



Downloading a needle in a haystack

T-REX 2026

07/10/2026

- **Red Team**
 - access to the internal network
 - target the hypervisors
 - recent vulnerabilities affect vCenter
 - CVE-2026-59309 (authentication bypass)
 - CVE-2026-59310 (RCE as root)

- **You gain access to the hypervisor**
 - you are happy
 - you want to retrieve the secrets of a domain controller
 - you decide to download the virtual machine's disk

Post-exploitation

DC01

ACTIONS

Summary

Monitor

Configure

Permissions

Datstores

Networks

Snapshots

Updates

Guest OS



LAUNCH REMOTE CONSOLE ⓘ

LAUNCH WEB CONSOLE

Virtual Machine Details

ACTIONS ▾



Power Status

Powered On

Guest OS

Microsoft Windows Server 2019 (64-bit)

VMware Tools

Not running, not installed ⓘ

DNS Name

IP Addresses

Encryption

Not encrypted



Usage

Last updated: 10/1/26, 6:00 PM

CPU

 0 MHz used

Memory

 0 MB used

Storage

 329.08 GB used

VIEW STATS

Problem

- **Downloading the disk contents will take ages**
 - multiple disks may be present and there is no way of knowing which one holds the interesting secrets
- **You do not have a NAS to store the contents**
- **Bandwidth monitoring can lead to a detection**

- **Exfiltration virtual machine**
 - clone the virtual machine to free the read lock
 - create a virtual machine
 - with the cloned disk attached
 - with a small disk for exfiltration (a few gigabytes)
 - copy the desired files onto the small disk
 - download the small disk
 - downside: tedious and time-consuming

- **Drop a binary on the hypervisor**
 - drop a binary (e.g. VMkatz) that will read the disk and extract the desired secrets
 - pre-requisite: gain shell access on the hypervisor
 - downside: not versatile

What is a disk

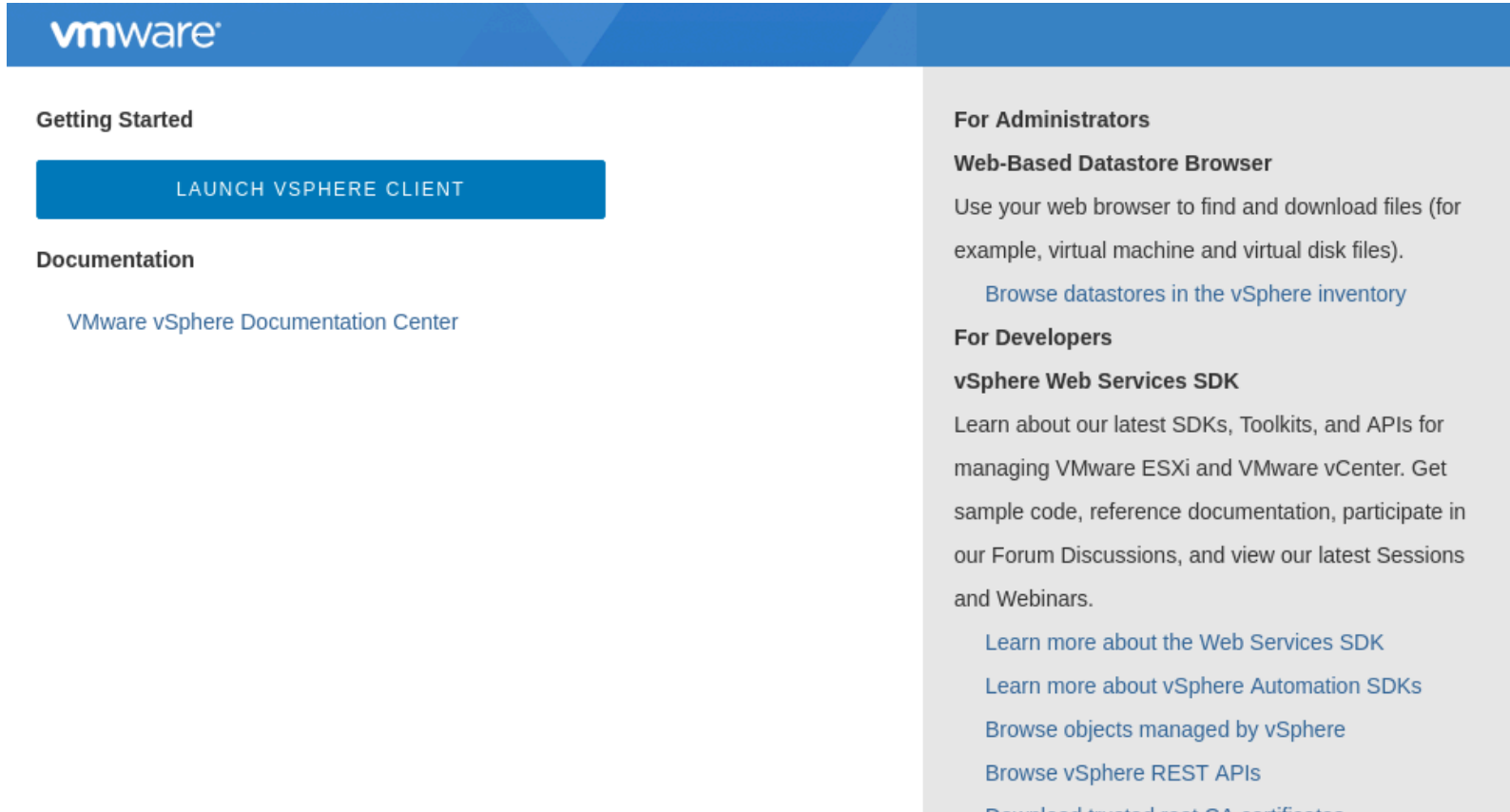
- **A disk is composed of partitions**
 - MBR / GPT
- **These partitions hold file systems**
 - ext4, NTFS
- **These file systems hold files**
 - on NTFS, Master File Table

Proposed solution

- **Find a way to read disks at a certain offset / size**
 - not possible through the standard UI
- **Read and parse the file system to retrieve only the files we are interested in**

Partial downloads

- vSphere hypervisors expose an endpoint to download files



The screenshot displays the VMware vSphere client interface. At the top, the VMware logo is visible. Below it, the 'Getting Started' section features a prominent blue button labeled 'LAUNCH VSPHERE CLIENT'. Under the 'Documentation' section, a link for 'VMware vSphere Documentation Center' is provided. On the right side, a sidebar lists resources for administrators and developers. The 'For Administrators' section includes a 'Web-Based Datastore Browser' with a description of its function and a link to 'Browse datastores in the vSphere inventory'. The 'For Developers' section includes the 'vSphere Web Services SDK' with a description and links to 'Learn more about the Web Services SDK', 'Learn more about vSphere Automation SDKs', 'Browse objects managed by vSphere', and 'Browse vSphere REST APIs'.

vmware

Getting Started

LAUNCH VSPHERE CLIENT

Documentation

VMware vSphere Documentation Center

For Administrators

Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

[Browse datastores in the vSphere inventory](#)

For Developers

vSphere Web Services SDK

Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESXi and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

[Learn more about the Web Services SDK](#)

[Learn more about vSphere Automation SDKs](#)

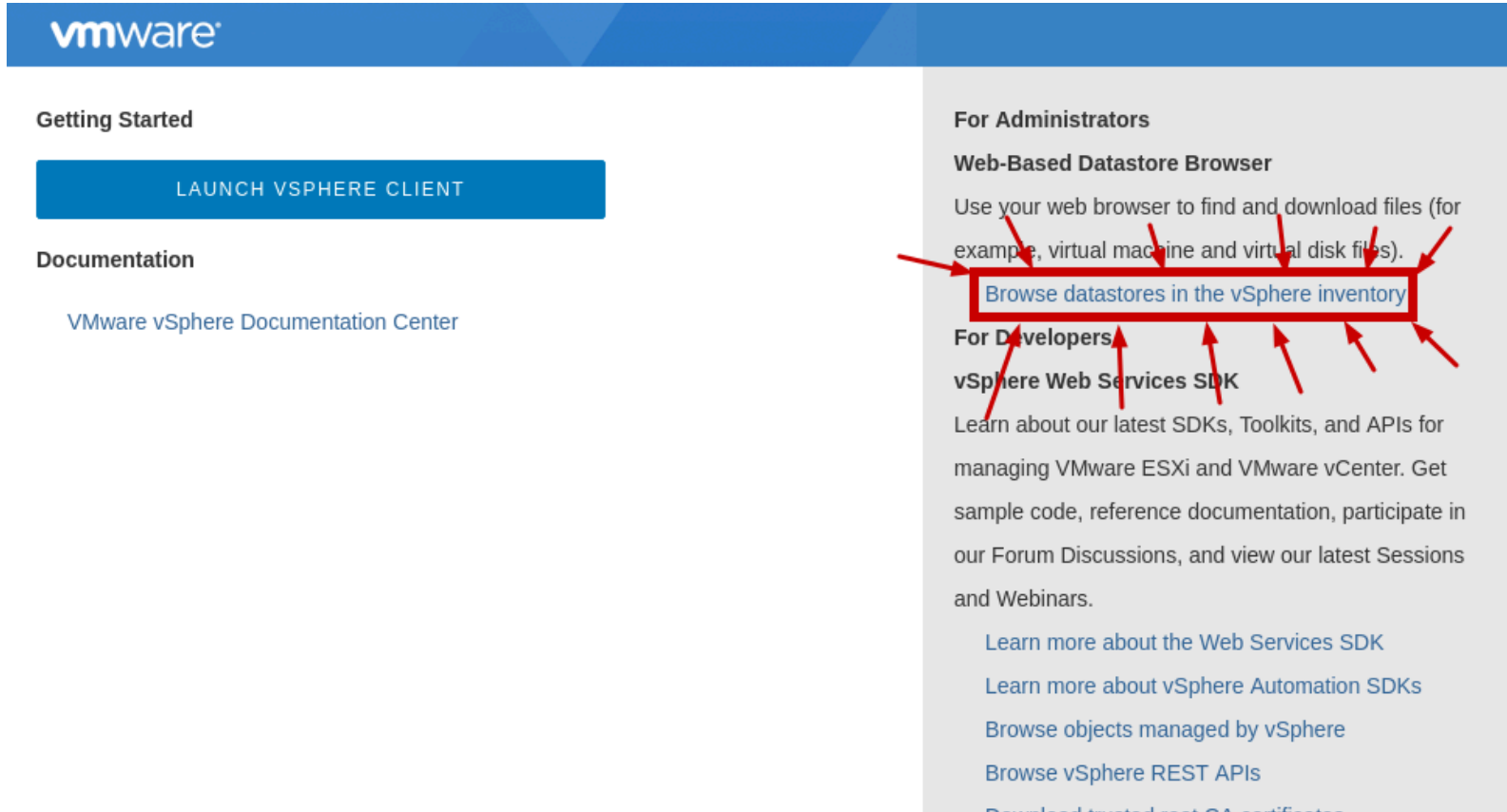
[Browse objects managed by vSphere](#)

[Browse vSphere REST APIs](#)

[Download trusted root CA certificate](#)

Partial downloads

- vSphere hypervisors expose an endpoint to download files



vmware

Getting Started

LAUNCH VSPHERE CLIENT

Documentation

VMware vSphere Documentation Center

For Administrators

Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

[Browse datastores in the vSphere inventory](#)

For Developers

vSphere Web Services SDK

Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESXi and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

[Learn more about the Web Services SDK](#)

[Learn more about vSphere Automation SDKs](#)

[Browse objects managed by vSphere](#)

[Browse vSphere REST APIs](#)

[Download trusted root CA certificate](#)

Partial downloads

- Complete directory listing of all datastores

Home	Logout	
Index of DC01 on datastore main-datastore in datacenter Datacenter		
Name	Last modified	Size
Parent Directory		-
DC01-000001-sesparse.vmdk	27-Sep-2026 08:31	125833216
DC01-000001.vmdk	27-Sep-2026 08:13	304
DC01-1.scoreboard	25-Sep-2026 17:18	7391
DC01-2.scoreboard	25-Sep-2026 17:18	7391
DC01-3960f029.hlog	25-Sep-2026 17:17	221
DC01-Snapshot1.vmem	27-Sep-2026 08:14	4294967296
DC01-Snapshot1.vmsn	27-Sep-2026 08:14	12062296
DC01-b2cc056b.vswp	27-Sep-2026 08:27	4294967296
DC01-flat.vmdk	27-Sep-2026 08:13	26843545600
DC01.nvram	25-Sep-2026 17:36	270840
DC01.scoreboard	27-Sep-2026 08:31	7391
DC01.vmdk	25-Sep-2026 17:21	444
DC01.vmsd	27-Sep-2026 08:13	412
DC01.vmx	27-Sep-2026 08:13	3135
DC01.vmx.lck	25-Sep-2026 17:18	0
DC01.vmx~	27-Sep-2026 08:13	3128
vmware-1.log	25-Sep-2026 17:18	124030
vmware-2.log	25-Sep-2026 17:18	124044

Partial downloads

- **Supports the Range header**

- e.g. I want to download the first 100 bytes of the disk

```
$ curl -kv -H 'Range: bytes=0-99' [...] \  
'https://vcenter.lab.local/folder/DC01/DC01-flat.vmdk?dcPath=Datacenter&dsName=main-datastore' | xxd  
[...]
```

```
< HTTP/2 206  
< accept-ranges: bytes  
< content-range: bytes 0-99/26843545600  
< content-length: 100  
[...]
```

```
00000000: 33c0 8ed0 bc00 7c8e c08e d8be 007c bf00 3.....|.....|..  
00000010: 06b9 0002 fcf3 a450 681c 06cb fbb9 0400 .....Ph.....  
00000020: bdb0 0780 7e00 007c 0b0f 850e 0183 c510 ....~..|.....  
00000030: e2f1 cd18 8856 0055 c646 1105 c646 1000 .....V.U.F...F..  
00000040: b441 bbaa 55cd 135d 720f 81fb 55aa 7509 .A..U..]r...U.u.  
00000050: f7c1 0100 7403 fe46 1066 6080 7e10 0074 ....t..F.f`.~..t  
00000060: 2666 6800 &fh.
```

Parsing and reading disks

- **Partial read primitive found**
- **How do we parse file systems painlessly?**
 - multiple existing tools can parse and read many file formats
 - qemu-nbd / mount
 - guestmount
 - VMkatz

Parsing and reading disks

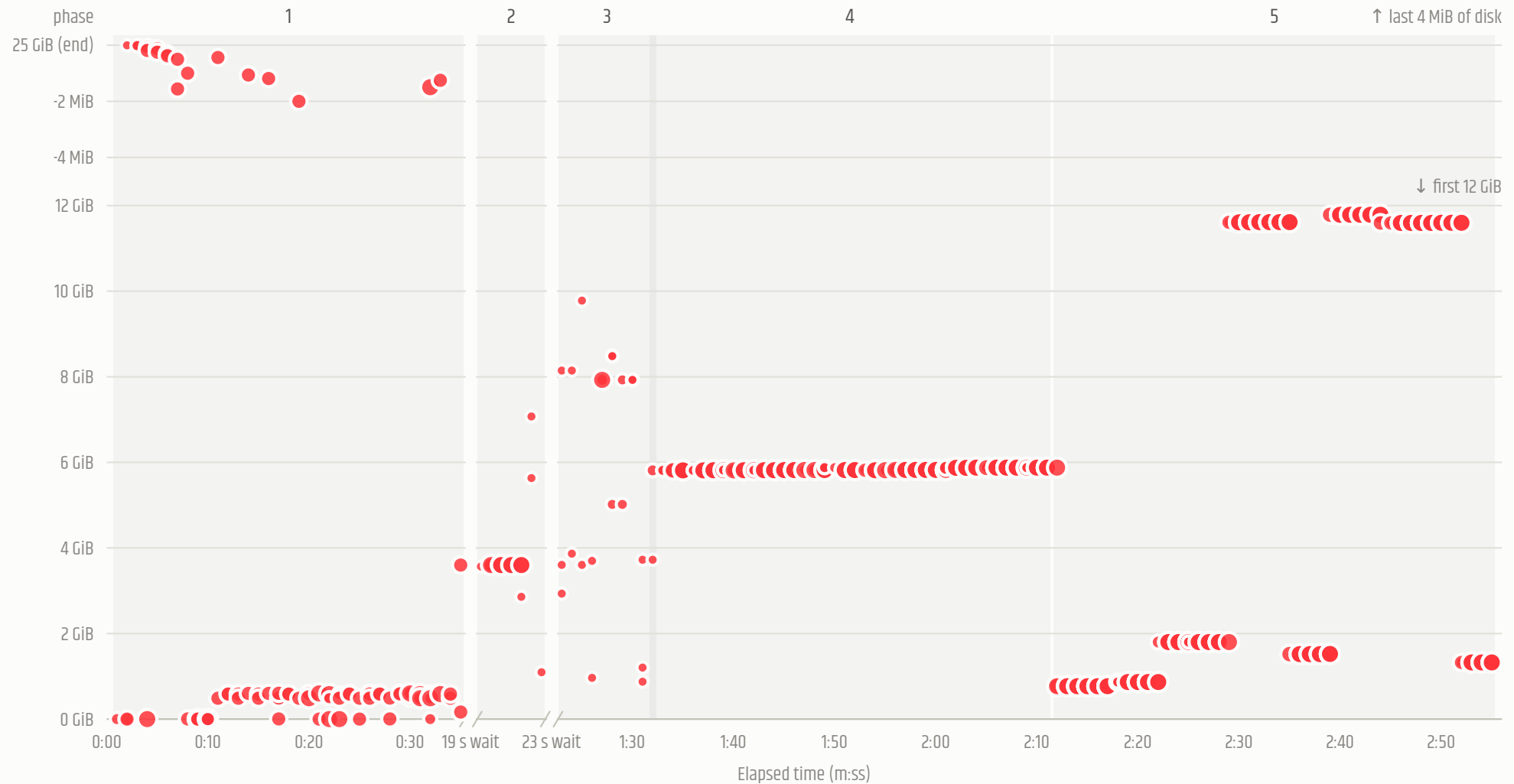
- **FUSE (Filesystem in UserSpaceE)**
 - software interface that lets you create file systems as a low-privileged user
 - e.g. sshfs, guestmount
- **We can create a FUSE driver**
 - kernel calls **read()** → we make an HTTP request with the Range header
 - kernel calls **readdir()** or **getattr()** → we make an HTTP request to the directory listing

Demo

- **Terrible performance**
 - 90 seconds with 2600 NTDS entries, longer depending on network latency / bandwidth
- **Still better than downloading the disk**
 - 2 hours and 20 minutes (25GB at 3MB/s)
- **Can we improve its performance?**

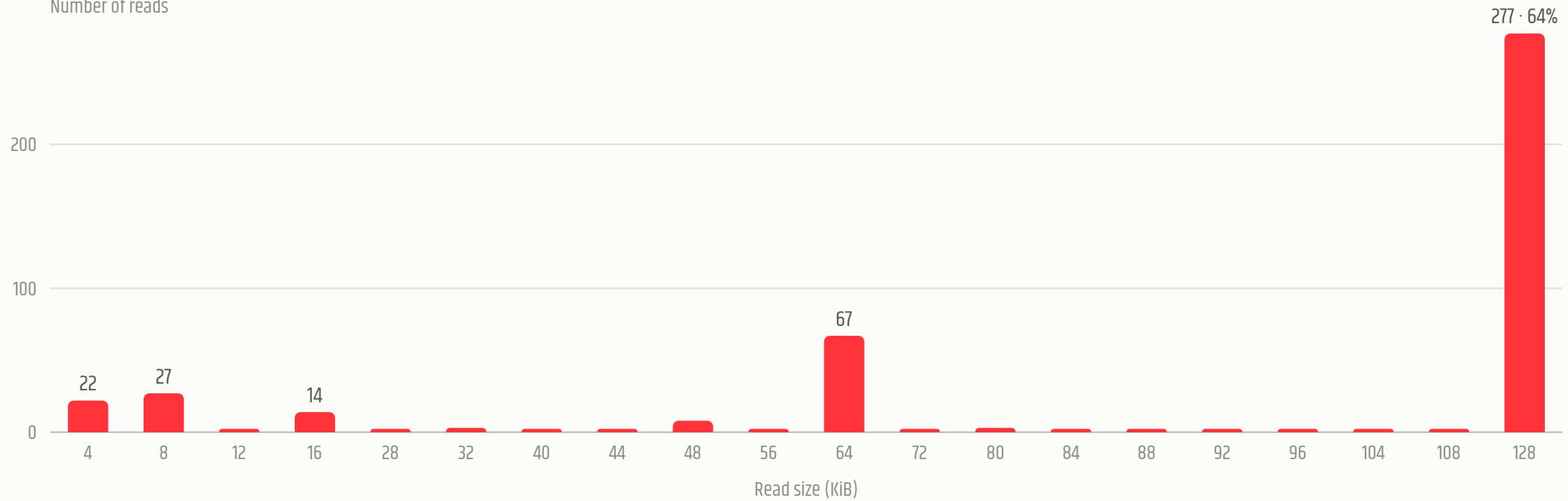
Performance

Disk access over time



Read size distribution

Number of reads



- **Maximum read size: 128KB**
 - limit defined in the FUSE module of the Linux kernel
 - no one wants to recompile that
- **HTTP requests are expensive (in time)**
 - latency
 - sending the request
 - waiting for the server to process the request (constant)
 - receiving the response
- **Reading 20MB of contiguous data will make 160 HTTP requests**
- **Data is often contiguous**
- **Conclusion: to maximize throughput, we must make less HTTP requests**

- **Simple readahead logic**

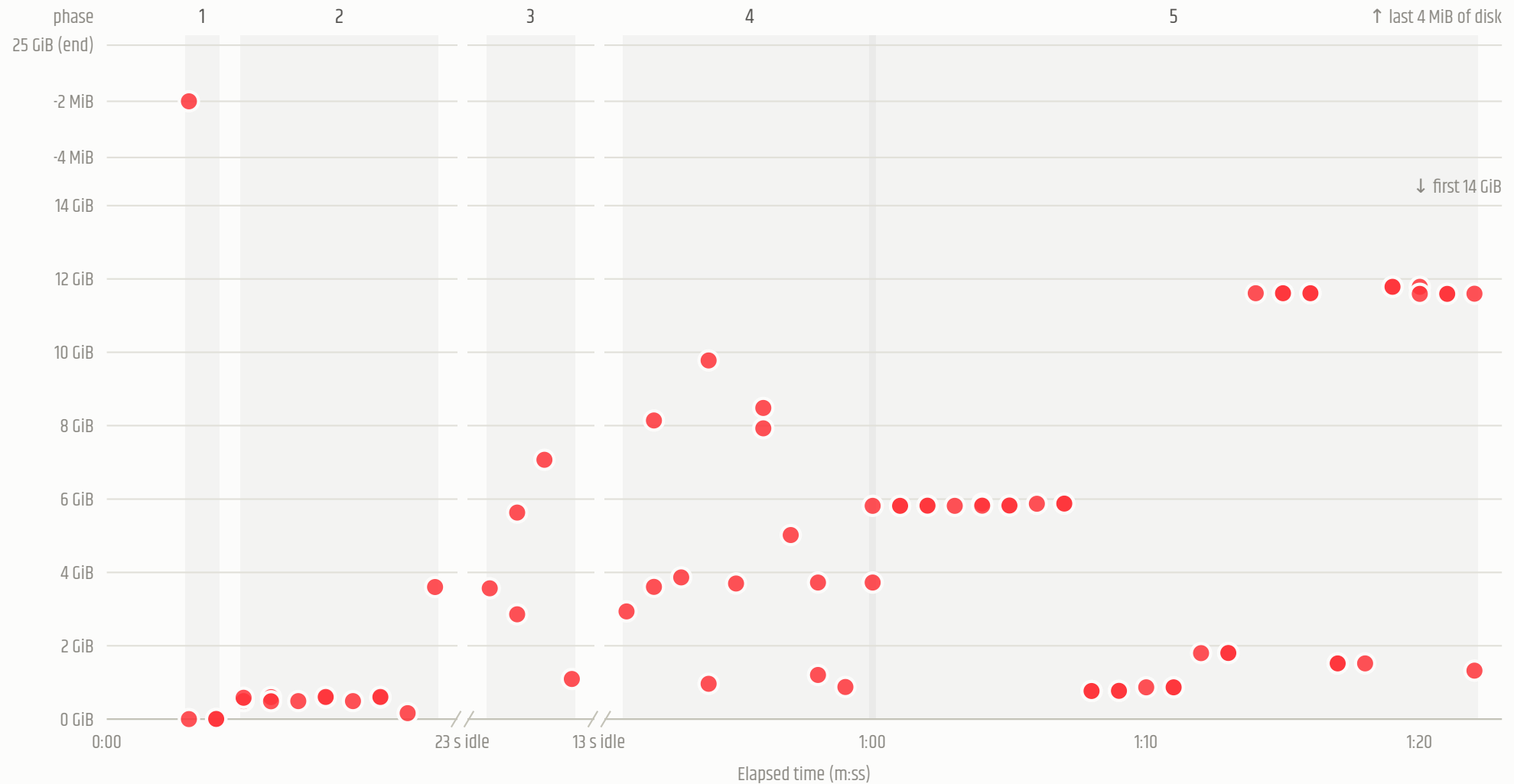
- we divide the disk in chunks of 2MB
- if the kernel wants to read bytes from that chunk, we download it and put it in a cache
- any subsequent reads in the chunk are retrieved from the cache

- **Time divided by 3**

- 30 seconds with 2600 NTDS entries in the lab

Performance

Disk access over time



Pre-requisites

- **ESX 3.5 or later (should be 100% of the time)**
 - Datastore browser enabled by default
- **Sufficient rights on the vCenter / ESX**
 - clone virtual machines (for live machines)
 - access the datastore browser



- Extensible
 - Artifactory example
- Everything is logged

<https://github.com/synacktiv/fusetea/>



<https://www.linkedin.com/company/synacktiv>



<https://twitter.com/synacktiv>



<https://synacktiv.com>

Un incident ? Contactez csirt@synacktiv.com.