Attacks on Intrusion Detection and Prevention

COMP 435
Fall 2017
Prof. Cynthia Sturton

Based on lectures given in Berkeley's CS161: Computer Security, http://www-inst.cs.berkeley.edu/~cs161/.

Poster Presentations

- Group info submitted (Google Form) by Tues., Oct. 31
- Group topic submitted (Sakai) by Wed., Nov 8
- Poster PDF submitted (Sakai) by Wed., Nov. 29
- Poster session in class on Wed., Dec. 6

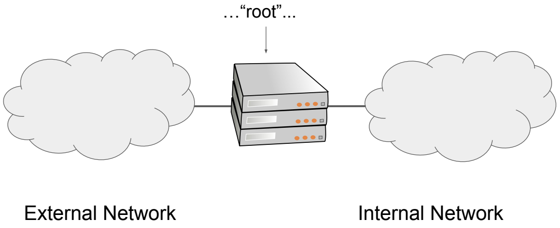
Attacking Packet Filters

- Exploit assumptions made by packet filter

Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
In	121.12.1.1	222.2.2.2	TCP	8080	Allow
Out	222.2.2.2	121.12.1.1	TCP	5150	Allow

Signature-based Filters

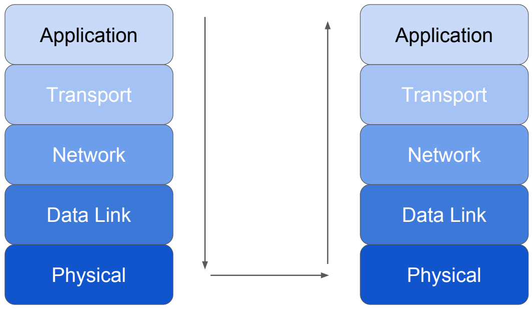
- Inspect the payload to find patterns on known attacks
    - E.g.,: Look for “root”
    - E.g.,: Look for “/etc/passwd”



…"root"...

External Network

Internal Network



Application

Transport

Network

Data Link

Physical

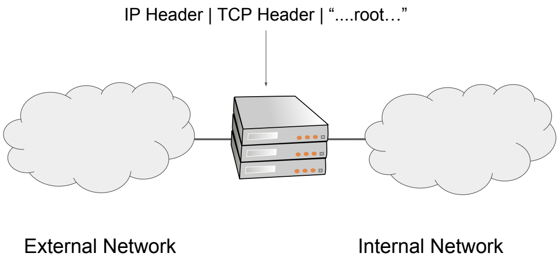
Application

Transport

Network

Data Link

Physical

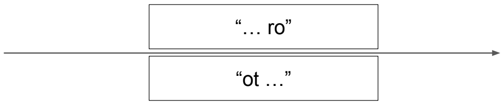


IP Header | TCP Header | "....root…"

External Network

Internal Network

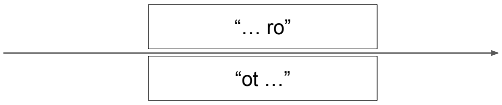
Attacking Signature-based Filters



"… ro"

"ot …"

Attacking Signature-based Filters

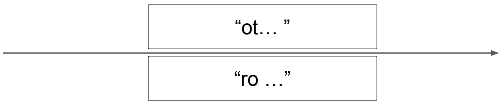


"… ro"

"ot …"

Fix: Track sequences of packets

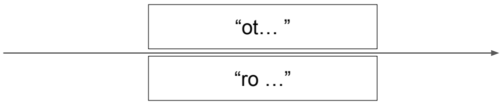
Attacking Signature-based Filters



"ot… "

"ro …"

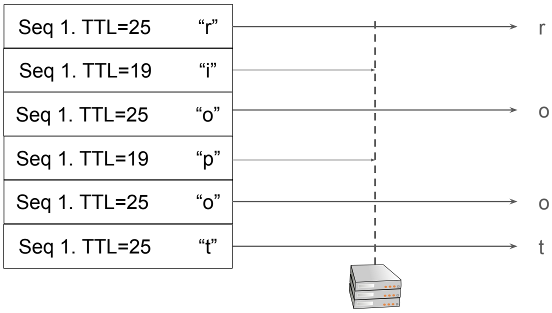
Attacking Signature-based Filters



"ot… "

"ro …"

Fix: Re-assemble TCP stream



Seq 1. TTL=25 "r" → r

Seq 1. TTL=19 "i"

Seq 1. TTL=25 "o" → o

Seq 1. TTL=19 "p"

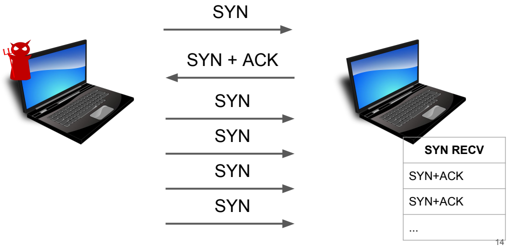
Seq 1. TTL=25 "o" → o

Seq 1. TTL=25 "t" → t

Attacking IDPS

- Code Injection
- DOS

SYN Flood: Attack on TCP Protocol



SYN RECV
SYN+ACK
SYN+ACK
...

Network vs Host Based IDPS

- Network
  - Covers many machines at once
  - Doesn’t touch end points
  - Doesn’t consume end-point resources
  - Single purpose
- Host
  - Direct visibility of end-point behavior
  - Not blocked by encryption
  - Less traffic