]HackingTeam[

InjectionProxy

RCS Streamline Injection Proxy

Configuration and Deployment

]HackingTeam[

INDICE

Table of Contents

]HackingTeam[

Description - JProxy

Jproxy is a transparent proxy that can inject/change arbitrary data in downloaded pages/attachment during an HTTP session.
It supports HTTP 1.0 and HTTP 1.1 on clients that have at least Virtual Host support.
It runs on all Linux OS.

Configuration

You can configure the proxy editing the file /etc/jproxy.conf:

Default Options

The options have the form: option=value (no space between).
You can set 3 options:

- **default_backdoor= default_path/default_bd:** Set the default path of the backdoor
- **default_extension=.ext:** Set the default extension to match (eg: .exe)
- **infect_file_log=path/file:** Set the log file path

Operation Mode Options

You can set 4 different modes.
Modes are separated by at least an empty line.

```
[decoy]   // reply with a HTTP 404 No Page Found
entry1..
entry2..
(empty line)
[reject]  // close the connection immediately
entry..
(empty line)
[proxy]  // proxy the connection without calling injection hook chain
entry...
(empty line)
[inject]  // proxy the connection calling properly the injection hook chain entry...
```

[decoy],[reject] and [proxy] rules consist of one field **ip-range**. Possible values are:

192.168.100.1	(for a single host ip)
192.168.50.*	(subnet 192.168.50.0-192.168.50.255)
10.*	(subnet 10.0.0.0-10.255.255.255)

[inject] rules consist of 5 fields:

- **ip-range**
- **backdoor-path**
- **extension**
- **max_file_size**
- **max_infection_count**

eg:
```
192.168.10.*    /tmp/exe_bd      .exe     2000000     4
```
(this means jproxy infects .exe PE files downloaded from 192.168.10.0-192.168.10.255 subnet, where the file size is less than or equal to ~2Mb, at most 4 times)

in the `backdoor-path` and `extension` we can set a "*****" to tell proxy to use `default_backdoor` or `default_extension` values.

Executable Options Parameter

The installed binary "inject_proxy" accepts a number of options:

-h	help
-V	print version and exit
-c <file>	use different configuration file
-b <address>	use this as the bind address (default 0.0.0.0)
-p port	use this as the listen port (default 80)

Eg:
```
bash# inject_proxy -c ./my_config.conf -b 192.168.10.1 -p 8080
```
the above command runs the injection proxy on the IP address 192.168.10.1 and port 8080.

]HackingTeam[

Deployment And Scenarios

Jproxy can be used in 3 different contexts: **On Gateway, Gateway Redirection, Bridging.**

On Gateway

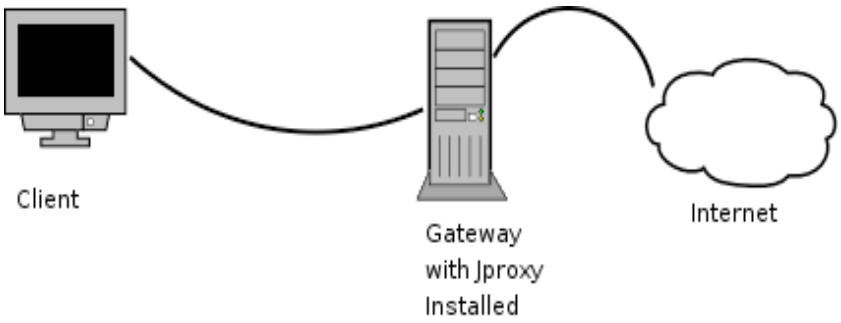
Prerequisites:

- Ability to install jproxy directly on the gateway
- Ability to redirect gateway traffic (local redirect/DNAT)
- Gateway is a Linux 2.4/2.6 box with NAT support

Involvements:

No Overhead and no new HW requirement

Scenario:



Logical Operations

We have to run the jproxy on the Gateway and redirect all the traffic of the target subnet/ip on the proxy itself (with iptables).
This is a standard reverse proxy configuration.

Gw Configuration Sample

```
iptables -t nat -A PREROUTING -s 10.0.0.0/24 -p tcp –dport 80 \
         -j DNAT –to-destination 10.0.0.1:8080
```

10.0.0.0/8 is the target subnet and 10.0.0.1:8080 is the local ip/port where inject_proxy is listening.

]HackingTeam[

Gateway Redirection

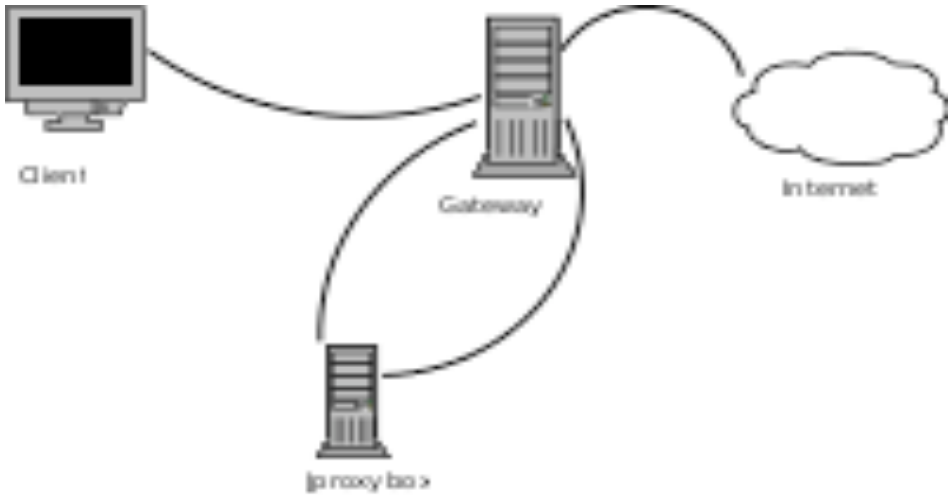
Prerequisites

- Ability to modify traffic on the Gateway (and possibly routing).
- GW must be a Linux 2.4/2.6 with iptables or a generic Firewall support.

Involvements

- Needs an external BOX for the Jproxy
- No overhead

Scheme:



Logical Operations

On the GW we redirect web traffic of the victim client to the jproxy box. On the jproxy box we get all web traffic and we forward request/reply through the GW itself (or different GW if we chose to use a different routing policy) .

Gw Configuration Sample

```
iptables -t nat -A PREROUTING -s 10.0.0.0/24 -p tcp –dport 80 -j DNAT \
         –to-destination 192.168.1.1:8080
```

10.0.0.0/24 is the target subnet, 192.168.1.1 is the jproxy box where we redirected web traffic.
In this case the GW must be enabled to route out the jproxy box traffic.

]HackingTeam[

Bridging

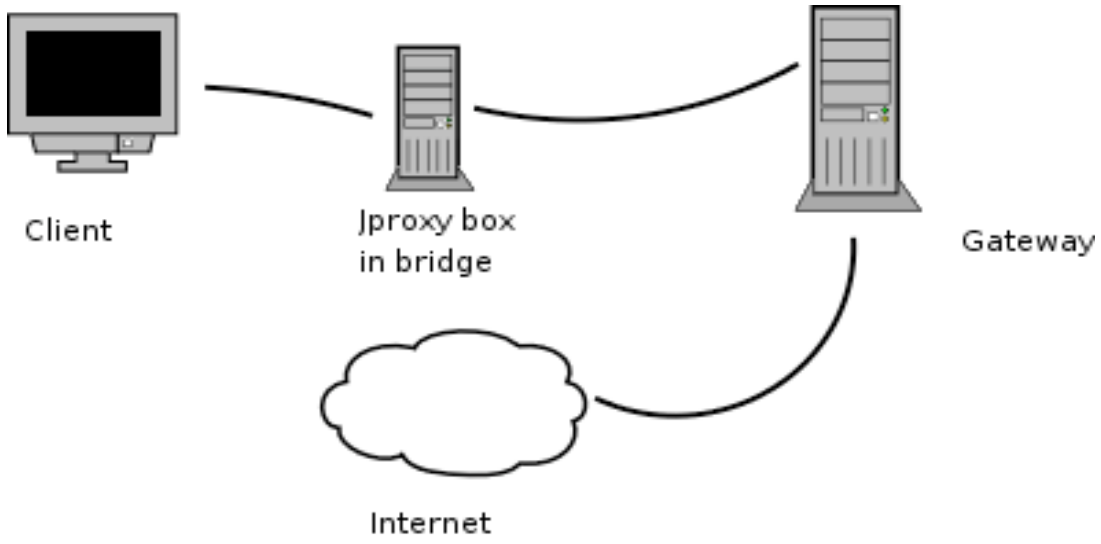
Prerequisites

No prerequisite.

Involvements

- Need an external box for the jproxy
- Need two ethernet interfaces on the jproxy box
- Jproxy box must have enough computational power to support all traffic between the victim client network and the GW

Scheme



Logical Operation

The Jproxy Box is placed between client network and GW. All traffic (not only web) passes through jproxy box and is forwarded transparently to the GW using bridged ethernet. Only web traffic is locally redirected to the jproxy box for inspection.