

TCP/IP

1. IP адреси, класове мрежи, CIDR (prefix, etc)

- Обяснение на netmask
- Broadcast, network адреси
- Обяснение на classful делението и CIDR
Вече се използва CAMO CIDR, другото е история
- Специални мрежи
127.0.0.0/8, 127.0.0.1
10.0.0.0/8 , 172.16.0.0/12, 192.168.0.0/16
169.254.0.0/16 - link local адреси (за zeroconf/Rendezvous, при липса на dhcp сървър и т.н.)
Multicast - 224.0.0.0/4
Резервирани - 240.0.0.0/4
- Интересни мрежи
24.0.0.0/8 - cable operators

2. IP протокол

4 bit version	4 bit header length	8 bit Type of service (TOS)	16 bit total length
16 bit identification	3 bit flags	13 bit fragment offset	
8 bit time-to-live	8 bit protocol	16 bit header checksum	
32 bit source IP address			
32 bit destination IP address			
options (ако има такива...)			
Data			

● Полета в пакета

Header length е в 32битови думи (по 4 байта), което ограничава опциите, които могат да се добавят

Total length е до 64k, но толкова големи пакети се ползват рядко (в мрежи с много голям bandwidth, основно оптични такива)

ToS – значението му е променяно много пъти в последните години
TTL
Протокол

Identification – използва се при фрагментация, еднакво за всички парчета от фрагментирания пакет

Брое на машини зад NAT чрез следене на това поле

Контролна сума - CRC32

● Опции на пакета

Security опции, RFC 1108 - дефинирани на ниво на секретност на пакет

Loose и Strict source routing, проблеми с тях - по подразбиране не се пропускат от повечето router-и, и доста операционни системи директно ги игнорират

Record route/timestamp - дават възможност за записване на пътя на пакета

● Фрагментация

Принцип на работа
 Цел
 Идеята за MTU

- Свойства на протокола

Unreliable packet transport – работа на протоколите от по-горно ниво е да се погрижат за сигурния транспорт

Пакет с грешна контролна сума се drop-ва, без да се върне грешка

Протоколът е оптимизиран от гледна точка на routing хардуера

- Атаки върху протокола

Strict/loose source routing – подслушване на трафика

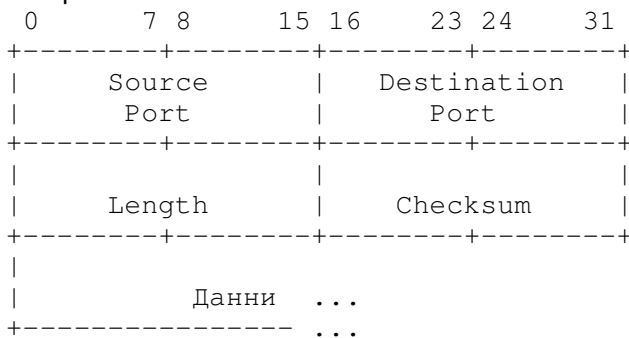
Предсказуем IP ID – IDLE scan, следене на трафика на дадена машина

Прескачане на firewall-и чрез фрагментация (разделяне на header-а на пакета от по-горно ниво в няколко фрагмента)

3. UDP

- Идея на протокола - протокол за изпращане на отделни пакети, негарантиращ нищо

- Кратко описание на header-а



- Атаки в/у протокола

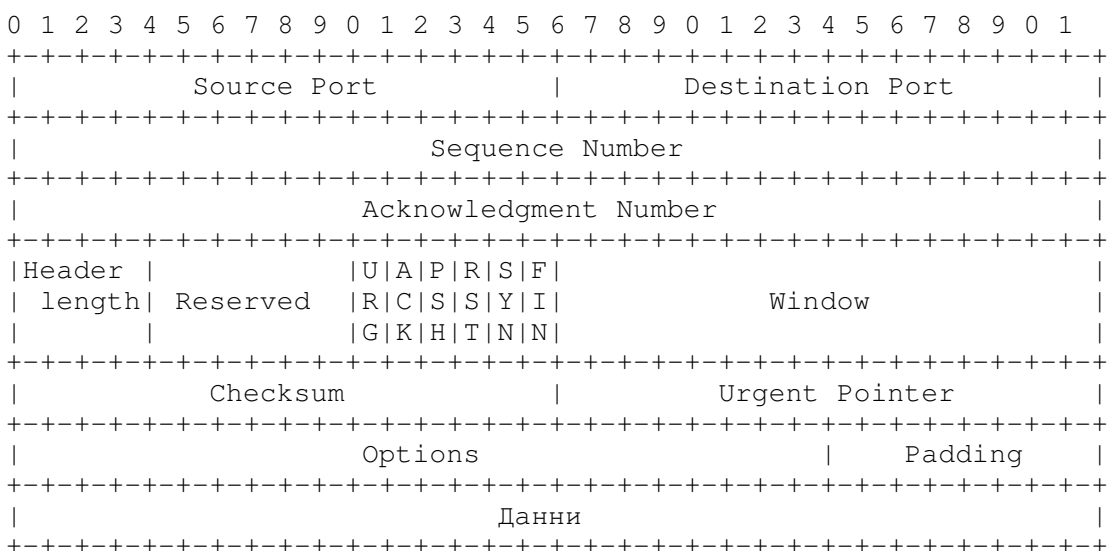
Поради липсата на sequence номера и т.н., се налага приложенията сами да се грижат за реда на пристигане на пакети и т.н., което създава предпоставки за проблеми

DNS spoofing

4. TCP

- Идея на протокола - reliable stream

- Кратко описание на header-а



- Флагове
 - SYN, FIN, RST
 - ACK
 - URGENT, PSH
 - Sequence и acknowledgment numbers
- Отваряне и затваряне на връзка
 - 3way handshake
 - Затваряне на връзка
 - Simultaneous open
- TCP options
 - Timestamp
 - MD5 аутентикация
- Sliding window, window scaling
- Timeout and retransmission
- Протоколът е сложен, който се интересува, да чете допълнително
- Атаки върху протокола
 - Blind TCP spoofing, предсказуеми ISN
 - Проблеми при TCP с голям window (пример – BGP сесиите)
 - SYN flood

5. ICMP

- echo request/reply
- "Time exceeded" (ttl expired in transit)
- ICMP source quench
- ICMP unreachable
 - Fragmentation Needed and Don't Fragment was Set (packet too big, can't fragment)
 - net/host/protocol/port unreachable
 - Други
- ICMP redirects - Допотопен routing протокол
- IRDP, timestamp req/rep, mask req/rep, information req/rep
- Други
- Атаки върху протокола
 - Използване на redirects за MITM
 - Използване на * unreachable за прекъсване на връзки
 - Използване на ping и други за задръстване на връзка
 - Използване на протокола за полу-анонимна комуникация

6. Network Address Translation и connection tracking(stateful firewalling)

- Разликата м/у firewall и packet filter
- Защо NAT не е истински firewall, а само добавка
- Моменти при NAT на UDP
- Multihomed hosts dilusions: достъп до един интерфейс на хост през другия
- Защо трябва да филтрираме както входящите, така и изходящите пакети

7. Routing протоколи

- RIPv1, RIPv2
 - Използваемост – почти не се използват, понеже са остарели
 - Версия 1 няма аутентикация на пакетите
 - Версия 2 използва MD5 и shared secret

- OSPF
 - Използваемост – де факто протокол за неглобални мрежи
 - Използва аутентикация чрез MD5 и shared secret
- Всички пакетно-базирани routing протоколи трябва да имат ограничение откъде приемат информация
- BGP
 - Използване на протокола – на него се крепи Internet
 - Кратко описание на протокола
 - Автономни системи
 - Префикси
 - Пътища
 - Проблеми, ако не се използва с MD5 аутентикация
- Общи проблем на routing протоколите
 - Аутентикация на заявките и машините
 - Announces на чужди мрежи

8. Организации, свързани с работата на Internet

- IANA
 - Основна адресация, портове
- RIPE, ARIN, APNIC, LACNIC
 - Адресация на локално (континентално) ниво
- ICANN
- IETF, IAB

Библиография:

W. Richard Stevens, TCP/IP Illustrated vol.1 – The protocols (достъпно на http://docs.ludost.net/Networking/TCP_IP_Illustrated_vol_1/)

Steven M. Belovin, Security Problems in the TCP/IP Protocol suite -

http://www.ja.net/CERT/Bellovin/TCP-IP_Security_Problems.html

M. Zalewski - Attractors and TCP/IP Sequence Number Analysis -

<http://www.bindview.com/Support/RAZOR/Papers/2001/tcpseq.cfm>

M. Zalewski - Attractors and TCP/IP Sequence Number Analysis, One Year Later -

<http://lcamtuf.coredump.cx/newtcp/>

Tsutomu Shimomura - How Mitnick Hacked Tsutomu Shimomura with an IP Sequence Attack -

http://www.totse.com/en/hack/hack_attack/hacker03.html

IP Smart Spoofing - <http://www.althes.fr/ressources/avis/smartspoofing.htm>

RFC1918 Address Allocation for Private Internets - <http://www.faqs.org/rfcs/rfc1918.html>

RFC2827 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing - <http://www.faqs.org/rfcs/rfc2827.html>

RFC3013 Recommended Internet Service Provider Security Services and Procedures -

<http://www.faqs.org/rfcs/rfc3013.html>

RFC2828 Internet Security Glossary - <http://www.faqs.org/rfcs/rfc2828.html>

SANS Institute resources - <http://www.sans.org/newlook/resources/>

Internet Engineering Task Force – <http://www.ietf.org/>

Internet Architecture Board – <http://www.iab.org/>

Internet Assigned Numbers Authority – <http://www.iana.org/>

Internet Corporation of Assigned Names and Numbers – <http://www.icann.org/>

RIPE NCC – <http://www.ripe.net/>

American Registry for Internet Numbers – <http://www.arin.net/>

Asia-Pacific Network Information Centre – <http://www.apnic.net/>

Latin America and Caribbean Internet Address Registry – <http://www.lacnic.net/>

North America Network Operators Group – <http://www.nanog.org/>