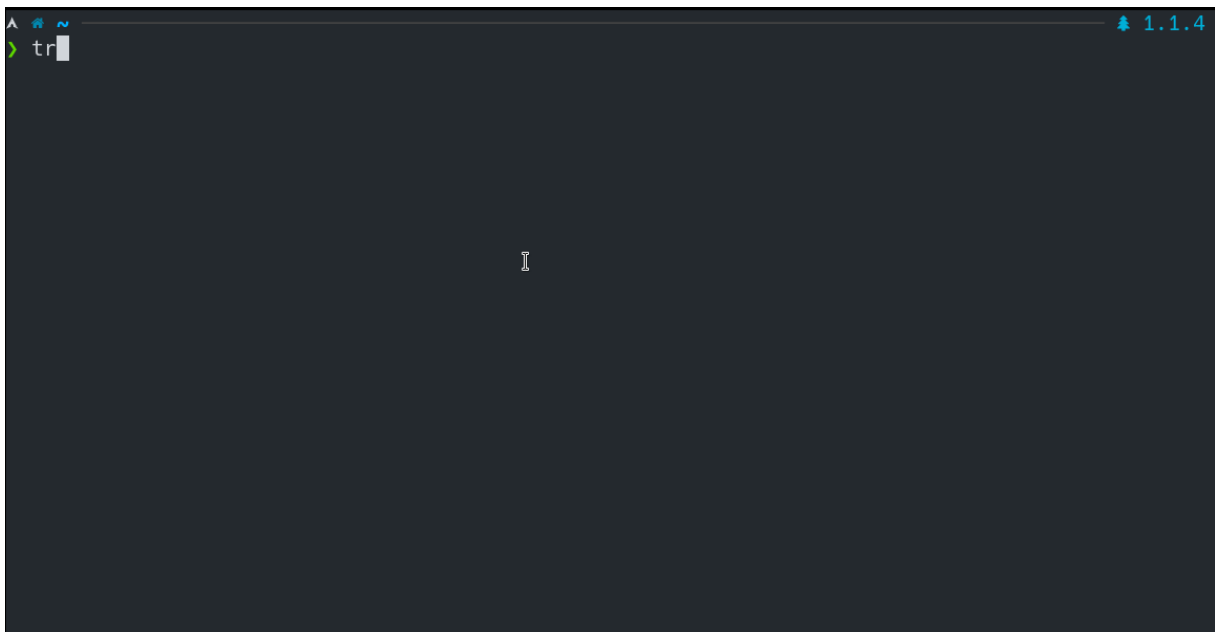

Traitor

Automatically exploit low-hanging fruit to pop a root shell. Linux privilege escalation made easy!

Traitor packages up a bunch of methods to exploit local misconfigurations and vulnerabilities in order to pop a root shell:

- Nearly all of GTFOBins
- Writeable `docker.sock`
- CVE-2022-0847 (Dirty pipe)
- CVE-2021-4034 (pwnkit)
- CVE-2021-3560



It'll exploit most sudo privileges listed in GTFOBins to pop a root shell, as well as exploiting issues like a writable `docker.sock`, or the recent dirty pipe (CVE-2022-0847). More routes to root will be added over time too.

Usage

Run with no arguments to find potential vulnerabilities/misconfigurations which could allow privilege escalation. Add the `-p` flag if the current user password is known. The password will be requested if it's needed to analyse sudo permissions etc.

```
1 traitor -p
```

Run with the `-a/--any` flag to find potential vulnerabilities, attempting to exploit each, stopping if a root shell is gained. Again, add the `-p` flag if the current user password is known.

```
1 traitor -a -p
```

Run with the `-e/--exploit` flag to attempt to exploit a specific vulnerability and gain a root shell.

```
1 traitor -p -e docker:writable-socket
```

Supported Platforms

Traitor will run on all Unix-like systems, though certain exploits will only function on certain systems.

Getting Traitor

Grab a binary from the releases page, or use go:

```
1 CGO_ENABLED=0 go get -u github.com/liamg/traitor/cmd/traitor
```

For go1.18:

```
1 CGO_ENABLED=0 go install github.com/liamg/traitor/cmd/traitor@latest
```

If the machine you're attempting privesc on cannot reach GitHub to download the binary, and you have no way to upload the binary to the machine over SCP/FTP etc., then you can try base64 encoding the binary on your machine, and echoing the base64 encoded string to `| base64 -d > /tmp/traitor` on the target machine, remembering to `chmod +x` it once it arrives.

In The News

- 20/06/21: Console 58 - Awesome newsletter featuring tools and beta releases for developers.
- 28/04/21: Intigriti Bug Bytes #120 - Recommended tools
- 09/03/21: Hacker News thread