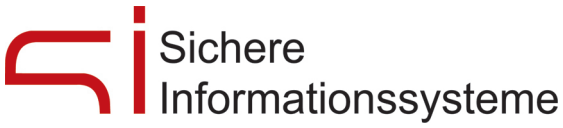


Reverse Engineering (REV3)

UE 05 – Firmware Analyse – Protokoll

Jakob Mayr

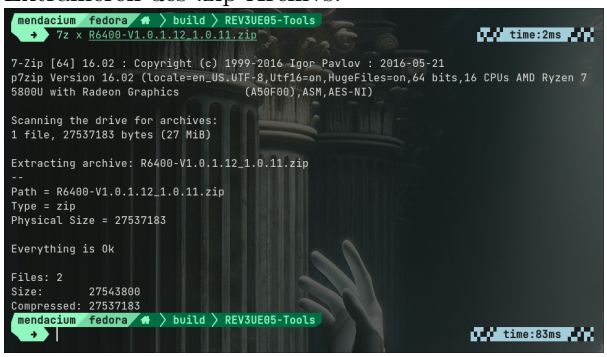
WS 2023/2024

File-Beschaffung

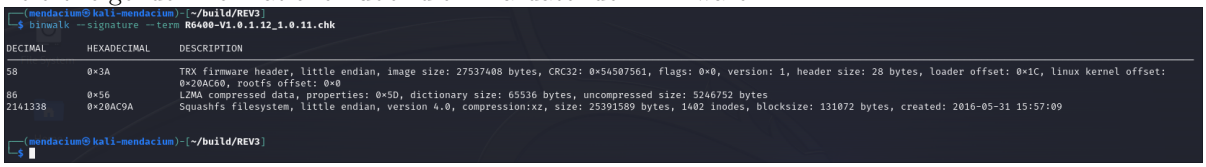
Die benötigte Firmware-Version kann direkt auf der netgear-Seite heruntergeladen werden:
`https://www.downloads.netgear.com/files/GDC/R6400/R6400-V1.0.1.12_1.0.11.zip`

Analyse Teilkomponenten

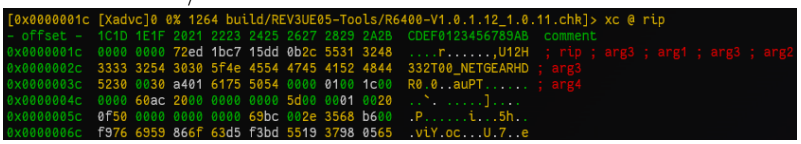
Extrahieren des .zip-Archivs:



Die Ausführung des Befehls `binwalk` mit der Option `--signature` auf die Datei `r6400-V1.0.1.12_1.0.11.chk` liefert folgende Informationen über die Binärdatei der Firmware:



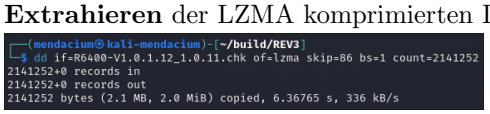
- **TRX Firmware-Header:** Das Binärbild enthält einen TRX Firmware-Header, der häufig bei Firmware-Dateien für Router oder ähnliche Geräte verwendet wird. Er ist in Little-Endian-Format mit einer Größe des Images von 27.537.408 Bytes und enthält einen CRC32-Prüfsummenwert. Betrachtet man den Bootloader an Stelle **0x1C** ("loader offset"), so findet man zu Beginn einen String "**U12H332T00_NETGEARHDR0.0**"(radare2 visual mode). Dies könnte eine Information über Name/Version des Bootloaders darstellen:

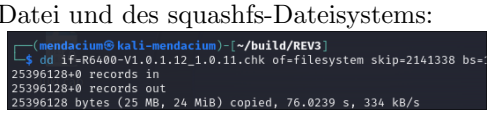


- **LZMA komprimierte Daten:** Der Teil der Datei enthält LZMA-komprimierte Daten. Dies schließt Eigenschaften, eine Wörterbuchgröße und die unkomprimierte Größe ein.
- **Squashfs-Dateisystem:** Das Binärbild umfasst ein Squashfs-Dateisystem. Squashfs ist ein komprimiertes, schreibgeschütztes Dateisystem für Linux. Die Version, der Kompressionstyp (xz), die Größe, die Anzahl der Inodes, die Blockgröße und das Erstellungsdatum werden ebenfalls angegeben.

Das Erstellungsdatum des Squashfs-Dateisystems ist der 31. Mai 2016 um 15:57:09 Uhr.

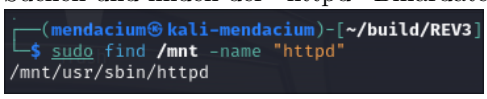
Extrahieren der LZMA komprimierten Datei und des squashfs-Dateisystems:





"**Mounten**" des Dateisystems in "`/mnt`":

Suchen und finden der "httpd"-Binärdatei:



httpd

Informationen (radare2) über die Binärdatei: