Router Audit Tool and Benchmark

February 20, 2002

George M. Jones

Introduction

- Subject: Router Audit Tool and Benchmark
- Premise: "The network is the computer"
- Corollary: Routers are the network.
- Audience: Network Engineers and
  Technical Security Auditors

Problems Solved

- Lack of Cisco IOS benchmark
- Lack of audit tool for IOS.
- Difficulty maintaining consistency.
- Difficulty detecting changes.
- Need to quickly fix incorrect settings.
- Need for reporting and customization.
- Need to check non-IOS devices.

Problems Not Solved

- Management Issues
- Poor Operations Practices
- Problems in vendor code.
- Problems inherent to protocols.
- Host-based problems (viruses, code red….)
- Bandwidth based DoS attacks
- New vulnerabilities
- Local configuration choices
- The need for competence and vigilance.

Approach

- Perl: “There’s more than one way to do it.”
- Start with “good” config. Define rules.
- Write a program to compare rules & configs.
- Rules forbid/require certain strings/patterns.
- CSV-like output and HTML reports

The Router Audit Tool (rat)

- Four Perl Programs
  - snarf: pull configs
  - ncat: reads rules & configs, writes CSVish output
  - ncat_report: reads CSVish files, writes HTML
  - rat: the program you run. Runs other programs.

A Quick Example

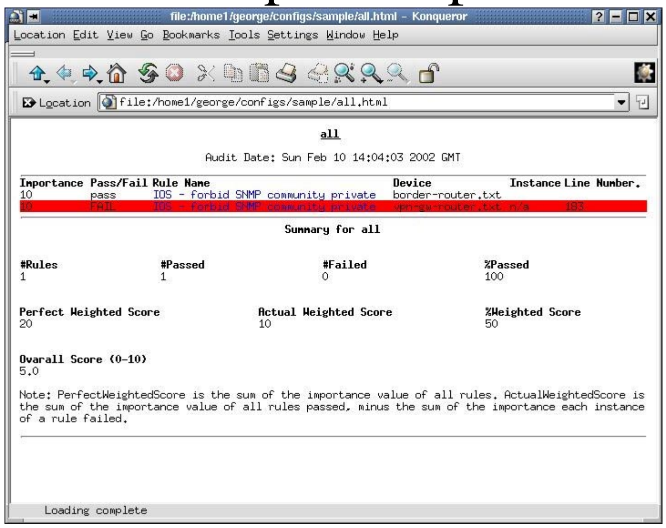
- Define a rule to forbid SNMP read-write community string “private”

```
RuleName:IOS - forbid SNMP community private
RuleClass:default,access
RuleVersion:version 1[12]\.*
RuleContext:Global
RuleType:Forbidden
RuleMatch:snmp community private
RuleImportance:10
RuleDescription:Don't use default SNMP community strings.\
SNMP allows management and monitoring of networked devices.\
"private" is a well know default community string.\
It should not be used
```

- Running the Tool

```
Rat --nosnarf border-router.txt vpn-gateway-router.txt
```

Sample Output



The Benchmark

- Defines what to check
- Based on NSA Router Security Configuration Guide
- “Level 1” = Default, “Level 2” = Optional.
- Basic checks, baseline for all routers.
- Some sites will need more optional rules.

The Rules

- Designed to protect the router itself.
- Four classes: services, access, logging, routing.
- 59 rules. 5 IOS 11 specific. 4 IOS 12 specific.

SNMP Rules

- Major SNMP Vulnerabilities outlined in CERT Advisory CA-2002-03
- RAT rules address this:
  - Disable SNMP
  - Forbid SNMP community public/private
  - Forbid SNMP without ACLs
  - Ingress/egress filters

More SNMP Defenses

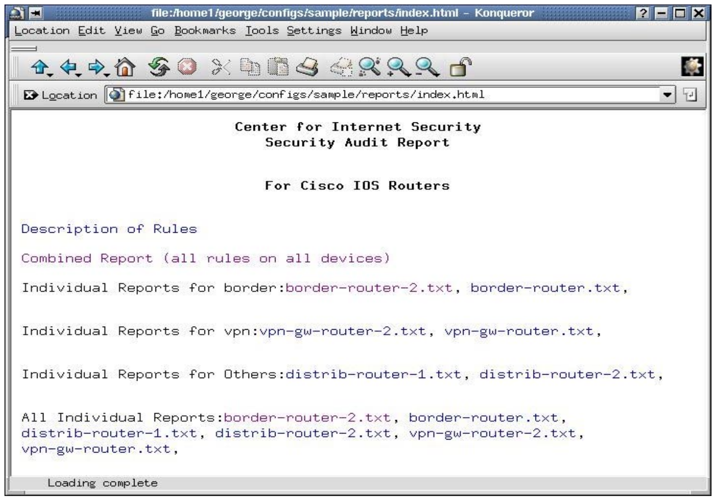
- Upgrade to patched IOS version
- Filter all SNMP at border (ingress)
  - access-list 123 deny udp any any eq snmp
  - access-list 123 deny udp any any eq snmptrap
- Change community strings
- Permit only known hosts to poll
  - access-list 123 permit udp host 1.2.3.4 any eq snmp

Using the Tool and Benchmark

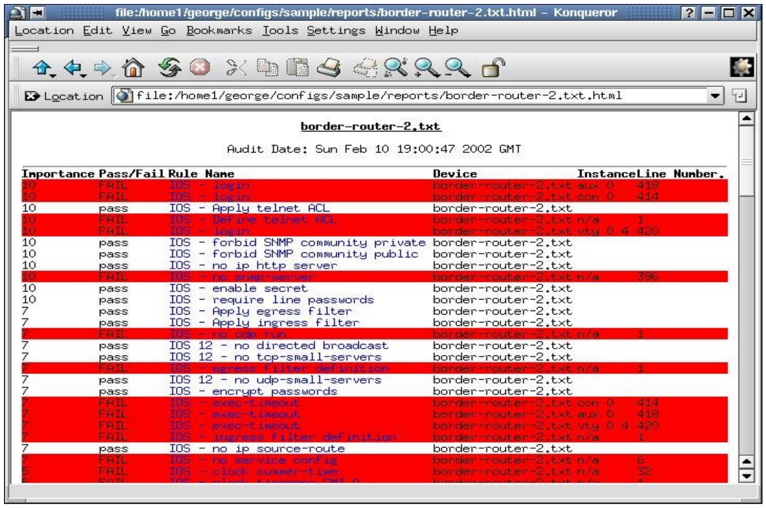
- Using “as is”
  - Minimum standards
  - Scoring
  - Fix problems found
- Customizing
  - Changing headings
  - Modifying rules
  - Adding rules/new devices

 13

Example: index page



Example: Single Report

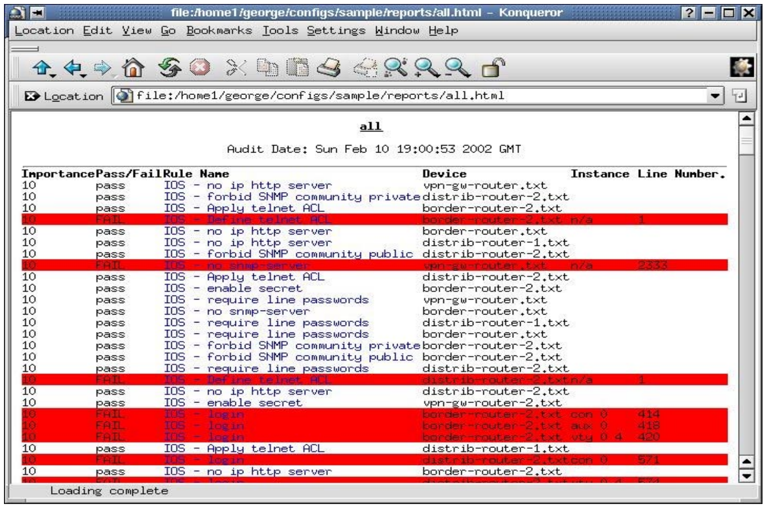


border-router-2.txt

Audit Date: Sun Feb 10 19:00:47 2002 GMT

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number.
10	FAIL	IOS - login	border-router-2.txt	aux 0	418
10	FAIL	IOS - login	border-router-2.txt	con 0	414
10	pass	IOS - Apply telnet ACL	border-router-2.txt		
10	FAIL	IOS - Define telnet ACL	border-router-2.txt	n/a	1
10	FAIL	IOS - login	border-router-2.txt	vty 0 4	420
10	pass	IOS - forbid SNMP community private	border-router-2.txt		
10	pass	IOS - forbid SNMP community public	border-router-2.txt		
10	pass	IOS - no ip http server	border-router-2.txt		
10	FAIL	IOS - no snmp-server	border-router-2.txt	n/a	396
10	pass	IOS - enable secret	border-router-2.txt		
10	pass	IOS - require line passwords	border-router-2.txt		
7	pass	IOS - Apply egress filter	border-router-2.txt		
7	pass	IOS - Apply ingress filter	border-router-2.txt		
7	FAIL	IOS - no cdp run	border-router-2.txt	n/a	1
7	pass	IOS 12 - no directed broadcast	border-router-2.txt		
7	pass	IOS 12 - no tcp-small-servers	border-router-2.txt		
7	FAIL	IOS - egress filter definition	border-router-2.txt	n/a	1
7	pass	IOS 12 - no udp-small-servers	border-router-2.txt		
7	pass	IOS - encrypt passwords	border-router-2.txt		
7	FAIL	IOS - exec-timeout	border-router-2.txt	con 0	414
7	FAIL	IOS - exec-timeout	border-router-2.txt	aux 0	418
7	FAIL	IOS - exec-timeout	border-router-2.txt	vty 0 4	420
7	FAIL	IOS - ingress filter definition	border-router-2.txt	n/a	1
7	pass	IOS - no ip source-route	border-router-2.txt		
7	FAIL	IOS - no service config	border-router-2.txt	n/a	6
5	FAIL	IOS - clock summer-time	border-router-2.txt	n/a	32

Example: Combined Report



Importance	Pass/Fail	Rule Name	Device	Instance	Line Number.
10	pass	IOS - no ip http server	vpn-gw-router.txt		
10	pass	IOS - forbid SNMP community private	distrib-router-2.txt		
10	pass	IOS - Apply telnet ACL	border-router-2.txt		
10	FAIL	IOS - Define telnet ACL	border-router-2.txt	n/a	1
10	pass	IOS - no ip http server	border-router.txt		
10	pass	IOS - no ip http server	distrib-router-1.txt		
10	pass	IOS - forbid SNMP community public	distrib-router-2.txt		
10	FAIL	IOS - no snmp-server	vpn-gw-router.txt	n/a	2333
10	pass	IOS - Apply telnet ACL	distrib-router-2.txt		
10	pass	IOS - enable secret	border-router-2.txt		
10	pass	IOS - require line passwords	vpn-gw-router.txt		
10	pass	IOS - no snmp-server	border-router.txt		
10	pass	IOS - require line passwords	distrib-router-1.txt		
10	pass	IOS - require line passwords	border-router.txt		
10	pass	IOS - forbid SNMP community private	border-router-2.txt		
10	pass	IOS - forbid SNMP community public	border-router-2.txt		
10	pass	IOS - require line passwords	distrib-router-2.txt		
10	FAIL	IOS - Define telnet ACL	distrib-router-2.txt	n/a	1
10	pass	IOS - no ip http server	distrib-router-2.txt		
10	pass	IOS - enable secret	vpn-gw-router-2.txt		
10	FAIL	IOS - login	border-router-2.txt	con 0	414
10	FAIL	IOS - login	border-router-2.txt	aux 0	418
10	FAIL	IOS - login	border-router-2.txt	vty 0 4	420
10	pass	IOS - Apply telnet ACL	distrib-router-1.txt		
10	FAIL	IOS - login	distrib-router-2.txt	con 0	571
10	pass	IOS - no ip http server	border-router-2.txt		

Future Work

- More Rules
- Other Devices
- Better Integration With Config Guide
- Windows Port?
- Any Volunteers?

Related Work

- UUNET net-sec config checker (unpub.)
- Cisco Netsys Baseliner (discontinued)
- NSA Router Security Configuration Guide
  - http://nsa2.conxion.com/Cisco/download.htm
- Improving Security on Cisco Routers
  - http://www.cisco.com/warp/public/707/21.html
- http://www.cymru.com/~robt/Docs/Articles/

Credits

- NSA Information Assurance Directorate
  - Produced Router Security Configuration Guide. Neal Ziring, the editor, has be very helpful
- John Stewart, Digital Island/Exodus
  - Much help with Perl,CVS, install process
- Eric Brandwine and Jared Allison
  - UUNET net-sec config checker
- Mark Krause & Neil Kirr, UUNET, Clint Kreitner, CIS, Alan Paller, SANS
  - For encouraging and supporting the work.

Availability and Feedback

- Availability
  - The tool and benchmark are available for public download from http://www.cisecurity.org/
- Feedback
  - rat-feedback@cisecurity.org
  - rat-announce[-subscribe]@cisecurity.org
  - rat-users[-subscribe]@cisecurity.org
- Questions ?

