elektrorevue
ISSN 1213 - 1539

Rok / Year:	Svazek / Volume:	Číslo / Number:	Jazyk / Language
2017	19	2	CZ

Generátor kybernetických útoků

Generator of Cyber Attacks

Jakub Frolka, Peter Halaška, Jan Hajný, David Smékal

frolka@feec.vutbr.cz, xhalas07@stud.feec.vutbr.cz, hajny@feec.vutbr.cz, smekal@phd.feec.vutbr.cz

Fakulta elektrotechniky a komunikačních technologií VUT v Brně

DOI: -

Abstract: The article deals with the security of computer networks based on TCP / IP protocol suite, in particular, testing the resistance to DDoS attacks and tools for generating malicious traffic. In the article the selected tools Hping3, Mausezahn and Trafgen are analyzed. For these tools the results of comparative measurements are presented. Based on the results of the experimental tests, the main contribution of this paper is design and implementation of the new tool for generation of DDoS attacks and its subsequent performance testing for individual attacks. The tool also has a unique web interface for its easier usage.

elektrorevue
ISSN 1213 - 1539

Rok / Year:	Svazek / Volume:	Číslo / Number:	Jazyk / Language
2017	19	2	CZ

Generátor kybernetických útoků

Generator of Cyber Attacks

Jakub Frolka, Peter Halaška, Jan Hajný, David Smékal

frolka@feec.vutbr.cz, xhalas07@stud.feec.vutbr.cz, hajny@feec.vutbr.cz, smekal@phd.feec.vutbr.cz

Fakulta elektrotechniky a komunikačních technologií VUT v Brně

DOI: -

Abstract: The article deals with the security of computer networks based on TCP / IP protocol suite, in particular, testing the resistance to DDoS attacks and tools for generating malicious traffic. In the article the selected tools Hping3, Mausezahn and Trafgen are analyzed. For these tools the results of comparative measurements are presented. Based on the results of the experimental tests, the main contribution of this paper is design and implementation of the new tool for generation of DDoS attacks and its subsequent performance testing for individual attacks. The tool also has a unique web interface for its easier usage.

elektrorevue
ISSN 1213 - 1539

Generátor kybernetických útoků

Jakub Frolka, Peter Halaška, Jan Hajný, David Smékal

Fakulta elektrotechniky a komunikačních technologií VUT v Brně
Email: frolka@feec.vutbr.cz, xhalas07@stud.feec.vutbr.cz, hajny@feec.vutbr.cz, smekal@phd.feec.vutbr.cz

Abstrakt *– Článek se zabývá bezpečností počítačových sítí založených na protokolové sadě TCP/IP, konkrétně testováním odolnosti proti DDoS útokům a nástroji na generování škodlivého provozu. V článku jsou analyzovány vybrané nástroje, Hping3, Mausezahn a Trafgen. Dále jsou pro tyto nástroje uvedeny výsledky porovnávacích měření. Na základě získaných výsledků z experimentálních testů, je hlavním přínosem článku návrh vlastního nástroje pro generování DDoS útoků a jeho následné výkonnostní testování pro jednotlivé útoky. Vytvořený nástroj také obsahuje unikátní webové rozhraní pro jeho snadnější ovládání.*

1 Úvod

S neustálým rozšiřováním možností datových komunikací a Internetu samotného je potřeba se věnovat i jejich nedílné součásti a to kybernetickým útokům. Velkým podílem jsou zastoupeny útoky založeny na bezpečnostních dírách TCP/IP (Transmission Control Protocol/Internet Protocol) protokolů, které mají za úkol omezení, nebo úplné odepření dostupnosti služeb. Tyto útoky nazýváme DoS (Denial of Service) útoky. Rozšířenou variantou DoS útoků jsou DDoS (Distributed Denial of Service), kdy je využíváno infikovaných zařízení tzv. agentů (botů). Protože DDoS útoky pochází z více zařízení, je těžší identifikovat nežádoucí komunikaci v té žádoucí a následně se proti ní bránit [1, 2]. Dle bezpečnostního reportu firmy Radware [3] tvořily v roce 2014 a 2015 právě útoky DDoS největší podíl všech kybernetických útoků. Z DDoS útoku je konkrétně útok typu SYN flood nejvíce rozšířený [3, 4].

V současnosti se pozornost soustředí na výzkum, vývoj a implementaci hardwarových generátorů provozu [5, 6]. Tato zařízení, přestože velmi výkonná, jsou složitě rozšiřitelná a neobsahují nejnovější typy útoků. Tyto slabiny hardwarových generátorů se v tomto článku snažíme odstranit použitím softwarových generátorů. Ty doposud nebyly podrobněji zkoumány především z výkonnostních důvodů. V tomto článku však představíme výsledky, které potvrzují dostatečný výkon těchto generátorů, pokud jsou správně nakonfigurovány. Z velkého množství nástrojů byly vybrány nástroje, které umožňují generovat útoky SYN flood, UDP flood, RST flood, ICMP flood, ARP flood, DNS flood a DHCP starvation. Čtenář může najít více podrobností o útocích například v [3, 7]. Vybranými nástroji jsou Hping3, Mausezahn a Trafgen, které jsou v následující kapitole popsány a porovnány, pomocí výsledků měření pro útoky SYN flood a UDP flood z hlediska počtu paketů za sekundu (p/s) a vytížení linky (MB/s).

Většinu nástrojů pro generování síťového provozu lze ovládat pouze z příkazového řádku. Ty nástroje, které obsahují grafické rozhraní, jsou často zpoplatněny, to je jeden z hlavních důvodů, který vedl k vytvoření nového nástroje, jenž je popsán v předposlední kapitole. Nově vytvořený nástroj, který nese název DosGen, je založen na jádru nástroje Trafgen. Pro DosGen byly vytvořeny šablony útoků a následně vytvořeno webové ovládací rozhraní, které uživateli zjednodušuje jeho ovládání. Tento nástroj byl také otestován a jeho výsledky prezentovány.

2 Nástroje pro DoS útoky

V současné době existuje mnoho nástrojů na provedení DoS/DDoS útoků vytvořených v různých programovacích jazycích, podporující různé typy útoků. Pro účely tohoto článku byly vybírány nástroje, které jsou vytvořeny v jazyce C a jsou volně šiřitelné pod licencí GNU GPL (GNU General Public License).

2.1 Hping3

Hping3 je nástroj určený pro generování a analýzu paketů patřící protokolové sadě TCP/IP. Je určen pro testování a ověření zabezpečení počítačových sítí, směrovačů, firewallů a dalších. Také umožňuje vytváření uživatelských skriptů pro manipulaci a analýzu paketů, pomocí jazyka Tcl (Tool Command Language). Dále podporuje zobrazení odpovědí od zařízení na kterých byl prováděn útok, podobně jako nástroj ping protokolu ICMP (Internet Control Message Protocol) a jeho odpovědi. Jeho výchozím podporovaným protokolem je TCP, ale podporuje i protokoly IP, ICMP a UDP (User Datagram Protocol) s libovolným nastavením jednotlivých položek v jejich hlavičkách. Program je volně šiřitelný pod licencí GNU GPL, disponuje textovým rozhraním a je určen pro operační systémy Linux, FreeBSD, Solaris, Windows a další. Jeho autorem je Salvatore Sanfilippo [8].

2.2 Mausezahn

Jedná se o rychlý generátor síťového provozu, který je využíván k testování VoIP (Voice over Internet Protocol) a multicastových sítí, ale také na ověření zabezpečení

elektrorevue
ISSN 1213 - 1539

a odolnosti počítačových systémů a sítí. Může být také použit pro hledaní chyb síťových aplikací, testování počítačových sítí při nestandardních situacích (jaké jsou např. při vlivu záplavy záměrně poškozených paketů, nebo zátěžových testů). Podporuje základní protokoly jakou jsou ARP (Address Resolution Protocol), IP, ICMP (částečně), TCP, UDP a další. Program je volně šiřitelný pod licencí GNU GPL, disponuje textovým rozhraním (podobnému k CISCO příkazovému prostředí). Nástroj je určen výhradně pro operační systém Linux a jeho autorem je Herbert Haas. Od smrti autora roku 2011 je udržován vývojářským týmem sady nástrojů Netsniff-NG, kterou je součástí [9, 10].

2.3 Trafgen

Trafgen je také, jako Mausezahn, součástí sady nástrojů Netsniff-NG. Jedná se o rychlý generátor síťového provozu určený k výkonnostnímu testování počítačových sítí a také k funkčnímu testování softwaru vkládáním na vstup programu náhodných, chybných nebo neočekávaných dat. Nástroj implicitně využívá maximální počet procesů, podle toho, kolik je dostupných procesorů (jader) na daném zařízení, toto implicitní nastavení je také umožněno manuálně změnit. Trafgen také umožňuje sestavení jednotlivých paketů pomocí vlastního nízkoúrovňového konfiguračního jazyku.

Mezi hlavní výhody nástroje Trafgen patří jeho funkce na principu tzv. zero-copy modelu. To znamená, že jádro operačního systému (kernel), při odesílání paketů nemusí z jeho prostoru odevzdávat kopii do uživatelského prostoru a opačně. Tím dochází ke zkrácení režijního času a snížení nároku na systémové zdroje daného zařízení. Jeho jedinou nevýhodou je nemožnost sestavení plnohodnotné relace komunikace.

Nástroj je volně šiřitelný pod licencí GNU GPL, disponuje textovým rozhraním a je určený pro distribuce OS Linux. Jeho autorem je Daniel Borkmann [11].

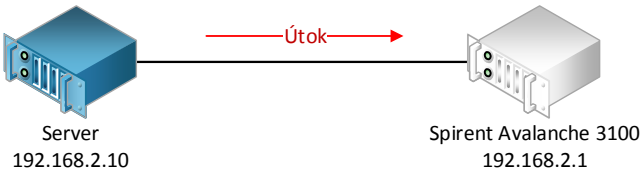
2.4 Experimentální porovnání nástrojů

Praktické porovnání nástrojů bylo soustředěno na určení nástroje, který dokáže generovat největší počet paketu za sekundu (p/s), zároveň bylo provedeno měření zaměřené na vytíženost linky (MB/s). Měření bylo provedeno v laboratorním prostředí a bylo zaměřeno na útoky SYN flood a UDP flood.

Nástroj Hping3 byl použit ve verzi 3.0.0-alpha-2, nástroj Mausezahn ve verzi 0.4.0 a nástroj Trafgen ve verzi 0.6.0. Měřené hodnoty byly získány způsobem, kdy po ustálení rychlosti nástrojů bylo odečteno pět hodnot a jejich průměr tvořil výslednou hodnotu.

Vybrané nástroje byly porovnány na experimentálním pracovišti, které je zobrazeno na obrázku 1, jehož podrobná konfigurace je následující:

- Server (generátor DoS útoků):
  - procesor: Intel® Xeon® L5520 @ 2,27 GHz, 8 MB cache, 4 jádra,
  - RAM: 32 GB,
  - NIC: 1 GbE, 10 GbE,
  - OS: Linux Ubuntu 14.04.3 LTS, 64bit, kernel: 3.13.0-68-generic.
- Měřící zařízení: Spirent Avalanche 3100.



Obrázek 1: Schéma zapojení zařízení v laboratoři.

Server obsahující operační systém Ubuntu byl použit jako generátor DoS útoků pro testování jednotlivých nástrojů. Vybrané nástroje byly postupně použity pro generování útoků, které byly cíleny proti měřícímu zařízení, které emulovalo běžný server poskytující služby uživatelům. Jako měřící zařízení byl použit Spirent Avalanche 3100 s programem Spirent TestCenter Layer 4–7 Application, který je určen na zátěžové a bezpečnostní testování síťových infrastruktur, webových aplikací, Triple Play systémů a dalších [5]. Měřící zařízení Avalanche při jednotlivých útocích sbíral statistiky, které jsou na konci této kapitoly prezentovány.

Aby mohly být vybrané nástroje porovnatelné, musí být testovány za stejných podmínek. Jednou z nich je velikost odesílaných paketů.

Nástroj Mausezahn implicitně podporuje TCP SYN paket o velikosti 74 B, kdežto nástroje Hping3 a Trafgen 54 B, proto byla hodnota 74 B zvolena jako společná. Aby bylo dosaženo stejné hodnoty 74 B u nástrojů Hping3 a Trafgen, byla do datové části paketů vložena výplň o velikosti 20 B. Minimální velikost UDP paketu bylo možné nastavit pro všechny nástroje na hodnotu 42 B a proto byla také použita.

Další společná nastavení:

- náhodná zdrojová IP adresa,
- staticky definovaná cílová IP adresa,
- náhodný zdrojový port,
- staticky definovaný cílový port.

Uvedené podmínky a nastavení platí pro útoky SYN flood i UDP flood. Protože SYN flood je založen na protokole TCP, je dalším použitým nastavením náhodné sekvenční číslo.

V tabulce 1 jsou uvedeny výsledky měření útoku SYN flood při použití síťového rozhraní NIC_{1GbE}, v tabulce 2 jsou výsledky pro rozhraní NIC_{10GbE}. V tabulkách 3 a 4,

elektrorevue
ISSN 1213 - 1539

jsou zaznamenány naměřené hodnoty pro útok UDP flood pro rozhraní NIC_{1GbE} a NIC_{10GbE}.

Pro přehlednost jsou naměřené hodnoty zobrazeny v grafu na obrázku 2, který porovnává nástroje v počtu paketů za sekundu a v grafu na obrázku 3 podle vytíženosti linky. Na základě těchto výsledku je zřejmé, že nejvyšších hodnot v odeslání paketů za sekundu, tak i vytíženosti linky, dosáhl nástroj Trafgen.

Důvodem pro tyto výrazné rozdíly v dosažených výsledcích je samotná funkce nástroje Trafgen a to především schopnost využívat více vláken procesoru a zero–copy mechanizmu.

Tabulka 1: Naměřené hodnoty při útoku SYN flood při použití NIC_{1GbE}.

Nástroj	**Počet paketů za sekundu [p/s]**	**Vytíž. linky [MB/s]**
Hping3	489 000	36
Mausezahn	400 000	30
Trafgen	1 170 000	87

Tabulka 2: Naměřené hodnoty při útoku SYN flood při použití NIC_{10GbE}.

Nástroj	**Počet paketů za sekundu [p/s]**	**Vytíž. linky [MB/s]**
Hping3	513 000	38
Mausezahn	400 000	30
Trafgen	6 657 000	493

Tabulka 3: Naměřené hodnoty při útoku UDP flood při použití NIC_{1GbE}.

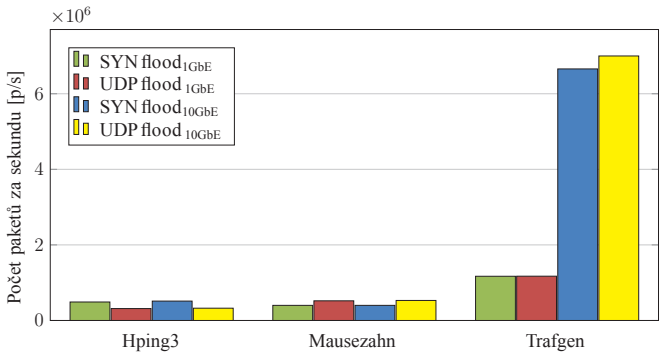
Nástroj	**Počet paketů za sekundu [p/s]**	**Vytíž. linky [MB/s]**
Hping3	315 000	19
Mausezahn	520 000	31
Trafgen	1 172 000	71,5

Tabulka 4: Naměřené hodnoty při útoku UDP flood při použití NIC_{10GbE}.

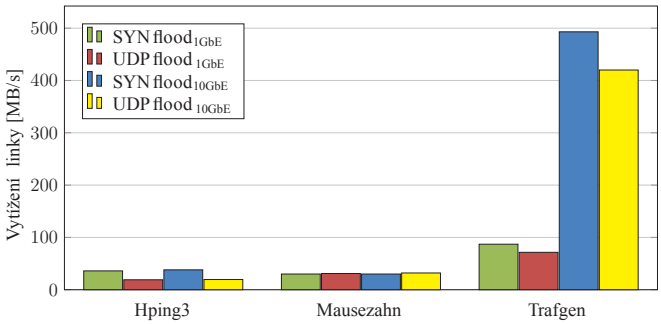
Nástroj	**Počet paketů za sekundu [p/s]**	**Vytíž. linky [MB/s]**
Hping3	325 000	19,5
Mausezahn	530 000	32
Trafgen	7 000 000	420

3 Nástroj DoSgen a jeho testování

V této kapitole je popsán vlastní návrh a implementace testovacího nástroje DoSgen, na základě výsledků uvedených



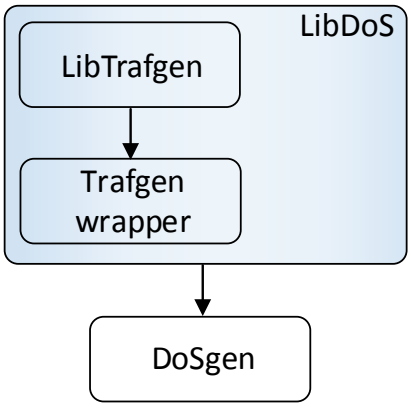
Obrázek 2: Porovnání nástrojů v počtu přenesených paketů za sekundu.



Obrázek 3: Porovnání nástrojů ve vytíženosti linky.

na konci kapitoly 2.4, byl vybrán nástroj Trafgen a následně jeho jádro vyjmuto ze sady nástrojů Netsniff-NG. Jádro Trafgenu bylo použito pro vytvoření knihovny, která je základem nového nástroje s názvem DoSgen.

Nástroj DoSgen je vytvořen v programovacím jazyku C a určen pro distribuce OS Linux. Jeho blokové schéma je znázorněno na obrázku 4.



Obrázek 4: Blokové schéma nástroje DoSgen.

Hlavní částí nástroje DoSgen je knihovna LibDos, která sdružuje dva moduly:

- LibTrafgen: nově vytvořená knihovna, která vznikla z nástroje Trafgen,

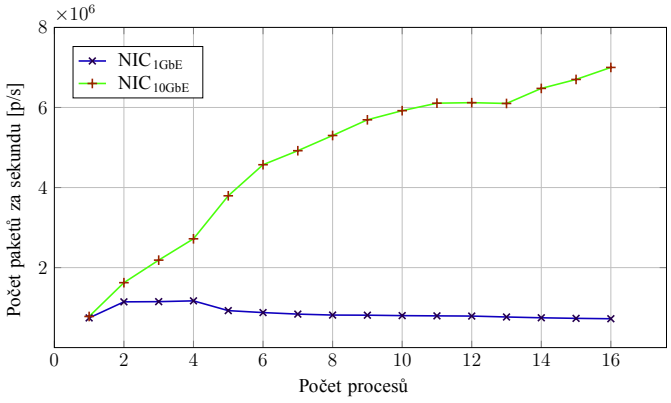
elektrorevue
ISSN 1213 - 1539

- Trafgen wrapper: modul vytvářející rozhraní k nástroji Trafgen.

Jelikož nástroj Trafgen vyžaduje na vstupu konfigurační soubory obsahující složení paketu pro daný útok, bylo v rámci vývoje nového nástroje DoSgen vytvořeno několik konfiguračních šablon pro jednotlivé útoky (tyto šablony jsou součástí modulu Trafgen wrapper), do kterých může uživatel vložit vybrané hodnoty (IP adresy, čísla portů a další). Nástroj DoSgen shromáždí veškeré vložené argumenty a spolu s konfiguračním souborem pošle na vstup nástroje Trafgen, tímto je útok spuštěn. Nástroj DoSgen byl vytvořen tak, aby mohla být knihovna LibDos rozšířena o další moduly nástrojů, které podporují generování jiných typů útoků, než které umožňuje nástroj Trafgen. Dále za účelem co největšího zjednodušení obsluhy, bylo vytvořeno ovládací grafické rozhraní ve formě webové aplikace. Ta je založena na softwarovém systému Node.js a vytvořená v programovacím jazyku JavaScript, HTML a CSS, dále byly využity technologie AJAX, framework Bootstrap a systém Masonry. Komunikace mezi webovou aplikací a uživatelem je zabezpečena protokolem HTTPS, pro přístup k aplikaci je nejprve vyžadována uživatelova autentizace pomocí přihlašovacího formuláře.

3.1 Testování nástroje DosGen

Funkce vytvořeného nástroje byla prověřena na testovacím serveru. Stejně jako Trafgen umožňuje nový nástroj DoSgen měnit vstupním parametrem počet použitých procesů proto, aby byl zjištěn maximální výkon nástroje, bylo nutné provést porovnání. Graf na obrázku 5 obsahuje naměřené hodnoty závislosti počtu paketů za sekundu na počtu procesů. Při použití síťového rozhraní NIC_{1GbE} je zřejmé, že mezi počtem procesů a počtu paketů za sekundu není přímá úměra. Lze ale vidět, že nejlepší výsledek je při počtu procesů 4, tato hodnota také odpovídá počtu jader procesoru testovacího serveru. Při použití NIC_{10GbE} platí přímá úměra a nejlepší výsledek byl dosažen při počtu procesů 16, tato hodnota odpovídá počtu logických jader procesoru.

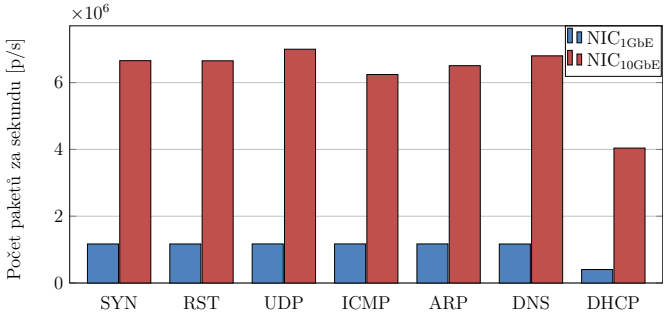


Obrázek 5: Závislost počtu paketů za sekundu na počtu procesů při útoku UDP flood.

Následně bylo provedeno testování výkonu nástroje pro jednotlivé útoky (SYN flood, RST flood, UDP flood, ICMP flood, ARP flood, DNS flood a DHCP starvation) v počtu přenesených paketů za sekundu. Pro srovnání jednotlivých útoků bylo použito nastavení, kdy byly útoky spuštěny pouze se čtyřmi procesy při měření s rozhraním NIC_{1GbE}. Pro rozhraní NIC_{10GbE} bylo provedeno měření s maximálním možným počtem procesů (tj. 16). Veškeré naměřené výsledky jsou uvedeny v tabulce 5 a v grafu na obrázku 6. Jak můžeme vidět z naměřených hodnot, tak malé rozdíly ve velikostech paketů mají minimální dopad na rychlost generování. Větší pokles rychlosti nastává až při útoku DHCP starvation, kdy je velikost jednotlivých paketů 286 B.

Tabulka 5: Porovnání jednotlivých útoků v počtu přenesených paketů za sekundu.

Útok	**Počet paketů za sekundu [p/s]**		**Velikost paketu [B]**
	NIC_{1GbE}	NIC_{10GbE}	
SYN flood	1 169 000	6 657 000	54
RST flood	1 169 000	6 653 000	54
UDP flood	1 172 000	7 000 000	42
ICMP flood	1 170 000	6 242 000	42
ARP flood	1 170 000	6 507 000	42
DNS flood	1 168 000	6 802 000	74
DHCP starvation	404 000	4 040 000	286



Obrázek 6: Porovnání útoků nástroje DoSgen v počtu přenesených paketů za sekundu.

4 Závěr

V první části článku byly popsány nástroje pro generování DoS útoků, a to konkrétně nástroje Hping3, Mause-

elektrorevue
ISSN 1213 - 1539

zahn a Trafgen. Tyto nástroje byly srovnány pomocí počtu generovaných paketů za sekundu (p/s) a také vytíženosti linky (MB/s). Měření byly provedeny pro síťové rozhraní NIC_{1GbE} a NIC_{10GbE}. Nejlepších výsledků dosáhl nástroj Trafgen. V další části byl popsán nově vytvořený nástroj DoSgen, který využívá jádro Trafgenu. Pro nově vytvořený nástroj byly také uvedeny výsledky testovacích měření, pomocí kterých se zkoumala závislost počtu procesů na přenesených paketů za sekundu. Při použití NIC_{1GbE} neplatila přímá úměra mezi p/s a počtem procesů, ale nejlepší výsledky byly dosaženy při počtu procesů rovnajícímu se počtu fyzických jader procesoru. Při použití NIC_{10GbE} přímá úměra platila a nejlepší výsledek byl dosažen při počtu procesů rovnajících se všech dostupných i logických jader procesoru. Dále bylo provedeno výkonnostní srovnání pro jednotlivé útoky v závislosti počtu paketů za sekundu, při výchozím nastavení velikostí paketů. Z uvedeného srovnání můžeme říci, že u jednotlivých útoků, kde se velikost paketů liší jen málo, nemá velikost paketu výrazný vliv na rychlost generování, pouze u útoku DHCP starvation, kdy je paket téměř pětkrát větší, došlo k razantnímu poklesu rychlosti generování.

Vytvořený nástroj DoSgen, je tedy možné využít pro bezpečnostní testování počítačových systémů a síťových infrastruktur, proti útokům SYN flood, RST flood, UDP flood, ICMP flood, ARP flood, DNS flood a DHCP starvation. Nástroj DoSgen je také možno s minimální úpravou rozšířit o další knihovny a tím rozšířit podporu dalších typů útoků.

Poděkování

Výzkum byl podpořen projektem GAČR 14-25298P "Research into cryptographic primitives for secure authentication and digital identity protection" a Národním programem udržitelnosti LO1401 a grantem VI20172019093 Ministerstva vnitra, Programem bezpečnostního výzkumu České republiky 2015-2020.

Literatura

[1] ABLIZ, M. *Internet Denial od Servie Attacks and Defence Mechanisms.* University of Pittsburg [online]. 2011, [cit. 2016-12-10]. 50s. Dostupné z: http://people.cs.pitt.edu/~mehmud/docs/abliz11-TR-11-178.pdf

[2] KENIG, R., MANOR, D., GADOT, Z., TRAUNER, D., Radware *DDoS Survival Handbook.* [online]. 2013, [cit. 2016-12-10]. 56 s. Dostupné z: https://security.radware.com/uploadedFiles/Resources_and_Content/DDoS_Handbook/DDoS_Handbook.pdf

[3] Radware *Global Application & Network Security Report 2015-2016.* [online]. [cit. 2016-12-10]. Dostupné z: https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=6442457234

[4] KHALIMONENKO, A., STROHSCHNEIDER, J., KUPREEV, O. *Kaspersky DDOS intelligence report for Q3 2016.* [online]. [cit. 2016-12-10]. Dostupné z: https://securelist.com/analysis/quarterly-malware-reports/76464/kaspersky-ddos-intelligence-report-for-q3-2016/

[5] *Spirent* [online]. [cit. 2016-12-10]. Dostupné z: http://www.spirent.com

[6] *Ixia* [online]. [cit. 2016-12-10]. Dostupné z: https://www.ixiacom.com/

[7] HALAŠKA, P. *Generátor kybernetických útoků.* Brno: Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. 2016. Diplomová práce.

[8] SANFILIPPO, S. *Hping* [online]. 2006 [cit. 2016-12-10]. Dostupné z: http://www.hping.org

[9] HAAS, H. *Mausezahn* [online]. 2010 [cit. 2016-12-10]. Dostupné z: http://www.perihel.at/sec/mz/

[10] *Netsniff-NG* [online] [cit. 2016-12-10]. Dostupné z: http://netsniff-ng.org/

[11] BORKMANN, D. *Trafgen - a fast, multithreaded network packet generator.* [online] [cit. 2016-12-10]. Dostupné z: http://manpages.ubuntu.com/manpages/zesty/man8/trafgen.8.html