Obrana před útokem DRDoS

Vložil/a cm3l1k1 [1], 14 Říjen, 2004 - 17:32

- Hacking [2]
- Hacking method [3]
- Security [4]

Napadení internetových serverů, při nichž se je útočníci snaží zahltit množstvým falešných požadavků na poskytnutí nějakých služeb nebo dat, nejsou dnes ničím zvlášť neobvyklím. Komplikovanost obrany je závislá jak na intenzitě útoku, tak na jeho přesném druhu. V CW 6/2003 se článek věnoval novějšímu typu útoku DRDoS – a v následujícím textu se zaměříme na způsob, jak mu čelit.

Tento článek vyšel v Computerworldu 14/2003 (http://www.cw.cz [5])

Napadení internetových serverů, při nichž se je útočníci snaží zahltit množstvým falešných požadavků na poskytnutí nějakých služeb nebo dat, nejsou dnes ničím zvlášť neobvyklím. Komplikovanost obrany je závislá jak na intenzitě útoku, tak na jeho přesném druhu. V CW 6/2003 se článek věnoval novějšímu typu útoku DRDoS – a v následujícím textu se zaměříme na způsob, jak mu čelit.

Jen pro připomenutí: Nová forma SYN flood útoku nazvaná **DRDoS (Distributed Reflection Denial of Service)** funguje tak, že útočník posílá na spoustu serverů v internetu pakety s příznakem SYN (pro inicializaci spojení), přičemž jako cílová je nastavena adresa „obětního“ serveru, tedy serveru, na který je útok směrován.

Servery přijmou SYN paket a odešlou paket s příznakem SYN/ACK na podvrženou adresu cílového serveru jako potvrzení inicializace spojení. Ten si ale žádné spojení nevyžádal, a tak paket zahodí. Správně by vše mělo fungovat tak, že server, který chce inicializovat spojení, pošle SYN paket, přijme jako potvrzení SYN/ACK a vše potvrdí ACK paketem (Three-Way Handshake). Cílový server ale SYN/ACK pakety zahodí, takže útočníkem využívané servery nedostanou zpět ACK potvrzení a v domění, že se paket někde ztratil, ho pošlou znovu. To se opakuje stále dokola. Tak se velmi zvýší intenzita útoku a cílový server nakonec zahltí SYN/ACK pakety.

S tímto typem útoku se přibližně před rokem setkal Steve Gibson, prezident společnosti Gibson Research, o kterém byla řeč v již zmíněném Computerworldu 6/2003. Na servery společnosti GRS se útočilo po dobu čtyř hodin, což způsobilo nemalé problémy. Jak již řekl Steve Gibson:“Filtrování příchozích paketů nepomáhá, protože to zpomaluje veškerý provoz a navíc útok přichází z mnoha IP adres.“ Pokud by ISP cílového serveru zablokoval veškeré pakety směrované na něj, tak by vlastně útočníkovy vyšlo celé jeho snažení – došlo by k nedostupnosti síťových služeb. Ke konci Gibson dodal:„Ale co se s tím dá dělat?“ Nabízím vám řešení.

Jak se bránit?

Cílový server (oběť) přece pakety SYN/ACK nemusí zahazovat, ale na zdrojové adresy (nevyžádaných spojení) může poslat RST paket. Co se stane? Vysvětleme si to na příkladě.
Útočník provede útok a jím využívané servery pošlou cílovému serveru paket SYN/ACK, ale už nebudou neustále posílat pakety v domění, že se ztratily, protože po obdržení RST paketu (reset – žádost o vynulování spojení) se ukončí plánovaná relace. Přerušíme tak nárust požadavků a tím zvýšení intenzity útoku.

Tohoto chování můžeme docílit správným nastavením IDS (Intrusion Detection System – systém

detekce průniku). Pokud váš IDS toto nastavení neumožňuje, nebo ho dokonce nemáte, vyzkoušejte nějaký zdarma šiřitelný IDS. Pro platformu Windows doporučuji produkt Snort (http://www.snort.org [6]), pro Linux Snort, nebo Trisentry (http://www.linuxzone.cz/index.phtml?ids=1&idc=94 [7]). Správné nastavení Snortu je náročné a rozhodně není vhodné pro lidi, kteří v této oblasti nemají žádné zkušenosti.

Alternativa

Další možný způsob ochrany je ten, že IDS nebude automaticky posílat RST paket, ale v případě zjištění DRDoS útoku spustí určitý program (detekci by mohl provést i tento program). Ten by si, pokud by šlo o open source, mohl každý administrátor upravit podle sebe. Program by měl být rychlý a měl by se spustit jen v případě útoku (s kontaktovaním administrátora), aby zbytečně nezatěžoval procesor. Kromě příznaku RST by mohl ještě přidat příznak URG (urgentní data, paket se zpracovává přednostně).

Velkou výhodou tohoto způsobu je to, že cílový server bude pořád normálně pracovat, tj. uživatelé se budou moci normálně připojit a využívat všech jeho služeb. Mimo jiné, abyste se vyhnuli určitému zatížení procesoru při odpovídání na SYN/ACK pakety, můžete požádat svého ISP, aby toto pravidlo aplikoval na jeho systémech. K vašemu serveru se tím pádem nedostane jediný útočníkem mířený paket.

Naprostá většina těchto útoků je právě (jak také uvedl Steve Gibson) vedena od lidí, kterým cílový server nějakým způsobem „vadí“. Takže si stáhnou nějakou utilitku z internetu, která tento útok umožňuje, a zahají ho. Podle mého názoru nemá nikdo takové připojení, aby mohl zahltit systém ISP (Internet Service Provider). Pokud by byl útok veden organizovanou skupinou, tak by k tomu dojít mohlo, ale to se stává velmi vyjímečně a vetšina útoků je v současné době vedena „z domova“. **Uvedený způsob je vhodnou obranou před DRDoS útoky a spoustě administrátorům může ušetřit nemalé problémy s útokem spojené.**

Trisentry - Trisentry je jednoduchý IDS k monitorování neobvyklých aktivit v systému. Obsahuje tři komponenty:
• hostsentry: tato komponenta analyzuje zvyky uživatelů, které se týkají interaktivní práce se systémem - monitoruje obvyklé časové rozmezí, kdy a odkud jsou jednotliví uživatelé přihlášeni a vyhodnocuje neobvyklá přihlášení.
• portsentry: je nástroj pro detekci příchozích port skenů, může na pokusy o skenování portů aktivně reagovat úpravou konfigurace tcp_wrappers či firewallu a tím předejít možnému útoku zvenčí.
• logsentry (dříve logcheck): tato komponenta usnadňuje adminstrátorovi systému analýzu systémového logu tím, že z něj vybírá neobvyklé události.
(pozn. Zdroj http://www.linuxzone.cz/index.phtml?ids=1&idc=94 [7])

SNORT - Jedná se o vynikající analyzér procházejících paketů (sniffer) a účinný detekční program pro odhalování bezpečnostních chyb v systému. Umožňuje detailní logování založené na definovaných pravidlech. Dokáže odhalit nejrůznější druhy útoků, scannování apod., umí velmi dobře spolupracovat i se Sambou.

(pozn. Zdroj [trisentry/snort] http://www.root.cz/clanek/1055 [8])

pozn. tento clanek jsem napsal v 16-ti letech, ted se na vec divam uz trochu jinak...

URL článku: https://www.security-portal.cz/clanky/obrana-p%C5%99ed-%C3%BAtokem-drdos

Odkazy:
[1] https://www.security-portal.cz/users/cm3l1k1
[2] https://www.security-portal.cz/category/tagy/hacking
[3] https://www.security-portal.cz/category/tagy/hacking-method
[4] https://www.security-portal.cz/category/tagy/security
[5] http://www.cw.cz
[6] http://www.snort.org

[7] http://www.linuxzone.cz/index.phtml?ids=1&idc=94
[8] http://www.root.cz/clanek/1055