TRUE STORY

USING DFIR TECHNIQUES TO RECOVER FROM INFRASTRUCTURE OUTAGES

Xavier Mertens | PTS23 | TLP:CLEAR

ONCE UPON A TIME…

- This is a **true** story but no firewall was hurt during the making of these slides!
- It started with a firewall crash…
- The appliance was rebooting a random intervals
- After a few days, it died… RIP!

$CUSTOMER CALLED ME

$Customer: “We have a firewall issue! We had a look and the SSD seems dead…”

Me: “Ok, do you have a spare SSD?”

$Customer: “Yes, we bought one on Amazon and we are ready to replace it”

Then the “magic” question arised:

Me: “Do you have a backup to restore the firewall config?”

$Customer: “… <silence> …”

LACK OF BACKUP PROCESS

- Well, $Customer had a backup but an old one (a few months old)
- Based on the frequent security policy updates, it would have cost a lot of time to restore everything!
  From a Consultant point of view, it’s intere$ting 🥳…
- The very beginning of the SSD was corrupt, preventing the OS to boot.
- What about trying to recover the previous config? 🤞🏻

IMAGING THE FIREWALL SSD

- First, let’s take an image of the faulty SSD
- Connect the acquisition laptop with a cross-cable to the firewall
- Boot the firewall via an USB stick, setup a NIC
  - Firewall: 192.168.254.1/24
  - Laptop: 192.168.254.2/24

IMAGING THE FIREWALL SSD (2)

- Start a listener on the laptop

```
# nc -l -p 8888 >pfsense.raw
```

- Image the SSD:

```
# dd if=/dev/mmcsd0 | nc 192.168.254.2 8888
```

- Light a candle and pray! 🙏🏻

EXTRACT THE CONFIGURATION

- Hopefully, the firewall was a pfSense, the current configuration is an XML file stored in /conf/config.xml. Having the config in a real DB would complicate the operations
- Which tool to use to extract the file from the disk image?
- My first attempt was bulk_extractor but it was too verbose. It looks for "structured information" (email addresses, credit card numbers, URLs, images, …).

LET'S MEET SCALPEL

- Scalpel is part of the well-known Sleuth kit (you probably know “autopsy”). The tool is pretty old (released in 2005) but it does the job.
- Scalpel helps to search for specific files based on “rules”, similar to YARA. Example:

```
# GIF and JPG files (very common)
gif    y    5000000      \x47\x49\x46\x38\x37\x61   \x00\x3b
gif    y    5000000      \x47\x49\x46\x38\x39\x61   \x00\x00\x3b
jpg    y    200000000    \xff\xd8\xff\xe0\x00\x10     \xff\xd9
jpg    y    200000000    \xff\xd8\xff\xe1             \xff\xd9
```

https://github.com/sleuthkit/scalpel

LET'S FINETINE SCALPEL

- The pfSense XML file is bit strange and Scalpel must be fine-tuned to detect them properly:

```
xml     n   10000000    <?xml    </pfsense>
```

- Let's run Scalpel against the disk image…

https://github.com/sleuthkit/scalpel

LET'S RUN SCALPEL

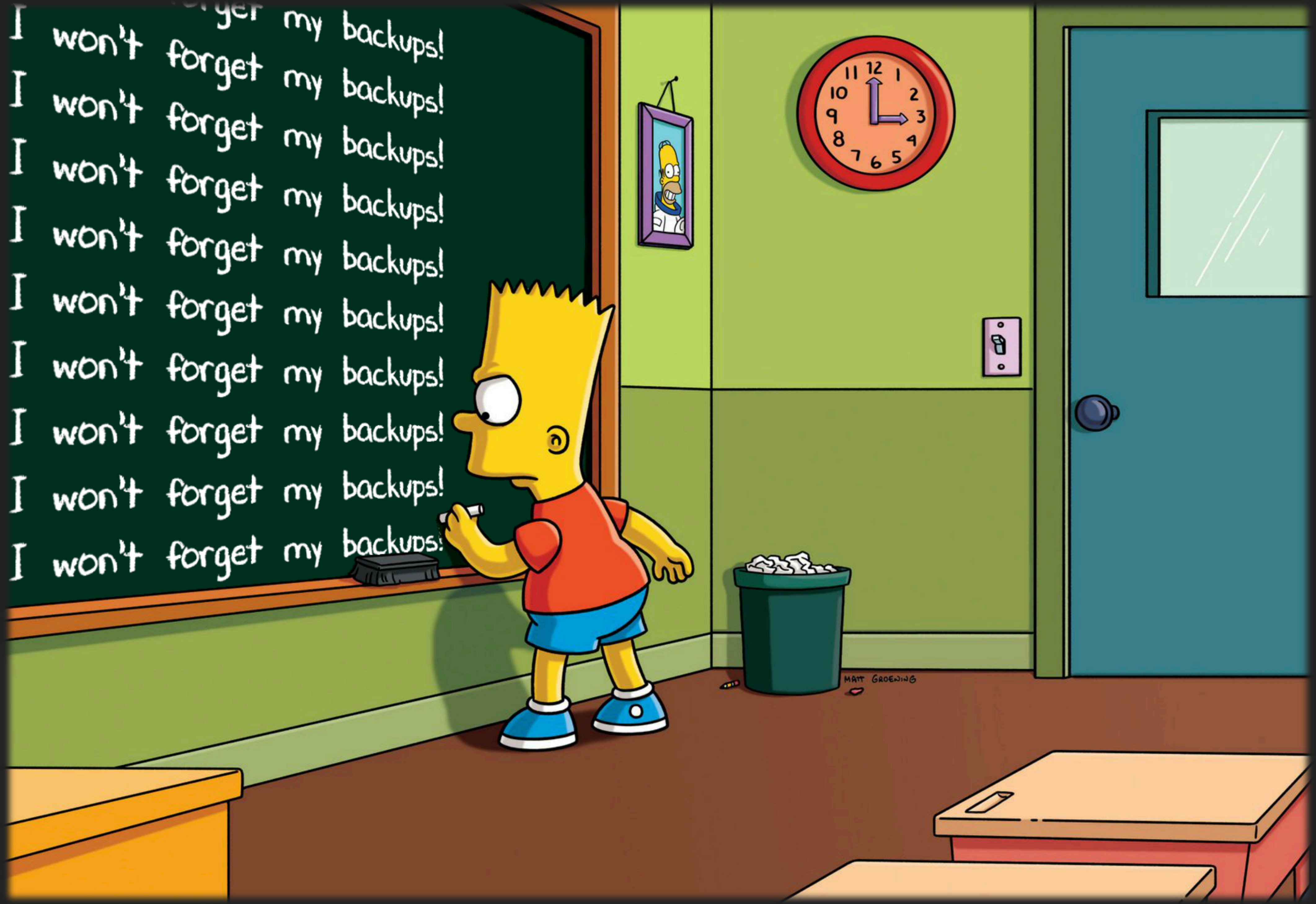
- Multiple files were found:

```
Scalpel version 1.60 audit file
Started at Thu May 22 12:28:06 2023
Command line:
scalpel -c /etc/scalpel/scalpel.conf -o /tmp/carved pfsense.raw
Output directory: /tmp/carved
Configuration file: /etc/scalpel/scalpel.conf
Opening target "H="
The following files were carved:
File          Start           Chop        Length        Extracted From
00000003.xml    156532736        NO          8384365        pfsense.raw
00000002.xml    156368896        NO          8548205        pfsense.raw
00000001.xml    156303360        NO          8613741        pfsense.raw
…
```

LET’S RUN SCALPEL

- After some manual checkes (based on the last changes), we identified the right configuration file
- The firewall was reinstalled from scratch, the restored configuration file copied at the right location, reboot and all was back!
- Beers! 🍻 🍻 🍻

THANK YOU, AND...


I won't forget my backups!
I won't forget my backups!
I won't forget my backups!
I won't forget my backups!
I won't forget my backups!
I won't forget my backups!
I won't forget my backups!
I won't forget my backups!
I won't forget my backups!
I won't forget my backups!
MATT GROENING