IT sérülékenység vizsgáló szoftverek összehasonlító elemzése

Törőcsik Marietta, Kozlovszky Miklós

Óbudai Egyetem, Neumann János Informatikai Kar

A sérülékenység vizsgálat szerepe az informatikai biztonság világában

A hírekben egyre több incidenst hallunk, melyben egy vállalat informatikai biztonsága sérült meg, adatokat loptak el vagy rendszereket tettek tönkre támadók. 2011-ben a Sony 174 millió dollárt vesztett egy informatikai támadás során, de olyan cégek, mint a Citigroup, AT&T is támadások áldozatául estek[1] az utóbbi időkben. A Verizon – informatikai támadások kivizsgálásával foglalkozó cég - 2012. évi jelentése szerint[2], 2011-ben a hozzájuk beérkezett panaszok alapján 174 millió adat kompromittálódott 855 incidens során. 2012-ben több ezer jelszó került nyilvánosságra, melyek hozzáférést biztosítanak többek között az amerikai haditengerészet, NASA,és több ország kormányzati rendszeréhez [3]. A példákban szereplő rendszerek informatikai biztonsága nem volt jó, voltak olyan biztonsági rések, amelyeket a támadók kihasználtak. Felmerül a kérdés, mit is jelent a jó informatikai biztonság? Lehetséges lett volna megelőzni ezeket a támadásokat, ha a vállalatok jobban odafigyelnek, többet költenek az adataik biztonságára?

Az informatikai biztonság lényege, hogy megelőzhetőek legyenek az ezekhez hasonló támadások. Mivel a vállalatoknak egy esetlegesen bekövetkező eseményre kell felkészülniük, emiatt sok vállalat felesleges költségnek tekinti, és csak a törvényeknek, szabályoknak, előírásoknak megfelelő minimális biztonságot valósítják meg[4]. A magas költségeken kívül az nehezíti biztonságos rendszer kiépítését, hogy sokszor a rendszer funkcionalitása és használhatósága az elsődleges célok, míg a rendszer biztonságossága háttérbe kerül[5]. Elsődlegesen a cél mindig a vállalat piaci sikerének biztosítása és az informatikai infrastruktúra feladata, hogy ezt maradéktalanul támogassa. Azonban nem csak a sikert akár vállalat bukását is előidézheti, ha a rossz informatikai biztonság miatt üzleti titkok, mint például az ügyfelek adatai, üzleti titkok, stratégiai tervek kerülnek nyilvánosságra. Emiatt fontos, hogy a vállalatoknak legyen kockázatkezelési terve, melyben a kockázatbecslés segítségével felmérhetik a vállalatot fenyegető veszély bekövetkezésének valószínűségét, illetve a bekövetkezéskor felmerülő károkat. Ezen információk birtokában a vezetés dönthet arról, elfogadja a kockázat által jelentett veszélyt a vállalatra nézve, vagy csökkenti, megszűnteti azt [6]. Nincs tökéletes biztonság. Nap, mint nap fedeznek fel, sérülékenységeket. Hardveres, illetve szoftveres hibákat és az informatikai rendszer eszközeinek a rossz konfigurációjából adódó hibákat együttesen sérülékenységeknek nevezik. Ezen sérülékenységek kezelésére jó példát mutat a Microsoft, ahol minden hónap első keddjén frissítéseket adnak ki a termékekhez. Amennyiben ezeket nem telepítjük, akkor az általunk futtatott operációs rendszer az idő folyamán, egyre több ismert sérülékenységet fog

tartalmazni. A sérülékenységek megtalálásában, illetve az általuk jelentett kockázat felmérésében segítenek a sérülékenység vizsgáló szoftverek.

Sérülékenység vizsgáló szoftverek

A sérülékenység vizsgáló szoftverek képességeinek megismeréséhez teszt eseteket és teszt környezetet definiáltunk valamint teszteléseket végeztünk, melyekhez egy oktatási, illetve egy kutatási célra használt infrastruktúra állt rendelkezésünkre, emellett egy további szimulációs tesztkörnyezet került kiépítésre megfelelően sebezhető gépekkel. Olyan sérülékenység vizsgáló szoftvereket kerestünk, melyeknek saját vizsgáló eszközük van és melyek aktív hálózati vizsgálattal keresik meg a hálózatunkban a sérülékenységet. Olyan gyártók termékeire koncentráltunk, melyeknek az elsődleges funkciójuk a sérülékenység vizsgálat, és nem csak kiegészítő funkcióként szerepel, gyakran más gyártók vizsgáló eszközeit használva.

AQualys informatikai biztonsággal, és sérülékenység menedzsmenttel foglalkozó vállalat. A 2012. év legjobb informatikai biztonsági gyártónak választották az informatikai biztonsággal foglalkozó SC magazin európai szavazásán. A Qualys honlapján lévő információ szerint a Forbes magazin által összeállított listán mely, a világ 100 legnagyobb vállalatát tartalmazza, 51 a Qualys ügyfelei közé tartozik. A QualysGuard felhő alapú, szoftver, mint szolgáltatás modell szerint igénybe vehető sérülékenység vizsgáló szoftver. [7]

A Rapid7 egy gyorsan fejlődő, informatikai biztonsággal foglalkozó cég. Nexpose nevű terméke 2012-ben elnyerte az IT biztonsági szakembereknek szóló SC magazin „Best Vulnerability Management Tool” díját [8]. Emellett számos tanúsítvánnyal rendelkezik, például azon szoftverek között volt, amik elsőként szerezték meg a United States Government Configuration Baseline (USGCB) tanúsítványt, és az első sérülékenység vizsgáló termékként kapta meg a Common Criteria Certification for Evaluation Assurance level Augmented (EAL3+) tanúsítványt.[9]

A Nessus sérülékenység vizsgáló szoftvert, 2005-ig nyílt forráskódú szoftverként fejlesztették, majd a Tenable a Nessus fejlesztője új liszensszel, zárt forráskódú szoftverként fejlesztette termékét tovább. Az Open Vulnerability Assessment Scannert (OpenVAS), a Nessus forráskódja alapján fejlesztik 2005 óta, nyílt forráskódú szoftverként. [10]

Szoftverek összehasonlítása

Az összehasonlító elemzéshez három kategória alapján határoztuk meg a szempontokat. Az első és talán a legfontosabb szempontok a sérülékenység vizsgáló szoftverek működésével szemben támasztott általános elvárások. Ezekről találtuk az irodalomkutatás alatt a legkevesebb információt, a szakirodalomban elsősorban a menedzsment funkciókra, illetve a felhasználói felület és az eredmények átláthatóságára koncentrálnak. Természetesen ezek is fontos szempontok, ezért ezeket is vizsgáljuk.

Terméktámogatás és felhasználói felület szempontjai

Dokumentáció és terméktámogatás a szoftverekhez. Ennél a szempontnál az interneten az adott szoftverhez található, dokumentáció, felhasználói útmutatókat használhatósága

Felhasználói felület használhatósága. Azt tűztük ki célnak, hogy megismerjük, mennyire könnyen, vagy éppen mennyire bonyolultan lehet kiigazodni a szoftverek felhasználói felületén, a felhasználói útmutatók, interneten található dokumentációk segítségével.

Működésük elemzésének szempontjai

- Feltérképezési pontosság: a hálózatot mindegyiknek pontosan fel kell tudnia térképezni. Mivel a szoftverek a vizsgálat során megállapított információk szerint szűkítik a hálózaton tesztelendő sérülékenységek halmazát, így fontos szempont, hogy a szoftverek már a vizsgálat elején pontosan határozzák meg a hálózaton elérhető szoftvereket, operációs rendszereket.
- Megismételhetőség: azaz van-e lehetőség, és ha igen milyen az ellenőrzések ismétlésére. Egy-egy ilyen ellenőrzést rendszeresen le kell futtatni a hálózaton, lehetőség van-e a beállítások elmentésére és a tesztelés időzítésére.
- Tesztelés időtartalma.
- Bővíthetőség: megadja, hogy amennyiben a hálózat bővül, melyik megoldást a legegyszerűbb az új hálózat méretéhez igazítani.

A kapott eredmények értékelési szempontjai

- Pontosság: A szoftverek eredményeinél az egyik legnagyobb probléma a hibás találat, ennek eredményeképpen egy nem létező hibát keresünk a hálózatunkon. Fontos, hogy a szoftverek minél kevesebb ilyen találatot adjanak eredményül, amellett, hogy lehetőleg minden valós hibát megtaláljanak.
- Visszakövethetőség: Az eredményekben szerepelnie kell a sérülékenység helyének, a hibapontos leírásának.
- Sérülékenység adatbázis mérete: A szoftverek a sérülékenység adatbázisukban található bejegyzések szerint vizsgálják a célpontot, ezért minél nagyobb ez az adatbázis, annál több sérülékenységre tesztelik a hálózatot.
- Sérülékenység érzékenység: talált (érvényes) hibák száma.
- Eredmények igények szerinti szűrése: egy-egy vizsgálat eredményeként sok olyan adatot kaphatunk, amikre nem feltétlenül van mindenkinek szüksége. Az eredményeket elemzőknek minél részletesebb adatokra van szükségük, míg a javításban résztvevők csak azokat a sérülékenységeket szeretnék a jelentésben látni, amelyeket ki kell javítaniuk, ezért fontos szempont a sérülékenység vizsgáló szoftvereknél, ha a jelentéseket az igényeinknek megfelelően hozhatjuk létre.
- Sérülékenységi hiba besorolási rendszerének pontossága: minden sérülékenység vizsgáló program meghatároz egy besorolási rendszert, hogy felhívja a figyelmet a valószínűleg nagyobb kockázattal járó sérülékenységekre. Emiatt fontos szempont, hogy minél több eredményül kapott sérülékenység súlyosságát értékeljük a hálózaton is ugyanolyan súlyosságúnak.

Összehasonlítás

Az elvégzett tesztek eredményeinek kiértékelése alapján elvégeztük a kiválasztott sérülékenységi szoftver megoldások összehasonlító elemzését.

Szempontok	QualysGuard	Nexpose	OpenVAS
Felhasználói felület	Bonyolult, sok opció, és beállítási lehetőség található benne. Jól elkülönült jogosultsági szintek, az egyes felhasználói osztályok a saját feladataiknak megfelelő felületet kapnak.	Egyszerűen kezelhető webes felület és API, azonban kevesebb beállítási opció	Webes felület, kliens alkalmazás, parancssoros környezet használható. A weben keresztül elérhető felületet választottuk, mely használata dokumentáció hiányában kezdetekben nehézséget okozott.
Dokumentáció, terméktámogatás	Felhasználói dokumentáció, videók, kérésre oktatás	Felhasználói dokumentáció.	Kevés dokumentáció.
Adatbázis nagysága	11000 CVE kompatibilis bejegyzés havonta kb. 25-szal nő[11]	kb. 28000 CVE kompatibilis bejegyzés [12]	25000 CVE kompatibilis bejegyzés[13]
Talált hibák száma	44	298	90
Fals pozitív	3	100	35
Tesztelés időtartama	43 perc	28 perc	32 perc
Rendszer feltérképezése	Az operációs rendszert ritkán határozta meg pontosan.	Többnyire felismerte a vizsgált célpont operációs rendszerét	Az operációs rendszert ritkán határozta meg pontosan
Megismételhetőség	A tesztelési paramétereket elmenthetjük, ezeket később, vagy időzítve újra futtathatjuk	A tesztelési paramétereket elmenthetjük, ezeket később, vagy időzítve újra futtathatjuk	A tesztelési beállítást újra meg kell adni, lehetőséget biztosít az időzítésre
Eredmények formája	Több szempont szerint lehet szűrni az eredményeket. szűrés minták létrehozására van lehetőség.	Több szempont szerint lehet szűrni az eredményeket	Kevesebb szempont alapján lehet szűrni az eredményeket, az egyik vizsgálat esetében üres PDF jelentést generált

Táblázat: sérülékenység vizsgáló szoftverek összehasonlító táblázata

A Qualys és a Nexpose által generált jelentések formátuma jól szerkesztett, könnyen olvasható, ezzel szemben az OpenVAS által exportált kimenet kevésbé struktúrált. További

negatívuma, hogy az OpenVAS az egyik vizsgálat eredményeit nem tudta a kijelölt formátumban menteni. A Qualys és a Nexpose főként fizető ügyfeleknek kínálja szolgáltatásait, ezért megfelelő minőségű terméktámogatás és felhasználói kézikönyv érhető el a szoftverekhez, azok használatának elsajátításához. Az OpenVAS esetében egy chatszoba, egy levelezőlista és egy hibakövető rendszer képezi a terméktámogatást, ahol könnyen előfordulhat, hogy választ sem kapunk a kérdésünkre. A QualysGuard nem érhető el külön telepíthető szoftverként, elsődlegesen SaaS szolgáltatásként nyújtja sérülékenység menedzsment megoldását. Abban az esetben, ha privát belső hálózatot szeretne az ügyfél vizsgálni, amely nem érhető el az internetről, fizikai készüléket vagy virtuálisgép lemezkép fájlt nyújtanak, amiket nem szükséges telepíteni, csak a hálózati kapcsolatot kell biztosítani, és a központi felületen keresztül menedzselhetőek. Ugyanez elmondható a Nexpose-ról is, ezen kívül telepítő binárisok is elérhetőek hozzá, vagyis külön szoftverként is installálható. Az OpenVAS használatához mindenképp a felhasználónak kell biztosítania a hardvert, amin futtatható a szolgáltatás.

Köszönetnyilvánítás

A szerzők ezúton mondanak köszönetet a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 „Kritikus infrastruktúra védelmi kutatások” projektnek a cikkhez végzet kutatások anyagi támogatásáért. A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Szeretnénk megköszönni a Qualys Inc.-nek, valamint az MTA SZTAKI-nak a tesztelésben nyújtott segítségüket, hogy rendelkezésünkre bocsájtották a szoftvereket, illetve az infrastruktúrát.

Továbbá szeretnénk megköszönni, Kotcauer Péternek, illetve Szenes Katalinnak a témában nyújtott segítségüket.

Irodalomjegyzék

[1]http://www.hotforsecurity.com/blog/top-5-corporate-losses-due-to-hacking-1820.html, 2012. november 10.
[2]http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf , 2012. november 10.
[3]http://hackmageddon.com/2012-cyber-attacks-timeline-master-index/, 2013. március.5.

[4] Chen, Tom - Wals, Patrick J.: Vulnerability Testing and Patching. In. Vacca, John R.: Computer and Information Security Handbook. Burlington, Morgan Kaufmann Publishers, 2009.
[5]Kimberly Graves: Certified Ethical Hacker Study Guide Indiana, Indianapolis Wiley Publishing, Inc., 2010, ISBN: 978-0-470-52520-3
[6] Szenes Katalin: Informatikai biztonsági módszerek kiterjesztése a vállalatirányítás, a működés, és a kockázatkezelés támogatására; Minőségés Megbízhatóság; nemzeti minőségpolitikai szakfolyóirat kiadja: az European

Organization for Quality (EOQ) Magyar Nemzeti Bizottsága XLVI. évf. 2012. / 5. sz., 252-257. o.ISSN: 0580-4485
[7]https://www.qualys.com , 2012. november 10.
[8] http://awards.scmagazine.com/winners/2012/130 , 2012. november 10.
[9]http://www.rapid7.com/company/news/press-releases/2012/usgcb-cyberscope.jsp, 2012. november 10.
[10] http://www.openvas.org/ , 2012. november 10.
[11]http://www.qualys.com/research/knowledge/, 2013. március 17.
[12]http://agdatacom.com/solutions/network-solutions/rapid-7/, 2013. március 17.
[13]http://www.openvas.org/news_archive.html, 2013. március 17.