Securing the Enterprise with Netfilter

Linux World Summit 2005

Michael Rash
Security Research Engineer
Enterasys Networks, Inc.

05/25/2005
Enterprise Requirements

- Features
- Manageability
- Stability
- Speed
- Scalability
- Support
- Cost
History of Netfilter

- ipfwadm (kernels 1.2.x - 2.0.x)
- ipchains (kernels 2.2.x)
- iptables (kernels 2.4.x - 2.6.x)

Enabled by default in the 2.6.x series
Netfilter Development Cycle

- Active developer community
- High traffic mailing lists
- Frequent releases

http://www.netfilter.org/
Filtering

- Kernel hooks within networking stack
- IP/Network
- Protocol
- Port Numbers
- TCP flags
- Mac addresses
- TOS
Network Address Translation (NAT)

- Source NAT (SNAT)
- Masquerading
- Destination NAT (DNAT)
Logging

Mar 26 10:54:00 orthanc kernel: DROP
IN=eth1 OUT=
MAC=00:0c:41:24:68:ef:00:80:c8:05:5b:af:08:00
SRC=192.168.10.2 DST=192.168.10.1
LEN=60 TOS=0x00 PREC=0x00 TTL=63
ID=9465 DF PROTO=TCP SPT=12296
DPT=65531 WINDOW=5840 RES=0x00 SYN
URGP=0 OPT
(020405B40402080A00047BC80000000001030302)
Logging (cont'd)

- Passive OS fingerprinting:

  192.168.10.2: Linux:2.6::Linux 2.4/2.6

  http://lcamtuf.coredump.cx/p0f.shtml
  http://www.cipherdyne.org/psad/
Netfilter State Tracking

- TCP (window tracking not enabled by default)
- UDP
- ICMP
Netfilter Modules

• New features
• Flexible architecture
• Disabling unneeded code
String Match Module

- Application layer string matching
- Example: Stopping the NAVIDAD worm:

```bash
# iptables -A INPUT -p tcp --sport 110 -d 192.168.10.1 -m string --string "NAVIDAD.EXE" -j REJECT --reject-with tcp-reset
```
ULOG Module

- Flexible logging daemon
- pcap output
- mysql output
TARPIT Module

- Effective defense against worm traffic
- Wastes TCP resources of the attacker

```
# iptables -A INPUT -p tcp --dport 6776 -j TARPIT
```
VPN

- Not integrated with Netfilter directly, but good solutions exist:
  - FreeS/WAN (now OpenSWAN, StrongSWAN)
    - ipsec
    - opportunistic encryption
  - OpenVPN
    - SSL
    - ported to Windows
Routing

• Quagga Routing Suite
  – ospf
  – rip
  – bgp

• Netfilter ROUTE target
Network Failover

- Keepalived implementation of VRRP
- Sync group across all member interfaces
- Email alerting
- Custom script execution

http://www.keepalived.org/
State Table Synchronization

- Not currently available
- Netfilter-failover project in development
Managing Netfilter

- Command line interface
- Easily scripted
- Easy version control and policy difference viewing
- `iptables-save` / `iptables-restore`
Fwbuilder

- Full GUI support for Netfilter
- Generates shell scripts
- NAT, logging, and state tracking are all supported
- Detection of rule shadowing
- Supports bridging policy
Fwbuilder Screenshots

- See accompanying files:
  - fwbuilder_policy.png
  - fwbuilder_nat.png
  - fwbuilder_options.png
Netfilter Performance

- Linux TCP/IP stack is fast
- GB/sec speeds are achievable

http://www.benzedrine.cx/pf-paper.html
Scalability

- Thousands of rules supported
- Simple shell scripts and iptables-save files simplify Netfilter deployment across multiple systems
- Linux 2.6.x implies Netfilter is already there
Upgrades

- Userland iptables binary
- Netfilter kernel modules
Support

- Difficult to purchase
- Rely on quality of open source
- Rely on responsiveness of community
Price

- Hard to beat. :)
Conclusion

- Netfilter is feature-ready for the Enterprise
- Performance, manageability, and support may not be as good as proprietary vendors, but may be good enough
- Hardware is cheap
- Low cost may make the difference