Table of Contents

Use iptables as Tarpit 3
- ***Install Software*** 3
- ***Configure Syslog-ng*** 4
- ***Useful Links*** 4

Use iptables as Tarpit

- A Tarpit is a service on a computer that delays incoming connections as long as possible. So the aggressor lost a lot of time.

Install Software

- **Tested with Ubuntu 10.04 Server 32-Bit.**
- For Arch there is a package available in AUR but it doesn't work as I tested it.

```
apt-get install xtables-addons-common xtables-addons-source
module-assistant --verbose --text-mode auto-install xtables-addons
```

- Finish: Now you can use Tarpit rules.
- For example:

```
iptables -A INPUT -p tcp --dport 20 -j TARPIT
```

- Unfortunately it seems impossible to make tarpit to the default action of a chain but you can tarpit to most recent ports.
- Example for very strict Rules:

```
/sbin/iptables -P FORWARD DROP
/sbin/iptables -P OUTPUT DROP
#allow answers to from inside established connections
/sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
#allow answers to from outside established connections on Port 80 and a ssh port
/sbin/iptables -A OUTPUT -p tcp --sport 80 -m state --state ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --sport 1234 -m state --state ESTABLISHED,RELATED -j ACCEPT
#allow connections to port 80
/sbin/iptables -A INPUT -p tcp --dport 80 -j ACCEPT
# Tarpit
/sbin/iptables -A INPUT -p tcp --dport 20 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 21 -j LOG -m limit --limit 20/min --log-prefix "FTP TARPIT: "
/sbin/iptables -A INPUT -p tcp --dport 21 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 22 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 23 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 25 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 110 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 143 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 443 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 445 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 220 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 993 -j TARPIT
```

```
/sbin/iptables -A INPUT -p tcp --dport 995 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 1080 -j TARPIT
/sbin/iptables -A INPUT -p tcp --dport 8080 -j TARPIT
########
##ssh host
/sbin/iptables -A INPUT -p tcp --dport 1234 -j ACCEPT
##logging
iptables -N LOGDROP
iptables -A LOGDROP -j LOG -m limit --limit 20/min --log-prefix "DROP: "
iptables -A LOGDROP -j DROP
# Drop all other traffic
iptables -A INPUT -j LOGDROP
#eof
```

- Hope at last I did not delete too much away. Before I did it the rule set was working.

Configure Syslog-ng

- Syslog-ng logging all messages according to iptables in:

  ```
  /var/log/syslog
  ```

- To create a single logging file you must reconfigure Syslog-ng:

```
filter f_iptables { facility(kern) and match("IN=") and match("OUT="); };
destination d_iptables { file("/syslog/iptables/$YEAR-$MONTH/iptables.log-$DAY"); };
log { source(s_all); filter(f_iptables); destination(d_iptables); flags(final); };
```

- These lines contain a final flag, that means after matching this filter the message processing end. So the message from iptabels doesn't appear in the file:

  ```
  /var/log/syslog
  ```

- You must add these line to syslog-ng config before the standard destinations are defined and after the standard sources.

Useful Links

Honeypot Projekt A Honeypot for example takes all request to a network none other answer and seems to answer it.

From:
https://www.eanderalx.org/ - **EanderAlx.org**

Permanent link:
https://www.eanderalx.org/linux/iptables_as_tarpit?rev=1287142554

Last update: **15.10.2010 11:35**