Reverse Engineering

Übung 1 - Gruppe 3

Ludwig Karpfinger	Armin Jeleskovic	Valentin Altemeyer
ludwig.karpfinger@hm.edu	a.jeleskovic@hm.edu	valentin.altemeyer@hm.edu

Aufgabe 1 - REMnux installieren

Aufgabe 2 - REMnux Tool Check

a) Aus welchen Quellen kann ein Tool von REMnux stammen?

Remnux kann wie jede andere Linux-Distro Software aus den angegebenen Quellen installieren. (abgesehen von sonstigen Paketmanagern, wie *snap, flatpack, AppImage*) Folgender Befehl zeigt die Repos an:

```
$ sudo grep -Erh ^deb /etc/apt/sources.list*
```

Es fällt auf, dass ein spezielles Remnux Repo vorhanden ist namens:

http://ppa.launchpad.net/remnux/stable/ubuntu. Diese Repo wurde durch *remnux.sls* hinzugefügt[1]

Die Besonderheit bei Remnux ist, dass der *Remnux Installer* automatisch Software installiert, konfiguriert und aktualisiert. Die Eigenschaften von Software, wie Download-Quelle, Installation Path, Hashnummer, Rechte, Abhängigkeiten und Configs, werden durch sogenannte *state files* bestimmt. Diese Files befinden sich auf GitHub und werden durch den *Remnux Installer* geladen.

[1] https://github.com/REMnux/salt-states/blob/master/remnux/repos/remnux.sls

Remnux nutzt gemäß den Remnux Docs[2] folgende Installationsquellen:

- pip
- gems
- npm
- apt Repos

b) Welche Tools stammen nicht aus Open Source Quellen?

Das Github Repo wurde im Ordner */Documents/* gecloned.

Lösung mit *grep*:

```
$ grep -r --include="*.sls"
> -Eio "source: (http|https)://[a-zA-Z0-9./?=_%:-]*"
> /home/remnux/Documents/salt-states/remnux/
> | grep -v "github"
> | cut -d'/' -f10
> | uniq -u
```

Output:

```
snapshots.mitmproxy.org
www.netresec.com
didierstevens.com
www.nowrap.de
bitbucket.org
www.mitec.cz
www.nowrap.de
www.cert.at
www.netresec.com
www.didierstevens.com
radare.mikelloc.com
```

Erklärung:

Es wird *command-chaining* verwendet. Das Tool *grep* sucht mittels *regex* nach allen URLs in allen *.sls* files. Ergebnisse, die den String *github* beinhalten, werden ausgeschlossen. Der *cut* Befehl filtert beim Output die Domains heraus. Der *uniq* Befehl eliminiert alle doppelten Ergebnisse.

[2] `https://docs.remnux.org/behind-the-scenes/technologies/debian-packages`

Aufgabe 3 - File Classification

Aufgabe 4 - Firmware Identifikation