

Van egy szerverünk, amely 4 kbyte méretű leveleket 3 db/sec sebességgel tud feldolgozni. A szerver egy 1024/1024 kbit/sec sebességű vonal végén van. Egy támadó folyamatosan leveleket küld a szerverre DoS támadási célzattal, olyan sebességgel, hogy a szerver kapacitását pontosan 100%-ban kösse le. A levél átvitele során 20% overhead (többlet) keletkezik a TCP,IP átvitel miatt. Hány százalékában használja ki a támadó az ADSL letöltési irányú csatornáját a támadás közben? (15 pont)

Megoldás: (szerintem)

Letöltési irányú? Na, mindegy...

1 db levél = 4 kbyte

1db levél adatforgalma = $4 + (4 \cdot 0,2) = 4,8$ kbyte

A szerver 3 db ilyen képes 1 mp alatt feldolgozni, tehát ennyit kell neki küldeni másodpercenként.

$4,8 \cdot 3 = 14,4$ kbyte $\rightarrow 14,4 \cdot 8 = 115,2$ kbit

$115,2 / 1024 = 0,1125 \rightarrow 11,25 \%$

5. Az Anonymous támadást próbál intézni a root DNS serverek ellen. 205 servert próbál leterhelni erősített (amplified) DNS támadás által, a sávszélesség elfoglalását célozva. Tegyük fel, hogy minden server szimmetrikus gigabit/s kapcsolattal rendelkezik és ez a bottleneck kapacitás. Tegyük fel, hogy 1 megabit/s szimmetrikus kapacitású támadó barátokat toboroznak, és végtelen kapacitású DNS servereket használnak a hárított-erősített támadásra. Az erősítést úgy érik el, hogy 60 byte-os IP query csomagra a DNS hosztok 4000 byte adatot (overhead-del) küldenek a célszerverekre. A támadást teljesen, egyenletesen elosztják a célpontok között. Úgy becsli a társaság, hogy tízszeresen kell túlterhelni a DNS root servereket a tartós siker érdekében, akár hosszabb távon is. Összesen kb. hány ilyen tag közreműködésére van szükség a sikeres támadáshoz? Válaszát indokolja! (10 p)

Megoldás:

205 site kapacitása 205 gigabit/s. Tízszeres túlterhelésük 2050 gigabit/s. $4000/60$ az erősítési arány, ami kb. 66,7. Így $2050\ 000\ \text{Mbit/sec} / 66.7 = 30\ 745\ \text{Mbit/sec}$ (31 472 Mbit/s, ha 1024-gyel számolunk) forgalom erősítés előtt. Egy tag 1 Mbit/s-re képes, így kb. 30 745 ember kell sikeres támadáshoz. Természetesen a való életben ez nem biztos, hogy igaz és hosszú távon (napok, hetek) kellene képesnek lennie támadniuk, miközben bűncselekményt követnek el. (A gigabit/megabit átváltásnál mind 1000 mind 1024-es váltószámot elfogadunk)

5. Unix/Linux hozzáférésvédelem az órán előadott módon. Tekintsük az alábbi `/etc/passwd` file részletet:

```
u1:x:1003:1004:,,,:/home/u1:/bin/bash
u2:x:1004:1005:,,,:/home/u2:/bin/bash
u3:x:1005:1006:,,,:/home/u3:/bin/bash
u4:x:1006:1007:,,,:/home/u4:/bin/bash
```

Az `/etc/group` file releváns része:

```
u1:x:1004:
u2:x:1005:
u3:x:1006:
u4:x:1007:
g1:x:1008:u1,u2
g2:x:1009:u2,u3,u4
g3:x:1010:u2,u3
```

A fájl hozzáférési jogosultságok az alábbiak:

```
root@gotcha:/adatbirt# ls -la
total 16
drwxr-xr-x  4 root root 4096 2011-04-22 10:49 .
drwxr-xr-x 25 root root 4096 2011-04-22 10:51 ..
drwxrwsr-x  2 u1  g1  4096 2011-04-22 10:50 d1
drwxr-xr-x  2 u2  g1  4096 2011-04-22 10:50 d2
```

```
root@gotcha:/adatbirt# ls -la d1
total 20
drwxrwsr-x 2 u1  g1  4096 2011-04-22 10:50 .
drwxr-xr-x 4 root root 4096 2011-04-22 10:49 ..
-rw----- 1 u1  u4    4 2011-04-22 10:50 f1
-rw-rw---- 1 u1  g1   16 2011-04-22 10:50 f2
-rwxrwxrwx 1 u1  g2    8 2011-04-22 10:50 f3
```

```
root@gotcha:/adatbirt# ls -la d2
total 16
drwxr-xr-x 2 u2  g1  4096 2011-04-22 10:50 .
drwxr-xr-x 4 root root 4096 2011-04-22 10:49 ..
-rw-r--r-- 1 root g1    7 2011-04-22 10:50 f4
--w----- 1 root g1    6 2011-04-22 10:50 f5
```

- Mely felhasználók tudják olvasni a `d1/f1` fájlt és miért? (2p)
- Mely felhasználóknál fut le sikeresen a `cp d1/f2 d2/f6` parancs? (2p)
- Ki tudja módosítani az `f2` fájl jogosultságait (pl. `chmod o+w d1/f2`)? (3p)
- Ki tudja lefuttatni az `rm d1/f3`; `cp d1/f1 d1/f3` parancsokat mind sikeresen, azaz kitörölni `f3`-at és helyére `f1`-et másolni? (3p)

Megoldás:

- csak `u1`, neki van olvasás joga és a directory-ba is be tud lépni
- `u2`, `root`, mert: `g1` és `u1` tudja olvasni `f2`-t, joguk van belépni `d2`-be, ott fájlt azonban `u2` tud csak csinálni.
- csak a tulajdonos, `u1` (és a `root`)
- a törlést csak `u1`, `u2` tudja elvégezni `f1`-et viszont ebből csak `u1` olvashatja `f1`-et, ő írni is tud az alkönyvtárba, tehát csak `u1`. (+`root`)

5. Unix/Linux hozzáférésvédelem az órán előadott módon. Tekintsük az alábbi /etc/passwd file részletet:

```
u1:x:1003:1004:,,,:/home/u1:/bin/bash
u2:x:1004:1005:,,,:/home/u2:/bin/bash
u3:x:1005:1006:,,,:/home/u3:/bin/bash
u4:x:1006:1007:,,,:/home/u4:/bin/bash
```

Az /etc/group file releváns része:

```
u1:x:1004:
u2:x:1005:
u3:x:1006:
u4:x:1007:
g1:x:1008:u1,u2
g2:x:1009:u2,u3,u4
g3:x:1010:u2,u3
```

A fájl hozzáférési jogosultságok az alábbiak:

```
root@gotcha:/adatbizt# ls -la
total 16
drwxr-xr-x  4 root root 4096 2011-04-22 10:49 .
drwxr-xr-x 25 root root 4096 2011-04-22 10:51 ..
drwxrwsr-x  2 u1  g1  4096 2011-04-22 10:50 d1
drwxr-xr--  2 u2  g1  4096 2011-04-22 10:50 d2
root@gotcha:/adatbizt# ls -la d1
total 20
drwxrwsr-x 2 u1  g1  4096 2011-04-22 10:50 .
drwxr-xr-x 4 root root 4096 2011-04-22 10:49 ..
-rw----- 1 u1  root    4 2011-04-22 10:50 f1
-rw-rw-r-- 1 u1  g1    16 2011-04-22 10:50 f2
-rwxrwxrwx 1 u1  g2     8 2011-04-22 10:50 f3
root@gotcha:/adatbizt# ls -la d2
total 16
drwxr-xr-- 2 u2  g1  4096 2011-04-22 10:50 .
drwxr-xr-x 4 root root 4096 2011-04-22 10:49 ..
-rw-r--r-- 1 root g1     7 2011-04-22 10:50 f4
--w----- 1 root g1     6 2011-04-22 10:50 f5
```

- mely felhasználók tudják kitörölni a d2/f4 fájlt és miért? (rm d2/f4)
- mely felhasználóknál fut le sikeresen a cp d2/f4 d2/f6 parancs?
- ki tudja módosítani az f2 fájl jogosultságait (pl. chmod o+w d1/f2)
- ki tudja lefuttatni a rm d1/f3; cp d1/f1 d1/f3 parancsokat mind sikeresen, azaz kitörli f3-at és helyére f1-et másolja?
- g2 csoport tagjai mely fájlokat tudják olvasni d1 alkönyvtárban (mindegyikük) a fenti eredeti listából? **(15p)**

Megoldás:

- csak u2, más nem írhat az alkönyvtárba (+root)
- csak u2, mert ő írhat d2-be, és tudja olvasni f4-et is.. (+root)
- csak a tulajdonos, u1 (és a root)
- a törlést csak u1,u2 tudja elvégezni f1-et viszont ebből csak u1 olvashatja, ő írni is tud az alkönyvtárba, tehát csak u1. (+root)
- f2,f3

5. Unix/Linux hozzáférésvédelem az órán előadott módon. Tekintsük az alábbi /etc/passwd file részletet:

```
u1:x:1003:1004:,,,:/home/u1:/bin/bash
u2:x:1004:1005:,,,:/home/u2:/bin/bash
u3:x:1005:1006:,,,:/home/u3:/bin/bash
u4:x:1006:1007:,,,:/home/u4:/bin/bash
```

Az /etc/group file releváns része:

```
u1:x:1004:
u2:x:1005:
u3:x:1006:
u4:x:1007:
g1:x:1008:u1,u2
g2:x:1009:u2,u3,u4
g3:x:1010:u2,u3
```

A fájl hozzáférési jogosultságok az alábbiak:

```
root@gotcha:/adatbizt# ls -la
total 16
drwxr-xr-x  4 root root 4096 2011-04-22 10:49 .
drwxr-xr-x 25 root root 4096 2011-04-22 10:51 ..
drwxrwsr-x  2 u1  g1  4096 2011-04-22 10:50 d1
drwxr-xr--  2 u2  g1  4096 2011-04-22 10:50 d2
root@gotcha:/adatbizt# ls -la d1
total 20
drwxrwsr-x 2 u1  g1  4096 2011-04-22 10:50 .
drwxr-xr-x 4 root root 4096 2011-04-22 10:49 ..
-rw----- 1 u1  root    4 2011-04-22 10:50 f1
-rw-rw-r-- 1 u1  g1    16 2011-04-22 10:50 f2
-rwxrwxrwx 1 u1  g2     8 2011-04-22 10:50 f3
root@gotcha:/adatbizt# ls -la d2
total 16
drwxr-xr-- 2 u2  g1  4096 2011-04-22 10:50 .
drwxr-xr-x 4 root root 4096 2011-04-22 10:49 ..
-rw-r--r-- 1 root g1     7 2011-04-22 10:50 f4
--w----- 1 root g1     6 2011-04-22 10:50 f5
```

- a.) mely felhasználók tudják kitörölni a d1/f1 fájlt és miért? (rm d1/f1) (2 pont)
- b.) mely felhasználóknál fut le sikeresen a cp d2/f4 d1/f6 parancs? (2 pont)
- c.) az u1 felhasználó (u1 aktív csoporttal) készít egy új fájlt d1-ben (touch d1/fu1), milyen csoport lesz a tulajdonosa a létrejövő fájlnek (2 pont)
- d.) A root felhasználó mely fájlokat tudja törölni az d1 alkönyvtárban (2 pont)
- e.) Ki tudja végrehajtani sikeresen az f2 fájl olvasási jogának teljes törlését? (chmod a-r d1/f2) (2 pont)

Megoldás:

- a.) u1 és u2, mert u1 és a g1 csoport tagjai írhatják az alkönyvtárat
- b.) d1-be u1 és a g1 írhat, tehát csak u1 és u2 jön szóba, ők mindketten hozzáférnek a f4 fájlhoz, tehát u1 és u2.
- c.) g1 lesz, mert csoport setgid jel van az alkönyvtáron
- d.) Az összeset, mert a root felhasználó speciális jogú
- e.) u1, ő a tulajdonosa (és a root)

Tekintsük az alábbi `/etc/passwd` file részletet:

```
alice:x:1003:1003:,,,:/home/alice:/bin/bash
bob:x:1004:1004:,,,:/home/bob:/bin/bash
tiger:x:1005:1005:,,,:/home/tiger:/bin/bash
piglet:x:1006:1006:,,,:/home/piglet:/bin/bash
mallory:x:1007:1007:,,,:/home/mallory:/bin/bash
```

A `/etc/group` file releváns része:

```
alice:x:1003:
bob:x:1004:alice
tiger:x:1005:
piglet:x:1006:
mallory:x:1007:
winnie:x:1008:tiger,piglet
cryptoland:x:1009:alice,bob,mallory,root
```

A fájl hozzáférési jogosultságok az alábbiak:

```
root@hbggyak:/thewood# ls -la
total 16
drwxrwsr-x  4 root winnie      4096 2010-04-08 11:23 .
drwxr-xr-x 23 root root        4096 2010-04-08 11:30 ..
drwxrwx---  2 root cryptoland  4096 2010-04-08 11:24 friends
drwxr-xr-x  2 alice winnie     4096 2010-04-08 11:25 secrets

root@hbggyak:/thewood# ls -la friends/
total 20
drwxrwx--- 2 root cryptoland  4096 2010-04-08 11:24 .
drwxrwsr-x 4 root winnie     4096 2010-04-08 11:23 ..
-rwxr--r-- 1 alice winnie     10 2010-04-08 11:26 a1
-rw-r--r-- 1 bob cryptoland   10 2010-04-08 11:26 a2
-rw----- 1 bob cryptoland   10 2010-04-08 11:26 a3

root@hbggyak:/thewood# ls -la secrets/
total 20
drwxr-xr-x 2 alice winnie     4096 2010-04-08 11:25 .
drwxrwsr-x 4 root winnie     4096 2010-04-08 11:23 ..
-rw-rw-r-- 1 alice winnie     10 2010-04-08 11:25 s1
-rw-r----- 1 tiger cryptoland 10 2010-04-08 11:26 s2
-rw-rw-r-- 1 alice winnie     10 2010-04-08 11:39 s3
```

A felhasználók (alice, bob, tiger, piglet, mallory) közül ki tudja végrehajtani sikeresen az alábbi parancsokat, miközben a `thewood` alkönyvtárban dolgozik:

- a) `cp friends/a1 secrets/s4`
- b) `cat secrets/s1`
- c) `ls -la friends`
- d) `cd friends`

[Minden alkérdés 0.5 pontot ér.]

Megoldás:

- a) alice
- b) mindenki: alice, bob, mallory, tiger, piglet
- c) alice, bob, mallory
- d) mindenki: alice, bob, mallory, tiger, piglet

Rövid kérdések: ezeket ITT válaszolja meg!

- a) Mi a DoS amplification támadás nagyon röviden? (4 p)
 - b) Milyen kategóriákba sorolhatjuk a lehetséges DoS védekezési módszereket? (3 p)
 - c) Adjon definíciót a *-tulajdonságra a Bell-LaPadula (BLP) modellben. (3 p)
 - d) Mi a spam ellenes greylisting lényege? (3 p)
 - e) Mondjon három TCP flag-et amire egy tűzfalban szűrő szabályt szokás építeni! (3 p)
 - f) Mi a célja a portscannelésnek? (3 p)
 - g) Adott két tűzfalszabály:
udp any 192.168.1.0/24 accept
udp 172.16.1.0/24 192.168.1.0/24 deny
Az órai definíciók szerint ez milyen típusú tűzfal inkonzisztencia problémát jelent? (3 p)
-

Megoldás:

- a) A kérésre vagy sokkal nagyobb válasz, vagy több válasz érkezik, így nagyobb támadás érhető el kisebb befektetéssel. DNS esetén akár 60-70x sávszélesség emészthető fel.
- b) prevention, detection and filtering, traceback and identification.
- c) *-property: for all (Si, Oj, append) in b , $fc(Si) \leq fo(Oj)$ and for all (Si, Oj, write) in b , $fc(Si) = fo(Oj)$ a subject at a given security level must not write to any object at a lower security level (no write-down). The *-property is also known as the Confinement property.
- d) adott email forrás, cél, forrás ip hármastól nem fogadunk el első alkalomra leveleket.
- e) SYN, FIN, ACK, RST, (URGENT, ECN, CWR-Reduced, Push)
- f) Tipikusan az aktuálisan használt TCP/UDP portok feltérképezése, az esetleges tűzfal szűrések kiderítése, a támadható szolgáltatások felderítése.
- g) shadowing, árnyékolás

4. Milyen három fő tűzfaltípust különböztettünk meg, és egy-egy mondatban mi a lényegi különbség közöttük (angol kifejezések is használhatóak)?

5. Mit jelent az, hogy a CRC lineáris az XOR műveletre nézve? Egyetlen képlettel válaszoljon!

7. Rajzolja fel a jelszó alapú hitelesítés általános modelljét!

10. Rajzolja fel az Access Control általános modelljét!

Megoldás:

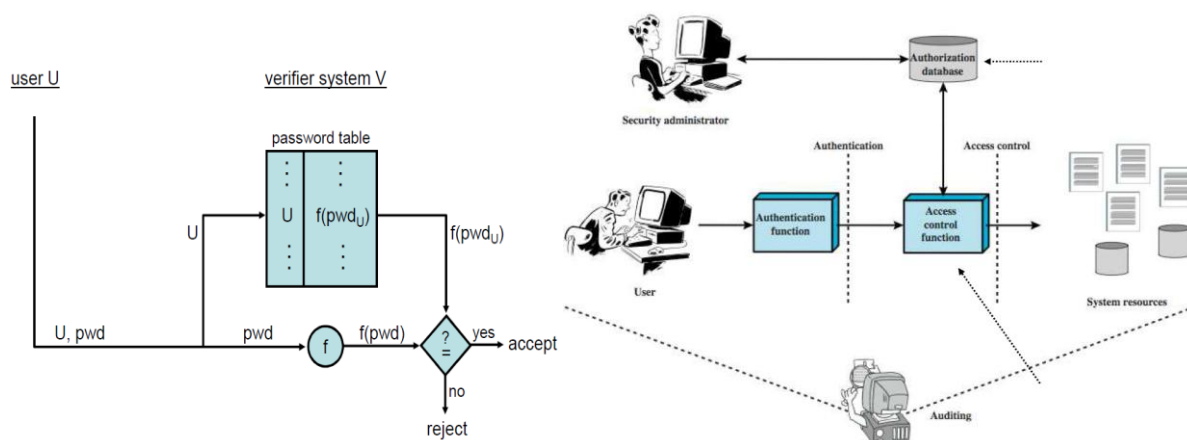
4.

- packet filtering:
 - IP, ICMP, TCP, UDP csomagfejléceket vizsgál
 - lehet statikus vagy dinamikus
- circuit-level gateways:
 - szállítási rétegben működik
 - kettébontja a TCP kapcsolatot
 - nincs filtering
 - azt figyeli, hogy mely kapcsolatokat szabad felépíteni
- application-level gateways
 - hasonló az előzőhöz, de képes figyelni az alkalmazás specifikus részleteket is (pl. HTTP üzenet tartalma, levelek tartalma)

5.

$$\text{CRC}(X \oplus Y) = \text{CRC}(X) \oplus \text{CRC}(Y)$$

7. és 10.



Rövid kérdések:

- a.) Mire használják a unix sticky bitet? (3 pont)
- b.) Mi a spam elleni harcban a DKIM megoldás? (3 pont)
- c.) Hogyan szinkronizálja az időt a Conficker bot? (3 pont)

Mutassa be a Bell-LaPadula modell három tulajdonságát (ss,ds,*) formálisan! (12 pont)

Megoldás:

- a.) sticky bit: +t, csak a tulajdonos törölheti a fájlt vagy alkönyvtárat. Hiába van esetleg írási joga az adott felhasználónak, nem törölheti.
- b.) DKIM: Minden e-mail a DNS rekordban tárolt nyilvános kulcshoz tartozó titkos kulccsal aláírásra kerül a kiküldő szerverek által, így kevesebb a lehetőség hamisított címmel levelet feladni.
- c.) Conficker szinkron: Fontosabb weboldalak (Google, Yahoo, ...) lekérdezésével megszerzett HTTP fejlécben található Date mezőt használja fel a szinkronizáláshoz.

ss-property: for all (S_i, O_j, read) in b , $f_c(S_i) \geq f_o(O_j)$.

a subject at a given security level may not read an object at a higher security level (no read-up).

***-property:** for all $(S_i, O_j, \text{append})$ in b , $f_c(S_i) \leq f_o(O_j)$ and for all (S_i, O_j, write) in b , $f_c(S_i) = f_o(O_j)$

a subject at a given security level must not write to any object at a lower security level (no write-down). The *-property is also known as the Confinement property.

ds-property: for all (S_i, O_j, A_x) in b , $A_x \in M[S_i, O_j]$

use of an access matrix http://en.wikipedia.org/wiki/The_Access_Matrix to specify the discretionary access control. An individual may grant to another individual access to a file based on the owner's discretion constrained by the MAC rules.

5. Bell-LaPadula modell M és f táblázatai az alábbiak:

M	F1	F2	F3	f	Classification	f	Clearance
A	R	R	RWA	F1	Unclassified	A	Top secret
B	R	RA	WA	F2	Secret	B	Secret
C	RWA	WA	RWA	F3	Top Secret	C	Unclassified

(R:Read W:Write A:Append)

A felhasználók a szabványos BLP műveleteket használják olvasás és írási hozzáférés kérésekhez (Get Access, Release Access + műveletek), a „b” tábla mindig ennek megfelelő, a H fát nem használjuk. Válaszait indokolja!

- Ki tudja elvégezni F2 olvasását? (3p)*
- Ki tudja elvégezni F3 írását (W)? (2p)*
- Ki tud hozzáírni (append) F2 fájlhoz? (3p)*
- Adja meg a *-property formális definícióját. (3p)*

Megoldás:

- M miatt csak A és B jön szóba, az ss-property miatt A és B jöhet szóba: A és B
- M miatt csak A, B, C mind szóba jön, a *-property miatt csak A
- M miatt csak B, C jön szóba, a *-property miatt mind B és C jó, tehát B és C.
- for all (Si, Oj, append) in b, $fc(Si) \leq fo(Oj)$ and for all (Si, Oj, write) in b, $fc(Si) = fo(Oj)$

Egy rendszergazda az alábbi tűzfalszabályokat állította be a 152.66.249.128/27-es hálózat védelmében egy csomagtovábbító tűzfalon, melyet a rendszer az órán ismertetett módon kezel:

```
src=any, sport=any, dst=152.66.249.135, dport=80, prot=tcp → ALLOW
src=any, sport=any, dst=152.66.249.128/27, dport=22, prot=tcp → ALLOW
src=152.66.249.135, sport=any, dst=any, dport=53, prot=tcp,udp → ALLOW
src=152.66.249.128/27, sport=any, dst=any, dport=69, prot=udp → DROP
src=152.66.249.0/27, sport=any, dst=152.66.249.128/27, dport=161, prot=tcp,udp →
ALLOW
src=any, sport=any, dst=152.66.149.128/27, dport=161, prot=tcp,udp → DROP
src=any, sport=any, dst=152.66.249.128/27, dport=110,143 prot=tcp → ALLOW
src=any, sport=any, dst=152.66.249.128/27, dport=8090, prot=tcp → DROP
src=152.66.249.0/24, sport=any, dst=152.66.249.128/27, dport=8090, prot=tcp → ALLOW
src=152.66.249.128/27, sport=any, dst=any, dport=any, prot=tcp,udp → ALLOW
src=any, sport=any, dst=152.66.249.128/27 dport=0-1000, prot=tcp → DROP
src=any, sport=any, dst=any dport=any, prot=any → ALLOW
```

A rendszergazda a naplófájlok alapján meglepődve észlelte, hogy a szabályokban valami hiba lehet, mert az alábbi célokat a szabályok nem jól valósították meg. Keresse meg hol van a hiba, miben hibázott a rendszergazda!

A rendszergazda célja volt:

- A 152.66.249.0-255 tartományból lehessen a 8090-es TCP portot elérni, máshonnan nem
- A védett hálózat felé az SNMP protokollt (161 UDP és TCP portok) a 152.66.249.0/27 hálózathoz szabad elérni, máshonnan nem
- A nem használt TCP és UDP portok 1000 alatt a védett hálózat irányában tiltva legyenek, amelyekre nincs specifikus egyéb szabály
- A DNS szolgáltatás (53-as TCP és UDP port) kívülről elérhető legyen, de csak a DNS szerveren (152.66.249.135) **(12p)**

Megoldás:

- pl. Rossz a tiltás és engedélyezés sorrendje, így az engedélyezés nem aktív
- A rendszergazda elírta az cél IP tartományt a tiltó szabályban, 249 helyett 149-et írt.
- Elfelejtette letiltani az UDP protokoll portjait az 11. (utolsó előtti) szabályban
- A harmadik szabályban a cél helyett a forrás lett beírva, vagy más értelmezésben a teljes szabály hiányzik

Adott az alábbi tűzfal szabályhalmaz:

1	tcp	10.1.1.0/25	any	deny
2	udp	any	192.168.1.0/24	accept
3	tcp	10.1.1.128/25	any	deny
4	udp	172.16.1.0/24	192.168.1.0/24	deny
5	tcp	10.1.1.0/24	any	accept
6	udp	10.1.1.0/24	192.168.0.0/16	deny
7	udp	172.16.1.0/24	any	accept

Keressen példát a következő inkonzisztenciátípusokra, és válaszát röviden indokolja!

a.) Shadowing (5 pont)

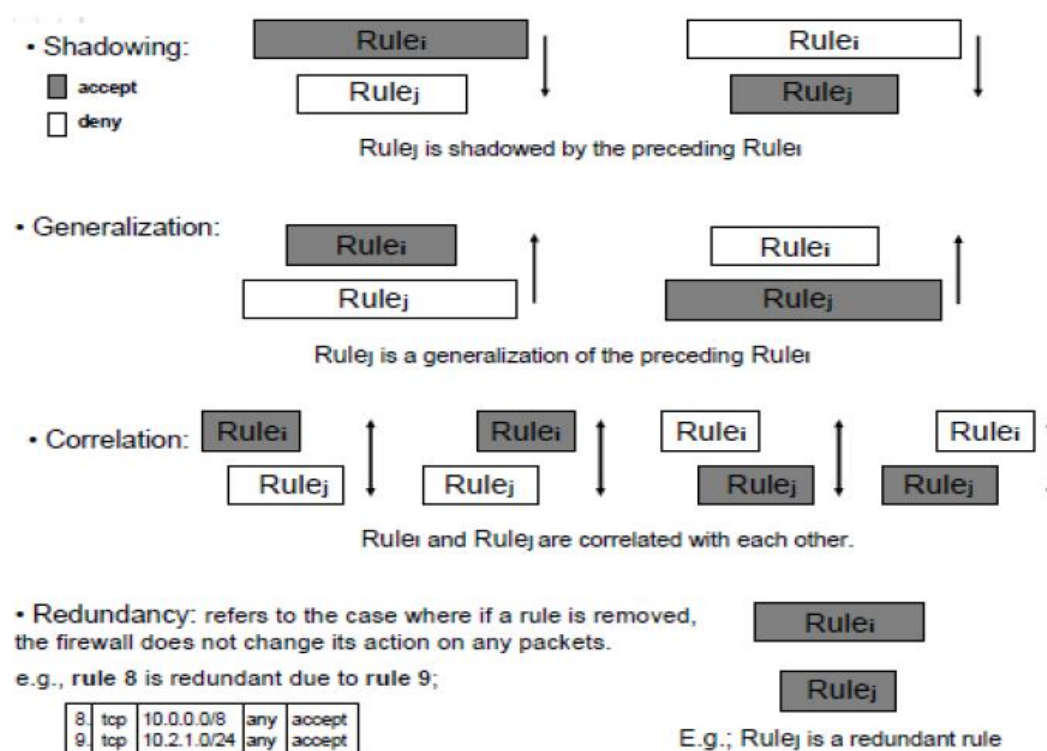
b.) Generalization (5 pont)

c.) Correlation (5 pont)

Megoldás:

- shadowing e.g., **rule 4** is shadowed by **rule 2**; **rule 5** is shadowed by *combination* of **rule 1** and **rule 3**;
- generalization e.g., **rule 7** is a generalization of **rule 4**,...
- correlation pl. **rule 2** and **rule 6** are correlated

Háttérismeret:



5. Adott az alábbi tűzfal szabályhalmaz:

Keressen példát a következő inkonzisztenciatípusokra, és válaszát röviden indokolja!

No.	Proto	Src	Dst	Decision
1	tcp	10.1.1.0/25	any	deny
2	udp	10.1.1.0/24	192.168.0.0/16	accept
3	tcp	10.1.1.0/24	any	accept
4	udp	192.168.1.0/24	10.1.1.0/24	deny
5	tcp	10.1.1.128/25	any	deny
6	udp	10.1.1.0/24	any	deny
7	udp	192.168.1.0/25	10.1.0.0/16	accept

a.) *Shadowing* (2p)

b.) *Generalization* (2p)

c.) *Correlation* (2p)

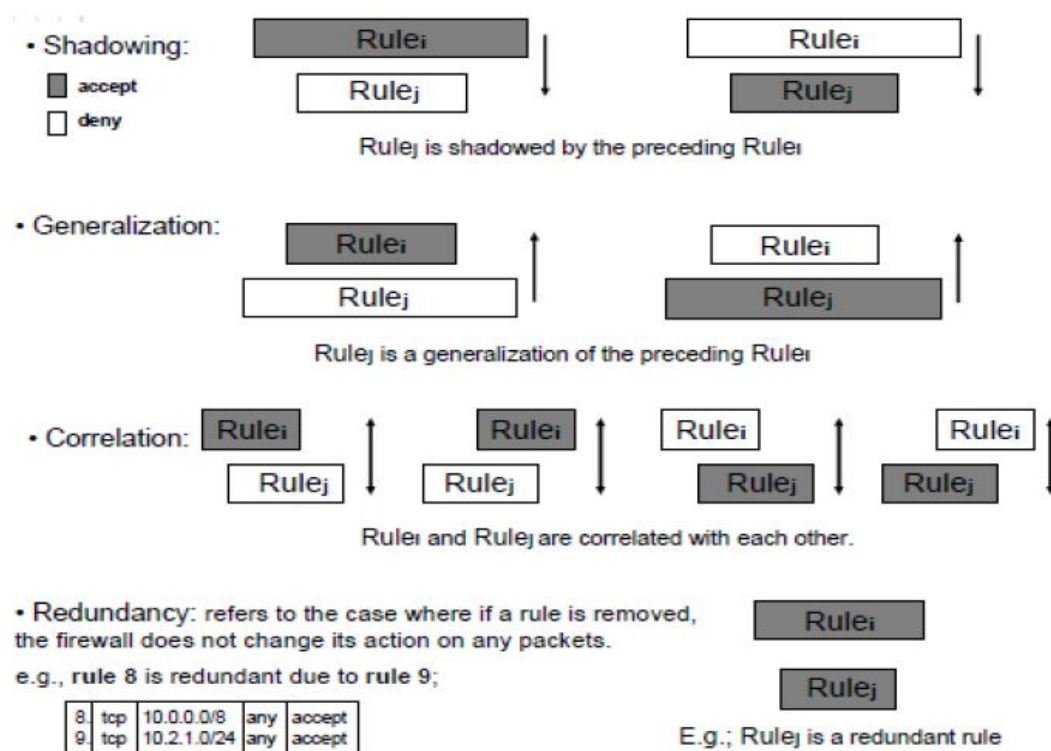
Megoldás:

a.) pl. 5-ös szabályt árnyékolja a 3-as

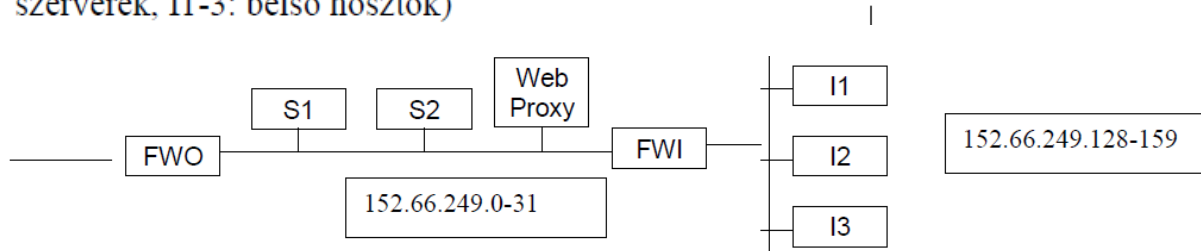
b.) pl. 6-os a 2-essel

c.) pl. 7-es a 4-essel

Háttérismeret:



6. Egy tűzfal topológiát az alábbi ábra mutat be (FWO: külső tűzfal az internet felé, FWI: belső tűzfal, Web proxy: egyfajta bástya hoszt webes lekérdezésekhez, S1,S2: szerverek, I1-3: belső hosztok)



Az FWO kifele minden kapcsolatkezdeményezést megenged, visszafelé csak az S1,S2 szerverekre enged SSH (TCP/22) kapcsolódást, illetve átengedi a már létrejött kapcsolatokat. A Web proxyt a belső hálózathoz bárki elérheti és rajta keresztül application level tűzfalként kezdeményezhet webes kéréseket korlátlanul. Az FWI az internetre minden kapcsolódást engedélyez (és a rá jövő válaszcsoomagokat is), továbbá S1, S2 felé SSH-t, illetve a Web proxy elérését engedi, befele semmit, minden más is tiltva van.

- Új féreg terjed az interneten, a 445-ös portra csatlakozást használva mindenkit feltör. Mi fog történni a DMZ-nkben és a belső hálózatunkban? (2p)*
- I3 gépen egy támadó program fut. S2 web szerverén futó alkalmazás ellen akar SQL injection támadást intézni, van rá lehetősége? (4p)*
- I3 gépen futó támadó program az interneten levő szerverek felé spam üzeneteket próbál továbbítani. Meg tudja ezt tenni? (2p)*
- S1-et feltörik kívülről, mert rossz SSH jelszava van. I1-en is fut egy SSH szerver, de a rossz jelszó nem azonos. Mekkora az esélye a támadónak I1 SSH jelszavainak feltörésére? (2p)*

Megoldás:

- Az égvilágon semmi, a 445-ös portra nem lehet csatlakozni egyik hálózatunkban sem
- U3 csatlakozni tud a web proxyra, az pedig az S2-re, ha a web szerver tényleg hibás, feltörhető valóban.
- Természetesen képes rá, FWI engedi, FWO mindent enged kifelé.
- Hiába törték fel S1-et, befele FWI nem enged SSH kapcsolódást így nem lehet kísérletezni, így a támadás esélye 0 a feltételek mellett.

5. Egy spamszűrő az órán ismertetett Bayes szűrést használja. Feltételezi, hogy $\Pr(S)=\Pr(W)=0,5$. Adatbázisa a következő adatokat tanulta meg:
 $\Pr(\text{olcsón}|S)=0,01$ $\Pr(\text{eladó}|S)=0,01$ $\Pr(\text{telek}|S)=0,05$
 $\Pr(\text{olcsón}|H)=0,001$ $\Pr(\text{eladó}|H)=0,005$ $\Pr(\text{telek}|H)=0,1$

Adott egy levél: „Telek olcsón eladó” tartalommal. Mekkora az esélye, hogy a levél spam? Számolja ki az órán tanult módon a levél kombinált spam-valószínűségét (három tizedes jegy precizitású részszámítások elegendőek)! (10p)

Megoldás:

Egyedi valószínűségek:

$$\Pr(S|\text{olcsón}) = \Pr(\text{olcsón}|S) / (\Pr(\text{olcsón}|S) + \Pr(\text{olcsón}|H)) = 0,01 / (0,01 + 0,001) = 0,909$$

$$\Pr(S|\text{eladó}) = 0,01 / (0,01 + 0,005) = 0,667$$

$$\Pr(S|\text{telek}) = 0,05 / (0,05 + 0,1) = 0,333$$

$$p = \Pr(S|\text{olcsón}) * \Pr(S|\text{telek}) * \Pr(S|\text{eladó}) /$$

$$(\Pr(S|\text{olcsón}) * \Pr(S|\text{telek}) * \Pr(S|\text{eladó}) + (1 - \Pr(S|\text{olcsón})) * (1 - \Pr(S|\text{telek})) * (1 - \Pr(S|\text{eladó})))$$

$$\text{azaz } p = 0,202 / (0,202 + 0,02) = 0,202 / 0,222 = 90,991\%$$

Háttérismeret:

- Bayes' theorem $P(A|B) = \frac{P(B|A) P(A)}{P(B)}$

- In case of spam:

$$\Pr(S|W) = \frac{\Pr(W|S) \cdot \Pr(S)}{\Pr(W|S) \cdot \Pr(S) + \Pr(W|H) \cdot \Pr(H)}$$

W: a word is in the email e.g. "Viagra"

S: the email is spam

H: the email is ham (good message, not spam)

$\Pr(S|W)$: The message is spam, if it contains the word W.

$\Pr(W|S)$: In a spam message, the probability of the existence of the particular word etc.

- About 80% of the internet e-mails are spam

$$\Pr(S) = 0.8; \Pr(H) = 0.2$$

- However, many bayesian spam filter make the assumption

$$\Pr(S) = 0.5; \Pr(H) = 0.5$$

- In this case $\Pr(S|W) = \frac{\Pr(W|S)}{\Pr(W|S) + \Pr(W|H)}$