



RAT v1.1 User Guide (Windows Version)

**CIS(<http://www.cisecurity.org>) CIS Benchmark & Security Tool 가 CIS Level 1/Lever
 2 Benchmark and Audit Tool for Cisco IOS Router , Cisco Router
 Router**

RAT Utility 가 Member Ship
 WINDOSW ,LINUX ,HP- UX , Solaris OS CIS

❖ **RAT**

	Download URL		
RAT	http://www.cisecurity.org	Windows	Download
PERL 5.6.1	http://www.activestate.com	Windows	Download
PERL CPAN Archives	http://ftp.kreonet.re.kr/pub/languages/CPAN/modules/by	Net::telnet	Download
Net::telnet	-module/Net/	Net::telnet::Cisco	Download
Net::telnet::Cisco			

❖ **Test**

- **RAT : Windows 2000 Professional**
- **: 7206 VXR**

❖

1. Perl Install

- www.activestate.com Perl 5.6.1 Version
Download
- Windows
- perl
- MRTG 가

2. RAT DownLoad

- <http://www.cisecurity.org> RAT Download
- C: \RAT (Directory)



3. Perl CPAN Archive

```
. http://ftp.kreonet.re.kr/pub/languages/CPAN/modules/by-module/Net/Net::telnet , Net::telnet::Cisco CPAN Module Download .  
. Download CPAN Module RAT 가 Directory Directory .  
. Activestate Perl Package Manager (PPM) CPAN Module Install .  
< > Dos Prompt ppm install Net-telnet , ppm install net-telnet-cisco  
. Winmake ? perl winmake.pl
```

4. RAT (ncat_config)

```
. Ncat_config , Config  
. Reporting 가 .  
. Ncat_config → Dos perl ncat_config Router  
. Menu , Router  
. <Dos >  
C: \ rat \ rat-1.1 \ bin>perl ncat_config  
ncat_config: Reading c: \ rat \ bin/etc/ncat.conf.MASTER  
Please answer the questions below about your network and  
router configuration. Type ? to get a short explanation of  
any parameter. If you are unsure about what value to give  
for a parameter, hit RETURN to take the default value.  
Select types of optional rules to be applied:  
ncat_config: Apply rules for class use_multiple_ntp_servers [no] ? y  
ncat_config: Apply rules for class exterior_router [no] ? y  
ncat_config: Apply rules for class tacacs_aaa [no] ?  
ncat_config: Apply rules for class localtime [no] ? y  
ncat_config: Skipping class "gmt". It is incompatible with "localtime".  
ncat_config: Apply rules for class snmp [no] ? y  
ncat_config: Apply rules for class exterior_router_with_2nd_if [no] ? y
```

Cisco Internal Use Only

Copyright ©2001 Cisco Systems, Inc. All rights reserved.



Change default configuration values:

ncat_config: Enter value for local_acl_num_egress [181] ?

ncat_config: Enter value for local_acl_num_ingress [180] ?

ncat_config: Enter value for local_acl_num_vty [182] ?

ncat_config: Enter value for local_address_internal_netblock_with_mask
[192.168.1.0 0.0.0.255] ? 188.188.100.5 0.0.0.255

ncat_config: Enter value for local_address_loopback [192.168.1.3] ? ?

Help for local value :

? The IP address of this router's loopback interface (if any)

Default value is: 192.168.1.3

ncat_config: Enter value for local_address_loopback [192.168.1.3] ? n

ncat_config: Enter value for local_address_ntp_host [1.2.3.4] ? n

ncat_config: Enter value for local_address_ntp_host_2 [5.6.7.8] ? n

ncat_config: Enter value for local_address_ntp_host_3 [9.10.11.12] ?

ncat_config: Enter value for local_address_syslog_host [192.168.1.3] ?

ncat_config: Enter value for local_address_telnet_acl_block_with_mask
[192.168.1.0 0.0.0.7] ? ?

Help for local value :

? The LAN address and netmask for the hosts permitted to telnet to the router.

Default value is: 192.168.1.0 0.0.0.7

ncat_config: Enter value for local_address_telnet_acl_block_with_mask
[192.168.1.0 0.0.0.7] ? 188.188.200.5 0.0.0.255

ncat_config: Enter value for local_address_telnet_acl_host [192.168.1.254] ? ?

Help for local value :

? The IP address of the host permitted to telnet to the router.

Default value is: 192.168.1.254

ncat_config: Enter value for local_address_telnet_acl_host [192.168.1.254] ?

ncat_config: Enter value for local_exec_timeout [5 0] ?

ncat_config: Enter value for local_external_interface [Ethernet0] ?

ncat_config: Enter value for local_external_interface_2 [Ethernet1] ?

Cisco Internal Use Only

Copyright ©2001 Cisco Systems, Inc. All rights reserved.

Page 3 of 3



```

ncat_config: Enter value for local_gmt_offset [0] ?
ncat_config: Enter value for local_loopback_num [0] ?
ncat_config: Enter value for local_timezone [GMT] ?
ncat_config: Writing c:\rat\bin\etc\ncat.conf...Done.
ncat_config: Now examine c:\rat\bin\etc\ncat.conf.
ncat_config: Edit c:\rat\bin\etc\ncat.conf.MASTER and rerun ncat_config if not
satisfactory.

```

5. Reporting

- . Ncat_config Reporting
- . sh running -config , config text
capture . → router.txt
- . RAT → perl rat router.txt (router config)
- . all.html , all.html Reporting

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	FAL	IOS - enable secret	router.bit	city 0 4	253
10	FAL	IOS - enable secret	router.bit	city 5 17	256
10	pass	IOS - forbid SNMP community private	router.bit		
10	FAL	IOS - forbid SNMP community public	router.bit	n/a	1
10	pass	IOS - enable secret	router.bit		
10	FAL	IOS - enable secret	router.bit	aux 0	252
10	pass	IOS - enable secret	router.bit		
10	FAL	IOS - enable the clock	router.bit	con 0	250
10	FAL	IOS - no aaa-serial	router.bit	n/a	241
10	FAL	IOS - login	router.bit	con 0	250
10	FAL	IOS - login	router.bit	aux 0	252
10	pass	IOS - no in http server	router.bit		
7	pass	IOS 12 - no directed broadcast	router.bit		
7	pass	IOS 12 - no tcp-small-servers	router.bit		
7	pass	IOS 12 - no udp-small-servers	router.bit		
7	FAL	IOS - no ip dhcp server	router.bit	n/a	1
7	FAL	IOS - no ip dhcp server	router.bit	con 0	250
7	FAL	IOS - no ip dhcp server	router.bit	aux 0	252
7	FAL	IOS - no ip dhcp server	router.bit	city 0 4	253
7	FAL	IOS - no ip dhcp server	router.bit	city 5 17	256
7	FAL	IOS - no ip dhcp server	router.bit	n/a	1
7	FAL	IOS - no ip dhcp server	router.bit	n/a	1
7	pass	IOS - no service config	router.bit		
5	pass	IOS 12 - no finger service	router.bit		
5	FAL	IOS - no ip dhcp server	router.bit	HS120	58
5	pass	IOS - enable logging	router.bit		
5	FAL	IOS - no ip dhcp server	router.bit	FastEthernet1/0	44
5	FAL	IOS - no ip dhcp server	router.bit	n/a	1
5	FAL	IOS - no ip dhcp server	router.bit	n/a	1



Rule Name	Click	Guide 가
, configuration	Sample config .	가
Rule	RAT utility download	rscg.pdf



□

. RAT Rule Level (Certcc Korea)

Level 1	Level 2
Apply egress filter Apply ingress filter Apply telnet ACL clock timezone Define telnet ACL disable aux egress filter definition enable logging enable secret encrypt passwords exec-timeout forbid SNMP community private forbid SNMP community public forbid SNMP read-write forbid SNMP without ACLs ingress filter definition logging buffered logging console critical logging trap debugging login no cdp run no ip bootp server no ip http server no ip proxy-arp no ip source-route no service config no snmp-server ntp server ntp source require external IF to exist require line passwords set syslog server vty transport telnet no identd service(IOS 11) no directed broadcast(IOS 11, 12) no finger service(IOS 11, 12) no tcp-small-servers(IOS 11, 12) no udp-small-servers(IOS 11,12)	aaa accounting commands aaa accounting connection aaa accounting exec aaa accounting network aaa accounting system aaa authentication enable aaa authentication login aaa new-model aaa source-interface Apply egress filter to 2nd IF Apply ingress filter to 2nd IF forbid clock summer-time - GMT Loopback0 must be only loopback Loopback0 must exist no local logins no tftp-server ntp server 2 ntp server 3 require clock summer-time - localtime require external IF 2 to exist service timestamps - GMT service timestamps - localtime tftp source-interface Tunnel interfaces must not exist



. RAT

Program	
Snarf	
Ncat	Rule CSV
Ncat_report	CSV ,HTML
rat	capture
Ncat_config	Rule

Reference Site

<http://nsa2.www.conxion.com/cisco/download.htm>

<http://www.cisco.com/warp/public/707/21.html>

<http://www.cymru.com/~robt/Docs/Articles/secure-ios-template.html>

<http://www.cisco.com/warp/public/707/advisory.html>

<http://www.cisecurity.org>

<http://www.kisa.or.kr>

<http://www.certcc.or.kr> (Unix Guide 가)