

Bezpečnosť v sieťach TCP/IP

Sieťovú bezpečnosť môžeme chápať ako infraštruktúru pozostávajúcu zo sieťových zariadení (servery, smerovače, prepínače, klientske počítače a pod.) a bezpečnostných politík definovaných sieťovými správcami, ktoré slúžia na ochranu pred prístupom do siete, resp. prístupom k jednotlivým sieťovým zdrojom.

Čo je to TCP/IP?

TCP/IP (Transport Control Protocol, Internet Protocol) sú protokoly, ktoré sa používajú na komunikáciu v sieti internet. Kto je schopný komunikovať pomocou TCP/IP, dokáže komunikovať na internete. TCP/IP vychádza z referenčného modelu ISO/OSI, kde na tretej vrstve modelu (NETWORK) sa nachádza IP a na štvrtej TCP (TRANSPORT). Na základe vrstvy NETWORK dokážu jednotlivé zariadenia navzájom komunikovať. Každá adresa IP (napr. 192.168.1.2) je definovaná voči hardvérovej adrese (MAC adresa, napr. 00:03:ba:08:55:95), ktorá patrí v rámci ISO/OSI do druhej vrstvy (DATA LINK). Vrstva NETWORK takisto zabezpečuje smerovanie, aby sa jednotlivé zariadenia našli.

Typy útokov

TCP session hijacking (kradnutie TCP sedenia) – typ útokov na používateľské sedenia. Najznámejším typom kradnutia sedenia je IP spoofing, kde útočník použije source-routované IP pakety na vloženie príkazov do už existujúcej

komunikácie medzi dvoma nodmi a tvári sa už ako autentizovaný používateľ. Tento typ útoku je možný na základe toho, že autentizácia sa vykonáva vždy na začiatku sedenia TCP. Chrániť sa proti tomuto útoku je možné pomocou šifrovaného spojenia. Pod pojmom IP spoofing môžeme chápať aj „kradnutie“ adresy IP (napr. na lokálnej sieti). Keďže väčšina smerovačov má vo svojich ACL (Access Control Lists, prístupové zoznamy) definované, ktorý paket má a ktorý nemá prístup na základe odosielateľovej adresy IP, je pre útočníka najjednoduchší spôsob „ukradnúť“ adresu IP, ktorá prístup má. Vcelku elegantné riešenie (no len vo vlastnej prepínanej lokálnej sieti) proti tomuto typu útoku je nasaďiť prepínače s funkciou port security, kde možno určiť, ktoré adresy MAC smú komunikovať cez konkrétny port prepínača. Ďalší častý typ kradnutia sedenia TCP je tzv. man in the middle – útočník používa sniffer na odchyťovanie komunikácie medzi nodmi. Takýmto spôsobom môže získať napr. heslá a iné citlivé údaje. Opäť najlepšia ochrana proti tomuto útoku je používať šifrované spojenia.

Denial-of-Service (odmietnutie služby) – pokus o zahmlenie služby alebo služieb bežiacich na konkrétnom systéme v sieti, napr. opakujúce sa posielanie náhodných dát po sieti a následné zahmlenie cieľového systému. Základný predpoklad na úspešný útok DoS je nutnosť väčšej šírky pásma u útočníka než v systéme, na ktorý útočí.

Vďaka tomu poznáme tzv. DDoS (Distributed Denial-of-Service), kde útočník použije viac nodov, ktoré sa nachádzajú na rôznych miestach v internete. Napríklad útok DDoS môže prichádzať z rôznych krajín alebo svetadielov. Väčšina nodov, ktoré sú zapojené v takýchto distribuovaných útokoch, ani nevie, že sú súčasťou niečoho takého. Zväčša ide o bežných používateľov siete internet, ktorí sú infikovaní napr. trójskymi koňmi. Zjednodušene povedané, útočník spustí útok DDoS jednoduchým „zapnutím“ infikovaného nodu.

Existuje viac typov útokov DoS, resp. DDoS:

SYN flood – útočník posielá obrovské množstvo požiadaviek TCP/SYN s neplatnou hlavičkou odosielateľa, na ktoré sa cieľový systém snaží odpovedať pomocou TCP/SYN-ACK, keďže je však pôvodný odosielateľ falošný a cieľový systém čaká na TCP/ACK a ostatné (hoci aj regulárne) požiadavky musia čakať na timeout pôvodných a začína vznikať väčšia a väčšia latencia. Najlepšia obrana pred SYN floodom sú tzv. SYN cookies, ktoré modifikujú protokol TCP pozdržaním alokovania systémových zdrojov, pokiaľ nedôjde k overeniu opačnej strany.

Smurfing – metóda, ktorá zneužíva ICMP (Internet Control Message Protocol). Problém spočíva v zneužití broadcastových adries, na ktorých sa nachádza viac hostov. Niektoré implementácie TCP/IP povoľujú odpovede či už na broadcastové adresy, alebo ich lokálne adresy (prvotná idea broadcastových adries bola niečo ako „ukáž mi, kto je na sieti“). Systémy, ktoré sú nesprávne nakonfigurované a odpovedajú na požiadavky ICMP na broadcastovú adresu, sa

Ako (ne)skrachovala moja firma

Príbeh o dvoch (ne)bezpečných riešeniach

Julo: Zdravím ťa, Tonko, dávno som ťa nevidel. Ako sa darí firme?

Tóno: Ahoj. Ty nevieš, že ja už skoro nemám firmu?

Julo: Čo sa stalo? Veď len nedávno si kúpil nový informačný systém, prijal nových ľudí...?

Tóno: To je na dlhšie. Pozvi ma na pivo a poviem ti.

Julo: No tak poď a rozprávaj.

Tóno: Poznal si moju firmu. Všetko išlo dobre, pokiaľ som mal tých pár ľudí, niekoľko počítačov, telefónov a fax. Potom sme kúpili nový soft, počítače zosieťovali a pripojili na internet.

Julo: No a čo? Ja tiež mám firemnú sieť.

Tóno: Začalo sa to nevinne. Zamestnanci začali popri práci surfovať na webe, kdekade sa registrovali a stahovali všelijaké hlúposti. Výsledok si vieš domyslieť. Čoskoro sme nerobili takmer nič iné, len riešili infikované počítače a napravovali spôsobené škody. Keď som chcel odpovedať klientom na e-mail, vyše pol hodiny som vymazával reklamnú poštu od predavačov Viagry a podobných artefaktov. Tuším sa to volá spam.

Julo: A prečo si to neriešil? Ja som v systéme nastavil podmienky na surfovanie tak, že som zamestnancom zamedzil nebezpečné stránky. Volá sa to blacklist. To si nevedel?

Tóno: Nie.

Julo: A aj automatické filtrovanie stránok, kde podľa obsahu stránky zamestnanec nemá čo robiť. Napríklad porno, čety a iné zábavky. A popritom o každom jednom viem, kde, kedy a koľko surfuje.

Tóno: A to sa dá?

Julo: Jasné. Dá sa viac. Teraz mám systém nakonfigurovaný tak, že mi analyzuje každý jeden e-mail a pustí len to, čo je neškodné, a spam odfiltruje. A o vírusoch ani nehovorím.

Tóno: To som mal vedieť vtedy. Ale počúvaj, to ešte nebolo všetko. Vieš, že som mal obchodníkov, ktorí boli skoro stále v teréne. Tak som im dal notebooky, aby mohli kedykoľvek pristupovať k aktuálnym firemným dátam.

Julo: Veď to je dnes bežné.

Tóno: Ale potom sa začali diať čudné veci. Začali miznúť objednávky, strácali sa faktúry a napokon aj tie nešťastné prevody na firemných účtoch.

Julo: Ty si fakt mimo. Volá sa to phishing, čo je z anglického password fishing. To znamená, že ak nemáš dobre zabezpečenú sieť, možno sa ti tam nejaký „konkurent“ naozaj dostal.

Tóno: To myslíš vážne?



Julo: Pozri, môj systém mi sústavne monitoruje neoprávnenú alebo neobvyklú aktivitu siete, zabezpečuje šifrovaný prenos a prístup k citlivým dátam. A pritom je to urobené tak dobre, že aj moji ľudia sa dostanú len k tomu, čo im jednotlivo povolim.

Tóno: To je to, čo sa volá firewall?

Julo: Áno, aj. Ale kompletne sa to riešenie volá KERBER. Všetko to máš v zopár moduloch a ovládanie v solídnom grafickom rozhraní. Keď vieš obsluhovať fax a mobil, naučíš sa robiť aj s Kerberom.

Tóno: Takže ak zabezpečím sieť, môžem odblokovávať účty a v pokoji sa venovať obchodu?

Julo: Jasné, ale daj si ešte pivo a dám ti kontakt na spoločnosť, čo ti o produkte KERBER povie viac, a rovno si ho môžeš aj objednať.

Tento príbeh je vymyslený. Reálne ohrozenie vašej firemnej siete je však skutočné. Rovnako skutočný je aj KERBER.

KERBER STRÁŽI VAŠE PODNIKANIE



SOMI Systems a. s.

ČSA 25, 974 01 Banská Bystrica

e-mail: obchod@somis.sk

www.kerber.sk

nazývajú *smurf amplifiers*. Útok sa vykonáva sfalšovaním zdrojovej adresy IP (adresa IP obeť) a takéto pakety sa následne smerujú na *smurf amplifiers*. Každý hosťiteľ pošle odpoveď zaslaním paketu v podobe odpovede (pokiaľ je „živý“). Takýmto spôsobom sa obeť na základe pôvodných požiadaviek ICMP sama zahltí a môže dôjsť ku kompletnému kolapsu. Brániť sa proti útokom *smurf* môžeme pomocou Smurf Amplified registra, ktorý spravuje databázu sietí, ktoré sú nesprávne nakonfigurované a môžeme ich na našich systémoch filtrovať.

ping flood – tento útok spočíva v zahltení systémom obrovským množstvom ping paketov. Podmienkou úspešnosti útoku je väčšia šírka pásma na útočnicovej strane. V linuxových distribúciách možno takýto útok vykonať jednoduchým príkazom *ping -f*. Obranou môže byť nastavenie rate-limitu na odpovede na ping, prípadne úplné filtrovanie takýchto požiadaviek.

Teardrop – útok *teardrop* používa na znefunkčnenie obeť zasielanie priveľkých a prekryvajúcich sa IP fragmentov, čo v prípade zlej implementácie TCP/IP v niektorých operačných systémoch môže spôsobiť až pád. Na tento útok sú náchylné operačné systémy Windows 3.1x, Windows 95, Windows NT a linuxové kernely verzie 2.0.32 a 2.1.63.

Nuke bomby – sú to pakety, ktoré využívajú chyby v aplikačných protokoloch, typickým príkladom je chyba v NetBIOS na systémoch Windows 95. Útok pozostával zo špeciálne upraveného (zničeného) paketu, ktorý na základe chyby spôsobil pád cieľového systému.

Komplexná ochrana proti útokom DoS a DDoS je aj IPS (Intrusion Prevention System), ktorý na základe prednastavených typov útokov dokáže reagovať filtrovaním takýchto požiadaviek.

DoS nemusí nevyhnutne pochádzať zo siete. Môže mať napr. povahu zneužitia aplikačných chýb a tým zahltenia CPU, RAM alebo iných hardvérových prostriedkov.

Neautorizovaný prienik – pokus o neautorizovaný prienik je taký všeobecný problém, že je vskutku zložitá opísať ho širšie. Zahŕňa obrovské množstvo rôznych druhov útokov. Cieľom týchto útokov je získať prístup k zdrojom, ku ktorým útočník nemá prístup (napr. možnosť vykonávať príkazy – shell), na základe chýb na systémoch či už z aplikačného hľadiska (napr. bug vo web serveri), alebo z hľadiska konfigurácie systému (napr. laicky napísaný PHP alebo CGI skript). Vo väčšine prípadov sú kompromitované servery, ktoré sa využívajú na ďalšiu nekalú činnosť útočníka, ako napr. redirektor iných útokov (čím viac redirektorov útočník použije, tým ťažšie je vystopovateľný) alebo ako nody pre spomínaný DDoS. Cieľom útočníka môžu byť aj dáta. Predstavte si situáciu, kde bol kompromitovaný váš firemný server, ktorý slúži ako centrálna úložisko dokumentov (informácie o zákazníkoch, firemná agenda, faktúry, zmluvy a pod.). Netreba asi zdôrazňovať, ako môžu byť takéto dáta využiteľné pre konkurenciu. Takisto sa môže stať, že útočníkom nebude vaša konkurencia, ale jednoducho script kiddies (vo voľnom preklade niekto, kto nevie, ako veci fungujú, ale používa verejne prístupné exploity na prienik), ktoré vám tie dáta zmažú.

Ako sa teda proti takýmto prienikom brániť?

Zálohy – pokiaľ nastane uvedená situácia, vždy máte možnosť návratu dát.

Single point of failure – snažte sa zabezpečiť takým spôsobom, aby sa na jednom systéme nenachádzali všetky služby (napr. firewall, IPS, mail server, file server). Keď útočník prelomí firewall, stále nemá prístup k mailom alebo file serveru.

Aktualizácia – pravidelnou aktualizáciou zabezpečíte, že sa na systéme nebudú nachádzať všeobecné diery a bugy a útočník bude mať v prípade útoku sťaženú situáciu.

Správne heslá – nastavujte zásadne len zložené heslá. Pokiaľ sa pozriete do logov svojho

systému, určite narazíte na množstvo robotov, ktoré skúšali rôzne útoky na uhádnutie hesla (v prípade robotov ide zväčša o slovníkové typy útokov).

Firewall – môžeme ním zabezpečiť prístup k jednotlivým službám, ktoré bežia na systéme, a jednoducho ním môžeme určiť, kto má a kto nemá prístup, na základe viacerých kritérií, ako je napr. zdrojová adresa IP alebo adresa MAC (v prípade lokálnej siete, keďže TCP/IP sa nachádza len v tretej a štvrtej vrstve modelu ISO/OSI, ako sme spomínali na začiatku, a adresa MAC patrí do druhej vrstvy).

VPN (Virtual Private Network) – vystavujte na internete len tie systémy, ktoré tam vyslovene musia byť. Zvyšné systémy, s ktorými potrebujete komunikovať len v rámci firemnej infraštruktúry, umiestnite do VPN, kde je komunikácia šifrovaná a systémy nie sú priamo viditeľné z internetu. Vďaka šifrovaniu je zaistená relatívna bezpečnosť prenášaných dát, no vždy je tu riziko útokov, ktoré smerujú zvnútra siete.

Sieťová bezpečnosť je zložitá problematika a netreba ju brať na ľahkú váhu, pretože v konečnom dôsledku môže mať na podnikanie fatálny dosah, či už v podobe odcudzených, alebo stratených dát, ale aj nefunkčných systémov (predstavte si svoju spoločnosť bez mailovej alebo internetovej komunikácie hoci len 24 hodín). Takisto treba mať na zreteli, že úroveň zabezpečenia nesmie byť prekážkou v reálnej práci, a preto treba hľadať vhodný kompromis medzi zabezpečením a obťažovaním používateľov systémov, lebo v prípade, že tí začnú predpísanú bezpečnostnú politiku obchádzať, môže prísť k neželaným dôsledkom.



■ MICHAL ŽILA
systémový administrátor
SOMI Systems a.s.

IT NEWS Google captcha úspešne prelomená

Nedávno spoločnosť Websense publikovala na svojom blogu veľmi zaujímavé informácie. Spoločnosti sa podarilo pri skúmaní bližšie nešpecifikovaného malwaru objaviť servery, ktoré bezplatne „lámú“ Google captchu a výsledok potom poskytujú ako text. Spameri vďaka týmto serverom vytvárajú obrovské množstvo kont Gmail, ktoré potom používajú na spamovanie. Úspešnosť je až 20 % (1 z 5 pokusov). Ak neviete, čo je to CAPTCHA, môžete si o nej prečítať na stránkach Wikipédie. Preto vynakladajú spameri toľko úsilia na vytvorenie automatizovaného systému na registráciu do free webmailov? Dôvodom je hneď niekoľko. V prvom rade vysoká anonymita. Vystopovať osobu, ktorá sa zaregistrovala napríklad na Gmail, je veľmi zložitá, nehovoriac o prípade, ak sa zaregistruje robot (malware) z napadnutého počítača obeť. Potom je akékoľvek úsilie odhaliť páchatela bezpredmetné. Ďalší dôvod je, že Gmail nikdy nebude zablokovaný alebo

označený ako spam. To značí, že každý e-mail z Gmailu vám príde do schránky, pretože nie je považovaný za spam. Tretia výhoda je obrovská masa používateľov. Je veľmi výhodné pre spamera používať server, ktorý je známy a populárny. V neposlednom rade je výhodou aplikačná kapacita populárnych webmailov. Je prakticky nepravdepodobné, že by Gmail „spadol“ po masívnom rozosielaní miliónov e-mailov v priebehu krátkej chvíle. To je jeho štandard a je na to pripravený, teda spamer sa môže schovať „v dave“. Potom je úspešnosť spamu oveľa vyššia – a tým aj zisky z neho. Preto sa spamerom oplatí dať si obrovskú námahu vytvoriť automatizovaný registračný systém, ako aj systém na „lámanie“ captcha. Podľa výskumu firmy Websense existujú servery (pravdepodobne v Rusku), ktoré fungujú ako Software as a Service (softvér ako služba, príkladom môže byť on-line konvertovacia služba Zamzar). Tieto servery akceptujú obrázky captcha z Google a následne sa snažia identifikovať text,

ktorý obsahujú (samozrejme zadarmo). Úspešnosť je veľmi zaujímavá, každý piaty obrázok captcha je úspešne prelomený a prevedený na text. To značí až 20-percentnú úspešnosť. Taktom možno vytvoriť státisíce účtov a poslať milióny spamov každý deň a stále využívať opísané benefity. Websense zatiaľ nevie (alebo nepublikovala) spôsob prelomenia captcha, ale pravdepodobných scenárov je päť.

- Existuje databáza ID (názov obrázka) a ich preklad na normálny text
- Používa sa veľmi pokročilý OCR skener na rozpoznanie textu
- Používa sa matematický softvér na výpočet hashu, ktorý je priradený k textu
- Najpravdepodobnejšie sa používa hlasový skener na hlasovú captchu, ktorá existuje ako alternatíva pre zrakovo postihnutých návštevníkov
- Veľmi populárne hlavne v Číne – využíva sa ľudský faktor. Lacní zamestnanci prepisujú celé hodiny captchu ručne

„Zvuková“ metóda patrí k tým najjednoduchším, aj keď sa vám to na prvý pohľad nemusí zdať. Existuje niekoľko veľmi šikovných riešení, ktoré dosahujú úspešnosť 98 % na „čistom“ hlase (bez postranných efektov, skreslenia zvuku atď.).

Naopak, veľmi nepravdepodobná je posledná metóda, aj keď ju veľmi hojne využívajú spameri a iné kriminálne živly po celom svete. Najčastejšie sú najímami bežní ľudia v Číne, ktorí za hodinu práce dostanú niekoľko centov až dolár. Ich pláca býva často trojnásobná oproti zvyšku rodiny, ktorý pracuje na poli. Odporcovia captcha už dlhší čas poukazujú na slabú schopnosť jednoslovej captcha ochrániť formuláre pred robotmi. Dnes prevláda názor, že by sa tvorcovia portálov nemali uchýľovať k vytváraniu vlastných riešení, ale používať originálny projekt. Nemôžem s týmto názorom nesúhlasiť a rovnako chcem dodať, že niektoré služby majú šialenú captchu, ktorá je takmer nečitateľná, ako napríklad IMDB. Keby autori podporili (aj finančne) už existujúci projekt, captcha by mohla dosahovať veľmi dobrú úroveň (netvrdím, že dnes nedosahuje). Už dnes je úspešnosť prelomenia viacslovnej captcha na úrovni promile. Ďalším dôkazom môže byť prípad, ktorý sa stal len nedávno. Partia ruských hackerov prelomila captchu Yahoo! a dosiahla až 35 % úspešnosť. Viac sa môžete dočítať v článku spoločnosti Websense.

■ RASTISLAV TUREK

