
BACK TO THE FUTURE
OWNING SYSTEMS OF THE PAST

About Us

- Brendan Dolan-Gavitt (@moyix) & Nick Gregory (@kallsyms)
- AI (and more!) @ XBOW

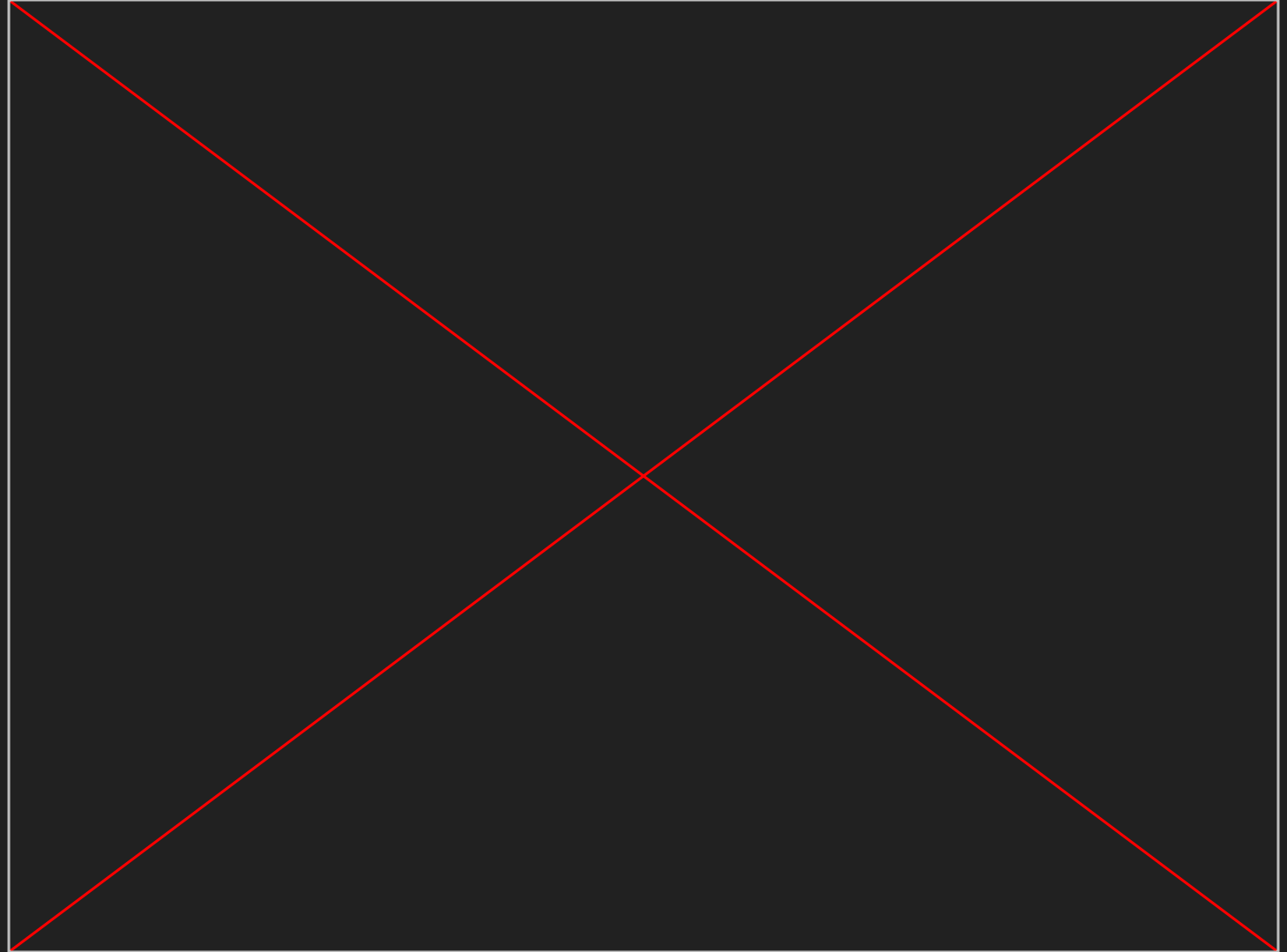
Overview

- Reverse Engineering (where bugs??)
- Emulator (how do i run??)
- Environment (debug pls)
  - Reproducible sample running
- Validators (no cheating kthx)

- Used codex + GPT 5.4/5.5/5.6

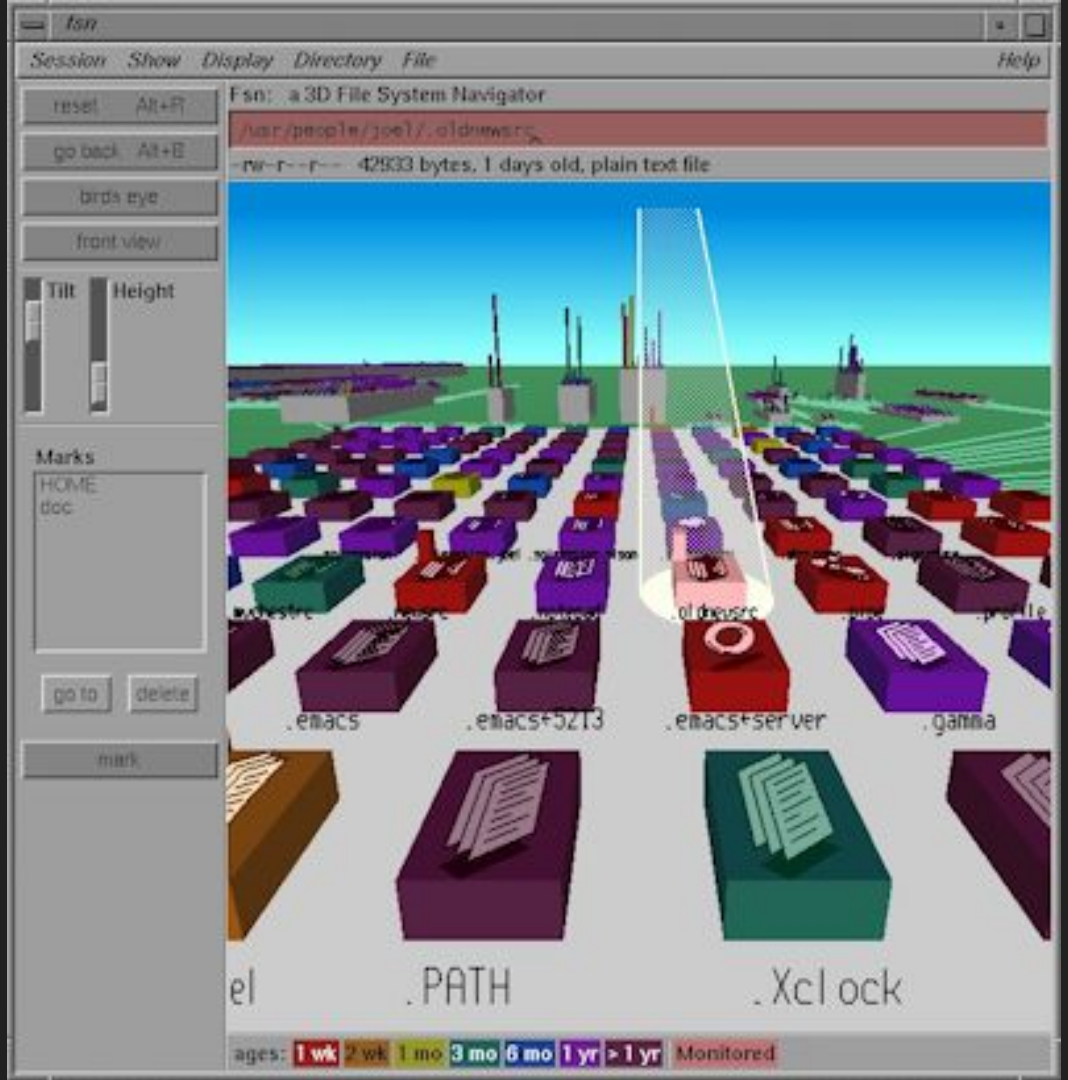
Roadblocks

- Not only bugs & exploits, but the emulator to run things in
- Archaeology required
  - Some licensing systems had to be bypassed…



Roadblocks

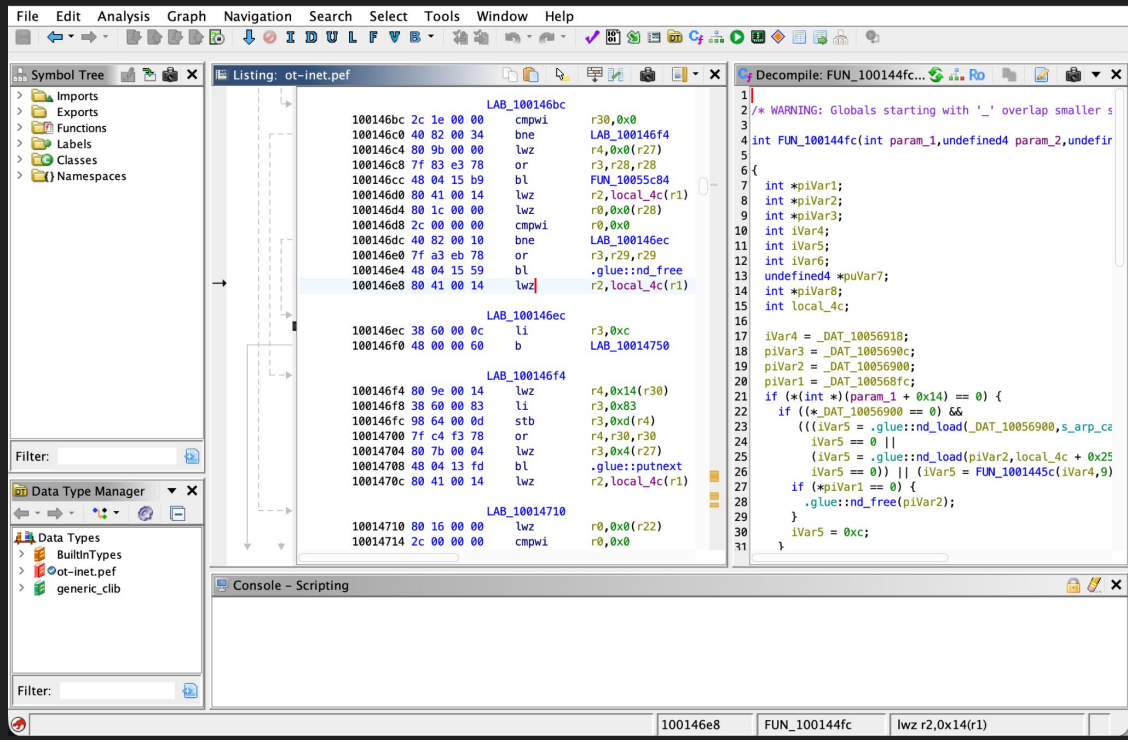
- Not only bugs & exploits, but the emulator to run things in
- Archaeology required
  - Some licensing systems had to be bypassed…
  - N different versions of libraries
- What even is the attack surface?
- Target selection


fsn
Session Show Display Directory File Help
reset Alt+R
go back Alt+B
birds eye
front view
Tilt
Height
Marks
HOME
doc
go to
delete
mark
Fsn: a 3D File System Navigator
/usr/people/joel/.oldnewsrc
-rw-r--r-- 42933 bytes, 1 days old, plain text file
.emacs
.emacs+5213
.emacs+server
.gamma
el
.PATH
.Xclock
ages: 1 wk 2 wk 1 mo 3 mo 6 mo 1 yr > 1 yr Monitored

RE

- Two strategies
  - GhidraMCP
  - Pre-decompilation

- “First you must ~~invent~~ RE the universe”



Emulators

- VAX on Alpha floating point
- Standalone emulators too slow, missing snapshots, etc.
- Standardize on QEMU
  - Snapshots
  - Performance
  - Forks are free, you can just make them

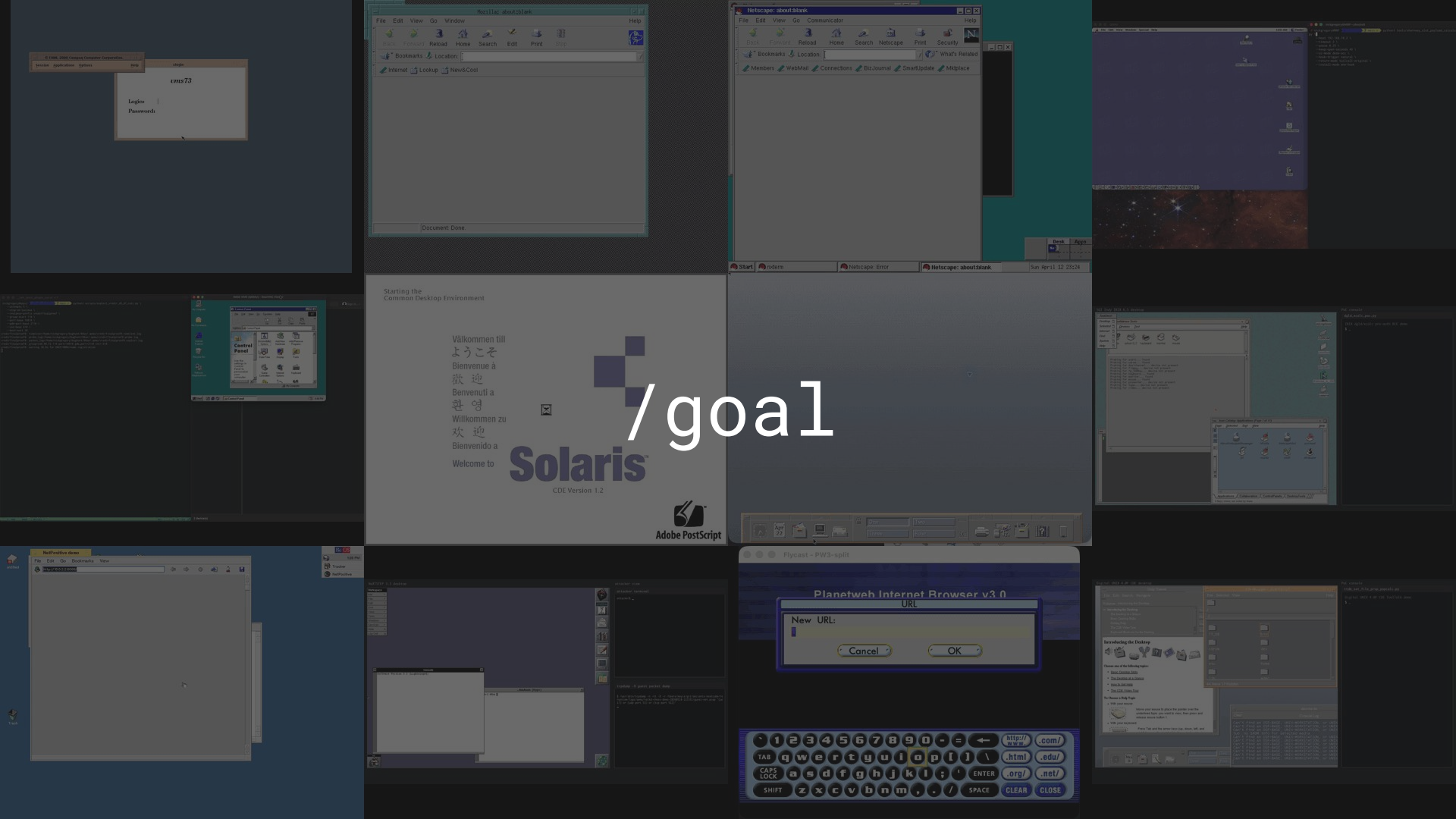
Environments

- Hunting down minor revisions
- Normal tomfoolery of OSs at the time
- How do the models debug on the systems?
  - Models picked dumb ways of doing things, taking 10 mins
  - Noninvasive hooking
  - Using detours + infra for doing this
- How do the models control the systems?
  - VNC keystrokes/mouse -> No
  - telnet/ssh in guest

Validation

- Flags (à la CTF)
  - Very in-distribution
  - Even without /goal, ran for days
- Screenshots

- No cheating!
  - Don’t have to make it foolproof from the start - telling it “no” will generally prevent that behavior down the line
  - No GDB!!1

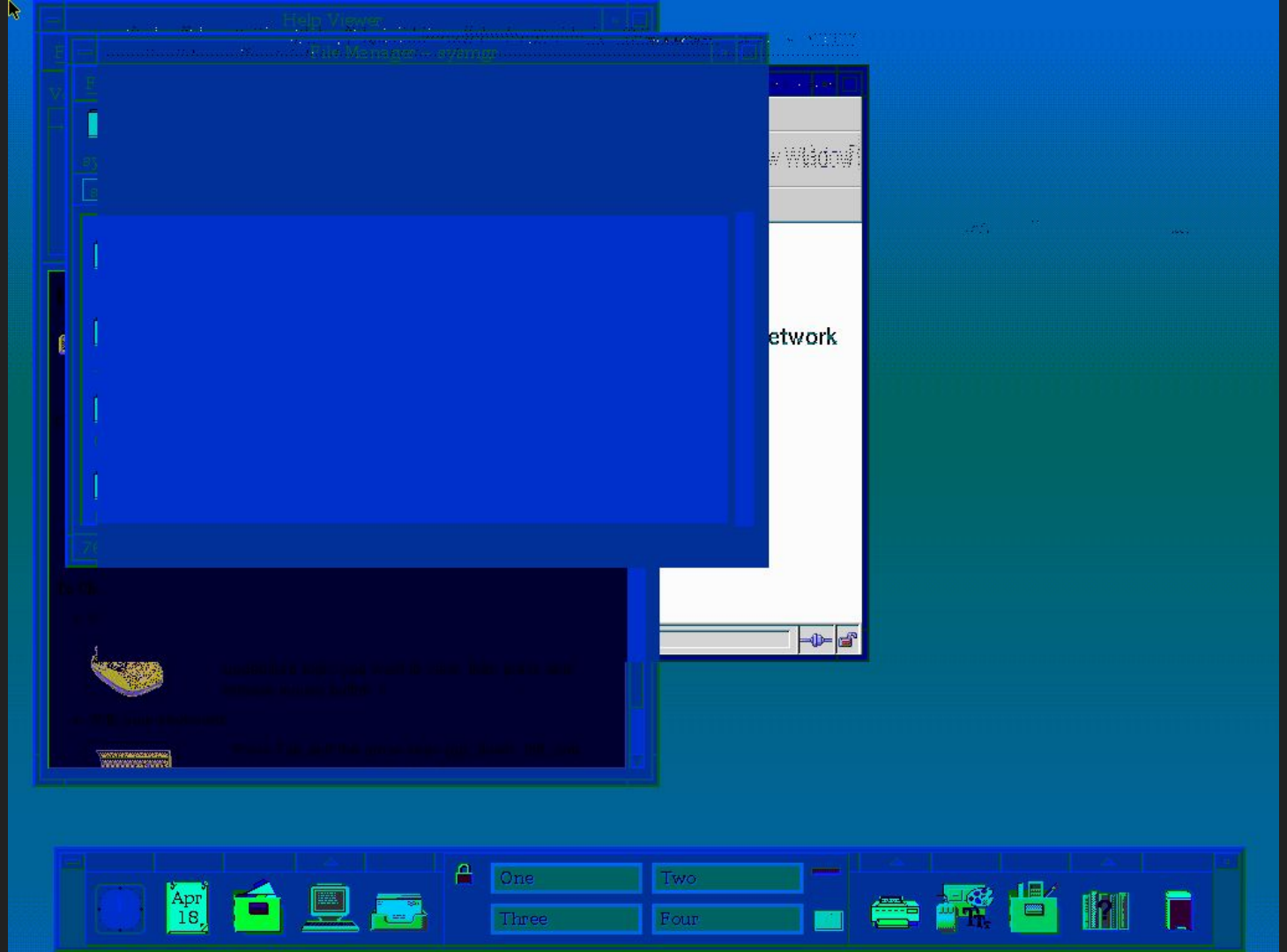

/goal

Model Weaknesses

- Modeling/testing externally
  - Belief old and new (or stock and custom) things are equivalent
- Not realizing its probing is messing things up (new images)
- Out of distribution
  - Esoteric architectures
  - Trying things in-distribution that don’t apply (tcache doesn’t apply to solaris libc…)
- Weaseling out of hard problems
  - Custom heap implementations
  - No patching binaries

Model Floundering

- 12 hours chasing… NULL deref
- “LGTM” with obvious graphics corruption


Help Viewer
etwork
Apr
18
One
Two
Three
Four

Model Floundering

- 12 hours chasing… NULL deref
- “LGTM” with obvious graphics corruption
- Cheating with GDB
- Cheating with ~~SSH~~ telnet

Targets (Browser)

- Mosaic 2.4, OpenVMS VAX 7.3
- Netscape 4.07, RHEL 5.2 i386
- Netscape 5.0, RHEL 5.2 i386
- IE 5, Solaris 2.6 SPARC (x2)
- Compaq Secure Web Browser, OpenVMS 8.3 Alpha
- Planetweb, Dreamcast SH-4
- WorldWideWeb.app, NeXTSTEP 3.3 68k
- NetPositive 2.2, BeOS 5.0 PPC

Targets (Core Network/Services)

- Mac OS 9.2.1, PowerPC
- Windows 98 SE, i386
- IRIX 6.5, MIPS
- Solaris 2.6, SPARC (x2)
- Tru64, Alpha

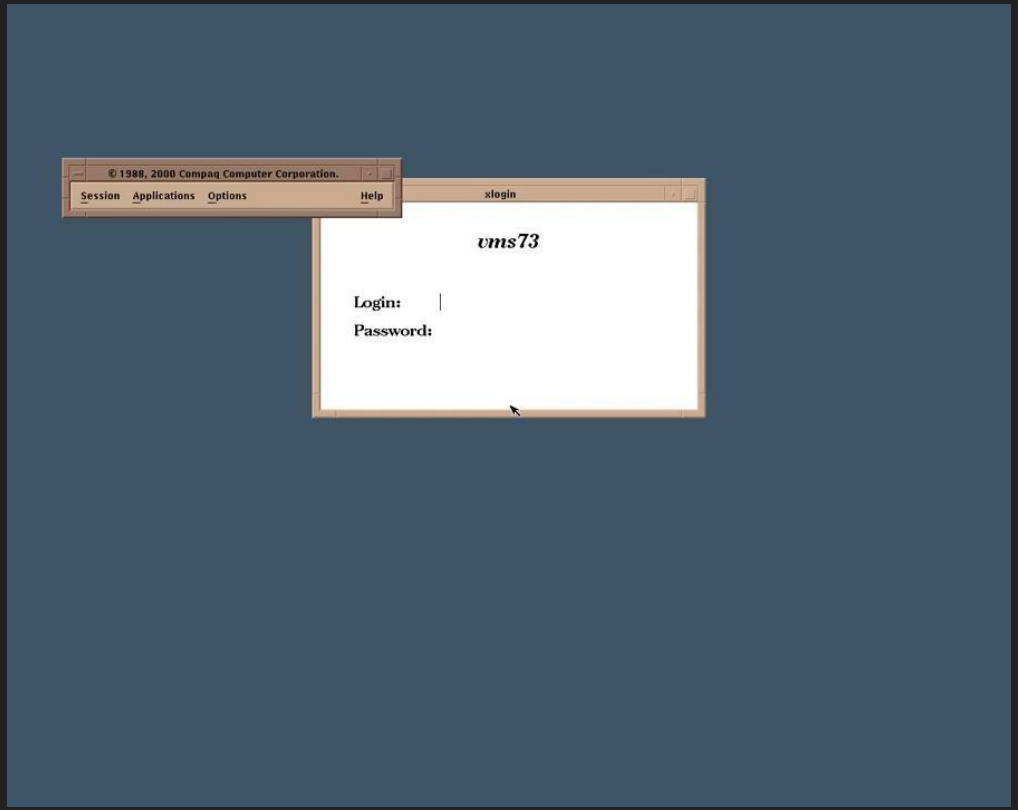
Targets (Other)

- FTP client, Symbolics Virtual Lisp Machine on Tru64 Alpha


vms73
Login:
Password:
Mozilla: about:blank
Netscape: about:blank
Starting the
Common Desktop Environment
Welcome to
Solaris
CDE Version 1.2
Adobe PostScript
Planetweb Internet Browser v3.0
URL
New URL:
Cancel
OK

The Fun Part

Mosaic 2.4, OpenVMS VAX 7.3



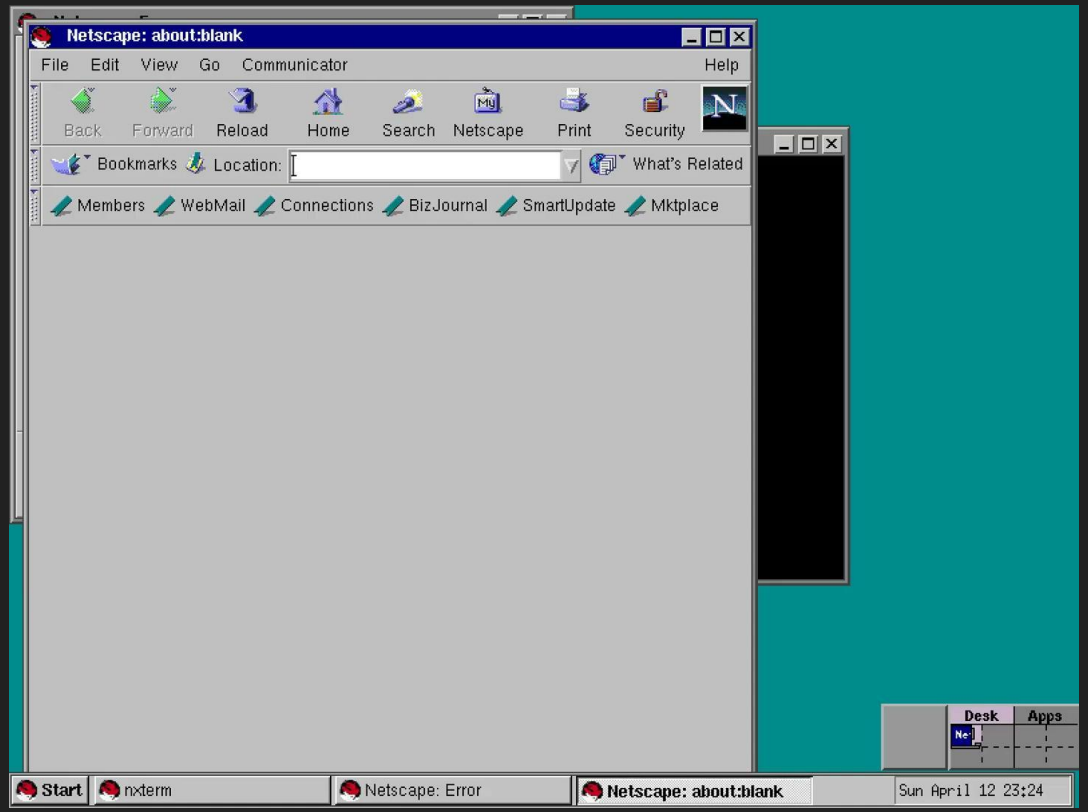
Sam Tobin-Hochstadt
@samth

If you are running Mosaic 2.4 on a VAX, please be aware that we are going to study your brain for science.

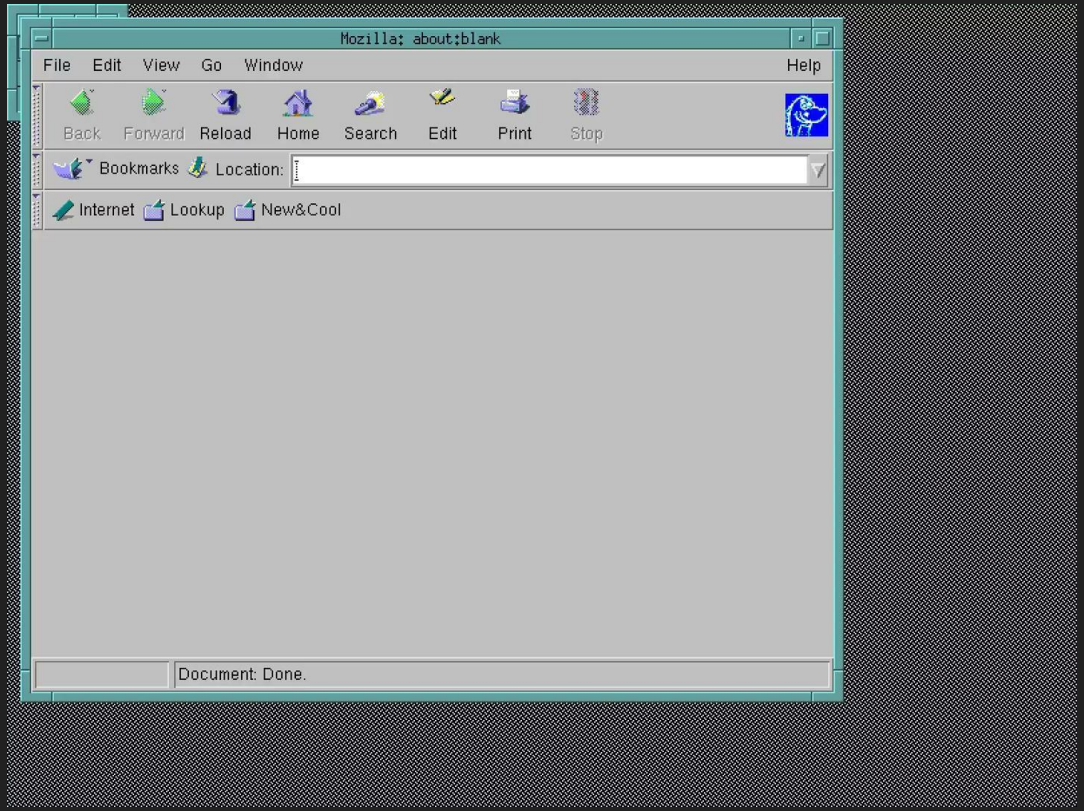
thaddeus e. grugq
@thegrugq

BREAKING: Do not sit on this!
If you are using this software you are vulnerable to a zero day. A piece of hacker code that unlocks your computer to viruses and malware.
AI has turbocharged hackers. They can now built cyber antiVAX systems faster than vendors can respond!

Netscape 4.07, RHEL 5.2 i386



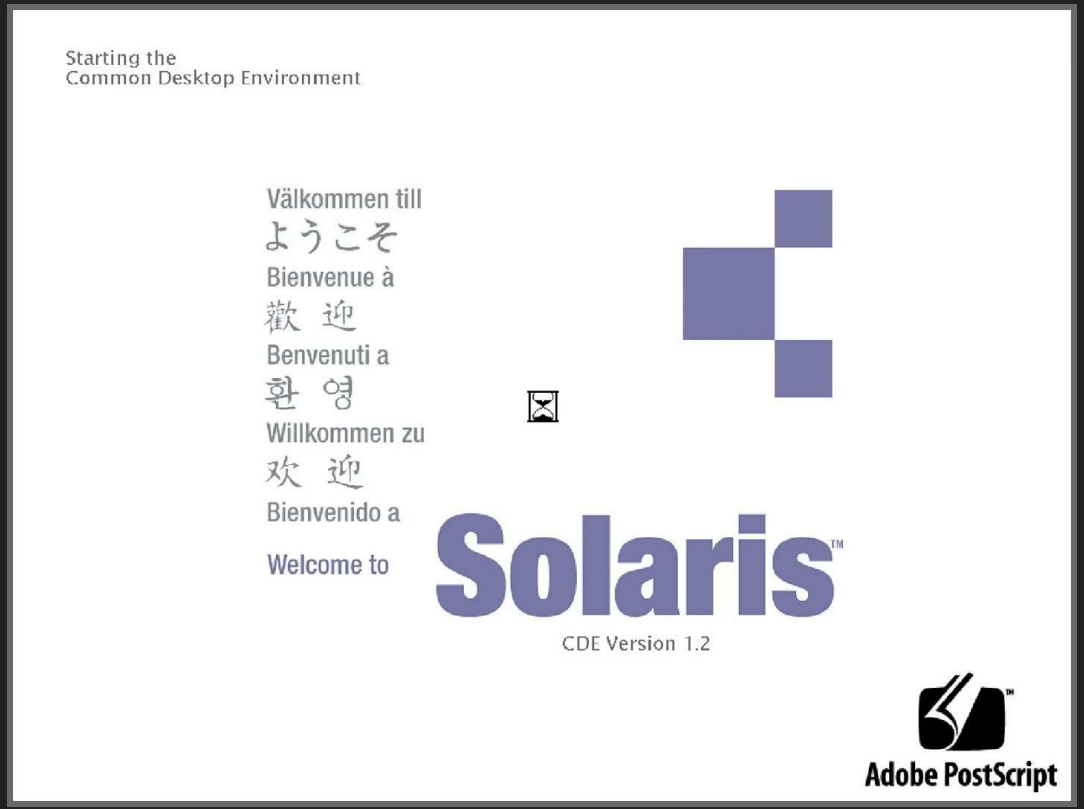
Netscape 5.0, RHEL 5.2 i386



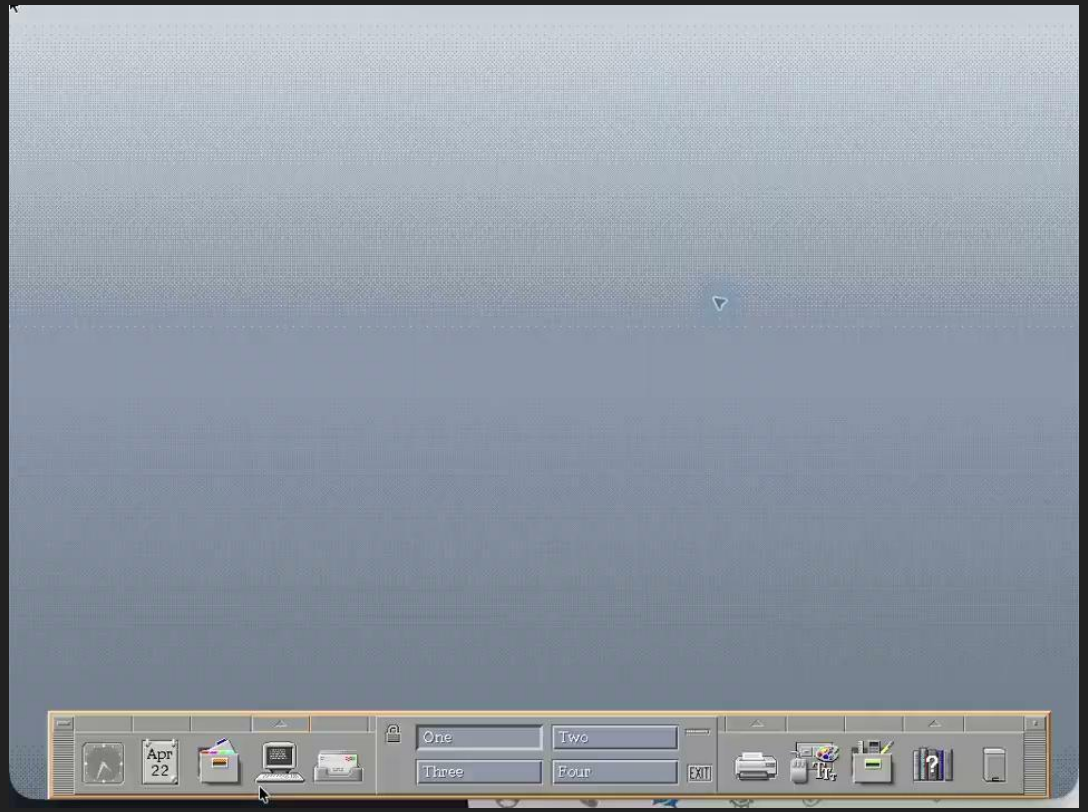
Dino A. Dai Zovi @dinodaizovi · Apr 12

Being able to just pop out exploits for EOL and specialized software will definitely have its operational uses...

IE 5, Solaris 2.6 SPARC



Compaq Secure Web Browser, OpenVMS 8.3 Alpha



Compaq Secure Web Browser, OpenVMS 8.3 Alpha

CVE-2017-5443: Out-of-bounds write during BinHex decoding

Reporter Chamal De Silva

Impact high

Description

An out-of-bounds write vulnerability while decoding improperly formed BinHex format archives.

References

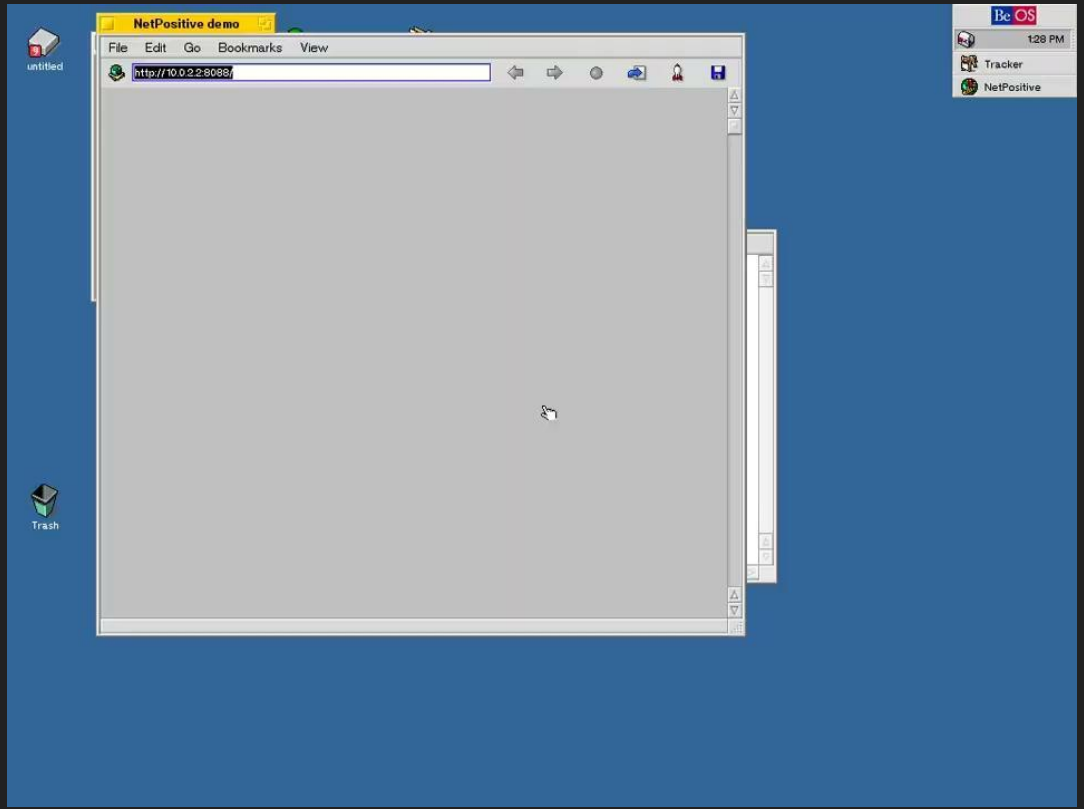
Bug 1342661

Planetweb, Dreamcast SH-4

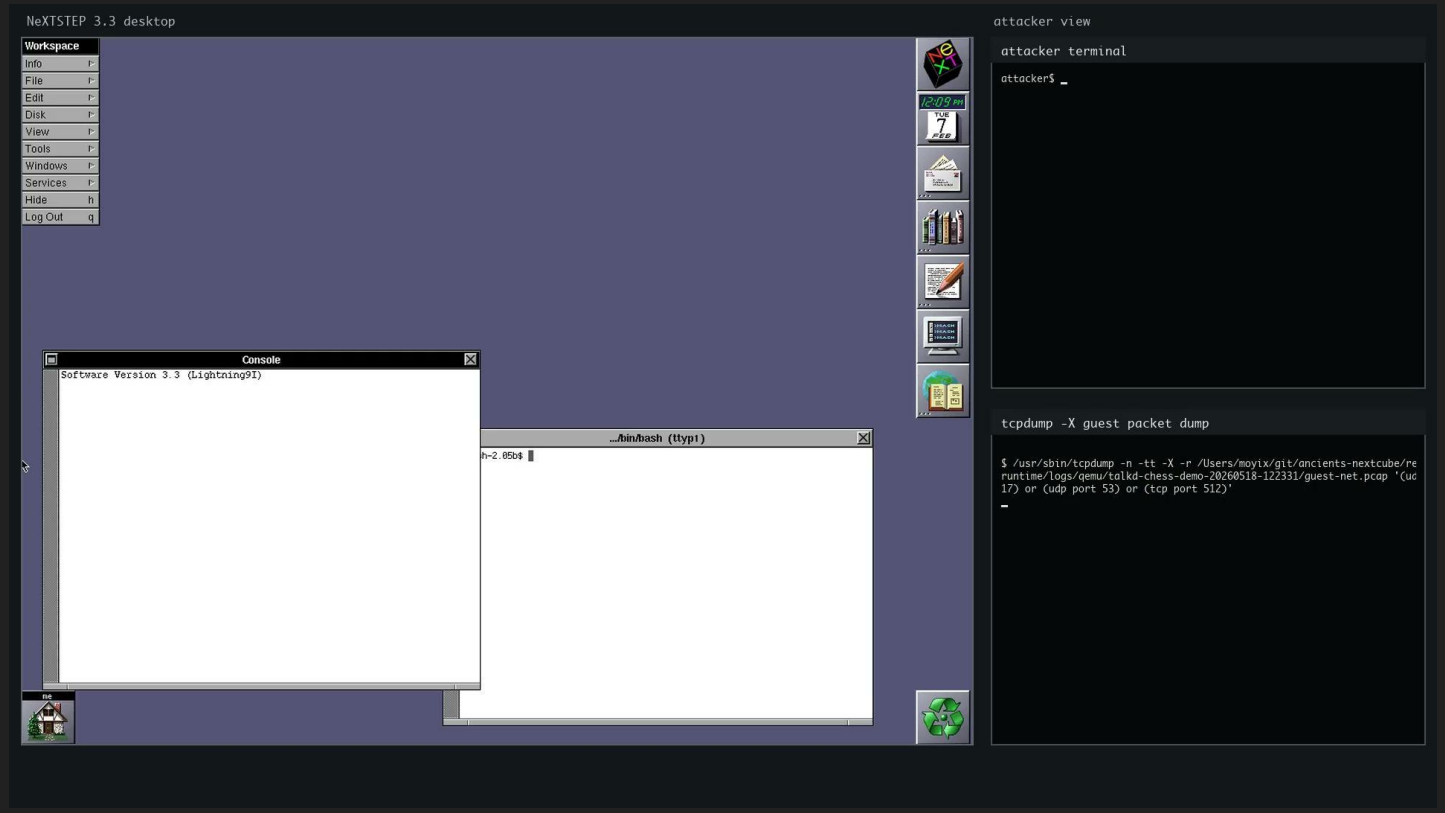
Sean Heelan
@seanhn

❤️Are you still employed? 😂

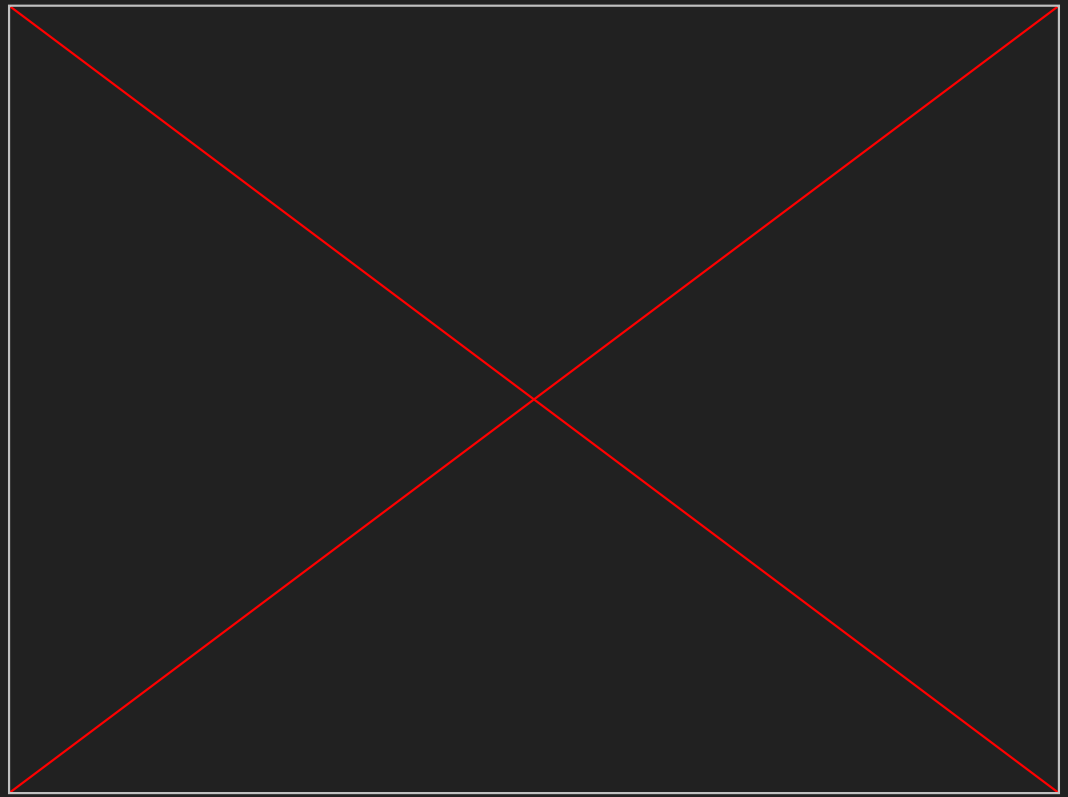
NetPositive 2.2, BeOS 5.0 PPC



talkd, NeXTSTEP 3.3 68k



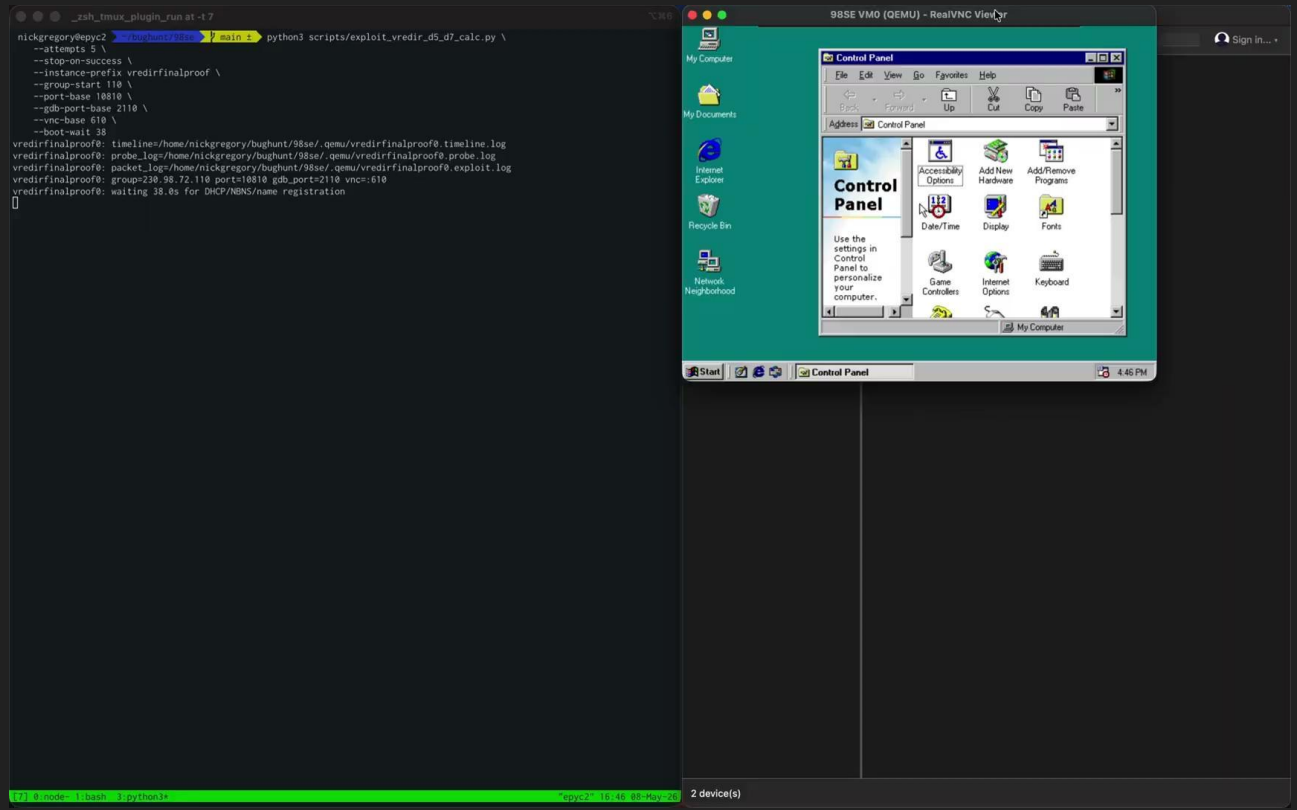
Mac OS 9.2.1, PowerPC



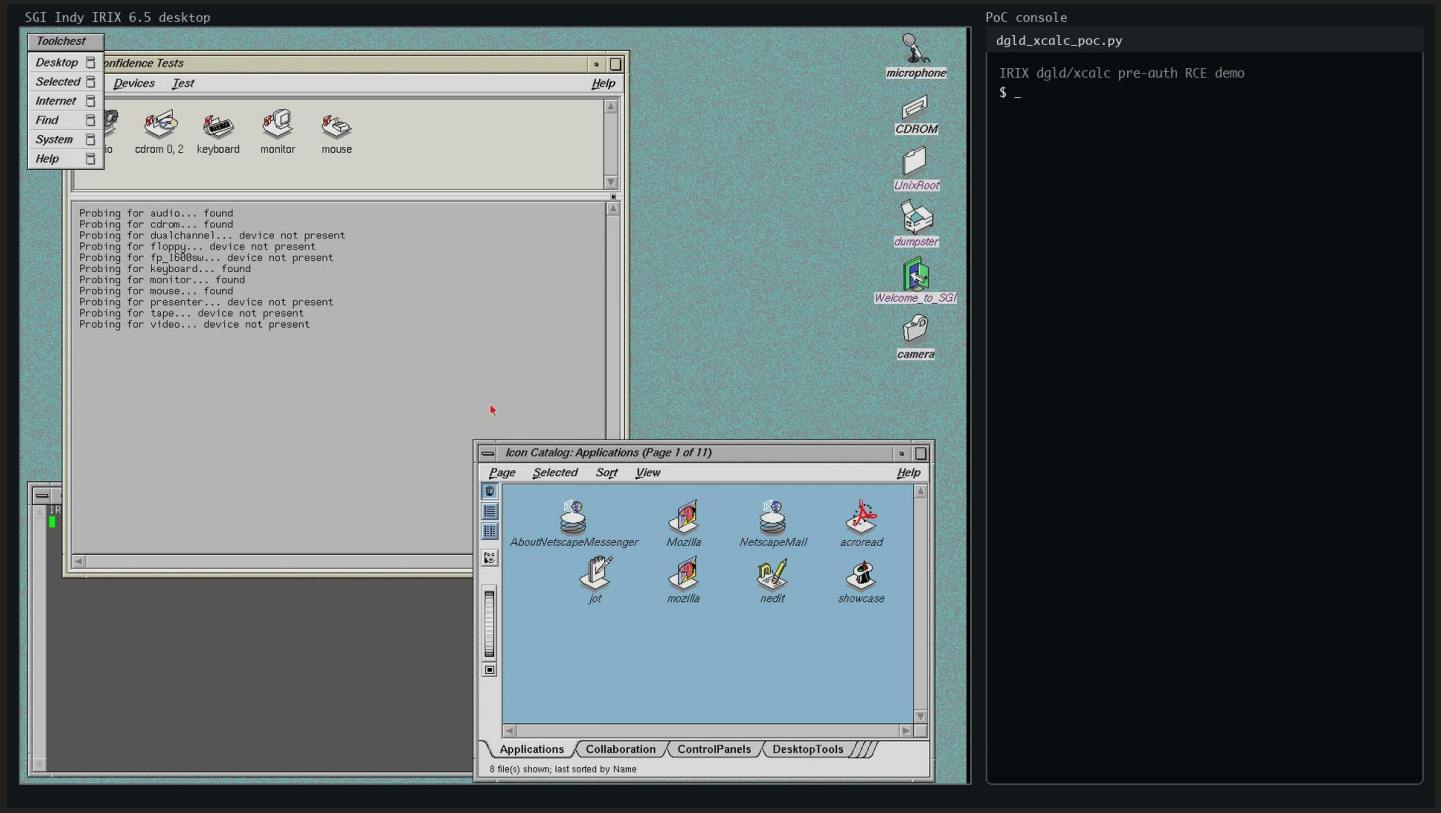
quadruple
@QuadBillionaire

unironically affected.

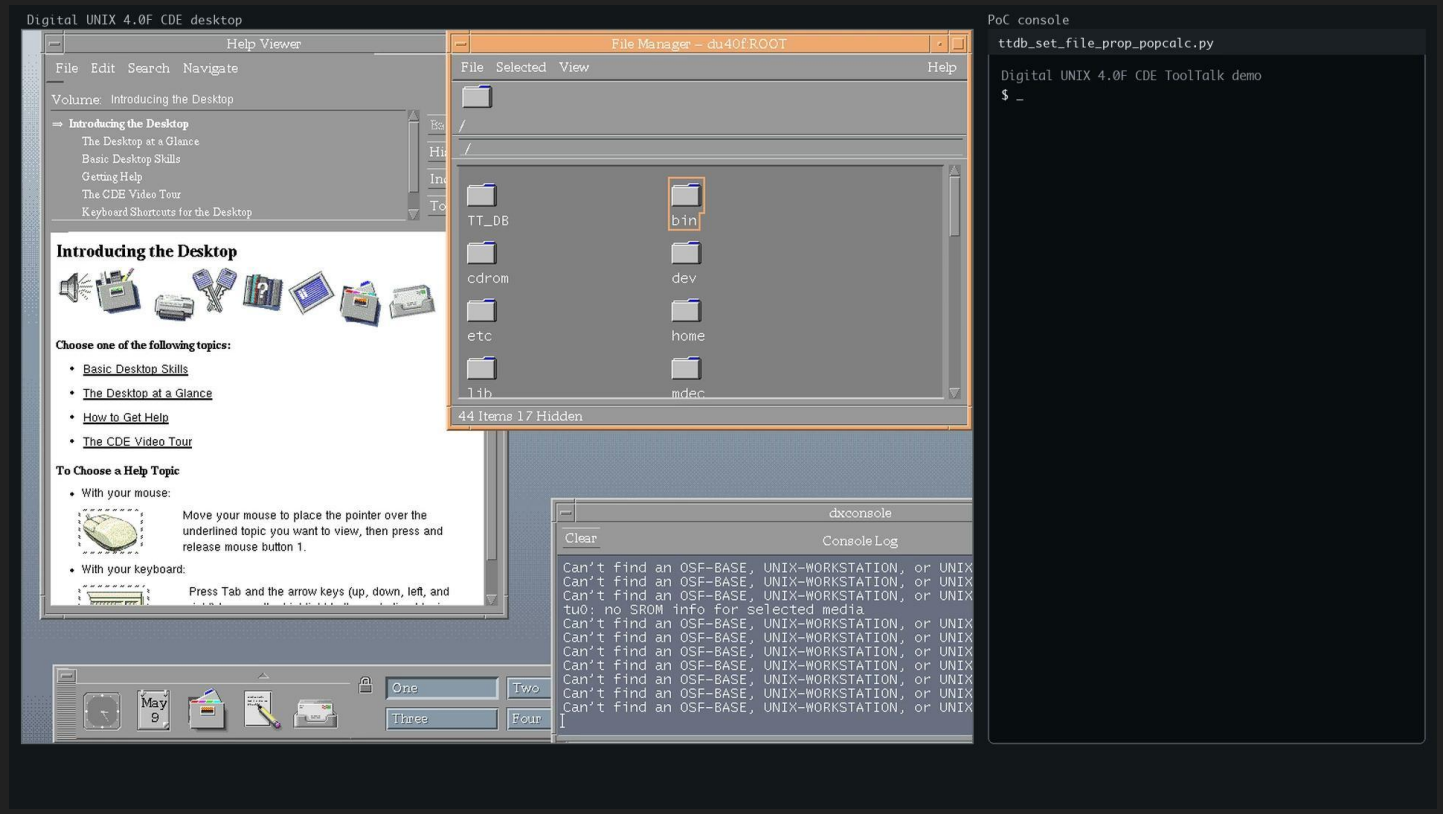
Windows 98 SE, i386



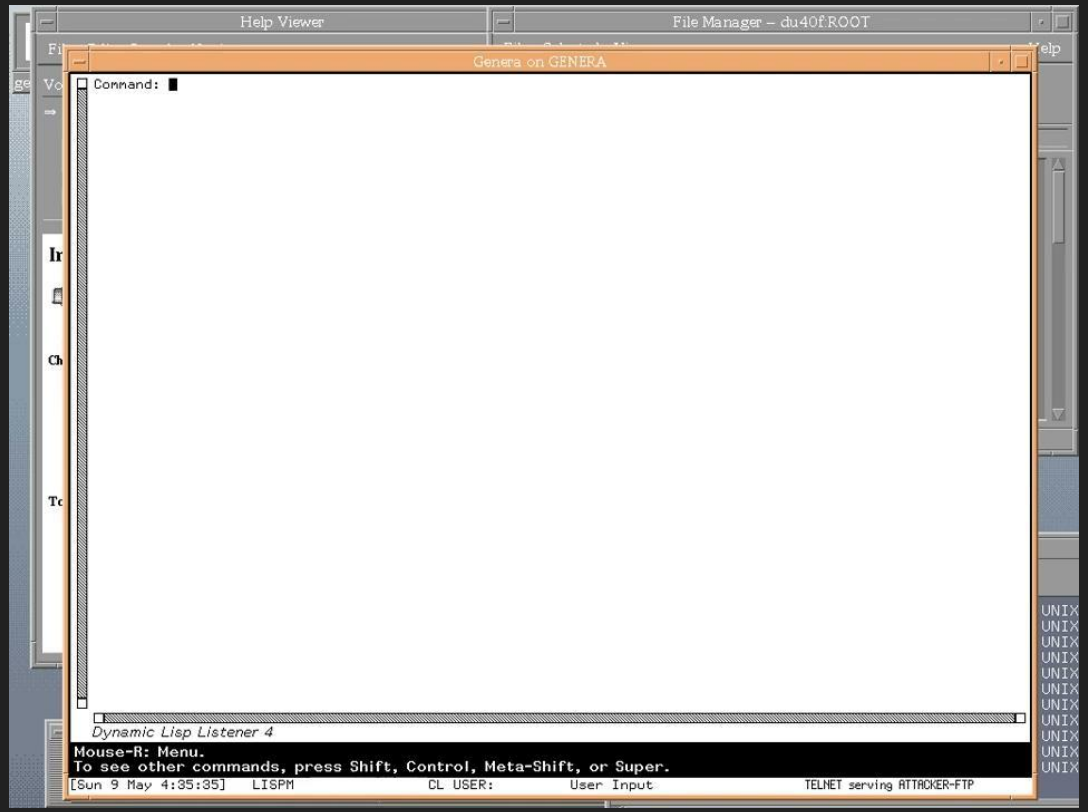
IRIX 6.5, MIPS


SGI Indy IRIX 6.5 desktop
Toolchest
Desktop
Selected
Internet
Find
System
Help
Devices
Test
Help
cdrom 0, 2
keyboard
monitor
mouse
Probing for audio... found
Probing for cdrom... found
Probing for dualchannel... device not present
Probing for floppy... device not present
Probing for fp_1600sw... device not present
Probing for keyboard... found
Probing for monitor... found
Probing for mouse... found
Probing for presenter... device not present
Probing for tape... device not present
Probing for video... device not present
microphone
CDROM
UnixRoot
dumpster
Welcome_to_SGI
camera
Icon Catalog: Applications (Page 1 of 11)
Page
Selected
Sort
View
Help
AboutNetscapeMessenger
Mozilla
NetscapeMail
acroread
jot
mozilla
nedit
showcase
Applications
Collaboration
ControlPanels
DesktopTools
8 file(s) shown; last sorted by Name
PoC console
dgld_xcalc_poc.py
IRIX dgld/xcalc pre-auth RCE demo
$ _

Tru64, Alpha


Digital UNIX 4.0F CDE desktop
Help Viewer
File Edit Search Navigate
Volume: Introducing the Desktop
Introducing the Desktop
The Desktop at a Glance
Basic Desktop Skills
Getting Help
The CDE Video Tour
Keyboard Shortcuts for the Desktop
Introducing the Desktop
Choose one of the following topics:
Basic Desktop Skills
The Desktop at a Glance
How to Get Help
The CDE Video Tour
To Choose a Help Topic
With your mouse:
Move your mouse to place the pointer over the underlined topic you want to view, then press and release mouse button 1.
With your keyboard:
Press Tab and the arrow keys (up, down, left, and
File Manager – du40f:ROOT
File Selected View Help
/
/
TT_DB
bin
cdrom
dev
etc
home
lib
mdec
44 Items 17 Hidden
dxconsole
Clear
Console Log
Can't find an OSF-BASE, UNIX-WORKSTATION, or UNIX
Can't find an OSF-BASE, UNIX-WORKSTATION, or UNIX
Can't find an OSF-BASE, UNIX-WORKSTATION, or UNIX
tu0: no SROM info for selected media
Can't find an OSF-BASE, UNIX-WORKSTATION, or UNIX
Can't find an OSF-BASE, UNIX-WORKSTATION, or UNIX
Can't find an OSF-BASE, UNIX-WORKSTATION, or UNIX
Can't find an OSF-BASE, UNIX-WORKSTATION, or UNIX
Can't find an OSF-BASE, UNIX-WORKSTATION, or UNIX
Can't find an OSF-BASE, UNIX-WORKSTATION, or UNIX
Can't find an OSF-BASE, UNIX-WORKSTATION, or UNIX
May 9
One
Two
Three
Four
PoC console
ttdb_set_file_prop_popcalc.py
Digital UNIX 4.0F CDE ToolTalk demo
$ _

FTP client, Symbolics Virtual Lisp Machine on Tru64 Alpha



Are These Production-Grade Exploits?

- LOL no
- LLM-generated exploits are currently very fragile
- Rely on constants, layout assumptions, etc. that frequently change outside of the idealized environment of the emulator
- Case study:
  - We had THREE RCE-class network-reachable bugs in OS 9.2.2
  - We had an additional port of the Netscape 4.7 vuln to OS 9.2.2
  - GPT-5.{5,6} couldn't make them work reliably on real hardware
- That's why the following demo is… not likely to work

Final Words

- Are these targets hard? No.

• The server accepted file creation but closed the session when the first 1 MiB write exceeded its
  still healthy, delete the zero/partial hard-created file through a fresh session, and retry with

• **Ran** PYTHONDONTWRITEBYTECODE=1 python3 -B scripts/afp_dsi_healthcheck.py --host 10.128.0.1 --port
  └ fail timeout: timed out

• **Ran** ping -c 1 -W 1000 10.128.0.1
  └ PING 10.128.0.1 (10.128.0.1): 56 data bytes

    --- 10.128.0.1 ping statistics ---
    1 packets transmitted, 0 packets received, 100.0% packet loss

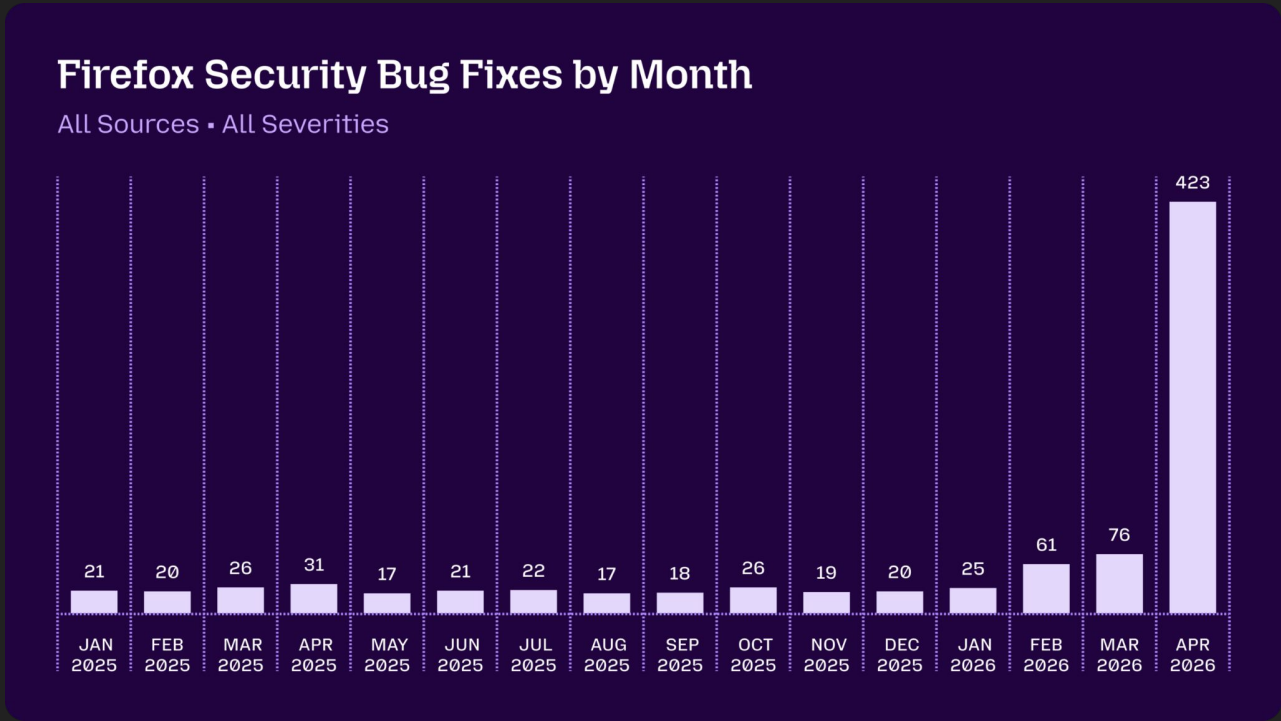
---

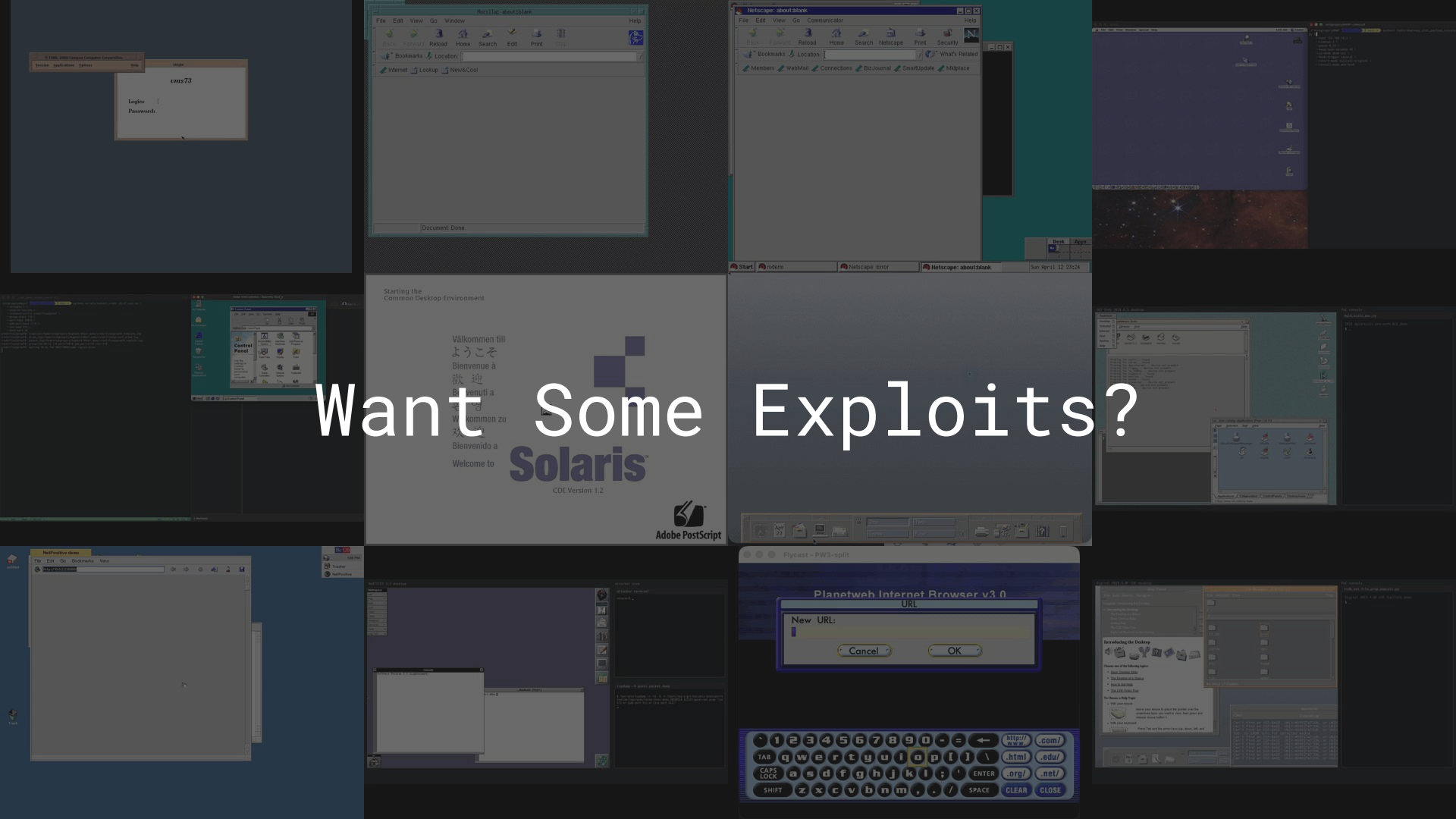
• The 1 MiB AFP write exceeded ShareWay's receive buffer and wedged the iBook's network stack; AFP

  After it returns, I'll delete the partial file and retry using 4 KiB writes within the 0x1210 rec

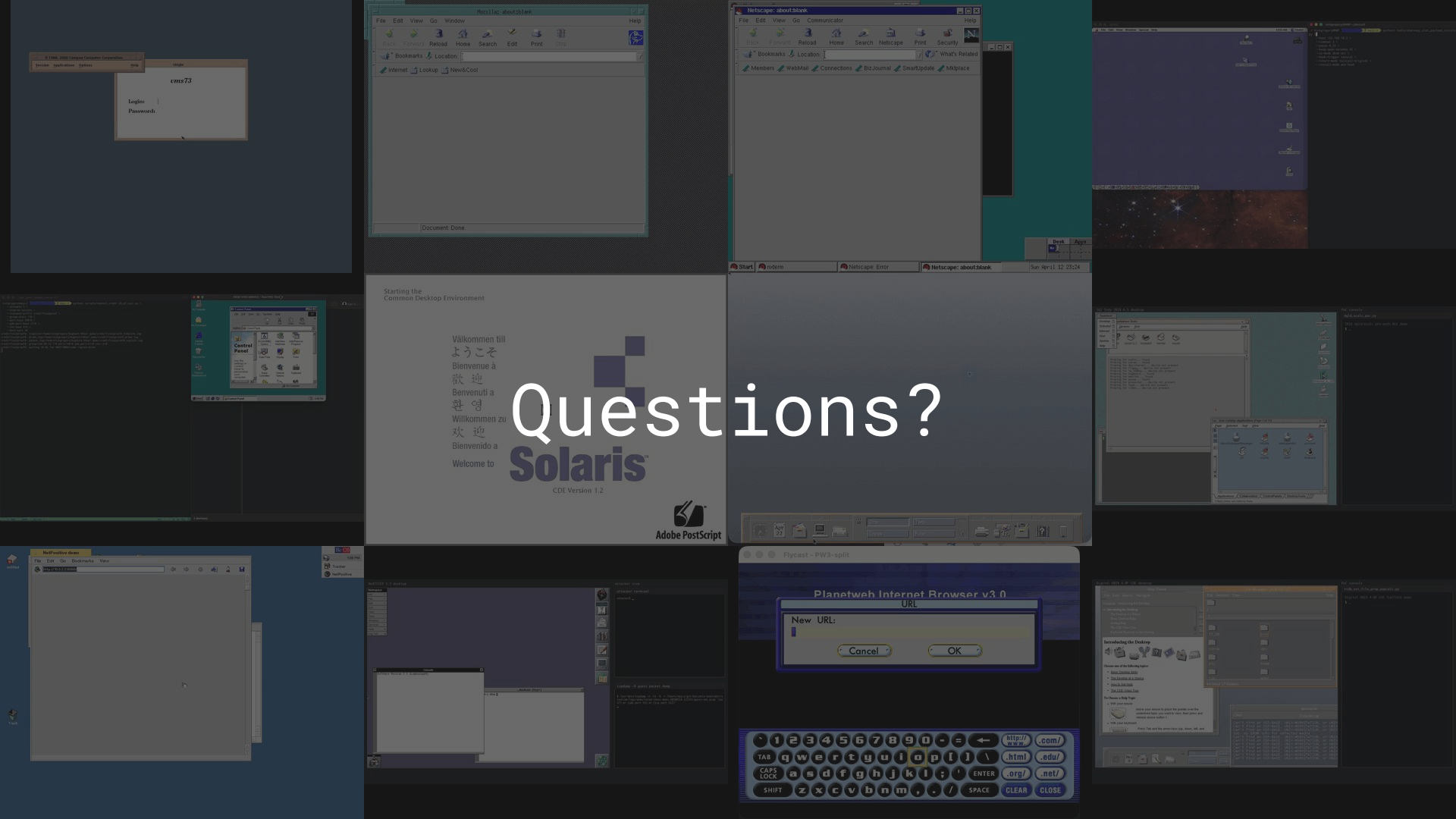
Final Words

- Are these targets hard? No.
- But:




Want Some Exploits?
vms73
Login:
Password:
Starting the
Common Desktop Environment
Välkommen till
ようこそ
Bienvenue à
歡迎
Willkommen zu
Bienvenido a
Welcome to
Solaris
CDE Version 1.2
Adobe PostScript
Planetweb Internet Browser v3.0
URL
New URL:
Cancel
OK

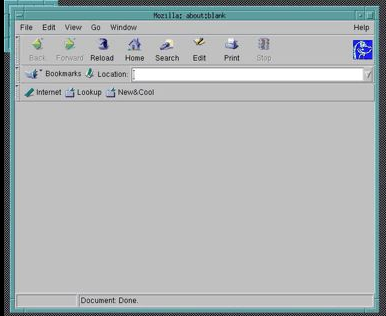

Free Odays


Questions?

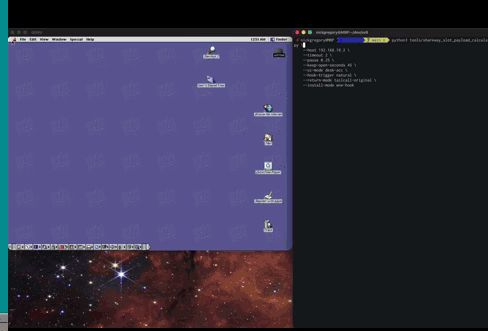
Quick Links

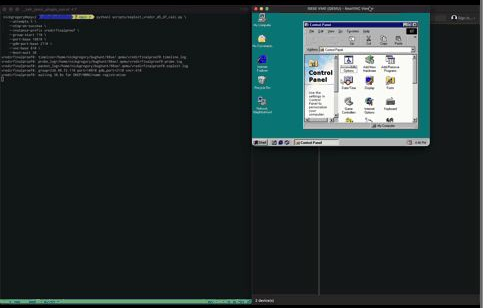
Recap https://x.com/moyix/status/2049549923457138954

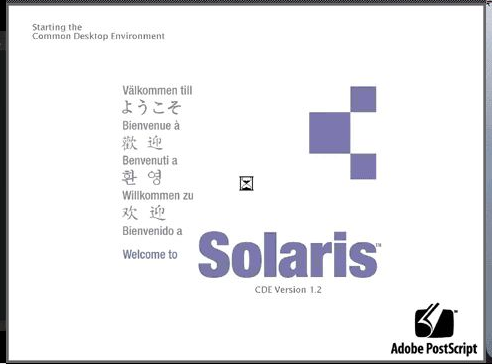

vms73
Login:
Password:

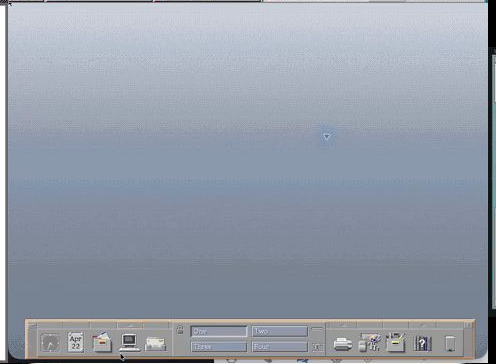

Mozilla: about:blank
File Edit View Go Window Help
Back Forward Reload Home Search Edit Print Stop
Bookmarks Location:
Internet Lookup New&Cool
Document: Done.

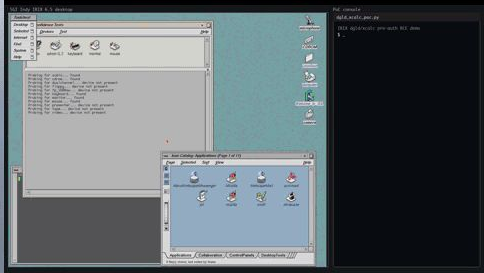

Netscape: about:blank
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security
Bookmarks Location: What's Related
Members WebMail Connections BizJournal SmartUpdate Mktplace
Start rxterm Netscape: Error Netscape: about:blank
Sun April 12 23:24

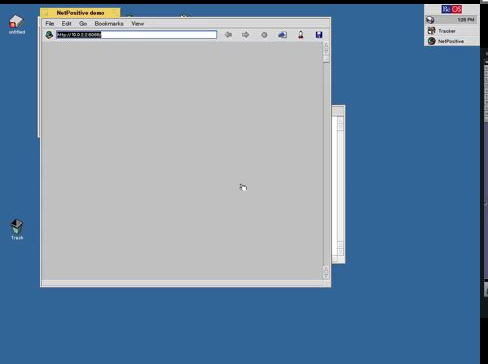


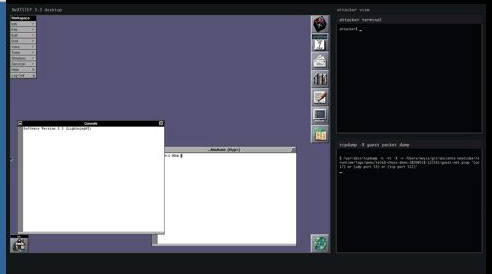



Starting the
Common Desktop Environment
Välkommen till
ようこそ
Bienvenue à
歡 迎
Benvenuti a
환 영
Willkommen zu
欢 迎
Bienvenido a
Welcome to
Solaris
CDE Version 1.2
Adobe PostScript






NetPositive demo
File Edit Go Bookmarks View




Flycast - PW3-split
Planetweb Internet Browser v3.0
URL
New URL:
Cancel
OK