HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Szabó András
szaboandras@mil.hu

PREVENTÍV HÁLÓZATVÉDELMI RENDSZEREK ALKALMAZÁSI LEHETŐSÉGEI A TÁMADÁSOK DETEKTÁLÁSÁRA, VALAMINT A MÓDSZEREK ELEMZÉSÉRE
I. RÉSZ

Absztrakt

Elméleti kutatásokat, összehasonlítások, valamint kísérletek segítségével vizsgáltam a hálózatvédelmi módszerek (tűzfal, IDS / IPS, proxy szabályok) hatásfokának javítási lehetőségeit. A bemutatott módszerek az eddig ismeretlen támadási minták felismerésére és gyűjtésére alapulva végzik a biztonságot támogató tevékenységüket. Összefoglaltam a különböző honeypot típusokat, valamint többféle csoportosítás alapján értékeltem ezen rendszerek előnyeit, valamint hátrányait.

In my survey I explored, compared, and demonstrated methods to increase the efficiency of the network defense system (firewall and IDS/IPS, proxy rule set). These methods support the detection and collection of unknown malicious codes, and attack vectors. I summarized the different honeypot types as well as I categorized them based on different methods. I compared the pros and contras of these honeypot types.

***Kulcsszavak**: preventív, IT biztonság, kiber, hálózatvédelem, honeypot, megtévesztés, ~ preventive, IT security, cyber, network security, honeypot, deception*

A HÁLÓZATVÉDELEM KORSZERŰ MÓDSZEREI

A hálózatvédelmi képességek kutatása során gyakran találkozunk más tudományterületek tapasztalatainak felhasználásával: a számítógépes vírusok kutatói párhuzamot vontak saját kutatásaik és a biológia eredményei között (Járványtan, Immunológia stb.), a mesterséges intelligencia kutatás az agy működésének feltárásával párhuzamosan fejlődik stb. Így nem meglepő, hogy a hadtudomány eredményei, módszerei is bizonyos mértékben alkalmazhatóak a virtuális tér védelmére.

A világtörténelem nagy stratégái, mindig is helyes logikai döntéseikre (a kívánt hatás eléréséhez szükséges mennyiségű, minőségű erők és eszközök, a megfelelő időben és helyen történő alkalmazása)[1], mint az erők megfontolatlan bevetésére alapozták sikerüket.

Az alkalmazott taktika függvénye, hogy a kívánt hatás eléréséhez milyen tekintetben kell fölénnyel rendelkeznünk az ellenséggel szemben[2]. Ezek az előnyök, hatásnövelő faktorok csak akkor érvényesülnek, ha a taktika, stratégia szintjén sikerül követni a meghatározott terveket, elgondolásokat. Amennyiben az ellenség ki tudja kényszeríteni, hogy a saját taktikáját kövessük, az ő hatásnövelő faktorai fognak érvényesülnek. Ennek folytán ismernünk kell eszközeit, és céljait, hogy azok ellenünk történő alkalmazását megelőzzük, hatásaik ellen védekezni tudjunk.

Ezen elméleti eszmefuttatás alkalmazható a kiberhadviselésben, hiszen naprakésznek kell lennünk az ellenséges entitás[3] taktikái és "támadási trendjei" terén annak érdekében, hogy felkészüljünk az általa gerjesztett fenyegetésre, és eredményesen vívjuk meg defenzív csatánkat a virtuális térben.

Fenyegetésekkel mindig is számolnunk kell, amennyiben elvárásokat[4] támasztunk az üzemelő informatikai hálózattal, rendszerrel szemben. Az informatikai biztonsági kontrollok segítenek felkészülni a rendszer „nyugalmi”, ideális állapotát megzavaró helyzetekre, az incidens teljes életciklusa (kialakulása, észlelése, kezelése) alatt. Ezt a célt csak abban az esetben tudja elérni, amennyiben feltételezzük és modellezzük a támadó szándékot, valamint ismerjük a támadó céljait, eszközeit.

Az informatikai védelmi eljárások az incidensre adott válasz alapján, az idősikon csoportosíthatóak [1.]:

- Preventív,
- Korrektív, vagy Reaktív,

---

[1] Lásd:pl.: ie. 480 - Thermopülai csata, ie. 202 - Zamai csata

[2] Erre számos példát találunk a történelemben:
a kiképzésbeli fölény, mellyel például a német Fallschirmjäger ejtőernyős csapatok rendelkeztek,
a mozgékonyság, dinamika okozta előny, melyre a német villámháborús harckocsi-ékek és vadászbombázók kombinált alkalmazása példa,
a mindent elsöprő tüzérség ereje: a katyusa, a szovjet rakéta-sorozatvetővel végrehajtott tűzcsapások,
a hírszerzés sikerei: a német tengeralattjáró hadviselés kudarcai részben az Enigma algoritmusának feltörése okozta,
a nagytávolságú fegyverek elrettentő ereje – A németek V1 és V2 rakétákkal végrehajtott, nagytávolságú csapásmérő műveletei,
a terep ismeretének kamatoztatása – a Finn halogató harc sikerei a szovjet offenzíva idején, vagy a váratlan támadás, meglepetés ereje - például a SAS Észak Afrikai bevetései során.

[3] Legyen az organikus: kiberbűnöző, hacker, cracker vagy mesterséges entitás: kártékony kód.

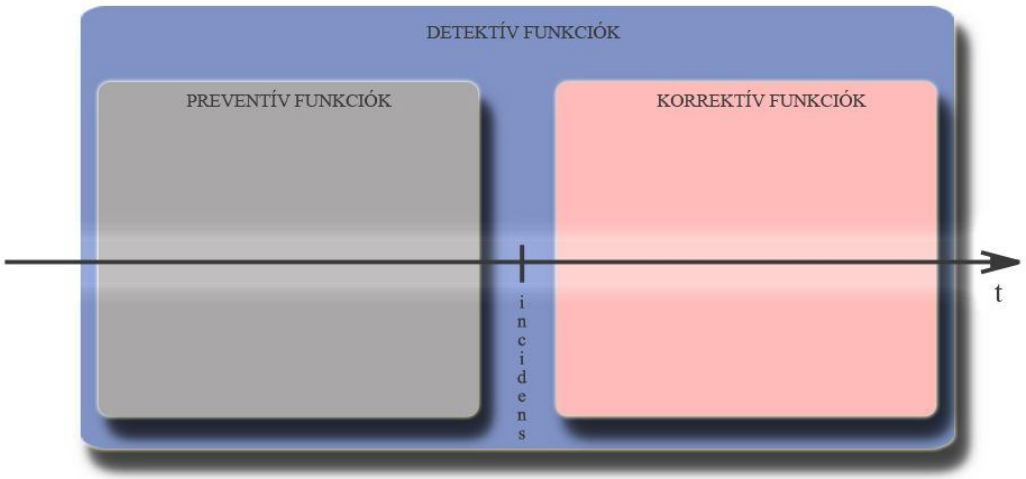
[4] Legyen az üzembiztonsági (szolgáltatás minősége, rendelkezésre állás), vagy információbiztonsági jellegű (bizalmasság, sértetlenség, rendelkezésre állás, hitelesesség, elszámolhatóság)

- Detektív tevékenységekre.

A *preventív funkciók* biztosítják a biztonsági incidensek megelőzését, a támadások alapjául szolgáló sérülékenységek megszüntetését, azok kihasználásának akadályozását.

A korrektív, *reaktív funkciók* a támadások bekövetkezte után aktivizálódnak, és próbálják megszüntetik a biztonsági incidens kiváltó okát, minimalizálják a károkat.

A *detektív funkciók* a támadások nyomainak gyűjtését, hiteles rögzítését, és megjelenítését végzik az incidens bekövetkezése előtt, alatt és után.



1. ábra A biztonsági kontrollok ábrázolása az incidens idősíkján

Az informatikai biztonsági alrendszerei (tűzfal, vírusvédelem, jogosultság kezelés, behatolás detektálás) ezeknek a funkcióknak egyikébe, vagy akár egyszerre többe is besorolható (pl.: a tűzfal alrendszer egyrészt a szabályrendszere alapján blokkolja a támadás, másrészt naplózza a próbálkozást).

A támadásokat klasszikusan kétféle módszerrel lehet detektálni [2][3][4]:

- ha ismerjük a támadást, a generált hálózati forgalom alapján mintákat (~*signature*) hozhatunk létre, a detektálás ekkor mintaillesztéssel zajlik (*knowledge-based IDS vagy signature based detection*);
- ha ismerjük a védett hálózat jellemzőit (forgalom típusa, eloszlása, végpontok, hálózati szolgáltatások), felállítható egy alapérték (~baseline), az ettől bizonyos mértékben történő eltérés indikálja a támadást, ez az úgynevezett anomália alapú detektálás (*behavioral-based* IDS vagy *anomaly based detection*).

A napjainkban alkalmazott határvédelmi eszközök általában mindkét eljárást alkalmazzák. Azonban hátrányuk, a magas hibaarány (a tévesen támadásnak felismert legitim forgalom, valamint a fel nem ismert támadások). Ezt a hibaarányt javíthatjuk plusz védelmi intézkedések bevezetésével, támogató tevékenységek alkalmazásával. Amennyiben ismert a kontroll hiányossága, az eszközök finomhangolásainak segítségével azok hatékonysága növelhető (a gyári beállításokat, vagy az úgynevezett bevált gyakorlatokat kiegészítik, illesztik a védett hálózathoz, a felhasználás jellegéhez). A következőekben egy ilyen támogató tevékenységet mutatok be, mely elősegíti a hálózatvédelmi eszközök kalibrációját, testre szabását.

Jelen dolgozat témája szorosan kapcsolódik Kassai Károly mk. ezredes úr doktori értekezésében [5] felvázolt, NATO- és nemzeti információvédelmi fejlesztési igényekhez.

HONEYPOT (~ MÉZES CSUPOR, CSALI RENDSZEREK)

Az elektronikai hadviselésben régóta alkalmazott ellentevékenység a megtévesztő célok („decoy", „chaff") alkalmazása, mely segítségével az ellenséges felderítő lokátorok, légvédelemi rakéták téveszthetőek meg, hamis céljelek generálásával. Ennek a védelmi tevékenységnek a logikáját követve, az informatikai hálózatok védelme során is hatékonyan alkalmazható a támadó megtévesztésére szolgáló csali rendszerek (*bait system*).

A „csali" (~ honeypot) olyan számítógépes rendszer, mely hálózati szolgáltatások, erőforrások, forgalmak szimulálása segítségével (valós erőforrások, információk) kifejezetten a szándékos támadások detektálására szolgál [6]. A támadási kísérletek, a sikeres támadások és a behatolások eszközeiről (támadási vektorok, malware-ek, exploit-ok) rögzítése mellett az elkövető szándékairól és a valós rendszer sérülékenységeiről is információval szolgál.

Ezen rendszerek (un.: produktív rendszer) a valós rendszerektől függetlenül, azokat nem akadályozva, és nem kompromittálva képesek detektálni a támadási szándékot, rögzíteni a támadási módszert, és a támadó tevékenységét [6].

Sokféle típusa és fajtája létezik, a hálózati topológiába történő elhelyezésére is számos módszer létezik, azonban az alábbiakban mind megegyeznek:

- céljuk a támadás detektálása (a módszer, az elkövető és a kiváltott hatás);
- a valós rendszerek tulajdonságait szimulálják;
- az automatizáltság mértékének függvényében intenzív felügyeletet, humán interakciót igényelnek;
- védelmi technológiák, és működési rendszabályok segítségével megakadályozzák a csali rendszer további támadásokra történő felhasználását (~kompromittálását).

A Csali rendszerek feladat szempontjából megközelítve lehetnek:

- kutatási célú (pl.:malware-ek, exploit-ok gyűjtése);
- védelmi célú (támadási kísérlet detektálása, a nyomok rögzítése).

A kutatási célú csapda az emulált platformok processzor architektúrájában, az operációs rendszer, szolgáltatások és frissítési szintek tekintetében széles palettát kell kínálnia, annak érdekében, hogy a minél több támadás irányuljon ellenük.

A védelmi célúak elsősorban a védett hálózat jellegzetességeit emulálják, minél inkább elmosva a valós és a produktum rendszerek közti különbségeket (feltűnő lenne, egy vállalati környezetben több, különböző patch-elési szintű, eltérő architektúrájú és verziójú operációs rendszer).

A védelmi célú honeypotok módszer alapján csoportosítóak a következő típusokra:

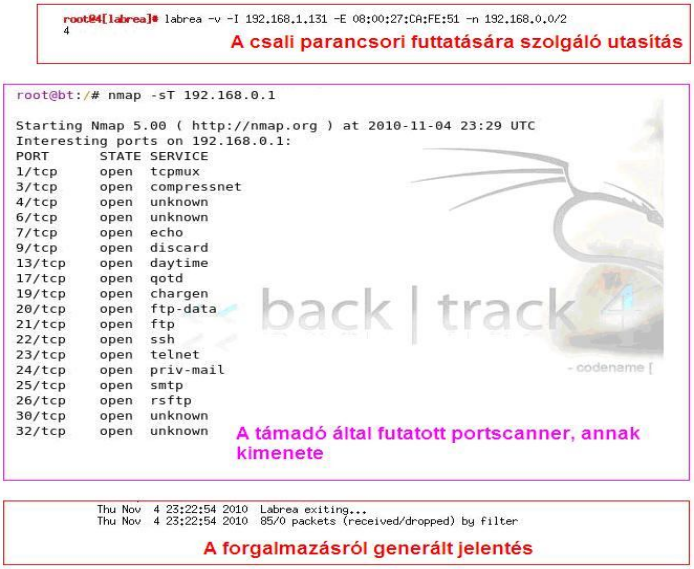
- „Szurokcsapda „ (~Tarpit);
- Forgalom-átirányító (Redirector);
- Internet szimulátor (Internet Simulation Environment).

A tarpit-ek célja a támadó lekötése, a DoS, DDoS támadások, az automatizáltan terjedő kártékony kódok terjedési sebességének csökkentése, melyet hamis célpontok imitálásával, valamint a válaszidő maximalizálásával[5] ér el.

Az alábbiakban összefoglaltam a szurokcsapdákban alkalmazható módszereket:

- IP címtartomány növelése (nem létező címekkel);
- hamis DNS bejegyzések;
- hamis adatkapcsolati- (CDP, ARP, RARP, Ethernet), hálózati (pl.:DHCP),valamint forgalomirányító hirdetések (pl.:RIP, OSPF, BGP);
- TCP ablak méretének 0 értéken tartása;
- TCP deszinkronizáció (hibás szekvenciaszám küldése);
- IP Csomagdarabolás[6];
- hibás FCS, CRC értékek;
- csomagismétlés kérése;
- késleltetés (delay, round trip time - RTT) növelése;
- hozzáférési listák (ACL - Access Control List) segítségével a bejövő/kimenő forgalom korlátozása (konkurens TCP kapcsolatok száma, sávszélesség stb.).

Az alábbi képen [2. ÁBRA] demonstrálom, a *labrea* honeypot alkalmazását, mely működése során a népszerű *nmap*[7] port scanner-t téveszti meg, egy „C" osztályú IP címtartomány összes kliensének emulálásával[8]. Az ábrán csupán egyetlen végpont nyitott portjainak ellenőrzését mutatom be az átláthatóság érdekében, azonban a végrehajtott tesztek során megvizsgáltam az összes emulált végpontot, melyek eltérő nyitott port kombinációkkal „tévesztettek meg".



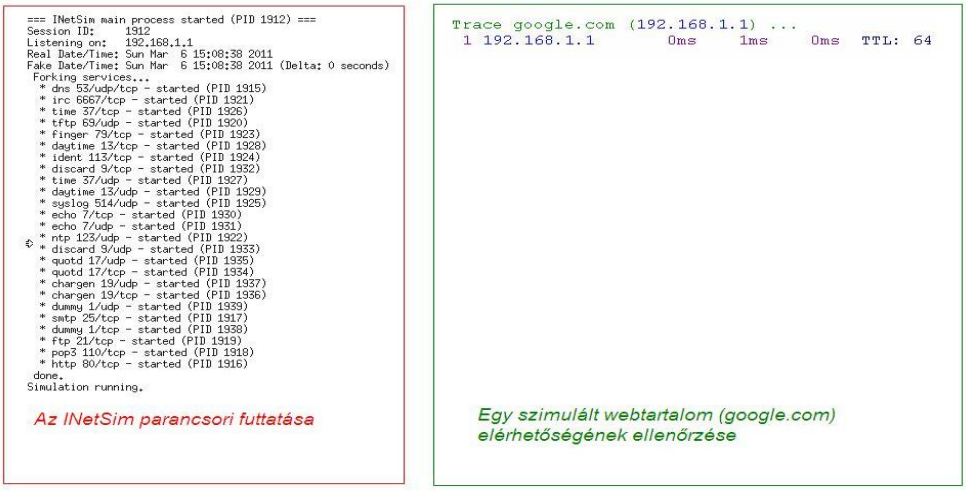
2. ábra A Labrea honeypot által megtévesztett nmap portscanner

[5] Erre a típusra példa a Labrea és a Jackpot nevű nyilvános forráskódú alkalmazás
[6] Pl.:a fragroute, fragrouter eszközök segítségével (lásd részletesen: http://monkey.org/~dugsong/fragroute/)
[7] Ingyenesen letölthető különböző operációs rendszerre a http://nmap.org/ oldalról
[8] A kérésekre adott differenciált válaszok érzékelhetőek a csomag késletetés változásával, és a nyitott portok váltakozásával

A redirector olyan rendszer, melyek a támadás érzékelése esetén a kapcsolódási kísérletet a honeypot irányába továbbítja, gyakorlatilag egy behatolás detektálási feladatkörrel kiegészített forgalomelosztó (Load Balancer). Ilyenre példa a Bait 'N' Switch Honeypot[7] rendszer.

A korszerű kártékony kódok aktivizációjuk (parancs-csatorna kiépítése, kártékony kód letöltése, hálózati felderítés és sérülékenység vizsgálat) előtt gyakran ellenőrzik a hálózati kapcsolat meglétét, az Internet elérést, azonban megfelelő konfiguráció mellett ezek megtévesztése is lehetséges. Az Internet szimulátor a kártékony kódok megtévesztésének gyakran alkalmazott eszköze, működése során a kérésre (DNS lekérdezések, http tartalmak, IRC[9] kapcsolatok) hamis válaszokat ad. Ennek segítségével a kártékony tartalmat publikáló weblapok, botnet vezérlők IP címei azonosíthatóak.

Az alábbi, laborkörnyezetben készített képernyőképeken [3. és 4. ÁBRA] jól látható, hogy a kliens a kéréseire *(trace google.com*, *blabla.com* oldal megnyitása) a szimulátor képes volt válaszokat generálni, tartalmat szolgáltatni.



3. ábra Az InetSim működésének ellenőrzése I.

```
03/08/11 20:29:36 Browsing http://blabla.com/
Fetching http://blabla.com/ ...
GET / HTTP/1.1
Host: blabla.com
Connection: close
User-Agent: Sam Spade 1.14

HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Connection: Close
Content-Length: 258
Content-Type: text/html
Date: Tue, 08 Mar 2011 19:29:34 GMT

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

4. ábra Az InetSim működésének ellenőrzése II.

[9] A botnetek vezérlésének gyakran alkalmazott eszköze (a http kérések/válaszok mellett), az uralom alá vont végpontok egy chat szolgáltatáson keresztül kapják utasításaikat.

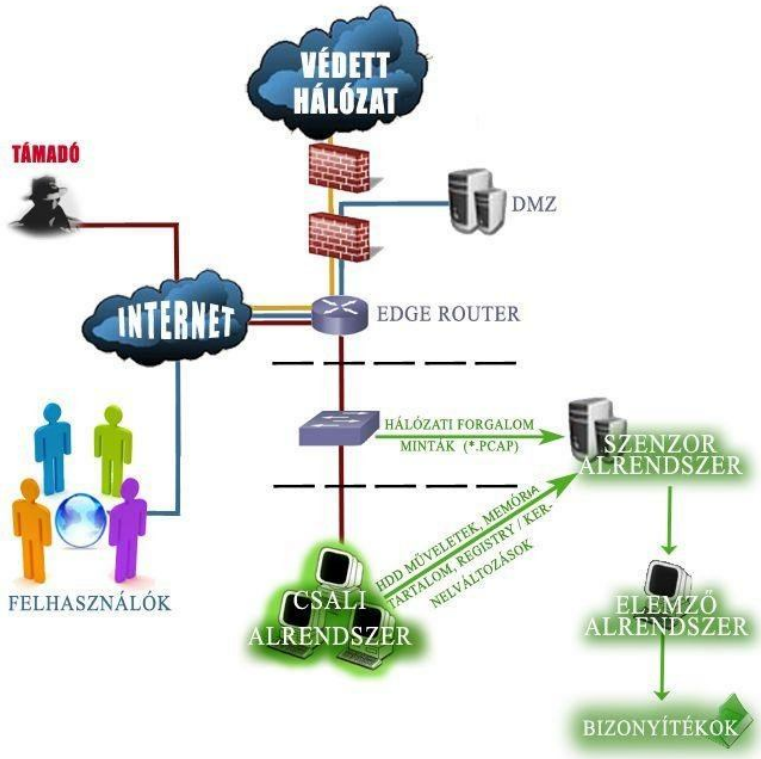
A szimuláció alapbeállítások melletti futtatásáról készültek a fenti képernyőképek. A szolgáltatott tartalom hamis volta egyértelműen detektálható ezek alapján (pl.: a 4.ÁBRA, a HTML kódban található szöveges információ alapján). Azonban az olyan, elsősorban a támadók által használt eszközzel, mint a Social-Engineer Toolkit (SET)[10] alkalmazásával, képesek vagyunk bármely weblap tartalmát klónozni[11], valamint azt lokálisan szolgáltatni.

A honeypot típusától (kutató vagy védelmi) függetlenül felépítésükben felismerhetünk azonos vonásokat, mely jegyeket az egyedi implementációk, speciális típusok sem nélkülözhetnek.

A HONEYPOT RENDSZEREK FELÉPÍTÉSE

1. „Csali" alrendszer (valós vagy emulált szolgáltatás, virtuális számítógép)
2. Szenzor alrendszer (forgalom és tevékenység rögzítése)
3. Elemző alrendszer (a nyomok elemzésére és megjelenítésére szolgál)

Honeypot hatékonysága a „csali" valósághűségétől, valamint az elemzés hatékonyságától függ, az egyik elem hatékonysága, a másik nélkül értékét veszi.



5. ábra Egy tipikus honeypot felépítése

Az egyes alrendszerek részletesen bemutatásra kerülnek cikkem második felében.

[10] Az alkalmazás részét képezi a Backtrack live CD alapú linux disztribúciónak
[11] A SET program Website Attack Vectors \ Site Cloner funkciójának felhasználásával

HONEYPOT FELHASZNÁLÁSI LEHETŐSÉGEK

Fontos kiemelni, hogy a honeypot rendszerek támogató védelmi szolgáltatásokat biztosítanak. Indirekt módon támogatják a biztonsági kontrollokat, ami annyit jelent, hogy közvetlen céljuk nem a támadás megakadályozása, hanem annak megértése, ismeretek gyűjtése a hatékony védelem kidolgozása érdekében. Az alábbiakban felsorolom azokat a felhasználási módokat, melyek elősegíthetik a hálózat védelmének fokozását.

Riasztás

Korai riasztási rendszerként (un.: Early Warning System) használva, a honeypot értesíti az üzemeltető állományt a biztonsági incidens bekövetkeztéről. A belső hálózaton terjedő férgek, felderítést végző hacker eszközök (*hacker tools*) forgalmat generálnak a riasztási rendszer IP tartománya (csalijainak) irányába, elárulva ezzel tevékenységüket.

Forgalom klasszifikációja

Internetszolgáltatók (ISP), incidenskezelő szervezetek (CERT) és globális hálózattal rendelkező szervezetek (pl.:kormányzati vagy gazdasági szektor) a honeypotok segítségével képessé válnak (a felhasználói jogok, adatvédelmi törvények megsértése nélkül) a kártékony forgalom szeparált megfigyelésére, valamint a fertőzött, támadó jellegű végpontok forgalomból történő kizárására.

Nagy intenzitású járványok (pl.:Slammer, CodeRed, Nimda, Blaster, Conficker stb.) esetén akár a végpontok karanténba helyezésével, a kártékony kód vezérlőcsatornájaként üzemelő hálózati végpontok lekapcsolásával, vagy szimulálásával (pl.:DNS rekordokba az adott kártékony domain IP-je helyett egy, a fertőtlenítés lépéseit leíró weblap címe kerül) is elősegíthetik a védekezést. Ennek a módszernek az alkalmazására már láthattunk példát az utóbbi években, például a coreflood [8] és a bredolab [9] botnetek esetén.

Információszerzés, tudásbővítés

Segítségével az üzemeltető állomány megismeri a támadó eszközeit, módszereit és céljait, elősegítve ezzel a naprakész védelem fenntartását.

A globális méretű csali és szenzorhálózatok lehetőséget biztosítanak az egyedi támadási módszerek elemzése mellett, a támadási trendek statisztikai analízisére. A világméretű hálózat segítségével az automatizált (hálózati férgek, alacsony tudásszintű, csak a mások által elkészített támadóeszközöket használó „script kiddie”-k) és a célzott támadások statisztikai módszerekkel megkülönböztethetőek. Hiszen ha több szenzortól gyűjtött naplóban is jelentkezik, ua. a forráscím által generált forgalom, ugyanolyan paramétereket, metaadatokat tartalmazó hálózati csomagokat, akkor azok azonos támadó platformról érkeznek[12].

Naplózás, mintagenerálás

A támadások és a kártékony kódok jellegre leginkább magához az Internethez hasonlíthatóak:

- dinamikusan változnak, adaptálódnak és frissülnek a technológiai fejlődéssel párhuzamban;
- nehezen kategorizálhatóak, nincsen egy mindenre kiterjedő katalógus, egységes rendező elv.

Mivel céljuk az egyediség, az újítás, nehezen írhatóak le, definiálhatóak a vírusadatbázisok számára. A honeypot működése során rögzíti a támadás forgatókönyvét,

[12] Legyen az botnet álal vezérelt, kompromittálódott végpont, un. „zombie” gép, vagy „script kiddie” által használt, "hangos" támadóeszköz.

valamint más biztonsági funkció támogatása érdekében mintákat készít a használt támadási technikáról. A behatolás megelőző rendszerek mintáinak[13], vírusirtó szignatúráknak (Antivirus signature) előállításával a későbbi detektálást gyorsítja fel (hasonlóan a biológia immunrendszer ellenanyag termeléséhez[10]).

Preventív védelem

Az úgynevezett tarpit, vagy "sticky honeypot" a támadó felderítő tevékenységét lassítja, hamis célok és lassú válaszidő segítségével.

Ennek a felhasználási módnak az alkalmazása hasonlít leginkább a valós csapdák funkciójára: hiszen célja, hogy minél tovább feltartoztassa-foglalkoztassa a behatolót.

Digitális nyomforrás[11]

Az elkövető ellen kezdeményezett jogi lépések egyik alappillére lehet a csali alrendszeren létrejött, a szenzor alrendszerrel hitelesen, és pontosan rögzített bizonyíték.

A Toulouse Egyetem [12] egyik kutatása kifejezetten a magas interakciójú honeypotok elemzésére, a támadó entitások klasszifikációjára fókuszál. A saját üzemeltetésű honeypotjaik naplóiból készített statisztikák, és a kiemelt minta-esetek segítségével demonstrálják az automatizált, és az emberi támadók által hagyott nyomok közti különbséget (gépelési hibák, bufferelt vagy karakterenként gépelt parancsok, gépelési sebesség, logikai hibák, a rendelkezésre álló információktól független, programozott feladat-végrehajtás, a kompromittált gép használatának céljai, stb.).

Audit eszköz

Kutatómunkám során számos esetben találkoztam, a honeypotok tulajdonságait részben vagy egészben felhasználó rendszerekkel (pl.: malware elemző környezetek[14]), valamint a veszprémi CheckVir tesztlabor[15] rendszerével (a kutatás eredményeit részletesen publikálta Leitold Ferenc [13]). Ennek a labornak a célja, hogy a különböző gyártók, fejlesztők víruskereső alkalmazásait a teljesítmény és hatékonysági paramétereik alapján, objektív módszerekkel értékelje. A tesztlabor kialakítása, működési elve egy magas interakciójú kliens honeypotokból álló hálózatra emlékeztet.

Természetesen számtalan más, védelmi célú eszköz tesztelésére biztosít lehetőséget egy honeypot rendszer. A csali rendszereket használhatjuk akár az automatizált sérülékenység-kereső eszközök (un.: vulnerability scanner) működésének ellenőrzésére, vagy a különböző tűzfal, behatolás-detektáló eszközök összehasonlítására, terhelési vizsgálatára (elkerülve ezzel az üzemelő rendszer működésének veszélyeztetését).

Nem legális alkalmazás

A védelmi célú, „jó-szándékú” alkalmazások mellett említést kell tenni az elkövetők által alkalmazható honeypotokra is, melyek az ellentámadások (melyet elsősorban a vetélytárs bűnszervezetek indítanak) detektálására, valamint a konkurencia technológiáinak kifürkészésére irányul. Hatékonyan alkalmazhatják az új támadási vektorok gyűjtésére, a botnetek parancscsatornájának kifürkészésre és a kontroll átvételére. Továbbá a publikusan elérhető eszközöket tanulmányozhatják, saját védelmük fokozására a honeypotok detektálásra ellenintézkedések dolgozhatnak ki (LÁSD pl.: virtualizáció detektálása), az implementációkban sérülékenységeket kereshetnek (a honeypotok kompromittálása érdekében).

---

[13] IDS signature

[14] Ilyenre példa a *High Security Lab* által üzemeltett *Network Telescope* elnevezésű kártékony kód gyűjtő rendszere, mely megtekinthető az alábbi URL-n: http://lhs.loria.fr/index.php?option=com_content&view=article&id=94&Itemid=84

[15] A kutatólabor technikai felépítése az alábbi linken érhető el: http://www.checkvir.hu/methodology

ÖSSZEFOGLALÁS

A csali és szenzor rendszerek a biztonság kialakításának és fenntartásának egy új megközelítését sugallják:

- A védelem hatékonysága nemcsak az egyes funkciók (jogosultság kezelés, határvédelem stb.) meglétététől, hanem azok naprakészségétől, felügyeletétől és összhangjától is függ[16].
- A fenyegetettség mértéke folyamatosan változó érték, a bekövetkezés valószínűségét nem lehetséges a védelmi kontrollokkal 0-ra csökkenteni (maradvány kockázatot feltételezünk).
- Nem elégséges az ismert támadási módok szűrése, folyamatosan készülni kell az ismeretlen fenyegetések kezelésére.
- A preventív kontrollok hatékonysága azok naprakészségétől függ.

Ez az új szemlélet a támadásokat megakadályozása mellett azok megértését (sérülékenység oka, támadó módszere, és az indok) is szükségesnek tartja.

Jelen írásom célja a honeypot rendszerek általános jellemzőinek, felépítésének bemutatása, annak érdekében, hogy az informatikai biztonsággal foglakozó kutatók (kártékony kódelemzők, hálózatbiztonsági szakemberek, tanácsadók stb.) számára megfelelő tudásbázist képezzen. Segítségével a céljaiknak, elvárásaiknak leginkább megfelelő rendszer tervezése, implementálása valósulhat meg.

A honeypot rendszerek vitathatatlan előnye, hogy képesek az incidensek teljes „életciklusa" alatt támogatni a védekezést. A bekövetkezés előtt képes nyomokat rögzíteni (detektív jelleg) a támadás korai fázisáról[17]. A preventív funkciókat indirekt módon, a támadó szándékának, „érdeklődési területének" jelzésével támogatja. A támadási kísérletek azonosítása (detektív és reaktív funkciók), hozzájárul az üzemeltetési rendszabályok és praktikák naprakészen tartásához, a sérülékenységi minták generálásához (szűrés), a konfigurációs és implementációs hibák kijavításához (sérülékenység megszüntetése).

A honeypotok felhasználási lehetőségeivel és működési elvével általánosságban foglalkozó kutatók, valamint az egyes eszközök leírásainak összevetése során észrevettem, hogy a működési elvek és alkalmazott technológiák szempontjából a valós implementációk nehezen kategorizálhatóak (általában több típus definíciójának is megfelelnek). Így összehasonlításuk, hatékonyságuk értékelése nehézkes. Ez a tény ösztönzött, a honeypotok működési elveinek és felhasználási lehetőségeinek összegyűjtésére, valamint további módszerek és lehetőségek kutatására.

Cikkem második felében, az első témakörhöz szorosan kapcsolódó területtel foglalkozom: a honeypot rendszerek felépítésével, alkotórészeivel (Csali alrendszer, szenzor alrendszer, elemző alrendszer). A kutatásom során szerzett tapasztalatok, bevált gyakorlatok említése mellett kitérek a témát érintő aktuális kutatásokra is.

Felhasznált irodalom

[1] Krasznay Csaba*: Kockázatkezelés – előadásanyag (online)*
Forrás: www.krasznay.hu/presentation/elte_02.ppt
letöltve: 2011.10.03

[16] Erre jó példa, hogy nem elégséges a biztonsági eseményeket rögzíteni (naplózni), hanem a különböző források (tűzfal-, authentikációs szerver-, szolgáltatás naplók) korrelációja és azok feldolgozása is szükséges (üzemeltető állomány értesítése, vagy automatikus reakció).

[17] Pl.: a támadó, vagy a kártékony kód a hálózat aktív IP címmel rendelkező végpontjait keresi, nyitott portokat és sérülékeny szolgáltatásokat azonosít

[2] *Behatolásdetektálás, IDS rendszerek – előadásanyag (online)*
Forrás: http://www.sze.hu/~heckenas/okt/ids.pdf letöltve: 2011.10.03

[3] *Red Hat Enterprise Linux 4.5.0 - Security Guide* - 9.1.1 fejezet (online)
Forrás: http://www.centos.org/docs/4/4.5/Security_Guide/s2-ids-types.html letöltve: 2011.10.03

[4] *Intrusion Detection System Overview Summary* oktatóanyag (online)
Forrás: http://ciscoarticles.com/CCSP-Cisco-Certified-Security-Professional/Intrusion-Detection-System-Overview-Summary.html letöltve: 2011.10.03

[5] Kassai Károly: *A Magyar Honvédség információvédelmének - mint a biztonság részének- feladatrendszere: doktori (PhD) értekezés* (2008), pp. 75-76.
Forrás: http://193.224.76.4/download/konyvtar/digitgy/phd/2008/kassai_karoly.pdf letöltve: 2011.10.03

[6] Lance Spitzner: *Build A Honeypot* (online)
Forrás: http://www.spitzner.net/honeypot.html letöltve: 2011.10.03

[7] Lorie W. Carter: *Setting Up a Honeypot Using a Bait and Switch Router*
Forrás:http://www.sans.org/reading_room/whitepapers/casestudies/setting-honeypot-bait-switch-router_1465 letöltve: 2011.10.03

[8] *US Government Takes Command of Coreflood* (online cikk)
Forrás:http://articles.yuikee.com.hk/newsletter/2011/04/a.html letöltve: 2011.10.03

[9] Landelijk Parket: *Dutch National Crime Squad announces takedown of dangerous botnet*
Forrás:http://www.om.nl/algemene_onderdelen/uitgebreid_zoeken/@154338/dutch_national_crime/ letöltve: 2011.10.03

[10]Jeffrey O. Kephart: *A Biologically Inspired Immune System for Computers*
Forrás:http://www.research.ibm.com/antivirus/SciPapers/Kephart/ALIFE4/alife4.distrib.html letöltve: 2011.10.03

[11] Illési Zsolt: *KRIMINÁLTECHNIKA SZEREPE AZ INFORMATIKAI VÉDELEM TERÜLETÉN,* Hadmérnök IV. Évfolyam 1. szám - 2009. március (online), p. 177, ISSN 1788-1919 Forrás: http://hadmernok.hu/2009_1_illesi.pdf letöltve: 2011.10.03

[12] E. Alata, V. Nicomette, M. Kaâniche, M. Dacier, M. Herrb: *Lessons learned from the deployment of a high-interaction honeypot* (online)
Forrás: http://arxiv.org/ftp/arxiv/papers/0704/0704.0858.pdf letöltve: 2011.10.03

[13] Leitold Ferenc: *VÍRUSVÉDELEM KIVÁLASZTÁSA*, Hadmérnök IV. Évfolyam, 4. szám, 2009. március (online), ISSN 1788-1919
Forrás: http://hadmernok.hu/2009_4_leitold.php letöltve: 2011.10.03