

]HackingTeam[

Remote Control System 7.1.0

Injection Proxy Appliance Manual

Summary

Remote Control System 6.2.0.....	1
Summary	2
1 Introduction	4
1.1 Injection technology.....	4
1.2 Features	4
1.3 Common Terminology	4
2 IPA Architecture	5
2.1 Traffic interception.....	6
2.1.1 Using a SPAN port.....	6
2.1.2 Using a TAP device	6
2.2 Traffic injection	7
3 Installation.....	8
3.1 Software installation	8
3.2 Post install configuration	13
3.3 Physical installation and cabling.....	14
4 IPA Configuration.....	15
4.1 Registering the IPA	15
4.2 Adding the rules	15

]Hacking**Team**[

1 Introduction

1.1 Injection technology

RCS Injection Proxy Appliance (RCS IPA) is an offensive security device developed to perform remote installation of Remote Control System.

By using man in the middle attack techniques and our proprietary streamline injection mechanism, it can transparently operate in different network scenarios, either on LANs or intra-switch segments.

RCS IPA rule-based configuration allows the user to setup a set of resources (i.e. executable files) and users (i.e. IP address, Radius authentication) to be injected.

Employing purpose-specific network hardware, RCS IPA is able to perform on network links up to several gigabits of bandwidth, using different physical connection standards (Gigabit Ethernet, SONET, E1/T1/J1).

1.2 Features

1.3 Common Terminology

Illustrated here are the concepts that will be commonly used during the rest of this document.

Target: the user (computer) on which you want to remotely install RCS.

Access Switch: the switching apparatus on which the target is connected. IPA needs to monitor a segment of this switch to be able to “see” the traffic of the target and eventually modify it.

User: the IPA identifies users by means of their identification on the network. This could be their IP address, Radius credentials, etc. This concept ideally matches Target, but will be used to distinguish the mean by which interesting connections are discriminated by IPA (i.e. by IP address).

Resource: a resource is intended as an object of interest to the IPA. Usually this consists of an EXE file sent through an HTTP connection. This is usually identified by configuring the IPA with a string that should match the URL of interesting resources (i.e. all EXE files).

2 IPA Architecture

RCS Injection Proxy Appliance can be plugged into any network in which a SPAN capable network switch is present or a TAP device is available to monitor the traffic.

RCS IPA, once deployed, will reside outside the customer network (Figure 1).

RNC (RCS Network Controller) will periodically poll the IPA to send it new configurations, monitor its state and collect the logs.

According to the received configuration, the IPA actively monitors all HTTP network connections and eventually modifies them as needed.

After the first configuration of the IPA, even if the connection to RNC isn't present anymore, the IPA will continue working, monitoring and injecting connections as configured, so an IPA can be configured beforehand, then deployed: the IPA will operate on its own, completely isolated from the RCS infrastructure (Set and Forget configuration).

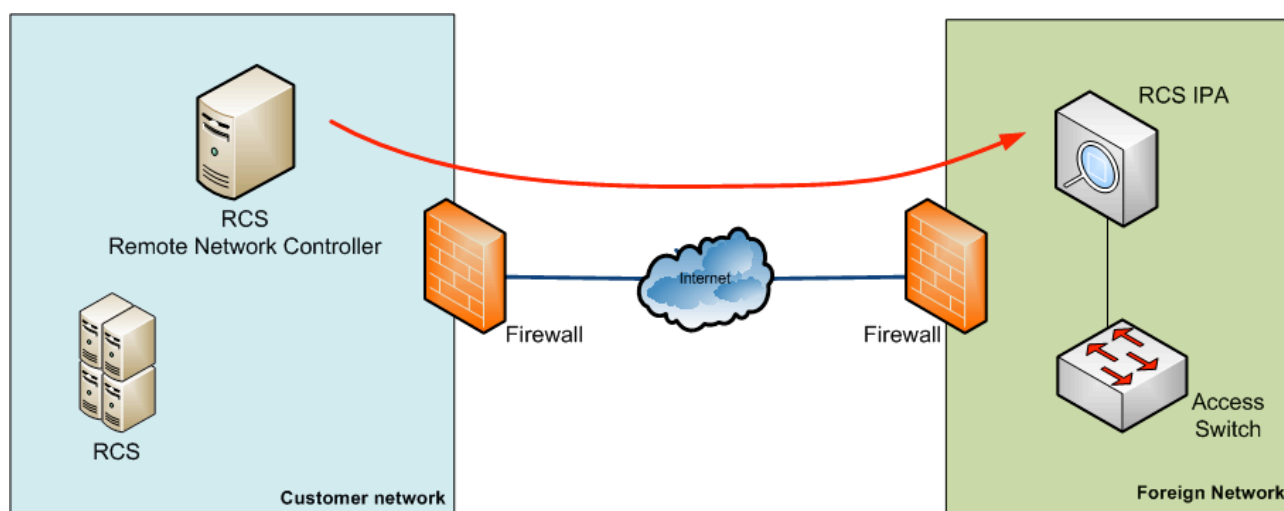


Figure 1 - IPA Architecture overview

RCS IPA can be inserted into the target network, by using a network switch and, if available, a tap device (Figure 2).

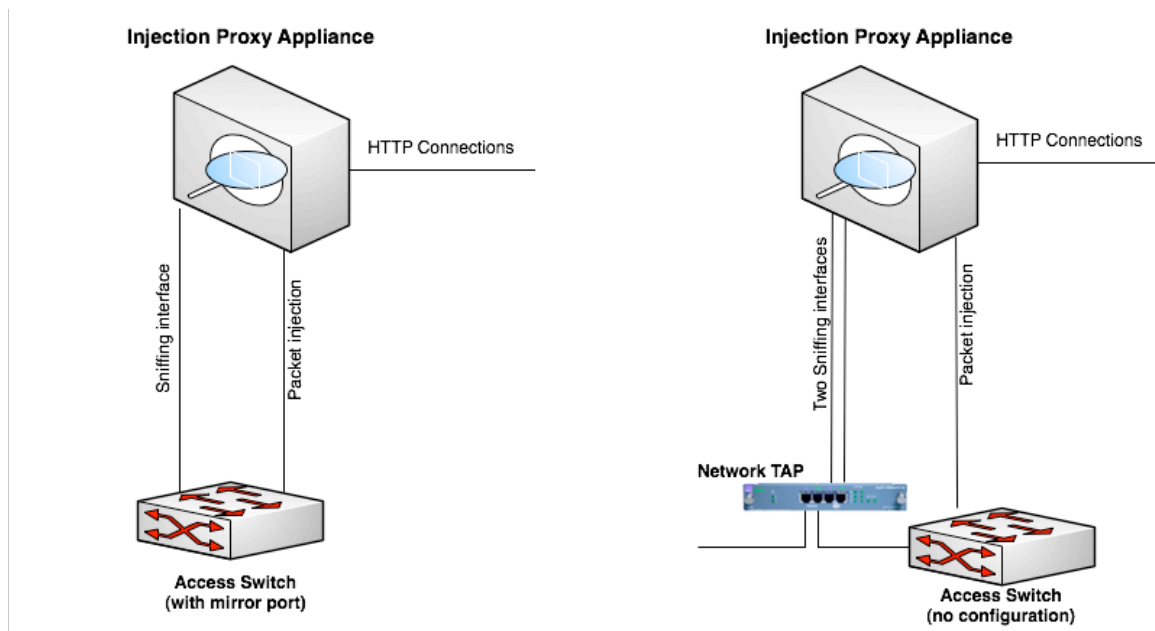


Figure 2 - IPA setup with and without TAP device

RCS IPA requires two network links to operate: one for intercepting the traffic, the other to inject traffic into the network.

2.1 Traffic interception

The RCS IPA monitors network traffic to detect HTTP connections.

There are two different solutions to replicate the network traffic and send it to the RCS IPA.

Since both solutions use passive interception, no degradation or interruption of service can be caused by RCS IPA.

2.1.1 Using a SPAN port

If you only have the Access Switch available, you can use one or more SPAN ports on the switch to monitor the traffic and send it to the IPA.

Using a SPAN port is the most common solution, but it carries a few drawbacks:

- CPU load on the switch may be sensibly higher due to SPAN port usage;
- if the SPAN port on the switch is already in use, it may not be possible to use it for IPA;
- viceversa, if the SPAN port is in use by IPA, this prevents any other usage of the same port for other purposes.

2.1.2 Using a TAP device

A TAP device may already be present on the network segment you want to monitor using RCS IPA.

Since using a TAP device does not carry any of the drawbacks of using a SPAN port, this is the preferred solution.

2.2 Traffic injection

RCS IPA examines the intercepted traffic looking for HTTP connections. In case a connection is found that matches the rules, some traffic is injected into the network to send the RCS payload together with the original data.

To inject the traffic, one link is needed on the Access Switch: this port must be configured to see all the VLANs that are present on the intercepted ports.

3 Installation

Before using the RCS Injection Proxy Appliance, you need to reset the system installing the software from the provided bootable media (i.e. CD).

Software installation is automated, requiring only a few confirmation steps.

IPA software can be installed either on dedicated appliances with wire-speed capture network cards or on standard Intel hardware, such as off-the-shelf laptops or netbooks.

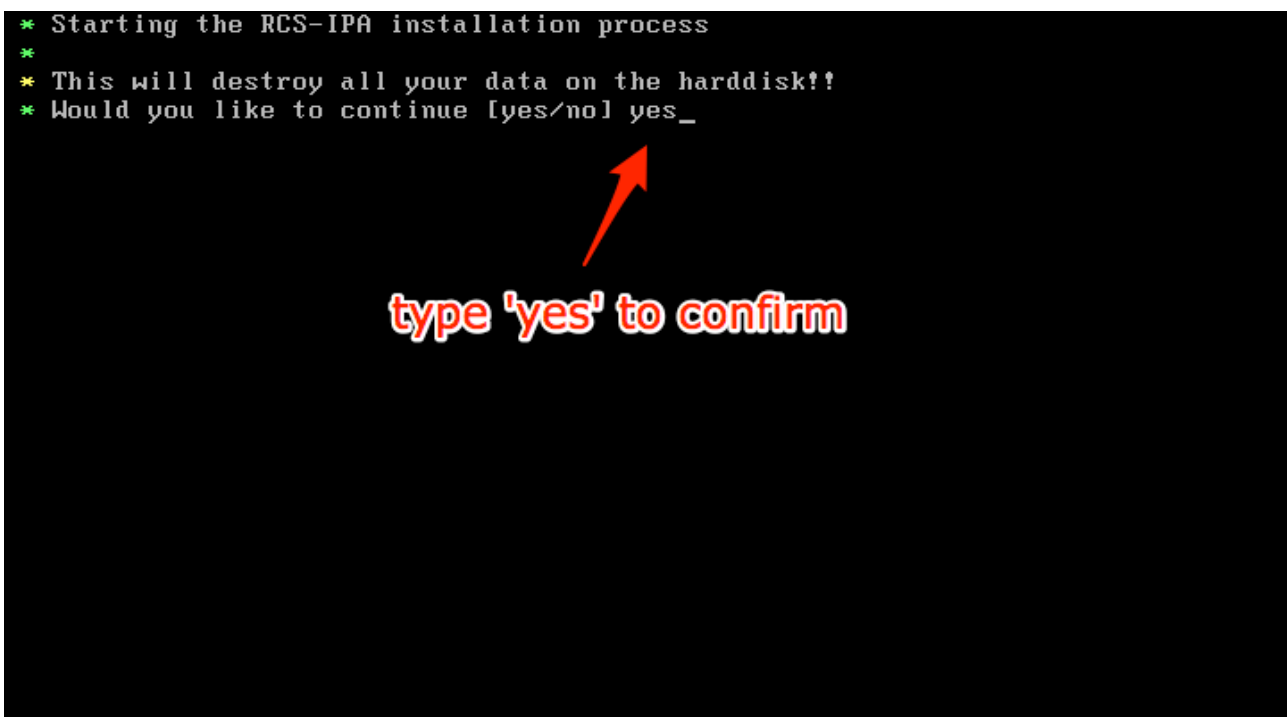
Installation is identical for both types of hardware, while there some minor differences in post install configuration.

3.1 Software installation

Installing the software on the appliance is done using the RCS IPA Installation CD.

Power up the system and insert the CD into the tray. If the system does not boot from the CD, you need to change the configuration of the BIOS and modify the boot sequence.

After the boot process completes, a confirmation screen appears:



```
* Starting the RCS-IPA installation process
*
* This will destroy all your data on the harddisk!!
* Would you like to continue [yes/no] yes_
```

type 'yes' to confirm

Figure 3 - Confirmation screen

Please be aware that all the data present on the system will be permanently erased.

If you want to continue, type 'yes' then press Enter.

]HackingTeam[

```
* creating the key(s) ... [ ok ]
* cryptsetup for /dev/sda3 to /dev/mapper/root ... [ ok ]
* cryptsetup for /dev/sda4 to /dev/mapper/rcsipa ... [ ok ]
* Formatting the partitions
* swap on /dev/sda1 ... [ ok ]
* boot on /dev/sda2 ... [ ok ]
* root on /dev/mapper/root ... [ ok ]
* data on /dev/mapper/rcsipa ... [ ok ]
* Mounting the partitions
* /dev/mapper/root on /tmp/root ... [ ok ]
* /dev/sda2 on /tmp/root/boot ... [ ok ]
* /dev/mapper/rcsipa on /tmp/rcsipa ... [ ok ]
* Creating and mounting the pseudo filesystem (proc, sys)
* /tmp/root/proc ... [ ok ]
* /tmp/root/sys ... [ ok ]
* Extracting the boot tarball (kernel and initrd) [ ok ]
* Installing the crypto key(s)
* repacking the initrd and installing the rootfs key ... [ ok ]
* datafs key to /tmp/root/rcsipa ... [ ok ]
* Extracting the root tarball [ ok ]
* Extracting the data tarball [ ok ]
* Setting up udev for the new networking device driver [ ok ]
* Finalizing the installation
* Installing grub ... [ ok ]
* Press ENTER to continue..._ press 'Enter' to continue
```

Figure 4 - Installation completed

The installation procedure may require up to 20 minutes to complete.

When completed, please press 'Enter' to continue.

```
File Network Access IPA System SYSCONF
Configuration:
  Hostname      : RCS_IPA
  IP address    :
  Netmask       :
  Gateway       :
  DNS server    : 192.168.200.100
```

Figure 5 - SYSCONF screen

]HackingTeam[

The SYSCONF screen allows you to setup the network interface. This configuration is relative to the injection interface.

To move inside the SYSCONF, you can use the following keys:

Key	Action
TAB	Open the menu
Arrow keys	Move within the menus

Normally, you want to use only the Network menu to configure the IP address, gateway and DNS, and the File menu to save the configuration.

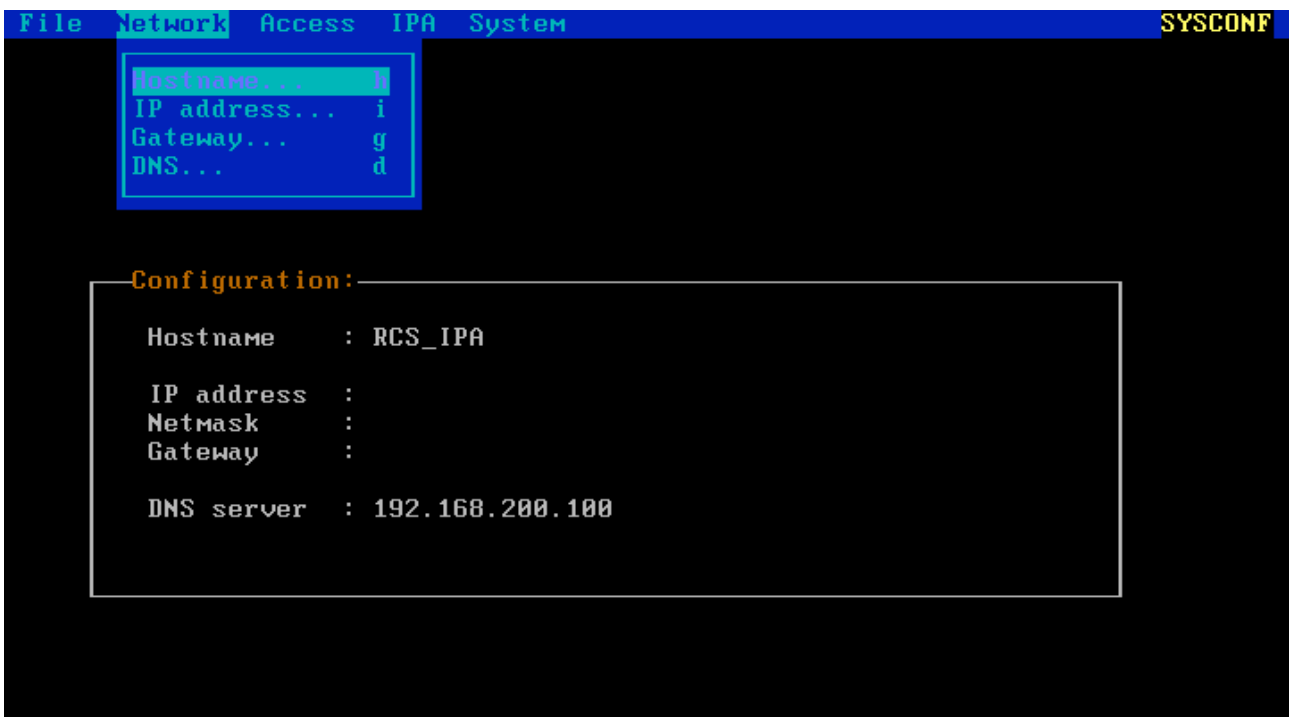


Figure 6 - Network menu

The Network menu gives you the following options:

Option	Action
Hostname	Change the hostname for the system (default is RCS_IPA)
IP address	Change the IP address and netmask
Gateway	Change the gateway
DNS	Change the DNS server (auto-detected if possible)

]HackingTeam[

Select IP address menu, then change IP and netmask.

The chosen IP address must be reachable from the RCS Network Controller (RNC).

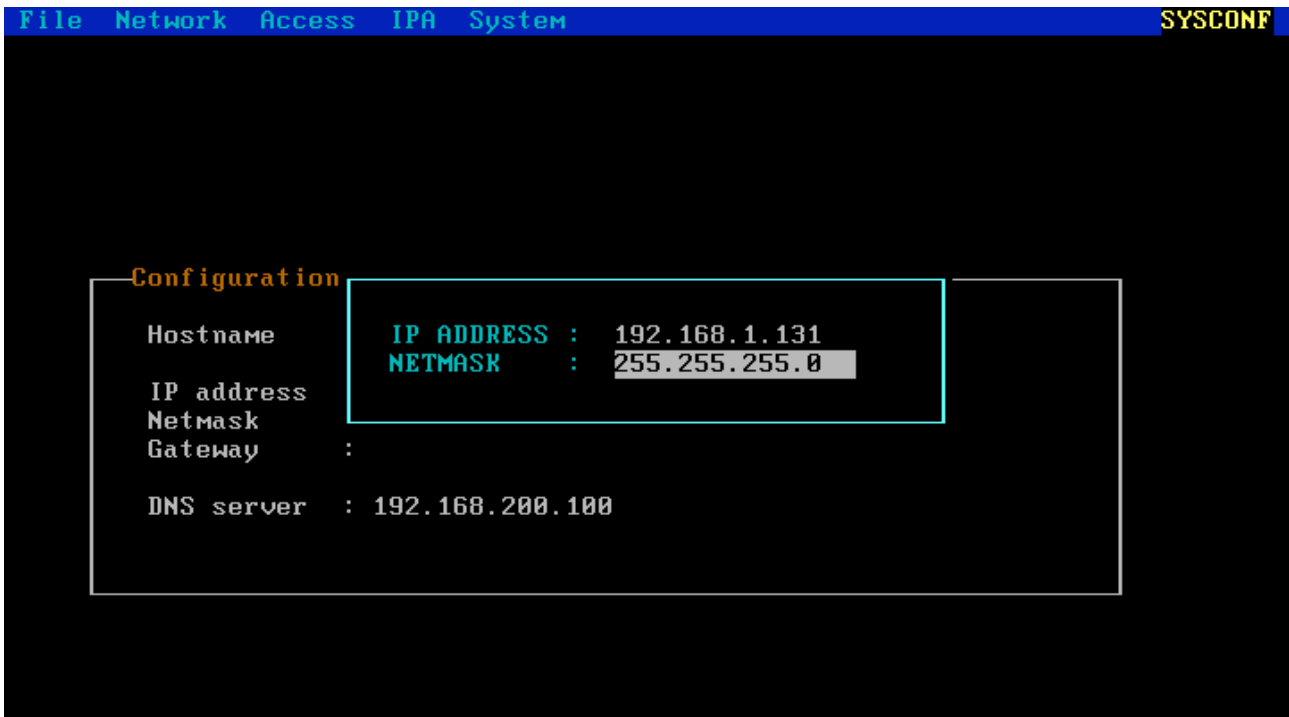


Figure 7 - Changing IP address and netmask

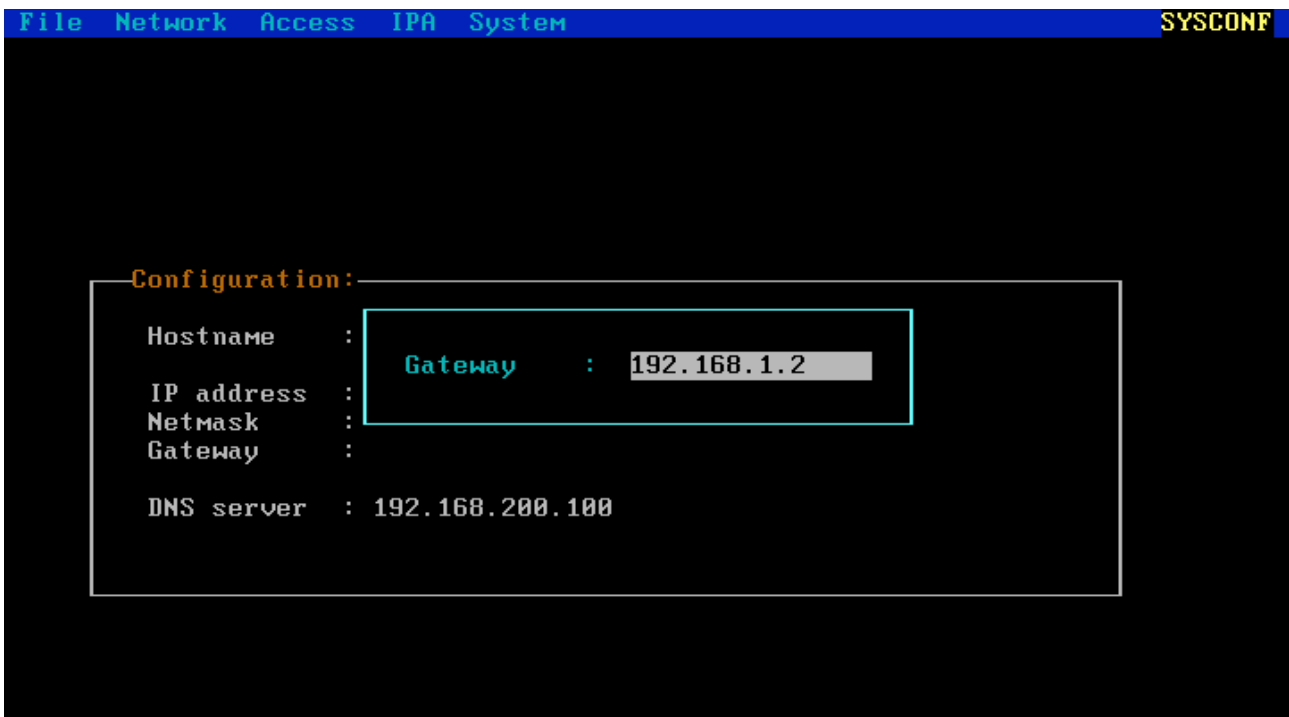


Figure 8 - Changing gateway

]HackingTeam[

```
File Network Access IPA System SYSCONF
Reload last conf C-r
Save configuration C-s
Activate configuration C-g
-
Exit C-x

Configuration:
-----
Hostname      : RCS_IPA
IP address    : 192.168.1.131
Netmask       : 255.255.255.0
Gateway       : 192.168.1.2
DNS server    : 192.168.200.100
```

Figure 9 - Saving the configuration

```
*
* A shell has been opened into the new filesystem.
* if you need to tune the new system before the first boot,
* do it now. You are in a chroot environment, so you can
* install a new kernel as you were in the live system.
*
* To finalize the installation exit from the current shell.
*
bash: no job control in this shell
livecd / # exit_
```

Figure 10 - Exiting from installation

```
* Installation completed
*
* Starting local ... [ ok ]

Welcome to the Gentoo Linux Minimal Installation CD!

The root password on this system has been auto-scrambled for security.

If any ethernet adapters were detected at boot, they should be auto-configured
if DHCP is available on your network. Type "net-setup eth0" to specify eth0 IP
address settings by hand.

Check /etc/kernels/kernel-config-* for kernel configuration(s).
The latest version of the Handbook is always available from the Gentoo web
site by typing "links http://www.gentoo.org/doc/en/handbook/handbook.xml".

To start an ssh server on this system, type "/etc/init.d/sshd start". If you
need to log in remotely as root, type "passwd root" to reset root's password
to a known value.

Please report any bugs you find to http://bugs.gentoo.org. Be sure to include
detailed information about how to reproduce the bug you are reporting.
Thank you for using Gentoo Linux!

livecd ~ # reboot_
```

Figure 11 - Rebooting the appliance

3.2 Post install configuration

Once the appliance rebooted, you can login into the system using the following default credentials:

Username: **root**

Password: **demorcs**

For your security, please change immediately the password for the root user.

Do not use a trivial password, and do not write it down anywhere.

By default, traffic monitoring and injection are both done on interface **eth0**.

If you have two network cards, you may want to use different ports for sniffing and injecting traffic, while if you have installed the IPA on an hardware accelerated appliance, you want to change the sniffing interface to use the accelerated network card.

To change how the network ports are used, edit the file **/rcsipa/etc/rcsredirect.conf**, then change the variables **sniffing_iface** and **response_iface** to the interfaces you want to use for each purpose.

In case you have hardware accelerated network cards, each port on them is named **dag0**, **dag1** and so on.

Non-accelerated network ports are named **eth0**, **eth1** and so on.

]HackingTeam[

In order to configure the communication with the RNC daemon, you have to copy two files from the Database server into the **/rcsipa/etc** directory:

- rcs-client.pem
- network.sig

Those two files can be found on the desktop of the database server in the RCS-Files directory.

NOTE: remember that the automatic configuration thru 'sysconfig' only configures the eth0. If you need special network configuration you have to edit /etc/conf.d/net accordingly. Please ask the HT support team how to do that.

3.3 Physical installation and cabling

Once the software has been installed onto the RCS IPA, you can proceed cabling the RCS IPA to the network segment to be monitored.

Strictly follow the configuration you made in the *rcsredirect.conf* file.

You can test the sniffing interface using *tcpdump*¹ (please refer to tcpdump manual for instructions on how to use it) to see if you discern the expected traffic.

When sniffing traffic to see if you are monitoring the correct network segment, try to look for target authentication factors, such as a specific IP address or Radius authentication headers.

The injection proxy also supports wifi connectivity. In this case you will need two different wifi network interface. One for monitor mode (sniffing) and one associated to the network you want to operate on. You also need to put the correct wifi password inside the *rcsredirect.conf* file.

The wifi key can be one of the following formats:

```
[WIFI]
wifi_key = "wep:64:s:\x12\x34\x56\x78\x90\x12\x34"
wifi_key = "wep:128:s:\x12\x34\x56\x78\x90\x12\x34\x56\x78\x90\xAB\xCD\xEF"
wifi_key = "wpa:psk:663eb260e87cf389c6bd7331b28d82f5203b0cae4e315f9cbb7602f3236708a6"
wifi_key = "wpa:pwd:password:BSSID"
```

¹ <http://www.tcpdump.org/>

4 IPA Configuration

Once the appliance has been installed and put in place, at least a first time configuration must be made.

4.1 *Registering the IPA*

The first step in using the RCS IPA is to register it using the RCSConsole.

Please refer to the Console User Manual (The Network Section -> Injection Proxies) for the registration procedure.

4.2 *Adding the rules*

A rule needs to be added to the IPA for each user and resource you want to inject.

Please refer to the Console User Manual (The Network Section -> Injection Proxies Rules) for adding a rule.

When adding a rule, a mean of identifying the target is needed: if operating within an ISP network, have them collaborate to provide you information about how to discriminate traffic from the target.

Otherwise, sniffing some traffic and analyzing it can be the only way you have to find out how to identify your target. In this respect, WireShark² is a very effective sniffing tool.

² <http://www.wireshark.org/>