ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ
V PRAZE

Fakulta elektrotechnická

Bakalářská práce

2014 Nguyen Ngoc Phuong

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

Pracoviště pro testování odolnosti proti útokům typu DoS

květen 2014

Student: Nguyen Ngoc Phuong

Vedoucí práce: Ing. Pavel Bezpalec, Ph.D.

Čestné prohlášení

Prohlašuji, že jsem zadanou bakalářskou práci zpracoval sám pod vedením vedoucího práce a používal jsem literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé bakalářské práce nebo její části se souhlasem katedry.

V Praze dne 23.5. 2014 Nguyen Ngoc Phuong

Poděkování

Děkuji Ing. Pavlovi Bezpalcovi, Ph.D, vedoucímu bakalářské práce, za trpělivost a jeho cenné rady, jimiž mi ochotně pomáhal během vypracování bakalářské práce a panu Pavlovi Kubíkovi za vstřícnost a pomoc s danou problematikou. Rád bych poděkoval také Ing. Janu Šebkovi za připomínky k práci. Dále děkuji své rodině a přátelům za podporu po celou dobu studia.

České vysoké učení technické v Praze
Fakulta elektrotechnická

katedra telekomunikační techniky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: **Nguyen Ngoc Phuong**

Studijní program: Komunikace, multimédia a elektronika
Obor: Síťové a informační technologie

Název tématu: **Pracoviště pro testování odolnosti proti útokům typu DoS**

Pokyny pro vypracování:

Navrhněte pracoviště pro automatizované testování odolnosti zařízení proti útokům typu DoS. Základ pracoviště tvoří HW platforma IXIA.

Seznam odborné literatury:

[1] HW platforma IXIA 400T. Firemní dokumentace, 2013 IXIA. - http://www.ixiacom.com/products/display?skey=ch_400t [online]
[2] IXIA IxNetwork Tcl Development Guide. Firemní dokumentace. 2013 IXIA. - http://downloads.ixiacom.com/library/user_guides/IxNetwork/6.30/EA_6.30_Rev_B/TCLIxNetworkDevGuide/TclIxNetworkDevGuide.pdf [online]

Vedoucí: Ing. Pavel Bezpalec, Ph.D.

Platnost zadání: do konce letního semestru 2014/2015

prof. Ing. Boris Šimák, CSc.
vedoucí katedry

L.S.

prof. Ing. Pavel Ripka, CSc.
děkan

V Praze dne 9. 12. 2013

Anotace

Tato bakalářská práce se zabývá tematikou DoS útoků a jejich realizací podle testovacího scénáře. K tomuto účelu bylo použito zařízení 400T firmy IXIA a jeho komplexní programový nástroj IxExplorer. Byla provedena simulace zařízení prostřednictvím simulačního programu IxChariot, dále byly provedeny realizace tří druhů DoS útoků prostřednictvím grafického rozhraní programu IxExplorer v námi navržené topologii laboratorní sítě. Pro tento účel byly vytvořeny testovací skripty v jazyce Tcl, které byly spuštěny pomocí konzole WishConsole. Během testování jsme sledovali provoz v síti a podle jeho záznamů, jsme zachytili pakety, které byly nadefinované dle vlastností konkrétního typu DoS útoku, z čehož vyplývá, že naše realizace byla úspěšná.

Klíčova slova

DoS útoky, IxChariot, IxExplorer, Tcl, WishConsole, skript.

Abstract This bachelor thesis deals with a topic of DoS attacks and its implementation according to a test scenario. For this purpose, the device 400T by IXIA and its complex software tool IxExplorer were used. A device simulation via the simulation software IxChariot was executed, implementations of three types of DoS attacks via the graphical interface of IxExplorer in a proposed lab network topology. For this purpose, test scripts in the Tcl language were created and launched by a console WishConsole. During the testing, we were recording the network traffic and we captured packets which were defined by characteristics of the specific type of a DoS attack. This showed that the performed implementation was successful.

Keywords

DoS attacks, IxChariot, IxExplorer, Tcl, WishConsole, script.

Obsah

1 Úvod

Tato bakalářská práce se zabývá problematikou síťových útoků typu Denial of Service (dále jen DoS). Na základě konzultací s panem vedoucím byly stanoveny následující body práce. Hlavní náplní bylo studium teoretických principů DoS útoků a softwarového ovládání zařízení IXIA 400T, které slouží jako analyzátor počítačových sítí a zároveň slouží také jako nástroj umožňující demonstraci síťových útoků typu DoS. V rámci práce bylo také nutné prozkoumat další funkce zařízení 400T, které umožňuje testovat sítě a jejich prostředí z hlediska odolnosti vůči síťovým útokům typu DoS, a to jak z hlediska hardwarového, tak softwarového vybavení (jedná se především o IxExplorer, který tvoří pracovní prostředí pro 400T. Hlavními úkoly práce bylo vytvoření testů sloužících pro simulaci DoS útoků dle konkrétního předem zadaného scénáře a vytvoření testovacích skriptů. Skripty v jazyce Tcl byly vytvořeny využitím programů IxExplorer, ScriptGen a WishConsole na straně vzdáleného serveru v rámci operačního systému(OS) IxOS. K tomu byl využit simulační program IxChariot, který obsahoval všechny potřebné komponenty včetně IxExplorer.

Síťové útoky typu DoS jsou v dnešní době velice aktuální tematikou a velkým problémem. K těmto typům útoků dochází na světě v různých regionech každou chvíli. Pro lepší představu je zde uveden odkaz na web, který ukazuje, v jakých oblastech světa dochází k těmto útokům, dostupné z:`http://www.digitalattackmap.com#anim=1&color=0&country=ALL&time=16185&view=map`. Jedná se o velice nebezpečné útoky, které mohou napáchat nemalé škody. Příkladem jsou bankovní společnosti, které nám poskytují elektronické bankovnictví. Pokud by útočníci dokázali zmíněnou službu vyřadit, bankovní společnosti by s postupem času prodělávaly velké množství peněz. Je zcela jasné, že takové útoky jsou trestným činem dle zákona č. 140/1961 sb.. Příkladem častých cílů útoků typu DoS jsou v celosvětovém měřítku webové stránky politických stran. Mezi další cíle útočníků patří servery zpravodajských portálů, škol či jiných institucí. Záměry útočníků mohou být různé, od způsobení finančních škod až po vyjádření nesouhlasu s informačním obsahem napadnutého serveru. Jelikož návodů na realizaci těchto útoku je na Internetu obrovské množství a útok může provést prakticky kdokoliv, je tedy v rukách administrátorů počítačových sítí, aby dokázali tomuto problému předejít.

Proč jsou tedy tématem práce DoS útoky a jejich realizace pomocí zařízení 400T? Primární funkce tohoto zařízení není páchat škody, ale zjišťovat kvalitu sítě, možné chyby či provádění zatěžovacích testů. To, že toto zařízení umí provést DoS útoky je jakousi výhodou, kterou ocení především administrátoři velkých firemních sítí. Díky 400T mohou administrátoři nalézt robustnější způsoby zabezpečení sítě, provést testy než se zprovozní síť do reálného provozu. Nebo ověření sítě, zda je připravena na aplikace nových technologií, které se firma či instituce chystá implementovat. Díky možnosti provádění testů pomocí skriptů přes konzoli, je jejich spuštění a spravování snažší a pohodlnější.

Práci lze dle jejího obsahu rozdělit na tři části: teoretickou, praktickou a vyhodnocení. První část práce se zabývá seznámením se se zařízením 400T, jeho programovým vybavením a základními fyzickými parametry. Je zde také detailně popsána teorie k DoS útokům, základní dělení, jejich vlastnosti a význam. Druhá část se dělí dále na tři podkapitoly. V první podkapitole je popsána simulace v programu IxChariot v rámci domácí počítačové sítě, její jednotlivé kroky a výsledky. V druhé podkapitole je zmíněna rozšířená teorie ke konkrétním typům DoS útoků, postupy při realizaci útoků a jejich výsledky. V poslední podkapitole je popsán postup při ověření správné funkčnosti

portů zařízení a dále vytvoření testovacích skriptů a jejich spuštění.

V rámci vyhodnocení jsou shrnuty a diskutovány dosažené výsledky.

2 Teoretický rozbor

2.1 Vlastnosti a softwarové vybavení zařízení IXIA 400T

2.1.1 Vlastnosti zařízení

V této kapitole jsou uvedeny parametry samotného zařízení IXIA 400T. Údaje v této kapitole byly převzaty z [1]. Jedná se o komplexní zařízení sloužící na testování kvality, propustnosti a bezpečnosti počítačové sítě. Dále toto zařízení může plnit funkci generátoru datového toku, který je definován podle požadavků uživatele. Díky této funkci je možné testovat odolnost námi testované sítě a najít lepší řešení pro její zabezpečení. V níže uvedených odstavcích jsou popsány pouze základní parametry zařízení a její důležité vlastnosti. Konkrétnější a detailnější informace je možno nalézt v manuálech na oficiálních stránkách výrobce (dostupné z `http://www.ixiacom.com/resources/network_test/test_library/user_guides/`).

Obr. 1: Zařízení IXIA 400T

V následujícím výčtu jsou poskytnuty hardwarové parametry zařízení:

- CPU: 1.66 Ghz,
- Paměť RAM: 2 GB,
- Hard disk: typ SATA, velikost 250 GB,
- Operační systém: Windows 7 Ultimate,
- Počet slotů pro paměť: 4,
- Podpora portů typu: COM, RJ11, RJ45, HD-DB 15 Super VGA, PS/2, USB.

Toto zařízení obsahuje následující komponenty:

- TCL klient pro realizaci automatizační skripty z Windows, Linux nebo UNIX,
- ScriptGen nástroj sloužící pro generování Tcl skriptů, konfiguraci hardwaru Ixia,
- Tcl Server softwarový modul pro podporu klienta Tcl na systémech Linux a UNIX.

Zařízení podporuje následující platformy:

- IXIA 250, IXIA 400T, IXIA 1600T,

- Optixia® XL10 , Optixia X16.

Tcl Client, ScriptGen a Tcl Server jsou určené pro následující seznam operačních systémů:

- Microsoft Windows NT/2000, XP, RH Linux, SunOS, Solaris,
- Tcl Server: Microsoft Windows NT/2000, XP.

Následující seznam informací poskytuje přehled podpory typů portů a jejich vlastností:

- podpora pro 10/100/1000 Ethernet i 10G Ethernet,
- podpora Packet Over Sonet (POS) a ATM,
- integrovaný PC regulátor s OS Win7 Ultimate ke správě a konfiguraci a analýze,
- vzdálená správa,
- port-level uživatel přiřazení umožňuje prostředky, které mají být sdíleny mezi více uživateli, což maximalizuje testování zdrojů a poskytuje bezpečné, nepřetržité testovací prostředí,
- současné ovládání až tisíce testovacích portů velkém měřítku, synchronizované testování výkonu,
- skriptované automatizované testovací balíčky poskytují pro jednoduché provádění škálovatelných srovnávání metriky.

Vlastnosti zařízení:

- navržen jako rozšíření standardního Tcl / Tk software pro vývoj vlastních aplikací Tcl
- poskytuje automatické generování příkazů Tcl z hardwarové konfigurace
- Tcl API příkaz struktura je v souladu s typickými aplikacemi Tcl jsou k dispozici na internetu
- zařízení pracuje na systémech Windows, UNIX a Linuxu

Výhody zařízení:

- umožňuje automatizaci, zkušební konfiguraci a provádění napříč až tisíci testovacích portů Ixia
- vytvořit vlastní skripty pro automatizaci často prováděných úloh nebo testů
- výrazně urychlit vývoj testů
- zjednodušení a zvýšení produktivity v oblasti vývoje produktů, zajištění kvality a výrobní testovací prostředí
- umožňuje snadnou správu hardware Ixia z příkazového řádku

2.1.2 Sofwarové vybavení zařízení

IxOS

Je programový balík, který obsahuje důležité knihovny a zastřešuje dále uvedené programy, sloužící pro obsluhu zařízení IXIA 400T. Aktuální verze IxOS je 6.30 EA SP2, ale v rámci práce je využita starší verze 5.70. Důležité je zmínit to, že IxOS je možné nainstalovat na operačních systémech Windows i UNIX. Jednotlivé kroky pro instalaci IxOS si může čtenář stáhnout ze stránek poskytovatele (dostupné z `http://www.ixiacom.com/resources/network_test/test_library/user_guides/#All_Software_-IxOS`).[10]

IxExplorer

Jedná se o jeden z nejdůležitějších programů, který má starosti nastavení parametrů a zachytávání provozu na portech. IxExplorer je programové vybavení, které poskytuje interaktivní grafické rozhraní ke správě a testování sítě. Dále umožňuje generování a analýzu provozu na druhé a čtvrté vrstvě na poli technologií síťového rozhraní včetně Ethernetu, 10 Gigabitového Ethernetu, ATM, POS nebo Frame Relay. Jednotlivé porty zařízení mohou být nakonfigurovány nezávisle na sobě tak, že každý z nich může provádět jiné úkony (filtrování, definování provozu atd.) Použitím IxExploreru jsou získány grafické a statické výsledky zkoušeného zařízení, čehož budeme využívat během našich simulací a testů. Prakticky veškeré nastavení a spouštění má na starosti tento program. Tento software mimo jiné poskytuje kompletní konfiguraci, monitorování a kontrolu testované sítě. [2]

IxChariot

IxChariot je přední testovací nástroj firmy IXIA pro simulaci reálných aplikací, simuluje zařízení a výkon systému v reálných podmínkách zatížení sítě. Obsahuje IxChariot konzoli, Performance koncové body a IxProfile. Tyto nástroje nabízí důkladné posouzení výkonnosti sítě a testování zařízení tím, že simuluje stovky protokolů přes tisíce koncových bodů sítě. Tento nástroj obsahuje již předem definované testovací skripty na testovaní konkrétních služeb např. IPTV,VoIP,VoD. Praktické provedení a použití je popsáno dále v praktické části, konkrétně v části Simulace v domácí síti. [3]

ScriptGen a WishConsole

Jedná se o dva programy používající předchozí zmíněný skriptovací jazyk. ScriptGen i WishConsole jsou součástí programového balíku IxOS. Při definování testu lze použít grafické rozhraní a za pomocí kurzoru vše jednoduše ručně nastavit. Tohle vše může být urychleno díky programu ScriptGen, který všechny jednotlivé kroky, které jsme zadávali ručně, sjednotí do jednoho výstupního skriptu v jazyce TCL. A pro jeho následné spuštění se použije konzole WishConsole. Jelikož jsou některé testy kvůli složitosti zdlouhavé na ruční zadávání, je použití skriptu pro uživatele mnohem rychlejší a pohodlnější. [2]

TCL

Výše zmíněné programy využívají jazyka Tcl z anglického znění Tool Command Language, který patří do rodiny skriptovacích jazyků. Tento jazyk byl vytvořen koncem roku 1987 panem Johnem Ousterhoutanem. Jedná se o jazyk, který je využíván díky jednoduchosti, rozšiřitelnosti a snadné implementaci do různých aplikací. Je zajímavostí, že přepínače a směrovače firmy Cisco využívají právě tento jazyk pro vlastní konfiguraci. Pro spuštění skriptu v rozhraní přes konzoli WishConsole je nutné znát základní příkazy. Pro úplnost je na konci podkapitoly poskytnut odkaz, kde se nachází podrobný návod pro práci s jazykem Tcl [4, 8].

2.2 Útoky typu DoS

V této části jsou popsány jednotlivé typy DoS útoků a jejich dělení. Základním principem a myšlenkou těchto útoků je snaha o znepřístupnění určité služby, zařízení, či sítě. Důvodem těchto útoků může být pomsta, vyjádření nesouhlasu či likvidace svých konkurentů. Provedení takového útoku je trestný čin, proto doporučujeme aby čtenáři nebrali tuto práci

jako návod k provedení útoku. Všechny testy a simulace v rámci této práce byly provedeny v laboratorním prostředí školy pod odborným vedením. Ovšem pokud si čtenář bude chtít vyzkoušet nějaké útoky, měl by se pohybovat na úrovni domácí privátní sítě nikoliv na úrovni veřejné sítě. Existuje hodně pramenů o tom jak se dělí DoS útoky a různě se prolínají nebo odporují. Bylo proto vybráno takové dělení, které je snadno pochopitelné a čtenář by si mohl díky tomu udělat lepší představu o dané problematice.

Následující dělení DoS útoků zohledňuje ty nejzákladnější běžně zmiňované parametry:

1. podle způsobu provedení:

- lokální: k provedení útoku je potřeba přístup na počítač, na který se provede útok,
- vzdálený: útok prováděn vzdáleně,

2. podle počtu útočících počítačů:

- distribuované útoky na kterém se podílí více počítačů z anglické Distributed Denail of service(DDoS),
- útoky prováděné jedním počítačem,

3. další dělení

- Flood DoS útoky,
- DoS útoky využívající chyb a vyčerpání systémových prostředků,
- DoS využívající Man in the middle útoky (Mitm),
- distribuované DoS útoky (DDoS),
- odrážející a zesilující DoS útoky.

V dalším textu je uveden detailnější popis některých z vyjmenovaných typů útoků a jejich konkrétní příklady.

2.2.1 Záplavové DoS útoky (DoS Flood)

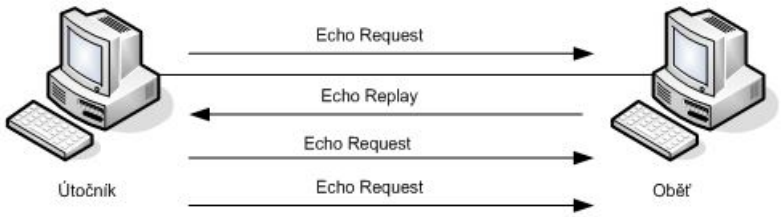
Jedná se o jeden z principiálně nejjednodušších útoků, který se stále dodnes používá. Fungují na základě vygenerování enormního datového toku, který zahltí linku počítače, což znemožní provoz. Obrana proti takovým útokům je velice těžká, pokud se jedná o distribuovaný útok.

Existuje mnoho typů DoS flood útoků, v dalším textu jsou popsány jednotlivé typy záplavových DoS útoků:

ICMP Flood:

Internet Control Message Protokol (ICMP) je součástí protokolové sady TCP/IP, definované specifikací RFC 792. Během přenosu paketů v síti pomocí protokolu IP dochází k chybám a ICMP vzniklé chyby oznámí odesílateli, ale pakety už neopravuje, to přenechává vyšší vrstvě. ICMP zprávy mají stejné první tři pole. První pole označuje o jakou ICMP zprávu se právě jedná, druhé pole specifikuje kód pro konkrétní typ zprávy a ve třetím poli je kontrolní součet, který slouží pro ověření integrity dat. Existuje několik typů zpráv ICMP, pro účel tohoto útoku jsou nejdůležitější Echo Replay a Echo Request. ICMP flood spočívá v tom, že se oběti rychle posílají ICMP Echo pakety s maximální velikostí. Větší efektivity toho útoku je dosaženo změnou zdrojové adresy, tím je zajištěno zahlcení linky dvakrát.

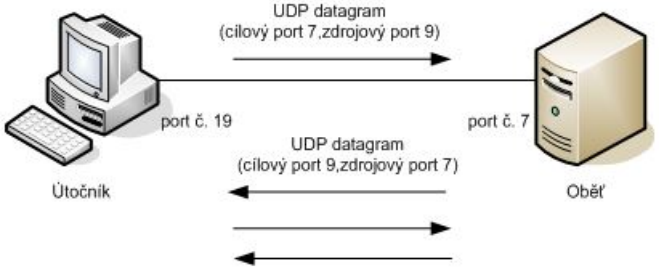
Jedná se obyčejný záplavový útok s poměrně lehkou realizací, který používá protokolu ICMP, nejčastěji jsou to pakety typu ICMP Echo (pakety využívající ping, sloužící k zjišťování dostupnosti počítače). Maximální velikost paketů by měla být 548B, ovšem operační systémy Linux umožňují definování velikosti až 65kB. Útočník posílá zprávu ICMP Request a cílový počítač odpovídá zprávou ICMP Replay. Poté změnou adresy odesílatele se linka napadeného počítače zahltí dvakrát. Linuxové systémy umožňují pomocí přepínače -f nastavit co nejrychlejší posílání paketů. Po každém odeslání ICMP Request se objeví na konzoli tečka a po každém přijatém ICMP Replay se tečka vymaže, což nám umožňuje sledovat, zda napadený počítač stíhá odpovídat nebo ne. Pokud napadený počítač nestíhá odpovídat, útok je úspěšný. Nevýhodou tohoto útoku je, že ICMP Echo pakety bývají filtrovány.



Obr. 2: Princip ICMP flood

UDP Flood:

UDP flood útok využívá protokolu User Datagram Prtokol (UDP) na 4.vrstvě OSI modelu, tedy transportní vrstvě. Na této vrstvě se kromě UDP nachází také protokol TCP. Hlavními rysy UDP na rozdíl od TCP je to, že UDP považován za nespolehlivý. Jelikož datagramy, které přenáší mezi počítači skrze síť, nemusí být doručeny do cíle a také nemusí být doručeny ve správném pořadí. Výhodou UDP je především jeho rychlost a jeho uplatnění najdeme především v aplikacích, které nevyžadují spolehlivost přenosu. Jak protokol UDP tak TCP používají pro rozlišení jednotlivých služeb, které běží na počítači, síťové porty. V našem případě nás budou zajímat porty č. 7 a č. 19. Na prvním zmíněném portu je ECHO protokol. Pro pochopení jak funguje tento protokol, je dále uveden příklad. Nechť probíhá komunikace mezi serverem a klientem. Pokud klient pošle data na serverový ECHO port, budou mu poslána bez jakýchkoliv úprav zpět. Na portu č. 19 je protokol CHARGEN. Tento protokol přijme doručená, ale zpět odesílateli posílá náhodná data. Opět se jedná o obyčejný záplavový útok využívající zacyklení pomocí služeb ECHO a CHARGEN. Obě služby jsou často ve výchozím nastavení spuštěny na systémech typu Linux u Windows tomu tak není. Nevýhodou je to, že tyto služby se už nepoužívají.



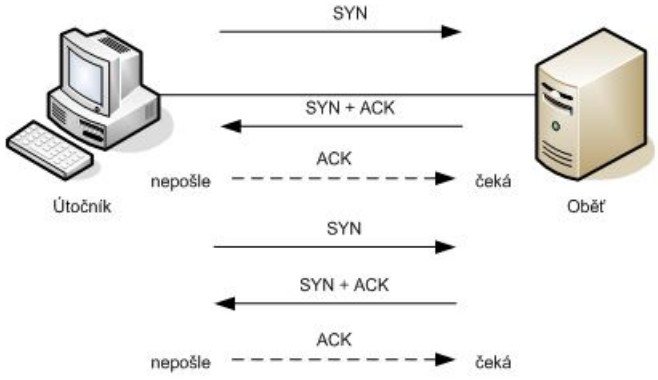
Obr. 3: Princip UDP flood

TCP Flood:

Potřebná teorie k proniknutí do tohoto typu útoku je založena na pochopení základních vlastností protokolu TCP. Jedná se o protokol pracující na transportní vrstvě a narozdíl od UDP je více používanější. Existuje více označení pro tento typ útoku například: SYN Flood, ACK Flood, RST Flood (sloužící k resetování spojení), FIN Flood, URG Flood, PSH Flood atd. V praxi jde o tentýž útok a liší se pouze tím, jak jsou nastaveny TCP pakety.

Primárním úkolem tohoto protokolu je navázání komunikace dvou služeb či aplikací na různých zařízeních. Při navázání komunikace dojde k vytvoření virtuálního okruhu, který je duplexní a dojde k přenosu dat. Protokol TCP stejně jako UDP používají pro rozlišení jednotlivých služeb, které běží na počítači, síťové porty v rozsahu od 0 do 65535.

TCP protokol se uplatňuje téměř pro všechny webové služby. Aby došlo k navázaní komunikace musí proběhnout TCP Handshake, někdy označován jako three-way handshake. V doslovném překladu se jedná o potřesení rukou a jedná se o způsob, který se požívá v TCP protokolu k navázaní komunikace. V následující příkladu je vysvětleno, jak TCP Handshake funguje. Počítač(PC) připojený k Internetu chce komunikovat s webovým serverem. PC pošle serveru inicializační paket s příznakem SYN, pokud server tento paket nebude chtít přijmout, tak ho ignoruje nebo pošle zpět PC paket s příkazem RST(z angl. reset). Ale v případě, že by server souhlasil s realizací komunikace, přijme inicializační paket a pošle PC paket s příznakem SYN+ACK(z angl. acknowledge). PC po přijmutí tohoto paketu pošle serveru paket s příznakem ACK , čímž sdělí serveru, že navázaní komunikace proběhlo v pořádku a nyní může probíhat komunikace mezi serverem a klientem(PC). Útok využívá metodiky serveru při obsluze klientů, která spočívá v opětovném vyslání paketu SYN+ACK a podržení daného spojení pro daného klienta při neobdržení paketu s příznakem ACK. Tím, že budeme generovat velké množství paketů s příznakem SYN, dojde k vyčerpání všech možných spojení s klienty a dojde k odstavení serveru pro ostatní, což je cílem útoku.Pro detailnější vědomosti o TCP Handshake jsou informace dostupé z: http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000.



Obr. 4: Princip TCP flood

Mass mailing list:

Jedná se o nejlehčí útok ze všech zmiňovaných. Cílem je snaha zahltit konkrétní e-mailovou schránku tak, aby už nepřijímala další potenciálně důležité zprávy. Kvůli malé kapacitě schránek byla realizace útoku v minulosti velice snadná. Dnes jsou kapacity sice větší, ale pokud dojde k zahlcení schránky tisíci emaily denně, nastane stav nepoužitelnosti také. Největší výhodou je nemožnost vystopovat útočníka.

E-mail bombs:

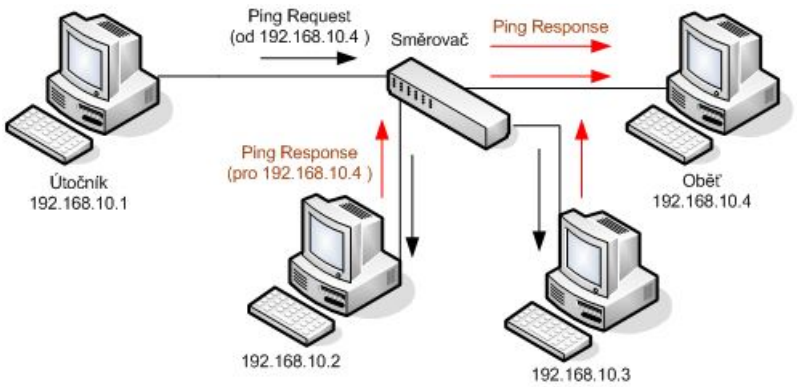
Je typ útoku obdobný k předchozímu s rozdílem, že se k tvorbě e-mailů používá program, nejčastěji psaný v jazyce C, C++ či Python. Cílem tohoto útoku je zhroucení vytypovaného poštovního serveru namísto znemožnění funkce jednotlivé schránky. Tento útok je efektivní, pokud je distribuovaný. Útočník si emaily sám generuje a posílá je na konkrétní adresu. Dalším typem DoS útoků, jsou útoky využívající vyčerpání systémových prostředků. Jde o útoky využívající chyb systému, které jsou způsobené především jejich špatným navržením. Tyto chyby mohou způsobit větší zátěž na procesoru nebo paměti. K útoku je zde potřeba většího datového toku a rychlosti připojení. Princip je založen na tom, útočník pošle velké množství paketů, procesor napadeného zařízení se přetíží a nestíhá reagovat a nastává režim nepoužitelnosti.

2.2.2 DoS útoky odrážejícího a zesilujícího typu

Ze všech vyjmenovaných typů útoků se jedná o nejmodernější typ, i když první zmínky prvních reflektivních útoku jsou z roku 1998. Jedná se typ útoků, který se provádí převážně ve velkém počtu tedy distribuovaně. Princip odrážejících nebo reflektujících útoků spočívá v zahlcení linky oběti. K zahlcení používá útočník jiné počítače nebo směrovače jako prostředníky. Útočník nemusí napadnout či poškodit prostředníky, ale využívá jejich služeb. Princip spočívá v tom, že poslaná data představující útok, neprochází jednou cestou, jelikož se při útoku mění počítače nebo směrovače, od kterých se útok odráží až dojde k oběti. Šance dohledat útočníka je v tomto případě téměř nulová, jelikož útočník používá zfalšovanou IP adresu.
Princip zesilujících útoků spočívá v tom, že se oběti pošle balík dat o nějaké velikosti, ale oběti dorazí balík dat o větší velikosti. Aby se balík dat zvětšil je nutná pomoc prostředníků.

Smurf:

Jedná se o útok zesilujícího záplavového reflektivního typu. Teoreticky se jedná o stejný útok jako je ICMP Flood jen s tím, že je tam navíc zesílení datové toku, které je specifické pro zesilující útoky. Toto zesílení je závislé na počtu počítačů v síti ve které je oběť. Princip spočívá v tom, že útočník pošle ping na IP adresu sítě s nastavením zdrojové IP adresy na IP adresu dané oběti. Tímto všechny počítače odpoví oběti "ICMP Echo Replay"paketem. Podobným útokem je Fraggle, který ale používá místo protokolu ICMP protokol UDP.



Obr. 5: Princip Smurf

TTL Expiration flood:

Pro pochopení principu tohoto záplavového odrážejícího útoku je nutné si uvědomit, co znamená TTL u IP protokolu. Z anglického Time to live, se jedná o hodnotu, kterou nastavuje operační systém pro veškerá odchozí data, která z počítače odcházejí do sítě. Hodnota TTL je primárně nastavená mezi hodnotami 64 a 255. Každým průchodem přes směrovač nebo jiné zařízení pracující s protokolem IP, je hodnota TTL snížena o 1. Jakmile data dosáhnou hodnoty TTL 0, data se zahodí a odesílateli pošle zařízení, že vypršel TTL. Důvodem je to, aby v sítí nekolovala do nekonečna ztracená data. Důležité je si uvědomit, že ne všechny zařízení zprávu o vypršení TTL posílají, často jsou filtrovány firewallem. Princip útoku je v nastavení IP adresy odesílatele se nastaví IP adresa oběti, nastaví se malé TTL a data se posílají náhodnému cíli. Hodnota TTL vzápětí vyprší a oběti přijde zpráva, že TTL vypršel. Zesílení tohoto útoku je minimální, ale jedná se o útok, který je snadno aplikovatelný.

Domain Name Server (DNS) amplification attack:

Pro pochopení principu tohoto útoku je nutné zadefinovat funkci DNS serveru. Jedná se o server, který má uloženou databázi jmen a ke každému jménu má přiřazenou IP adresu. Když se DNS serveru pošle dotaz na nějakou webovou stránku, odpoví zpět IP adresou. Principem toho záplavového reflektivního útoku s velkým zesílením, je posílání DNS dotazů se zdrojovou IP adresou oběti na DNS server umístěný někde v Internetu a je dostupný pro všechny. Běžné DNS servery využívají UDP a TCP protokoly. Pokud se používá protokol UDP, odpovědi z DNS serveru mohou dosáhnout objemu 512 B. Průměrná velikost odpovědi je 80 B, což znamená, že útočník může dosáhnout téměř sedmínásobného zesílení. Ještě většího zesílení se dosáhne při použití rozšířených DNS serverů (EDNS), protože jejich odpovědi mohou být větší než 4 KB. Otázkou je, jakou položit otázku, aby server odpověděl zprávou o maximální velikosti? Útočníci si koupí nebo se nabourají do domény a vloží do ní dlouhý textový záznam, sloužící jako komentář. Poté vytvoří seznam veřejných DNS serverů, které budou používat. Útok se provede tak, že útočník pošle všem DNS serverům ze seznamu dotazy na doménu, která je upravená o textové záznamy a jako IP adresu odesílatele nastaví adresu oběti. DNS servery vzápětí začnou posílat odpovědi a tím se oběti zahltí linka. Podle dostupných informací se jedná o jeden z velmi nebezpečných útoků.

2.2.3 DoS útoky využívající vyčerpání systémových prostředků

SYN Flood:

Útok spočívá v chybné prvotní implementaci spojení TCP Handshake. Útočník, v této situaci klient, posílá serveru příznak SYN k navázání komunikace a server mu nazpět odešle SYN + ACK a server čeká na ACK od útočníka. V síti se pakety často ztrácejí a server čekající na odpověď si usmyslí, že paket nebyl doručen a pošle znovu příznak SYN + ACK. Po určité době pokud nepřijde serveru příznak ACK, tak vymaže toto spojení. Problém nastává ve chvíli, kdy útočník pošle více příkazů SYN a vyčerpá serveru všechna možná spojení s klienty, což způsobí odstavení serveru pro jiné klienty. Příznak SYN má pouhých 42 bytů a proto nezáleží na rychlosti spojení a je možnost zfalšovat IP adresy. Jako ochrany před tímto útokem může být využito snížení doby čekání na odpověď serveru. Jde o podobný typ útoku jako u útoků využívajících chyb implementace, které jsou způsobené špatným navržením. Tyto chyby mohou způsobit větší zátěž na procesoru nebo na paměti a k útoku je zde potřeba většího datového toku a rychlost připojení zde také hraje roli. Princip je v tom, že útočník pošle velké množství paketů, procesor napadlého zařízení se přetíží a nestíhá reagovat a nastane režim nepoužitelnosti.

RPC Named Pipes:

Jedná se o nepříliš známý typ útoku. Využívá chyb Remote Procedure Call (systém Win NT bez SP4). Dnes je téměř nefukční.

Stream a Raped:

Jsou to navzájem podobné útoky. Není o nich moc zmínek, pouze informace z irelevantních zdrojů. Některé zdroje uvádějí, že jejich princip spočívá ve špatném zpracování poškozených paketů některých OS, což následně způsobí nežádoucí zatížení procesorové jednotky (CPU).

Land attacks (Banana attacks):

Existuje hodně variant těchto útoků. Princip spočívá v posílání zfalšovaných paketů (zdrojová a cílová IP jsou cíle) a dosáhnou zacyklení a zhroucení systému. Jako řešení se zde nabízí využití firewallu.

Fork bomb:

Jedná se o lokální DoS útok. Využívají programy, které mnohokrát spustí samy sebe. Způsobí vyčerpání či zatížení systému a je sto procentně účinný. Praktická ukázka dostupná z `http://www.youtube.com/watch?v=U7jc70zm2X8` nebo pro linuxové systémy dostupná z `http://www.youtube.com/watch?v=Q9Mdy7H8Qmc`.

Netkill:

Využívá vyčerpání operační paměti a tím dojde ke zmrazení cíle. Jedná se o podobný útok typu SYN Flood s tím rozdílem, že dojde k úplnému navázání spojení.

Ping of death:

Využívá ICMP Echo Request paketu (max. velikost 65.535 bytů). Útočníci danou velikost nedodrželi a proto některé OS zkolabovaly. Útočníci využili toho, že pakety takové velikosti se musí fragmentovat a každému dílčímu paketu se přidává informace o fragment offsetu, která umožní přidat další data do paketu. Důvodem zhroucení bylo to, že byla překročená paměť, která byla určená pro přečtení paketu. Dnes je tento útok zcela zablokován.

Teardrop:

Je útok obdobný Ping od death. Spočívá v posílání fragmentovaných IP paketů, které se překrývají. Pošlou se dva fragmenty tak, že druhý přepíše kus prvního. Využívá špatné implementace sestavování IP datagramu, jedná se o chybu OS.

2.2.4 DoS útoky typu Man in the Middle (Mitm)

Mitm je typ útoků, kdy útočník přesměruje všechen síťový provoz přes sebe a může kontrolovat provoz. Oběť přitom nemusí vědět, že je útočník v síti a odposlouchává síťový tok. Pokud se oběť připojí na elektronické bankovnictví nebo se přihlásí na e-mailový účet či

na účet sociální sítě, útočník může citlivé informace jako je uživatelské jméno a heslo zneužít. Další typy Mitm jsou ARP Cache poisoning, DHCP Spoofing, ICMP Redirecting, Port stealing, DNS Spoofing.

2.2.5 Distribuované DoS útok (DDoS)

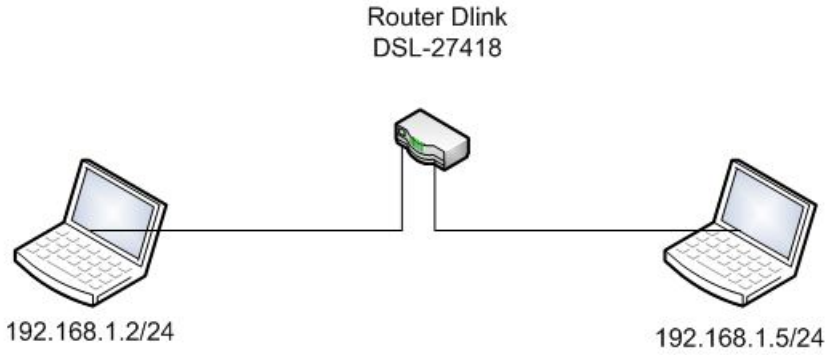
DDoS útoky se liší od klasických DoS útokům tím, že se na nich podílí větší množství uživatelů. Prakticky se jedná o různé typy DoS útoků například záplavového typu jen s tím,že je prováděn více uživateli ve stejnou dobu. K takovému útoku se často používají napadené počítače, které se nazývají "zombie". Tyto počítače má útočník pod kontrolou a vlastník o tom nemusí vědět.

Informace obsažené v celé kapitole Útoky typu DoS jsou čerpány ze stejných zdrojů. [5] [6]

3 Praktická část

3.1 Ukázka simulace zařízení v domácí síti

Následující kapitola slouží jako motivace a ukázka prostředí, pro které byly vytvořeny test. skripty, resp. scénáře. K tomuto účelu posloužil program IxChariot verze 6.7, který slouží pro simulaci činnosti zařízení IXIA 400T. V rámci této části bylo vyzkoušeno spuštění skriptů, které jsou již nadefinované výrobcem. Výhodou programu IxChariot je to, že po nainstalování do kteréhokoliv počítače, tak ho přemění v zařízení, které disponuje některými základními funkcemi jako 400T.
Testovaná topologie se skládá ze dvou počítačů a jednoho směrovače, pro jejich propojení byly použity standardní UTP kabely s délkou 2 m. Na obou počítačích byl spuštěn OS Microsoft Windows 7 Home Premium. Na prvním počítači (PC1) byl nainstalován IxChariot 6.7, ze kterého byly testy spuštěny. Na druhém počítači (PC2) byl nainstalován v pozadí běžící IxChariot Enpoint, který simuloval koncové zařízení.[9] Příkazem ping byla před samotným testováním ověřena funkčnost propojení mezi PC1 a PC2.

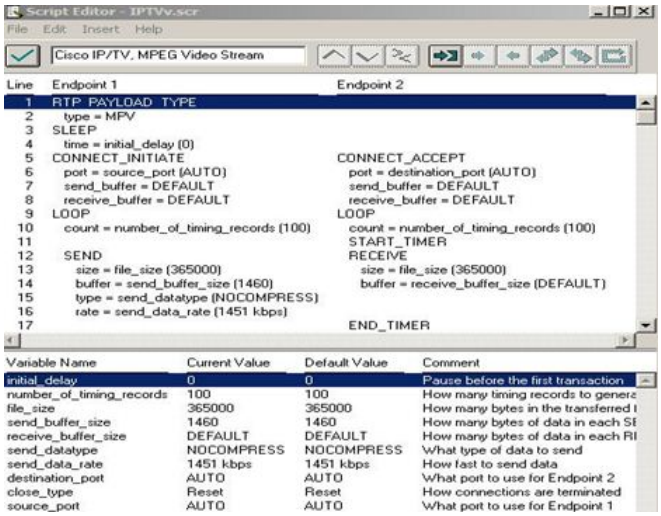


Obr. 6: Topologie domácí sítě

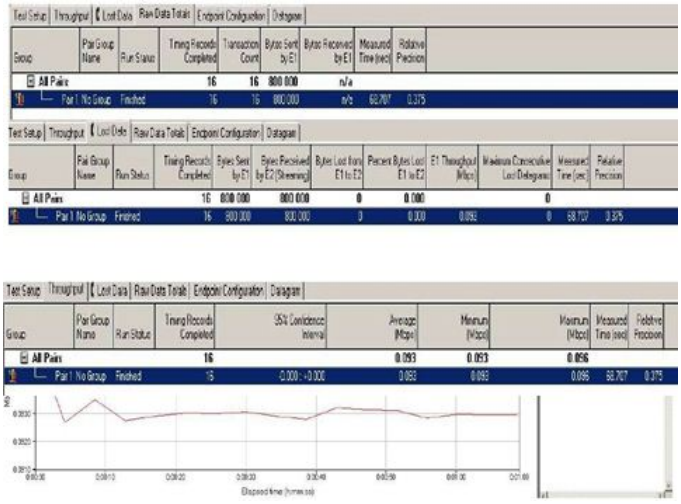
Software od firmy IXIA podporuje řadu předdefinovaných testů sloužících pro testování provozu sítě až po jejich monitorování. Tyto testy jsou určeny především pro testováním velkých sítí, takže v rámci seznámení s ovládáním tohoto programu bylo provedeno pár testů, které pomohly s orientací v tomto prostředí. Pro účel této práce byl vybrán test IPTV Testing.

3.1.1 IPTV Testing

Jedná se o testování pomocí protokolu IPTV, který podporuje jak vysílání "live", tak i Video on Demand (VoD), což je systém umožňující uživatelům sledovat videa podle své volby. Účastníci IPTV potřebují připojení k set-top boxu. Videa jsou většinou komprimována do formátu MPEG-2, nebo MPEG-4 a live vysílání je ve formátu IMGP. Pro samotné testování je potřeba vytvoření minimálně jedné skupiny příjemců a každá z nich musí obsahovat alespoň jednoho účastníka. Použitím testovacího skriptu IPTVa.src byl emulován přenos typu multicast a přijímání IPTV videa. Nejprve bylo v testovacím skriptu nastaveno, jak velká data budou přenášená. Výchozí hodnota byla změněna na 50 kB, dále je zde také možnost nastavení rychlosti, kterou budou jednotlivé pakety vysílány. Z výsledků jde vidět, že množství přenesených dat je 800 kB, což odpovídá 16 přenosům po 50 kB. Propustnost byla velmi malá, vlivem nastavení nízké přenosové rychlosti. Zároveň nedošlo k žádné ztrátě dat, důvodem by mohlo být to, že se jedná o malou uzavřenou síť.



Obr. 7: Ukázka nastavení parametrů testovacího skriptu



Obr. 8: Výsledek testovaní IPTVa.src

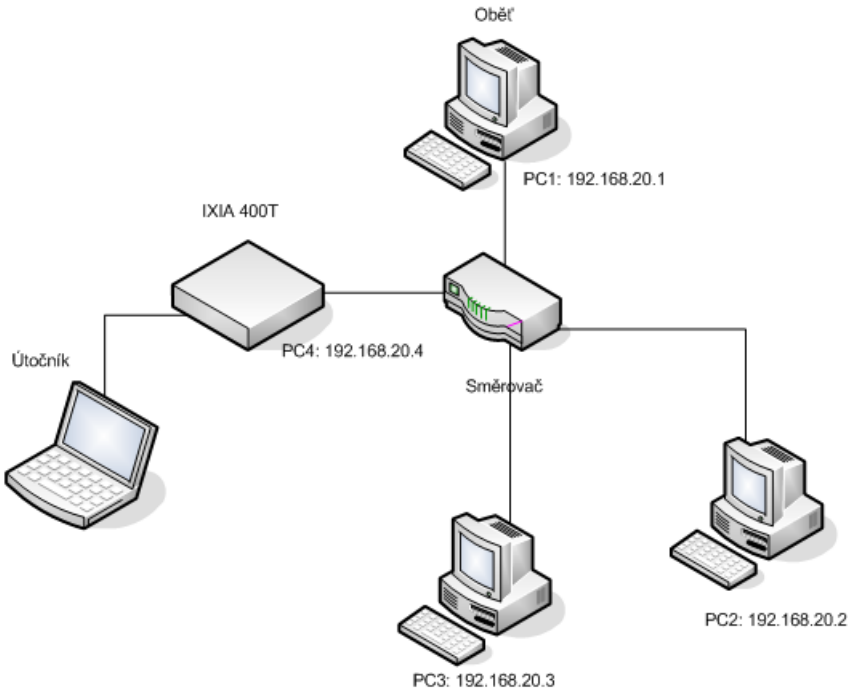
3.2 Realizace testovacích scénářů

V této části je popsána provedená simulace tří typů DoS útoků a to UDP, ICMP a SYN flood. Pro všechny zmíněné útoky byla uvedena stejná topologie sítě, protože jde především o vyzkoušení provedení testovacího útoku za pomocí zařízení IXIA 400T. Veškeré definice a nastavení parametrů pro jednotlivé typy útoků byly provedeny v programu IxExplorer, který je součástí IxOS. Program IxExplorer také umožňuje nahlédnout do paketů generovaného toku dat, což posloužilo jako kontrola toho, zda vyslané pakety odpovídají jejich dříve provedené definici. Hlavními cíli této praktické části je realizovat zmíněné útoky a zjistit, zda byly úspěšné. Testovací scénáře byly provedeny v rámci sítě LAN v laboratorních podmínkách školy a pod odborným dohledem.

3.2.1 Topologie sítě

Jedná se o jednoduchou topologii typu hvězda. V centru sítě byl umístěn přepínač a do něj byly zapojeny pomocí UTP kabelů tři osobní počítače a zařízení IXIA 400T, které je ovládané

útočníkem. Na PC1 nainstalován protokolový analyzátor Wireshark, který nám umožní na sledovat pakety, které jsou v síti, a detailněji je zkoumat. Zmíněná topologie je uvedena na Obr. 9.



Obr. 9: Topologie sítě

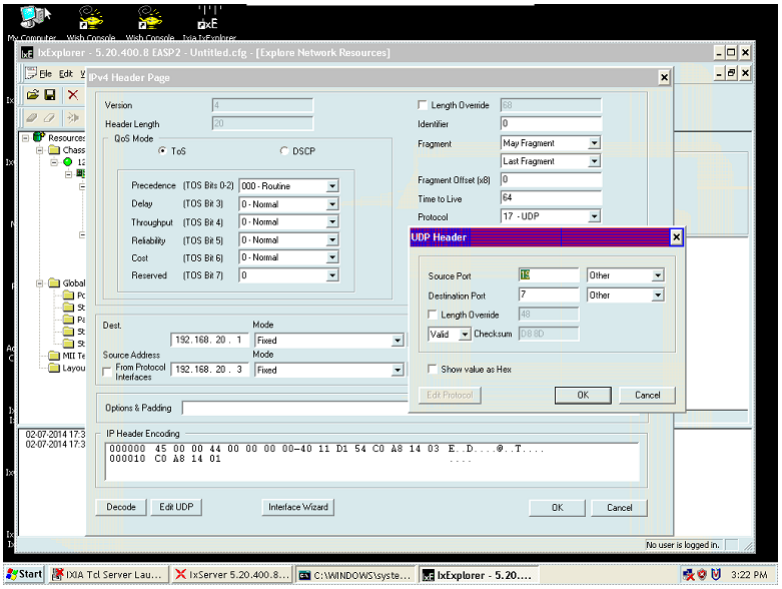
3.2.2 UDP flood

Při simulování tohoto typu útoku byly v rámci UDP využity porty č.7 a č.19. Před samotným provedením útoku, je potřeba znát počet uživatelů a jejich IP adresy v rámci sítě, ve které bude prováděno testování. Za pomocí programů jako je Free IP Scanner, Wireless Network Watcher je možné tyto informace snadno a rychle získat. Důležité je uvědomit si, že u systému rodiny Windows jsou služby ECHO a CHARGEN ve výchozím stavu vypnuté a u Linuxu je to naopak. Pro tento test není potřebné tyto služby zapínat, jelikož je třeba hlavně zachytit datový tok, který bude generován z IXIA 400T.

Princip tohoto útoku spočívá v tom, že útočník pošle datagram na ECHO port oběti s tím, že v datagramu bude zdrojová IP adresa jiné počítače než útočníkova a zdrojový port bude nastaven na 19 a dojde k zacyklení mezi počítači.

V programu IxExplorer byly nastaveny potřebné parametry, aby bylo možno provést UDP flood. Byl nadefinován nový datový tok s názvem "udp"a nastaven protokol IPv4, konkrétně ICMP/IP. Poté byla v konfigurační části nastavena cílová IP adresa oběti, v tomto případě to byl PC1 s IP adresou 192.168.20.1 a jako zdrojová adresa byla nastavena jedna ze zařízení v síti. Zvolili jsme PC3 s IP adresou 192.168.20.3.

Dále bylo nutné také nastavit, aby porty byly posílány z konkrétního portu na port, který byl vyžíván. Cílový port byl nastaven na 7, tedy na ECHO port na zařízení oběti tedy PC1. Zdrojový port bude port č. 19 a bude nastaven na PC3. Je také možné nastavit MAC adresu jak u zdroje, tak u cíle, ale jelikož v jedné síti nemohou být(přesněji to není doporučeno) dvě stejné MAC adresy, nebude tento krok prováděn. Veškerá nastavení v grafickém rozhraní programu IxExplorer byla zaznamenána na Obr. 10 a náhled do jednotlivých datagramů v Packet View je zobrazen na Obr. 14 .



Obr. 10: Nastavení UPD flood

3.2.3 ICMP flood

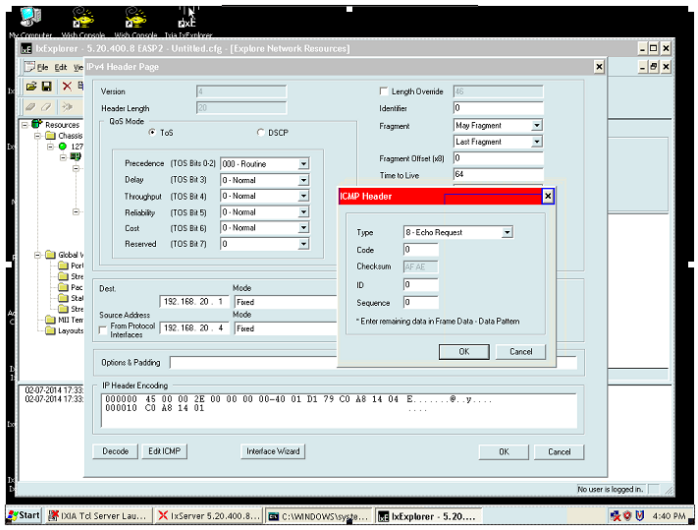
Jelikož veškerý generovaný datový tok bude procházet přes přepínač, je nutné pro účel této práce nastavit firewall tak, aby tento tok prošel. V reálném provozu jsou ICMP Echo pakety filtrovány. Při provádění samotného útoku byl za prvé v prostředí programu IxExplorer nadefinován nový datový tok s názvem "ICMP". Cílem útoku bylo zařízení PC1. V nastavení byl vybrán protokol IPv4, konkrétně protokol ICMP/IP a v konfigurační části byla nastavena jako cílová IP adresa adresa zařízení PC1, tedy 192.168.20.1. Zdrojová IP adresa nyní byla adresa zařízení IXIA 400T. Pokud by měl být útok anonymního charakteru, byla by nastavena zdrojová adresa PC2, či PC3. Zařízení IXIA umožňuje nastavit velikost ICMP paketu od 64 B do 1518 B. Byla nastavena maximální kapacita. Dalším potřebným nastavením bylo vyplnění ICMP hlavičky. Zde bylo nadefinováno, že náš generovaný datový tok bude obsahovat ICMP pakety typu ICMP Request. Veškerá nastavení v grafickém rozhraní programu IxExplorer byla zaznamenána na Obr. 11 a náhled do jednotlivých datagramů v Packet View je zobrazen na Obr. 16

3.2.4 SYN flood

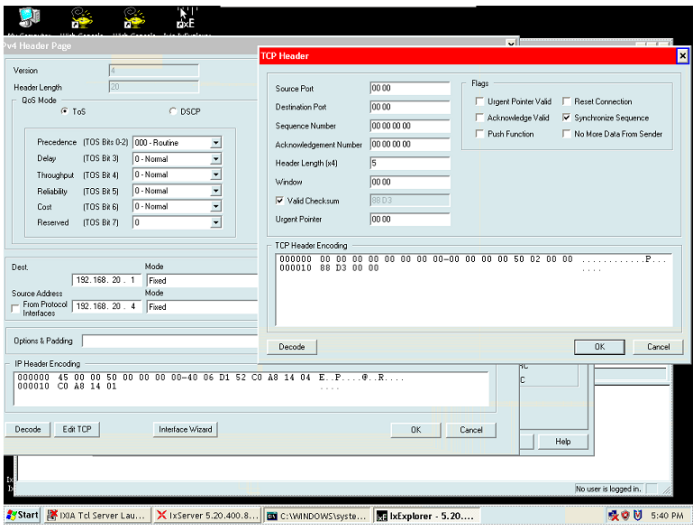
V prostředí IxExplorer byl opět vybrán protokol IPv4, přesněji TCP/IP. V konfigurační části byla nastavena zdrojová IP adresa IXIA 400T, tedy 192.168.20.4 a cílová IP adresa webového serveru 192.168.20.1. Bylo také nutné nastavit, že generovaný tok bude obsahovat jen pakety s příznakem SYN. Veškerá nastavení opět v grafickém rozhraní programu IxExplorer byla zaznamenána na Obr. **??** a náhled do jednotlivých datagramů v Packet View je zobrazen na Obr. 14

3.2.5 Výsledek realizace testovacích scénářů

Datový tok byl generován po dobu jedné minuty a za pomocí analyzátoru Wireshark byl zachycen objem dat ve výši 976 MB. Výsledný výstupní .pcap soubor je uložen v příloze ve formě DVD. Na Obr. 15, Obr. 17, Obr. 19 je možno vidět podrobné informace odchycené komunikace, tedy datového toku, které byly postupně generovány. Z těchto obrázků je také zřejmé to, že nadefinované parametry byly zachovány. Protokoly souhlasí, zdrojové a cílové



Obr. 11: Nastavení ICMP flood



Obr. 12: Nastavení SYN flood

IP adresy a porty jsou správně. Na základě těchto informací lze tvrdit, že všechny testovací scénáře byly realizovány správně a jejich funkce odpovídají předpokladům.

3.3 Vytvoření testovacích skriptů

Jednotlivé testy, které mohou být prováděny IXIA 400T je možné provádět pomocí IxExplorer nebo WishConsole. Doposud byla veškerá činnost prováděna v grafickém rozhraní IxExplorer, nyní však bude využíváno zadávání příkazů do konzole. Práce v ní je pro obsluhu pohodlnější a rychlejší, ale je potřeba mít jisté zkušenosti s jazykem Tcl, v IxExplorer toto není potřeba, protože se jedná o grafické rozhraní. Dále je popsáno vygenerování a spouštění skriptů.

Bylo využito již nadefinovaných útoků z předchozí kapitoly, ze kterých byly za pomocí programu Scriptgen vygenerovány skripty v jazyce Tcl. Do těchto vygenerovaných skriptů lze jednoduše nahlédnout a zasáhnout, jelikož se jedná o obyčejné textové soubory.

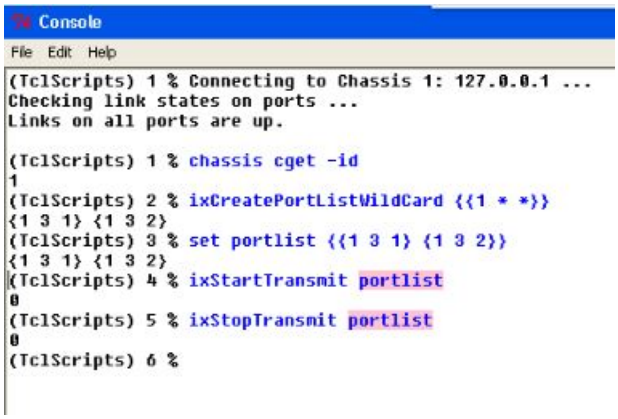
Ke spouštění těchto skriptů byla využita již zmíněná konzole ve verzi 5.200.400. Samotný proces spouštění skriptů lze stručně shrnout následovně. Nejprve je potřeba vygenerovaný skript do konzole načíst, poté nadefinovat na jakém portu bude spuštěn a v závěru pak pomocí příkazů skript spustit či zastavit.

Přehled základních příkazů ve WishConsole:

- chassis cget -id - zjištění ID chassis,
- ixCreatePortListWildCard - výpis všech dostupných portů chassis,
- set portlist - nadefinování portů,
- ixStartTransmit portlist - zapnutí generování datového toku,
- ixStopTransmit portlis- vypnutí generování datového toku. [8]

Podrobnější přehled všech příkazů ve WishConsole naleznete v příručce Tcl Development Guide.[8]

Pro ověření, zda skripty vykonávají očekávanou činnost, byla provedena v naší topologii realizace tří typu DoS útoků za pomocí konzole WishConsole. Skripty a záznamy zrealizovaných útoků najdete v příloze ve formě DVD.



Obr. 13: Práce ve WishConsole

3.3.1 Ověření správné funkčnosti portů

Během procesu vytváření skriptů se vyskytl problém se samotným spuštěním těchto skriptů. Jedna z prvních domněnek byla nesprávná funkčnost portů zařízení 400T. Byl proto proveden test, který vyhodnocoval správnou funkčnost portů zařízení. Jednotlivé kroky tohoto testu jsou uvedeny v dalším textu. Hlavní testovaní bylo prováděno pomocí softwaru IxExplorer.

Před samotným testováním portu 01 a portu 02, byly oba porty propojeny kříženým UTP kabelem.

Princip testu spočíval v tom, že byl z jednoho portu generován datový tok do druhého a obráceně. Cílem bylo ověřit, zda se oba porty chovají správně. Byl nadefinován datový tok a spuštěn proces generování. Snímek nadefinovaného datového toku je možno vidět na Obr. 8 a Obr. 28.

Test z portu 01 do portu 02 V okně Statistic View byly zaznamenány výsledky testování, např. kolik bajtů a rámců bylo přeneseno z portu 01 na port 02. Na níže uvedených obrázcích je možno vidět počet poslaných bajtů z portu 1 viz Obr. 27 a počet přijatých bajtů na portu 02 viz Obr. 24.

Test z portu 02 do portu 01 Jednalo se o prakticky identický postup, který již byl proveden v předchozím odstavci. Hodnoty přijatých Obr. 24 a odeslaných rámců Obr. 25 a bajtů se shodují. Podle těchto hodnot lze říci, že porty pracují správně.

V rámci této kapitoly byla ověřena správnost fyzického nastavení portů na zařízení IXIA 400T. Bylo využito návodu daného výrobcem.[7]

4 Vyhodnocení

V první části bakalářské uvedeny jak fyzické parametry, tak i programové vybavení zařízení IXIA 400T. Dále byla popsána problematika DoS útoků, jejich dělení, principy a vlastností.

Následující část byla zaměřena na praktické úkoly. Nejprve byla provedena simulace zařízení a vyzkoušení aplikace testovacího skriptu prostřednictvím simulačního programu IxChariot v rámci domácí sítě LAN.

Poté byly ve zvolené topologii sítě provedeny tři DoS útoky, a to UDP, ICMP a SYN flood. Ze záznamů síťového provozu lze říci, že realizace těchto útoků byla úspěšná.

Dále byly v rámci práce vytvořeny a spuštěny testovací skripty za pomocí programů IxExplorer, ScriptGen a WishConsole. Vygenerované skripty byly úspěšně spuštěny, což opět potvrzuje zobrazený záznam síťového provozu.

Na základě předchozích tvrzení lze shrnout, že všechny zadané úkoly byly úspěšně splněny.

Téma síťových útoků je kvůli jejich rostoucímu počtu velice aktuální. Práce čtenáři sděluje výstižným způsobem možnost otestování odolnosti jeho sítě vůči DoS útokům různých druhů. V budoucí navazující práci bych chtěl toto téma dále studovat, zejména testy odolnosti služby IP telefonie. Dále bych se chtěl zabývat metodami aktivní a pasivní obrany vůči těmto hrozbám.

Seznam použité literatury

[1] Ixia Deliver on: Product 400T. IXIA. IXIA - Deliver On [online]. Dostupné z http://www.ixiacom.com/products/display?skey=ch_400t [cit. 2014-02-06]

[2] IxExplorer Users Guide, Release 6.60 EA Patch1, 2013, dostupné z http://downloads.ixiacom.com/library/user_guides/IxOS/6.60_EA/EA_6.60_Rev_B/IxExplorer/IxExplorer.pdf [cit. 2014-02-06]

[3] IxChariot Getting Started Guide, Release 7.30, Rev. A, 2012, dostupné z http://downloads.ixiacom.com/library/user_guides/IxChariot/7.30SP1/EA_7.30_SP1/IxChariotGettingStarted.pdf

[4] Ogrocký A. a Uličný S.: Směrované a přepínané sítě: TCL skriptování pod prvky Cisco [online]. 2007, dostupné z: http://www.cs.vsb.cz/grygarek/SPS/projekty0607/TCL.pdf [cit. 2014-02-06]

[5] Haller M.: LUPA.CZ. [online], 2006, dostupné z: http://www.lupa.cz/serialy/utoky-typu-dos/#ic=serial-box&icc=more [cit. 2014-02-06]

[6] Ping D. a Abe S.: Detecting DoS attacks using packet size distribution . Bio-Inspired Models of Network, Information and Computing Systems, 2007. Bionetics 2007. 2nd. Tokyo, 2007, [cit. 2014-02-06]. 978-963-9799-05-9.

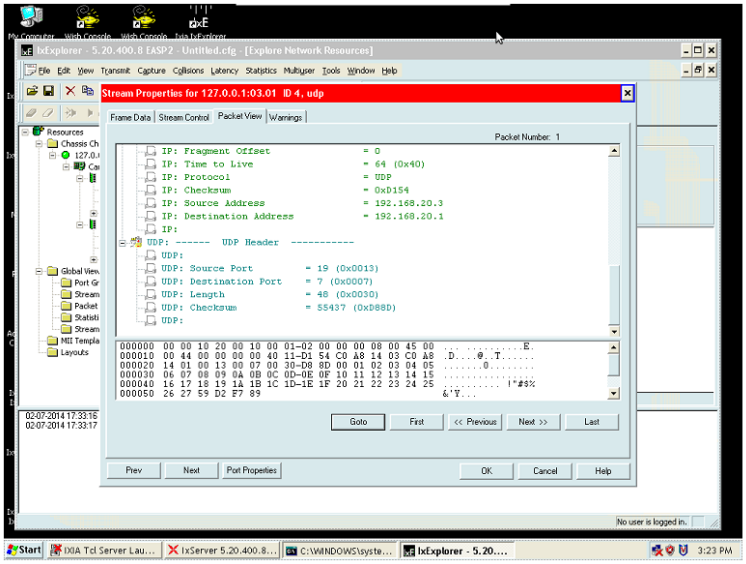
[7] Ixia Users Guide 6.60 EA,dostupné z http://downloads.ixiacom.com/library/user_guides/IxOS/6.60_EA/EA_6.60_Rev_B/GettingStartedGuide/index.html[cit. 2014-02-06]

[8] Ixia Tcl Development Guide 6.62 EA, dostupné z http://downloads.ixiacom.com/library/user_guides/IxOS/6.62_EA/EA_6.62_Rev_A/TclDevelopmentGuide/TclDevelopmentGuide.pdf[cit 2014-05-06]

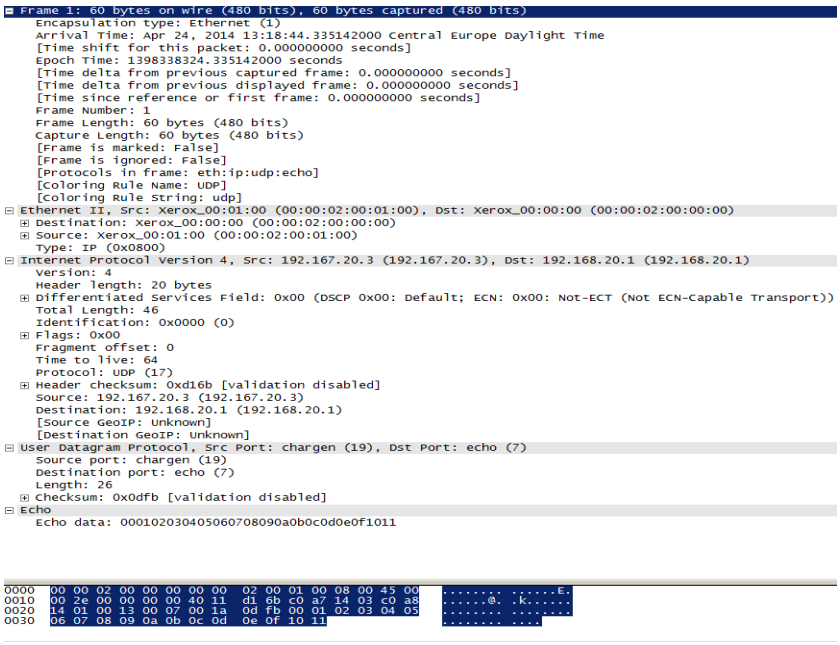
[9] Chariot Performance Endpoints 7.30 EA, dostupné z http://downloads.ixiacom.com/library/user_guides/IxChariot/7.30SP1/EA_7.30_SP1/ChariotPerformanceEndpoints.pdf[cit 2014-05-06]

[10] Getting Started Guide 6.62 EA, dostupné z http://downloads.ixiacom.com/library/user_guides/IxOS/6.62_EA/EA_6.62_Rev_A/GettingStartedGuide/GettingStartedGuide.pdf[cit 2014-05-06]

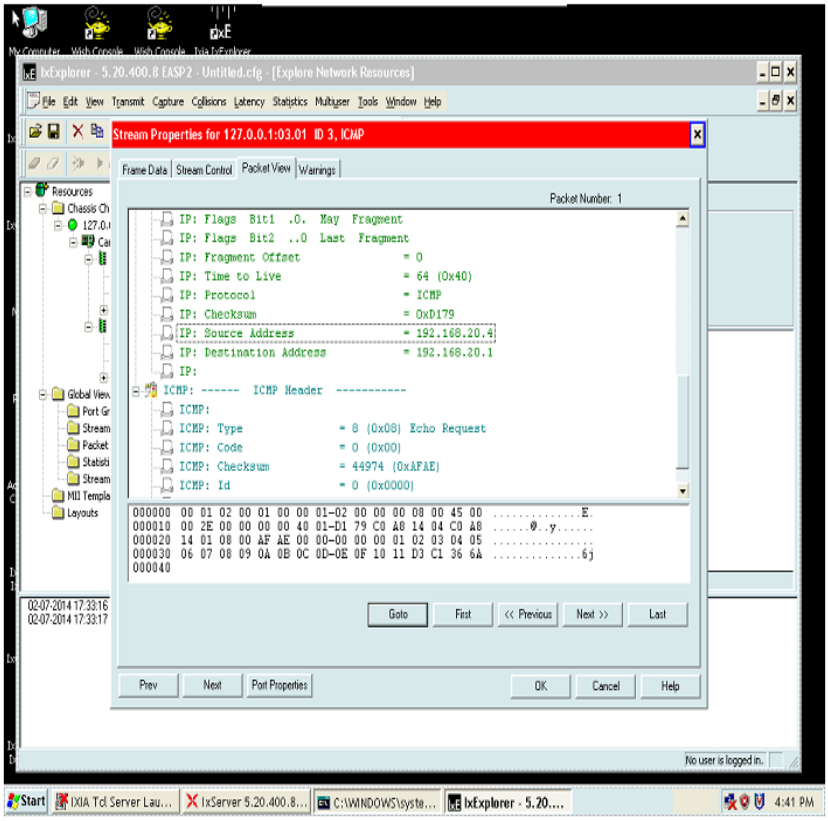
Přílohy



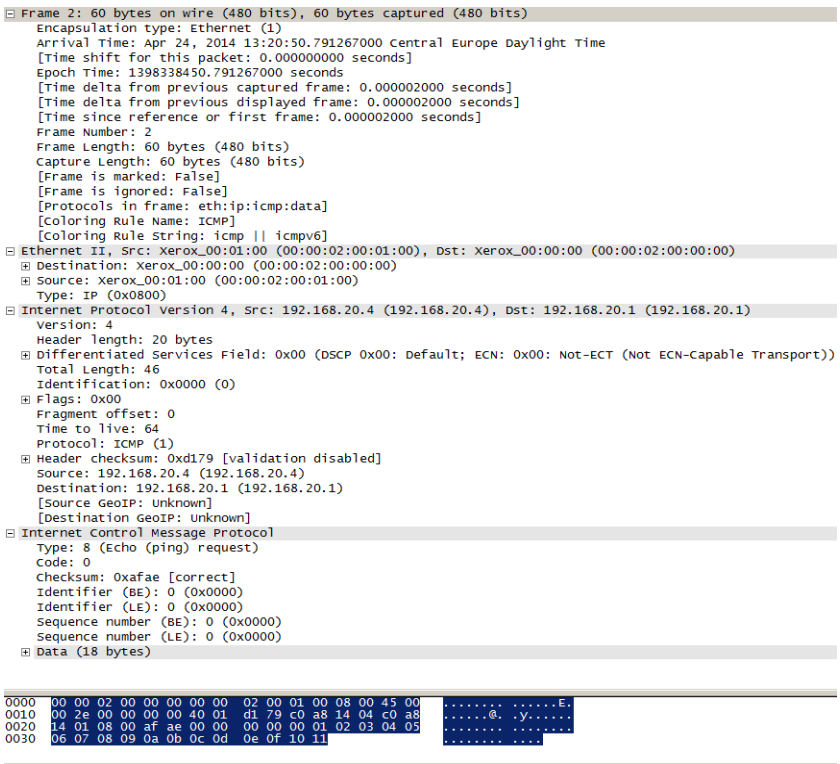
Obr. 14: Packet View, který ukazuje nadefinovaný datagram



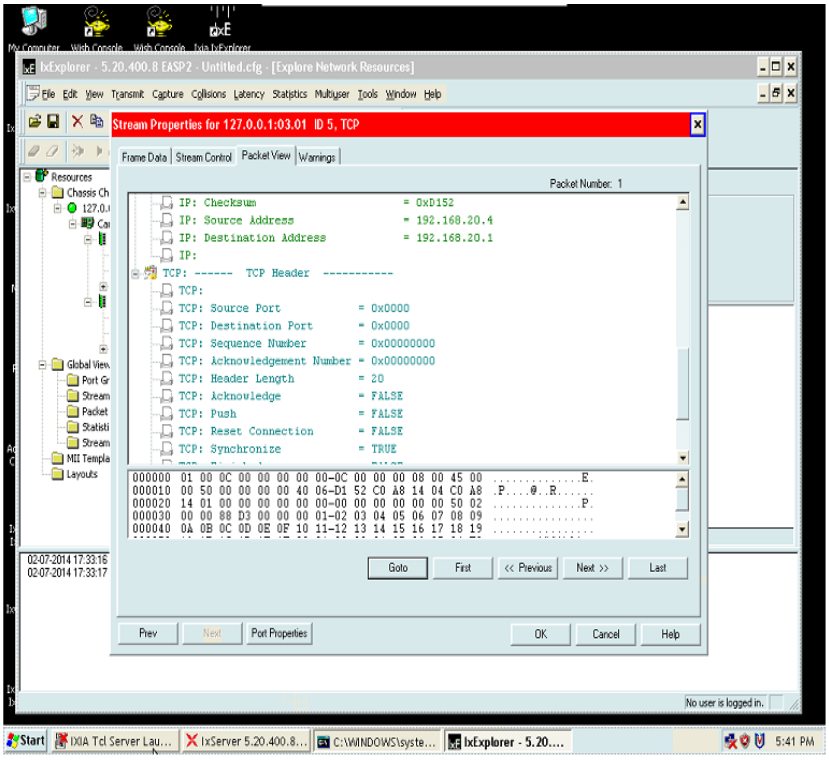
Obr. 15: Wireshark



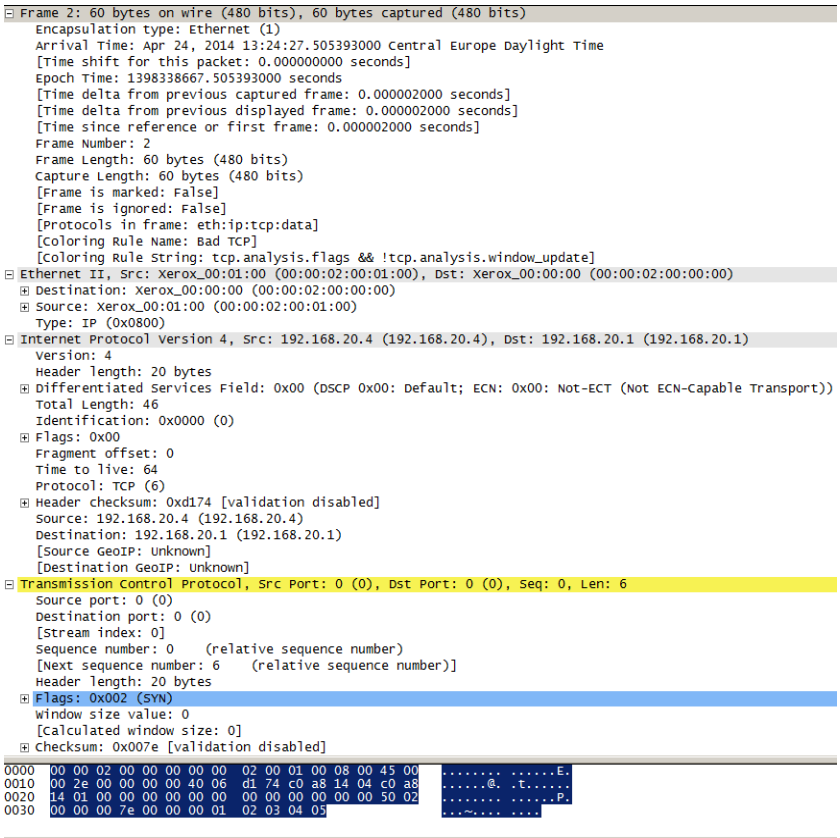
Obr. 16: Náhled do struktury generovaných paketů



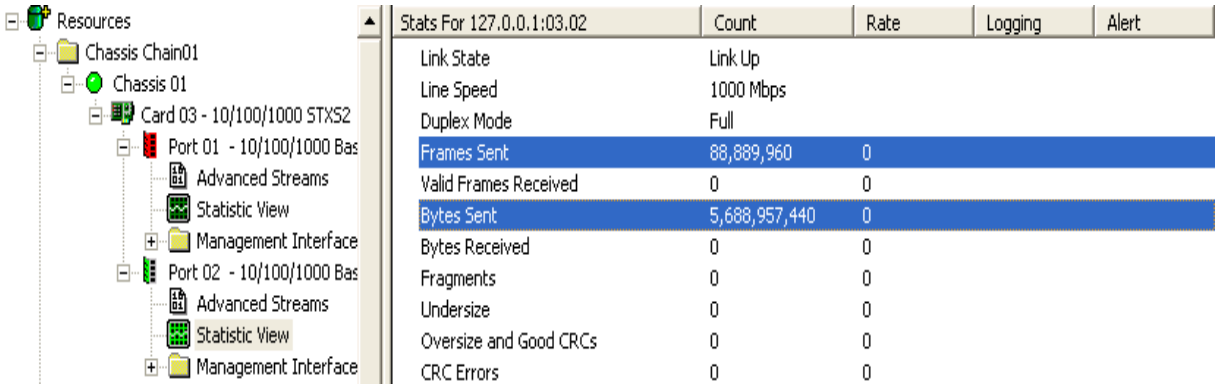
Obr. 17: Wireshark



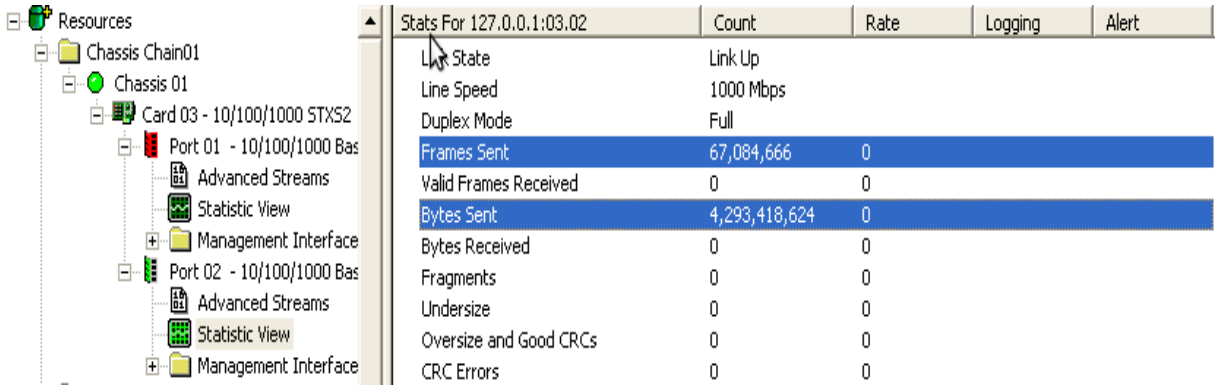
Obr. 18: Náhled do struktury generovaných toku



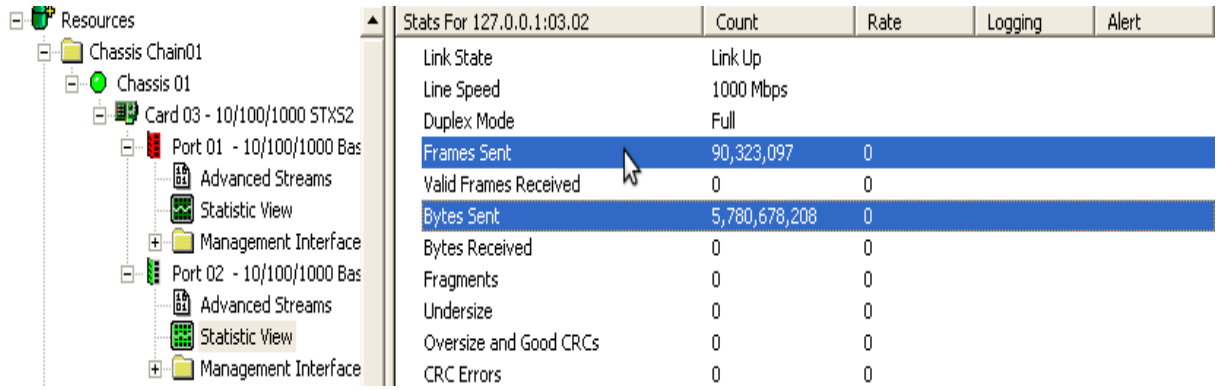
Obr. 19: Wireshark



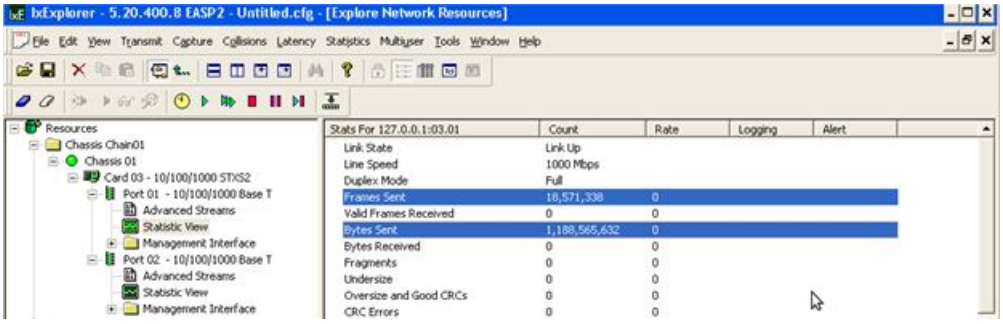
Obr. 20: Záznam poslaných dat, UDP flood



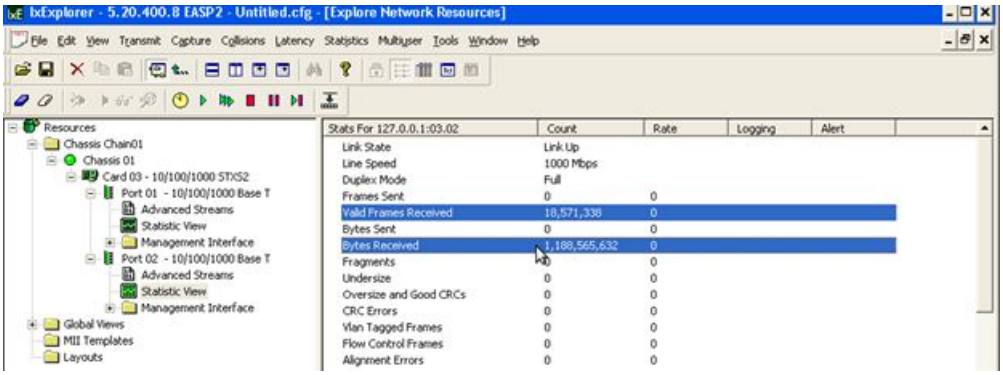
Obr. 21: Záznam poslaných dat, ICMP flood



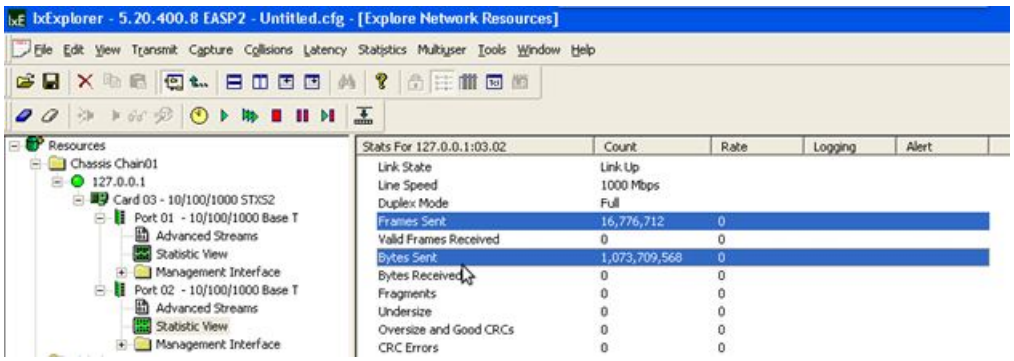
Obr. 22: Záznam poslaných dat, SYN flood



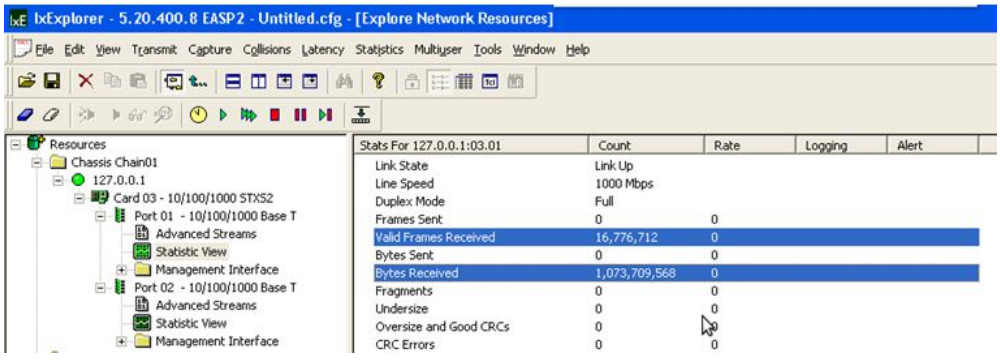
Obr. 23: mujdatovytok(1-2) - poslané bajty a rámce z portu 01



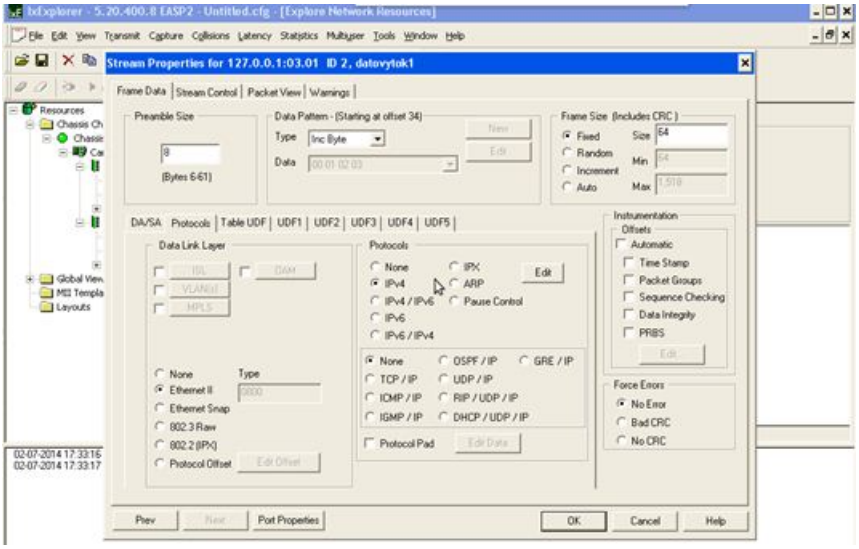
Obr. 24: mujdatovytok(1-2) - přijaté bajty a rámce na portu 02



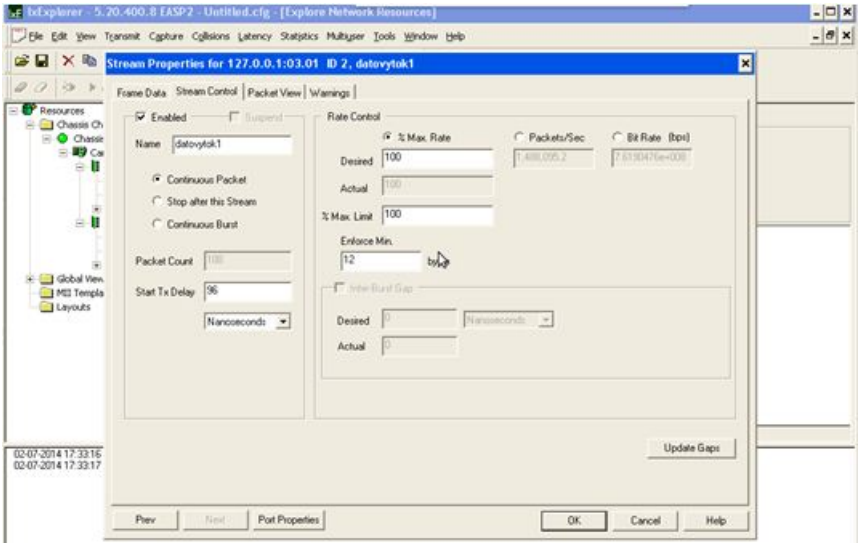
Obr. 25: mujdatovytok(2-1) - poslané bajty a rámce z portu 02



Obr. 26: mujdatovytok(2-1) - přijaté bajty a rámce na portu 01



Obr. 27: Definovaní datového toku část 1.



Obr. 28: Definovaní datového toku část 2.