Jegyzőkönyv

Biztonság és védelem az informatikában c. tárgy

8. feladat

Készítette:

Csomor Bence, TVIK4I

2021.04.08.

**Personal Firewall működési módok**

A személyes tűzfal olyan alkalmazás, amely ellenőrzi a számítógép felé irányuló és onnan érkező hálózati forgalmat, engedélyezve vagy megtagadva a kommunikációt a biztonsági irányelvek alapján. Általában alkalmazásréteg-tűzfalként működik.

A személyes tűzfal méretarányosan különbözik a hagyományos tűzfalaktól. A személyes tűzfal általában csak azt a számítógépet védi, amelyre telepítve van, összehasonlítva egy hagyományos tűzfallal, amelyet általában két vagy több hálózat, például útválasztó vagy proxykiszolgáló közötti kijelölt interfészre telepítenek. Ennélfogva a személyes tűzfalak lehetővé teszik a biztonsági házirend meghatározását az egyes számítógépeknél, míg a hagyományos tűzfal vezérli a házirendet az általa összekapcsolt hálózatok között.

A tűzfalak segítenek megvédeni a belső hálózatot a hackerek ellen, A tűzfalnak azonban vannak bizonyos korlátai.

Ha a rendszert rosszindulatú programok, kémprogramok vagy hasonló szoftverek veszélyeztetik, ezek a programok a tűzfalat is kezelhetik, mivel mindkettő ugyanazon a rendszeren fut. Lehetséges, hogy ilyen módon megkerülhető vagy akár teljesen le is állítható a szoftveres tűzfal.

A tűzfal nem tud értesíteni, ha helytelenül van beállítva.

A tűzfal korlátozhatja az internetről való hozzáférést, de nem biztos, hogy megvédi a hálózatát a vezeték nélküli és a rendszerekhez való egyéb hozzáféréstől.

A tűzfalak és a virtuális magánhálózatok nem az egyetlen megoldás a magándokumentumok és e-mailek védelmére, amelyeket vagy egy szervezeten belül, vagy más, a szervezeten kívüli üzleti kapcsolattartóknak küldenek.

A létrehozott riasztások esetleg érzéketlenné tehetik a felhasználókat a riasztásokra azáltal, hogy figyelmeztetik a felhasználót az esetleg nem rosszindulatú tevékenységekre.

Az operációs rendszerrel vagy más kernel módú tűzfalakkal vagy biztonsági szoftverekkel együttműködő szoftver tűzfalak instabilitást és / vagy biztonsági hibákat okozhatnak.

**Személyi tűzfal módok:**

Interaktív mód:

Lehetővé teszi egyedi konfiguráció létrehozását a személyes tűzfalhoz. Ha kommunikációt észlel, és a kommunikációra nem vonatkoznak semmilyen szabályok, akkor egy ismeretlen kapcsolatot jelentő párbeszédablak jelenik meg. A párbeszédablak lehetőséget ad a kommunikáció engedélyezésére vagy megtagadására, és az engedélyezés vagy elutasítás döntése új szabályként menthető a személyes tűzfalhoz. Ha új szabály létrehozása mellett dönt, akkor az összes ilyen típusú jövőbeli kapcsolat engedélyezett vagy blokkolt lesz a szabály szerint.

Tanuló mód:

Automatikusan létrehozza és elmenti a szabályokat; ez a mód alkalmas a személyes tűzfal kezdeti konfigurálására. Nincs szükség felhasználói beavatkozásra, mert az ESET Endpoint Security előre meghatározott paraméterek szerint menti a szabályokat. A tanulási mód nem biztonságos, és csak addig kell használni, amíg a szükséges kommunikációra vonatkozó összes szabályt meg nem teremtették.

Előre definiált szabály alapú mód:

Az alapértelmezett mód. Ez a mód azoknak a felhasználóknak alkalmas, akik a tűzfal egyszerű és kényelmes használatát kedvelik, és nincs szükségük szabályok meghatározására. Létrehozhatók egyedi, felhasználó által definiált szabályok, de automatikus módban nem szükségesek. Az automatikus mód engedélyezi az adott rendszer összes kimenő forgalmát, és blokkolja a legtöbb bejövő forgalmat (kivéve a Trusted Zone forgalmának egy részét, az IDS és a speciális opciók / Engedélyezett szolgáltatások, valamint a bejövő forgalom válasza az ugyanazon távoli webhelyre irányuló legutóbbi kimenő kommunikációra engedélyezve).

Szabály alapú mód:

Blokkol minden olyan kapcsolatot, amelyet nem határoz meg egy speciális szabály, amely lehetővé teszi számukra. Ez a mód lehetővé teszi a haladó felhasználók számára, hogy olyan szabályokat definiáljanak, amelyek csak a kívánt és biztonságos kapcsolatokat engedélyezik. Az összes többi meghatározatlan kapcsolatot a személyes tűzfal blokkolja.

**Tesztelés:**

A tűzfalnak általában két feladata van, amelyek megvédik a számítógépet a külső támadásoktól, és biztosítják, hogy a programok ne használják vissza a hálózati kapcsolatot. A támadás elleni védelem teszteléséhez olyan fizikai számítógépet használunk, amely az útválasztó DMZ portján keresztül csatlakozik. Ez egy közvetlenül az internethez csatlakoztatott számítógép hatását eredményezi. Ez fontos a tesztelés szempontjából, mert az útválasztón keresztül csatlakoztatott számítógép gyakorlatilag láthatatlan az Internet egésze számára. Port tesztekkel és más webalapú tesztekkel találtuk el a tesztrendszert. A legtöbb esetben azt tapasztaljuk, hogy a tűzfal teljesen elrejti a tesztrendszert ezekből a támadásokból, az összes portot lopakodó módba állítva.

A beépített Windows tűzfal kezeli az összes port eltulajdonítását, így ez a teszt csak egy kiindulópont. De itt is különböző vélemények vannak. A Kaspersky tervezői nem látnak értéket a portok lopakodásában, amíg a portok zárva vannak, és a tűzfal aktívan megakadályozza a támadásokat.

A programkezelés a legkorábbi személyes tűzfalakon rendkívül praktikus volt. Valahányszor egy ismeretlen program megpróbált hozzáférni a hálózathoz, a tűzfal felugrott egy lekérdezéssel, amelyben megkérdezte a felhasználót, hogy engedélyezi-e a hozzáférést. Ez a megközelítés nem túl hatékony, mivel a felhasználónak általában fogalma sincs a helyes műveletről. A legtöbben csak mindent megengednek. Mások minden alkalommal a Blokk gombra kattintanak, amíg nem törnek meg néhány fontos programot; utána mindent megengednek. Ennek a funkciónak a gyakorlati ellenőrzését egy óra alatt kódolt apró böngésző segédprogram segítségével végezzük, amely mindig ismeretlen programnak minősül.

Néhány rosszindulatú program megkísérli megkerülni ezt a fajta egyszerű programvezérlést megbízható programok manipulálásával vagy álcázásával. Amikor találkozunk egy régi iskola tűzfalaival, szivárgás tesztnek nevezett segédprogramok segítségével teszteljük képességeit. Ezek a programok ugyanazokat a technikákat használják a programirányítás kikerüléséhez, de rosszindulatú teher nélkül. Egyre kevesebb olyan szivárgástesztet találunk, amelyek még mindig működnek a modern Windows verziókban.

A spektrum másik végén a legjobb tűzfalak automatikusan beállítják az ismert jó programok hálózati engedélyeit, kiküszöbölik az ismert rossz programokat, és fokozzák az ismeretlenek felügyeletét. Ha egy ismeretlen program megpróbál gyanús kapcsolatot létrehozni, a tűzfal ekkor beindul, hogy leállítsa azt.

A szoftver nem tökéletes és nem is lehet tökéletes, ezért a rossz fiúk keményen dolgoznak, hogy biztonsági réseket találjanak a népszerű operációs rendszerekben, böngészőkben és alkalmazásokban. Kihasználják a rendszer biztonságának veszélyeztetését a talált sebezhetőségek felhasználásával. Természetesen a kihasznált termék gyártója a lehető leghamarabb kiad egy biztonsági javítást, de amíg ezt a javítást ténylegesen nem alkalmazza, addig sebezhetővé válik.

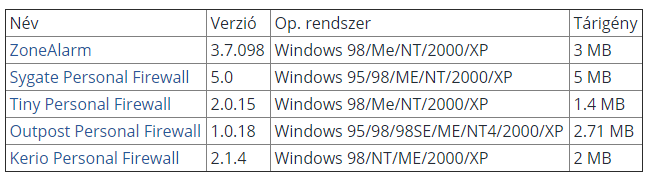
A legokosabb tűzfalak hálózati szinten fogják el ezeket a támadási támadásokat, így soha nem is érik el a számítógépet. Még azok számára is, akik nem keresnek hálózati szinten, sok esetben az antivírus-komponens eltörli az erőforrás rosszindulatú programjainak hasznos terhelését. A CORE Impact penetration eszközt arra használjuk, hogy minden tesztrendszert körülbelül 30 legutóbbi kihasználással érjünk el, és rögzítsük, mennyire védte őket a biztonsági termék.

Végül egy józan ész ellenőrzést hajtunk végre, hogy kiderüljön, egy rosszindulatú program-kódoló könnyen kikapcsolhatja-e a biztonsági védelmet. Egy be / ki kapcsolót keresünk a rendszerleíró adatbázisban, és teszteljük, hogy használható-e a védelem kikapcsolására (bár évek óta találunk egy terméket, amely sebezhető a támadás szempontjából). Megpróbáljuk leállítani a biztonsági folyamatokat a Feladatkezelő használatával. És ellenőrizzük, hogy lehetséges-e a termék alapvető Windows-szolgáltatásainak leállítása vagy letiltása.

Az ICSA Labs által minősített termékek közül érdemes tűzfalat választani.

De nagyon jó termékek találhatók az otthoni használatra szabadon letölthető tűzfalak között is. Ezek nemegyszer a kereskedelmi forgalomban lévő termék kissé lebutított változata.

Néhány otthoni felhasználásra szabadon letölthető tűzfal:



A Windows XP már tartalmazza az Internet Connection Firewall (ICF) nevű tűzfalat. Hátránya, hogy a számítógépünkről kimenő forgalmat nem szűri, azt feltételezve, hogy kifelé csak engedélyezett adat megy.

források:

<https://en.wikipedia.org/wiki/Personal_firewall>

<https://help.eset.com/ees/6/en-US/index.html?idh_config_epfw_basic_group.htm>

<https://www.pcmag.com/news/how-we-test-antivirus-and-security-software>

<https://www.cert.hu/szemelyes-tuzfalak-a-tiny-personal-firewall-hasznalata>