Biztonságos programozás

1. feladat

a.) Milyen típusú sérülékenységet tartalmaz az alábbi forráskód és miért? (2 pont) #include #include #include #include int main(int argc, char **argv) { char buffer[64]; gets(buffer); }

b.) A main függvényhez tartozó frame pointerhez (pl.: EBP) képest, hol helyezkedik el a buffer nevű lokális változó (mi a kezdőcíme)? Az egyszerűség kedvéért tekintsünk egy hagyományos x86-os architektúrát, és egy jól ismert compilert (pl.: gcc). (3 pont)

c.) Hogyan képes egy támadó kihasználni az alábbi sérülékenységet? Milyen címet írna felül a main függvényhez tartozó stackframe-en? Egy ilyen cím felülírásához milyen hosszú (bájtban mérve) input-ra lenne szüksége? (7 pont)

Megoldás:

a.) [+] Stack overflow/buffer overflow (1p) [+] A buffer lokális változóba a gets() függvény segítségével tetszőleges méretű felhasználói inputot lehet elhelyezni, s így a bufferből kiindexelve érvénytelen címre mutató pointert tud egy esetleges támadó dereferálni. (1p)

b.) A main függvényhez tartozó frame pointerhez (pl.: EBP) képest, hol helyezkedik el a buffer nevű lokális változó (mi a kezdőcíme)? Az egyszerűség kedvéért tekintsünk egy hagyományos x86-os architektúrát, és egy jól ismert compilert (pl.: gcc).

[+] EBP-64, hiszen egy 64 bájtos lokális változóról van szó, s alignment nélkül az EBP alatt (alacsonyobb címen) közvetlenül helyezkedik el. (3p)

2. feladat

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 p)

u1 és u2, mert u1 és a g1 csoport tagjai írhatják az alkönyvtárat

b.) mely felhasználóknál fut le sikeresen a cp d2/f4 d1/f6 parancs? (2 p)

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

c.) az u1 felhasználó (u1 aktív csoporttal) készít egy új fájlt d1-ben (touch d1/fu1), milyen csoport lesz a tulajdonosa a létrejövő fájlnak? (2 p)

g1 lesz, mert csoport setgid jel van az alkönyvtáron

d.) a root felasználó mely fájlokat tudja törölni az f1 alkönyvtárban? (2 p)

Az összeset, mert a root felhasználó speciális jogú

e.) ki tudja végrehajtani sikeresen az f2 fájl olvasási jogának teljes törlését? (chmod a-r d1/f2) (2 p)

u1, ő a tulajdonosa (és a root)

3. feladat

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-x 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 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:/adatbizt# 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

a.) Mely felhasználók tudják olvasni a d1/f1 fájlt és miért? (2p)

csak u1, neki van olvasás joga és a directory-ba is be tud lépni

b.) Mely felhasználóknál fut le sikeresen a cp d1/f2 d2/f6 parancs? (2p)

u2, root, mert: g1 és u1 tudja olvasni f2-t, joguk van belépni d2-be, ott fájlt azonban u2 tud csak csinálni.

c.) Ki tudja módosítani az f2 fájl jogosultságait (pl. chmod o+w d1/f2)? (3p)

csak a tulajdonos, u1 (és a root)

d.) 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)

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)

4. feladat

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 ..

drwxrws--- 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:/adatbizt# ls -la d1

total 20

drwxrws--- 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:/adatbizt# 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

a.) mely felhasználók tudják olvasni a d1/f3 fájlt és miért? (2p)

Az u1 felhasználón és g1 csoporton kívül más nem fér hozzá az alkönyvtárhoz, a fájlhoz mindenkinek van ugyan olvasás joga, de ezért csak u1 és a g1 csoport tagjai: u1 és u2

b.) mely felhasználóknál fut le sikeresen a cp d1/f1 d2/f6 parancs?(2p)

senkinél, vagy csak az u2 felhasználónál: A d2-be csak u2 írhat, de u2 nem olvashatja az f1 fájlt

c.) ki tudja módosítani az f3 fájl jogosultságait (pl. chmod o+w d1/f3) (2p)

csak a tulajdonosa u1 és a root

d.) ki tudja törölni az f3 fájlt? (2p)

u1 és u2, a törléshez az alkönyvtárra kell írás jog

5. feladat

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) (2p)

u1 és u2, mert u1 és a g1 csoport tagjai írhatják az alkönyvtárat

b.) mely felhasználóknál fut le sikeresen a cp d2/f4 d1/f6 parancs? (2p)

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.) az u1 felhasználó (u1 aktív csoporttal) készít egy új fájlt d1-ben (touch d1/fu1), milyen csoport lesz a tulajdonosa a létrejövő fájlnak (2p)

g1 lesz, mert csoport setgid jel van az alkönyvtáron

d.) A root felasználó mely fájlokat tudja törölni az f1 alkönyvtárban (1p)

Az összeset, mert a root felhasználó speciális jogú

e.) Ki tudja végrehajtani sikeresen az f2 fájl olvasási jogának teljes törlését? (chmod a-r d1/f2) (1p)

u1, ő a tulajdonosa (és a root)

6. feladat

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 u4 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 d2/f4 fájlt és miért? (rm d2/f4) (2p)

csak u2, más nem írhat az alkönyvtárba (+root)

b.) Mely felhasználóknál fut le sikeresen a cp d2/f4 d2/f6 parancs? (2p)

csak u2, mert ő írhat d2-be, és tudja olvasni f4-et is.. (+root)

c.) Ki tudja módosítani az f2 fájl jogosultságait (pl. chmod o+w d1/f2) (2p)

csak a tulajdonos, u1 (és a root)

d.) Ki tudja lefuttatni a rm d1/f3; cp d1/f1 d1/f3 parancsokat mind sikeresen, azaz kitörlni f3-at és helyére f1-et másolni? (2p)

a törlést csak u1,u2 tudja elvégezni f1-et viszont ebből csak u1 olvashatja, ő írni is tud az alkönyvtárba, tehát csak u1. (+root)

7. feladat

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-x 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 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:/adatbizt# 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

a.) Mely felhasználók tudják olvasni a d1/f1 fájlt és miért? (2p)

csak u1, neki van olvasás joga és a directory-ba is be tud lépni

b.) Mely felhasználóknál fut le sikeresen a cp d1/f2 d2/f6 parancs? (2p)

u2, root, mert: g1 és u1 tudja olvasni f2-t, joguk van belépni d2-be, ott fájlt azonban u2 tud csak csinálni.

c.) Ki tudja módosítani az f2 fájl jogosultságait (pl. chmod o+w d1/f2)? (3p)

csak a tulajdonos, u1 (és a root)

d.) 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)

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)

8. feladat

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 2

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 u4 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 d2/f4 fájlt és miért? (rm d2/f4) ű

csak u2, más nem írhat az alkönyvtárba (+root)

b.) mely felhasználóknál fut le sikeresen a cp d2/f4 d2/f6 parancs?

csak u2, mert ő írhat d2-be, és tudja olvasni f4-et is.. (+root)

c.) ki tudja módosítani az f2 fájl jogosultságait (pl. chmod o+w d1/f2)

csak a tulajdonos, u1 (és a root)

d.) ki tudja lefuttatni a rm d1/f3; cp d1/f1 d1/f3 parancsokat mind sikeresen, azaz kitörli f3-at és helyére f1-et másolja?

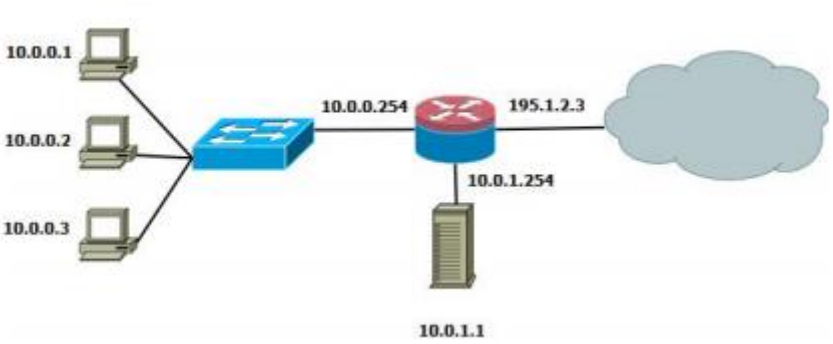
a törlést csak u1,u2 tudja elvégezni f1-et viszont ebből csak u1 olvashatja, ő írni is tud az alkönyvtárba, tehát csak u1. (+root)

e.) g2 csoport tagjai mely fájlokat tudják olvasni d1 alkönyvtárban (mindegyikük) a fenti eredeti listából? (15p)

f2,f3

Tűzfal

1. feladat



Az ábrán látható elrendezésben szeretnénk a Linux alapú tűzfalat bekonfigurálni. A belső hálózaton a gépek a 10.0.0.0/24 hálózatban vannak. A DMZ-ben (10.0.1.0/24) egy webszerver működik a 10.0.1.1-es címen. A tűzfal lábai a következők: eth0 kifelé, eth1 befelé, eth2 a DMZ irányába. Írjon iptables parancsokat a következő formátumban a részfeladatok megoldásához (a paraméterek sorrendjét lehetőleg ne változtassa meg, az alapértelmezett szabályokra ne alapozzon): iptables [-t TÁBLANÉV] -A LÁNC [-p PROTOCOL] [-i INIF] [- o OUTIF] [-s SOURCE] [--sport SPORT] [-d DESTINATION] [-- dport DPORT][--to ADD:PORT] -j ACTION

a) A belső hálózaton lévő gépek elérhetik a webszerver HTTP portját a DMZ-ben, és az válaszolhat is, ha az interfészek és a címek megfelelőek (állapotmentes megoldást írjon, 2 parancs) (2 p).

iptables –A FORWARD –p tcp –i eth1 –o eth2 –s 10.0.0.0/24 –d 10.0.1.1 –dport 80 –j ACCEPT

iptables –A FORWARD –p tcp –i eth2 –o eth1 –s 10.0.1.1 –sport 80 –d 10.0.0.0/24 –j ACCEPT

b) A tűzfalon futó SSH szerver csak a belső hálózatból kaphasson csomagot, és a tűzfal mint feladó általában is csak a belső hálózatnak küldhessen csomagot (ügyeljen a megfelelő lánc választásra, az interfészeket nem kell megadni, 4 parancs) (4 p).

a. iptables –A INPUT –p tcp –s 10.0.0.0/24 –dport 22 –J ACCEPT

b. iptables –A INPUT –p tcp –dport 22 –J DROP

c. iptables –A OUTPUT –d 10.0.0.0/24 –J ACCEPT

d. iptables –A OUTPUT –J DROP

c) A webszerver a külső hálózatból is elérhető legyen a nyilvános cím megfelelő portjain (HTTP és HTTPS forgalom is lehetséges legyen, 2 parancs) (4 p)

a. iptables –t NAT –A PREROUTING –p tcp –d 195.1.2.3 –dport 80 –to 10.0.1.1:80 –J DNAT

b. iptables –A PREROUTING –p

d) A tűzfalon áthaladó bármilyen LDAP-nak címzett forgalom (389-es port) logolva legyen (1 parancs). (1 p)

iptables –A FORWARD –dport 389 –j LOG

e) Sorolja fel, hogy ingress szűrés esetén milyen szabályokra lenne szükség (elég mondatban, nem kell szabály, 2 mondat). (1 p)

a. Külső interfészről nem érkezhet csomag belső címes feladóval

b. Külső interfészről nem érkezhet csomag DMZ címes feladóval

2. feladat

UDP portszkennelést végzünk egy gépen, 1000 lehetséges portra. Minden porton egy kísérletet végzünk, és max. 5 másodpercig várunk a válaszra, utána sikertelennek tekintjük a tesztet. A célgépen 100 UDP port van nyitva, ezekről a válasz kéréseinkre 1 másodperc alatt érkezik meg. A tesztelést 5 szálon végezzük el. A szkennelő gép sebességét tekintsük végtelennek.

a.) Mennyi a minimális idő, ami alatt a portszkennelés lefut és miért? (3p)

A portszkennelés összesen 100 nyitott port esetében 1-1 másodpercig tart (100 sec), 900 zárt portra 5-5 másodpercig (4500 sec), összesen 4600 sec. 5 szálon ezt optimális esetben ez 920 másodperc alatt lefut.

b.) Ha naív módon úgy implementáljuk a szkennelést, hogy előre beosztjuk melyik szál melyik portot fogja ellenőrizni, mekkora lehet a leggyorsabb és a leglassúbb szál futási ideje közötti különbség a legrosszabb esetben? (4p)

Rossz esetben lesz olyan szál, amelyik 200 db. 5 másodperces futást fog kapni és egyetlen 1 másodperceset sem, így az a szál 200x5 = 1000 másodperc alatt fut le. Egy szerencsés szál megkapja mind a 100 db. 1 másodperc alatt lefutó feladatot, és így 100 x 1 s + 100 x 5 s = 600 s alatt is végezhet. A különbség 400 s.

3. feladat

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)

pl. 5-ös szabályt árnyékolja a 3-as

b.) Generalization (2p)

pl. 6-os a 2-essel

c.) Correlation (2p)

pl. 7-es a 4-essel

4. feladat

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	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

a.) Shadowing (2p)

pl. 4-es szabályt árnyékolja a 2-es

b.) Generalization (2p)

pl. 7-es a 4-est

c.) Correlation (2p)

pl. 2-es a 6-ossal

5. feladat

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 szerver 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 szervereket 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 szervereket 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 Mbit/sec /66.7 = 30 745 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)

6. feladat

Keressen példát az alábbi tűzfal szabályhalmazban a következő inkonzisztenciatípusokra, és válaszát röviden indokolja!

#	prot	source	destination	action
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

a.) Shadowing (3p)

shadowing e.g., rule 4 is shadowed by rule 2; rule 5 is shadowed by combination of rule 1 and rule 3;

b.) Generalization (3p)

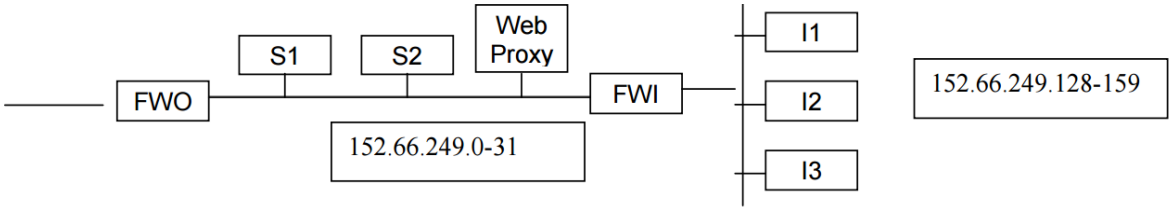
generalization e.g., rule 7 is a generalization of rule 4,…

c.) Correlation (3p)

correlation pl. rule 2 and rule 6 are correlated

7. feladat

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

a.) Új féreg terjed az interneten, a 445-ös portra csatlakozást használva mindenkit feltör. Mi fog történni a DMZ-nkben és a belső hálózatunkban? (2p)

Az égvilágon semmi, a 445-ös portra nem lehet csatlakozni egyik hálózatunkban sem

b.) I3 gépen egy támadó program fut. S2 web szerverén futó alkalmazás ellen akar SQL injection támadást intézni, van rá lehetősége? (4p)

U3 csatlakozni tud a web proxyra, az pedig az S2-re, ha a web szerver tényleg hibás, feltörhető valóban.

c.) I3 gépen futó támadó program az interneten levő szerverek felé spam üzeneteket próbál továbbítani. Meg tudja ezt tenni? (2p)

Természetesen képes rá, FWI engedi, FWO mindent enged kifelé.

d.) 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)

Hiába törték fel S1-et, befele FWI nem enged SSH kapcsolódást így nem lehet kísérletezni, így a támadás esélye 0 a feltételek mellett.

8. feladat

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.) A 152.66.249.0-255 tartományból lehessen a 8090-es TCP portot elérni, máshonnan nem

pl. Rossz a tiltás és engedélyezés sorrendje, így az engedélyezés nem aktív

b.) A védett hálózat felé az SNMP protokollt (161 UDP és TCP portok) a 152.66.249.0/27 hálózatból szabad elérni, máshonnan nem

A rendszergazda elírta az cél IP tartományt a tiltó szabályban, 249 helyett 149-et írt.

c.) A nem használt TCP és UDP portok 1000 alatt a védett hálózat irányában tiltva legyenek, amelyekre nincs specifikus egyéb szabály

Elfelejtette letiltani az UDP protokoll portjait az 11. (utolsó előtti) szabályban

d.) A DNS szolgáltatás (53-as TCP és UDP port) kívülről elérhető legyen, de csak a DNS szerveren (152.66.249.135) (12p)

A harmadik szabályban a cél helyett a forrás lett beírva, vagy más értelmezésben a teljes szabály hiányzik

9. feladat

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	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

a.) Shadowing (2 pont)

pl. 4-es szabályt árnyékolja a 2-es

b.) Generalization (2 pont)

pl. 7-es a 4-est

c.) Correlation (2 pont)

pl. 2-es a 6-ossal