Insertion, evasion, denial-of-service, and other network tomfoolery
Intrusion Detection System (examples are Bro or Snort)

Gateway Router

Port mirror

IDS

Machines on the network that should be protected (perhaps passively)

The Nasty, Terrible, Internet
IDS is looking for signatures

• Typically regular expressions, like ".*<script>.*</script>.*" appearing in an input to a web form, indicating a Javascript XSS attack.

• How can we (the attacker) get the IDS to see one thing and the victim to see another?

• A stupid example: Great Firewall of China censors “GET falungong.html”, but if you send two packets: “GET fa” and “lungong.html” the endhost reassembles them fine but the GFW is fooled.

• Or, “GET fa%61lungong.html”
A not so useful distinction

Figure 4: Insertion of the letter 'X'

Figure from Ptacek and Newsham
A not so useful distinction

Figure 5: Evasion of the letter 'A'

Figure from Ptacek and Newsham
“Information only has meaning in that it is subject to interpretation”

—Computer Viruses, Theory and Experiments by Fred Cohen, 1984
“The only laws on the Internet are assembly and RFCs”

–Phrack 65 article by julia@winstonsmith.info
IP reassembly

- Routers (or endhosts, if they want) can break IP packets up into fragments that the receiver has to reassemble
- Ambiguity in the way overlapping IP fragments are put back together into an IP packet
- All of the following images were plagiarized from:
  
  https://www.sans.org/reading-room/whitepapers/detection/ip-fragment-reassembly-scapy-33969
Figure 1: 6 Fragmented Packets (Shankar & Paxson, 2003)(Novak, 2005)

Reassembled using policy: First (Windows, SUN, MacOS, HPUX)

Reassembled using policy: Last/RFC791 (Cisco)

Reassembled using policy: Linux (Linux)

Reassembled using policy: BSD (AIX, FreeBSD, HPUX, VMS)

Reassembled using policy: BSD-Right (HP Jet Direct)

Figure 2: 5 Reassembly Methods (Shankar & Paxson, 2003)(Novak, 2005)
Step 1 - Attacker Crafts Linux and Windows Exploit fragments targeting a Windows host.

Step 2 - IDS correctly assembles packets as the target host would and alerts that the attack has occurred.

IDS VIEW

Windows on Windows. Successful attack ALERT!!!

Step 3 - Analyst Examines the full packet capture, sees a Linux exploit targeting Windows and dismisses the false positive.

ANALYST VIEW

Linux on Windows failed attack. Stupid IDS. Next packet!!

ATTACKER VIEW

Windows Exploit
Linux Exploit

Figure 3: Views of the attacker, IDS and analyst.
Figure 4: Wireshark uses BSD reassembly technique
TCP is even worse...

- From
  http://www.icir.org/vern/papers/TcpReassembly/
Another example: TTL limiting

- Victim is 10 hops away from you (the attacker)
- IDS is 7 hops away from you, 3 from the victim
- Send a SYN with TTL 64
- Get a SYN/ACK from the victim
- Send a RST with TTL 9
- Send an ACK with TTL 64
- Victim sees SYN, sends SYN/ACK, gets ACK, you have an open connection and can send them data
- IDS sees SYN in one direction, SYN/ACK in the other, then RST and assumes the connection was reset, ACK and all packets that follow (with data) are ignored by the IDS
A layer 7 example (XSS) due to Jeff Knockel

- Suppose "<script>...</script>" is blacklisted
- Use "<script>..." instead, many browsers will happily run the script anyway despite the missing closing tag
- Information only has meaning in that it is subject to interpretation
  - IDS interprets things one way, web browser another
Physical layer injection

- From

Figure 2: A typical packet’s interpretation contrasted with that of a PIP.
Denial-of-Service (DoS) for IDS

• Exhaust the IDS's resources in some way
  – CPU
  – Memory
  – Bandwidth
• Fail-open (just let stuff through) vs. fail-closed (slow down the network)
• Example: On accident, Tony brought down the Computer Science Dept. network
• Other examples
DoS in general

- Exhaust some kind of resource, e.g.:
  - Optimistic ACK to exhaust bandwidth
  - PING of death (large PING) causes crash
  - Exhaust CPU in layer 7
  - More examples: http://www.isi.edu/~mirkovic/bench/attacks.html
  - SYN flood: Older hosts had either a fixed amount of half-open connections they could keep track of or no limitations at all, attack is to send lots of SYNs and never ACK or RST
    - Defenses: SYN backlog policies and SYN cookies
SYN cookies and SYN backlogs

- **SYN cookies**
  - Special kind of SYN/ACK
  - See [https://cr.yp.to/syncookies.html](https://cr.yp.to/syncookies.html)
  - Can confirm ACK number and reconstruct the necessary state for a connection without having kept any state after sending the SYN cookie

- **SYN backlog examples**
  - Linux reserves $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}$th, and so on for successively older SYNs, prunes 5 times a second
  - FreeBSD has 512 buckets of 30, you can't predict what bucket you fall into (in theory)
Resources

- Ptacek and Newsham, Insertion Evasion and Denial of Service: Eluding Network Intrusion Detection