VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2017 Jan Klimeš

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

KYBERNETICKÉ ÚTOKY V PROGRAMU JMETER
CYBER ATTACKS IN JMETER

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Jan Klimeš
AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Číka, Ph.D.
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Jan Klimeš ***ID:*** 174326
Ročník: 3 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Kybernetické útoky v programu JMeter

POKYNY PRO VYPRACOVÁNÍ:

V teoretické části práce prostudujte nástroj určený na zátěžové testování serverů JMeter. Zaměřte se zejména na jeho možné rozšíření pomocí modulů nebo externích knihoven. V praktické části bakalářské práce navrhněte a implementujte rozšíření nástroje Jmeter o síťové útoky (D)DoS za pomocí externí knihovny trafgen (nejméně 4 útoky), popřípadě modulů založených na knihovnách Jmeter. Proveďte testování a výkonnostní analýzu realizované implementace. Dosažené výsledky vhodně prezentujte.

DOPORUČENÁ LITERATURA:

[1] HALILI, Emily H. Apache JMeter: A practical beginner's guide to automated testing and performance measurement for your websites. Packt Publishing Ltd, 2008.

[2] ERINLE, Bayo. Performance Testing with JMeter 2.9. Packt Publishing Ltd, 2013.

Termín zadání: 1.2.2017 ***Termín odevzdání:*** 8.6.2017

Vedoucí práce: Ing. Petr Číka, Ph.D.
Konzultant:

doc. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Bakalářská práce se zabývá bezpečností sítí založených na protokolu TCP/IP. Hlavním cílem práce je vytvoření rozšiřujících modulů pro aplikaci JMeter, které přidávají funkce pro softwarové generování DoS útoků záplavového typu SYN flood, UDP flood, DNS Server attack a DNS Amplification s využitím aplikace Trafgen. Teoretická část práce popisuje kybernetické útoky obecně, související síťové protokoly a samotnou aplikaci JMeter. Praktická část práce obsahuje popis grafického rozhraní rozšiřujících modulů, jednotlivé třídy ze kterých se moduly skládají a výsledky testování.

KLÍČOVÁ SLOVA

kybernetický útok, DoS, JMeter, SYN flood, UDP flood, DNS Server attack, DNS Amplification, Trafgen

ABSTRACT

Bachelor thesis deals with the security of computer networks based on TCP/IP protocol stack. The main aim is to create extension modules for application JMeter that add features to the software generate DoS attacks, SYN flood, UDP flood, DNS Server attack and DNS Amplification using applications Trafgen. The theoretical part generally describes cyber attacks, associated with network protocols and application JMeter itself. The practical part contains a description of the graphical interface of the expansion modules, each class which the modules consist of and test results.

KEYWORDS

cyber attack, DoS, JMeter, SYN flood, UDP flood, DNS Server attack, DNS Amplification, Trafgen

KLIMEŠ, Jan *Kybernetické útoky v programu JMeter*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, Rok. 56 s. Vedoucí práce byl Ing. Petr Číka, PhD.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Kybernetické útoky v programu JMeter“ jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor(ka) uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil(a) autorská práva třetích osob, zejména jsem nezasáhl(a) nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom(a) následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora(-ky)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Petru Číkovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci. Také bych chtěl poděkovat mé rodině a dětem za podporu a trpělivost.

Brno ....

podpis autora(-ky)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM VÝPISŮ

ÚVOD

Kybernetické útoky jsou realitou současnosti. Spolu s rostoucími objemy přenášených dat a počty uživatelů internetových služeb, přichází na řadu otázka spolehlivosti a odolnosti těchto služeb proti kybernetickým útokům. Provozovatelé těchto služeb na jedné straně investují nemalé částky do vývoje nových služeb, ale na druhé straně jsou nuceni investovat i do testování odolnosti svých produktů proti kybernetickým útokům. V případě, kdy je kybernetický útok dostatečně masivní nebo sofistikovaný, může způsobit nedostupnost služby a následné propady příjmů, reputace nebo nefunkčnost dalších systémů, které jsou na dané službě závislé.

Pro testování internetových služeb existuje nespočet různých aplikací, které realizují vybraný typ kybernetického útoku. Pokud požadujeme provést více typů kybernetických útoků současně, je nejprve nutné nastavit parametry jednotlivých testovacích aplikací pro konkrétní typ útoku a potom je jednotlivě spouštět. Toto je sice funkční řešení, nevýhodou však je nejednotné rozhraní pro konfiguraci jednotlivých aplikací dle konkrétního typu kybernetického útoku.

Existují ale aplikace, které poskytují jednotné grafické rozhraní pro nastavení a spouštění více typů kybernetických útoků nebo penetračních testů. Jednou z nich je opensource aplikace JMeter [1], která je jedním z projektů organizace Apache.

Tato bakalářská práce se zabývá problematikou vývoje rozšiřujících modulů pro aplikaci JMeter, které přidávají možnost spouštět čtyři kybernetické útoky typu Denial of Service (DoS) přímo z grafického rozhraní JMeteru s využitím externí knihovny Trafgen, která slouží jako výkonný generátor paketů. Konkrétně se jedná o kybernetické útoky SYN Flood, UDP Flood, DNS Server attack a DNS Amplification. V závěru práce jsou shrnuté výsledky testování a výkonnostní analýza realizované implementace.

1 KYBERNETICKÉ ÚTOKY DOS

1.1 Definice

Cílem kybernetických útoků typu DoS je odepření přístupu ke službě pro legitimního uživatele z důvodu přetížení nebo vyčerpání zdrojů služby. Toho lze dosáhnout vysíláním co největšího počtu specifických požadavků na napadenou službu (např. webová stránka), až dojde k zahlcení síťového připojení nebo vyčerpání systémových zdrojů webového serveru natolik, že nebude možné se ke službě připojit.

1.2 Základní rozdělení DoS útoků

Organizace CERT Coordination Center rozděluje DoS na tři základní typy [2]:

- útoky spotřebující vzácné, omezené nebo neobnovitelné zdroje
- útoky poškozující nebo modifikující konfigurační informace
- útoky zaměřené na fyzické poškození síťového rozhraní nebo jeho záměnu

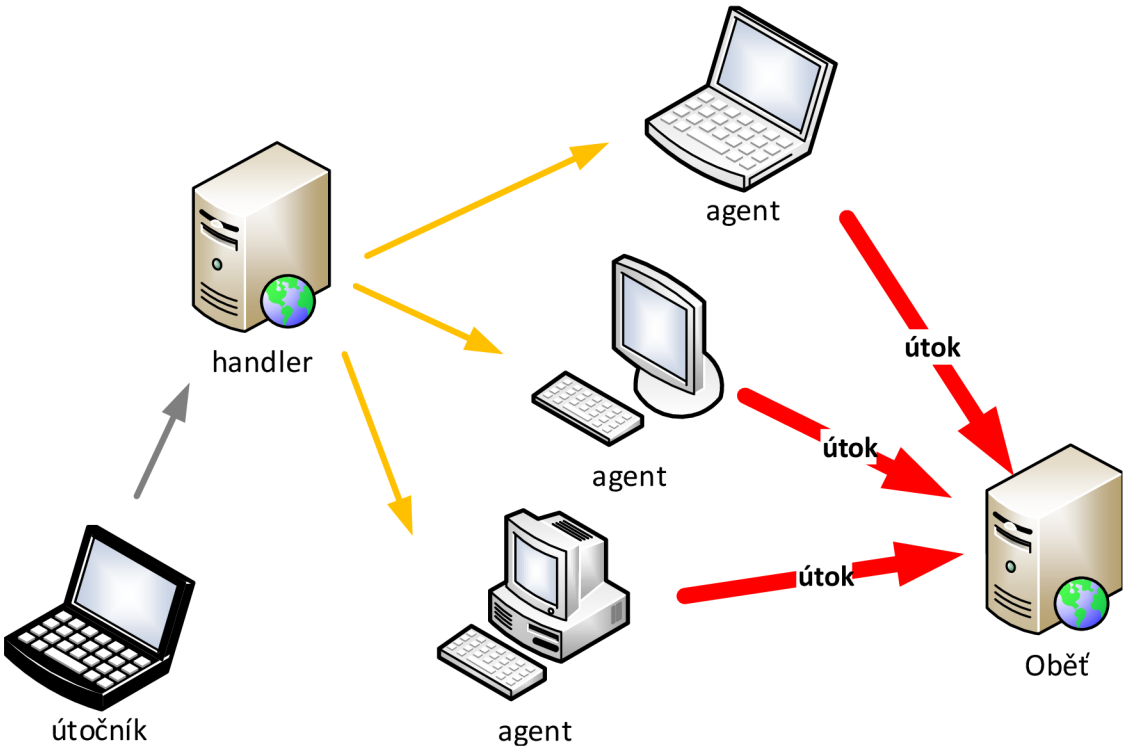
U zvolených útoků SYN flood, UDP flood, DNS Server attack a DNS Amplifiction se jedná o typy útoků spotřebovávající omezené zdroje oběti jako je kapacita síťového připojení, velikost paměti nebo procesorový čas serveru.

1.2.1 Dělení DoS útoků podle počtu útočících zařízení

Z pohledu počtu útočících zařízení se označení DoS používá v případě, kdy je útok veden z jednoho zařízení [3]. Zpravidla se jedná přímo o počítač útočníka.

Jelikož v současnosti disponují servery větší kapacitou síťového připojení, než mají k dispozici běžné počítače uživatelů připojené k internetu, je efektivnější zasílat požadavky paralelně z více počítačů s různou kapacitou připojení. Tento typ útoky se nazývá Distributed Denial of Service (DDoS) [3].

K provedení DDoS útoku využívá útočník dva základní prvky. Jedním prvkem jsou tzv. agenti, kterými jsou útočníkem ovládnuté počítače připojené k síti. Ovládnutí počítačů může způsobit spuštění souboru s virem nebo využití nezáplatované chyby v operačním systému nebo jiném softwaru. Tyto agenti jsou někdy v některé literatuře označováni také jako „bot“ nebo „zombie“ a jsou zdrojem vlny odesílaných škodlivých paketů. Skupina agentů (botů), která je pod kontrolou útočníka je označována jako botnet. Druhým nutným prvkem je další typ napadnutých počítačů, tzv. handlery, které ovládají agenty. Samotný útočník organizuje DDoS útok skrytě přes handlery a je tak lépe chráněn před odhalením. Celkový pohled na jednotlivé role při DDoS útoku ukazuje obrázek 1.1.



Obr. 1.1: Organizace DDoS útoku.

Počet agentů v botnetu může dosahovat i několik tisíc počítačů vysílající pakety z různých částí internetu. Proto je DDoS útok velmi účinný a je velmi složité ochránit servery před tímto typem útoku.

1.2.2 Dělení podle typu spotřebovávaných zdrojů

DoS útok může být zaměřen na vyčerpání určitého zdroje atakované oběti. Podle typu vyčerpaného zdroje dělíme na:

- síťové zdroje,
- serverové zdroje,
- aplikační zdroje.

Vyčerpání síťových zdrojů

Útoky cílené na síťové zdroje se pokouší zabrat co největší šířku pásma síťového připojení oběti pomocí velkého objemu vygenerovaných paketů. Legitimní pakety s požadavky uživatelů tak mohou být z důvodu zahlcení sítě zahazovány nebo odezva může být velmi dlouhá.

Vyčerpání serverových zdrojů

Tento typ útoku se snaží vyčerpat hardwarové zdroje serveru jako je CPU, RAM nebo diskové úložiště. Pokud je CPU vytížen na maximum nebo je alokovaná celá paměť RAM nebo dojde k zaplnění diskové kapacity, tak nejenom že nebude možné zpracovávat legitimní požadavky uživatelů, ale může dojít k pádu internetové služby nebo operačního systému serveru.

Vyčerpání aplikačních zdrojů

Tento typ DoS útoku zneužívá pro vyčerpání zdrojů oběti slabiny aplikačních protokolů Hypertext Transfer Protocol (HTTP), HTTP Secure (HTTPS), Domain Name System (DNS), Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP) a dalších [4].

1.2.3 Dělení podle frekvence vysílaných paketů

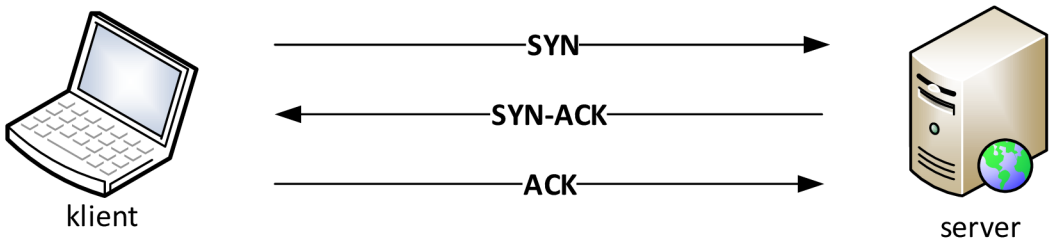
Při návrhu pluginu můžeme pracovat s intenzitou vysílaných paketů. Vysokou intenzitou vysílané pakety jsou označovány flood (záplavové) DoS útoky. Pro flood útoky jsou charakteristické parametry jako počet vysílaných paketů za sekundu (pps, packet per second) a šířka pásma (Mbps). Naopak nízkou intenzitou vysílané pakety jsou označovány pomalé DoS útoky. Pomalé útoky jsou využívány pro účely vyčerpání aplikačních zdrojů slabinami protokolů [4].

1.2.4 Dělení podle typu spojení

DoS útoky rozdělujeme podle typu spojení na spojové (connection-oriented) a nespojové (connectionless). Při spojovém typu útoku využíváme například vlastností Transmission Control Protocol (TCP). Při nespojovém typu útoku využíváme například protokol User Datagram Protocol (UDP) [4].

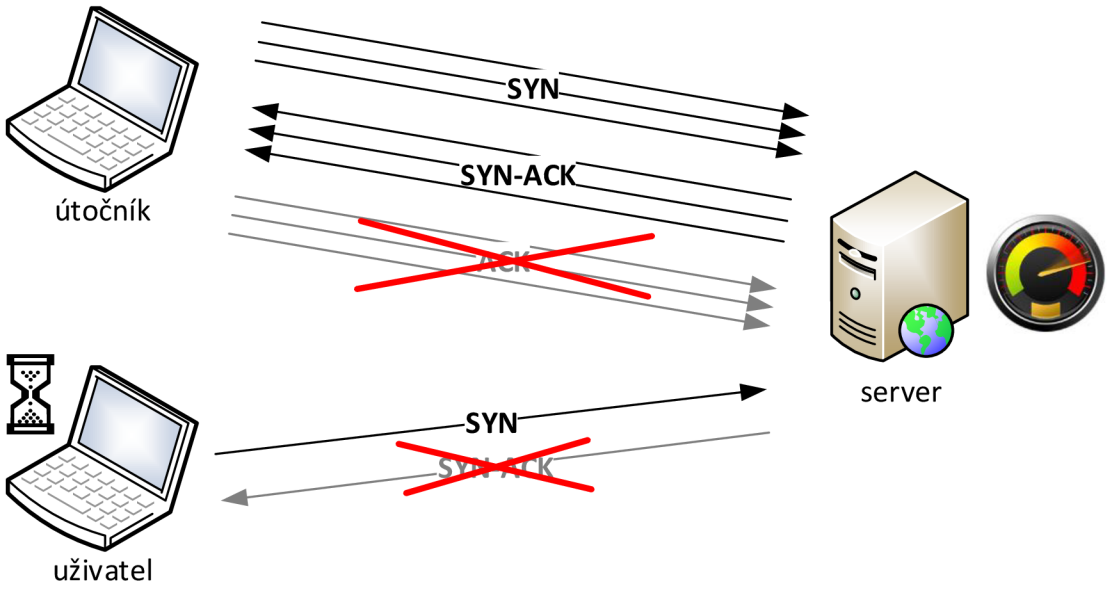
1.3 DoS útok TCP Syn flood

Útok obecně označovaný jako TCP Syn flood [4], zneužívá principu tříkrokového navazování spojení u spojového protokolu TCP. Pro otevření spojení je nutné nejprve odeslat serveru paket typu SYN, vyčkat na potvrzovací odpověď serveru v paketu SYN-ACK a poté teprve klient odešle paket typu ACK čímž otevře spojení pro přenos informace, jak ukazuje obrázek 1.2



Obr. 1.2: Třícestné navázání spojení u protokolu TCP.

Pokud ale využijeme tuto vlastnost TCP protokolu a jako klient zabráníme odesláním paketu ACK serveru, server bude po nějakou dobu čekat na přijetí paketu ACK od klienta pro otevření komunikace a ukládat si informaci o stavu do paměti. Pokud zašleme dostatečný počet SYN paketů bez ACK odpovědi, dojde k vyčerpání zdrojů serveru a odepření legitimního požadavku SYN jiného uživatele viz obrázek 1.3



Obr. 1.3: Popis komunikace při SYN flood.

Pokud navíc v paketu SYN zfalšujeme IP adresu odesílatele, server služby odešle potvrzovací paket SYN ACK na tuto zfalšovanou IP adresu, která ale zahajovací požadavek typu SYN neodeslala a potvrzovací paket SYN ACK zahodí.

1.3.1 TCP protokol

Jedná se o spojový protokol transportní vrstvy. Minimální délka hlavičky TCP protokolu je 160 bitů. Za hlavičkou následují bity přenášených informací. Rozložení jednotlivých parametrů v hlavičce je znázorněno na obrázku 1.4. Popis jednotlivých parametrů hlavičky viz tabulka 1.1 [5].

Pro generování paketů útoku SYN flood jsou důležité zejména parametry čísla odchozího a příchozího portu a parametr SYN. Datagram TCP protokolu je vložen do paketu síťového protokolu Internet protocol version 4 (IPv4), viz kapitola 1.3.2.

<table>
<tr><td colspan="8">16-bit source port number</td><td colspan="8">16-bit destination port number</td></tr>
<tr><td colspan="16">32-bit sequence number</td></tr>
<tr><td colspan="16">32-bit acknowledgement number</td></tr>
<tr><td colspan="4">4-bit lenght header</td><td colspan="2">reserved (6 bits)</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="8">16-bit window size</td></tr>
<tr><td colspan="8">16-bit checksum</td><td colspan="8">16-bit urgent pointer</td></tr>
<tr><td colspan="16">Options (if any)</td></tr>
</table>

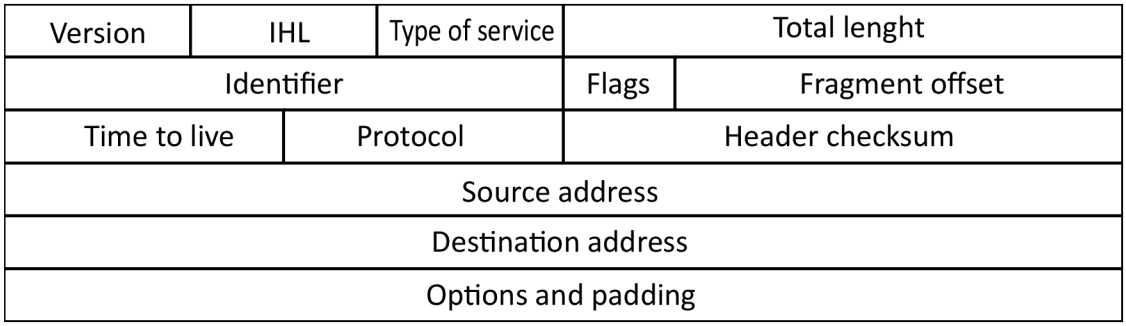
Obr. 1.4: Hlavička paketu TCP datagramu

Tab. 1.1: Parametry hlavičky TCP datagramu

Parametr	bitů	Popis
Source port	16	číslo odchozího portu
Destination port	16	číslo cílového portu
Sequence number	32	číslo sekvence
Acknowledgement	32	potvrzený byte
4 bit lenght header	4	délka hlavičky
reserved	6	rezervováno pro budoucí použití
URG	1	urgentní data
ACK	1	potvrzení
PSH	1	indikuje okamžité předání dat do aplikace
RST	1	indikuje okamžité přerušení spojení
SYN	1	indikuje žádost o otevření nového spojení
FIN	1	indikuje ukončení přenášení dat
Window size	16	množství dat v paketu kvůli plynulosti přenosu
Checksum	16	validace dat v paketu
Urgent pointer	16	ukazatel sekvence posledního paketu s URG daty
Options	0 - 320	dodatečné vlastnosti paketu a zarovnání hlavičky

1.3.2 IPv4 protokol

IPv4 je protokol třetí síťové přenosové vrstvy OSI modelu. Paket se skládá z provozní hlavičky a samotných přenášených dat. Délka hlavičky je vždy 160 bitů. Rozložení jednotlivých parametrů v hlavičce ukazuje obrázek 1.5. Popis jednotlivých parametrů hlavičky viz tabulka 1.2 [5]. Pro účely generování paketů útoků SYN flood a UDP flood jsou důležité zejména parametry IP adresy odesílatele a příjemce paketu.



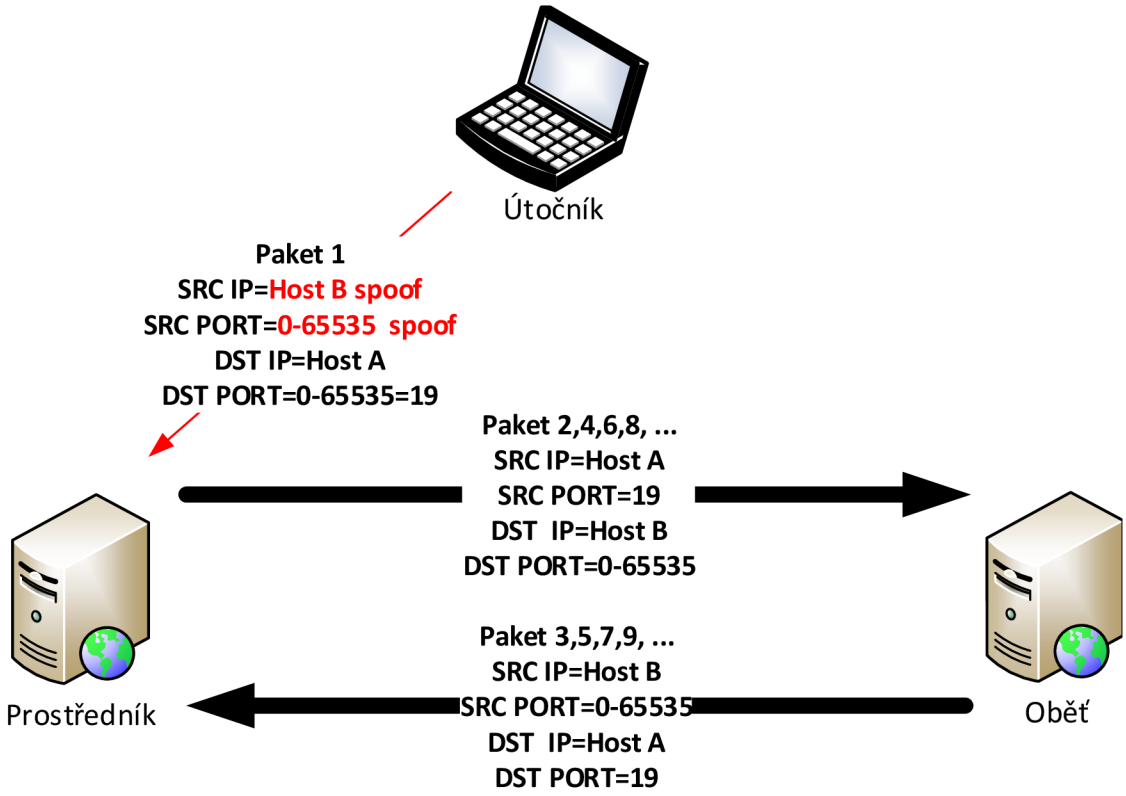
Obr. 1.5: Hlavička TCP/IP protokolu

Tab. 1.2: Parametry hlavičky TCP/IP paketu

Parametr	bitů	Popis
Version	4	Typ paketu, IPv4 nebo IPv6
IHL	4	Internet Header Length, délka hlavičky paketu v jednotkách po 4 bytech (5 je 20 bytes)
Type of service	8	priorita paketu při přenosu
Total lenght	16	délka paketu v bytech
Identifier	16	hodnota identifikátoru pro rekonstrukci paketu z několika fragmentů
Flags	3	parametr fragmentace paketu
Fragment offset	13	Označení pozice fragmentu v rámci paketu
Time to live	8	maximální počet předání paketů mezi přepojovacími uzly, než bude paket zahozen
Protocol	8	protokol (TCP, UDP, ICMP, atd.)
Header cheksum	16	kontrolní součet hlavičky pro detekci chyb při přenosu
Source address	32	IP adresa odesílatele paketu
Destination address	32	IP adresa příjemce paketu
Options and padding	32	dodatečné vlastnosti paketu a zarovnání hlavičky

1.4 DoS útok UDP flood

Kybernetický útok UDP flood využívá vlastnosti UDP protokolu, u kterého je spojení nestavové, kde se v přenášených datagramech nepřenáší informace o spojení. Útočník generuje pakety s podvrženou IP adresou odesílatele na různé cílové porty prostředníka. Prostředník ale odesílá pakety s reakcí na podvrženou adresu oběti. Oběť v ideálním případě reaguje také odesláním paketu na prostředníka. Pokud se útočníkovi podaří najít co nejvíce kombinací otevřených a komunikujících portů mezi prostředníkem a obětí naroste prudce množství přenášených paketů viz obrázek 1.6. Důsledkem může být přetížení síťového připojení oběti a odepření požadavků pro legitimní dotazy.



Obr. 1.6: Popis komunikace při útoku UDP flood.

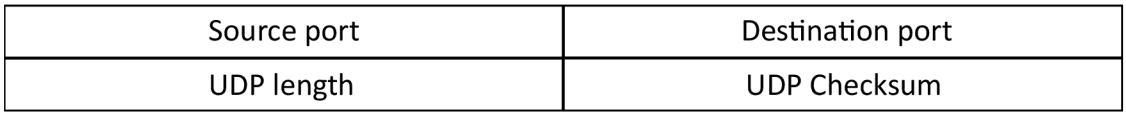
1.4.1 UDP protokol

Jedná se o nespojovaný typ protokolu, který neudržuje informace o aktuálním spojení. Data přenášená tímto protokolem nemají žádnou záruku doručení a proto je tento protokol využíván hlavně pro přenos multimediálních dat a streamů.

Pro návrh a vývoj pluginu, který generuje pakety DoS útoku UDP flood je nutné znát účel jednotlivých parametrů hlavičky UDP protokolu. Délka hlavičky je 64 bitů.

Rozložení jednotlivých parametrů v hlavičce ukazuje obrázek 1.7. Popis jednotlivých parametrů hlavičky viz tabulka 1.3 [5]. Pro účely generování paketů útoků UDP flood jsou důležité zejména parametry zdrojového a cílového portu.

Paket UDP protokolu je vložen do paketu protokolu Transmission Control Protocol/Internet protocol (TCP/IP), který je popsán v kapitole 1.3.2.



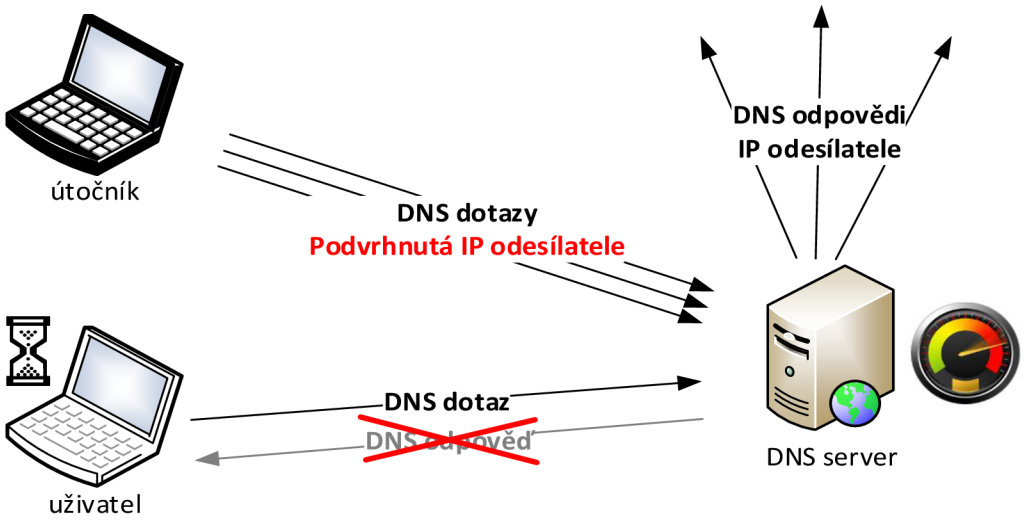
Obr. 1.7: Hlavička UDP protokolu.

Tab. 1.3: Parametry hlavičky UDP datagramu.

Parametr	bitů	Popis
Source port	16	číslo odchozího portu
Destination port	16	číslo cílového portu
UDP lenght	16	délka UDP segmentu
UDP checksum	16	kontrolní součet

1.5 DoS útok na DNS Server

Jedná se o útok, kdy útočník odesílá velký objem dotazů na DNS server [4]. DNS server následně odesílá velké množství odpovědí na podvržené IP adresy což vede k vyčerpávání síťových a serverových zdrojů. Odpovědi na legitimní dotazy uživatelů jsou z důvodu přetížení DNS serveru odesílány se zpožděním nebo vůbec. Aby útočník ztížil detekci IP adresy zdroje, podvrhne útočník zdrojovou IP adresu v odesílaných UDP datagramech. Popis komunikace na obrázku 1.8



Obr. 1.8: Komunikace při útoku na DNS server.

1.5.1 DNS protokol

Jedná se o aplikační protokol, který slouží k překladu doménových jmen na IP adresy [6]. Pro přenos informací se používá transportní protokol UDP nebo TCP. Pro běžné dotazy klientů je z důvodu rychlosti odezvy využíván transportní protokol UDP. Transportní protokol TCP je primárně využíván pro přenos zón mezi DNS servery, ale i pro běžné dotazy klientů. Oba transportní protokoly používají port 53.

Rozložení jednotlivých parametrů v hlavičce ukazuje obrázek 1.9. Popis jednotlivých parametrů hlavičky viz tabulka 1.4 [6].

<table>
<tr><td colspan="8">Transaction ID (16 bits)</td></tr>
<tr><td>Q
R</td><td>OpCode
(4 bits)</td><td>A
A</td><td>T
C</td><td>R
D</td><td>R
A</td><td>Z
(3 bits)</td><td>RCode
(4 bits)</td></tr>
<tr><td colspan="8">QDCOUNT</td></tr>
<tr><td colspan="8">ANCOUNT</td></tr>
<tr><td colspan="8">NSCOUNT</td></tr>
<tr><td colspan="8">ARCOUNT</td></tr>
<tr><td colspan="8">Sections: Question, Answer, Authority, Additional Information
(variable lenght)</td></tr>
</table>

Obr. 1.9: Hlavička paketu DNS protokolu.

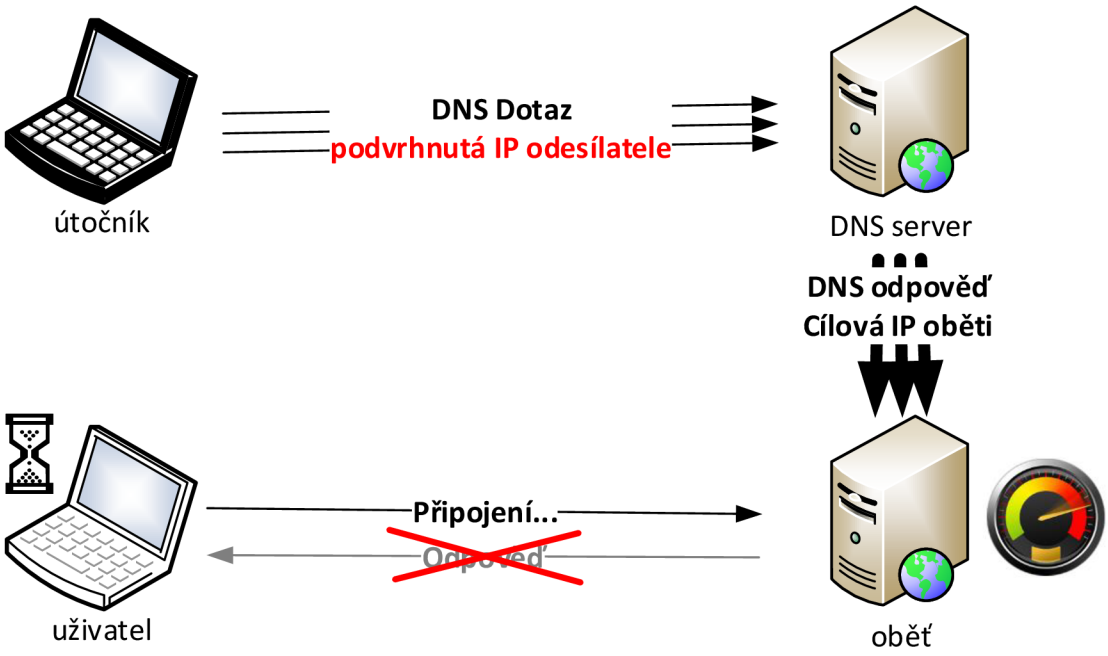
Pro účely návrhu a vývoje pluginu pro generování paketů útoků DNS Server attack a DNS Amplification jsou důležité zejména parametry Transaction ID, QR, OpCode, QDCOUNT a Section s dotazem na překlad konkrétní adresy.

Tab. 1.4: Parametry hlavičky DNS protokolu.

Parametr	bitů	Popis
Transaction ID	16	generuje klient, server kopíruje do odpovědi, toto párování umožňuje odesílat více dotazů současně
QR	1	0 pokud je zpráva dotazem, 1 pokud je zpráva odpovědí
OpCode	4	Typ otázky, stejný v dotazu i odpovědi: 0 - standardní otázka QUERY, 1 - inverzní otázka IQUERY, 2 - otázka na status STATUS, 4 - notify otázka NOTIFY, 5 - update otázka UPDATE
AA	1	0 - odpověď není autoritativní, 1 - odpověď je autoritativní
TC	1	1 - odpověď byla zkrácena na 512 bajtů. Pokud má klient zájem o celou odpověď, pak musí dotaz zopakovat protokolem TCP
RD	1	1 - pokud klient požaduje rekurzivní překlad, důležité pro dotaz
RA	1	1 - pokud server umožňuje rekurzivní překlad, důležité pro odpověď
Z	3	rezervováno pro budoucí použití
RCode	4	Výsledkový kód odpovědi: 0 - bez chyby (NoError), 1 - chyba ve formátu dotazu, server jej neumí interpretovat (FormErr), 2 - server neumí odpovědět (ServFail), 3 - jméno z dotazu neexistuje (negativní odpověď), tuto odpověď mohou vydat pouze autoritativní name servery (NXDomain), 4 - server nepodporuje tento typ dotazu (Notlmp), 5 - Server odmítá odpovědět, např. z bezpečnostních důvodů (Refused)
QDCOUNT	16	číslo určující z kolika vět se skládá dotaz
ANCOUNT	16	číslo určující z kolika vět se skládá odpověď
NSCOUNT	16	číslo určující z kolika vět se skládá sekce obsahující odkazy na autoritativní name servery
ARCOUNT	16	číslo určující z kolika vět se skládá sekce doplňující informace
Sections	var	Sekce konkrétního dotazu, odpovědi, autoritativní name servery, doplňující informace

1.6 DoS útok DNS Amplification

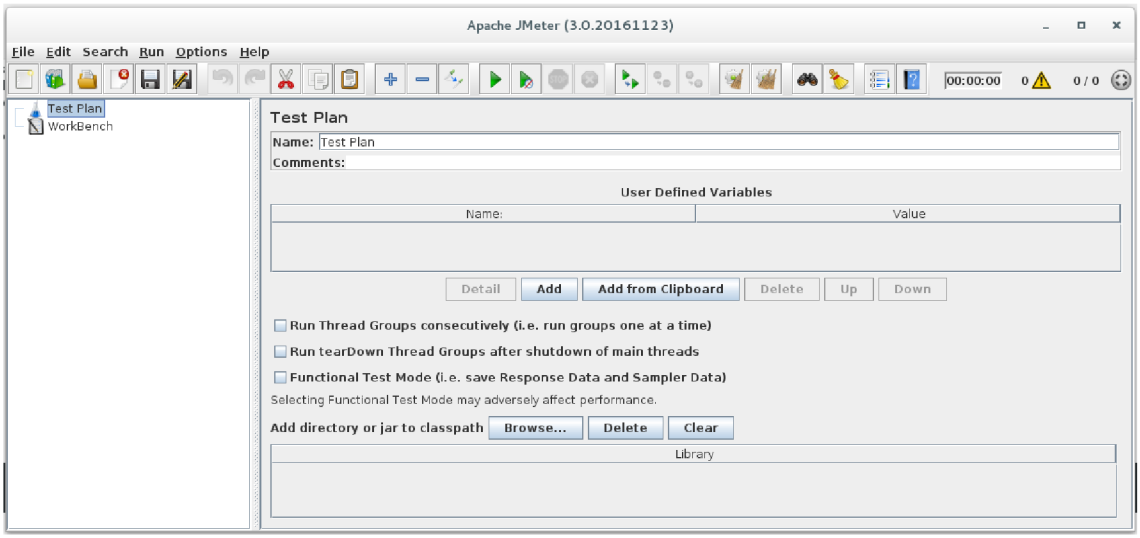
Útok DNS Amplification (zesilující), využívá DNS server jako prostředníka [4]. Útočník odesílá dotazy na DNS server, který má zpravidla větší kapacitu síťového připojení než útočník. V těchto paketech je podvrhnutá IP adresa odesílatele na IP adresu oběti. Dotazy jsou vybrány tak, aby datová velikost odpovědi, které jsou odesílány z DNS serveru na IP adresu oběti, byla větší než samotný dotaz na DNS server. Tento datový tok má za cíl vyčerpávání síťových a serverových zdrojů oběti. Legitimní uživatel, který se chce připojit k takto napadnutému serveru dostává odpovědi se zpožděním nebo vůbec, viz obrázek 1.10.



Obr. 1.10: Komunikace při útoku na DNS Amplification.

2 JMETER

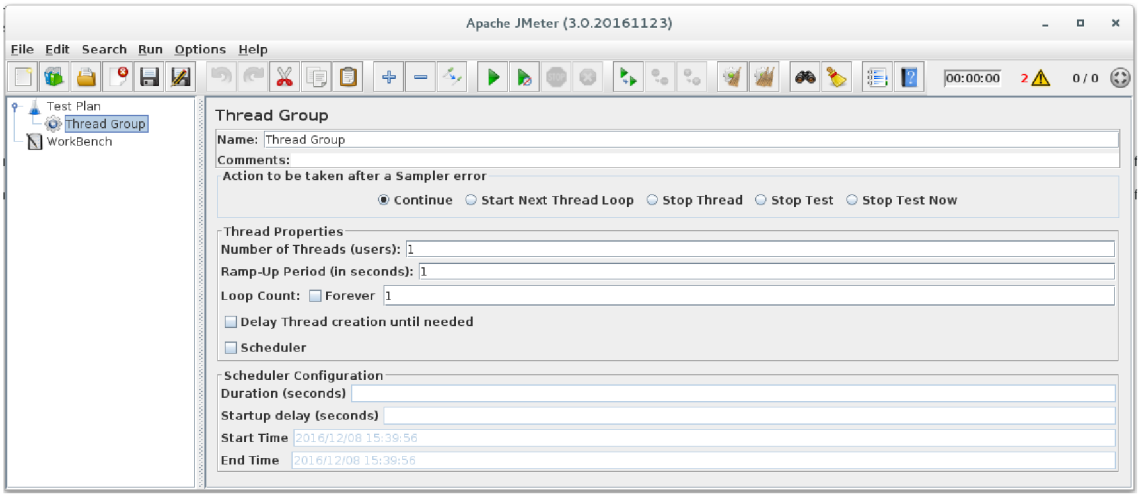
Jmeter [1] je open source aplikace vyvíjená od konce 90. let pro účely automatizovaného testování aplikačních a síťových protokolů. A to nejen po stránce výkonu a zátěže, ale i po stránce funkčnosti výstupních dat síťové aplikace na základě definovaných vstupních proměnných. Typickým objektem testování je webový server, který je připojen do sítě IP protokolem a na kterém běží internetová aplikace komunikující aplikačním protokolem HTTP. Jmeter je rozšiřitelný pomocí pluginů, které rozšiřují možnosti testování síťových protokolů TCP a UDP nebo aplikačních protokolů jako například, HTTP, FTP a dalších.



Obr. 2.1: Úvodní obrazovka aplikace JMeter.

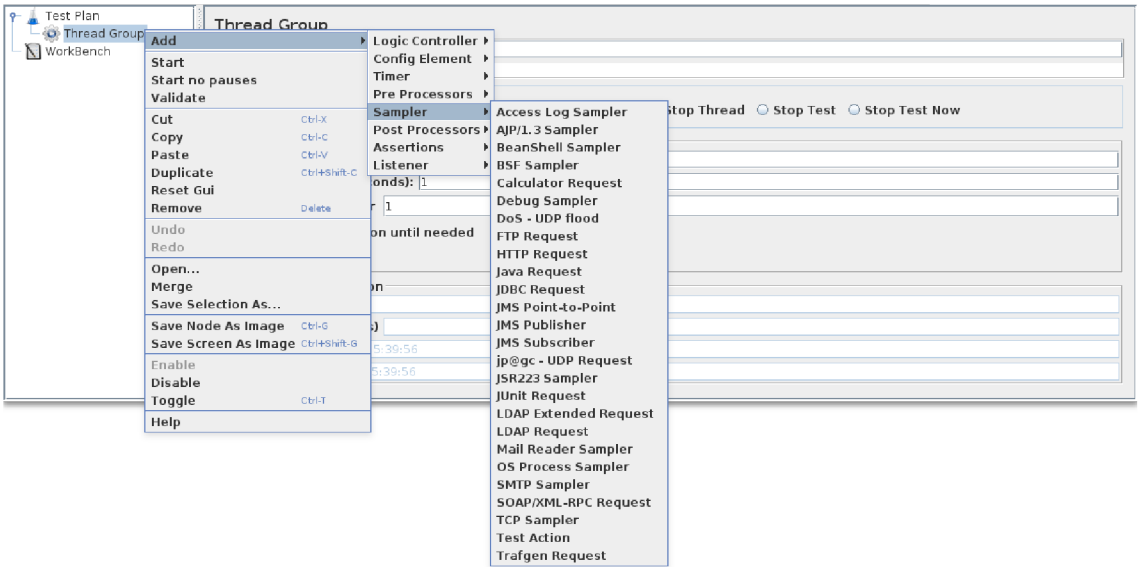
2.1 Testovací plán a základní elementy

Testovací plán [7] definuje jakým způsobem testovat konkrétní parametry daného protokolu. Protože jsou testovány protokoly typu klient server, musí každý testovací plán obsahovat základní element Thread Group, kde je nutné nastavit počet vláken (klientů) odesílající dotazy serveru viz obrázek 2.2.



Obr. 2.2: Možnosti konfigurace elementu Thread Group.

Důležitým elementem je Sampler (vzorek, mustr) klientem odesílaných požadavků na server definovaný parametry vybraného komunikačního protokolu. Dostupné Samplery některých protokolů, viz obrázek 2.3.



Obr. 2.3: Přidání Sampleru do testovacího plánu.

Dalšími elementy testovacího plánu, které je možné přidat pro Thread Group viz tabulka 2.1

Tab. 2.1: Přehled dostupných elementů pro Thread Group.

Název elementu	Popis
Logic Controller	logický kontrolér, nastavení pořadí zpracovávání použitých Samplerů
Config Element	konfigurační element, definování proměnných a jejich výchozích hodnot pro další použití v Samplerech
Timer	časování, konfigurace časových mezer mezi dvěma požadavky klienta
Pre Processors	předzpracování, konfigurace změn nastavení dalšího dotazu Sampleru na základě předchozí odpovědi serveru
Post Processors	po zpracování, modifikace přijatých dat od serveru vyžádaných Samplerem
Assertions	tvrzení, nastavení validace pro funkční testování přijatých odpovědí na základě odeslaných dotazů Sampleru
Listeners	naslouchače, nastavení logování a zobrazení grafů, tabulek a statistik výsledků Samplerů

2.2 Rozšíření JMeteru přídavným modulem

JMeter je vyvíjen na principu přídavných modulů, které využívají základní třídy jádra JMeteru. Elementy popsané v předchozí kapitole jsou jednotlivě vyvinuté moduly v jazyce JAVA. Zkompilované soubory JAR jsou uloženy ve složce JMeteru. Po spuštění JMeteru si jádro naimportuje moduly na základě nakopírovaných JAR souborů. Vývoj softwaru metodou rozšiřujících modulů umožňuje efektivnější vývoj nových funkcí.

2.2.1 Trafgen

Knihovna Trafgen [8] je velmi výkonný generátor síťových paketů. Patří do balíčku síťových aplikací Netsniff-NG. Z výkonnostních důvodů je knihovna vyvíjena v low-level jazyce, v asembleru.

Pro nastavení parametrů paketů využívá knihovna Trafgen vstupní konfigurační soubor s vlastní syntaxí. Ten je definován hlavičkovými funkcemi jednotlivých protokolů, viz tabulka 2.2

Tab. 2.2: Hlavičkové funkce konfiguračního souboru Trafgen.

Hlavičková funkce	Popis
eth()	linková vrstva
pause()	ovládání toku dat na linkové vrstvě
pfc()	ovládání toku dat podle priority
vlan()	VLAN protokol
mpls()	multiprotokolové přepojováí podle návěstí
arp()	ARP protokol
ipv4()	IPv4 hlavička
ipv6()	IPv6 hlavička
icmp4()	ICMP verze 4 protokol
icmp6()	ICMP verze 6 protokol
udp()	UDP hlavička
tcp()	tcp hlavička

Konfigurační soubor je při spuštění Trafgenu kompilován C preprocesorem. Příklad typického konfiguračního souboru je uveden v následujícím výpisu 2.1.

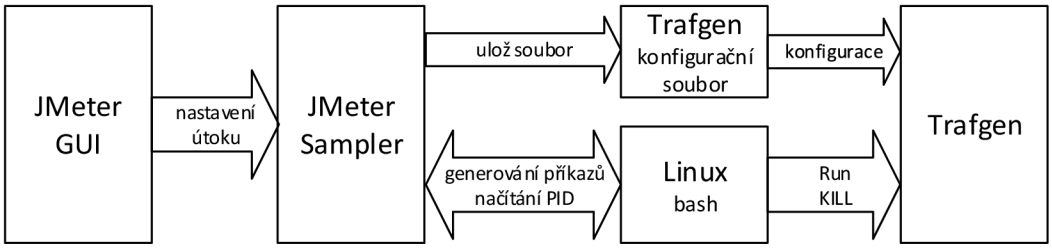
Výpis 2.1: Příklad konfiguračního souboru Trafgen.

```
#define ETH_P_IP  0x0800
{
  eth(daddr=00:0c:29:68:18:22,
      saddr=00:0c:29:b1:21:65,
      proto=ETH_P_IP),

  ipv4(ttl=64, ver=4, len=59, flags=0b01000000, frag=0, df,
       da=192.168.0.254, sa=192.168.0.1),

  tcp(sport=1025, dport=80,
      seq=drnd(), aseq=0, hlen=40, syn, win=16),

  fill('B',12),
}
```

2.2.2 Propojení JMeteru s externí knihovnou Trafgen

Komunikace mezi javovou aplikací JMeter běžící pod JVM a konzolovou aplikací Trafgen naprogramovanou v asembleru je realizována pomocí konzolových příkazů Linuxu.

Uživatel v grafickém rozhraní JMeteru nastaví parametry útoku a spustí testovací plán. Parametry jsou zpracovány rozšiřujícím modulem, Samplerem JMeteru, který vygeneruje a uloží konfigurační soubor pro Trafgen. Modul následně pomocí konzolových příkazů spustí na pozadí Trafgen s požadovanými parametry a odkazem na konfigurační soubor paketu. Ukončení běžícího Trafgenu je realizováno načtením PID Trafgenu a ukončením tohoto procesu v Linuxu příkazem KILL. Schéma propojení viz obrázek 2.4.



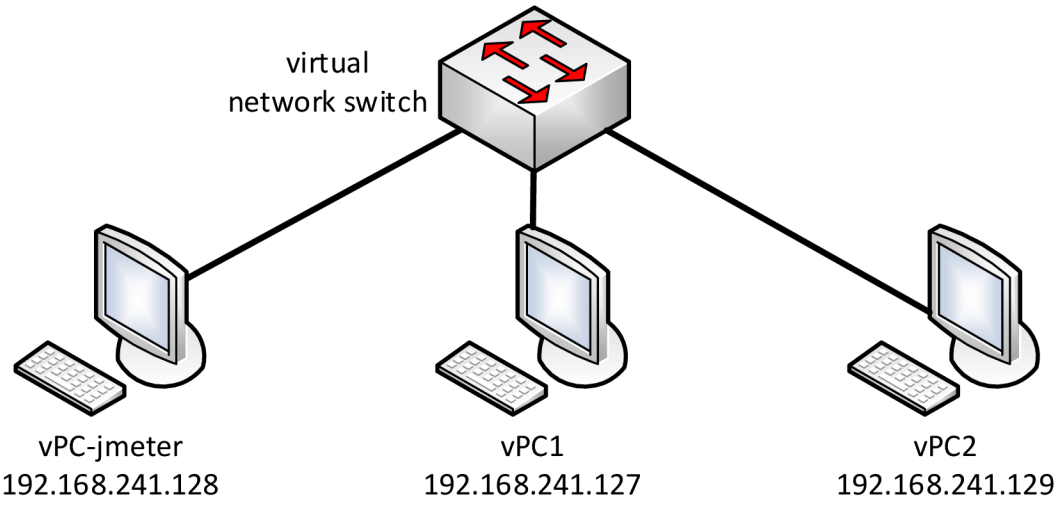
Obr. 2.4: Schéma propojení JMeteru a Trafgen.

3 VÝVOJ MODULŮ KYBERETICKÝCH ÚTOKŮ

3.1 Konfigurace prostředí pro vývoj a testování

Vývoj a testování modulů kybernetických útoků je realizován na počítači s procesorem Intel Core i5-5200 2,2 GHz se 16 GB RAM a SSD diskem 240 GB. Operační systém je Windows 10 Pro x64.

Na počítači je nainstalován VMware Workstation 11, kde jsou vytvořeny tři virtuální počítače (vPC-jmeter, vPC1 a vPC2) a jedna virtuální síť, kterou jsou virtuální počítače propojeny, viz obrázek 3.1.



Obr. 3.1: Topologie sítě testovacího prostředí.

Na virtuálním počítači vPC-jemeter je nainstalován operační systém CentOS 7 x64, vývojové prostředí Eclipse Neon.1 se zdrojovým kódem aplikace JMeter 3.0 a zdrojovými kódy jednotlivých modulů.

Virtuální počítače vPC1 a vPC2 slouží pro testování funkčnosti jednotlivých modulů. Na obou je nainstalován operační systém CentOS 7 x64, DNS Server BIND a Wireshark.

Konfigurace zdrojového kódu JMeter 3.0 v Eclipse

Pro konfiguraci zdrojových kódů v Eclipse je nutné ze stránek jmeter.apache.org stáhnout soubor s archivem zdrojových kódů a rozbalit je do pracovní složky Eclipse příkazem viz výpis 3.1.

Výpis 3.1: Rozbalení zdrojových kódů JMeteru.

```
tar -zxvf apache-jmeter-3.0_src.tgz -C ~/workspace/
```

Následně je třeba vytvořit v Eclipse nový projekt který je nutné pojmenovat stejně jako je jméno složky v pracovním adresáři workspace.

Potom je nutné zkompilovat zdrojový kód. V Eclipse zobrazíme okno Ant (Window > Show View > Ant). Zde je nutné přidat kompilační soubor Build.xml, který se nachází v hlavní složce projektu. V nově zobrazeném menu kompilátoru Ant spustíme příkaz **download_jars**, která stáhne další potřebné soubory. Potom spustíme příkaz **install default**. Nyní lze spustit JMeter z Eclipse spuštěním příkazu **run_gui** z okna Ant.

Instalace knihovny Trafgen

Knihovna Trafgen je součástí instalačního balíčku Netsniff-NG. Automatické stažení z repozitáře a následnou instalaci provede příkaz viz výpis 3.2.

Výpis 3.2: Instalace utility Trafgen.

```
yum install netsniff-ng
```

Spouštění aplikace JMeter

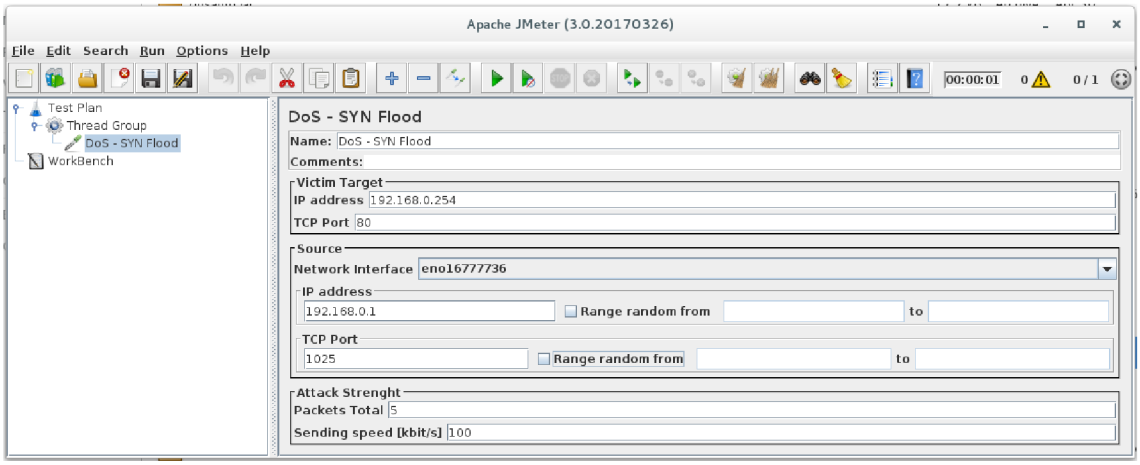
Aplikaci JMeter je doporučené spouštět pod uživatelským účtem s právy root, viz výpis 3.3 Pokud nebude JMeter spuštěn s právy root, bude nutné při každém spuštění testovacího plánu zadat heslo uživatele root.

Výpis 3.3: Spuštění JMeteru s právy uživatele root.

```
sudo -s ~/workspace/apache-jmeter-3.0/bin/jmeter
```

3.2 Modul DoS - SYN Flood

Grafické rozhraní modulu SYN Flood, viz obrázek 3.2, je rozděleno do tří základních částí, kde jsou umístěny prvky rozhraní pro nastavení parametrů cíle útoku, zdroje útoku a síly útoku. Popis a účel jednotlivých prvků rozhraní je popsáno v tabulce 3.1.



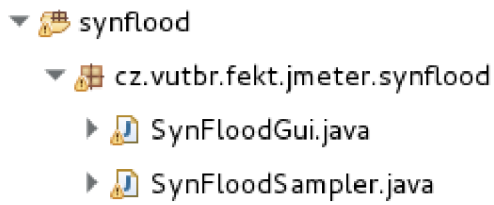
Obr. 3.2: Grafické rozhraní modulu SYN Flood.

Tab. 3.1: Popis grafického rozhraní modulu SYN Flood.

Název prvku	Popis
Victim Target	parametry pro nastavení cíle útoku
IP address	IP adresa cíle útoku
TCP Port	číslo TCP portu cíle útoku
Source	parametry pro nastavení zdroje útoku
Network Interface	síťové rozhraní, ze kterého budou odesílány pakety
IP address	IP adresa, která bude nastavena u odesílaných paketů jako odchozí. Po zaklikutí Range random je možné zadat rozsah IP adres, ze kterých bude náhodně vybrána odchozí IP adresa
TCP Port	číslo TCP portu, který bude nastaven u odesílaných paketů jako odchozí. Po zaklinutí Range random je možné zadat rozsah TCP portů, ze kterých bude náhodně vybrán odchozí TCP port
Attack Strenght	parametry pro nastavení síly útoku
Packets Total	Celkový počet vygenerovaných paketů. Pokud je zadána 0, jsou pakety generovány tak dlouho, dokud uživatel neukončí test JMeteru
Sending speed	Rychlost odesílání paketů v kbit/s

Popis zdrojových kódů balíčku DoS - SYN Flood

Balíček modulu SYN Flood se skládá ze tříd SynFloodGui a SynFloodSampler, viz obrázek 3.3.



Obr. 3.3: Třídy modulu SYN Flood.

Třída SynFloodGui

Tato třída obsahuje objekty grafického rozhraní modulu SYN Flood. Importovány jsou třídy grafického rozhraní javax.swing JLabel, JTextField, JCheckBox a JComboBox. Navíc tato třída dědí z rodičovské třídy AbstractSamplerGui metody testovacího elementu, které jsou důležité pro spolupráci s jádrem JMeteru, viz výpis 3.4

Výpis 3.4: Zkrácený výpis zdrojového kódu souboru SynFloodGui.java

```
public class SynFloodGui extends AbstractSamplerGui {

   public TestElement createTestElement() {
      SynFloodSampler sampler = new SynFloodSampler();
      modifyTestElement(sampler);
      final ScheduledExecutorService
        service = Executors.newSingleThreadScheduledExecutor();
        service.schedule(new Runnable() {
           @Override
            public void run() {
               configure(sampler);
            }
         }, 10000, TimeUnit.MILLISECONDS);
    return sampler;
    }
   public void modifyTestElement(TestElement te) {}

   public void configure(TestElement element) {}
}
```

Třída SynFloodSampler

Tato třída obsahuje metody pro ovládání externí knihovny Trafgen pomocí bash příkazů spouštěných na pozadí, dle proměnných nastavených v grafickém prostředí JMeteru.

Při spuštění testu je vytvořen vstupní konfigurační soubor pro aplikaci Trafgen s konfigurací paketu, viz výpis 3.5

Výpis 3.5: Konfigurační soubor synflood.cfg

```
#define ETH_P_IP  0x0800
{
  eth(daddr=00:0c:29:68:18:22,
      saddr=00:0c:29:b1:21:65,
      proto=ETH_P_IP),

  ipv4(ttl=64, ver=4, len=59, flags=0b01000000, frag=0, df,
       da=192.168.0.254, sa=192.168.0.1),

  tcp(sport=1025, dport=80,
      seq=drnd(), aseq=0, hlen=40, syn, win=16),

  fill('B',12),
}
```

Následně je na pozadí spuštěna aplikace Trafgen pomocí bash konzole příkazem pkexec s definovanými parametry a odkazem na vytvořený konfigurační soubor paketu, viz výpis 3.6.

Výpis 3.6: Bash příkaz pro spuštění Trafgen s parametry.

```
pkexec /home/tester/netsniff-ng/trafgen/trafgen
--in synflood.cfg --out eth0 --cpp --num 5 --rate 100kbits
```

Ukončení Trafgen s grafického rozhraní JMeteru je realizováno metodou killTrafgen viz výpis 3.7, která vygeneruje příkaz do bash konzole pro ukončení běžících procesů Trafgen dle PID.

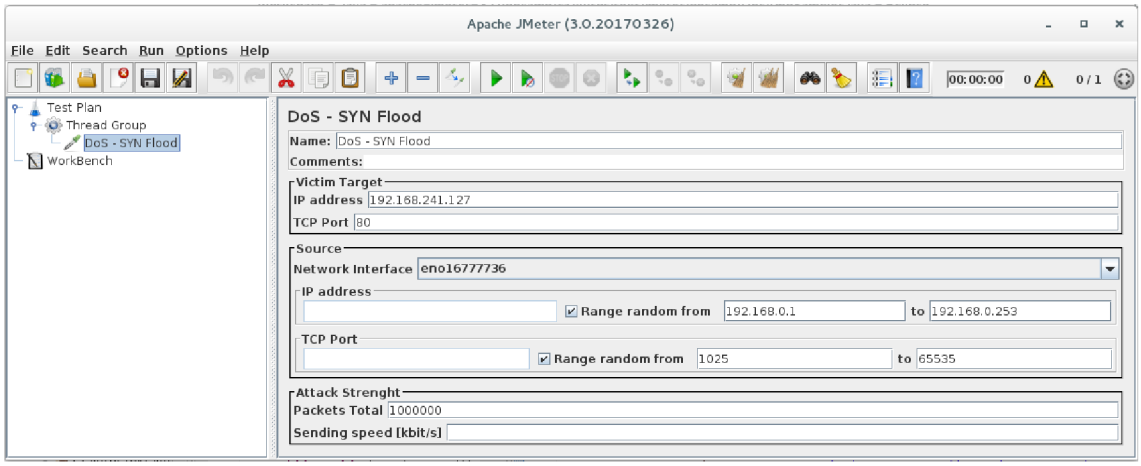
Výpis 3.7: Metoda killTrafgen generující příkaz pro ukončení Trafgen.

```
public static void killTrafgen(String PIDS)
    throws InterruptedException {
        String command= "pkexec␣kill␣-SIGKILL␣" + PIDS;
        String[] args = new String[] {"/bin/bash","-c",command};
        try {
             Process pr = new ProcessBuilder(args).start();
             pr.waitFor();
            } catch (IOException e) {
                   e.printStackTrace();
                   }
            }
}
```

3.2.1 Testování modulu DoS - SYN Flood

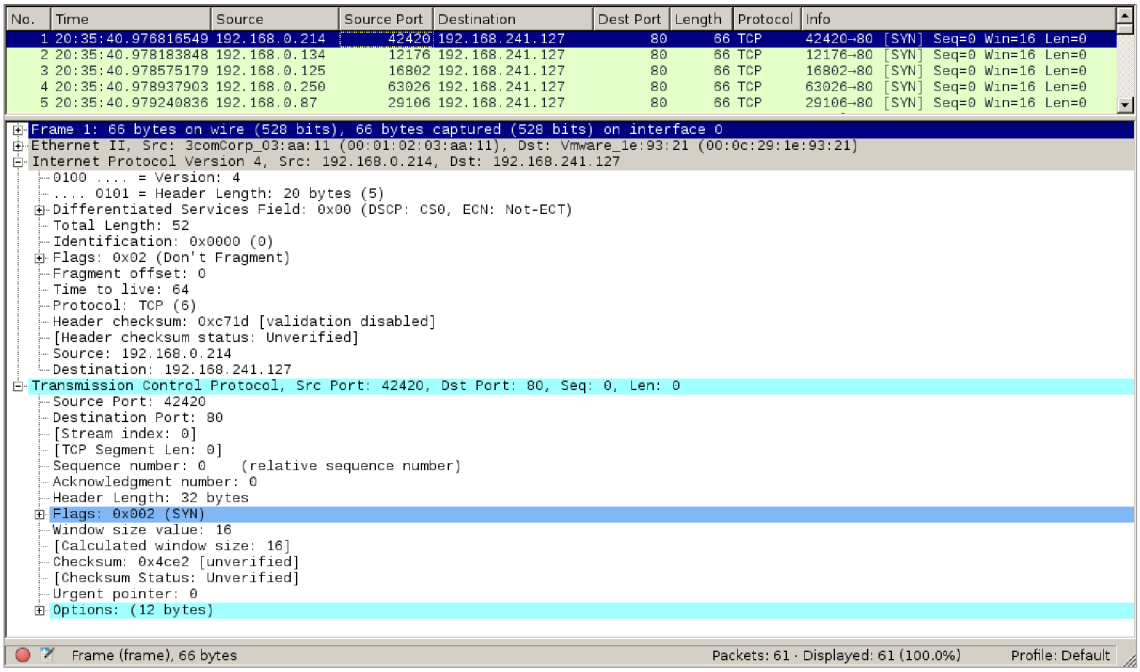
Testování funkčnosti rozhraní

Nastavení testovacího plánu Jmeteru a modulu SYN Flood pro účely testování je zobrazeno na obrázku 3.4.



Obr. 3.4: Nastavení modulu SYN Flood pro testování.

Na obrázku 3.5 je vidět detail jednoho z paketů odeslaného modulem SYN Flood dle nastavení testovacího plánu v JMeteru.



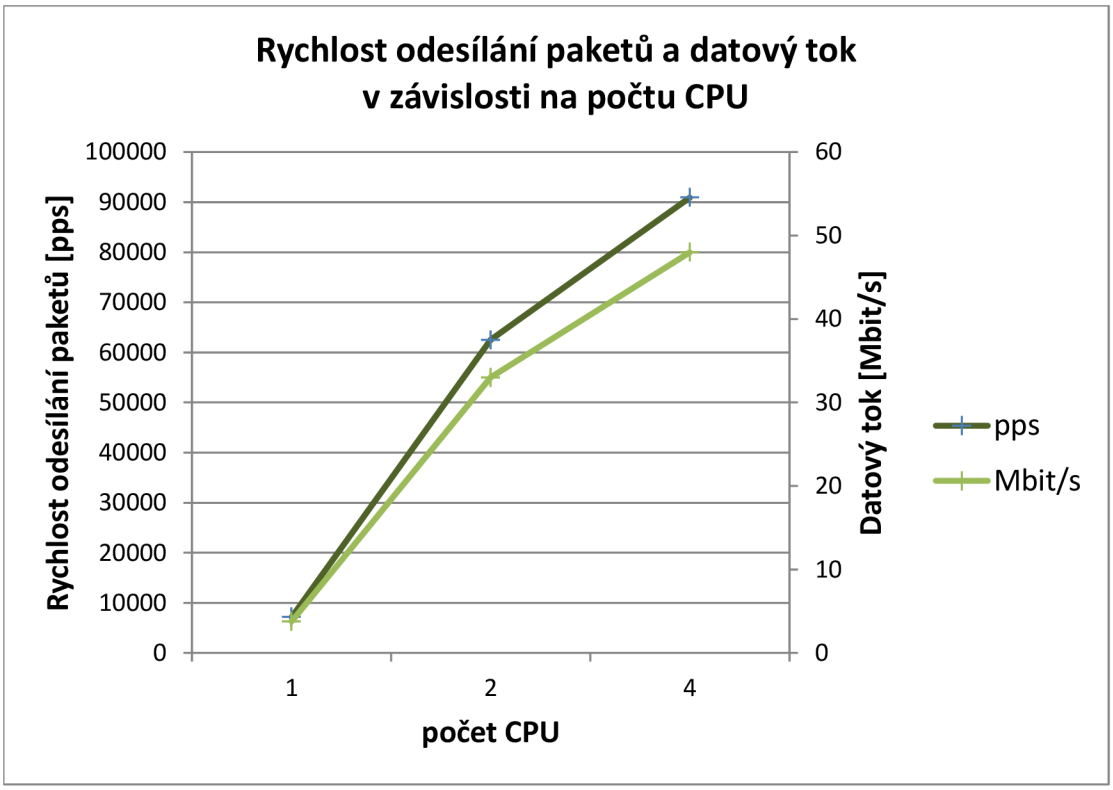
Obr. 3.5: Detail paketu SYN Flood.

Testování výkonnosti

V tabulce 3.2 jsou zapsány naměřené hodnoty výkonosti modulu SYN Flood v závislosti na počtu procesorů virtuálního počítače. Naměřené hodnoty jsou vyneseny do grafu na obrázku 3.6.

Tab. 3.2: Naměřené hodnoty modulu SYN Flood.

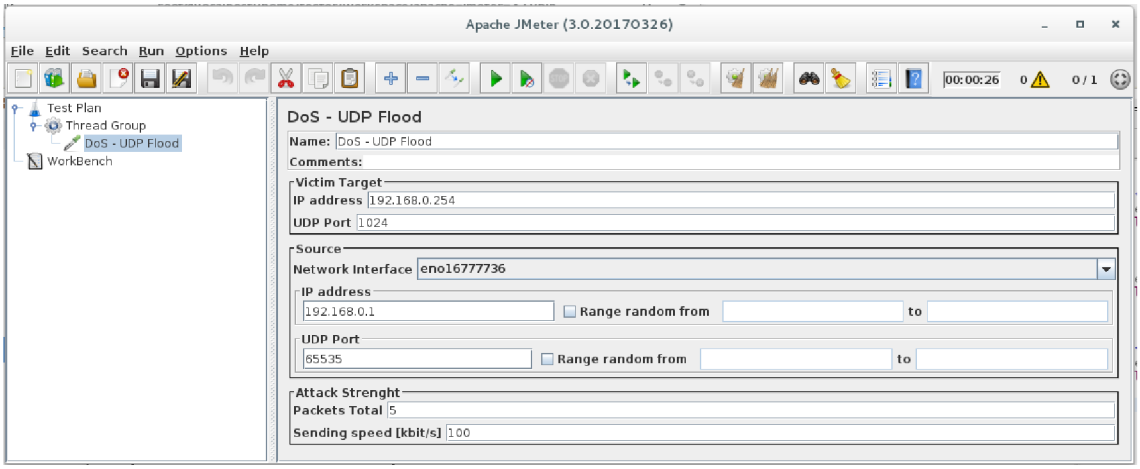
Počet CPU	Čas [s]	Rychlost odesílání [pps]	Datový tok [Mbit/s]
1	140	7143	3,77
2	16	62500	33
4	11	90909	48



Obr. 3.6: Graf výkonosti modulu SYN Flood v závisloti na počtu CPU.

3.3 Modul DoS - UDP Flood

Grafické rozhraní modulu UDP Flood, viz obrázek 3.7, je rozděleno do tří základních částí, kde jsou umístěny prvky rozhraní pro nastavení parametrů cíle útoku, zdroje útoku a síly útoku. Popis a účel jednotlivých prvků rozhraní viz tabulka 3.3.



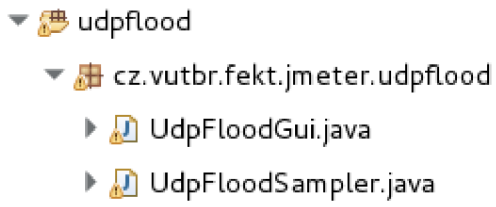
Obr. 3.7: Grafické rozhraní modulu UDP Flood.

Tab. 3.3: Popis grafického rozhraní modulu UDP Flood.

Název prvku	Popis
Victim Target	parametry pro nastavení cíle útoku
IP address	IP adresa cíle útoku
UDP Port	číslo UDP portu cíle útoku
Source	parametry pro nastavení zdroje útoku
Network Interface	síťové rozhraní, ze kterého budou odesílány pakety
IP address	IP adresa, která bude nastavena u odesílaných paketů jako odchozí. Po zaklikutí Range random je možné zadat rozsah IP adres, ze kterých bude náhodně vybrána odchozí IP adresa
UDP Port	číslo UDP portu, který bude nastaven u odesílaných paketů jako odchozí. Po zaklinutí Range random je možné zadat rozsah UDP portů, ze kterých bude náhodně vybrán odchozí UDP port
Attack Strenght	parametry pro nastavení síly útoku
Packets Total	počet paketů, které budou odeslány a potom dojde k ukončení Sampleru. Pokud je zadáno 0, jsou pakety odesílány, dokud nedojde k ukončení Sampleru
Sending speed	rychlost odesílání paketů v kbit/s

Popis zdrojových kódů balíčku DoS - UDP Flood

Balíček modulu UDP Flood se skládá ze tříd UdpFloodGui a UdpFloodSampler, viz obrázek 3.8.



Obr. 3.8: Třídy modulu UDP Flood.

Třída UdpfloodGui

Tato třída obsahuje objekty, metody a proměnné grafického rozhraní modulu UDP Flood. Zdrojový kód je odvozen ze třídy SynFloodGui modulu SYN Flood a je upraven pro potřeby modulu UDP Flood.

Třída UdpFloodSampler

Tato třída obsahuje metody pro ovládání externí aplikace Trafgen pomocí příkazů v příkazovém řádku spouštěných na pozadí, dle proměnných nastavených v grafickém prostředí JMeteru.

Při spuštění testu je vytvořen vstupní konfigurační soubor pro aplikaci Trafgen s konfigurací paketu, viz výpis 3.8

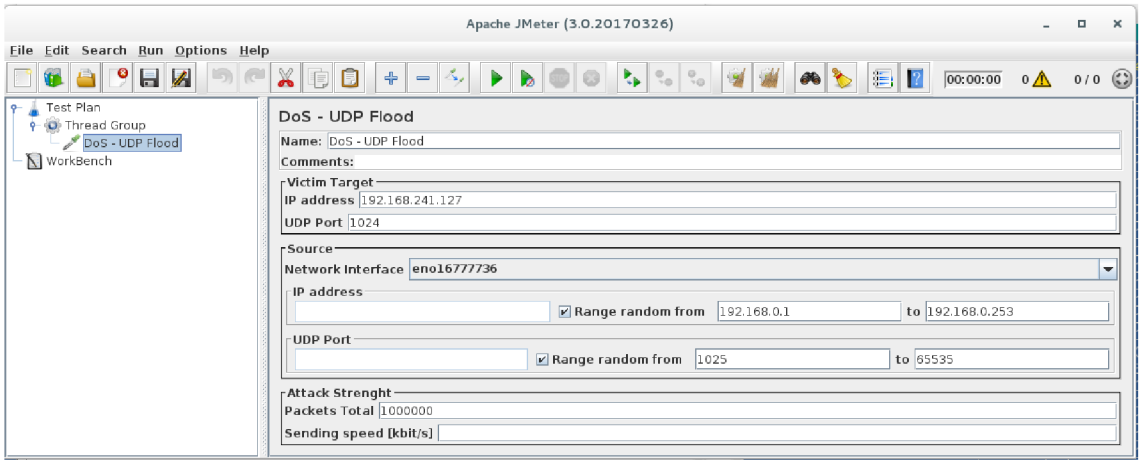
Výpis 3.8: Konfigurační soubor udpflood.cfg

```
#define ETH_P_IP   0x0800
{
  eth(daddr=00:0c:29:68:18:22,
  saddr=00:01:02:03:aa:11,
  proto=ETH_P_IP),
  ipv4(ttl=64, ver=4, flags=0b01000000, frag=0, df,
  da=192.168.0.254, sa=192.168.0.1),
  udp(sport=65535, dport=1024),
  fill('B',18),
}
```

3.3.1 Testování modulu DoS - UDP Flood

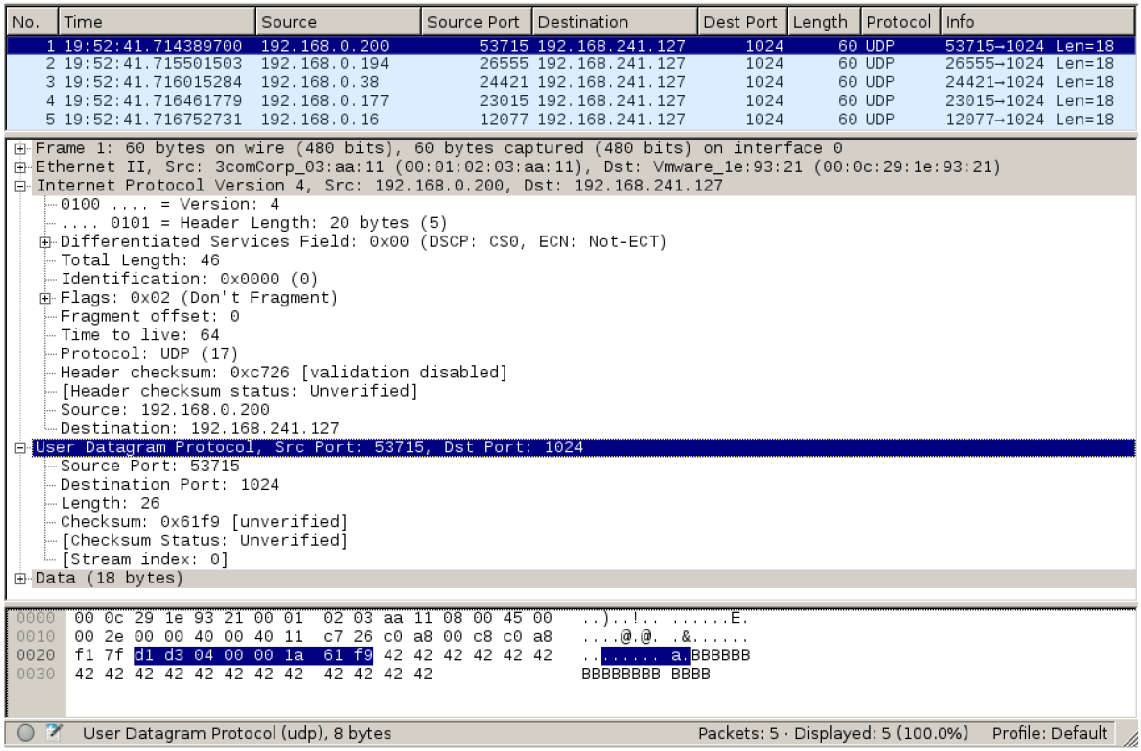
Testování funkčnosti rozhraní

Nastavení testovacího plánu JMeteru a modulu UDP Flood pro účely testování je zobrazeno na obrázku 3.9.



Obr. 3.9: Nastavení modulu UDP Flood pro testování.

Na obrázku 3.10 je detail jednoho z paketů odeslaného modulem UDP Flood dle nastavení testovacího plánu v JMeteru.



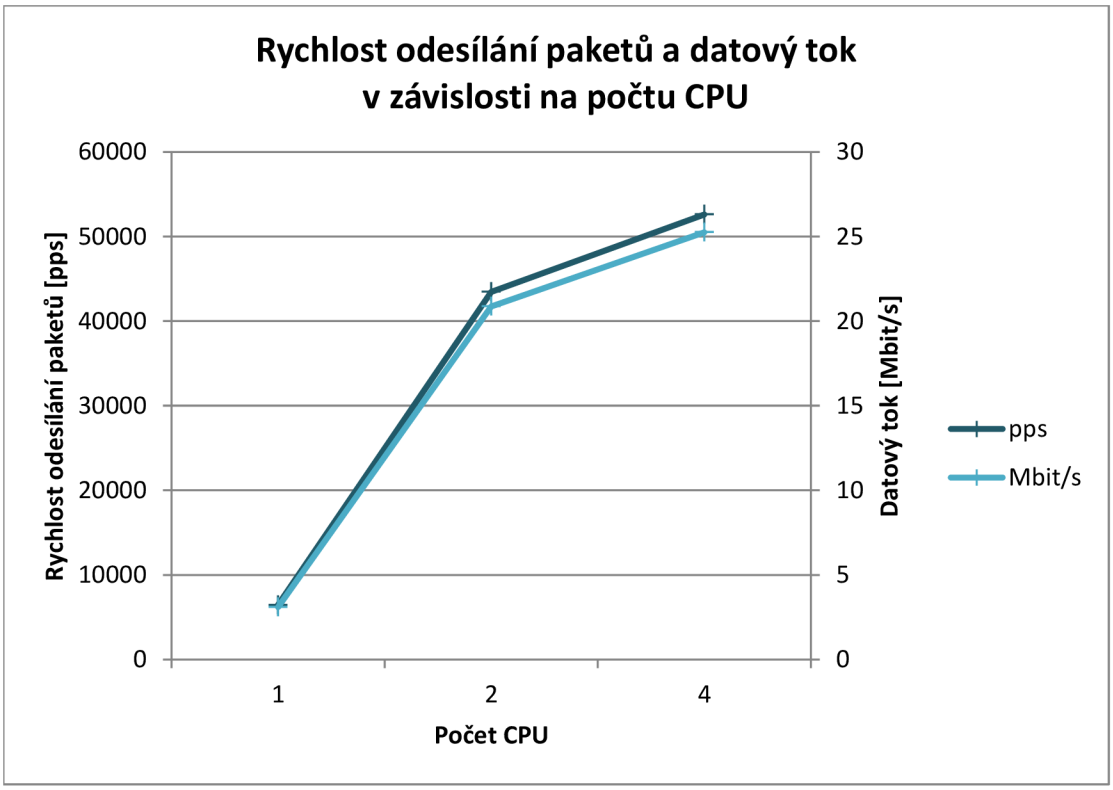
Obr. 3.10: Detail paketu UDP Flood.

Testování výkonnosti

V tabulce 3.4 jsou zapsány naměřené hodnoty výkonosti modulu UDP Flood v závislosti na počtu procesorů virtuálního počítače. Naměřené hodnoty jsou vyneseny do grafu na obrázku 3.11.

Tab. 3.4: Naměřené hodnoty modulu UDP Flood.

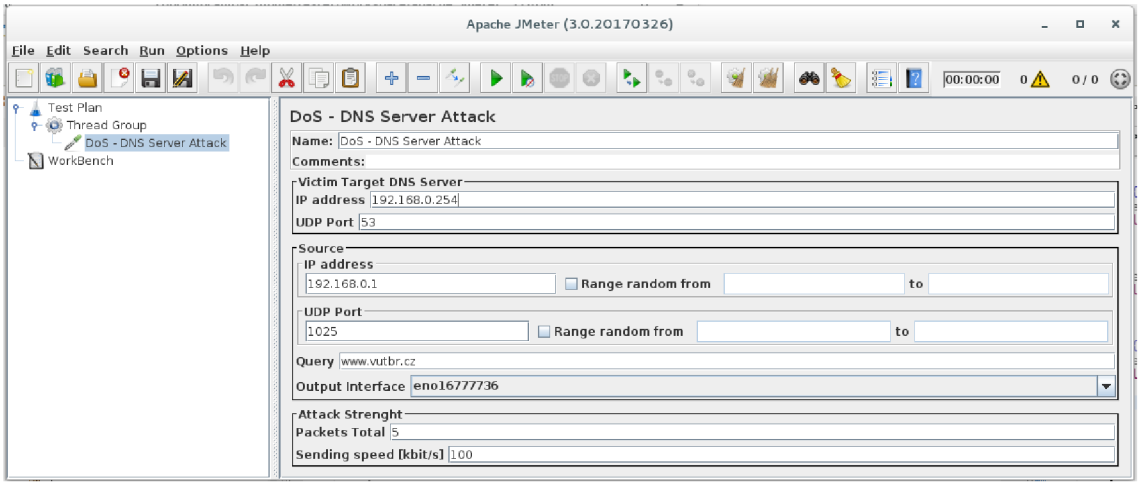
Počet CPU	Čas [s]	Rychlost odesílání [pps]	Datový tok [Mbit/s]
1	155	6452	3,1
2	23	43478	20,87
4	19	52631	25,26



Obr. 3.11: Graf výkonosti modulu UDP Flood v závislosti na počtu CPU.

3.4 Modul DoS - DNS Server Attack

Grafické rozhraní modulu DNS Server Attack, viz obrázek 3.12, je rozděleno do tří základních částí, kde jsou umístěny prvky rozhraní pro nastavení parametrů cíle útoku, zdroje útoku a síly útoku. Popis a účel prvků rozhraní viz tabulka 3.5.



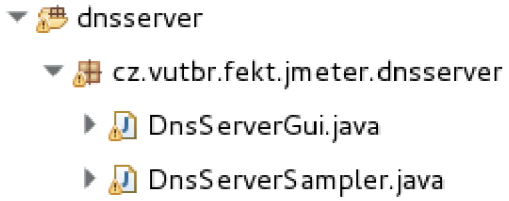
Obr. 3.12: Grafické rozhraní modulu DNS Server Attack.

Tab. 3.5: Popis grafického rozhraní modulu DNS Server Attack.

Název prvku	Popis
Victim Target DNS Server	parametry pro nastavení cíle útoku
IP address	IP adresa DNS serveru, na který bude zaslán paket s dotazem na překlad
UDP Port	číslo UDP portu DNS serveru, zpravidla 53
Source	parametry pro nastavení zdroje útoku
IP address	IP adresa zdroje dotazu, kam bude DNS server odesílat odpověď. V odesílaném paketu bude nastavena jako odchozí. Po zakliknutí Range random je možné zadat rozsah IP adres
UDP Port	číslo UDP portu, který bude nastaven u odesílaných paketů jako odchozí. Po zaklinutí Range random je možné zadat rozsah UDP portů, ze kterých bude náhodně vybrán odchozí UDP port
Query	dotaz, na který bude DNS server odpovídat
Output Interface	síťové rozhraní, které bude použito k odesílání paketů
Attack Strenght	parametry pro nastavení síly útoku
Packets Total	počet paketů, které budou odeslány a potom dojde k ukončení Sampleru. Pokud je zadáno 0, jsou pakety odesílány, dokud nedojde k ukončení Sampleru
Sending speed	rychlost odesílání paketů v kbit/s

Popis zdrojových kódů balíčku DoS - DNS Server Attack

Balíček modulu DNS Server Attack se skládá ze tříd DnsServerGui a DnsServerSampler, viz obrázek 3.13.



Obr. 3.13: Třídy modulu DNS Server Attack.

Třída DnsServerGui

Tato třída obsahuje objekty, metody a proměnné grafického rozhraní modulu. Zdrojový kód je odvozen ze třídy UdpFloodGui modulu UDP Flood. Třída je rozšířena o proměnnou parametru QUERY pro zadání dotazu pro DNS Server.

Třída DnsServerSampler

Tato třída obsahuje metody pro ovládání externí knihovny Trafgen pomocí bash příkazů spouštěných na pozadí, dle proměnných nastavených v grafickém prostředí JMeteru.

Pro účely DNS protokolu je tato třída rozšířena o funkci pro parsování a zápis parametru QUERY do konfiguračního souboru paketu viz výpis 3.9.

Výpis 3.9: Parsování DNS Query.

```
String[] parsed = this.getPropertyAsString(QUERY).split("\\.");
      String out = "";
      for (int i = 0; i < parsed.length; i++) {
        int lenght = parsed[i].length();
        String hex = null;
        if(lenght<10){
          hex = "␣␣␣0x0" + Integer.toHexString(lenght);
        }else {
          hex = "␣␣␣0x" + Integer.toHexString(lenght);
        }
        out = hex + ",␣␣" + "\""+parsed[i] + "\"," + "\n";
        writer.write(out);
      }
```

Při spuštění testu je vytvořen vstupní konfigurační soubor pro aplikaci Trafgen s konfigurací paketu, viz výpis 3.10

Výpis 3.10: Konfigurační soubor dnsserver.cfg

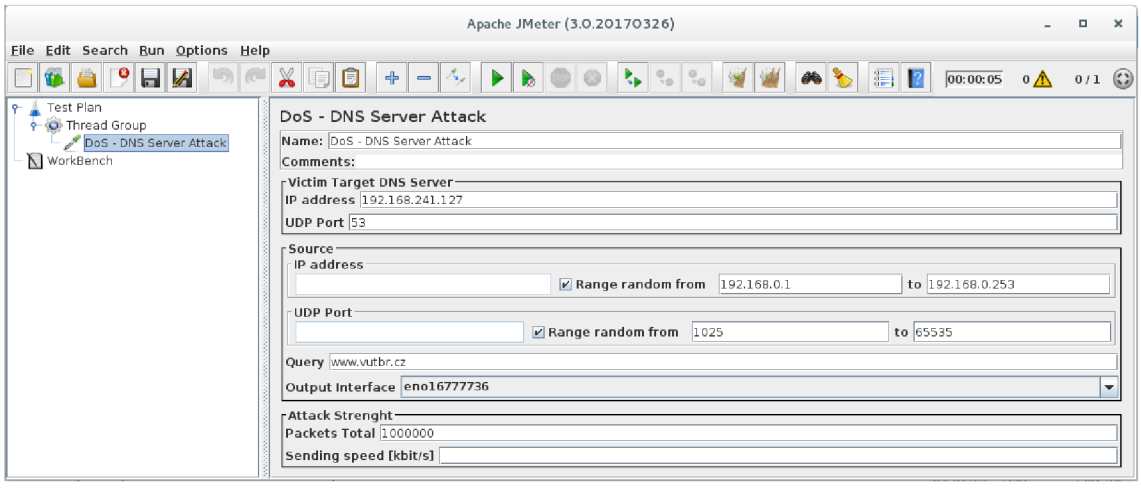
```
#define ETH_P_IP  0x0800
{
  eth(daddr=00:0c:29:68:18:22,
  saddr=00:01:02:03:aa:11,
  proto=ETH_P_IP),

  ipv4(ttl=64, ver=4, flags=0b01000000, frag=0, df,
  da=192.168.241.127, sa=192.168.0.1),

  udp(sport=1025, dport=53),
```

```
    drnd(2), const16(0x0100), const16(1),
    const16(0), const16(0), const16(1),

    0x03,  "www",
    0x05,  "vutbr",
    0x02,  "cz",
    0x00,
    const16(28), const16(1),

    0x00, const16(41), const16(4096), 0x00,
    0x00, 0x00, 0x00
    const16(0)
}
```

3.4.1 Testování modulu DoS - DNS Server Attack

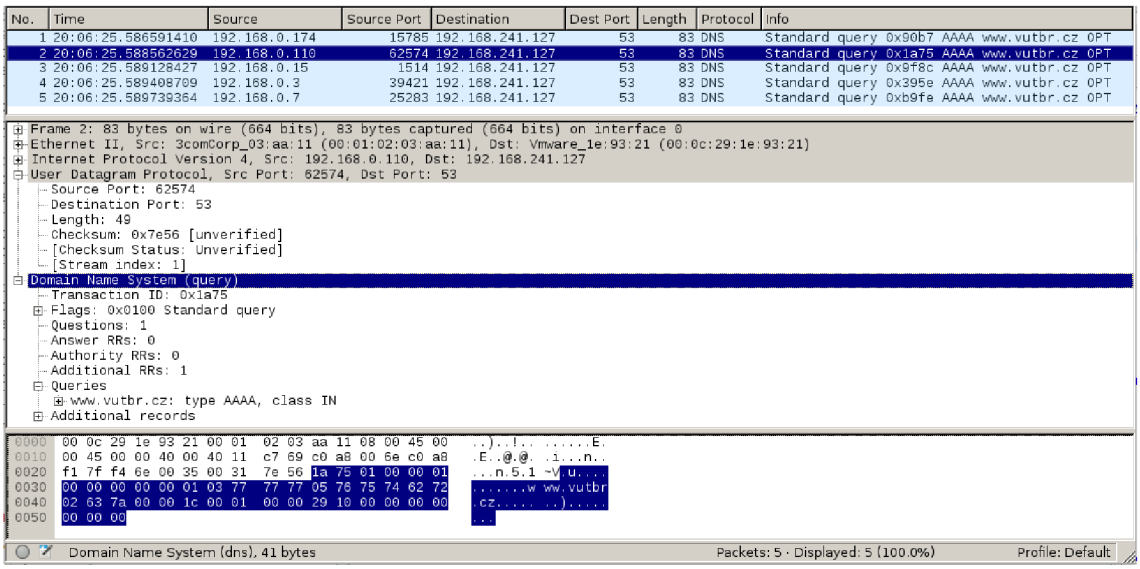
Testování funkčnosti rozhraní

Nastavení testovacího plánu JMeteru a modulu DNS Server Attack pro účely testování je zobrazeno na obrázku 3.14.



Obr. 3.14: Nastavení modulu DNS Server Attack.

Na obrázku 3.15 je vidět detail jednoho z paketů vyslaného modulem DNS Server Attack dle nastavení testovacího plánu v JMeteru.



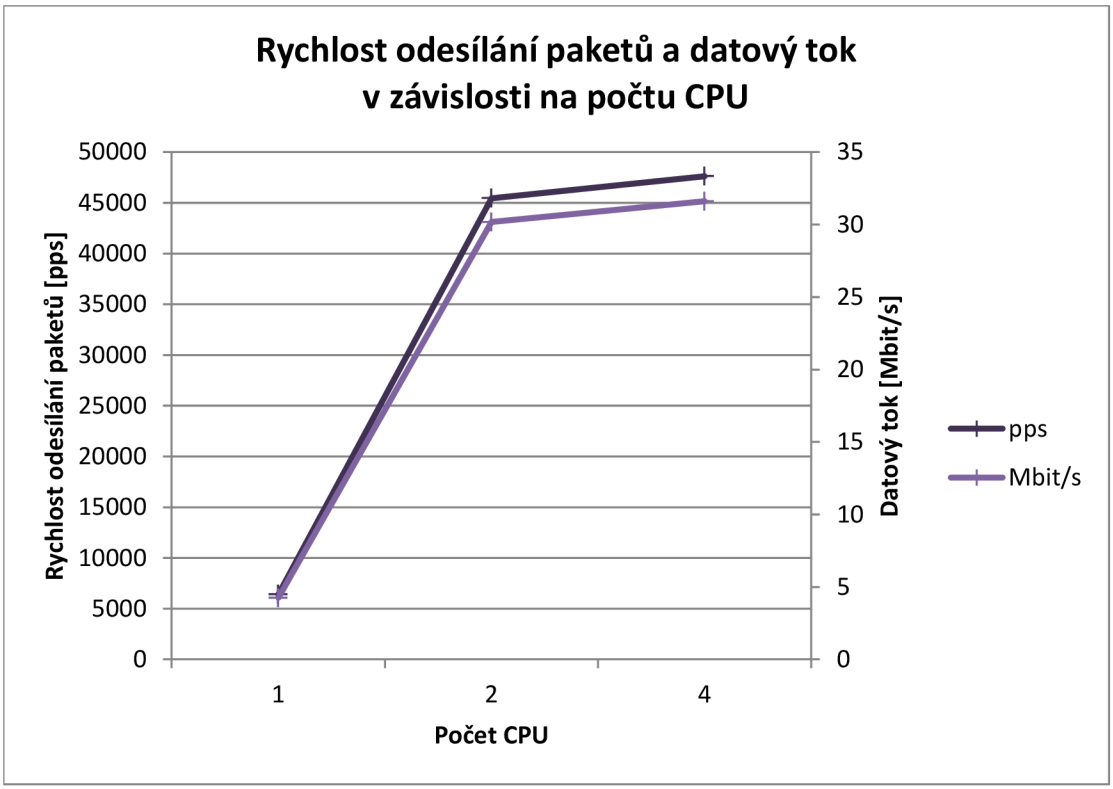
Obr. 3.15: Detail paketu DNS Server Attack.

Testování výkonnosti

V tabulce 3.6 jsou zapsány naměřené hodnoty výkonnosti modulu DNS Server Attack v závislosti na počtu procesorů virtuálního počítače. Naměřené hodnoty jsou vyneseny do grafu na obrázku 3.16.

Tab. 3.6: Naměřené hodnoty modulu DNS Server Attack.

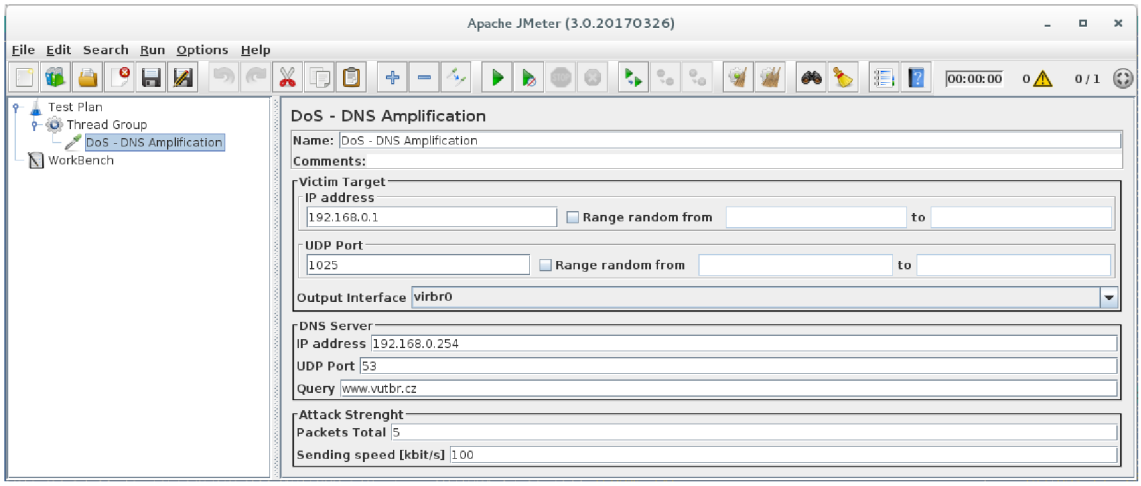
Počet CPU	Čas [s]	Rychlost odesílání [pps]	Datový tok [Mbit/s]
1	156	6410	4,26
2	22	45454	30,18
4	21	47619	31,61



Obr. 3.16: Graf výkonnosti modulu DNS Server Attack v závisloti na počtu CPU.

3.5 Modul DoS - DNS Amplification

Grafické rozhraní elementu DNS Amplification je zobrazeno na obrázku 3.17. Popis jednotlivých prvků rozhraní viz tabulka 3.7.



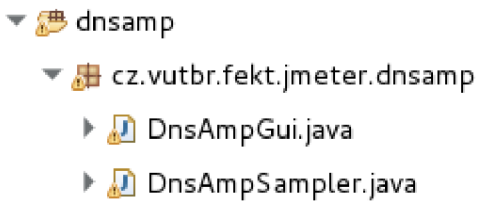
Obr. 3.17: Grafické rozhraní modulu DNS Amplification.

Tab. 3.7: Popis grafického rozhraní modulu DNS Amplification.

Název prvku	Popis
Victim Target	parametry pro nastavení cíle útoku
IP address	IP adresa cíle útoku, kam bude DNS server odesílat odpověď. V odesílaném paketu bude nastavena jako odchozí. Po zakliknutí Range random je možné zadat rozsah IP adres
UDP Port	číslo UDP portu cíle útoku, kam bude DNS server odesílat odpověď. V odesílaném paketů bude nastaven jako odchozí. Po zakliknutí Range random je možné zadat rozsah UDP portů
Output Interface	síťové rozhraní, které bude použito pro odesílání paketů
DNS Server	parametry pro nastavení zdroje útoku
IP address	IP adresa DNS serveru, na který bude zaslán paket s dotazem na překlad
UDP Port	číslo UDP portu DNS serveru, zpravidla 53
Query	dotaz, na který bude DNS server odpovídat
Attack Strenght	parametry pro nastavení síly útoku
Packets Total	počet paketů, které budou odeslány a potom dojde k ukončení Sampleru. Pokud je zadáno 0, jsou pakety odesílány, dokud nedojde k ukončení Sampleru
Sending speed	rychlost odesílání paketů v kbit/s

Popis zdrojových kódů balíčku DoS - DNS Amplification

Balíček modulu DNS Amplification se skládá ze tříd DnsAmpGui a DnsAmpSampler, viz obrázek 3.18.



Obr. 3.18: Třídy modulu DNS Amplification.

Třída DnsAmpGui

Tato třída obsahuje objekty a metody grafického rozhraní modulu. Zdrojový kód je odvozen ze třídy DnsServerGui a je upraven pro potřeby modulu DNS Amplification.

Třída DnsAmpSampler

Tato třída obsahuje metody pro ovládání externí aplikace Trafgen pomocí bash příkazů spouštěných na pozadí, dle proměnných nastavených v grafickém prostředí JMeteru.

Při spuštění testu je vytvořen vstupní konfigurační soubor pro aplikaci Trafgen s konfigurací paketu, viz výpis 3.11

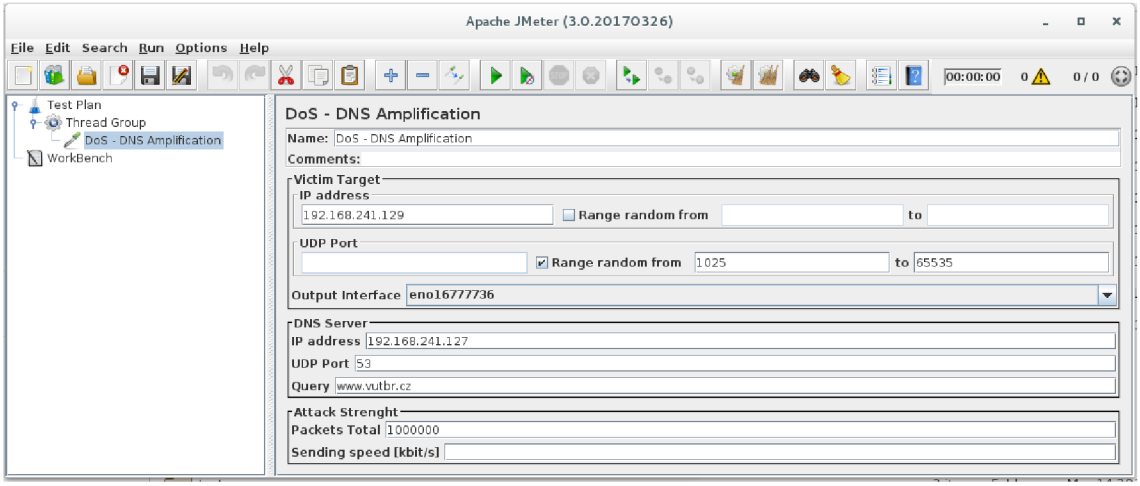
Výpis 3.11: Konfigurační soubor dnsamp.cfg

```
#define ETH_P_IP  0x0800
{
  eth(daddr=00:0c:29:1e:93:21,
  saddr=00:01:02:03:aa:11,
  proto=ETH_P_IP),

  ipv4(ttl=64, ver=4, flags=0b01000000, frag=0, df,
  da=192.168.241.127, sa=192.168.241.129),

  udp(sport=drnd(1025, 65535), dport=53),

   drnd(2), const16(0x0100), const16(1),
   const16(0), const16(0), const16(1),

   0x03,  "www",
   0x05,  "vutbr",
   0x02,  "cz",
   0x00,
   const16(28), const16(1),

   0x00, const16(41), const16(4096), 0x00,
   0x00, 0x00, 0x00
   const16(0)
}
```

3.5.1 Testování modulu DoS - DNS Amplification

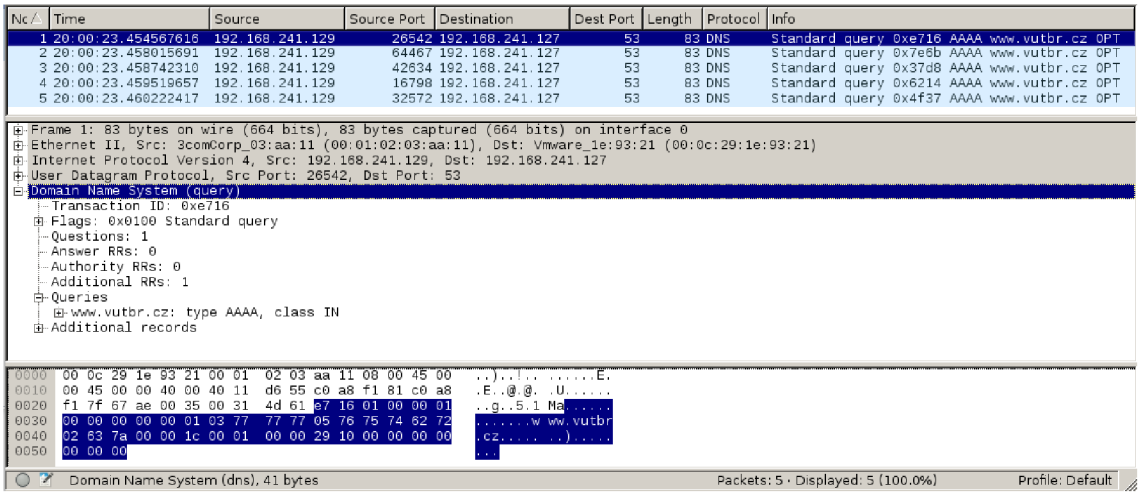
Testování funkčnosti rozhraní

Nastavení testovacího plánu JMeteru a modulu DNS Amplification pro účely testování je zobrazeno na obrázku 3.19.



Obr. 3.19: Nastavení elementu DNS Amplification.

Na obrázku 3.20 je vidět detail jednoho z paketů odeslaného modulem DNS Amplification dle nastavení testovacího plánu v JMeteru.



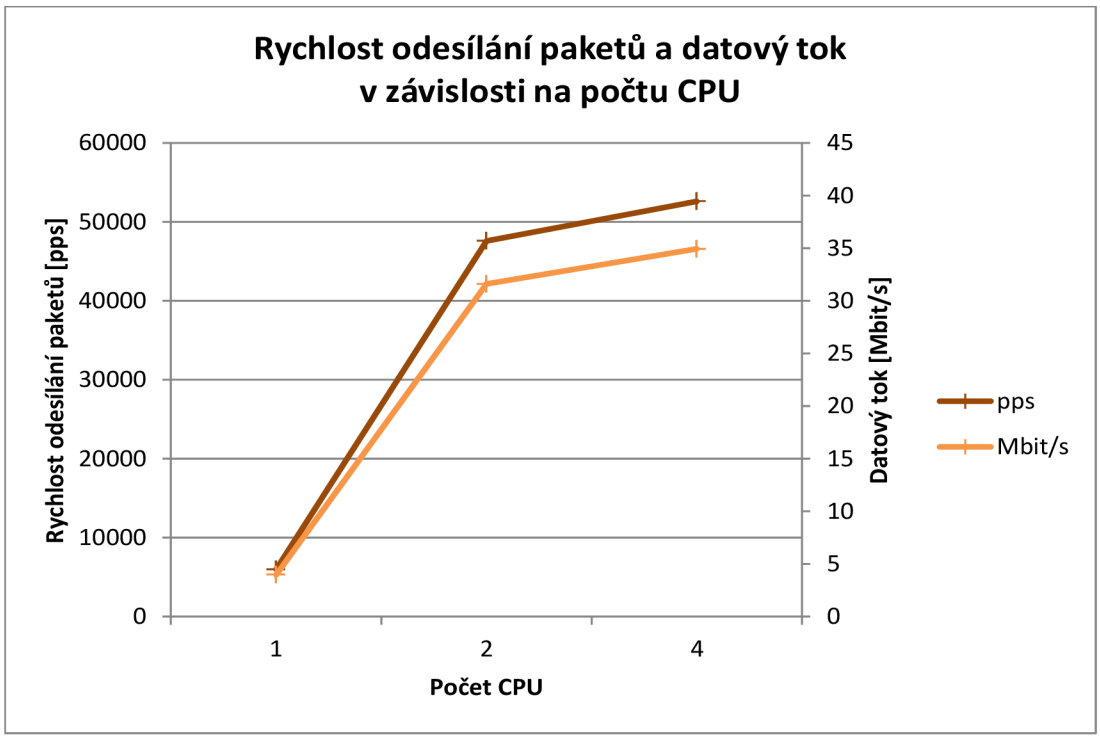
Obr. 3.20: Detail paketu DNS Amplification.

Testování výkonnosti

V tabulce 3.8 jsou zapsány naměřené hodnoty výkonnosti modulu DNS Amplification v závislosti na počtu procesorů virtuálního počítače. Naměřené hodnoty jsou vyneseny do grafu na obrázku 3.21.

Tab. 3.8: Naměřené hodnoty modulu DNS Amplification.

Počet CPU	Čas [s]	Rychlost odesílání [pps]	Datový tok [Mbit/s]
1	167	5988	3,98
2	21	47619	31,62
4	19	52631	34,95

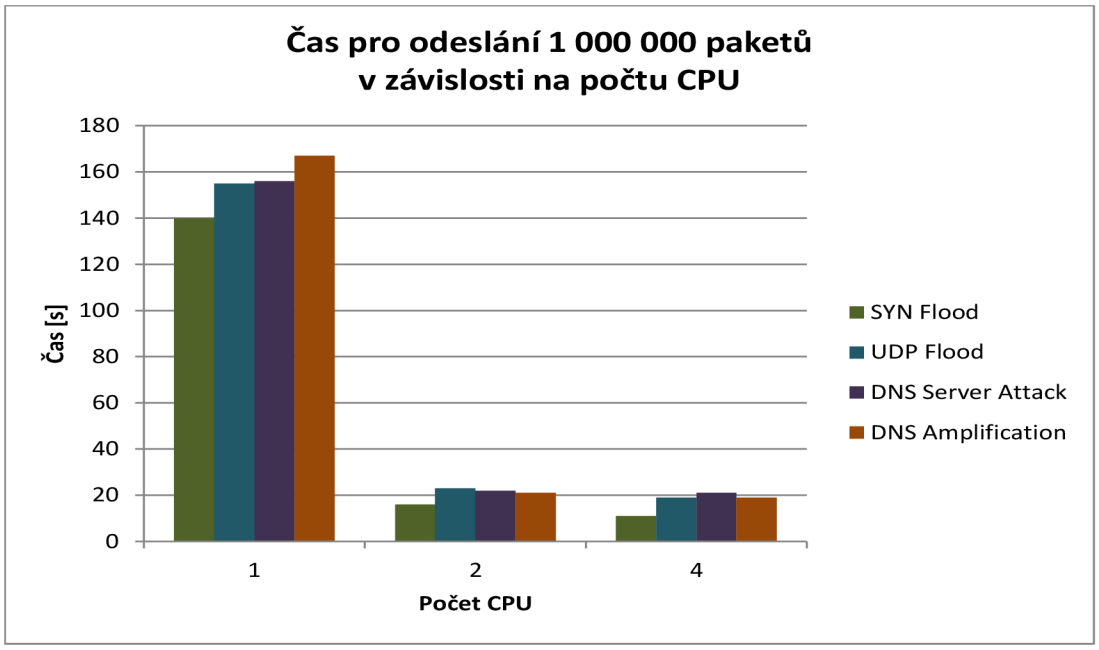


Obr. 3.21: Graf výkonnosti modulu DNS Amplification v závisloti na počtu CPU.

3.6 Výkonnostní analýza modulů

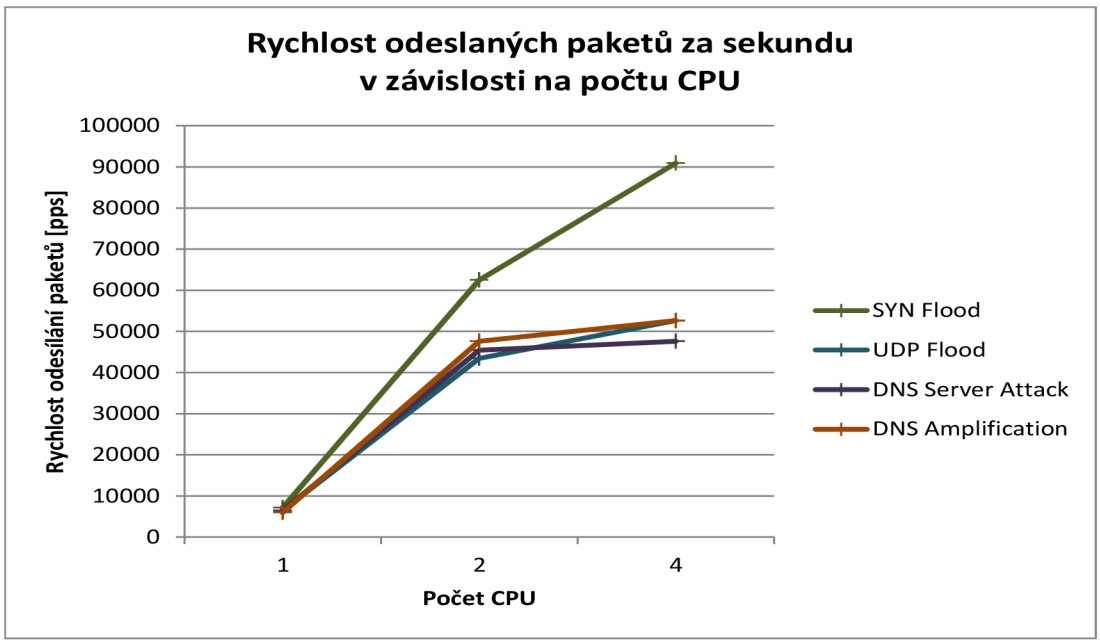
Graf naměřených hodnot výkonosti všech modulů, podle času potřebného pro odeslání 1 000 000 paketů, maximální rychlostí v závislosti na počtu nastavených CPU virtuálního stroje, viz obrázek 3.22.

Z grafu je patrná závislost potřebného času pro odeslání paketů na počtu nastavených CPU. Porovnáním výkonosti jednotlivých modulů se jeví jako nejvýkonnější modul SYN Flood s časem 140 sekund následovaný UDP Floodem. Pravděpodobným důvodem je menší velikost vygenerovaného paketu než u modulů DNS Server Attack a DNS Amplification, které generují větší pakety z důvodu vložení dotazu DNS protokolu.aw



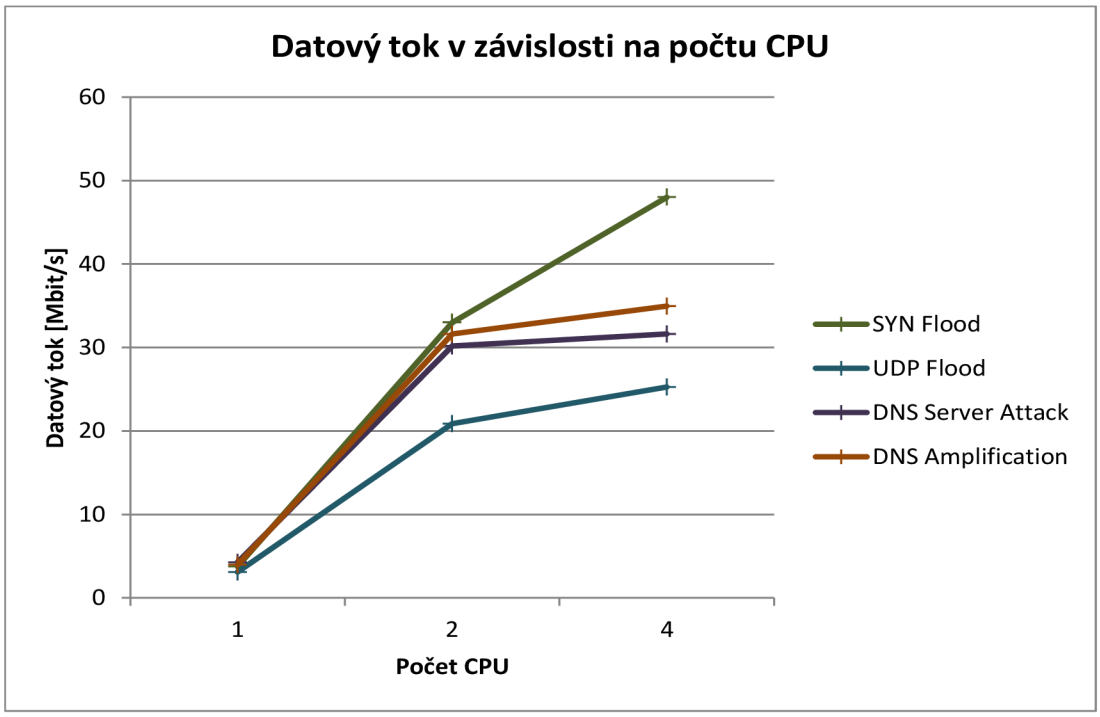
Obr. 3.22: Srovnání výkonu modulů podle počtu CPU.

Graf naměřených hodnot výkonnosti všech modulů, podle maximální rychlosti odeslaných paketů za sekundu v závislosti na počtu nastavených CPU virtuálního stroje, viz obrázek 3.23. Nejvyšší rychlosti odesílání paketů za sekundu dosahuje modul SYN Flood s hodnotou 90 909 pps. Ostatní moduly dosahují hodnot od 48 000 do 52 000 pps.



Obr. 3.23: Graf závislosti rychlosti odesílání paketů na počtu CPU.

Graf naměřených hodnot výkonnosti všech modulů, podle maximálního datového toku v závislosti na počtu nastavených CPU virtuálního stroje, viz obrázek 3.24. Nejvyšší datový tok generuje modul SYN Flood s rychlostí 48 Mbit/s. Nejnižší datový tok naopak generuje modul UDP Flood.



Obr. 3.24: Graf závislosti datevého toku na počtu CPU.

4 ZÁVĚR

Bakalářská práce se zabývá problematikou kybernetických útoků typu DoS. Cílem práce bylo rozšířit pomocí přídavných modulů možnosti spouštění vybraných kybernetických útoků přímo z grafického rozhraní aplikace JMeter využitím externí knihovny Trafgen pro generování síťových paketů.

Teoretická část práce pojednává o kybernetických útocích typu DoS obecně. V této kapitole je popsáno jak jsou definovány kybernetické útoky typu DoS a podle kterých vlastností je dále dělíme a rozlišujeme. V této kapitole jsou podrobně popsány principy vybraných kybernetických útoků SYN Flood, UDP Flood, DNS Server attack a DNS Amplification včetně popisu parametrů protokolů, které jsou nutné konfigurovat pro generování síťových paketů.

Druhá kapitola se věnuje samotné aplikaci pro zátěžové testování JMeter. Popisuje ovládání aplikace a konfiguraci testovacích plánů pro spouštění zátěžových testů. Dále je v této kapitole popsána externí knihovna Trafgen, která je použita jako výkonný generátor síťových paketů. V závěru této kapitoly je popsán princip propojení externí knihovny Trafgen s aplikací JMeter pomocí rozšiřujících modulů.

Praktická část práce se zabývá samotným vývojem jednotlivých modulů. V úvodu kapitoly je popsáno použité vývojové a testovací prostředí. Dále jsou v této kapitole podrobně popsány jednotlivé vyvinuté moduly včetně popisu grafických rozhraní a důležitých částí zdrojových kódů včetně výsledků měření a testování jednotlivých modulů. Závěr této kapitoly se věnuje výkonnostní analýze všech vyvinutých modulů.

Vyvinuté moduly jsou uloženy na přiloženém DVD včetně všech zdrojových kódů a ukázkových konfiguračních souborů.

LITERATURA

[1] HALILI, Emily H. *Apache JMeter: A practical beginner's guide to automated testing and performance measurement for your websites*. Packt Publishing Ltd, 2008.

[2] Denial of Service Attacks. *CERT* [online]. 1997, [cit. 19. 11. 2016]. Dostupné z URL: <`https://www.cert.org/information-for/denial_of_service.cfm`>.

[3] Understanding Denial-of-Service Attacks. *US-CERT* [online]. 4. 11. 2009, poslední aktualizace 4. 2. 2013 [cit. 19. 11. 2016]. Dostupné z URL: <`https://www.us-cert.gov/ncas/tips/ST04-015`>.

[4] DDoS Survival Handbook. *RADWARE* [online]. 2016, [cit. 20. 11. 2016]. Dostupné z URL: <`https://www.radware.com/ddoshandbook`>.

[5] DUCK,M. READ,R. *Data Communications and Computer Networks for Computer Scientists and Engineers*. Pearson Education Limited, ISBN-10: 0-13-093047-4, UK, 2003

[6] DOSTÁLEK,L. KABELOVÁ,A. *Velký průvodce protokoly TCP/IP a systémem DNS*. Computer Press, ISBN 80-7226-323-4, Praha: 2000

[7] ERINLE, Bayo. *Performance Testing with JMeter 2.9*. Packt Publishing Ltd, 2013.

[8] Netsniff-NG toolkit. *NETSNIFF-NG* [online]. 2017, [cit. 19. 5. 2017]. Dostupné z URL: <`http://netsniff-ng.org/`>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

BIND	Berkeley Internet Name Domain
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IP	Internet Protocol
IPv4	Internet protocol version 4
JVM	Java Virtual Machine
PID	process identification number
pps	packet per second
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet protocol
UDP	User Datagram Protocol

SEZNAM PŘÍLOH

A OBSAH PŘILOŽENÉHO DVD

- `/` ..... kořenový adresář přiloženého DVD
  - `dns-amp` ..... adresář se soubory modulu DNS Amplification
    - `dnsamp.cfg` ..... příklad konfiguračního souboru Trafgen
    - `dnsamp.jar` ..... soubor modulu pro import do JMeteru
    - `dnsamp.zip` ..... archiv zdrojových kódů modulu
  - `dns-server` ..... soubory modulu DNS Server Attack
    - `dnsserver.cfg` ..... příklad konfiguračního souboru Trafgen
    - `dnsserver.jar` ..... soubor modulu pro import do JMeteru
    - `dnsserver.zip` ..... archiv zdrojových kódů modulu
  - `syn-flood` ..... soubory modulu SYN Flood
    - `synflood.cfg` ..... příklad konfiguračního souboru Trafgen
    - `synflood.jar` ..... soubor modulu pro import do JMeteru
    - `synflood.zip` ..... archiv zdrojových kódů modulu
  - `udp-flood` ..... soubory modulu UDP Flood
    - `udpflood.cfg` ..... příklad konfiguračního souboru Trafgen
    - `udpflood.jar` ..... soubor modulu pro import do JMeteru
    - `udpflood.zip` ..... archiv zdrojových kódů modulu
  - `Kybernetické-útoky-v-programu-Jmeter.pdf` .... bakalářské práce v PDF