ISP/NSP Security Workshop, SANOG 6, 16-23 July, 2005
Thimphu, Bhutan

Router and Routing Security

Setting up console Password

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# line console 0
router (config-line)# login
router (config-line)# password console-password
router (config-line)#^Z
router #
```

Setting up Aux Password

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# line aux 0
router (config-line)# login
router (config-line)# password aux-password
router (config-line)#^Z
router #
```

Setting up Virtual Terminal (VTY) Password
Since there are more than one VTYs, the configuration is slightly different

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# line vty 0 4
router (config-line)# login
router (config-line)# password vty-password
router (config-line)#^Z
router #
```

Checking the new configuration

```
router#sh run
line con 0
     password console-password
     login
line aux 0
     password aux-password
     login
line vty 0 4
     password vty-password
     login
```

Enabling Encryption

```
router (config)# service password-encryption
router (config)# ^Z
```

Re-view your configuration and save it

```
router#wr
```

Enabling privilige level password

```
router (config)# enable secret enable-secret
router (config)# ^Z
```

If you have enable password, instead of a enable secret, the secret takes precedence over the password. As usual, please use the password encryption and save the configuration.

Enabling Local Usernames

```
router (config)# username gaurab password gaurab-pass
router (config)# ^Z
```

Creating Local username without password

```
router (config)# username system nopassword
router (config)# ^Z
```

Enabling Local Authentication on VTY terminal

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# line vty 0 4
router (config-line)# login local
router (config-line)#^Z
router #
```

Disabling login on AUX port

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# line aux 0
router (config-line)# login local
router (config-line)# no password
router (config-line)# transport input none
router (config-line)# no exec
router (config-line)# exec-timeout 0 1
router (config-line)#^Z
router #
```

In the above example, note the tricky way to completely disable login. First you enable local login, but do not assign a password, which will disslow anyone from logging in. If you do 'no login', it'll allow password less access to everyone.

Limiting Access by IP Address

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# access-list 10 permit 192.168.0.1
router (config)# access-list 10 permit 192.168.0.240
router (config)# access-list 10 deny any
router (config)# line vty 0 4
router (config-line)# access-class 10 in
router (config-line)#^Z
router #wr
```

Setting up timeout

```
router (config)# line vty 0 4
router (config-line)# exec-timeout 5 0
router (config-line)#^Z
router #wr
```

Limiting http server by IP

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# access-list 20 permit 192.168.0.1
router (config)# access-list 20 deny any
router (config)# ip http access-class 20
router (config)#^Z
```

Disabling http server

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# no ip http server
router (config)#^Z
router #wr
```

Viewing Privilege Levels

```
router>show privilege
Current privilege level is 1
router>enable
password: enable secret
router#show privilege
Current privilege level is 15
router #
```

Moving between Privilege Levels

```
router#show privilege
Current privilege level is 15
router #disable 5
router#show privilege
Current privilege level is 5
router #enable 10
router#show privilege
Current privilege level is 10
```

Viewing rights in different Privilege Levels

```
router #disable 0
router>show privilege
Current privilege level is 0
router>?
Exec Commands:
 disable
 enable
 exit
 help
 logout
router>
```

Assinging Privilege level Password

```
router (config)# enable secret level 7 level7-password
router (config)# ^Z
router #
```

Now entering the new privilege level

```
router# enable 7
router#
```

Assigning default Privilege Level to the AUX port

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# line aux 0
router (config-line)# login
router (config-line)# privilege level 7
router (config-line)#^Z
router #
```

You can also assign similar default privilege levels to other lines.

Username privilege levels

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# username gaurab privilege 5
router (config)# username system privilege 0
router (config)#^Z
router #
```

Setting up Warning Banners

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# banner login $
Enter TEXT message. End with the Character  '!'.
Warning !!!
This system belongs to ISP Lahai. Any unauthorized access to
this system will violate laws of the country and will result in
procecution.
$
!
router (config)#^Z
router (config)#
```

Setting up Information to users.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# banner exec $
Enter TEXT message. End with the Character  '!'.
IMPORTANT Information
Please be careful with the commands you issue in this mode.Take
a backup of any configuration changes before writing them to
the router.
$
!
router (config)#^Z
router (config)#
```

Unnecessary Protocol and Services

ICMP

Internet Control Message Protocol is invaluable for testing network connectivity and determining network paths. Ping and Traceroute uses ICMP. Path MTU discovery also uses ICMP.

Path MTU Discovery uses ICMP Type 3 code 4, Ping uses ICMP type 0, and traceroute uses ICMP type 11.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# access-list 103 permit icmp any any 3 4
router (config)# access-list 103 permit icmp any any 0
router (config)# access-list 103 deny icmp any any
router (config)# access-list 103 permit ip any any
router (config)# int eth0/0
router (config-if)# ip access-group 103 in
router (config-if)#^Z
router #
```

Blocking ICMP Redirects and ICMP directed broadcast on interfaces. ICMP broadcast is well known smurf attack.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# int eth0/0
router (config-if)#no ip redirects
router (config-if)#no ip directed broadcast
router (config-if)#^Z
router #
```

Blocking ICMP Redirects from reaching your router, you should do this on your edge / border routers

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# access-list 105 deny icmp any any redirect
router (config)# access-list 105 permit ip any any
router (config)# int Fa0/0
router (config-if)#ip access-group 105 in
router (config-if)#^Z
router #
```

Blocking ICMP Unreacheables. Using ICMP Unreacheable message is a common way to scan your system for possible open ports. Disabling it makes the job of the cracker harder.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# access-list 102 deny icmp any any time-stamp-request
router (config)# access-list 102 deny icmp any any information-request
router (config)# access-list 102 permit ip any any
router (config)# int eth0/0
router (config-if)#ip access-group 102 in
router (config-if)#^Z
router #
```

Team Cymru recommended ICMP filters

```
access-list 2001 remark Specifically block ICMP fragments
access-list 2001 deny icmp any any fragments
access-list 2001 remark Permit inbound ping.
access-list 2001 permit icmp any any echo
access-list 2001 remark Permit inbound ping response.
access-list 2001 permit icmp any any echo-reply
access-list 2001 remark Permit Path MTU to function.
access-list 2001 permit icmp any any packet-too-big
access-list 2001 remark Permit time exceeded messages for traceroute and loops.
access-list 2001 permit icmp any any time-exceeded
access-list 2001 remark And explicitly block all other ICMP packets
access-list 2001 deny icmp any any
access-list 2001 remark Permit everything else (or add additional ACLs here).
access-list 2001 permit ip any any
```

(from : http://www.cymru.com/Documents/icmp-messages.html)

Blocking Source Routing. Source Routing allows a packet to specifiy how it should be routed through a network. This should be disabled.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# int eth0/0
router (config-if)#no ip source-route
router (config-if)#^Z
router #
```

Blocking small Services. In some older IOS releases, small TCP and UDP servers like echo, daytime and chargen services may be enabled by default. These should be disabled.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# no service tcp-small-servers
router (config)# no service udp-small-servers
router (config-if)#^Z
router #
```

Cisco Discover Protocol. It's a protocol used by Cisco routers/switches to find information about connected routers. On the internet, this means like publishing full information about your cisco devices. CDP should be disabled on all routers and switches.
Disabling CDP Globally

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# no cdp run
router (config)#^Z
router #
```

Disabling CDP on a particular interface

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# int eth0/0
router (config-if)#no cdp enable
router (config-if)#^Z
router #
```

Stopping Other Serives.
There are quite a few services that are not necessary for the functioning of your router. You should disable all of them.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# no ip finger
router (config)# no ip bootp server
router (config)# no ip name-server
router (config)# no service config
router (config)# no boot network
router (config)# no service pad
router (config)# int eth0/0
router (config-if)#no ip proxy-arp
router (config-if)#no ip mask-reply
router (config-if)#^Z
router #
```

Simple Network Management Protocol (SNMP)

First try this from your linux console.

```
# snmpwalk -v1 192.168.0.201 public
```

This should be enough to convince you that enabling snmp is a bad idea. There are 3 versions of SNMP commonly used. SNMP v1 and v2c use the same security model, v3 has enhanced security model.

SNMP Checklist

- Do not enable read/write access unless absolutely necessary
- Choose difficult to guess community string
- limit SNMP access to specific IP addresses using ACLs
- Limit SNMP output with views

Completely disabling SNMP

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# no snmp-server
router (config)#^Z
router #
```

Configuring Read-only SNMP Access

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# snmp-server community Really10ng1 RO
router (config)#^Z
router #
```

Using ACLs to limit SNMP access. Completely disabling SNMP

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# access-list 6 permit 192.168.0.1
router (config)# access-list 6 permit 192.168.0.200
router (config)# access-list 6 deny any
router (config)# snmp-server community community RO 6
router (config)#^Z
router #
```

SNMP views

SNMP views can be defined to only provide a subset of the full SNMP table. You can define your own views for doing so.

```
router (config)# snmp-server view tcp-view tcp include
router (config)# snmp-server community tcponlycommunitystring view tcp-view
router (config)# ^Z
```

You can define what each view includes by using OID numbers. Otherwise, you can use the known SNMP table names such as IP, ICMP, TCP, SYSTEM, INTERFACES etc.

After creating a view, please re-run the snmpwalk command from your linux console.

SNMP v3

(The SNMP v3 is only supported by IOS images 12.0(3)T and higher.)

There are three levels of SNMPv3. These are NoAuthNoPriv, AuthNoPriv and AuthPriv. The cisco equivalent for these are noauth, auth, and priv respectively.

Secure Routing and Anti-spoofing

Ingress Filters are needed to limit the packets entering your network. The rule is anything that claims to be coming from your internal network on an external interface should be dropped.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)#access-list 18 deny 192.168.0.0 0.0.0.255
router (config)#access-list 18 deny 172.16.0.0 0.0.0.255
router (config)#access-list 18 permit any
router (config)#int fa0/0
router (config-if)#ip access group 18 in
router (config-if)#^Z
router #
```

You should block the RFC 1918 space from entering your network from external interfaces. Refer to the Cymru Bogon List (www.cymru.com) for a complete list of bogons. At minimum you should block
127.0.0.0/8
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
224.0.0.0/4
240.0.0.0/5
255.255.255.255/32

```
You can put this ingress access list in any edge router

access-list 18 deny 0.0.0.0 0.0.0.0
access-list 18 deny 127.0.0.0 0.255.255.255
access-list 18 deny 10.0.0.0 0.255.255.255
access-list 18 deny 172.16.0.0 0.15.255.255
access-list 18 deny 192.168.0.0 0.0.255.255
access-list 18 deny 224.0.0.0 15.255.255.255
access-list 18 deny 240.0.0.0 7.255.255.255.0
access-list 18 permit any
```

Egress Filters
By rule, you should only allow packets originating from your own network only to be annouced on the internet. You should block all others.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)#access-list 20 permit 192.168.0.0 0.0.0.255
router (config)#access-list 20 deny any log
router (config)#int fa0/0
router (config-if)#ip access group 20 out
router (config-if)#^Z
router #
```

Enabling Unicast Reverse Packet Forwarding

```
router#conf t
Enter Configuration Commands, one per line.
router (config)#ip cef
router (config)#int fa0/0
router (config-if)#ip verify unicast reverse-path
```

```
router (config-if)#^Z
router #
```

Routing Protocol Security – Making your OSPF secure

You can use either plain-text of MD5 authentication for OSPF.
First you need to enable ospf authentication on each of your interface.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)#int fa0/0
router (config-if)#ip ospf message-digest-key 1 md5 mykey
router (config-if)#exit
router (config)int eth0/0
router (config-if)#ip ospf message-digest-key 1 md5 mykey
router (config-if)#exit
router (config)#^Z
router #
```

Now, you need to enable authentication on the OSPF configuration. Assuming your OSPF AS is 100

```
router#conf t
Enter Configuration Commands, one per line.
router (config)#router ospf 100
router (config-router)#area 0 authentication message-digest
router (config-router)#exit
```

Routing Protocol Security – Making your BGP secure

BGP authentication is much simpler, as it is based on per-peer authentication information. Which means that you can enable password with a few peers and leave out others, until they are ready.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)#router bgp 100
router (config-router)#network 10.0.200.0 255.255.255.0
router (config-router)#neighbor 192.168.0.200 remote-as 101
router (config-router)#neighbor 192.168.0.200 password commonbgppassword
router (config-router)#^Z
```

Route Filtering with BGP Prefix Lists. BGP Prefix lists provide an extended mechanism to filter ingress and egress routes. This are easier to handle then access-lists. Similar to access lists, you have to first define the prefix list, then apply it to particular peers. Using peer-groups can let you apply common filters across many peers.

```
router (config-router)#neighbor 192.168.0.200 password commonbgppassword
router (config-router)#neighbor 192.168.0.200 prefix-list peer-in in
router (config-router)#neighbor 192.168.0.200 prefix-list peer-out out router
(config-router)#^Z
```

Using and Cofiguring NTP Service. Again you can use access lists

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# ntp server 192.168.0.1
router (config)# ntp master 10
router (config)# ntp access-group serve-only 15
router (config)#^Z
router #
```

Logging to syslog from Cisco Routers
Cisco Routers can log information in six different ways, console logging, buffered logging, terminal logging, syslog, snmp traps and AAA accounting. Logging to a secure syslog server will provide longer term audit trail.

First you need to set up the Timestamps

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# service timestamps log datetime msec logcaltime show-timezone
router (config)#^Z
router #
```

Now sending logs to a syslog server

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# logging 192.168.0.1
router (config)# service sequence-numbers
router (config)#^Z
router #
```

If you have your syslog server configured with additional facilities, you can send it to that specific log file on syslog.

Book Reference
Much of the lab materials for this lab are from one single book.

Hardening Cisco Routers by Thomas Akin. Published by O'reilly.

```
! Router  configuration for 192.168.0.100
! Example for BGP peering with 192.168.0.200

router#conf t
Enter Configuration Commands, one per line.
! Inbound prefix-list
router (config)# ip prefix-list 200-in permit 10.0.200.0/24
router (config)# ip prefix-list 200-in deny 0.0.0.0/0 le 32
! Outbound Prefix-list
router (config)# ip prefix-list 200-out permit 10.0.100.0/24
router (config)# ip prefix-list 200-out deny 0.0.0.0/0 le 32
! Null route ( If you don't have a route for the network that
! you are announcing then bgp will not announce your network prefix)
! In real environments you usually static/ospf/ibgp routes
router (config)# ip route 10.0.100.0 255.255.255.0 null0
! BGP configuration
router (config)#router bgp 100
router (config-router)#no synchronization
router (config-router)#no auto-summary
! announce your network
router (config-router)#network 10.0.100.0 mask 255.255.255.0
! configure your peers 192.168.0.200
router (config-router)#neighbor 192.168.0.200 remote-as 200
! configure inbound prefix-list
router (config-router)#neighbor 192.168.0.200 prefix-list 200-in in
! configure outbound prefix-list
router (config-router)#neighbor 192.168.0.200 prefix-list 200-out out
```