő technológiák és fogalmak: STP/RSTP, BPDU, root bridge, port roles*
   Tanúsítványok és bizalom: Mutassa be a digitális tanúsítvány, a hitelesítésszolgáltató és a bizalmi lánc fogalmát! Ismertesse a tanúsítvány ellenőrzésének célját és a hibás ellenőrzés következményét! Különítse el a titkosított kapcsolatot a megfelelően hitelesített végponttal létrehozott kapcsolattól! *Fő technológiák és fogalmak: Certificate, CA, chain of trust, validation*
8. **Linkaggregáció és kapacitás:** Mutassa be a linkaggregáció és az LACP működési elvét! Különítse el az összesített kapacitást egyetlen adatfolyam sebességétől! Egyszerű példán ismertesse egy tagkapcsolat kiesésének hatását, és röviden hasonlítsa össze a Layer 2 és Layer 3 aggregált interfész használatát! *Fő technológiák és fogalmak: LAG, LACP, port-channel, Layer 2/Layer 3*
   Többrétegű alkalmazás felhőarchitektúrája: Mutassa be a megjelenítési, alkalmazási és adatréteg feladatát és kapcsolatait! Ismertesse az egyes komponensek önálló méretezésének és elkülönítésének előnyeit! Egyszerű ábrán szemléltesse az adat útját és a rétegek közötti szükséges hozzáféréseket! Indokolja a menedzselt vagy saját üzemeltetésű komponensek választását! *Fő technológiák és fogalmak: Multi-tier architecture, presentation/application/data tier, managed/self-managed service*
9. **Az alapértelmezett átjáró redundanciája:** Mutassa be az első ugrás redundanciáját a HSRP példáján! Ismertesse a virtuális címek és az aktív/tartalék szerep feladatát! Egy kiesési példán mutassa be a prioritás, a preempt és a tracking szerepét, különítve az átjáróhibát a külső kapcsolat hibájától! *Fő technológiák és fogalmak: HSRP, virtual IP/MAC, active/standby, preempt, tracking*
   Terheléselosztás és állapotellenőrzés: Mutassa be a terheléselosztó szerepét és a hálózati, illetve alkalmazási szintű elosztás különbségét! Ismertesse az

állapotellenőrzés és a munkamenet-kezelés jelentőségét! Mutassa be, mi történik egy alkalmazáspéldány kiesésekor, és milyen feltételekkel maradhat használható a szolgáltatás! *Fő technológiák és fogalmak: Load balancing, network/application layer, health check, session management*

10. **IPv4-alhálózatok kialakítása:** Mutassa be az IPv4-cím, a maszk és a prefix szerepét! Egy több szervezeti egységből álló telephely példáján indokolja az alhálózatok méretezését és a bővítési tartalékot! Különítse el a helyi és távoli célhoz történő továbbítást! *Fő technológiák és fogalmak: IPv4, subnetting, CIDR, default gateway*
    Régiók, rendelkezésre állási zónák és hibatartományok: Ismertesse a régió és a rendelkezésre állási zóna szerepét! Mutassa be, milyen hibák ellen véd a többzónás vagy többrégiós kialakítás, és mely függőségek maradhatnak közösek! Indokolja az elhelyezést a késleltetés, rendelkezésre állás és költség alapján! *Fő technológiák és fogalmak: Region, availability zone, failure domain, multi-zone/multi-region*
11. **IPv6-címek és helyi elérhetőség:** Mutassa be az IPv6-cím felépítését és a globális, link-local és ULA címek szerepét! Hasonlítsa össze az IPv4 ARP és az IPv6 szomszédfelderítés feladatát! Egyszerű példán különítse el a helyi szomszéd és a távoli hálózat elérését! *Fő technológiák és fogalmak: IPv6, global unicast, link-local, ULA, ARP, Neighbor Discovery*
    Mentések védelme és helyreállíthatósága: Mutassa be a mentések elkülönítésének és hozzáférés-védelmének célját! Ismertesse az offline vagy módosíthatatlan példányok szerepét a közös hibák és támadások ellen! Mutassa be, hogyan ellenőrizné a tényleges visszaállíthatóságot! *Fő technológiák és fogalmak: Backup isolation, offline/immutable backup, restore test*
12. **Címtervezés és útvonal-összegzés:** Ismertesse az IPv4-alhálózatokra bontás és az útvonal-összegzés kapcsolatát! Egyszerű példán mutassa be, hogyan hirdethetők több alhálózat útvonalai egy közös prefixszel, és mi a túl tág összegzés kockázata! Röviden térjen ki az IPv6-címtervezés eltérő szempontjaira! *Fő technológiák és fogalmak: IPv4, subnetting, CIDR, route summarization, IPv6*
    Felhő-erőforrások szervezése és governance: Mutassa be az erőforrások szervezeti és környezeti elkülönítésének célját! Ismertesse a névkonvenciók, címkék, szabályzatok és kvóták szerepét! Mutassa be, hogyan támogatják ezek a felelősségek tisztázását, az ellenőrizhetőséget és a költségek hozzárendelését! *Fő technológiák és fogalmak: Governance, naming convention, tags, policies*
13. **Automatikus hálózati konfiguráció:** Vezesse végig a DHCPv4 kezdeti címkiosztását egy cím nélküli kliens esetén! Ismertesse a broadcast/unicast, a DHCP-relay és a bérletmegújítás szerepét! Röviden hasonlítsa össze ezt az IPv6 RA/SLAAC és DHCPv6 megoldásával, az átjáró megismerésére is kitérve! *Fő technológiák és fogalmak: DHCPv4, DORA, DHCP-relay, lease, IPv6 RA/SLAAC, DHCPv6*
    Helyi, publikus és hibrid infrastruktúra összehasonlítása: Hasonlítsa össze a helyi, publikus felhős és hibrid elhelyezést! Mutassa be a kontroll, az integráció, a késleltetés és az üzemeltetési felelősség szempontjait! Indokolja az elhelyezési döntést egy alkalmazás adatkezelési és üzleti követelményei alapján! *Fő technológiák és fogalmak: On-premises, public cloud, hybrid infrastructure, responsibility boundary*
14. **Névfeloldás és szolgáltatáselérés:** Mutassa be a DNS hierarchiáját, a rekurzív és autoritatív kiszolgálók szerepét! Egyszerű lekérdezésen ismertesse a gyorsítótárazás és a DNS TTL jelentőségét! Különítse el a sikeres névfeloldást a szolgáltatás tényleges elérhetőségétől! *Fő technológiák és fogalmak: DNS, recursive resolver, authoritative server, caching, TTL*

Alkalmazások felhőbe költöztetése: Mutassa be a meglévő alkalmazás felhőbeli futtatási környezetének kiválasztási szempontjait és a szükséges alkalmazásváltoztatások szerepét! Ismertesse a függőségek, az adatmozgatás és a kiesési idő jelentőségét! Térjen ki a tesztelésre, a visszaállítási tervre és az átállás utáni működési és biztonsági ellenőrzésre! Indokolja a migrációs megoldást a várható előnyök, a kockázat és a ráfordítás alapján! *Fő technológiák és fogalmak: Workload, runtime/platform selection, application dependencies, data migration*

15. **Routing tábla és csomagtovábbítás:** Ismertesse a közvetlen, statikus és dinamikusan tanult útvonalak fogalmát és szerepét! Különítse el az adminisztratív távolság és a metrika szerinti útvonalválasztást a longest prefix match működésétől! Egyszerű routing tábla alapján vezesse le a következő ugrás és a kimenő interfész meghatározását! *Fő technológiák és fogalmak: Routing table, administrative distance, metric, longest prefix match*
    Támadási felület és rendszermegerősítés: Mutassa be a támadási felület és a hardening kapcsolatát! Ismertesse a szükségtelen szolgáltatások és jogosultságok csökkentésének szerepét! Egyszerű rendszerpéldán mutassa be, hogyan egészítik ki egymást a megelőző, észlelő és korlátozó intézkedések! *Fő technológiák és fogalmak: Attack surface, hardening, least privilege, defense in depth*
16. **Távolságvektoros útvonalválasztás:** Mutassa be a distance-vector útvonalválasztás információcseréjét a RIP példáján! Ismertesse a metrika és a frissítések szerepét! Egyszerű hálózaton vezesse le, hogyan ismernek meg a routerek egy új célhálózatot, és mutassa be a megközelítés fő korlátait! *Fő technológiák és fogalmak: RIP, distance-vector routing, metric, route update*
    Publikus és privát szolgáltatáselérés a felhőben: Mutassa be a publikus végpont és a privát szolgáltatáselérés különbségét! Ismertesse a kimenő kapcsolat, a bejövő közzététel és a névfeloldás szerepét! Egyszerű ábrán indokolja, mely komponensek legyenek közvetlenül elérhetők, és hol lehet szükség köztes proxyra! Magyarázza el, hogyan egészíti ki egymást a hálózati szűrés és a hitelesítés a szolgáltatás védelmében! *Fő technológiák és fogalmak: Public endpoint, private access, inbound/outbound connectivity, DNS*
17. **Útvonalválasztási hurkok és konvergencia:** Mutassa be, hogyan alakulhat ki routinghurok késve frissülő útvonalinformációból! A RIP példáján ismertesse a split horizon és a route poisoning szerepét! Hasonlítsa össze az L3 hurokkezelést az L2 STP-megoldásával, és ismertesse a TTL/Hop Limit korlátját! *Fő technológiák és fogalmak: Routing loop, RIP, split horizon, route poisoning, TTL/Hop Limit*
    Automatizált erőforrás-létrehozás és infrastruktúra mint kód: Mutassa be a kézi és deklaratív erőforrás-kezelés különbségét! Ismertesse az ismételhetőség, a verziókezelés és a konfigurációeltérés jelentőségét! Magyarázza el, hogyan támogatja az infrastruktúra mint kód a jóváhagyott biztonságos alapkonfiguráció következetes alkalmazását és ellenőrzését! Mutassa be az automatizálás előnyeit és kockázatait több környezet egységes kialakításakor! *Fő technológiák és fogalmak: Infrastructure as Code/IaC, declarative configuration, version control, configuration drift*
18. **Link-state útvonalválasztás:** Mutassa be a link-state útvonalválasztás működését az OSPF példáján! Ismertesse az LSDB és az SPF-számítás szerepét! Egyszerű hálózaton vezesse végig a cost alapján történő útvonalválasztást és egy kapcsolat kiesésének hatását! *Fő technológiák és fogalmak: OSPF, LSDB, SPF, cost, convergence*
    Felhőalapú adatbázisok és menedzselt szolgáltatások: Hasonlítsa össze a saját üzemeltetésű és menedzselt adatbázist! Ismertesse a relációs és nem relációs

megoldások választási szempontjait az adatmodell és a hozzáférési igény alapján! Mutassa be a rendelkezésre állás, a mentés és az üzemeltetési felelősség jelentőségét! Térjen ki a hozzáférés-szabályozás, valamint a tárolás és továbbítás közbeni titkosítás szerepére az adatok védelmében! *Fő technológiák és fogalmak: Self-managed/managed database, relational/non-relational database, backup, availability*

19. **Szomszédság és adatbázis-szinkronizáció:** Mutassa be, hogyan alakítanak ki az OSPF-routerek szomszédkapcsolatot és egyeztetik topológiai adatbázisukat! Vezesse végig a szomszédság és az adatbázis-szinkronizáció fő lépéseit! Röviden magyarázza meg a DR/BDR szerepét közös Ethernet-hálózaton! *Fő technológiák és fogalmak: OSPF, Hello, adjacency, LSDB synchronization, DR/BDR*
    Sérülékenységek és javításuk priorizálása: Ismertesse a CVE és a CVSS szerepét! Különítse el a technikai súlyosságot a tényleges kockázattól! Egy példán indokolja a javítás sorrendjét a kitettség és az üzleti hatás alapján, és mutassa be az eredmény ellenőrzésének célját! *Fő technológiák és fogalmak: CVE, CVSS, exposure, patching, risk*
20. **Hierarchikus útvonalválasztás:** Mutassa be, miért osztjuk area-kra az OSPF-hálózatot, és mi az Area 0 és az ABR szerepe! Különítse el a saját terület topológiáját a más területekről kapott elérhetőségi információtól! Röviden hasonlítsa össze a normál, stub és NSSA területek információigényét és külső útvonalkezelését! *Fő technológiák és fogalmak: OSPF areas, backbone, ABR, normal/stub/NSSA*
    Számítási kapacitás méretezése és skálázása: Hasonlítsa össze a vertikális és horizontális skálázást! Mutassa be a kapacitás, a terhelés és a válaszidő kapcsolatát! Ismertesse az automatikus skálázás működési elvét és korlátait, valamint az alul- és túlméretezés költség- és szolgáltatási hatását! *Fő technológiák és fogalmak: Scale up/down, scale out/in, autoscaling, capacity*
21. **Redisztribúció és külső útvonalak:** Ismertesse a redisztribúció fogalmát és célját különböző útvonalforrások között! Az OSPF példáján mutassa be az ASBR szerepét és a külső prefix hirdetését! Ismertesse a visszahirdetés kockázatát és a szűrés szerepét! *Fő technológiák és fogalmak: Redistribution, OSPF, ASBR, external route, route filtering*
    Alkalmazásállapot és többpéldányos működés: Különítse el az állapottartó és állapot nélküli alkalmazáskomponenseket! Mutassa be a munkamenet, a közös adattárolás és a gyorsítótár szerepét többpéldányos működésnél! Ismertesse az állapotkezelés hatását a skálázásra és a példányok cseréjére! *Fő technológiák és fogalmak: Stateful/stateless application, session state, shared storage, cache*
22. **A BGP szerepe és az útvonalak megosztása:** Ismertesse a BGP célját és prefixhirdetésének elvét! Mutassa be az eBGP és az iBGP szerepét, a NEXT_HOP és a belső routing kapcsolatát! Hasonlítsa össze a default route és a részletes BGP-útvonalak alkalmazását; röviden térjen ki a route reflector céljára! *Fő technológiák és fogalmak: Default route, eBGP/iBGP, NEXT_HOP, route reflector*
    Eseményvezérelt és aszinkron alkalmazásműködés: Mutassa be a közvetlen szinkron hívás és az üzenetközvetítőn keresztüli kommunikáció különbségét! Ismertesse a sor és a publikálás-feliratkozás modell szerepét! Mutassa be a terhelési csúcsok, az ismételt feldolgozás és a komponenshibák kezelésének szempontjait! *Fő technológiák és fogalmak: Synchronous/asynchronous communication, message broker, queue, publish/subscribe*
23. **BGP-útvonalválasztás és routingpolitika:** Mutassa be a BGP routingpolitika és az útvonal-attribútumok szerepét! Egy kétkijáratos példán vezesse végig a választást a LOCAL_PREF és az AS_PATH alapján! Ismertesse a NEXT_HOP elérhetőségének

feltételét és a routingpolitika eltérését a pusztán legrövidebb út keresésétől! *Fő technológiák és fogalmak: BGP, LOCAL_PREF, AS_PATH, NEXT_HOP*

Biztonsági események és kezdeti reagálás: Különítse el a biztonsági eseményt és az incidenst! Mutassa be a naplók és riasztások szerepét az észlelésben! Egyszerű esetben indokolja az elkülönítés, a bizonyítékmegőrzés és a szolgáltatás helyreállításának fő szempontjait! *Fő technológiák és fogalmak: Security event/incident, logging, detection, containment*

24. **MPLS és címkealapú továbbítás:** Mutassa be az MPLS működési elvét és kapcsolatát az IP-routinggal! Egyszerű szolgáltatói hálózaton szemléltesse a címkék használatát a csomag továbbítása során! Ismertesse a forgalomelkülönítés szerepét, és különítse el azt a titkosítástól! *Fő technológiák és fogalmak: MPLS, label switching, push/swap/pop, traffic isolation*

    Felhőszolgáltatások összekapcsolása és függőségei: Mutassa be az alkalmazás és a menedzselt szolgáltatások közötti függőségeket! Ismertesse az időkorlátok, újrapróbálkozások és hibaterjedés szerepét! Egyszerű szolgáltatási ábrán mutassa be, hogyan korlátozható egy függő komponens hibájának hatása! *Fő technológiák és fogalmak: Service dependencies, timeout, retry, failure propagation*

25. **Címfordítás és elérhetőség:** Mutassa be az IPv4 NAT/PAT működését és a fordítási tábla szerepét a visszirányú forgalomban! Egyszerű példán vezesse végig a címek és portok változását! Különítse el a címfordítást a hozzáférési védelemtől, és röviden térjen ki az IPv6 NAT nélküli elérésére! *Fő technológiák és fogalmak: NAT, PAT, translation table, inbound access*

    Felhőköltségek és fogyasztásalapú működés: Mutassa be a számítási, tárolási és adatforgalmi költségek fő tényezőit! Ismertesse a kihasználtság, a kapacitásvállalás és a rugalmas fogyasztás közötti kompromisszumokat! Mutassa be a költségek hozzárendelésének, a kereteknek és a költségriasztásoknak a szerepét! *Fő technológiák és fogalmak: Compute/storage/data transfer costs, utilization, commitment, cost allocation*

26. **TCP-kapcsolatok létrehozása és lezárása:** Vezesse végig a TCP háromutas kézfogását és szabályos lezárását a jelzőbitek, sorszámok és nyugták szerepével! Röviden ismertesse az RST jelentőségét! Különítse el a kapcsolat létrejöttét az alkalmazási kérés sikerétől! *Fő technológiák és fogalmak: TCP, SYN/ACK/FIN/RST, sequence/acknowledgement numbers*

    Erőforrások életciklusa és környezetek elkülönítése: Mutassa be a fejlesztési, teszt- és éles környezet elkülönítésének célját! Ismertesse az erőforrások létrehozásának, módosításának és megszüntetésének szempontjait! Mutassa be az elfelejtett erőforrások költség- és biztonsági hatását! *Fő technológiák és fogalmak: Development/test/production, resource lifecycle, decommissioning*

27. **Megbízható adatátvitel és adatvesztés:** Mutassa be a TCP sorszámozásának, nyugtázásának és újraküldésének szerepét! Egyszerű üzenetváltáson szemléltesse egy elveszett adat helyreállítását! Hasonlítsa össze ezt az UDP szolgáltatásával és az alkalmazásra háruló feladatokkal! *Fő technológiák és fogalmak: TCP/UDP, acknowledgement, retransmission, reliability*

    Zero Trust és hozzáférési döntések: Ismertesse a Zero Trust alapelveit! Mutassa be az identitás, az eszközállapot és a legkisebb jogosultság szerepét egy erőforrás elérésében! Különítse el a hozzáférés célzott ellenőrzését a pusztán belső hálózati jelenléten alapuló bizalomtól! *Fő technológiák és fogalmak: Zero Trust, identity, device posture, least privilege*

28. **Áramlásszabályozás és torlódás:** Különítse el a fogadó kapacitásának védelmét a hálózati torlódás kezelésétől! Mutassa be a TCP fogadói és torlódási ablakának szerepét! Egyszerű példán indokolja, miért nem határozza meg önmagában a névleges linksebesség a tényleges átvitelt! *Fő technológiák és fogalmak: TCP, receive window, congestion window, latency*
    Konténeres alkalmazások életciklusa: Mutassa be a konténerkép és a futó konténer különbségét! Ismertesse a telepítés, a frissítés, az állapotellenőrzés és a példánycsere szerepét! Mutassa be a tartós adatok és a konfiguráció elkülönítésének jelentőségét! *Fő technológiák és fogalmak: Container image, running container, deployment, health check*
29. **MTU és csomagméret alagutakban:** Mutassa be az MTU és a TCP MSS kapcsolatát! Ismertesse az alagút többletfejlécének hatását a csomagméretre! Mutassa be az IPv4 töredezés és a Path MTU Discovery szerepét, rövid IPv6-összehasonlítással! *Fő technológiák és fogalmak: MTU, MSS, tunneling, fragmentation, PMTUD*
    Monitoring és szolgáltatási állapot: Mutassa be az infrastruktúra-metrikák és az alkalmazási állapotellenőrzések különbségét! Ismertesse a naplók, metrikák és elosztott nyomkövetés szerepét, valamint a naplóadatok összekapcsolásának és védelmének jelentőségét! Magyarázza el, hogyan állapítható meg, hogy egy szolgáltatás a felhasználó számára valóban működik-e! Térjen ki arra, miért nem jelent minden riasztás tényleges hibát vagy biztonsági incidenst! *Fő technológiák és fogalmak: Metrics, logs, distributed tracing, application health check*
30. **ACL-ek kiértékelési logikája:** Mutassa be a címek, protokollok és portok alapján történő csomagszűrést! Ismertesse a szabálysorrend, a first match és az implicit deny működését! Egyszerű kliens–szerver igényből vezessen le engedélyező és tiltó szabályokat, a visszirányú forgalommal együtt! *Fő technológiák és fogalmak: ACL, address/port matching, first match, permit/deny*
    Hibrid hálózati összeköttetések: Hasonlítsa össze az interneten kialakított VPN és a dedikált kapcsolat szerepét! Mutassa be a címzés, az útvonalválasztás és a névfeloldás összhangjának szükségességét! Indokolja a kapcsolatválasztást a késleltetés, a kapacitás, a rendelkezésre állás és a költség alapján! *Fő technológiák és fogalmak: VPN, dedicated connection, addressing, routing*
31. **Állapottartó tűzfal és proxy:** Hasonlítsa össze a stateless szűrés, a stateful tűzfal és az alkalmazási proxy működését! Egy kliens–szerver példán mutassa be a kapcsolatállapot és a visszirányú forgalom kezelését! Ismertesse az aszimmetrikus útvonal következményét! *Fő technológiák és fogalmak: Stateful/stateless filtering, proxy, connection state, asymmetric routing*
    Webalkalmazások biztonsági alapjai: Mutassa be a hibás bemenetkezelés és hozzáférés-ellenőrzés kockázatait! Egyszerű példán ismertesse az alkalmazási védelem és a hálózati szűrés eltérő szerepét! Ismertesse az OWASP szerepét az alkalmazásbiztonsági kockázatok rendszerezésében! *Fő technológiák és fogalmak: Input validation, access control, OWASP, application security*
32. **Védett hálózati összeköttetések:** Hasonlítsa össze a site-to-site és a remote-access VPN felépítését! Egyszerű ábrán mutassa be az alagút belső és külső forgalmát! Ismertesse a hitelesítés, titkosítás és integritásvédelem szerepét az IPsec vagy TLS-alapú megoldás példáján! *Fő technológiák és fogalmak: VPN, tunneling, IPsec/TLS, authentication, encryption*
    Felhőalapú alkalmazáselérés és késleltetés: Mutassa be a hálózati távolság és a késleltetés hatását a felhőalkalmazások használatára! Ismertesse a gyorsítótárazás és a tartalomelosztás szerepét! Különítse el a statikus tartalom gyorsítását az alkalmazási

és adatbázis-műveletek késleltetésének csökkentésétől! *Fő technológiák és fogalmak: Latency, caching, content distribution/CDN, static content*

33. **Wi-Fi-csatornák és átviteli minőség:** Mutassa be a csatornaválasztás, csatornaszélesség és interferencia hatását a Wi-Fi működésére! Ismertesse az OFDM-alvivők és a QAM szerepét működési elv szintjén! Indokolja a sebesség és a jelminőség közötti kompromisszumot! *Fő technológiák és fogalmak: Wi-Fi, channel overlap, OFDM, QAM, SNR*

    Virtualizált erőforrások és teljesítmény: Mutassa be a fizikai és virtuális erőforrások kapcsolatát! Ismertesse az erőforrás-megosztás, a túlzott konszolidáció és az erőforrás-verseny hatását! Mutassa be, hogyan különíthető el az alkalmazás hibája a futtatókörnyezet kapacitásproblémájától! *Fő technológiák és fogalmak: Virtual/physical resources, resource sharing, excessive consolidation, resource contention*
34. **Vezeték nélküli közeg-hozzáférés:** Mutassa be a CSMA/CA működését és a visszaigazolás, illetve újraküldés szerepét! Hasonlítsa össze a vezetékes és vezeték nélküli közeg használatát! Egyszerű példán ismertesse a megosztott rádiós kapacitás és a rejtett állomás problémáját! *Fő technológiák és fogalmak: Wi-Fi, CSMA/CA, ACK, retransmission, hidden node*

    Felhőbeli hálózati hozzáférés-szabályozás: Mutassa be az alhálózati és erőforráshoz rendelt forgalomszabályok eltérő hatókörét! Ismertesse az útvonaltábla és a hozzáférési szabály együttműködését! Egyszerű ábrán mutassa be, mi szükséges egy alkalmazás és adatbázis közötti kapcsolat engedélyezéséhez! Indokolja, hogyan ellenőrizné, hogy az engedélyezett kapcsolat működik, a nem engedélyezett hozzáférés pedig tiltott! *Fő technológiák és fogalmak: Subnet/resource-level rules, route table, access rule*
35. **Wi-Fi-csatlakozás és védelem:** Mutassa be a kliens és az access point közötti kapcsolat kialakulásának fő lépéseit! Hasonlítsa össze a Personal és Enterprise hozzáférést a WPA2/WPA3 példáján! Ismertesse az IEEE 802.1X és a RADIUS szerepét a vállalati hitelesítésben! *Fő technológiák és fogalmak: Association, WPA2/WPA3, Personal/Enterprise, 802.1X, RADIUS*

    Konténerek biztonsági határai: Mutassa be a konténeres izoláció lehetőségeit és korlátait! Ismertesse a megbízható képek, a minimális jogosultság és a gazdarendszer védelmének szerepét! Különítse el a csomagolhatóságot a biztonságosságtól! *Fő technológiák és fogalmak: Container isolation, trusted image, least privilege, host security*
36. **Biztonsági célok és kockázatalapú védelem:** Mutassa be a bizalmasság, a sértetlenség és a rendelkezésre állás jelentését! Különítse el a védendő értéket, a fenyegetést, a sérülékenységet és a kockázatot! Egyszerű szolgáltatási példán indokoljon védelmi intézkedést az üzleti hatás és a fennmaradó kockázat alapján! *Fő technológiák és fogalmak: CIA, asset, threat, vulnerability, risk*

    Alkalmazásfrissítés és szolgáltatásfolytonosság: Mutassa be az alkalmazás telepítésének és frissítésének szerepét, valamint a szolgáltató és az ügyfél felelősségi határait! Ismertesse az állapotellenőrzés és a visszaállítás szerepét! Mutassa be az alkalmazásverzió, a függőségek és a konfiguráció kezelésének jelentőségét a szolgáltatás működésében! *Fő technológiák és fogalmak: Deployment, application update, responsibility boundary, health check*
37. **Kriptográfiai mechanizmusok szerepe:** Hasonlítsa össze a szimmetrikus és aszimmetrikus titkosítás, a hash és a digitális aláírás célját! Egyszerű példán mutassa be, melyik milyen biztonsági tulajdonságot támogat! Ismertesse a kulcsok védelmének

jelentőségét! *Fő technológiák és fogalmak: Symmetric/asymmetric encryption, hash, digital signature*

Elosztott felhőszolgáltatás hibakeresése: Mutassa be az alkalmazás, a hálózat és a menedzselt szolgáltatások hibáinak elkülönítését! Ismertesse a metrikák, naplók és nyomkövetési adatok együttes használatát! Egy lassú vagy időszakosan hibás szolgáltatás példáján indokolja a vizsgálat lépéseit és hatókörét! Magyarázza el, hogyan ellenőrizné a javítás eredményét és azt, hogy a szükséges védelmi beállítások változatlanul érvényesülnek! *Fő technológiák és fogalmak: Metrics, logs, traces, application/network/service troubleshooting*

38. **Hálózati hibák szisztematikus vizsgálata:** Egy kliens IP-címmel rendelkezik, de egy távoli webszolgáltatást nem ér el. Mutassa be a hibakeresés logikáját, a választott vizsgálatok eredményeinek értelmezésével! Különítse el a hálózati, szállítási és alkalmazási hibákat, valamint a sikeres elérhetőségi tesztet a működő szolgáltatástól! *Fő technológiák és fogalmak: TCP/IP, DNS, ICMP, TCP, ACL/firewall*

    Magas rendelkezésre állás és katasztrófa utáni helyreállítás: Különítse el a magas rendelkezésre állás és a katasztrófa utáni helyreállítás célját! Mutassa be a zónák, régiók és közös függőségek szerepét! Ismertesse az RPO és az RTO jelentését, és indokoljon megoldást az elfogadható adatvesztés, kiesési idő és költség alapján! *Fő technológiák és fogalmak: High availability/HA, disaster recovery/DR, region, availability zone, RPO, RTO*
39. **Hálózati failover és kapcsolatfolytonosság:** Egy elsődleges és tartalék internetkijárat példáján mutassa be a hibafelismerést és az útvonalváltást! Ismertesse, mi történik az új és a már fennálló kapcsolatokkal, ha a NAT vagy a stateful tűzfal állapota nem kerül át a tartalék eszközre! Különítse el az IP-elérhetőséget a munkamenet folytonosságától! *Fő technológiák és fogalmak: Failover, convergence, NAT, connection state*

    Titkok és hitelesítési adatok kezelése: Mutassa be a jelszavak, API-kulcsok és egyéb titkok kezelésének kockázatait! Ismertesse a központi tárolás, a hozzáférés-korlátozás és a rotáció szerepét! Különítse el az alkalmazás konfigurációját a titkos hitelesítési adatoktól! *Fő technológiák és fogalmak: Secrets, API keys, secret store, access control, rotation*
40. **Telephelyek hálózatainak integrációja:** Egy akvizíció után korábban önálló telephelyek hálózatait kell összekapcsolni. Mutassa be a címterek összehangolásának, a szegmentációnak és a WAN-kapcsolatoknak a fő döntéseit! Indokolja a statikus vagy dinamikus routing választását és egy redundáns megoldást! *Fő technológiák és fogalmak: Address overlap, VLAN/subnet, WAN/VPN, OSPF/BGP, redundancy*

    Felhőarchitektúra értékelése műszaki és üzleti szempontból: Egy választott alkalmazás példáján indokolja a futtatási, tárolási és szolgáltatási modell fő választásait! Mutassa be a rendelkezésre állás, a teljesítmény, a költség és az üzemeltethetőség közötti kompromisszumokat! Térjen ki az identitáskezelés, az elkülönítés és az adatvédelem összehangolására! Ismertesse a döntéshez ellenőrizendő feltételezéseket és méréseket, valamint a választott megoldás mellett fennmaradó kockázatokat! *Fő technológiák és fogalmak: Compute/storage/service model, availability, performance, cost*

A felelettel szembeni elvárások:

A vizsgatétel két részből áll. A felelet során mind az A, mind a B kérdést ki kell fejteni. A hálózati, felhőszolgáltatási és biztonsági témák a két részben szerepelnek; a biztonsági kérdés önálló elméleti téma vagy az adott megoldáshoz kapcsolódó szempont is lehet.

Mutassa be a kérdésben megadott fogalmakat és működési összefüggéseket! Legyen képes egyszerű példán alkalmazni az ismereteket, összehasonlítani a megoldásokat és indokolni a döntéseket! Ahol releváns, térjen ki a biztonságra, a rendelkezésre állásra, az üzemeltetési ráfordításra és a költségre!

A működést szükség szerint egyszerű ábrával szemléltesse! Ha a kérdés nem ad meg konkrét adatokat, válasszon szakmailag következetes példát, és nevezze meg a feltételezéseit! Tervezési kérdésnél a fő döntések és kompromisszumok bemutatása szükséges, nem teljes rendszerterv.

A szóbeli kérdezés a fogalmak, működési elvek és összefüggések megértését, valamint alkalmazását vizsgálja. Az egyszerű példában szükséges protokollműködést helyesen kell levezetni.

A „Fő technológiák és fogalmak” sor az értelmezést segíti, nem külön felsorolási feladat. A magyar és a szokásos angol megnevezések egyaránt használhatók.