HADMÉRNÖK

VII. Évfolyam 2. szám - 2012. június

Papp Zoltán
pappz.szeged@gmail.com

A SZÁMÍTÓGÉP-HÁLÓZATOK TŰZFALAINAK TÁMADÁSA

Absztrakt

A számítógép-hálózatok kiterjedésének növekedésével, illetve összetettségének fejlődésével, valamint a rajtuk futó szolgáltatások és alkalmazások számának emelkedésével együtt nőtt azon veszélyforrások száma is, melyeket kihasználva illetéktelenek hozzáférhetnek a számítógépeken kezelt adatokhoz, módosíthatják az alkalmazások futtatási paramétereit, különböző jogosultságokat szerezhetnek maguknak. A számítógépekre leselkedő veszélyek elhárításának alapvető eszközei a tűzfalak, melyek feltérképezése, illetve kiiktatása, vagy működésüknek korlátozása elsődleges cél lehet egy rendszer támadásának megkezdéseként.

Along with the increasing penetration and complexity of computer networks as well as the growing number of applications and services supported by them, the number of potential threat sources has also increased, which can be abused by unauthorized persons to gain access to the data stored and handled on these computers, to modify the execution parameters of the applications and to obtain various authorizations. The fundamental tools for protecting computers from threats are firewalls, the mapping and elimination of which, or the limitation of their operation may be the primary objective for beginning the attack on a system.

Kulcsszavak: *tűzfal, számítógép-hálózatok támadása ~ firewall, computer-network attack*

BEVEZETŐ

A számítógépek az információs társadalom életének minden területén megjelentek, és összekapcsolásuk révén egyre nagyobb – bár nem homogén – információs rendszerek alakultak ki. Napjainkban gyakorlatilag már minden szervezet, akár gazdasági társaság, akár államigazgatási, rendészeti szerv csatlakozik az Internethez, ami elengedhetetlen feltétele annak, hogy a működésükhöz szükséges információs folyamatok hatékonysága elérje a kívánt szintet. Az érintett szervezetek a hálózataik összekapcsolódása révén irányítják földrajzilag távol lévő szervezeti egységeiket, cserélnek adatot velük, és persze tartják a kapcsolatot ügyfeleikkel.

A hatékonyság és a gyorsaság, összességében pedig a gazdaságosság szempontjából a különböző rendeltetésű szervezetek egyike sem engedheti meg magának, hogy ne csatlakozzon az Internethez, élvezze annak előnyeit, azonban az előnyök mellett számos kockázat is felmerülhet. A szervezetek információs folyamatainak, illetve az általuk nyújtott szolgáltatások akadályozása, valamint a rendszereikben kezelt értékes információk megszerzése különböző motivációkkal bíró támadók célja lehet. Az információkon alapuló szolgáltatások kiesése konkrétan is megfogalmazható, akár számszerűen is leírható társadalmi, egyéni, gazdasági és katonai érdekeket sérthet, ami miatt ezeknek a rendszereknek a védelme kiemelt feladata minden országnak, költségvetési, rendvédelmi, katonai és gazdasági szervezetnek.

Az információs rendszerekben alkalmazott biztonsági eszközök, megoldások közül a tűzfalak tekinthetők a hálózatok első védelmi vonalának, így ezek érzékelhetik az esetleges támadásokat először, ami azt is jelenti egyben, hogy ezek a hálózat ellen indított támadások első célpontjai.

TŰZFALAK

A tűzfalak alkalmazásának célja, hogy központosítsa a számítógép-hálózatban lévő hoszt hozzáféréseit, hardveres és szoftveres megoldások révén akadályozza meg az illetéktelen behatolást, illetve a határfelületen keresztül áramló forgalmat megszűrje. A hálózatot ért támadás kiküszöbölése alapvetően nem cél, de a behatolás valószínűségét hatékonyan tudják csökkenteni.

A hálózatvédelemben a tűzfalak alkalmazásával:

- ellenőrzési pontok létesíthetők mind a kimenő, mind pedig a bejövő forgalom megfigyelése, szűrése és forgalmi statisztikák készítése céljából;
- a rendszerben lévő hosztok száma, struktúrája elrejthető a támadók elöl;
- az esetleges támadótevékenység detektálhatóvá válik, így hatékony riasztó- és megfigyelőrendszer alakítható ki;
- lehetőség van a felhasználók azonosítására;
- a szolgáltatások egyetlen kommunikációs ponton engedélyezhetők,
- az engedélyezett műveletek köre alkalmazásonként szabályozható, naplózható;
- egy szervezetnek telephelyei között lehetősége van automatikus titkosításra [1:239].

A hardverkomponensek olyan hálózatfelosztó eszközök lehetnek, mint a router vagy a proxy.

A routerek, vagyis az útválasztók feladata, hogy egy otthoni hoszt, vagy pedig egy szervezet hálózata és az Internet, vagy pedig egyes országok közötti hálózatok összekapcsolja, azok közötti adatforgalmat irányítsa. A számítógépes hálózatok működését legelterjedtebben leíró OSI (Open Systems Interconnection) modell réteges struktúrájában a router a harmadik, úgynevezett hálózati rétegben működik. A számítógép-hálózatok forgalma különböző típusú adatcsomagokban zajlik, melyek a feladótól a címzettig akár több eszközön is

keresztülutaznak. A továbbítás során minden érintett eszköznek tudnia kell, hogy milyen irányba küldje tovább a fogadott csomagot, továbbá döntéseket is kell hoznia amennyiben több útvonal is ismert. A routerek végzik az adatcsomagok megfelelő irányba való továbbítását, és hozzák meg az útirányokra vonatkozó döntéseket.

A proxy szerverek a számítógép-hálózatokban köztes elemként a kliensek kéréseit továbbítják más szerverek felé. A kliens csatlakozva a proxy szerverhez, és valamilyen szolgáltatást – csatlakozást, adatletöltést (fájlt, weboldalt), vagy más erőforrást – igényel, ami egy másik szerveren található. A proxy szerver a kliens helyett csatlakozik a megadott szerverhez, és megigényli a szolgáltatást számára. A proxy esetlegesen megváltoztathatja a kliens kérését vagy a szerver válaszát, és alkalomadtán kiszolgálhatja a kérést a szerverhez való csatlakozás nélkül is [2].

A proxy szerverek azonban kliensek hatékonyabb kiszolgálás túl kiválóan alkalmasak arra is, hogy anonim hozzáférést biztosítsanak bizonyos szolgáltatásokhoz, ami nem szükségszerűen jelent jogtalan, vagy jogellenes felhasználást. Az anonim hozzáférések egyfajta plusz védelmet nyújtanak a hálózaton a rosszindulatú támadóként fellépő hosztok ellen. A különböző hálózati szolgáltatásokat használó alkalmazások aktivitásuk során IP azonosítókat, jelszavakat, cookie adatokat hagynak hátra, melyeket megszerezve a támadók képesek lehetnek az adott kommunikációs csatornát támadni. Ilyen esetekben a tűzfalak nem tudnak teljes biztonságot nyújtani, ezért a rosszindulatú személyek és programok előtt azonosíthatatlan, az IP címet rejtő módon kell kommunikálni, amire több lehetőség is rendelkezésre áll:

- A grátisz (ingyenes) proxy szerverek igénybevétele lehet a legegyszerűbb és legolcsóbb megoldás, melyek egyszerű közvetítőként működnek a felhasználó és a szolgáltatást nyújtó kiszolgáló között. A cél URL-t a proxy hívja meg, így a felhasználó paraméterei a lekérdezett szerver számára nem válnak ismertté, csak a proxy kapcsolati azonosítóját látja. Ez a kapcsolati módszer azonban nem minden esetben megbízható, mivel némely alkalommal épp a támadók próbálják meg az ingyenes hozzáférés ígéretével a gyanútlan felhasználó adatait megszerezni.
- A kereskedelmi anonimizáló megoldások – fentiekkel azonos működési elv mellett – lényegesen nagyobb biztonságot nyújtanak. Egyes szolgáltatások több ezer proxy szerver szolgáltatását integrálják magukba.
- Egy támadó szempontjából – mindkét szolgáltatási mód esetében – figyelembe veendő paraméter lehet a kérdéses proxy szerver logolási módszere, ami alapján a támadó azonosítható. Előzőek alapján a jogellenes felhasználók körében a "logolásmentes" proxy szerverek a legnépszerűbbek.
- A szintén ingyenes TOR (The Onion Router) anonimizáló kliens használatakor a felhasználó csatlakoztatja számítógépét a TOR hálózathoz, és így a többi felhasználóval együtt több száz mini proxy szerver egyesülését állítja elő. A kliens konfigurálható node-nak (amelyen csak adatok futhatnak át) vagy TOR-exit-nek (amelyen keresztül a kliens adatokat küldhet a hagyományos internetre). Itt a hálózat minden tagja titkosítva kommunikál egymással. A kezdeményező hoszt a kérését titkosítva több, véletlenszerűen kiválasztott node-on keresztül – node-onként továbbtitkosítva – eljuttatja el egy TOR-exit-nek, amely az igényelt adatokat lekérdezi, és a választ hasonló módon juttatja vissza a kezdeményezőnek. Az alkalmazott titkosítási protokollnak megfelelően a csatorna kiépítésében résztvevő node-k, TOR-exit-ek nem tudják, hogy honnan indult el az adatcsomag, és mit tartalmaz.

A fenti megoldás lehetővé teszi a hálózaton az anonim jelenlétet, de egyik legfőbb felhasználási területe a cenzúrázott internetes tartalmak megjelenítése.

A proxy szerverek alkalmazásának azonban van néhány hátránya is. A hosszabb "kerülőutak" megnövelik az adatcsomagok célba érkezésének idejét, lassítják az adott szolgáltatás elérését, továbbá vannak olyan internetes szolgáltatások (például fórumok, közösségi oldalak), melyek nem teszik lehetővé az anonim hozzáférést. További kockázati tényező, hogy a különböző weboldalakba, kliensekbe már számos beépített programot integráltak, melyek biztonsági réseinek felhasználásával a képzett támadók képesek kinyerni az eredeti IP-címet.

A szoftveres tűzfalak a védendő számítógépre telepítve a hardvereszközök funkcióit (szűrés, naplózás, állapotfigyelés, stb.) képesek szinte maradéktalanul elvégezni, azonban a védett hoszt erőforrásait jelentős mértékben leköthetik, így más funkciók hatékonyságát leronthatják, ezért célszerű mindig hardveres megoldást választani.

Tűzfalak csoportosítása:

- külső: a teljes helyi hálózatot részben elválasztja az internettől;
- belső: helyi hálózatnak egy különösen védendő részét zárja el annak többi részétől, így az internettől is;
- személyes: egy adott számítógépre elhelyezett szolgáltatás.

Tűzfalak típusai:

- Csomagszűrés: Ez minden hálózati-tűzfal alapfunkciója. Az adatcsomagok egyszerű szűrése a cél-port, valamint forrás- és célcím, egy – a tűzfal-adminisztrátor által előredefiniált – szabályrendszer alapján történik. A megvizsgál csomagok vagy továbbításra, vagy pedig megsemmisítésre kerülnek. A fejlett tűzfalak – a működési szabályaik feltérképezésének akadályozása érdekében – a kritikusnak ítélt csomagokat csendben dobják el, így a kérdéses kapcsolat visszajelzés megszakad, illetve létre sem jön.
- Állapot szerinti szűrés: Ez a típusú szűrés az előbb vázolt csomagszűrés egy kibővített formája, ami az OSI modell hetedik rétegében egy rövid vizsgálatot hajt végre, és minden adatcsomagról egy állapottáblát hoz létre, melynek segítségével felismeri az adatcsomagok közti összefüggéseket, és szükség esetén az aktív kapcsolathoz tartozó munkafolyamatokat le is állíthatja. Így a kapcsolat felépítése után a tűzfal az állapottábla segítségével felismeri, hogy a kliens és a külső rendszer közötti adatcsomag-forgalom a valós igényeket elégíti-e ki, így amikor a külső rendszer olyan adatokat küld, melyeket a belső kliens nem kért, akkor a tűzfal blokkolja az átvitelt.
- Alkalmazásszintű tűzfal: Az alkalmazásszintű tűzfalak az OSI modell magasabb rétegeinek információit is elemzik. A forgalomhoz tartozó – forrás, cél és szolgáltatás (például a HTTP kérésekben az URL hosszát és tartalmát) – adatokon túl figyelik az adatcsomagok tartalmát is. Ez a módszer lehetővé teszi az úgynevezett dedikált proxy-k alkalmazását is, melyek specializált tartalomszűrést és malware-szkennelést is lehetővé tesznek.
- Anonymus proxy: Az alkalmazás-szintű tűzfalak integrált proxykat használnak, melyek felépítik a kapcsolatot a kliensek és a célrendszerek között, gyakorlatilag harmadik félként épülnek be a kommunikációba. Mint fentebb vázoltuk a kiszolgáló szerver számára csak a proxy címe lesz látható, mint feladó, nem pedig a kliensé, ezért a helyi hálózat struktúrája nem feltérképezhető a külső rendszer irányából, így megakadályozható a közvetlen kapcsolat a külső és a védett hálózat között. Közvetítő szerepet játszik a kettő között: a belülről érkező kéréseket feldolgozza, majd azokkal azonos értelmű kérést küld a külső szerver felé, az azokra érkező

válaszokat pedig ugyanilyen módon továbbítja a belső hálózat felé. Elég biztonságosnak mondható és általában egyszerűen konfigurálható.

– Tartalomszűrés: A tűzfal egy tartalomszűrő használatával a kapcsolat hasznos adatait kiértékelni, illetve az áthaladó adatokat ellenőrizni tudja.
  Jellegzetes felhasználási területei:
    - URL-szűrés és vírusfigyelés. Mindkét feladathoz többnyire kiegészítő programokra (URL-szűrőre, víruskeresőre) van szükség, a tűzfalak általában nem tartalmazzák ezeket a lehetőségeket;
    - a lekért weboldalakról az ActiveX és JavaScript kiszűrése;
    - bizalmas céginformációk kiszűrése;
    - kulcsszavak alapján nem kívánt weboldalak zárolása;
    - nem kívánt (például: file-megosztási) alkalmazás-protokollok blokkolása.

- Behatolás-felismerő és megelőző rendszerek: A behatolás-felismerő rendszerek (IDS) és a behatolás-megelőző rendszerek (IPS) napjaikban már szinte minden tűzfalba kiegészítő funkcióként integrálva vannak. A tűzfalon átmenő kommunikációs minták alapján képesek felismerni a behatolási próbálkozásokat. A különbség az, hogy míg az IDS csak a támadást csak felismeri képes, addig az IPS blokkolni is tudja. Léteznek olyan megoldások is, melyek ideiglenes tűzfalszabályokat hoznak létre a támadótól érkező kapcsolat-felvételi kérelmek blokkolások érdekében.

Általános esetben egy modern tűzfal a fenti módszerek közül többet is alkalmaz, mivel ezek a hibrid megoldások hatékonyabban képesek növelni a kérdéses rendszer biztonságát.

TŰZFALAK TÁMADÁSA:

A támadók egyik fontos célja lehet – a kérdéses számítógépes-hálózat topológiájának megismerésén túl – az alkalmazott tűzfal szűrési szabályainak megismerése, mely információkból több előny kovácsolható. Felderíthető, hogy milyen típusú forgalom bonyolódik a tűzfalon, továbbá a szűrt portok ismeretében, azok megkerülésével is indítható támadás.

Különböző portszkennelési technikákkal (például TCP, TCP SYN, TCP FIN, UDP, FTP proxy, Snow blind, Zombie scan [3:11]) fel lehet deríteni a kérdéses hálózati berendezésen futó alkalmazásokat, illetve a zárt portok is azonosíthatóak, ha a célhoz vezető úton nincs tűzfal. Abban az esetben pedig, amikor alkalmaznak tűzfalat, akkor csak nyitott portokat lehet meghatározni.

A tűzfalszabályok felderítésének leghatékonyabb módja a FireWalk technika. Módszer elve azon alapszik, hogy a tűzfal távolságának (X) meghatározása után az adatcsomag fejlécének Time To Live (TTL) mezőjét X+1 értékre állítva a támadó szkennelést hajt végre az egyik porton, majd a tűzfal reakciójából következtet az érvényben lévő szabályra. Amennyiben a kérdéses portot átengedi a szabályrendszer, akkor a router továbbítani próbálja az adatcsomagot, de a lejárt TTL miatt ez sikertelen lesz, ezért egy ICMP Time-Exceeded üzenetet generál a forrásnak. A szűrt port esetében az adatcsomag azonnal eldobásra kerül, és a támadóhoz nem ér vissza semmiféle válasz. A fenti elvi módszer – a tűzfalak konfigurációinak sokrétűsége miatt – csak ritkán alkalmazható, ezért a gyakorlatban többféle fejlesztését, típusát alkalmazzák inkább [3:12].

A tűzfal szabályok felderítését követően a támadónak – az eredmények függvényében – többféle módszer áll rendelkezésére, hogy a védelmi rendszeren áthatoljon [4]:

– Tördelés: Az IP csomagok kis darabokra való tördelésével elérhető, hogy bizonyos tűzfalak figyelmen kívül hagyják az így álcázott csomagokat. A tördelt adatcsomagokat a tűzfalnak össze kell állítania ahhoz, hogy értelmezni és szűrni

tudja, azonban ez igen erőforrás-igényes művelet. A tördelés ellen védekezni kell, a legtöbb hálózatba a tördelt csomagok fogadása engedélyezve van, de erre csak speciális esetben van szükség, így célszerű tiltani, illetve korlátozni az adatcsomagok tördelést.

- Forrás routing: A forrás routing egy olyan forgalomirányító mechanizmus, ahol nem a közvetítő routerek, hanem a forrás határozza meg az utat a hoszthoz. Ez főként hálózati problémák kiküszöbölésére alkalmazható, azonban a célszámítógép megtámadására is használható. A támadó tudva a célszámítógépek közötti megbízható kapcsolatról, a forrás routingot felhasználhatja arra, hogy a veszélyes csomagokat a megbízható hosztról érkezettnek tűntesse fel. Az ilyen típusú biztonsági fenyegetés miatt a csomagszűrő routert könnyedén lehet úgy konfigurálni, hogy visszautasítsa a forrás route opciót tartalmazó csomagokat [5].
- Forrásport hamisítás: Ez a módszer csak egyszerű csomagszűrők ellen hajtható végre. Elve azon alapul, hogy e típusú tűzfalakon a válaszforgalmat is engedélyezni kell. Ilyen esetben ismert portok forrásként beállításával tetszőleges port elérhető a tűzfalon keresztül. Az állapot szerint szűrő tűzfalak nyomon követik a kapcsolatok irányait, és automatikusan engedélyezik a válaszforgalmat, a proxy tűzfalak esetében pedig a beépített protokollok nem engedélyeik a forgalmat.
- TCP, IP nem használt mezők, illegális értékek: A támadók találhatnak olyan, gyakorlatban nem használt, értelmetlen fejlécbeállításokat, amik átengedésre késztetik, vagy leállítják a tűzfalat. Ezek ellen a fölösleges szolgáltatások tiltásával, korlátozásokkal lehet védekezni.
- Támadás a tűzfal operációs rendszere ellen:A tűzfal operációs rendszere ellen is készülhet olyan – biztonsági hiányosságot kihasználó – program, mellyel a támadó képes hozzáférni a tűzfal konfigurációs beállításaihoz, amiből meg tudja ismerni a szabályokat, illetve képes is azokat módosítani.
- IPS támadása: Az egyes behatolás-megelőző rendszerek ideiglenes tűzfalszabályt hoznak létre, ami egy támadó IP-cím felől érkező összes további kapcsolódási próbálkozást blokkolja. Ha viszont a támadó hamis küldő-címmel ellátott csomagokat küld a rendszernek, akkor ezzel el tudja érni, hogy ne legyen hozzáférés a hamis című klienshez. Ezzel egymás után le tudja választani az összes címet a rendszerről, amelyekre épp szükség lenne a működéshez (DNS-szerver stb.).

ÖSSZEGZÉS

Az összekapcsolt és kiterjedt számítógép-hálózatok korában kiemelt fontosságú a rendszerek üzembiztonsága, illetve az azokban kezelt információk, valamint a rendszerek által nyújtott szolgáltatások folytonossága. Ezeknek a céloknak a megvalósításában a különböző típusú tűzfalak hangsúlyos szerepet kapnak. Fontos funkciójuk révén ezeknek a védelmi megoldásoknak, valamint működési szabályainak a felderítése, illetve az után megtévesztése, manipulációja és kiiktatása a számítógép-hálózatok elleni támadások első lépésben végrehajtandó feladata.

A tűzfalak ellen indított támadások alapját sok esetben az teszi lehetővé, hogy a konfigurációs beállítások a gyári, vagy szoftveres tűzfalak esetében a telepítési alapértékeken maradnak, és nincsenek a hoszt sajátosságainak figyelembe vételével beállítva. Általános alapelvként elmondható, hogy tűzfalak esetében minden fölösleges szolgáltatást le kell tiltani, alkalmazni kell a „minden tilos, ami nem engedélyezett” elvet. Erős szűrési szabályok használata mellett a tűzfal képességeiről, működési, paramétereiről, valamint a védendő hálózatrészről minél kevesebb információt kell szolgáltatni.

A védelmi rendszerek, így a tűzfalak is funkciójukat akkor tudják maradéktalanul betölteni, ha megfelelő biztonság politikai koncepcióba illesztve, a megfelelő képzettségű személyzet, a hálózat sajátosságainak megfelelő konfigurációban üzemelteti, és lehetőleg a technológia legmagasabb színvonalát képviselje.

Felhasznált irodalom

[1] Haig Zsolt, Várhegyi István - Hadviselés az információs hadszíntéren, Zrínyi Kiadó, Budapest 2008.,

[2] http://hu.wikipedia.org/wiki/Tűzfal_(számítástechnika) (letöltve: 2011. 07. 10.)

[3] Szabó István - Tűzfal szabályok felderítése, Híradástechnika LXI. Évfolyam 2006/5., ISSN *0018-2028*

[4] http://nmap.org/man/hu/man-bypass-firewalls-ids.html (letöltve: 2011. 07. 05.)

[5] http://www.itbiztonsag.hu/tuzfalak.html (letöltve: 2011. 07. 08.)