Today’s outline

- NAT, Firewalls
- IDS
- DDoS

TCP/IP Protocol Stack

Application protocol (e.g. HTTP) → TCP protocol → IP protocol → Data

Basic Firewall Concept

- Separate local area net from internet

Firewall goals

- Prevent malicious attacks on hosts
  - Port scan, syn flooding, ...
  - Worm propagation
    » Exploit buffer overflow in program listening on network
- Provide defense in depth
  - Defend everywhere
  - Programs contain bugs and are vulnerable to attack
  - Network protocols may contain:
    » Design weaknesses (SSH CRC)
    » Implementation flaws (SSL, NTP, FTP, SMTP...)

Packet Filtering

- Uses transport-layer information only
  - IP Source Address, Destination Address
  - Protocol (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type
- Examples
  - DNS uses port 53
    » Block incoming port 53 packets except known trusted servers
- Issues
  - Stateful filtering
  - Encapsulation: address translation, other complications
  - Fragmentation
Packet Filtering Examples

- Policy: Do not allow outbound email
  - Implementation?
- Policy: Do not allow inbound connections
  - Implementation?
- Policy: Do not allow HTTP GET requests
  - Implementation?

Normal IP Fragmentation

Flags and offset inside IP header indicate packet fragmentation

Abnormal Fragmentation

Low offset allows second packet to overwrite TCP header at receiving host

NAT: Network Address Translation

All datagrams leaving local network have same single source NAT IP address: 138.76.29.7, different source port numbers

Advantages of NAT

- Motivations for NAT
  - Limited address space
  - Prevent unsolicited inbound requests
    » Port numbering: host behind NAT not reachable as server
  - Avoid renumbering if provider changes
    » Small/mid-sized LANs inherit address space from ISP
- Addresses hidden by NAT
  - Normal routing
    » Outgoing msg from 171.64.78.90 contains sending address
    » Recipient or observer can access 171.64.78.90
  - Addressing with NAT
    » NAT rewrites outgoing packet so recipient sees public addr only
    » An outside computer cannot see 171.64.78.90
Stateful or Dynamic Packet Filtering

Application layer (HTTP)

- Turn click into HTTP request

April 20, 2011

Transport layer (TCP)

- Break message into packets (TCP segments)
- Should be delivered reliably & in-order

General intrusion detection

- Many intrusion detection systems
  - Close to 100 systems with current web pages
  - Network-based, host-based, or combination
- Two basic models
  - Misuse detection model
    » Maintain data on known attacks
    » Look for activity with corresponding signatures
  - Anomaly detection model
    » Try to figure out what is “normal”
    » Report anomalous behavior
- Fundamental problem: too many false alarms

April 20, 2011

Intrusion Detection

- Attacks can be OS specific
  - Bugs in specific implementations
  - Oversights in default configuration
- Attacker scans network to find vulnerabilities
  - Port scan tries many ports on many IP addresses
  - If characteristic behavior detected, mount attack
    » SGI IRIX responds TCPMUX port (TCP port 1)
    » If machine responds, SGI IRIX vulnerabilities can be tested and used to break in
- Port scan activity can be detected
IDS Circumvention

- IDS circumvention
- Outsource vulnerability detection
  » Live demo!
- Obfuscate attack code

(D)DoS

- (Distributed) Denial of Service Attack
- Anything that keeps legitimate users away
- Dumb, Smart, & in between

Floods

- Lots of Packets – works!
- ICMP Ping Flood
- Syn Flood
  Resource Exhaustion Attack
  Start TCP handshake; never finish

Syn Flood Mitigation

- Problem: syn queue overflow
- Intuition: ACK must include (server’s ACK#+1) as client’s ACK#
- Solution: encode a secret value in the ACK#
  - Initial ACK# = (time) * (MSS) * s(serverip, serverport, clientip, clientport, t)
  - Server can reconstruct & verify all information from SYN using cookie value

Reflection Attack

- Problem: Source & Destination address fields in IP packets not authenticated
- Problem: When receiving unexpected SYN, must respond with RST
- Attack: Set SRC=target, DST=any, FLAGS=syn
- What happens?
Aside: Backscatter

- Source spoofer – usually picks a random source address
- Individual IP vantage point – looks like noise
- Large segment of IPv4: can see attacks

Questions?

- As an attacker:
  - Manipulate assumptions
  - Use Rice’ s Theorem to your advantage
  - Use old attacks in new domains
- As a defender:
  - Defense in depth
    - Trust once, verify everywhere
  - Randomize anything that could be guessed
  - Think like an attacker :)

Application level DDoS

- IRC Botnet
- Voluntary Botnets
  - LOIC
  - slowloris