

Pécsi Tudományegyetem
Műszaki és Informatikai kar
Rendszer és Szoftvertechnológiai Tanszék

CSALÁS DETEKTÁLÁS SIP ALAPÚ TELEFONKÖZPONTON

LANG VINCE

Készítette: Lang Vince

Évfolyam: Mérnökinformatikus BSC 4.

Belső Konzulens: Gyurák Gábor

Beosztás: mesteroktató

Külső Konzulens: Forray László

Beosztás: VoIP és alkalmazásfejlesztési csoportvezető

TARTALOMJEGYZÉK

1. Tartalom

1.	Tartalom	2
2.	Bevezetés és célkitűzés:.....	4
2.1.	Elméleti és gyakorlati jelentősége:	4
2.2.	Célkitűzés	5
3.	Alapfogalmak	6
3.1.	VoIP.....	6
3.2.	SIP és PJSIP	6
3.3.	Fraud Detection	6
3.4.	Port Knocking.....	7
4.	IP-alapú telefonközpontok áttekintése	8
4.1.	FreePBX	8
4.2.	MikoPBX.....	9
4.3.	Asterisk.....	9
5.	Tervezés.....	10
5.1.	Felkészülés	10
5.2.	Az eszközök.....	11
6.	Szerver konfigurálása	13
6.1.	Asterisk telepítése.....	13
6.2.	Port knocking implementálása	13
6.3.	Fontos portok átkonfigurálása	13
7.	Konfigurációs fájlok felépítése.....	14
7.1.	MySQL Connector – ODBC (Open Database Connectivity).....	14
7.2.	ODBC Function.....	14

7.3.	PJSIP konfiguráció	14
7.4.	Dial Plan	15
8.	Csalásdetektálás konfigurációja és óvintézkedések	17
8.1.	Csalásdetektálás jelentősége és küszöbértékek kiválasztása	17
8.2.	Kiberbiztonsági tudatosság: Az emberi hiba csökkentése.....	17
8.3.	Adatok szerepe a csalásdetektálásban	17
8.4.	Küszöbértékek meghatározása	18
8.5.	Gyanús viselkedés felismerése	18
8.6.	Védelmi mechanizmusok	19
9.	Védelem kivitelezése.....	20
9.1.	Alap küszöbérték meghatározása	20
9.2.	Küszöbérték csökkentése EU-n belüli hívások alapján.....	20
9.3.	Alkalmazás és finomhangolás	21
9.4.	Gyanús tevékenységek azonosítása	21
9.5.	További védelem és téves letiltások kezelése.....	21
10.	További fejlesztések	22
10.1.	Mesterséges intelligencia alkalmazása	22
10.2.	Átfogó cégszintű aktivitásfigyelés.....	22
10.3.	Előnyök.....	23
11.	Irodalomjegyzék	24
12.	Felhasznált képek	25
13.	Köszönetnyilvánítás	26
14.	Nyilatkozat	27

2. Bevezetés és célkitűzés:

2.1. Elméleti és gyakorlati jelentősége:

A Voice over IP (VoIP) technológia jelentős áttörést hozott a telekommunikációban, hiszen az internetes hálózatokon keresztüli kommunikációval nemcsak költséghatékonyabbá tette a hanghívásokat, hanem lehetővé tette az integrációt más digitális rendszerekkel is, mint például a videokonferencia vagy az üzenetküldés, ami tovább növeli alkalmazási területüket az üzleti és magánszférában egyaránt. A technológia népszerűsége azonban nemcsak előnyöket, hanem komoly biztonsági kihívásokat is magával hozott. [1] Az egyik legsúlyosabb ilyen probléma az illetéktelen fiókhozzáférés, amely során támadók megszerzik a felhasználók hitelesítési adatait, majd ezekkel jogosulatlan hívásokat kezdeményeznek, gyakran jelentős anyagi károkat okozva.

Azonban a VoIP technológia elterjedése új biztonsági kihívásokat is magával hozott. Az internetalapú kommunikáció sebezhetővé válhat különböző támadásokkal szemben, mint például az adathalászat, a szolgáltatásmegtagadási támadások (DDoS), vagy a céges hálózatba történő illetéktelen behatolás. Különösen aggasztóak az olyan csalási formák, mint a Toll Fraud és a Phreaking, amelyek során támadók jogosulatlanul használják a vállalati telefonrendszereket, gyakran jelentős anyagi károkat okozva. [2]

Az ilyen jellegű csálások rendkívüli pénzügyi terhet rónak a cégekre. Egyes becslések szerint évente több milliárd dolláros kárt okoznak világszerte, különösen azoknak a vállalkozásoknak, amelyek nagy volumenben használnak VoIP szolgáltatásokat. A védekezés és a károk megelőzése tehát nemcsak a biztonság, hanem a gazdasági fenntarthatóság szempontjából is kiemelt jelentőségű.

Az ilyen fenyegetések felismerése és megelőzése érdekében létfontosságú olyan fraud detection megoldásokat kidolgozni, amelyek valós időben képesek azonosítani a szokatlan aktivitásokat, például a hirtelen megnövekedett hívásforgalmat vagy a gyanús földrajzi helyekről érkező hozzáférési kísérleteket. Ezen rendszerek bevezetése nemcsak a pénzügyi veszteségek csökkentéséhez járul hozzá, hanem a felhasználók és ügyfelek bizalmának fenntartásában is kulcsszerepet játszik.

A kutatásomban nagy szerepet játszott a Pécsi Tudományegyetem Műszaki és Informatikai Karával együttműködő TARR Kft., amely egy 100%-ban magyar tulajdonú távközlési szolgáltató. Tevékenységi körei közé tartozik a digitális kábeltévé, internet, valamint a vezetékes és mobiltelefon szolgáltatás. Nagy problémát okoz náluk a már említett „telefonos díjcsalás” vagy „hívásköltség-csalás”. Mint más internet alapú telefonközpontnál is, Magyarországon is nagy problémákat okoznak ezek a fajta csalás típusok. TARR Kft.-nél akár havi 400-500 ezer Forint-os számlázási többletet kell kifizetnie a szolgáltatónak.

Legnagyobb megpróbáltatásuk abban mutatkozott ki, hogy internet alapú telefonos kommunikációjú szolgáltatást biztosítanak a megrendelő cégeknek és náluk akár feltöréses támadással, vagy social engineering-el (pszichológiai manipulációval) illetéktelenek szerzik meg a bejelentkezési információkat. Ezekből a hibákból adódóan a fenyegető aktorok (threat actors) végre tudják hajtani azokat a támadásokat, amelyek során jogosulatlan hívásokat kezdeményeznek, rendszerint magas költségű nemzetközi vagy prémiumszámokra.

2.2.Célkitűzés

A szakdolgozat célja egy hatékony fraud detection rendszer kidolgozása az Asterisk-alapú VoIP telefonközpontok számára, amely képes felismerni és megelőzni az illetéktelen fiókhozáféréseket és a kapcsolódó csalási tevékenységeket, mint például a Toll Fraud és a Phreaking. A kutatás során az alábbi célokat kívánom elérni:

- A VoIP rendszerek biztonsági réseinek azonosítása és a megelőzésükhöz szükséges konfigurációs változtatások kidolgozása, beleértve az erős jelszavak alkalmazását, az IP-alapú hozzáférési szabályok bevezetését és a naplózási mechanizmusok optimalizálását.
- Egy valós idejű figyelő- és riasztórendszer fejlesztése, amely képes gyorsan azonosítani a szokatlan eseményeket és megfelelő védelmi intézkedéseket tenni.
- Az eseménynaplók és a hívásrészletező adatok elemzése alapján riasztási mechanizmusok kidolgozása, amelyek az anomáliák felismerésére alapozva csökkentik a kockázatokat.
- Egy felhasználóbarát riportáló rendszer létrehozása, amely megkönnyíti a rendszergazdák számára a gyanús tevékenységek kezelését és nyomon követését.

3. Alapfogalmak

3.1.VoIP

A VoIP (Voice over Internet Protocol) technológia lehetővé teszi a hangalapú kommunikációt az interneten keresztül, megszüntetve a hagyományos telefonhálózatok függőségét. A VoIP rendszerek IP-alapú protokollokat használnak a hangadatok csomagokra bontására és továbbítására, ami költséghatékonyabb és rugalmasabb kommunikációt biztosít. Az előnyei közé tartozik a földrajzi függetlenség, a könnyű integráció más informatikai rendszerekkel, például CRM-ekkel, és az alacsonyabb hívási költségek. Ugyanakkor a VoIP sebezhetőségei, mint például az illetéktelen hozzáférések vagy a hívásmanipuláció, komoly biztonsági kockázatot jelentenek.

3.2.SIP és PJSIP

A SIP (Session Initiation Protocol) a VoIP rendszerek alapvető protokollja, amelyet hívások kezdeményezésére, kezelésére és bontására használnak. A SIP egyszerűsége és széles körű kompatibilitása miatt népszerű, de korlátozott funkcionalitást kínál, különösen nagyobb, összetettebb rendszerekben.

A PJSIP a SIP egy modern implementációja, amely több fejlett funkciót biztosít, például jobb skálázhatóságot és egyszerűbb konfigurációt. Támogatja a többregisztrációs kapcsolatot, a bővített NAT kezelést és az aszinkron híváskezelést. Míg a SIP-t gyakran kisebb rendszereknél használják, a PJSIP előnyeit főleg komplex, nagyobb méretű rendszereknél, például Asterisk-alapú környezetekben lehet kiaknázni.

3.3.Fraud Detection

A Fraud Detection rendszerek célja a VoIP rendszerekben előforduló csalások, például az illetéktelen fiókhozzáférések, a Toll Fraud vagy a Phreaking felismerése és megelőzése. Ezek a rendszerek jellemzően a hálózati forgalom és a hívásrésztelező adatok elemzésére építenek. Az észlelés alapja lehet az anomáliák figyelése, például szokatlan hívási minták, ismétlődő bejelentkezési kísérletek vagy ismeretlen IP-címekről érkező hozzáférések. A Fraud Detection rendszerek riasztásokat generálhatnak és automatikusan blokkolhatják a

gyanús aktivitásokat, jelentősen csökkentve a pénzügyi károk és a szolgáltatás megszakításának kockázatát.

3.4.Port Knocking

A Port Knocking egy hálózatbiztonsági technika, amely hatékony védelmet nyújt a port szkennelő robotok szemben is. Ezek a botok általában szekvenciálisan próbálnak nyitott portokat találni a rendszeren, de a Port Knocking koncepciója ezt megakadályozza azáltal, hogy a portok addig nem jelennek meg nyitottként, amíg a helyes "kopogási" sorrendet végre nem hajtják. Ez a sorrend egy előre meghatározott, titkosított séma szerint történik, amely több port érintését is magában foglalhat különböző sorrendben.

Mivel a tapogatózó botok általában nem képesek az ilyen speciális szekvenciák követésére, és az általuk használt algoritmusok nem készülnek fel a Port Knocking logikájára, a technika hatékonyan akadályozza meg az illetéktelen hozzáférési kísérleteket. Ezáltal nemcsak a brute-force támadások, hanem a potenciálisan veszélyes forgalom előzetes észlelése és blokkolása is megvalósítható, miközben a rendszer teljesen rejtve marad a jogosulatlanok előtt.

4. IP-alapú telefonközpontok áttekintése

Az internetes telefonközpontok (IP PBX – Internet Protocol Private Branch Exchange) olyan távközlési rendszerek, amelyek a hagyományos telefonhálózatok helyett internetes protokollt (IP) használnak a hangalapú kommunikáció lebonyolítására. Ezek a rendszerek lehetővé teszik a belső és külső hívások kezelését egyetlen, központosított platformon, miközben támogatják az olyan modern szolgáltatásokat, mint a videóhívások, az üzenetküldés, a hangposta és a konferenciahívások.

Az IP-alapú telefonközpontok gazdaságosabb alternatívát jelentenek a hagyományos PBX rendszerekkel szemben, mivel csökkentik a hívási költségeket, egyszerűbb integrációt tesznek lehetővé más digitális rendszerekkel, és könnyen skálázhatók a vállalati igényeknek megfelelően. A legnépszerűbb platformok közé tartozik a FreePBX, a MikoPBX és az semmiből felépített saját konfigurálású Asterisk szerver, amelyek mindegyike különböző előnyöket és funkciókat kínál.

4.1.FreePBX

A FreePBX egy nyílt forráskódú, webalapú felügyeleti felülettel rendelkező IP telefonközpont, amely az Asterisk rendszeren alapul. Elsősorban kis- és középvállalkozások számára készült, és egyszerű telepítést, valamint könnyű kezelhetőséget biztosít. A FreePBX lehetővé teszi az adminisztrátorok számára, hogy grafikus felületen keresztül konfigurálják a hívásirányítási szabályokat, a mellékeket, a hangpostát és egyéb szolgáltatásokat, így minimális műszaki tudással is használható.

A rendszer támogatja a SIP protokollt, a hangposta e-mailes továbbítását, valamint a rugalmas hívásirányítást. Emellett számos kiegészítő modul érhető el hozzá, amelyek további funkciókkal bővítik, például híváskövetéssel vagy CRM integrációval. A FreePBX előnye a rugalmasság és az alacsony költség, míg hátránya, hogy nagyobb rendszerek esetében bonyolultabb konfigurációt igényelhet.

4.2.MikoPBX

A MikoPBX egy zárt forráskódú, professzionális IP telefonközpont megoldás, amelyet kifejezetten vállalati környezetek számára terveztek. Az egyik fő előnye a felhasználóbarát felület és az egyszerű telepítés, amely akár percek alatt beállítható a felhasználói igényekhez. A MikoPBX erőteljes biztonsági funkciókkal rendelkezik, például tűzfalintegrációval, és lehetővé teszi az adminisztrátorok számára a jogosulatlan hozzáférések egyszerű blokkolását.

A rendszer támogatja a távoli elérést és az automatikus frissítéseket, amelyek biztosítják a folyamatos működést és a naprakész biztonsági javításokat. A MikoPBX ideális választás lehet azoknak a cégeknek, amelyek előnyben részesítik a zárt forráskódú megoldásokat és a professzionális támogatást. Hátránya, hogy kevésbé testreszabható, mint a nyílt forráskódú alternatívák, és magasabb licencköltségekkel járhat.

4.3.Asterisk

Az Asterisk az egyik legismertebb és legszélesebb körben használt nyílt forráskódú IP telefonközpont megoldás, amelyet digitális és analóg telefonhálózatok kezelésére egyaránt alkalmaznak. Rugalmasságának köszönhetően az Asterisk lehetőséget biztosít arra, hogy teljesen egyedi telefonrendszereket hozzunk létre, így szinte bármilyen igényre szabható. [3]

A rendszer támogatja a SIP, PJSIP és más VoIP protokollokat, valamint számos hagyományos távközlési protokollt is. Az Asterisk lehetővé teszi komplex funkciók megvalósítását, például IVR (Interactive Voice Response), konferenciahívások, automata hívásirányítás, valamint valós idejű hívásmonitorozás. Az adminisztrációhoz többféle felhasználói felület is elérhető, például a FreePBX.

Az Asterisk legnagyobb előnye, hogy teljes mértékben testreszabható és skálázható, azonban használata magasabb szintű technikai tudást igényel. Emiatt leginkább olyan vállalkozások és szakemberek választják, akik részletes kontrollt szeretnének a telefonrendszerük felett, és nem riadnak vissza a mélyebb technikai beállításoktól.

5. Tervezés

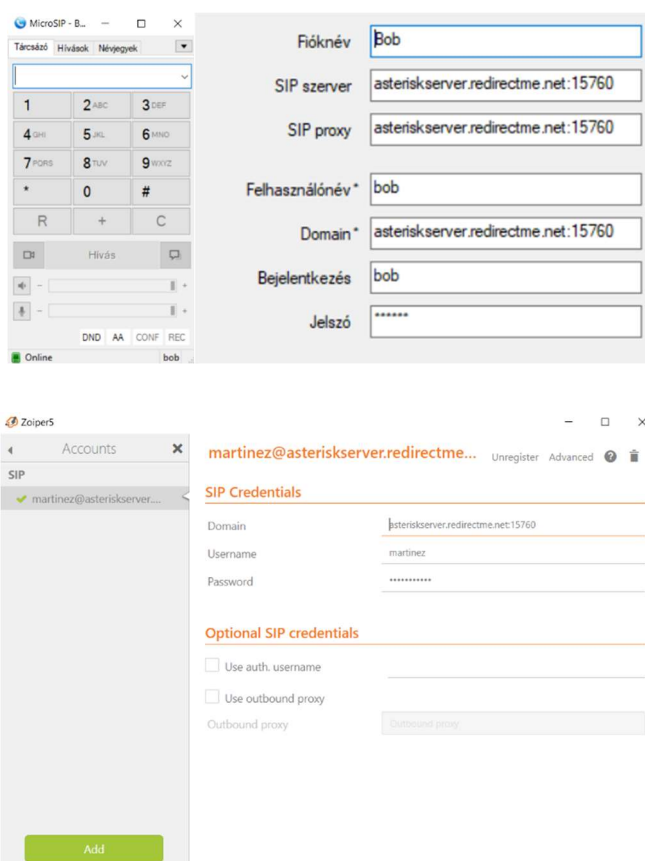
5.1.Felkészülés

A VoIP-alapú telefonközpontok tervezésekor számos szempontot kell figyelembe venni, hogy a rendszer hatékonyan működjön és ellenálló legyen a lehetséges kihívásokkal szemben. Az alábbi területek különösen fontosak:

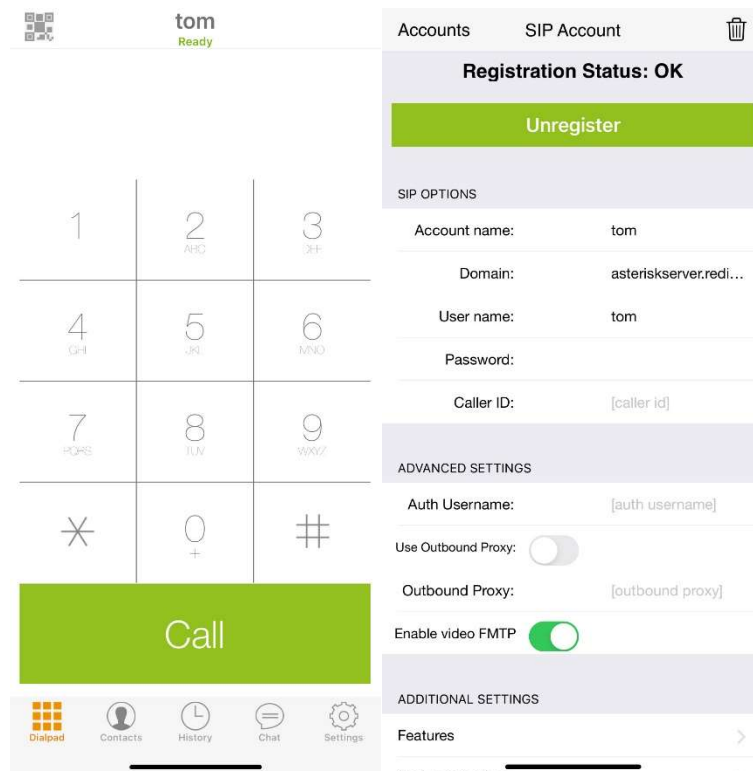
- Biztonsági kihívások: A VoIP rendszerek fokozottan ki vannak téve a támadásoknak, mint például az illetéktelen hozzáférések, brute-force támadások, Toll Fraud vagy Phreaking. A tervezés során kiemelt figyelmet kell fordítani az erős hitelesítési mechanizmusokra, például jelszó-erősségi követelmények bevezetésére és IP-alapú hozzáférési szabályokra.
- Hálózati infrastruktúra: Megfelelő sávszélesség és alacsony késleltetés szükséges a jó minőségű hang- és videohívások biztosításához. Továbbá, a hálózatnak támogatnia kell a QoS (Quality of Service) mechanizmusokat, hogy prioritást biztosítson a valós idejű kommunikációnak.
- Skálázhatóság: A rendszer tervezésekor figyelembe kell venni a jövőbeni bővítési lehetőségeket, hogy a telefonközpont képes legyen kezelni a növekvő számú felhasználót és a forgalomnövekedést.
- Kompatibilitás: Fontos, hogy a választott telefonközpont rendszer kompatibilis legyen a meglévő hardverrel és szoftverrel, például IP-telefonokkal és SIP-trónkökkel.
- Monitoring és naplózás: A rendszernek rendelkeznie kell olyan valós idejű monitorozási és naplózási funkciókkal, amelyek lehetővé teszik a problémák gyors felismerését és a csalási tevékenységek azonosítását.

5.2. Az eszközök

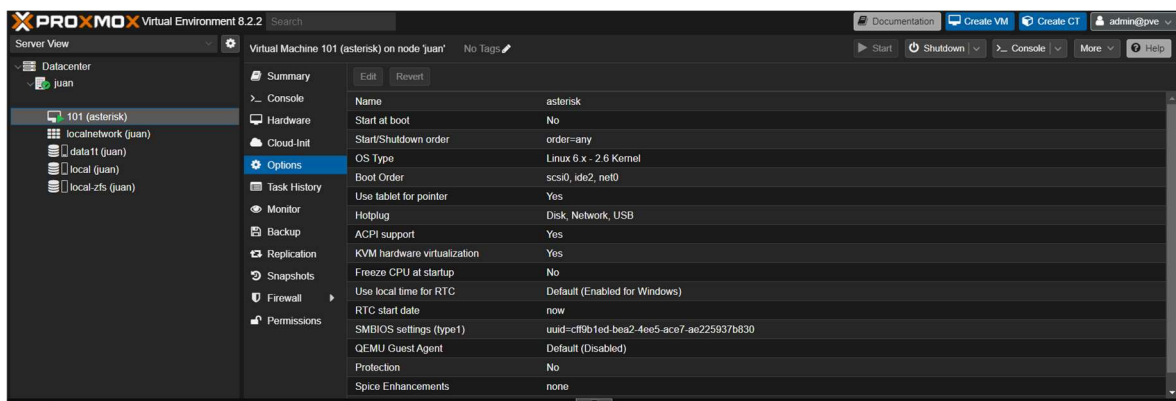
Az Asterisk szerver egy Proxmox platformon futtatott Debian operációs rendszerű virtuális gép, amelyet a Tarr Kft. üzemeltet. A szerver hardverkonfigurációja magában foglal egy 1 Gb/s sebességű hálózati kártyát, 5 GB RAM-ot, 4 CPU magot és 40 GB tárhelyet, így biztosítva a VoIP-alapú telefonközpont hatékony működését. A virtuális gép publikus IP-címmel rendelkezik, amely lehetővé teszi a külső hálózatokkal való közvetlen kapcsolódást, például SIP-trónkók és távoli felhasználók csatlakozását. A Proxmox környezet rugalmas és megbízható alapot nyújt a rendszer futtatásához, biztosítva az egyszerű menedzsmentet és a zavartalan működést. Ezen felül a SIP Klienseket telepítettem saját számítógémemre (Zoiper, MicroSIP), valamint IOS-es készülékekre (Zoiper).



5.2.1. MicroSIP és Zoiper alkalmazások



5.2.2. IOS-es Zoiper alkalmazás



5.2.3. Proxmox kezelőfelület

6. Szerver konfigurálása

A projekt keretében egy Debian alapú szervert konfiguráltam, amelyre telepítettem az Asterisk VoIP rendszert. A cél az volt, hogy egy biztonságos és megbízható környezetet hozzak létre, amely védi a rendszert az illetéktelen hozzáférési kísérletektől és támadásoktól.

6.1. Asterisk telepítése

Az Asterisk telepítését a hivatalos Debian csomagkezelő rendszer segítségével végeztem el. A telepítés után konfiguráltam a SIP protokollt és a PJSIP modult, amelyek lehetővé teszik a VoIP-alapú kommunikációt. A beállítás során külön figyelmet fordítottam a felhasználói hitelesítés erősítésére, például erős jelszavak és IP-alapú hozzáférés-szabályok használatával.

6.2. Port knocking implementálása

A szerver biztonságának fokozása érdekében port knocking technikát implementáltam az SSH hozzáférés védelmére. Ez a megoldás lehetővé teszi, hogy a szerver alapértelmezetten zárt SSH portja csak egy előre meghatározott "kopogási" szekvenciát követően váljon elérhetővé. Ez hatékony védelmet nyújt a brute-force támadások és tapogatózó botok ellen, mivel az SSH port nem látható a jogosulatlan felhasználók számára.

6.3. Fontos portok átkonfigurálása

A biztonság növelése érdekében a legfontosabb szolgáltatások alapértelmezett portjait átkonfiguráltam. Az alábbi módosításokat hajtottam végre:

- SSH: Az alapértelmezett 22-es portot áthelyeztem egy nem szabványos, magasabb portszámra (50382/TCP), hogy elkerüljem az automatizált támadásokat.
- SIP/PJSIP: Az alapértelmezett 5060-as port helyett egy egyedi portot állítottam be a SIP kommunikációhoz (15760/UDP), csökkentve ezzel a VoIP rendszerekre irányuló támadások kockázatát.
- MySQL: Az alapértelmezett 3306-os portot egyedi értékre cseréltem (43947/TCP), hogy a MySQL adatbázis is védve legyen a szokásos portokon történő támadásoktól.

7. Konfigurációs fájlok felépítése

A VoIP rendszerek működése során az Asterisk konfigurációs fájljai biztosítják a rendszer alapvető beállításait, a különböző modulok közötti kommunikációt, valamint a híváskezelés szabályait. A következő fájlok kiemelt szerepet töltenek be az Asterisk rendszer működésében és a hívástörténetek visszatekintésében.

7.1.MySQL Connector – ODBC (Open Database Connectivity)

Ennek a fájlnak nagy szerepe van abban, hogy a SIP kliensek és maga a szerver honnan kérje le, vagy hol módosítsa az adatokat. Debian alapú rendszerben nem létezik a mysql-connector-odbc nevű pakege-et, így manuálisan, útmutató segítségével kellett letölteni, majd konfigurálni azt. [4]

7.2.ODBC Function

A func_odbc.conf fájlban egyedi adatbázis-függvények hozhatók létre, amelyek segítségével dinamikusan kezelhetők az ODBC-MySQL adatbázisban tárolt adatok. Az itt megadott lekérdezések lehetővé teszik, hogy az Asterisk valós időben érje el és módosítsa az adatbázis tartalmát. Például egy hívásszámláló funkció létrehozható, amely minden bejövő híváskor frissíti a felhasználói adatokat.

```
[CHECK_NOT_EU_CALL_COUNT]
dsn=asterisk-connector
readsql=SELECT not_eu_calls FROM call_counts WHERE user_id='${SQL_ESC(${ARG1})}'

[INCREMENT_NOT_EU_CALL_COUNT]
dsn=asterisk-connector
writesql=UPDATE call_counts SET not_eu_calls=not_eu_calls+1 WHERE user_id='${SQL_ESC(${VAL1})}'

[CHECK_EU_CALL_COUNT]
dsn=asterisk-connector
readsql=SELECT eu_calls FROM call_counts WHERE user_id='${SQL_ESC(${ARG1})}'

[INCREMENT_EU_CALL_COUNT]
dsn=asterisk-connector
writesql=UPDATE call_counts SET eu_calls=eu_calls+1 WHERE user_id='${SQL_ESC(${VAL1})}'
```

7.3.PJSIP konfiguráció

A pjsip.conf fájl szolgál arra, hogy megadjuk a Internetes hívás által használt protokoll típusát, portját, külső elérési címét és a felhasználói ügynököt, amely a webes tartalmak

lekéréséért és a végfelhasználóval való interakció megkönnyítéséért felel. A globális beállításokon kívül itt tudjuk létrehozni a felhasználói fiókokat, amelyekhez meghatározhatjuk a jogosultságokat, a hozzáférési szabályokat és a kommunikációs paramétereket. Ezek a fiókok lehetővé teszik, hogy a felhasználók a rendszer funkcióit egyedi igényeik szerint használják, miközben a biztonsági követelményeknek is megfelelnek.

A profilok alkalmazásával a fiókokhoz alapbeállításokat rendelhetünk, amelyek a közös konfigurációkat egyszerűsítik, például a kodekek, a csatlakozási szabályok vagy a hangposta paramétereinek egységesítése révén. Ugyanakkor lehetőség van egyedi beállítások megadására is, például külön jelszavak, IP-alapú korlátozások vagy eltérő hívási szabályok használatára, amelyek a személyre szabott hozzáférést biztosítják.

```
[global]
type=global
user_agent=Asterisk
transport=transport-udp

[transport-udp]
type=transport
protocol=udp
bind=0.0.0.0:15760
external_media_address = asteriskserver.redirectme.net
external_signaling_address = asteriskserver.redirectme.net
local_net = 192.168.1.0/24

;===TOM extension
[tom](endpoint-basic)
auth=tom
aors=tom
callerid=Tom <+36301234567>

[tom](auth-userpass)
password=tom123
username=tom

[tom](aor-single-reg)

;=====ENDPOINT TEMPLATES

[endpoint-basic](!)
type=endpoint
context=extensions
disallow=all
allow=ulaw,alaw,gsm

[endpoint-outside](!)
type=endpoint
context=outside
disallow=all
allow=ulaw,alaw

[auth-userpass](!)
type=auth
auth_type=userpass

[aor-single-reg](!)
type=aor
max_contacts=2
```

7.3.1. PJSIP konfiguráció részlet

7.4.Dial Plan

Az extensions.conf fájl az Asterisk rendszer dial planjának alapvető konfigurációs fájlja. A dial plan határozza meg, hogyan kezeli és irányítja a rendszer a bejövő és kimenő hívásokat. Ez egy logikai szabályrendszer, amely lépésről lépésre meghatározza, hogy a különböző mellékek és hívási helyzetek esetén milyen műveletek történjenek.

Fő funkciója a hívásátirányítás, valamint itt lehet meghivatkozni a fucn_odbc.conf fájlban megadott funkciókat és az adatbázisból való olvasási értékeket visszakapni vele, vagy innen írni az adatbázisba. Továbbá rugalmassága lehetővé teszi, hogy az egyedi igényekhez és folyamatokhoz megfelelően igazítsuk a híváskezelést. Magát a csalás detektálás funkcióját is meg lehet itt valósítani, akár külső script-ek nélkül is.

```
[[globals]]
CURRENT_DATE=${STRFTIME(${EPOCH},,%Y-%m-%d)}

[extensions]
exten => 06301234567,1,Goto(extensions,+36301234567,1)
exten => 06301234568,1,Goto(extensions,+36301234568,1)
exten => 06301234569,1,Goto(extensions,+36301234569,1)
exten => 00551199999999,1,Goto(+551199999999,1)

exten => +36301234567,1,NoOp(Calling Tom)
same => n,GoSub(check_mynumber,s,1)
same => n,Dial(PJSIP/tom,,g)
same => n,NoOp(CDR állapot: ${DIALSTATUS})
same => n,GoSub(checkifanswered_eu,s,1)
same => n,Hangup

exten => +36301234568,1,NoOp(Calling Jerry)
same => n,GoSub(check_mynumber,s,1)
same => n,NoOp(${ODBC_GET_AVG_OF_FRAUD_COUNTRIES(${CALLERID(name)}}))
same => n,Dial(PJSIP/jerry,,g)
same => n,NoOp(CDR állapot: ${DIALSTATUS})
same => n,GoSub(checkifanswered_eu,s,1)
same => n,Hangup
```

7.4.1. Részlet a Dial Planból

8. Csalásdetektálás konfigurációja és óvintézkedések

8.1.Csalásdetektálás jelentősége és küszöbértékek kiválasztása

A VoIP rendszerekben a csalásdetektálás alapvető célja a szokatlan és gyanús tevékenységek azonosítása és megfelelő kezelése. Az illetéktelen hozzáférés nemcsak technikai támadások, például brute-force módszerek vagy rendszerek feltörése révén történhet, hanem az emberi tényezők szerepe is jelentős. Gyakori probléma a gyenge jelszavak alkalmazása, a figyelmetlenség vagy a kiberbűnözők által alkalmazott megtévesztő taktikák, mint például az adathalászat és a social engineering.

8.2.Kiberbiztonsági tudatosság: Az emberi hiba csökkentése

A felhasználók oktatása és képzése kiemelten fontos a VoIP rendszerek biztonságának megőrzése érdekében is. A vállalatok számára ajánlott kiberbiztonsági tréningek keretében az alkalmazottak megismerhetik a leggyakoribb támadási technikákat, mint például az adathalászat vagy az álcázott információszerzési kísérletek (social engineering). Az ilyen képzések lehetőséget adnak arra, hogy a felhasználók tisztában legyenek a gyenge jelszavak használatából adódó kockázatokkal, és megtanulják, hogyan hozzanak létre erős, egyedi jelszavakat. Emellett hangsúlyt kell fektetni a gyanús e-mailek és üzenetek felismerésére, valamint a hitelesítési folyamatok biztonságos kezelésére. [5]

Az oktatás során bemutatathatók a támadók által alkalmazott módszerek, miközben gyakorlati példákon keresztül tanulhatják meg az alkalmazottak, hogyan reagáljanak helyesen a potenciális fenyegetésekre. Ezek az intézkedések hozzájárulnak ahhoz, hogy a felhasználók magabiztosabban és felelősségteljesebben kezeljék a biztonsági helyzeteket. Az ilyen programok nemcsak az egyéni hibalehetőségeket csökkentik, hanem hosszú távon a vállalat teljes biztonsági szintjét is emelik, biztosítva a VoIP rendszerek megbízhatóságát és ellenállóképességét.

8.3.Adatok szerepe a csalásdetektálásban

A csalásdetektálás hatékonysága nagyban múlik a rendelkezésre álló adatokon. Minél több adat áll rendelkezésre, annál pontosabban meghatározhatók azok a minták és határértékek,

amelyek alapján az anomáliák felismerhetők. Például egy felhasználói fiók, amely korábban rendszeresen EU-n belüli hívásokat bonyolított, hirtelen nagy mennyiségű hívást kezd kezdeményezni EU-n kívüli, magas kockázatú országokba. Ez a viselkedés gyanúsabbnak tekinthető, mint ha egy újonnan létrehozott fiók indítaná ugyanezeket a hívásokat, hiszen a meglévő mintázatból való eltérés kockázatosabb tevékenységet jelezhet.

8.4. Küszöbértékek meghatározása

A küszöbértékek kiválasztása az egyik legfontosabb lépés a családetektáló rendszer kialakításában. Ezek a határértékek határozzák meg, hogy milyen szintű aktivitást tekint a rendszer normálisnak, és mikor indítson gyanús tevékenység miatt riasztást. Az ilyen küszöbértékek meghatározásakor figyelembe kell venni a hívási mintákat, az adott fiók szokásos viselkedését, valamint a célországok kockázati besorolását.

- Hívásszám EU-n kívüli országokba: A rendszer figyelheti, hogy egy adott időszakon belül hány hívás indul olyan országokba, ahol prémiumszolgáltatások érhetők el.
- Kockázatos célországok: A Cyber Dependent Crimes Index [6] adatai alapján azonosíthatók azok az országok, amelyek magasabb kockázatot jelentenek. Ezekbe az országokba irányuló hívásokra szigorúbb küszöbértékeket lehet beállítani.

A küszöbértékek dinamikus beállításával elérhető, hogy a rendszer érzékeny legyen a normától való eltérésekre, miközben minimalizálja a téves riasztások számát.

8.5. Gyanús viselkedés felismerése

A gyanús tevékenység azonosítása során a rendszer nemcsak a célországokat és a hívásszámokat veszi figyelembe, hanem a felhasználói fiók előzményeit is. Ha egy fiók korábban kizárólag belföldi vagy EU-n belüli hívásokat kezdeményezett, majd hirtelen nagy mennyiségű hívást indít EU-n kívüli prémiumszámokra, az nagy valószínűséggel gyanús tevékenységet jelez. Ezzel szemben egy újonnan létrehozott fiók esetében az EU-n kívüli hívások nem feltétlenül tekinthetők anomáliának, mivel az ilyen fiókoknál még nincs kialakult normális viselkedési minta.

Az ilyen viselkedések azonosítása segíthet abban, hogy a rendszer gyorsan reagáljon a lehetséges visszaélésekre, például az IP-alapú korlátozások bevezetésével.

8.6.Védelmi mechanizmusok

A csalásdetektáló rendszer lépésenként reagál a gyanús tevékenységekre:

1. Elsődleges védelem: Az azonosított gyanús tevékenység esetén a rendszer először az érintett IP-címet tiltja le, hogy megakadályozza a további hozzáférési kísérleteket az adott címről.
2. Fiók védelem: Ha a támadó új IP-címről próbálkozik, és a gyanús tevékenység folytatódik, a rendszer automatikusan deaktiválja a felhasználói fiókot, megakadályozva a további visszaéléseket.

9. Védelem kivitelezése

Az EU-n belüli hívások figyelése alapvető szerepet játszik a nem EU-s hívások maximális küszöbértékének dinamikus kezelésében. A módszer célja, hogy az EU-n belüli hívások számának növekedésével arányosan csökkentse azt az értéket, amely meghatározza, hogy egy adott fiók hány nem EU-s hívást kezdeményezhet anélkül, hogy a rendszer gyanús tevékenységként érzékelne.

9.1. Alap küszöbérték meghatározása

Az alap küszöbérték kis mintánál 14, amelyet az országok crime score-ja alapján számoltam ki. Ezek a crime score-ok egy adott ország kiberbűnözési kockázatát jelölik, és a Cyber Dependent Crimes Index [7] adatain alapulnak. Az értékek átlagolása alapján, valamint a Tarr Kft. külső konzulensével egyeztetve alakult ki ez az induló érték. Az alap küszöbérték figyelembe veszi a rendszer általános forgalmát és a bűnözési kockázatokat, azonban szükség esetén az aktuális adatok és hívási minták alapján tovább finomítható.

9.2. Küszöbérték csökkentése EU-n belüli hívások alapján

Az EU-n belüli hívások számának növekedésével a nem EU-s hívások maximális küszöbértékét az alábbiak szerint csökkentjük:

- 50 és 75 közötti EU-n belüli hívás esetén: A nem EU-s hívások küszöbértékéből 2 hívási mennyiséget vonunk le.
- 75 és 100 közötti EU-n belüli hívás esetén: A nem EU-s hívások küszöbértékéből 4 hívási mennyiséget vonunk le.
- 100 és 150 közötti EU-n belüli hívás esetén: A nem EU-s hívások küszöbértékéből 6 hívási mennyiséget vonunk le.
- 150 és 200 közötti EU-n belüli hívás esetén: A nem EU-s hívások küszöbértékéből 8 hívási mennyiséget vonunk le.
- 200 fölötti EU-n belüli hívás esetén: A nem EU-s hívások küszöbértékéből 10 hívási mennyiséget vonunk le.

Például, ha az alap küszöbérték 14, és egy fiók EU-n belüli hívásainak száma eléri a 100-at, a nem EU-s hívásokra vonatkozó küszöbérték 14-ről 8-ra csökken.

9.3. Alkalmazás és finomhangolás

Ez a módszer biztosítja, hogy a rendszer dinamikusan alkalmazkodjon a felhasználók szokásos viselkedéséhez, miközben az anomáliákat hatékonyan azonosítja. Az alap küszöbérték és a csökkentési arányok pontos beállításához rendszeres adatgyűjtés és elemzés szükséges, amelyet a Tarr Kft. konzulense által ajánlott megközelítések és a privát cégek által biztosított diagnosztikai adatok segítenek finomhangolni.

9.4. Gyanús tevékenységek azonosítása

A módszer figyelembe veszi a felhasználói viselkedés kontextusát is. Például:

- Ha egy fiók korábban kizárólag EU-n belüli hívásokat bonyolított le, majd hirtelen nem EU-s prémiumszámokra kezdeményez nagy mennyiségű hívást, az gyanús tevékenységként azonosítható.
- Az újonnan létrehozott fiókok esetén a rendszer kevésbé érzékeny az EU-n kívüli hívásokra, mivel nincs előzetes minta, amihez viszonyítani lehetne.

A cél az, hogy minimalizáljuk a téves riasztásokat, miközben hatékonyan felismerjük a potenciális visszaéléseket.

9.5. További védelem és téves letiltások kezelése

Amennyiben a rendszer tévesen tiltana le egy fiókot, lehetőséget biztosít a felhasználók számára, hogy az üzemeltetővel felvegyék a kapcsolatot a probléma megoldása érdekében. Az üzemeltető az eset kivizsgálása után feloldhatja a tiltást, és szükség esetén finomhangolhatja a rendszer beállításait a hasonló helyzetek elkerülése érdekében.

10. További fejlesztések

10.1. Mesterséges intelligencia alkalmazása

A mesterséges intelligencia a versenyszférában egyre nagyobb szerepet tölt be, mivel nemcsak a hatékonyságot növeli, hanem lehetőséget ad a folyamatos innovációra és a döntéshozatal minőségének javítására is. Számos vállalat a mesterséges intelligenciát a versenyelőny elérésének egyik kulcsfontosságú eszközeként értékeli, ugyanakkor alkalmazását akadályozhatják az erőforrások korlátozottsága és a megfelelő technológiai tudás hiánya. Az MI nemcsak a biztonság és a csalásdetektálás terén játszik kulcsszerepet, hanem hosszú távon a fenntartható fejlődést és a vállalatok globális versenyképességét is elősegíti. [8]

A csalásdetektálás hatékonyságának növelése érdekében érdemes megfontolni a mesterséges intelligencia (AI) technológiák alkalmazását. Az AI-alapú rendszerek képesek a nagy mennyiségű hívásadatot automatikusan elemezni, és mintázatokot azonosítani, amelyek emberi szem számára nem mindig láthatók. Az olyan gépi tanulási algoritmusok, mint a felügyelt tanulás (supervised learning) vagy a mélytanulás (deep learning), lehetővé teszik az anomáliák korai felismerését, például a szokatlan hívási minták vagy a gyanús IP-címek aktivitásának észlelését.

Az AI továbbá adaptívan képes finomhangolni a küszöbértékeket, figyelembe véve a rendszer folyamatosan változó forgalmi mintáit. Ezáltal a mesterséges intelligencia nemcsak az aktuális fenyegetések kezelésére alkalmas, hanem a rendszer előrejelző képességét is javítja, minimalizálva a potenciális károkat.

10.2. Átfogó cégszintű aktivitásfigyelés

Amennyiben a kidolgozott megvalósítás során több felhasználói fiókot is feltörtek volna, érdemes a rendszert cégszintű szintre kiterjeszteni. Ez azt jelenti, hogy az egyes fiókok aktivitásán túl a vállalat egészének hívási mintáit és viselkedését is átfogóan figyelni kell. Az ilyen átfogó megközelítés lehetővé teszi a globális anomáliák, például szokatlan forgalomnövekedések vagy koordinált támadások felismerését.

A cégszintű monitorozás során az alábbi szempontokat érdemes figyelembe venni:

- Aggregált forgalmi minták elemzése: A teljes vállalati hívásforgalom összesítése és az anomáliák azonosítása.
- Globális küszöbértékek bevezetése: Az egész vállalatra kiterjedő hívási szabályok kialakítása, például a nem EU-s hívások összesített korlátozása.
- Fiókok közötti kapcsolat elemzése: Az egyes fiókok tevékenységének összevetése, hogy azonosíthatók legyenek a kapcsolódó vagy összefüggő támadások.

10.3. Előnyök

Az AI bevezetése és a cégszintű aktivitásfigyelés kiterjesztése számos előnnyel jár:

- Hatékonyabb családetektálás: Az AI-alapú rendszerek gyorsabbak és pontosabbak, mint a manuális szabályalapú megközelítések.
- Proaktív védelem: A mesterséges intelligencia segítségével a rendszer nemcsak reagál a támadásokra, hanem előre jelzi a lehetséges fenyegetéseket is.
- Egységesített biztonság: A vállalati szintű monitorozás biztosítja, hogy minden fiók és részleg összehangoltan védve legyen, csökkentve a rést a fiókok között.

11. Irodalomjegyzék

- [1] J. S. Marcus, C. Wernick és E. Dieter, The regulation of Voice over IP (VoIP) in Europe, Bad Honnef: WIK-Consult, 2008.
- [2] Kyung-Il Kim, N.-W. Cho, T. Kim és M. Kim, „Toll Fraud Detection of VoIP Service Networks in Ubiquitous Computing Environments,” p. 6, 2015.
- [3] Sangoma, „The Asterisk Project,” Sangoma, [Online]. Available: <https://docs.asterisk.org/>. [Hozzáférés dátuma: 16 október 2024].
- [4] MySQL, „MySQL Documentation,” Oracle, [Online]. Available: <https://dev.mysql.com/doc/>. [Hozzáférés dátuma: 26 október 2024].
- [5] R. Gyarak, *A biztonságtudatosság szerepe, avagy kérdések a kiberbiztonságról*, Budapest, Pest: Magyar Rendészet, 2022.
- [6] M. Shaw, N. Kaysser, F. M. Underwood, G. Macfadyen, A. Sergi, S. Betti, S. Chin, K. Amerhauser, M. McLaggan, M. Hunter, R. Scaturro, J. Eligh és S. Broad, „Global Organized Crime Index,” Global Initiative, 2023. [Online]. Available: https://ocindex.net/rankings/cyber-dependent_crimes?f=rankings&view=List&group=Country&order=DESC&continent=1&criminality-range=0%2C10&state-range=0%2C10
- [7] K. Amerhauser, M. McLaggan és M. Hunter, Measuring the Scope and Scale of Economic Crimes and Illicit Financial Flows, Genf: Global Initiative Against Transnational Organized Crime, 2023.
- [8] A. Zakariás, *Mesterséges intelligencia a versenyszférában: vállalati attitűdök és akadályozó tényezők*, Budapest: Gazdaság- és Vállalkozáskutató Intézet, 2024.

12. Felhasznált képek

5.2.1.	MicroSIP és Zoiper alkalmazások.....	11
5.2.2.	IOS-es Zoiper alkalmazás.....	12
5.2.3.	Proxmox kezelőfelület.....	12
7.3.1.	PJSIP konfiguráció részlet.....	15
7.4.1.	Részlet a Dial Planból	16

13. Köszönetnyilvánítás

Elsősorban szeretném megköszönni Gyurák Gábor tanár úr motivációját, fáradhatatlan felkészítését és bizalmát, hogy elkészíthessem ezen a projektet. Nélküle, illetve az ő általa átadott tudás nélkül nem tudtam volna megvalósítani ezt a projektet.

Emellett szeretnék köszönetet mondani Forray Lászlónak, a TARR Kft. VoIP és alkalmazásfejlesztési csoportvezetőjének, hogy sűrű időbeosztása mellett is tudott nekem segíteni a projekt megvalósításban és koordinálásában.

Végül, szeretném megköszönni kedves páromnak, valamint hallgató társaimnak a megannyi biztatásukat és türelmüket, illetve az általuk létrehozott környezetet, ahol el tudtam készíteni a projektet.

14. Nyilatkozat

Alulírott, Lang Vince, a Tudományos Diákköri dolgozat készítője, aláírásával nyilatkozik, hogy a következők igazak és érvényesek a saját Tudományos Diákköri dolgozatra:

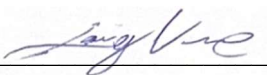
A jelen dolgozat teljes egészében és kizárólag az alulírott munkája, saját gondolatai és kutatási eredményei alapján készült.

A felhasznált irodalmi forrásokat teljes körültekintéssel és tisztességes módon kezelte, megfelelően hivatkozott rájuk a dolgozat megfelelő részeiben, és elkerülte a plágiumot.

A munkája során minden vonatkozó jogszabályt, egyetemi irányelvet és etikai szabályt betartott.

Ezen nyilatkozattal az alulírott kijelenti, hogy a Tudományos Diákköri dolgozat a saját eredeti munkája, és semmilyen módon nem sérti mások szellemi tulajdonjogait vagy etikai normáit.

Dátum: 2024. 12. 04.

Aláírás: 

Lang Vince