NETWORK ATTACKS

INFO 310

THE NETWORK

- Connects all of the things
- Attacks either:
  - Target the network itself (BGP Sink Hole)
  - Manipulate the network to target a host (MITM)
  - Are used to carry an attack to a host (DDoS attacks)
- As new protocols and means of communication are adopted the attack surface and capabilities change

TARGET THE NETWORK – BGP SINK HOLE

- BGP – Border Gateway Protocol
  - Used to exchange routing information between autonomous systems
  - Connects ISPs together
  - BGP neighbors are "peers"
  - Peers update each other with routes
  - It is a system built on trust

TARGET THE NETWORK – BGP SINK HOLE

- IP address
  - 32 bits
  - 4 x 8 bit bytes
  - Usually written like -> 11.22.33.44
  - Range from 0.0.0.0 to 255.255.255.255
- Subnet mask
  - A smaller piece of an IP range
  - Devices in a subnet share a common most-significant bit-group

TARGET THE NETWORK – BGP SINK HOLE

- IP address A: 192.168.1.1
- IP address B: 192.168.1.2
- IP address C: 192.168.2.3

TARGET THE NETWORK – BGP SINK HOLE

- IP address A: 192.168.1.1
  - Subnet: 255.255.255.0
- IP address B: 192.168.1.2
  - Subnet: 255.255.255.0
- IP address C: 192.168.2.3
  - Subnet: 255.255.255.0

TARGET THE NETWORK – BGP SINK HOLE

- IP address A: 192.168.1.1
  - Subnet: 255.255.0.0
- IP address B: 192.168.1.2
  - Subnet: 255.255.0.0
- IP address C: 192.168.2.3
  - Subnet: 255.255.0.0

TARGET THE NETWORK – BGP SINK HOLE

- IP address A: 192.168.63.1
  - Subnet: 255.255.0.0
- IP address B: 192.168.31.2
  - Subnet: 255.255.0.0

TARGET THE NETWORK – BGP SINK HOLE

- Subnet: 255.255.224.0 /19
  - Binary: 11111111.11111111.11100000.00000000
- IP address A: 192.168.63.1
  - Binary: 11000000.10101000.00111111.00000001
  - Binary: 11111111.11111111.11100000.00000000
- IP address B: 192.168.31.2
  - Binary: 11000000.10101000.00011111.00000010
  - Binary: 11111111.11111111.11100000.00000000
- IP address B: 192.168.34.2
  - Binary: 11000000.10101000.00100010.00000010
  - Binary: 11111111.11111111.11100000.00000000

TARGET THE NETWORK – BGP SINK HOLE

- Pakistan decides it does not want its citizens to access Youtube.com because there is an offensive video there and they decide their 182 million citizens simply can't handle themselves like adults
- They don't own the domain
- They can remove the DNS records for the ISPs they control, but people can use external ISPs like Google's
- They can firewall off the site but that requires a lot of hardware (see China)
- They decide to change their BGP table to "sink hole" the site and take it offline

TARGET THE NETWORK – BGP SINK HOLE

- Youtube has the address block: 208.65.152.0/22 (208.65.152.0 - 208.65.155.255)
- Pakistan Telecom advertises the block: 208.65.153.0/24 (208.65.153.0 - 208.65.153.255)
- A /24 subnet (255.255.255.0) is a "longer match" than /22 (255.255.252)
- Because Pakistan Telecom's block is more specific their routes take priority and traffic flows to their network where it is dropped
- Can you think of how to prevent this?
- Can you think of legitimate uses for this?

MORE INFO

- https://www.wired.com/2008/02/pakistans-accid/
- https://arstechnica.com/uncategorized/2008/02/insecure-routing-redirects-youtube-to-pakistan/

MANIPULATE THE NETWORK - MITM

- https://www.youtube.com/watch?v=hI9J_tnNDCc

- If you want to learn more:
  - https://www.youtube.com/watch?v=VvIn4_HfIVg
  - https://www.youtube.com/watch?v=tW_NMG2IZ5s
  - https://www.youtube.com/watch?v=gNhyjPxuy5w
  - https://www.youtube.com/watch?v=qzNv6e1z1_E

MANIPULATE THE NETWORK - MITM

- What can you do now that you are in the middle of the connection?

MANIPULATE THE NETWORK - MITM

- Intercept traffic
- Manipulate traffic
- SSL Strip
- DNS Spoofing

ATTACK OVER THE NETWORK - DDOS

- Dinner reservation example
- IP Spoofing
- NTP/DNS amplification
- IoT DDoS
- Go read (seriously) - https://idea.popcount.org/2016-09-20-strange-loop---ip-spoofing/