МРЕЖОВИ АТАКИ

Доц. Д-р Иван Богомилов, маг. Стефан Стефанов – НБУ

Атаките в мрежовата среда имат за цел придобиване на неоторизирана или унищожаване на информация, нарушаване на функционалността на системите и неоторизиран достъп до мрежови ресурси. Атаките основно могат да се разделят на 2 групи – насочени към операционната система на устройствата и мрежови атаки. Вторият тип атаки са насочени към протоколите от TCP/IP стека, осигуряващ комуникациите в мрежата.

I. Атаки в каналния слой

1. Прескачане на VLAN

VLANs (Virtual Local Area Network) са метод, при който се сегментира логически мрежата на втори слой, като по този начин се получава разделяне на броудкаст домейна. Необходимо е маршрутизиращо устройство, за да може да се пренесе трафик от един VLAN в друг. Това обаче не е сам по себе си гарантиран метод за защита на мрежата. Злонамерен потребител може лесно да „прескочи" от един VLAN в друг, т.е да изпраща трафик към мрежи, в които не е оторизиран, а също и да подслушва трафик от тях, като използва вратички в DTP (Dynamic Trunking Protocol). Този протокол се използва, за да се договарят автоматично trunk връзките между комутаторите. Trunk връзка е връзка между комутатори от второ ниво (суичове), по която се позволява да минава трафика от множество VLAN-и. Това се прави чрез използването на 802.1Q протокола.

Договарянето на връзката се извършва, използвайки състоянието на порта според DTP (има 5 възможни състояние, описани на таблицата по-долу).

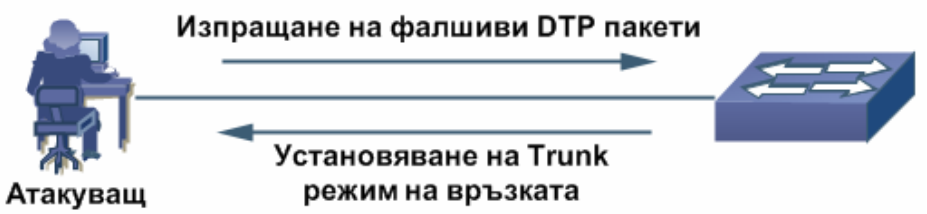
Таблица DTP състояния

Състояние	**Описание**
On	Портът е настроен да бъде trunk.
Off	Портът е настроен като порт за достъп(access port) и не е trunk.
Auto	Портът е настроен автоматично да договаря статуса си. Ще стане trunk, ако портът от другата страна иска да бъде trunk.
Desirable	Като auto, с тази разлика, че портът изпраща активни съобщения, че иска да бъде trunk.

Таблица DTP състояния	
Състояние	**Описание**
Nonegotiate	Портът не слуша никакви DTP пакети и е настроен да бъде trunk. Няма никакви договаряния в случая.

По принцип повечето мрежови устройства са настроени да носят по техните trunk връзки всички VLAN-ове. При 802.1Q протокола, който се използва от DTP, четири байта се добавят към хедъра на Ethernet фрейма и в тях едно от полетата показва принадлежността на фрейма към съответния VLAN (другите полета се използват за приоритет - QoS на втори слой, за контролна информация и други). Това е процедурата при влизането на фрейма в даден trunk. Когато фреймът напуска trunk и влиза в друг комутатор, 802.1Q хедърът се премахва, CRC сумата на края на фрейма се пресмята и фреймът се връща обратно към нормалния си формат. [1]

„Прескачане" от един VLAN в друг VLAN използва описания механизъм на работа на DTP. При него се създават фалшиви DTP пакети, с които се цели да бъде заблуден отсрещния комутатор, че злонамереният компютър също е комутатор. Изпраща се DTP съобщение, което указва, че компютърът, имитиращ комутатор иска тази линия да е trunk. Когато истинският комутатор види това съобщение, при включено автоматично уговаряне на trunk, връзката от нормална става trunk и атаката е осъществена успешно. Този процес е илюстриран на фигура 1:



Фигура 1 "Прескачане" на VLAN

Защитата от този вид атаки не е сложна. Конфигурират се всички портове, които няма да се използват за trunks, като access портове. В резултат на това всякакви DTP пакети, получени от такъв порт, ще бъдат счетени за анормални и порта ще се постави в специален изключен режим. При Cisco Catalyst комутаторите трябва да се въведат следните команди в конзолата:

Задава се портът да е access:

Switch(config-if)#switchport mode access

Ако даден порт трябва да е trunk:

Switch(config-if)#switchport mode nonegotiate

Switch(config-if)#switchport trunk allowed vlans [vlan range]

С първата команда се спира DTP протокола и се прави порт trunk без никакви

уговорки. Втората команда е препоръчителна и определя кои VLAN-и могат да преминават по trunk връзката. [2]

Spanning-tree атаки

Spanning Tree Protocol (STP) е създаден, за да прекъсва безконечно зацикляне на пакети в мрежи с повече от едно трасе до различни точки [3]. Зациклянето на пакети в такава мрежа води до по-голямо натоварване на мрежовите устройства и до изчерпване капацитета на връзката. Това прави STP протокола задължителен. Чрез него устройствата си обменят съобщения BPDU (Bridge Protocol Data Unit) на всеки две секунди. Всеки комутатор изпраща BPDU съобщения, като в едно от полетата включва своя bridge ID (приоритет на комутатора + MAC адрес на порт). Комутаторът с най-малък bridge ID се определя за корен на дървото (root bridge). Целта е да се създаде йерархия от тип "дърво" и да се избере нейн корен, до който всички устройства, участващи в топологията, да имат само една действаща връзка (тя се определя от различни фактори - на първо място е капацитетът на връзката, после MAC адрес на порта). По този начин става невъзможно зацикляне на пакети. По забранените връзки не се движи потребителски трафик, но преминават BPDU пакети, така че ако активната връзка бъде прекъсната, да може да се активира почти моментално резервната (3-50 секунди в зависимост от имплементацията на протокола). [1]

Злонамерен потребител може да се възползва от начина на работа на STP протокола. Това става чрез създаването и изпращането на фалшиви BPDU пакети, твърдящи че потребителят, който пред реалните устройства се представя за комутатор, има най-нисък bridge ID, в следствие на което истинските устройства приемат, че злосторникът е корена на STP дървото. Така се разваля настоящата структура и се създава нова, в която са възможни зацикляния, които могат да сринат мрежата.

Ефективна защита от този тип атака е използването на BPDU Guard функцията при Cisco Catalyst комутатори. BPDU Guard затваря всеки порт предварително конфигуриран с PortFast командата (това са портовете, към които са свързани потребители, а не комутатори). Когато на такъв порт се получи каквото и да е BPDU съобщение, портът се поставя в изключен режим. Командата е следната:

Switch(config)#spanning-tree portfast bpduguard

2. Запълване на MAC (Media Access Control) таблицата

Атаки от този тип не могат да сринат дадена мрежа, но могат да служат като необходима предпоставка за това (използват се при атаки от тип „отвличане на сесия"). Те се възползват от основният принцип на работа на всеки нормален комутатор. Разликата между комутатор и хъб е в това, че за разлика от хъба, комутаторът не изпращя всяко получено съобщение на всичките си портове, а директно на правилния порт. Това е възможно чрез употребата на т.нар. MAC таблица, в която се съхраняват зависимостите между MAC адрес и физически порт. Механизмът на попълване на таблицата е елементарен - проверява се адреса на подателя на всеки получен пакет и ако го няма в MAC таблицата, той се попълва като се асоциира с порта, на който е получен пакета. След това се проверява адреса на получателя спрямо таблицата и пакетът се изпраща на съответния порт. Ако липсва запис за адреса на получателя пакетът се разпраща на всички портове, освен този, от който е дошъл. MAC таблицата се пази в памет от тип Cache, или тук се нарича CAM (content addressable memory) памет. Нормалната големина на паметта е 128 килобайта. Когато тя се препълни, комутаторът минава в режим на хъб. [1] [2] [3]

Тази атака лесно може да се осъществи, като се изпратят множество произволни пакети, всеки с различен адрес на подател. Достъпна програма за целта е Linux Macof. Въпреки че такъв вид атака не може да разруши дадена мрежа, тя може значително да улесни подслушването в нея.

Защита от този тип атаки: Необходима е употребата на port security (сигурност на портовете). Чрез тази функционалност може да се ограничи броят, както и точно да се специфицират, MAC адресите, които се допускат до даден порт. Ако такъв порт получи пакет с адрес на подателя, различен от разрешения, портът автоматично се изключва. Конфигурацията е на две стъпки:

1) Switch(config)#mac address-table static 09-00-0D-31-00-5F vlan 4 interface fastethernet 0/0

Статично задаване на разрешения MAC адрес и VLAN. Тази команда определя, че само потребител с MAC адрес 09-00-0D-31-00-5F, който принадлежи на VLAN 4, може да се свързва с порт fastethernet0/0.

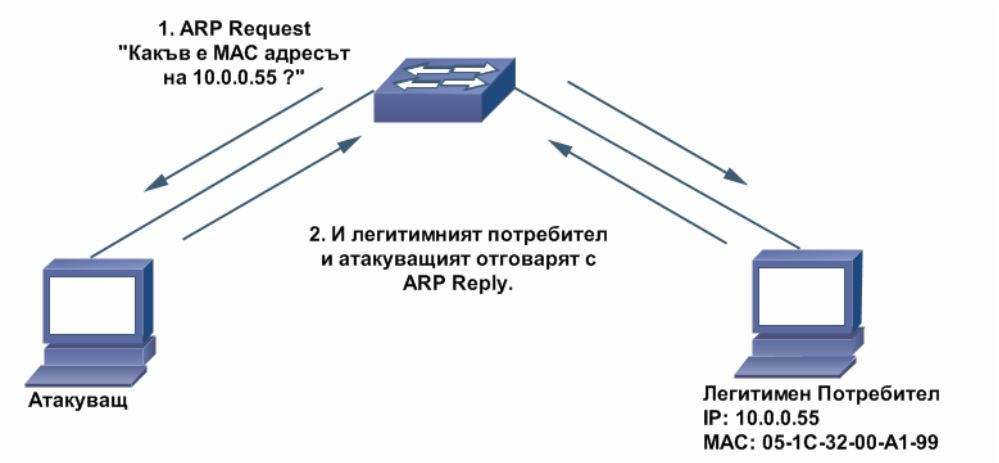
2) Switch(config)#switchport port-security violation shutdown

Определя се какво да е действието, ако бъде открито нарушение. В случая – изключване на порта.

3. ARP атаки

ARP атаките обикновено не се използват самостоятелно, а като част от друга атака. ARP протоколът дефинира връзката между адреса на мрежовия слой (IP) и този на каналния слой (MAC). ARP запитвания (requests) се броудкастват, когато даден потребител знае IP адреса, но не и MAC адреса на търсения host. Съответният хост отговаря с ARP отговор (replay), в който записва своя MAC адрес. Така всеки хост въз основа на запитвания и отговори

изгражда динамична локална ARP таблица на съответствие (IP адрес – MAC адрес). Злонамерен потребител може да преправи ARP отговора (reply), записвайки своя MAC адрес, с цел да насочи трафика от определен host към него. Понеже легитимният потребител също отвръща на ARP запитването, за да е успешна атаката трябва преправения отговор да стигне първи до запитващия. На фигура 2 е показан процеса на ARP атаката:



Фигура 2 "ARP атака"

Защитата от този тип атаки е като за всички потребители и комутатори ясно се дефинира, към кой порт кой адрес се асоциира. Командите за това бяха показани при предишната атака (Атака от тип запълване на MAC таблицата).

Друг начин е да се следи в локалната ARP таблица за повече от едно съответствие „IP адрес – MAC адрес".

4. VTP атаки

VLAN Trunking Protocol (VTP) е управляващ протокол, чиято цел е да намали ръчното конфигуриране на големи мрежи. Той служи за синхронизация на броя и имената на VLAN-ите в дадена мрежа. Целта е тези параметри да бъдат въведени само на един комутатор и те автоматично, чрез този протокол, да се появят в конфигурациите на всички комутатори в мрежата (VTP domain). При VTP протокола комутаторите могат да работят в три режима – Transparent (прозрачен), Server (сървър) и Client (потребител). Промени, нанесени във VLAN конфигурацията на комутатор в режим сървър,моментално се разпространяват по всички други комутатори от тип сървър и потребител, но не и в „прозрачните" комутатори. За да се следи коя е най-новата версия на VLAN конфигурацията, се използва т.нар. „configuration revision number". При всяка извършена промяна този номер се увеличава с едно. [1]

Злонамерен потребител може да се възползва от този протокол, да се обяви за сървър и да изпрати в мрежата конфигурация с ревизионен номер по-висок от настоящия, в следствие на което да заличи валидната досегашна

конфигурация. Това автоматично кара всички портове да се асоциират с VLAN 1 и така се разрушава защитата, която VLAN-ите осигуряват.

Тази атака често се използва заедно с атака от тип „прескачане" на VLAN, защото е необходимо нарушителят да се представи като комутатор и да изгради trunk линия.

За защита от този тип атаки има две възможности:

1) Да се спре VTP протокола (неприложимо за големи мрежи) - всички комутатори се конфигурират като прозрачни и в тях ръчно се въвежда VLAN конфигурацията:

Switch#vlan database

Switch(vlan)#vtp transparent

Switch(vlan)#vlan 2 name TU-Sofia

2) Да се създадат пароли, чрез които да се защитят VTP операциите – въвежда се парола и всички vtp съобщения, които не са с тази парола, се пренебрегват:

Switch(vlan)#vtp password tu-s0fia

5. Проблеми със сигурността на втори слой, свързани с маршрутизатори

Тези проблеми са свързани със CDP (Cisco Discovery Protocol). CDP протоколът е собственост на Cisco Systems и работи само между техни устройства (маршрутизатори и комутатори). Той се използва за събиране на информация в даден маршрутизатор относно адреси на трети слой, платформа, операционна система и други не пряко свързаните с него комутатори и маршрутизатори. CDP не поддържа криптиране и няма методи за автентикация на участващите в комуникацията устройства. Нарушителят може да се представи като Cisco устройство и да получи информация за легалните устройства в мрежата, т.е. за структурата й. Също така в по-старите версии на Cisco IOS (операционната система, която се ползва от тези устройства) има бъг, който кара устройството да излезе от строя при множество, получени за кратък период от време, CDP пакети. [1] [2]

Този проблем със сигурността може да бъде решен по два начина:

1) Най-доброто решение е да се спре изцяло CDP протокола, тъй като ползата от него е много ограничена:

Router(config)#no cdp run

2) Може да се ограничат интерфейсите, на които да се пускат CDP пакетите:

Router(config-if)#no cdp enable

II. Атаки в мрежовия слой

Проблемите със сигурността на мрежовия слой са много, поради усложняване на протоколите. Осигуряването на защита на мрежово ниво е от изключителна важност за общата защита на мрежата.

1. Проблеми, свързани със сигурността на метода за конфигуриране на устройствата

Повечето мрежови устройства могат да се конфигурират по няколко начина. Най-често използваните са: отдалечена терминална връзка (Telnet, SSH); през конзолния интерфейс; отдалечено чрез SNMP (Simple Network Management Protocol); през уеб интерфейс, използвайки HTTP (напоследък се използва само HTTPS – secure HTTP).

Използването на чист HTTP не се препоръчва по две причини. Първата е, че се отваря порт 80 към устройството, който е предпочитан порт за атаки. Втората е, че някои от по-старите операционни системи на Cisco имат бъг, който позволява на неоторизирано лице да види системната конфигурация. Това е съществен недостатък, защото злонамерен потребител, въоръжен с хеша от паролата, може много лесно да види самата парола чрез определена програма. Следва конфигурацията на маршрутизатора на неоторизиран потребител:

http://ip address/level/99/exec/show/config

Фигура 3. "Бъг в операционната система на Сиско"

Фигура 3 илюстрира как е използван бъга в ОС на маршрутизатора и неоторизирано е придобита конфигурацията. Използван е MD5 хеш алгоритъм (от командите enable password, service password-encryption) и самия хеш код.

MD5 не се разкодира лесно, но благодарение на това, че Cisco ползва (в по-старите IOS) едни и същи променливи за MD5 алгоритъма, е възможно да се направи таблица на съответствията между паролите и хеша им. Програма, в която е използван този недостатък на паролите, е Boson GetPass! и на фигура 4 се вижда придобитата парола:

Фигура 4 "Boson GetPass"

Този проблем лесно се решава, като се забрани използването на HTTP:

Router(config)#no ip http server

Или чрез ограничаване на потребителите, които имат достъп до него:

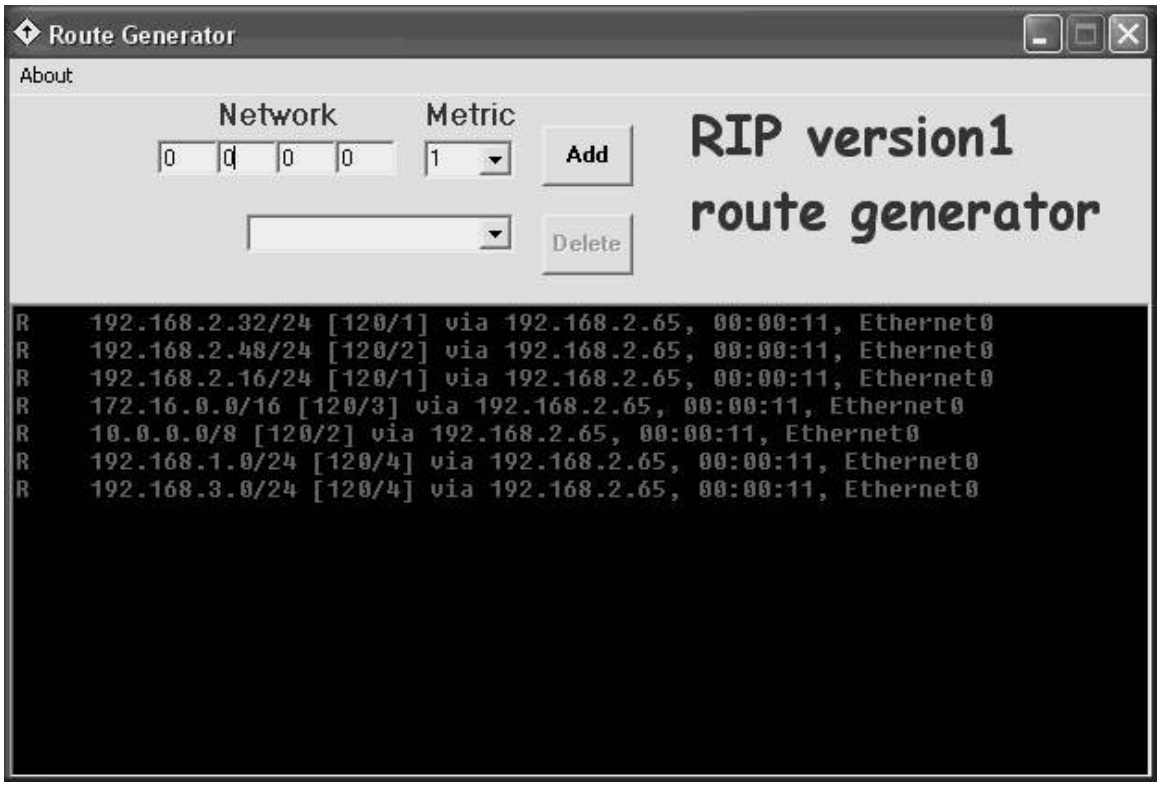
Router(config)#access-list 1 permit host 10.0.0.5

Router(config)#ip http server 1

По аналогичен начин трябва да се забрани или ограничи използването на Telnet протокола, защото и той има недостатъци по отношение на сигурността. Също така, трябва винаги да се ползва последната операционна система. [1] [4]

2. Проблеми, свързани с инжектирането на зловредни маршрути

Някои от по-старите маршрутизиращи протоколи (RIP v1) не поддържат оторизация на съобщенията, чрез които се обновява маршрутизиращата таблица. Това е потенциален проблем, защото злонамерен вътрешен потребител може да инжектира неправилни маршрути и това до доведе до невъзможност за достъп до определени мрежи. Програма, която може да „отрови" маршрутизиращата таблица (route poisoning) за RIP v1 е показа на фигура 5:



Фигура 5 "Програма за route poisoning"

В този случай винаги се препоръчва за защита да бъде използвана автентикация. При RIP v2 това става със следните команди:

- Първо е необходимо да бъде създаден „ключодържател" (key-chain) и да се посочи парола:

Router(config)#key chain MYCHAIN

Router(config-keychain)#key 1

Router(config-keychain-key)#key-string cisco

- След това трябва да се асоциира вече създадения ключодържател с всички интерфейси, на които работи RIP и да се включи MD5 автентикацията:

Router(config)#interface fastethernet 0/0

Router(config-if)#ip rip authentication key-chain MYCHAIN

Router(config-if)#ip rip authentication mode MD5

Router(config)#interface serial 0/0

Router(config-if)#ip rip authentication key-chain MYCHAIN

Router(config-if)#ip rip authentication mode MD5

Описаните по-горе механизми се използват при инструмента за атака IP spoofing.

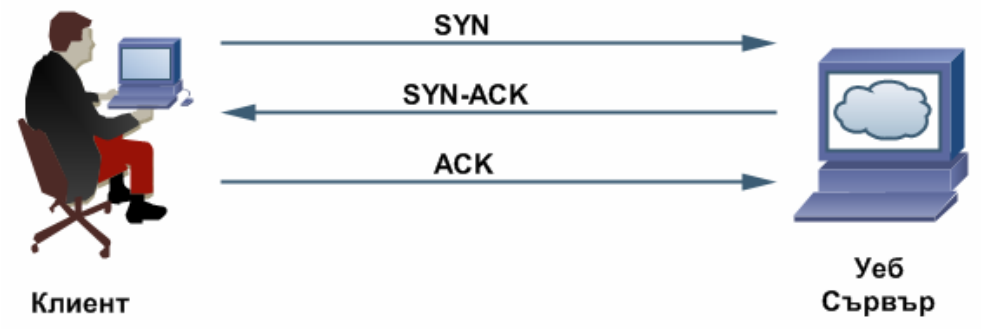
III. DoS атаки

DoS (Denial of Service) атаките се използват, за да се наруши нормалното функциониране на дадена система или мрежа. Нарушителят цели да претовари системата или дадения мрежов ресурс, което да доведе до невъзможност за обработка на постъпващите пакети, в следствие на което те биват отхвърляни (drop). Целта на атакуващия е да се откаже достъп на легитимни потребители до съответната услуга. Този вид атаки често се използват в комбинация с други атаки, като целта им е да елиминират системите за сигурност преди реалната атака. Най-често при DoS атака се прави опит да се отворят множество фалшиви TCP връзки. Също така се използва и фалшив ICMP и UDP трафик. Устройството, към което е насочена атаката, се опитва да обработи всички заявки за връзки и по този начин изчерпва наличните си ресурси. Три типа широко разпространени DoS атаки са [3] [5]:

- TCP SYN претоварващи атаки;
- Land.c атаки;
- Smurf атаки.

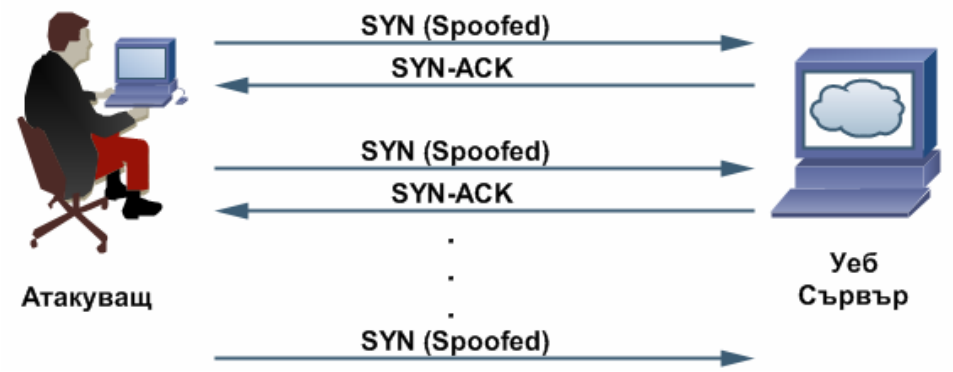
1. TCP SYN претоварващи атаки

Тези атаки са базирани на механизма на установяване на TCP сесия (TCP three-way handshake). Установяването на връзката при TCP се извършва от тройна размяна на пакети, както е показано на фигура 6:



Фигура 6 "Three-way handshake"

В примера клиентът се опитва да установи връзка с уеб сървъра. Първо той изпраща SYN (синхронизиращ) пакет до сървъра с цел да се синхронизират поредните номера на TCP пакетите, които ще се обменят между клиента и сървъра. SYN пакетът съдържа ISN (initial sequence numbers) на клиента и флагови полета със следните стойности SYN=1, ACK=0. С втория пакет сървърът едновременно потвърждава, че е получил ISN номерата на клиента, и изпраща своите ISN номера (SYN=1, ACK=1). Последната стъпка в този процес на обмяна, е пак от страна на инициатора, който изпраща потвърждение (ACK пакет) на сървъра. Връзката вече е установена.



Фигура 7 "TCP SYN претоварване"

При TCP SYN претоварването (фиг. 7) се получава претоварване на мишената на атаката чрез използване на множество подправени (spoofed) SYN пакети (изпращат се от фалшиви IP адреси – IP spoofing) , които имитират валидни заявки за връзки. Тези пакети биват изпратени до сървъра, който отговаря със SYN-ACK пакети, но последната стъпка от процеса (потвърждаването с ACK пакети) не настъпва. Изградените връзки са в т.н. полуотворено състояние. При достатъчно голямо количество SYN пакети, изпратени от нарушителя, обектът на атаката се претоварва и спира да отговаря на всички постъпващи заявки за връзки, включително и на реалните. Получава се отказ на обслужване. Подправянето на SYN пакетите най-често се състои в подмяна на адреса на подателя, с цел да се прикрие самоличността на атакуващия или да се заобиколи дадена защитна стена, като се използва адрес, който е разрешен от нейният лист за контрол на достъпа. Допълнително тази техника нанася двойна вреда, защото освен мишената, и машините, чиито IP адреси са използвани при атаката, получават множество пакети от самата мишена.

Всяка полуотворена връзка (използва се термина ембрионална връзка) заема ресурс, и следователно броят на тези връзки е краен. След достигане на този брой, устройството спира комуникациите с потребителите, докато тези ембрионални връзки не се затворят и изчистят от стека.

SYN атаките са прости атаки, но те все още се използват масово и имат успех. Някои от факторите за това са:

- SYN пакетите са част от нормалния мрежови трафик, и следователно е много трудно да се филтрират;
- За изпращането на SYN пакети не е необходим канал с голяма пропускливост, т.е. всеки обикновен потребител разполага с ресурса да извърши такава атака;
- Лесно се променя адреса на подателя, поради факта, че не се изисква отговор от мишената. В следствие на това за администраторите е много трудно да филтрират тази атака. [3] [15]

Противодействието на SYN атаките може да се реализира в няколко плана [6]:

- Лимит на броя на полуотворените връзки, както и дефиниране на максималния интервал от време, в което те да са полуотворени. След изтичане на това време, те се прекратяват и се подменят с нови.
- Използване на SYN cookies. При отговор на SYN пакета хостът, отговарящ със SYN/ACK пакет криптира поредния номер (Sequence Number). При това не се стартира полуотворена връзка. Едва след получаване на пакет с правилния пореден номер се започва с three – way hand shake процедура.

2. Land.c атаки

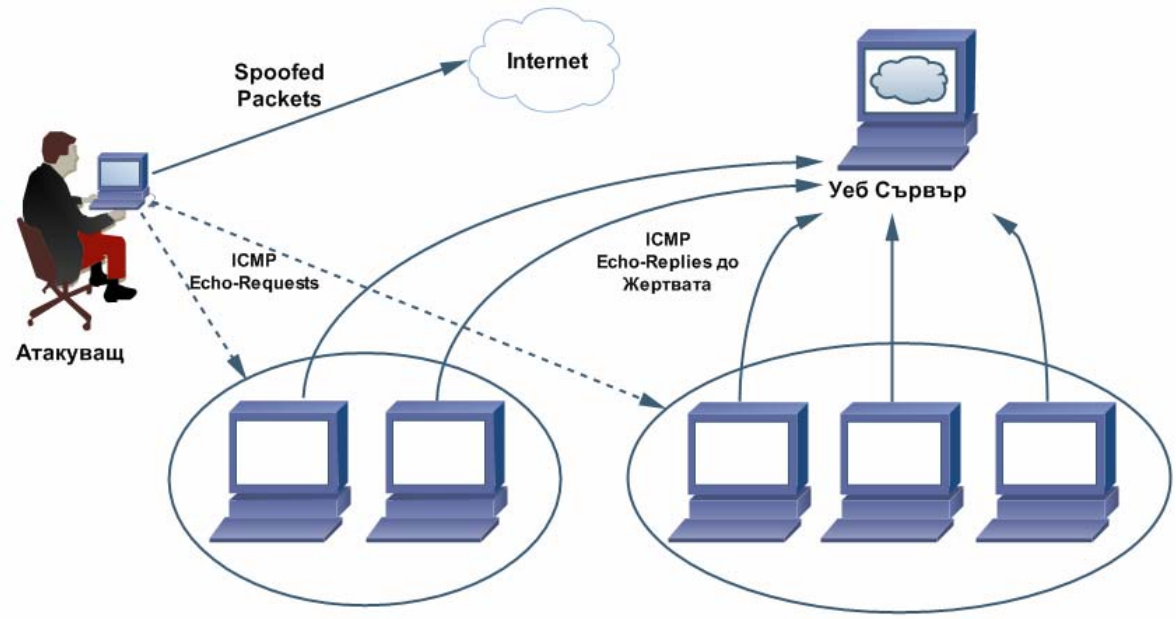
Изключително прост и ефективен пример за DoS атака. Атакуващият изпраща множество SYN пакети с еднакви адреси и портове на подателя и получателя. Целта на тази атака е да накара жертвата да изпраща отговор на тези пакети сама на себе си. Процесът е цикличен и скоро машината-жертва остава без ресурси и спира да предоставя услуги. При тази атака атакуващият използва ресурсите на жертвата срещу самата нея. [5]

3. Smurf атаки

Атакуващият претоварва канала на жертвата, като препраща безполезен трафик към мрежата й. При тази атака се използват фалшиви ICMP (Internet Control Message Protocol) echo-request пакети и broadcast адреси, които карат мрежовите устройства да ги препращат на всичките си интерфейси.

ICMP протоколът се използва да обработва грешки (главно да ги съобщава) и да контролира връзката на 3 слой. Друга широка употреба е ping услугата (Windows ползва ICMP за ping, Unix, Linux, Cisco IOS, използват UDP пакети на произволен висок порт).

При Smurf атаките, ICMP echo-request пакети се изпращат към broadcast адреса на отдалечена мрежа, с цел да се наруши нормалната работа на мрежата. На фигура 8 е показано действието на една такава атака:



Фигура 8 "Smurf атака"

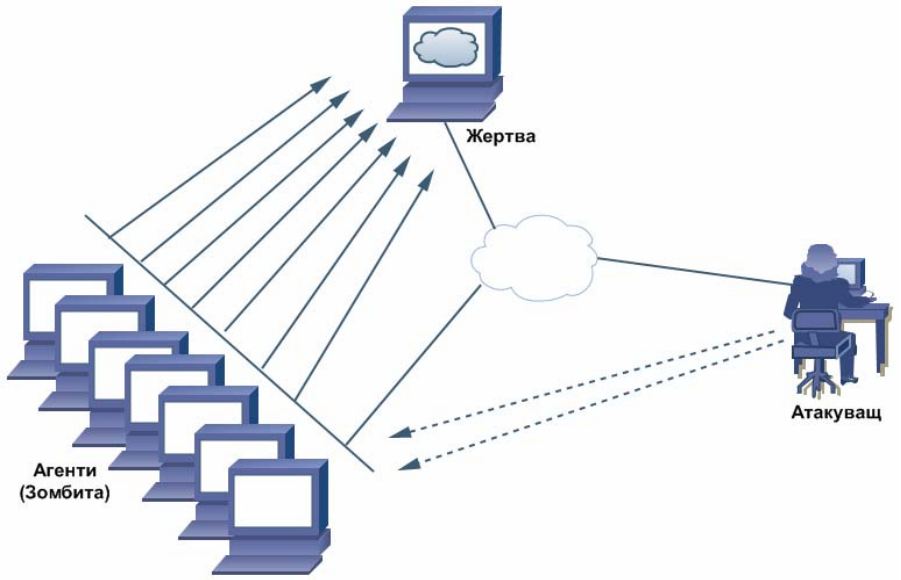
Неволните посредници в тази атака изпращат ICMP echo-reply пакетите си към адреса на жертвата на атаката. Следователно, за да е успешна тази атака, тук също трябва да се използва техниката с преправяне на адреса на подателя (spoofing). Тази атака не претоварва жертвата, но блокира канала й.

Вариация на Smurf атака е Fraggle атаката, но тя използва UDP (user-datagram protocol) вместо ICMP. Fraggle атаките използват CHARGEN и ECHO протоколите, които работят на UDP портове 19 и 7. Тези два протокола действат на принципа на ICMP ping командата. CHARGEN и ECHO, ако са активирани на дадена машина, изпращат отговор на всеки, който генерира трафик на съответните портове. Атакуващият може да се възползва от това, като създаде безкраен цикъл, който да препраща трафик между тези портове. [3] [5]

4. Разпределени атаки от тип „отказ на услуги"

DDoS (Distributed Denial-of-Service) атаките са значително по-трудни за осъществяване. При тях атакуващият използва различни системи, свързани към Интернет, за да атакува определена жертва и това ги прави много трудни за проследяване и противодействие. Подготовката на атаката се състои в това, че нарушителят предварително разбива защитата на няколко машини в Интернет и ги поставя под свой контрол, като инсталира на тях вреден код. Тези, вече компрометирани, компютри се наричат агенти, ботове или зомбита, поради факта, че следват сляпо командите на атакуващия. Нарушителят използва тези агенти, за да извърши координирана атака от всички ботове към жертвата. Тази атака заема мрежовите ресурси на атакувания. Тя е високо ефективна, тъй като е координирана (общият ресурс на всички зомбита е много по-голям от този на

нарушителя) и изключително трудна за проследяване. По правило атакуващият контролира зомбита от обществено достъпна машина (в интернет кафе или клуб), през прокси или като използва техниката на подправяне на адреса си. Фигура 9 показва нагледно този вид атака:



Фигура 9 "DDoS атака"

5. Отвличане на сесия (Session Hijacking)

При отвличането на сесия (Session Hijacking), атакуващият пресича вече осъществена сесия или връзка между две системи [5]. Най-често такива атаки се използват при TCP връзки, защото при тях имаме реално изграждане на сесия и следенето й чрез поредни и потвърждаващи номера. Целта на този вид атака е нарушителят да се внедри между двата крайни потребителя и да ги накара да разговарят с него, а не помежду си. Тази техника е различна от ip spoofing-а, защото при него е необходимо, макар и с подправен адрес, автентикиране пред отсрещната страна. При отвличането на сесия двете страни в разговора вече са се автентикирали преди атакуващият да се намеси в сесията между тях. При повечето стандартни комуникации всякакви защити като стени и автентикация са преди да бъде установена дадена връзка, след което започват да се предават пакетите в чист вид, без криптиране или друг вид защита (това се преодолява чрез частните виртуални мрежи). Ако на този етап сесията бъде отвлечена, се прескачат всички приложени защитни механизми.

Възможни са два типа отвличания на сесии:

- *Активно* – отвлича се сесията с цел да се прескочи защитата на жертвата и да се изпрати подменена информация към нея;
- *Пасивно* – атакуващият отвлича сесията и действа като скрито прокси, което не пречи на комуникацията, а само я подслушва.

Трябва да се прави разлика между атака от тип „повтаряне на сесията" и от тип „отвличане на сесията". При „повтаряне на сесия" се улавят пакети,

препарват се и се препращат към жертвата (фиг.10). При една истинската атака от типа „отвличане на сесия” се преправя адреса и се настройват поредните номера (ISN – Initial Sequence Number), така че да съвпаднат с тези на инициатора на връзката. Често е необходимо да се извърши и атака от тип DoS срещу инициатора, с цел да бъде изваден от строя, за да може да се заеме мястото му в разговора (фиг. 11).

Фигура 10 "Атака от тип „повтаряне на сесия”

Фигура 11 "Атака от тип „отвличане на сесия”

Атаките от тип „отвличане на сесията” от своя страна се делят на два вида:

- Открито преправяне;
- Сляпо преправяне.

- **Открито преправяне**

Това е най-лесният начин за отвличане на сесия. Изисква се само да се прихванат няколко пакета от разговора. Това обаче може да се окаже проблем в една йерархично подредена комутируема мрежа. Има няколко възможни решения. За първото е необходим достъп до комутатор по пътя на разговора и ако той е Cisco трябва да се осигурят права над него и да се настрои Switch Port

Analyzer (SPAN) порт. Тогава може да се препраща трафик от други избрани портове или от цели VLAN-ове към SPAN порта.

Ако няма достъп до комутатор или няма как да се конфигурира SPAN порт остава второто решение. Използвайки програма от типа на Linux MACOF може да се изпратят множество пакети, с които да се запълни таблицата на комутатора, така че да премине в режим на HUB (този метод е неуспешен срещу Cisco комутатори).

- **Сляпо преправяне**

Използва се, когато е невъзможно прихващането на пакети от разговора. Тогава трябва да се познаят стойностите на поредните и потвърждаващите номера (seq и ack) . Стъпките са следните:

- Избира се мишена;
- Регистрира се и се следи активна сесия, в която тази мишена участва;
- Разпознават се seq и ack номерата.
- Извършва се DoS атака срещу единия от участващите в разговора;
- Отвлича се сесията.

Най-трудната фаза е разпознаването на seq и ack номерата. Те се записват в 32 битови полета в TCP хедъра (следователно са между 1 и 4 294 967 295; 0 не е разрешена стойност). Всеки байт се следи, но само последователния номер на първия байт от сегмента се записва в TCP хедъра. Според RFC 793 трябва seq номера да бъде увеличаван на всеки 4 микросекунди. Някой от операционните системи не се съобразяват с това и имат свой начин на инкрементиране на този номер. При BSD и Linux поредните номера се увеличават с 128,000 на всяка секунда (броячът се превърта на всеки 9:32 часа). Фактът, че не е необходимо да се уцели точния seq номер, а просто трябва попадението да е в текущия TCP прозорец, допълнително улеснява интрузията. Пример за TCP прозорец е даден на фигура 12:

Фигура 12 "TCP прозорец"

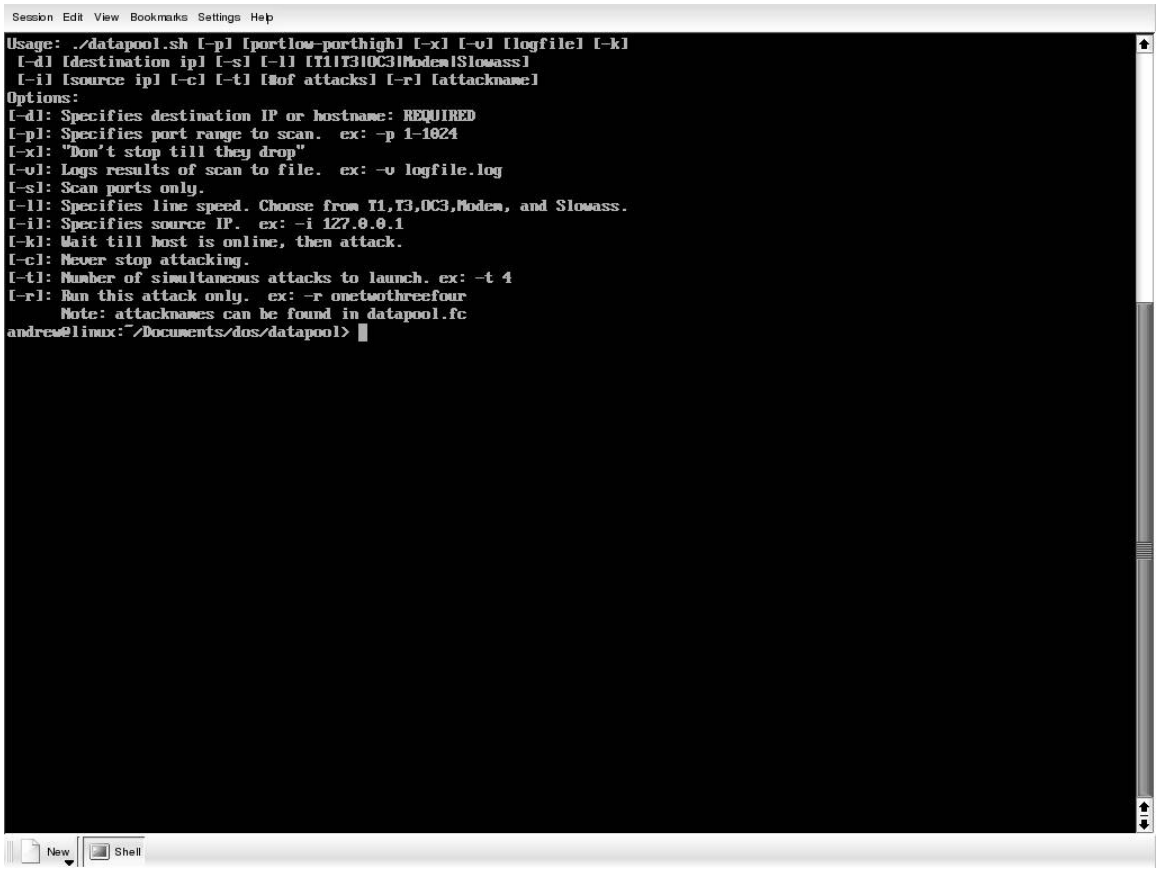
Въпреки вероятностния характер на тази операция, успехът е само въпрос на време.

Cisco Adaptive Security Appliance (Cisco ASA), най-новата серия продукти на Cisco Systems в областта на мрежовата сигурност, предлага решения и за този тип атаки. Защитната стена подменя seq и ack номерата (произлизащите от вътрешните устройства номера са псевдопроизволни, докато генерираните от ASA са напълно произволни) на всички пакети, които излизат от нея, и по този начин елиминира шансовете за сляпо отвличане на сесия, стига нарушителят да не се намира в един и същ LAN сегмент с мишените. Целият процес остава прозрачен за крайния потребител. [3] [5].

IV. Инструменти за извършване на атаките

Популярни инструменти за извършване на DoS атаки са: Datapool, Hgod, Jolt2 [7].

- **Datapool** – работи под Linux и поддържа над 100 вида DoS атаки. Фигура 13 показва елементарното меню на програмата, с което всеки може да извърши атака:



Фигура 13 "Меню на програмата Datapool"

Синтаксисът на командите варира, като минималният е да се напише само адрес на получателя (жертвата). Следният ред показва типична команда, която има за цел да атакува потребител с адрес 192.168.10.10, като нарушителят се скрива зад фалшив адрес - 192.168.10.9 :

#./datapool.sh -d 192.168.10.10 -p 1-1024 -v results.log -l T1 -I 192.168.10.9 -c -t 100

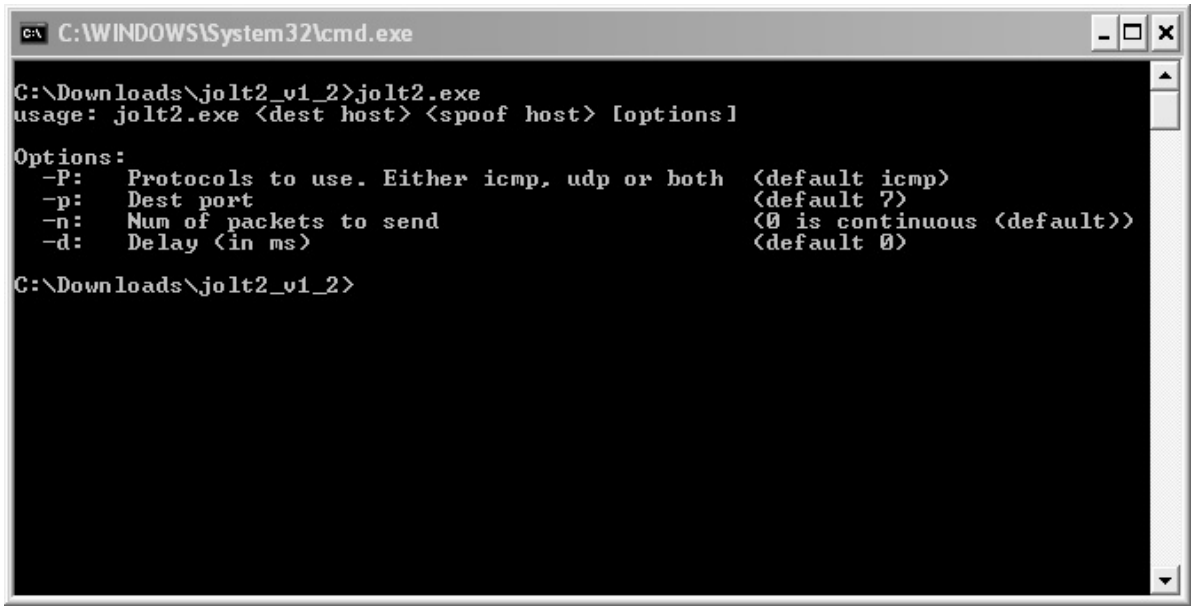
- **v** се използва, за да могат резултатите да се запишат в лог;

- **l** определя скоростта (в случая T1);

- **c** казва на програмата да не спира, докато мишената не бъде разбита;

- **t** указва на програмата колко едновременни сесии да използва. За повече сесии се изискват и повече ресурси на атакуващата машина.

- **Jolt 2** – Работи и под Linux и под Windows. Тя също позволява на атакуващия да скрие адреса си чрез spoofing. Фигура 14 показва опциите, които дава този софтуер:



Фигура 14 "Меню на програмата Jolt2"

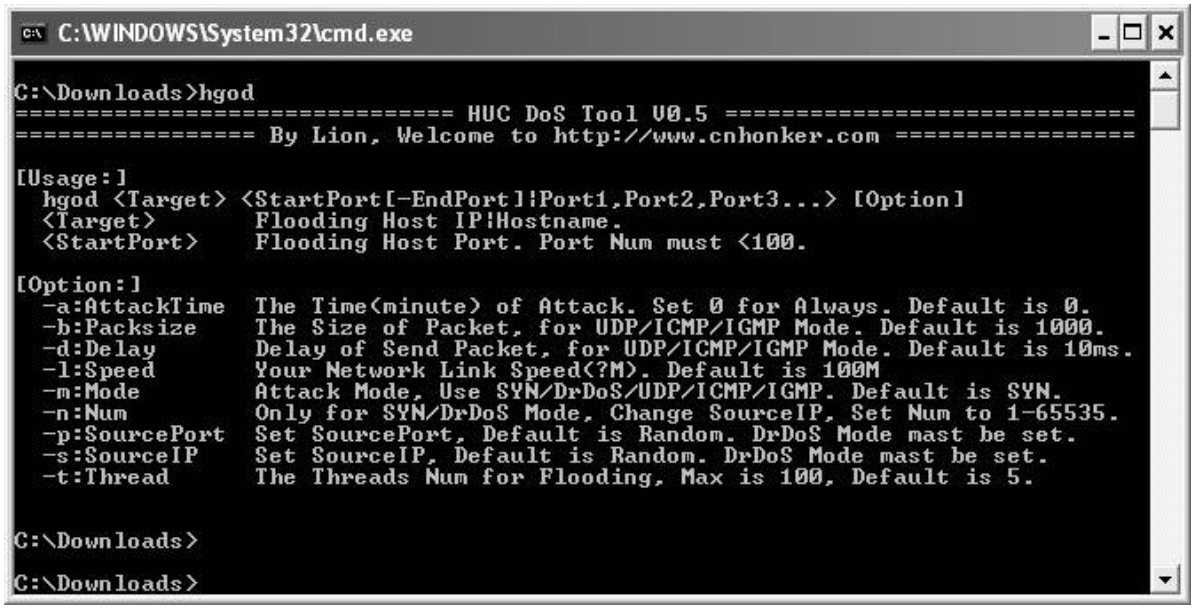
- **P** : Посочва протокол, чрез който ще се проведе атаката (ICMP, UDP)

- **p** : Порт на получателя

- **n** : Брой на пакетите, които ще се изпратят

- **d** : Закъснение между изпратените пакети

- **Hgod** е още една програма, която работи под Windows XP. Позволява подправяне на адреса на подателя. Има възможност да се избира протокол, на който да се основата атаката (TCP/UDP/ICMP/IGMP) и номер на порта (само при TCP/UDP). Поддържа множество DoS атаки, но по принцип най-използваната е TCP SYN атаката. На фигура 15 са показани опциите на тази програма:



Фигура 15 "Меню на програмата Hgod"

Примерен ред, чрез който може да се проведе атака срещу 192.168.10.10 на порт 80 (масово отворен порт заради разпространението на HTTP), използвайки адрес 192.168.10.9, е следният:

Hgod 192.168.10.10 80 –s 192.168.10.9

Използвана литература:

[1] Cisco Network Associate Curriculum (CCNA), 2006

[2] Cisco Security Appliance Command Reference

[3] Cisco Network Security Curriculum, 2006

[4] Frahim J., Cisco ASA All-in-One Firewall IPS and VPN Adaptive Security Appliance, Cisco Press, 2005

[5] Network Security Video Training, CBT Nuggets, 2006

[6] Христо Христов, Венцислав Трифонов, "Надеждност и сигурност на комуникациите", Нови знания, София, 2005 г.

[7] Интернет: google.com, en.wikipedia.org