

Evasion techniques



Cyberdefense Seminar 2011

Franck Gigant - 113533IV

Introduction

- ▶ 1995: IDS became popular
- ▶ Attacks could be detected
- ▶ Lead to evasion techniques



Summary

- I. Definition
- II. Examples
- III. How to fight it
- IV. Conclusion



- ▶ First apparition in 1998 in a research paper by Thomas Ptacek and Timothy Newsham
- ▶ Evasion techniques are a means to disguise and/or modify cyber attacks to avoid detection and blocking by information security systems.

- ▶ TCP/IP: RFC 791 (1981) p. 23

The implementation of a protocol must be robust. Each implementation must expect to interoperate with others created by different individuals. While the goal of this specification is to be explicit about the protocol there is the possibility of differing interpretations. **In general, an implementation must be conservative in its sending behavior, and liberal in its receiving behavior.** That is, it must be careful to send well-formed datagrams, but must accept any datagram that it can interpret (e.g., not object to technical errors where the meaning is still clear).

- ▶ Advanced evasions techniques

Some simple evasion techniques:

▶ Pattern-Matching Weaknesses

Pattern:

GET /cgi-bin/phf?

Obfuscation:

GET /cgi-bin/aaaaaaaaaaaaaaaaaaaaa/..%25%2fp%68f?

▶ Unicode Evasion Techniques

Multiple representations of a single character:

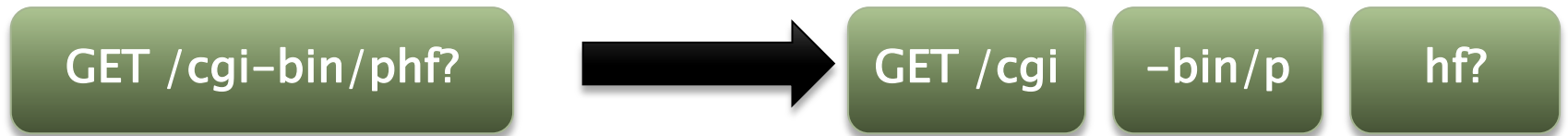
'\ ' can be represented as 5C, C19C and
E0819C

- ▶ Denial of Service (DoS) Attacks

Crashing log server, or flood it with false positives.

That way, attacks could go unnoticed.

▶ Session Splicing



Some complex evasion techniques:

▶ Fragmentation

Use the sequence number of different protocols
Overlap:

Packet 1:
GET /cgi-bin/

Packet 2:
aaaaaaaaaaaaaaaaaaaaaaaa/../../phxx

Packet 3:
f?

- ▶ Fragmentation (2)

Overwrite:

Packet 1:

GET /cgi-bin/

Packet 2:

some_normal_filename.cgi

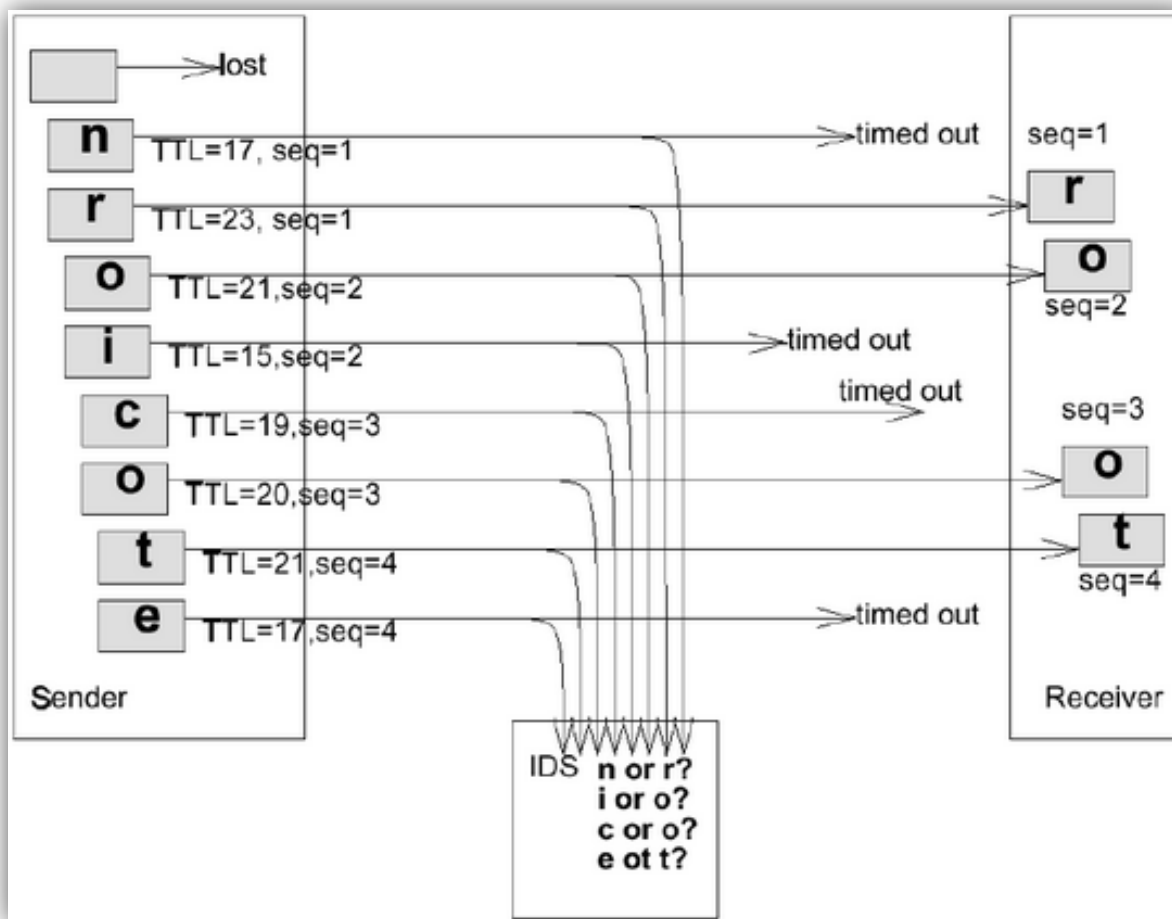
Packet 3:

/aaa/../../aaa/../../aaa/../../phxx

Packet 4:

f?

▶ Time-To-Live Attacks:



▶ Invalid RST Packets:

- TCP protocol use RST packets to end two-way communications
- TCP protocol use checksum to ensure that communication is reliable

▶ Polymorphic Shellcode:

- Most IDSs contain signatures for commonly used strings within shellcode
- Create a code that is able to encode and decode itself

- ▶ Centralized management
- ▶ Normalization
 - Unicode / UTF8
 - Fragmented packets
 - Time-to-live field
- ▶ Packet Interpretation Based on Target Host

- ▶ Hackers have the advantage
- ▶ Evasion techniques have to be taken seriously
 - Prolonging viruses lives
 - Hackers are ready to spend money in
- ▶ A lot of IPS still not detect from evasion techniques

Questions?

