Degree of freedom in conntrack helpers

Éric Leblond

August 22th 2011

Introduction

- Which degree of freedom are offered by conntrack helper
- Can client open everything on a server ?
- In Patrick we trust
- but let's check

Principle

- look at nf_ct_expect_init in helper code
- study which argument are used
  - if variable is build from conntrack entry
  - if variable is build from header data
  - if variable is build from packet data
- determinate degree of freedom
  - Which range of ports ?
  - Is protocol a variable ?

Current results

Helper lists

Module	Source address	Port Source	Destination address	Destination port	Protocol	Option
amanda	Fixed	0-65535	Fixed	In CMD	TCP	
ftp	Fixed	0-65535	In CMD	In CMD	TCP	Loose = 1 (default)
ftp	Full	0-65535	In CMD	In CMD	TCP	Loose = 0
h323	Fixed	0-65535	Fixed	In CMD	UDP	
h323 q931	Fixed	0-65535	In CMD	In CMD	UDP	
irc	Full	0-65535	Fixed	In CMD	TCP	
netbios_ns	Network connected to iface	Fixed	Fixed	Fixed	UDP	
pptp	Fixed	In CMD	Fixed	In CMD	GRE	
sane	Fixed	0-65535	Fixed	In CMD	TCP	
sip rtp_rtcp	Fixed	0-65535	Fixed	In CMD	UDP	sid_direct_media = 1 (default)
sip rtp_rtcp	Full	0-65535	In CMD	In CMD	UDP	sid_direct_media = 0
sip signalling	Fixed	0-65535	Fixed	In CMD	In CMD	sip_direct_signalling = 1 (default)
sip signalling	Full	0-65535	In CMD	In CMD	In CMD	sip_direct_signalling = 0
tftp	Fixed	0-65535	Fixed	In Packet	UDP	

Good result

- Server message trigger opening of their own port
- Dangerous protocol features:
  - Are disabled by default
  - Can be enabled via /proc

Yellow card was sometimes not far

- Some modules had problems
- This is the case of FTP

```
/* Thanks to Cristiano Lincoln Mattos
   <lincoln@cesar.org.br> for reporting this potential
   problem (DMZ machines opening holes to internal
   networks, or the packet filter itself). */
if (!loose) {
ret = NF_ACCEPT;
goto out_put_expect;
}
daddr = &cmd.u3;
```

No declaration

- There is nothing but review to check the degree of freedom
- Manual check required a labs
  - Server is needed to reproduce the trafic
  - Client also
- No document exist to describe the degrees of freedom
- Manual checking is error prone

No homogeneity

- Some modules have good protection, other not:
  - SIP module has > 1024 port limit
  - FTP has none

Document

- Add a file to Documentation in kernel source
  - Document options in /proc
  - Document degree of freedom
- Require from new helper have fill in information before patch acceptation

Automatized tests

- Need infrastructure
- Need dev power
- How to script

Discussion

- Who's volunteer ?
- For what ?