CanSecWest/core03

SÉCURITÉ.ORG

Router forensics DDoS/worms update

Nicolas FISCHBACH
Senior Manager, IP Engineering/Security - COLT Telecom
nico@securite.org - http://www.securite.org/nico/

version 1.01

we make business straight.forward

CanSecWest/core03

Agenda

- **Router architecture**
  - > Hardware, memory and IOS
- **Configuration**
  - > Logging and Integrity checking
- **Incident**
  - > Evidence
  - > Environment
- **Denial of Service**
  - > Attacks and Detection
  - > Trends
- **Conclusion**

SÉCURITÉ.ORG

CanSecWest/core03

Router architecture (1)

» **Hardware**

> Depending on the model/series (at least)

- mother board
- CPU (RISC - MIPS or Motorola)
- memory
- bus
- I/O interfaces

> Becomes much more complex (GSR for example)

- distribute tasks (CPU takes only care of basic “running the system” tasks and not routing/forwarding)
- Line Card (own CPU), Engines, etc.
- ASICs

CanSecWest/core03

Router architecture (2)

» **Memory**

> Flash (non volatile)

- contains the (compressed) IOS image and other files

> DRAM/SRAM (volatile)

- contains the running IOS
- store the routing table(s), statistics, local logs, etc.
- divided into regions (processor, I/O, I/O 2).

> NVRAM (non volatile)

- contains the startup configuration (*startup-config*)
- *boot config <file system><config>* configures an alternative location

> BootROM

- contains the ROMMON code (POST, IOS loading, etc.)

CanSecWest/core03

Router architecture (3)

» **IOS**
> Proprietary, closed source OS running on RISC CPUs
> Closed source, closer to a "port" than a "fork" from (BSD) Unix (zlib, ssh, SNMP bugs, etc.)
> ELF 32-bit MSB executable, statically linked, stripped
> IPCs for communications between the RP (Route Processor and the LCs (Line Cards) on the GSR series

"Inside Cisco IOS software architecture" - Cisco Press :
- "In general, the IOS design emphasizes speed at the expense of extra fault protection"
- "To minimize overhead, IOS does not employ virtual memory protection between processes"
- "Everything, including the kernel, runs in user mode on the CPU and has full access to system resources"

CanSecWest/core03

Router architecture (4)

» **Cisco IOS rootkit/BoF/FS : open questions/issues**
> No (known) local tools/command to interact and "play" with the kernel, memory, processes, etc.
- What is possible with gdb (gdb {kernel¦pid pid-num}) ?
- Is the ROMMON a good starting point (local gdb) ?
> What can be done in enable engineer mode (Catalyst) ?
> Is it possible to upload a modified IOS image and start it without a reboot ?
> A lot of different images exists and are in use - what kind of tool would be needed ?
> What will happen with IOS-NG (support for loadable modules) ?

CanSecWest/core03

Router configuration (1)

» **Before going live**

> Turn off all the unneeded services

- See “Protecting your IP network infrastructure”, slides 44+
- New features in 12.3
  - . auto-secure script
  - . local accounting in XML format

> Lots of data are volatile: log/poll as much as you can (but keep CPU and/or memory impact in mind)

- (authenticated) NTP sync.
- run syslog (local, size limited buffer)
- log events generated by services (routing protocols for ex.)
- SNMP traps/poll
- AAA logs and events
- ../..

CanSecWest/core03

Router configuration (2)

» **Before going live (cont.)**

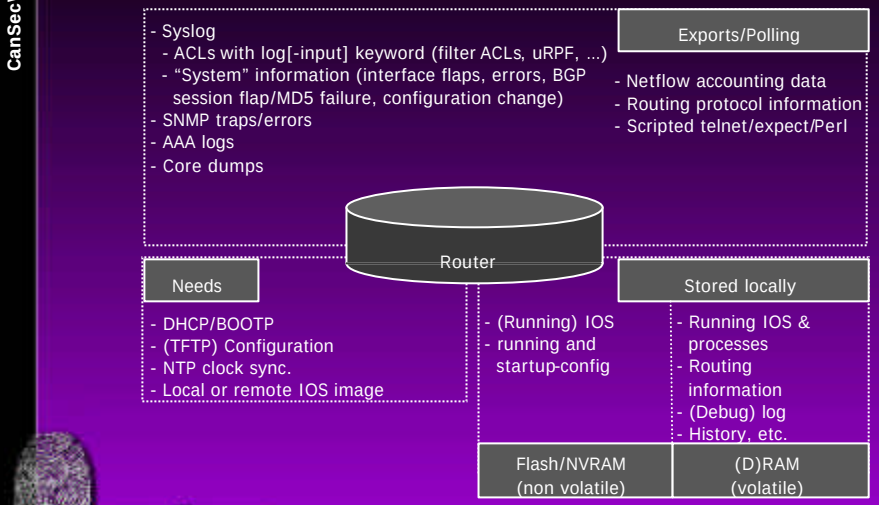
> Lots of data are volatile: log/poll as much as you can (but keep CPU and/or memory impact in mind)

- Netflow accounting flows
- core dump (automatic upload)
- ACLs (filtering and application/service access control)
- *config-register* (Configuration Register) - 0x2102
- scheduler tuning
- *debug sanity* (checks on malloc/free, performance impact)

CanSecWest/core03

Router configuration (3)

» **Available data and elements**



CanSecWest/core03

Integrity checking (1)

» **Four steps to build a tripwire-like for IOS/CatOS**

> 1. Store your routers and switches configurations in a central (trusted and secure) repository (CVS for example)

> 2. Get the configuration from the device (scripted telnet, Perl, expect, tftp, scp, etc.) or have the device send you the configuration (needs a RW SNMP access - not recommended)

```
snmpset -c <community> <router's IP> .1.3.6.1.4.1.9.2.1.55.<TFTP server's IP> s <file>
```

> 3. Check : automatically (cron/at job), when you see "configured by <xyz>" or a router boot in the logfile or when you get the "configuration changed" SNMP trap

> 4. Diff the configuration with your own script or use tools like CVS, Rancid, CW, etc.

CanSecWest/core03

Integrity checking (2)

» **Limitations and details**

> You still have to trust the running IOS/CatOS (no Cisco "rootkit" yet) and your network (MITM attacks)

> The configuration is transmitted in clear text over the network (unless you use scp or IPsec to encrypt the traffic)

> Do not forget that there are two "files": startup-config and running-config

> Do the same for the IOS/CatOS images

> Cisco MIBs : CISCO-CONFIG*

CanSecWest/core03

Incident (1)

» **Decisions**

> Depending on your network architecture: effect on the network availability

- no routing/forwarding
- cold/hot spare (flash, NPE/RP, LC, etc.)

> How to connect ?

- Telnet/SSH or via the console or serial port ?

> What needs to be done before and after reboot

- local logs and (enable) commands to use
- which configuration register to use (*config-register*) ?

> If you can't connect/change to *enable* mode on the router ?

- password reset/recovery
- *nmap*, *snmpwalk*, etc.
- network environment

CanSecWest/core03

Incident (2)

» **Commands to use**

> Make sure you save all the commands and output !

> Avoid entering the configuration mode

> "enable"/"user" EXEC mode ?

Configuration and users

show clock detail
show version
show running-config
show startup-config
show reload
show users/who

Local logs, process and memory

show log/debug
show stack : stack state
show context : stack information
show tech-support : incomplete
show processes {cpu, memory}
content of *bootflash:crashinfo*

Network informations

show ip route
show ip ospf {summary, neighbors, etc)
show ip bgp summary
show cdp neighbors : Cisco Discovery Protocol
show ip arp
show {ip} interfaces
show tcp brief all
show ip sockets
show ip nat translations verbose
show ip cache flow : Netflow
show ip cef : Cisco Express Forwarding
show snmp {user, group, sessions}

File systems

show file descriptors: lsof like
show file information <url>: file like

SÉCURITÉ.ORG

13

CanSecWest/core03

Incident (3)

» ***debug* mode**

» **Flash memory**

> Details on the content (files, state, type, CRC, etc)

- *show <file system>*

> Ciscoflash: ftp://ftp.bbc.co.uk/pub/ciscoflash/

» **DRAM/SRAM**

> Informations on memory regions

- *show buffers*
- *show memory*
- *show region*

» **NVRAM**

> Information about the startup configuration/mode

- *show bootvar*

SÉCURITÉ.ORG

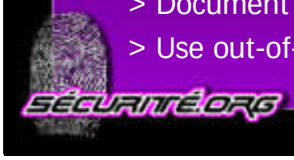
14

CanSecWest/core03

Incident (4)

» **Environment**
  > Application logs
    - syslog, TACACS, NMS, etc.
  > Side effect on network traffic and the infrastructure ?
  > Network traces
    - IDS
    - Mirror (SPAN) port on a switch (depending on the architecture)
    - Netflow exports
    - In-line devices/taps

» **General recommendations**
  > Document and date every single step
  > Use out-of-band communications as much as possible



CanSecWest/core03

Denial of Service (1)

» **Limited resources**
  > Link bandwidth
  > CPUs cycles and memory
  > Queue sizes
  > Forwarding performance vs “received” packets processing

» **Detection and mitigation**
  > Data-center vs core infrastructure approach
    - Data-center (“in-line”)
    - Infrastructure (Netflow)
  > Detection
    - ACLs and queue counters
    - Netflow based
    - NMS (CPUs, interface counters, etc)
    - Customers

CanSecWest/core03

Denial of Service (2)

» **Detection and mitigation (cont.)**
  > Mitigation
    - ACLs and CAR
    - null0 routing (blackholing) , sinkhole routing, traffic rerouting and “cleaning” (using routing protocols or MPLS VPNs)
    - De-aggregate block and stop to announce specific prefixes
    - Mark with special community
  > Traceback
    - ACLs
    - Netflow
    - source-tracking feature
    - null0 interface counters
    - etc.

CanSecWest/core03

Denial of Service (3)

» **Impact on the Internet**
  > Propagation speed
  > Routing stability
  > Default free routing in the core (magnet) ?
  > Large scale filtering: “transit network” vs ”large firewall”

» **(Latest) type of attacks**
  > Attacks
  > “Special” small packets vs large packets
  > Propagation speed
  > Built-in “intelligence” (random vs targeted propagation)
  > Network/routing protocol stability
  > Active bots and botnets

CanSecWest/core03

Denial of Service (4)

» **Trends**
  > Attacks shifting from end systems towards core devices/infrastructure routers
    - ACLs, queues, CPU
  > Bot networks and communications
  > Monitoring using a “honeybot net”
  > Running an own botnet

» **Community**
  > nsp-security mailing-list
    - http://puck.nether.net/mailman/listinfo/nsp-security
  > Honeybot approach
    - watch IRC/P2P/etc based communications
    - run bots in “safe mode”

SÉCURITÉ.ORG

CanSecWest/core03

Conclusion

» **Conclusion**
» **Presentation**
  > http://www.securite.org/presentations/secip/
» **See also**
  > IP Backbone Security
    - http://www.securite.org/presentations/secip/BHUS-IPBackboneSecurity.ppt
  > Protecting your IP network infrastructure
    - http://www.securite.org/presentations/secip/BHAMS2001-SecIP-v105-full.ppt

» **Q&A**

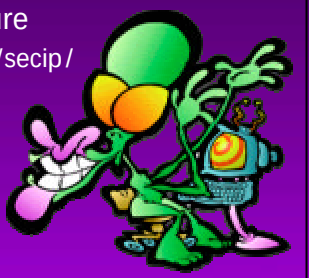


Image: http://www.inforamp.net/~dredge/funkycomputercrowd.html

SÉCURITÉ.ORG