CCIE Security Version 5
Advanced Technologies Class

Copyright © www.ine.com

Fragmentation Attacks

What is IP fragmentation?

What is the fragmentation attack?

What IOS tools can be used to mitigate it?

Copyright © www.ine.com

MTU vs. Datagram Size Overview

- Minimum MTU
  - For IPv4 it's 68 bytes
  - For IPv6 it's 1280 bytes
- Minimum MTU should not be confused with minimum datagram size that any host must be able to accept
  - For IPv4 it's 576 bytes
  - For IPv6 it's 1280 bytes

Copyright © www.ine.com

MTU Overview

▷Default MTU over Ethernet

- 1500 bytes for IPv4
- 1500 bytes for IPv6, as defined in RFC 2464

Copyright © www.ine.com

MTU Overview

- ▷Due to additional encapsulations along the path (MPLS, GRE, IPsec)
  - End-to-end MTU becomes smaller
- ▷How do we prevent packets from being dropped in the transit path
  - Layer 3 packet fragmentation and reassembly
  - MTU adjustment on the end-hosts

Copyright © www.ine.com

Packet Fragmentation

- Packet fragmentation is in general not desired
  - Packet reassembly is computationally expensive and inefficient
  - Major security concerns
- In IPv4
  - Both hosts and routers can perform layer 3 fragmentation
- In IPv6
  - Only hosts can perform layer 3 fragmentation

Copyright © www.ine.com

MTU Adjustment

- In both IPv4 and IPv6 , the MTU can be changed
  - Statically
  - Dynamically
- Dynamic MTU adjustment in IPv4
  - Named Path MTU Discovery, defined din RFC 1191
- Dynamic MTU adjustment in IPv6
  - Named Path MTU Discovery, defined din RFC 1981
  - Hosts can self-adjust MTU based on RA messages

Copyright © www.ine.com

Path MTU Discovery

▷For IPv4

- End-hosts set the ‘**Don’t Fragment Bit’** in the packet
- Transit layer 3 devices drop the packet and send back an ‘ICMP Packet Too Big’ leaking its MTU
- End-hosts adjust the MTU accordingly

Copyright © www.ine.com

Path MTU Discovery

▷For IPv6

- ‘**Don’t Fragment Bit’** is built-in, though it doesn’t exist
- Transit layer 3 devices drop the packet and send back an ‘ICMP Packet Too Big’ leaking its MTU
- End-hosts adjust the MTU accordingly

Copyright © www.ine.com

Path MTU Discovery

- Due to ICMP being in general filtered, Path MTU Discovery may not work
  - In IPv4, routers will fragment and traffic will work
  - In IPv6, routers cannot fragment and traffic will be dropped
- An alternate method for PMTUD has been proposed in RFC 4821
  - Not really implemented

Copyright © www.ine.com

Fragmentation Attacks

- Based on TCP, UDP, ICMP fragments:
  - https://en.wikipedia.org/wiki/IP_fragmentation_attack
  - https://en.wikipedia.org/wiki/Denial-of-service_attack
- DDoS fragmentation attack examples
  - Teardrop
  - Nuke
  - Rose

Copyright © www.ine.com

Fragmentation Attack Mitigation

- Methods defined in RFC 1858
- IOS Mitigation Tools
  - ACL Filtering
  - Rate-limit (CAR – Committed Access Rate)
  - Policing (successor of CAR)
  - Unconditional packet discard via MQC (ACL/NBAR)
  - Virtual Fragmentation Reassembly
  - Zone-Based Policy Firewall

Copyright © www.ine.com

Knowledge is Power!

Copyright © www.ine.com