ATTACKS ON IP PROTOCOL

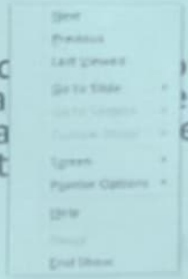
- IP SPOOFING AND IP FRAGMENTATION
- A maximum transmission unit also called as MTU, is a term used in networking and operating systems. It defines the largest size of the packet that can be transmitted as a single entity in a network connection. The size of the MTU dictates the amount of data that can be transmitted in bytes over a network.
- Why MTU size is 1500?
- So where did 1,500 bytes come from? It appears that it is a legacy value originally derived from a combination of hardware limits and a need to choose a value that would play well on shared network segments, witho causing too much transmission latency when busy and not bringing too much header overhead.

IP Spoofing

IP spoofing, or IP address spoofing, refers to the creation of Internet Protocol (IP) packets with a false source IP address to impersonate another computer system. IP spoofing allows cybercriminals to carry out malicious actions, often without detection.

This might include stealing your data, infecting your device with Malware or crashing your server.

It's one of many tools that hackers use to gain access to computers to mine them for sensitive data, turn them into zombies (computers taken over for malicious use), or launch Denial-of-Service (DoS) attacks. Of the different types of spoofing, IP spoofing is the most common.



IP spoofing, or IP adc ofing, refers to the creation of Internet Protocol (IP) packets with a fa e IP address to impersonate another computer system. IP spoofing a ercriminals to carry out malicious actions, often without detect

ATTACKS ON IP PROTOCOL

- IP SPOOFING AND IP FRAGMENTATION
- A maximum transmission unit also called as MTU, is a term used in networking and operating systems. It defines the largest size of the that can be transmitted as a single entity in a network connection. of the MTU dictates the amount of data that can be transmitted in over a network.
- Why MTU size is 1500?
- So where did 1,500 bytes come from? It appears that it is a legacy originally derived from a combination of hardware limits and a nee choose a value that would play well on shared network segments, causing too much transmission latency when busy and not bringin much header overhead.

Internet Layer

- Logical transmission of packets over Internet
- Compared to network layer in OSI model
- Functions of internet Layer
  - Transmits data packet to the link layer
  - Routes the data packets
  - Resemble out-of-order packets
  - Error handling in transmission and fragmentation of data packets

(vi) Again we have the IP datagram which given its identification through the 5^{th} & 6^{th} bytes.

In our packet the 5^{th} & 6^{th} bytes are 00 & 03 respectively

$\therefore$ Identification of the packet $=(0003)_{16}$

$=(0003)_{10}$

(vii) The type of service (TOS) is provided by the DS (differentiated service) field in the IP datagram which has the format

The DS is given in the 2^{nd} byte as $(00)_{16}$ in our datagram

$\therefore$ TOS bits =0000=default

$\therefore$ The type of service provided by the packet is defaul

(iii) We know that

Data size = Total length – header length

Total length $=(54)_{16}$

$= 01010100$

$=(84)_{10}$

Header length = 20 bytes (in decimal)

∴Data size = 84-20 = 64 bytes

(iv) According to the IP datagram format the checksum is provided in the 11^{th} & 12^{th} bytes of the packet

In our datagram the 11^{th} & 12^{th} bytes all 0's which is $(0000)_{16}$

∴The checksum is not used in the given packet.

(iii) We know that

Data size = Total length – header length

Total length $=(54)_{16}$

$= 01010100$

$=(84)_{10}$

Header length = 20 bytes (in decimal)

∴Data size = 84-20 = 64 bytes

(iv) According to the IP datagram format the checksum is provided in the 11^{th} & 12^{th} bytes of the packet

In our datagram the 11^{th} & 12^{th} bytes all 0's which is $(0000)_{16}$

∴The checksum is not used in the given packet.

(vi) Again we have the IP datagram which given its identification through the 5^{th} & 6^{th} bytes.

In our packet the 5^{th} & 6^{th} bytes are 00 & 03 respectively

$\therefore$ Identification of the packet $=(0003)_{16}$

$=(0003)_{10}$

(vii) The type of service (TOS) is provided by the DS (differentiated service) field in the IP datagram which has the format

The DS is given in the 2^{nd} byte as $(00)_{16}$ in our datag

$\therefore$ TOS bits =0000=default

$\therefore$ The type of service provided by the packet is d

Question 1:

An IP datagram has arrived with the following information in header in Hex
450000540003000020060000 7C4E0302B40E0F02.

i) Are there any options?

ii) is the packet fragmented?

iii) What is the size of data?

iv) Is a checksum used?

v) How many more routers can the packet travel to?

vi) What is the identification number of the packet?

vii) What is the type of the service?

Justify your answer with reason.

(v) We know the IP datagram format , the time to live for datagram is given the 9th byte of the IP packet.

In our packet the 9th byte is $(20)_{16}$

$\therefore$ TTL=$(20)_{16}$

=0010 0000

TTL=$(32)_{10}$

$\therefore$The datagram can travel 32 more routers.

(Internet service Provider (ISP) have routeres)

Ans-

(i) Given that IP datagram is

45000054000300002006000007C4E0302

B40E0F02

Now, HLEN=$(5)_{16}$

∴ Header length= 5*4 = 20bytes

Option size = header length- actual header size

Also, option are present after first 20 bytes which is not present in the given datagram

Thus the IP datagram does not have any options

IP datagram is in hex format- drbbm made simple.

45000054000300002006000007C4E0302 B40E0F02

4	5	00	0054	00 03	0 /2 Half bit appr r.	0/ | 000 2 half bit Appr.	20	06	0000
4 bits	4 bits	8 bits	16 bits	16 bits	3 bits	13bits	8 bits	8 bits	16 bits
ver	HLEN	Service type	Total Length	Identification	flags	Fragment offset	Time To live	protocol	Header checksum

7 C4E0302	B40E0F02		
32 bits (Ipv4) :4bytes	128byte(ipv6)		
Source Ip address	Destination ip address	options	data

Bit change may be attack-network attack

Question 1:

An IP datagram has arrived with the following information in header in Hex 45000054000300002006000007C4E0302B40E0F02.

i) Are there any options?

ii) is the packet fragmented?

iii) What is the size of data?

iv) Is a checksum used?

v) How many more routers can the packet travel to?

vi) What is the identification number of the packet?

vii) What is the type of the service?

Justify your answer with reason.