SZAKMAI VIZSGA PRÓBA · INFOSZAKMAIVIZSGA.HU

INFORMATIKAI RENDSZER- ÉS ALKALMAZÁS-ÜZEMELTETŐ TECHNIKUS

PRÓBA SZAKMAI VIZSGA

Szerverek telepítése és beállítása
Nehéz „B” feladatlap

Projektfeladat – B) Hálózatok és szerverek telepítése és beállítása vizsgarész, II. feladat

Ajánlott időtartam: 60 perc

Elérhető pontszám: 20 pont

Beadott dokumentumok	
Piszkozati pótlapok száma	

Értékelésre az alábbi állományokat adom be:	
Szerverek telepítése és beállítása	

INFOSZAKMAIVIZSGA.HU

Általános tudnivalók

- Egy biztonsági incidens után a cég rendszerét kell **megerősítened** és a műveleteket **naplóznod** három virtuális gépen: egy **Windows Server** tartományvezérlőn, egy **Ubuntu Linux** kiszolgálón és egy **Windows 10** kliensen.
- Ez **nehéz** nehézségű feladatsor: a feladatok a **célt** írják le, a megoldás módját önállóan kell megtalálnod. A beállításaidat a kliensről is ellenőrizned kell: amit tiltasz, az ne menjen; amit naplózol, az megjelenjen.
- A feladat elkészítésére 60 perc áll rendelkezésedre.
- A feladatok végén zárójelben, dőlt betűvel jelöljük, miről kell képernyőképet készítened, és milyen néven kell elmentened. A képeket PNG formátumban a **képernyőképek helye** mappába mentsd! A fájlnév eleje mindig a feladat sorszáma, például: `02_tartomanyvezerlo.png`. Ha egy feladathoz több kép kell, a kiterjesztés elé írj sorszámot: `02_tartomanyvezerlo2.png`.
- A feladatleírásban nem szereplő, de a működéshez szükséges paramétereket szabadon megválaszthatod.
- Ahol a feladat jelszót ír elő, ott a **TovivalTanulok1234!** jelszót használd.
- Munkád rendszeres mentésére ügyelj!
- A mellékelt mappában ezeket találod:
  - **Feladatleírás**
    - Jelen dokumentum, ennek mentén haladva kell elkészítened a feladatot. Ehhez a feladatsorhoz nincs kiadott forrásfájl: minden szkriptet és beállítást neked kell megírnod.
  - **képernyőképek helye mappa**
    - ide kell mentened a képernyőképeket a feladatoknál megadott néven

infoszakmaivizsga.hu

Kiinduló környezet

A feladatot nulláról, frissen telepített gépekkel kezded. Előre beállított virtuális gépre nincs szükséged. A gépeket **Oracle VirtualBox** (7.x) alatt futtasd.

Virtuális gép	Operációs rendszer (frissen telepítve)	Javasolt erőforrás
ISV-DC	Windows Server, asztali felülettel (Desktop Experience)	2 vCPU, 4 GB RAM
isv-linux	Ubuntu Server LTS, a telepítéskor létrehozott saját felhasználóddal, OpenSSH szerverrel	1 vCPU, 2 GB RAM
ISV-KLIENS	Windows 10 Pro vagy Education *(a Home kiadás nem léptethető tartományba!)*	2 vCPU, 4 GB RAM

IP-cím terv – tartomány: `infoszakmaivizsga.local` (NetBIOS-név: `ISV`)

Gép	Gépnév	IP-cím / maszk	DNS-kiszolgáló
Windows Server	ISV-DC	192.168.50.10 / 24	192.168.50.10
Ubuntu Server	isv-linux	192.168.50.20 / 24	a NAT-kártyáról kapja
Windows 10	ISV-KLIENS	192.168.50.100 / 24	192.168.50.10

VirtualBox hálózati kártyák

Virtuális gép	1. hálózati kártya	2. hálózati kártya
ISV-DC	Belső hálózat: `isv-lan`	–
isv-linux	NAT	Belső hálózat: `isv-lan`
ISV-KLIENS	Belső hálózat: `isv-lan`	–



Tovi javaslata az infoszakmaivizsga.hu-tól

A biztonsági beállításoknál a legfontosabb szabály: amit megerősítesz, azt **ki is kell próbálni**, méghozzá annak a szemszögéből, akit korlátozol. Ezért ennek a feladatsornak a lényege a kliensről végzett ellenőrzés: a naplóban megjelenik-e az esemény, a tiltott program tényleg nem indul-e, a támadónak látszó gépet kizárja-e a rendszer.

Előkészítés

1. Állítsd be VirtualBoxban mindhárom gép hálózati kártyáit a *VirtualBox hálózati kártyák* táblázat szerint! *(Készíts képernyőképet az isv-linux gép 2. hálózati kártyájának beállításáról, és mentsd el* **`01_halozati_kartya.png`** *néven!)*

Windows Server – ISV-DC

A) Tartományvezérlő, címtár PowerShell-lel

2 pont

2. Állítsd be a gép nevét (**ISV-DC**) és statikus IP-címét az IP-cím terv szerint, majd hozd létre az **infoszakmaivizsga.local** erdőt (NetBIOS: **ISV**), és léptesd a kiszolgálót tartományvezérlővé! *(Készíts képernyőképet a tartományvezérlővé léptetés utáni Server Managerről, és mentsd el* **`02_tartomanyvezerlo.png`** *néven!)*

3. **PowerShell-lel** hozd létre a **Munkatarsak** és a **Diakok** szervezeti egységet, a **Diakok** globális biztonsági csoportot, valamint a **feher.tamas** (Munkatarsak) és a **kiss.anna**, **nagy.bence** (Diakok, a Diakok csoport tagjai) felhasználót (jelszó: **TovivalTanulok1234!**)! *(Készíts képernyőképet a parancsokról és az Active Directory konzolról, és mentsd el* **`03_cimtar.png`** *néven!)*

B) Naplózási házirend és objektumhozzáférés-naplózás

2 pont

4. Hozz létre egy **ISV-naplozas** nevű csoportházirendet a tartományra, amely bekapcsolja a **sikeres és sikertelen bejelentkezések**, valamint a **fiókbejelentkezés** naplózását (a részletes naplózási házirend *Bejelentkezés/kijelentkezés* és *Fiókbejelentkezés* kategóriája)! Kapcsold be az **objektum-hozzáférés (fájlrendszer)** naplózását is! *(Készíts képernyőképet a házirend Beállítások (Settings) lapjáról, és mentsd el* **`04_audit_gpo.png`** *néven!)*

5. Hozd létre a `C:\Bizalmas` mappát (benne egy `terv.txt` fájllal), oszd meg, és állíts be rá **naplózási bejegyzést (SACL)**: a **Diakok** csoport minden **sikeres és sikertelen** hozzáférése naplózódjon! *(Készíts képernyőképet a mappa Speciális biztonsági beállítások → Naplózás lapjáról, és mentsd el* **`05_sacl.png`** *néven!)*



Tovi javaslata az infoszakmaivizsga.hu-tól

Az objektumhozzáférés naplózásához **két** dolog kell egyszerre: a házirendben bekapcsolt audit, **és** magán az objektumon beállított naplózási bejegyzés (SACL). Ha csak az egyiket állítod be, nem lesz napló! A részletes (Advanced Audit) házirendet használd, mert finomabb, mint a klasszikus, és ezek keveredését kerüld el.

C) Szoftverkorlátozás házirenddel

2 pont

6. Hozz létre egy **ISV-szoftverkorlat** nevű csoportházirendet a **Diakok** szervezeti egységre, amely **Szoftverkorlátozási házirenddel** (Software Restriction Policies) eléri, hogy a diákok alapból csak a rendszer- és a *Program Files* mappákból futtathassanak programokat! Tilts le kifejezetten egy programot (például a `mspaint.exe`-t) a felhasználói profil mappáiban is! *(Készíts képernyőképet a biztonsági szintekről és a további szabályokról, és mentsd el* **`06_srp.png`** *néven!)*



Tovi javaslata az infoszakmaivizsga.hu-tól

A Szoftverkorlátozási házirend (SRP) a Windows minden kiadásán működik, ezért használjuk itt. Figyelj, hogy a rendszergazdákat **ne** zárd ki (az SRP-nek van „Minden felhasználó, kivéve a helyi rendszergazdákat" beállítása)! A modern, de csak Enterprise/Education kiadáson kikényszeríthető megoldás az **AppLocker** – a vizsgán érdemes tudnod, hogy a kettő ugyanazt a célt szolgálja.

D) Windows Defender tűzfal házirendből

2 pont

7. Egy **ISV-tuzfal** nevű csoportházirenddel (a tartományra) állítsd be a tartományi profil tűzfalát: a bejövő forgalom alapból tiltva, de engedélyezve maradjon a tartomány működéséhez szükséges forgalom, valamint külön szabállyal a **fájl- és nyomtatómegosztás (SMB)** és az **ICMP (ping)** a belső hálózatból! A szabályok a klienseken is érvényesek legyenek. *(Készíts képernyőképet a házirend bejövő szabályairól, és mentsd el* **`07_tuzfal_gpo.png`** *néven!)*

Ubuntu Server – isv-linux

A feladatokat a telepítéskor létrehozott saját felhasználóddal végezd, a rendszergazdai műveleteket `sudo` használatával.

E) SSH-bekeményítés és fail2ban

2 pont

8. Állítsd be a gép nevét (**isv-linux**) és a belső kártya statikus címét az IP-cím terv szerint! Hozd létre a **help1** felhasználót (**TovivalTanulok1234!**), és állíts be hozzá a Windows 10 kliensről kulcsalapú SSH-belépést! *(Készíts képernyőképet a `ip a` kimenetéről és a kliensről való jelszó nélküli belépésről, és mentsd el* **`08_ssh_kulcs.png`** *néven!)*

9. Keményítsd be az SSH-kiszolgálót (saját fájllal az `sshd_config.d` mappában): **root ne** léphessen be, **jelszavas** hitelesítés tiltva (csak kulcs). Telepítsd és állítsd be a **fail2ban**-t a **sshd** szolgáltatásra: **3** sikertelen próbálkozás után **10 percre** tiltsa az adott IP-t! *(Készíts képernyőképet a `sudo sshd -T | grep -Ei "permitrootlogin|passwordauthentication"` és a `sudo fail2ban-client status sshd` kimenetéről, és mentsd el* **`09_fail2ban.png`** *néven!)*



Tovi javaslata az infoszakmaivizsga.hu-tól

A fail2ban a naplóból (`/var/log/auth.log`) figyeli a sikertelen belépéseket, és a tűzfalban tiltja a kitartó IP-ket. A saját beállításaidat mindig a `jail.local` fájlba írd, ne a `jail.conf`-ba (azt egy frissítés felülírja)! Mivel a jelszavas belépést kikapcsoltad, a teszthez a kliensről **szándékosan jelszavas** próbálkozást indíts (`-o PubkeyAuthentication=no`), hogy a fail2ban elkapja.

F) Auditnapló (auditd)

2 pont

10. Telepítsd az **auditd**-t, és állíts be állandó szabályokat: naplózza a `/etc/passwd` és a `/etc/shadow` **módosítását** (kulcs: `felhasznalok`), valamint egy általad létrehozott `/srv/bizalmas/titok.txt` fájl minden **megnyitását** (kulcs: `titok`)! A szabályok újraindítás után is maradjanak meg. *(Készíts képernyőképet a szabályfájlról és a `sudo auditctl -l` kimenetéről, és mentsd el* **`10_auditd.png`** *néven!)*

11. Válts ki eseményeket (hozz létre egy felhasználót, és olvasd el a titok.txt-t), majd keresd vissza őket **ausearch**-csel a kulcsok alapján! *(Készíts képernyőképet az `ausearch -k titok` és az `ausearch -k felhasznalok` releváns találatáról, és mentsd el* **`11_ausearch.png`** *néven!)*

G) Naplóelemzés pipeline-nal

2 pont

Ezt a részt a Windows 10 kliens J) része után végezd el, amikor már vannak sikertelen SSH-próbálkozások a naplóban.

12. Egyetlen parancssorral (pipeline) írasd ki, hány **sikertelen** SSH-belépési kísérlet volt összesen az `/var/log/auth.log` alapján! *(Készíts képernyőképet a parancsról és az eredményéről, és mentsd el* **`12_sikertelen.png`** *néven!)*
13. Gyűjtsd ki azokat az **IP-címeket**, ahonnan sikertelen próbálkozás érkezett, a próbálkozások számával együtt, csökkenő sorrendben, és mentsd a home mappádba `tamadok.txt` néven! *(Készíts képernyőképet a parancsról és a fájl tartalmáról, és mentsd el* **`13_tamadok.png`** *néven!)*

H) Automatikus frissítések, naplóforgatás

2 pont

14. Állítsd be az **unattended-upgrades** csomagot úgy, hogy a **biztonsági** frissítéseket automatikusan telepítse! Ellenőrizd a beállítást próbafuttatással. *(Készíts képernyőképet a beállításfájl releváns soráról és a `sudo unattended-upgrade --dry-run` kimenetéről, és mentsd el* **`14_frissites.png`** *néven!)*
15. Készíts egy `/etc/logrotate.d/isv-audit` beállítást a `tamadok.txt`-hez hasonló saját riportnaplóra: **heti** forgatás, **4** tömörített példány, új fájl létrehozása forgatás után! Ellenőrizd próbafuttatással (`-d`). *(Készíts képernyőképet a beállításfájlról és a `sudo logrotate -d /etc/logrotate.d/isv-audit` kimenetéről, és mentsd el* **`15_logrotate.png`** *néven!)*

Windows 10 kliens – ISV-KLIENS

Ebben a részben a kliensről ellenőrzöd a megerősítéseket: amit tiltasz, az ne menjen; amit naplózol, az jelenjen meg.

I) Tartomány, szoftverkorlátozás, naplózás ellenőrzése

2 pont

16. Nevezd át a gépet **ISV-KLIENS** névre, állítsd be a hálózatát, és léptesd a tartományba! Jelentkezz be `ISV\kiss.anna` (Diakok) felhasználóként, és ellenőrizd a `gpresult /r`-rel, hogy érvényesek rá a házirendek! *(Készíts képernyőképet a `gpresult /r` kimenetéről, amelyen látszanak az ISV-házirendek, és mentsd el* **`16_gpresult.png`** *néven!)*

17. Próbáld elindítani kiss.anna-ként a letiltott programot (Paint / `mspaint.exe`): a rendszernek meg kell akadályoznia. Ezután nyisd meg a `\\ISV-DC\Bizalmas` megosztást (ez naplózott esemény)! A szerveren az Eseménynaplóban keresd meg a diák hozzáféréséről és a letiltott programról szóló bejegyzést! *(Készíts képernyőképet a tiltott program hibaüzenetéről, és mentsd el* **`17_tiltott_program.png`** *néven! A szerver Eseménynaplójában a megfelelő biztonsági eseményről készült képet mentsd el* **`17_tiltott_program2.png`** *néven!)*

J) A behatolásvédelem kipróbálása

2 pont

18. A kliensről indíts SSH-kapcsolatot az isv-linux **help1** felhasználójához, de **szándékosan rossz jelszóval**, jelszavas módban (`ssh -o PubkeyAuthentication=no help1@192.168.50.20`), **legalább háromszor**! A fail2ban-nak ki kell tiltania a kliens IP-címét. *(Készíts képernyőképet a próbálkozásokról és arról, hogy a további kapcsolat már nem jön létre (timeout), és mentsd el* **`18_brute.png`** *néven!)*

19. A szerveren (a VirtualBox ablakából, konzolon) ellenőrizd a **fail2ban** állapotát: a kliens IP-címének a tiltólistán kell lennie. Oldd fel a tiltást (`fail2ban-client set sshd unbanip ...`), és igazold, hogy a kulcsos belépés újra működik! *(Készíts képernyőképet a `sudo fail2ban-client status sshd` kimenetéről a tiltott IP-vel, majd a feloldás utáni sikeres kulcsos belépésről, és mentsd el* **`19_ban.png`** *és* **`19_ban2.png`** *néven!)*

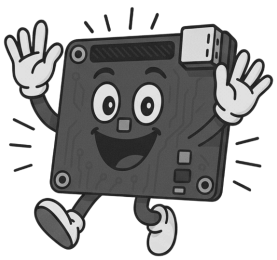


Tovi javaslata az infoszakmaivizsga.hu-tól

Ha a tiltás után a kliens SSH-ja „Connection timed out” üzenetet ad (és nem „Permission denied”-et), az a jó jel: a fail2ban a tűzfalnál **eldobja** a csomagokat, nem is jut el a bejelentkezésig. Vigyázz, hogy a saját gépedet (vagy a szerver saját hálózatát) soha ne tiltsd ki: ezért van a fail2ban-ban az `ignoreip` lista, ahová a megbízható címek kerülnek.

Pontösszesítő

Gép	Feladatrész	Elérhető	Elért
Windows Server	A) Tartományvezérlő, címtár PowerShell-lel	2 pont	
	B) Naplózási házirend, objektumhozzáférés	2 pont	
	C) Szoftverkorlátozás házirenddel	2 pont	
	D) Windows Defender tűzfal házirendből	2 pont	
Ubuntu Server	E) SSH-bekeményítés és fail2ban	2 pont	
	F) Auditnapló (auditd)	2 pont	
	G) Naplóelemzés pipeline-nal	2 pont	
	H) Automatikus frissítések, naplóforgatás	2 pont	
Windows 10	I) Tartomány, szoftverkorlát, naplózás	2 pont	
	J) A behatolásvédelem kipróbálása	2 pont	
	Összesen	**20 pont**	



Ha szeretnél felkészülni a 13-os informatikai szakmai vizsgára rövid videókon, online futtatható szervereken és automatikus kiértékelésű feladatokon keresztül, akkor keresd fel az **infoszakmaivizsga.hu**-t!

infoszakmaivizsga.hu