

# 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 screenshot shows a Konqueror browser window with the address bar set to `file:/home1/george/configs/sample/all.html`. The main content area displays an audit report for a system named 'all', dated Sun Feb 10 14:04:03 2002 GMT. The report includes a table of rules, a summary, and an overall score.

Importance	Pass/Fail	Rule Name	Device	Instance Line Number
10	pass	IIS - forbid SNMP community private	border-router.txt	
10	fail	IIS - forbid SNMP community private	border-router.txt	100

**Summary for all**

<b>#Rules</b>	<b>#Passed</b>	<b>#Failed</b>	<b>%Passed</b>
1	1	0	100

**Perfect Weighted Score**: 20  
**Actual Weighted Score**: 10  
**%Weighted Score**: 50

**Overall Score (0-10)**: 5.0

Note: PerfectWeightedScore is the sum of the importance value of all rules. ActualWeightedScore is the sum of the importance value of all rules passed, minus the sum of the importance each instance of a rule failed.

Loading complete



# 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

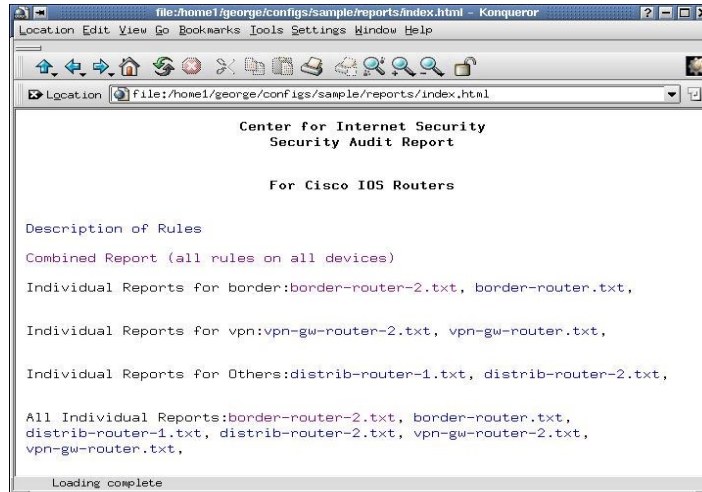
# More SNMP Defenses

- 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

# Example: index page



# Example: Single Report

file:/home1/george/configs/sample/reports/border-router-2.txt.html - Konqueror

Location Edit View Go Bookmarks Tools Settings Window Help

file:/home1/george/configs/sample/reports/border-router-2.txt.html

**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	0	414
10	FAIL	IOS - login	border-router-2.txt	con 0	414
10	pass	IOS - Apply telnet ACL	border-router-2.txt		
10	FAIL	IOS - set the telnet ACL	border-router-2.txt	0	420
10	FAIL	IOS - login	border-router-2.txt	0	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 - enable secret	border-router-2.txt	0	426
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	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 - encrypt passwords	border-router-2.txt	0	430
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	434
7	FAIL	IOS - exec timeout	border-router-2.txt	aux 0	434
7	FAIL	IOS - exec timeout	border-router-2.txt	0	430
7	FAIL	IOS - ingress filter definition	border-router-2.txt	0	430
7	pass	IOS - no ip source-route	border-router-2.txt		
7	FAIL	IOS - no service config	border-router-2.txt	0	430
7	FAIL	IOS - clock source 1.8432	border-router-2.txt	0	430

# Example: Combined Report

file:/home1/george/configs/sample/reports/all.html - Konqueror

Location Edit View Go Bookmarks Tools Settings Window Help

Location file:/home1/george/configs/sample/reports/all.html

**all**

Audit Date: Sun Feb 10 19:00:53 2002 GMT

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	pass	IDS - no ip http server	vpn-gw-router.txt		
10	pass	IDS - forbid SNMP community private	distrib-router-2.txt		
10	pass	IDS - Apply telnet ACL	border-router-2.txt		
10	pass	IDS - no ip http server	border-router.txt		
10	pass	IDS - no ip http server	distrib-router-1.txt		
10	pass	IDS - forbid SNMP community public	distrib-router-2.txt		
10	pass	IDS - Apply telnet ACL	distrib-router-2.txt		
10	pass	IDS - enable secret	border-router-2.txt		
10	pass	IDS - require line passwords	vpn-gw-router.txt		
10	pass	IDS - no snmp-server	border-router.txt		
10	pass	IDS - require line passwords	distrib-router-1.txt		
10	pass	IDS - require line passwords	border-router.txt		
10	pass	IDS - forbid SNMP community private	border-router-2.txt		
10	pass	IDS - forbid SNMP community public	border-router-2.txt		
10	pass	IDS - require line passwords	distrib-router-2.txt		
10	pass	IDS - no ip http server	distrib-router-2.txt		
10	pass	IDS - enable secret	vpn-gw-router-2.txt		
10	FAIL	IDS - login	border-router-2.txt	zon 0	414
10	FAIL	IDS - login	border-router-2.txt	zon 0	415
10	FAIL	IDS - login	border-router-2.txt	vtu 0 d	420
10	pass	IDS - Apply telnet ACL	distrib-router-1.txt		
10	pass	IDS - no ip http server	border-router-2.txt		

Loading complete



# 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 Baseline (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 ?