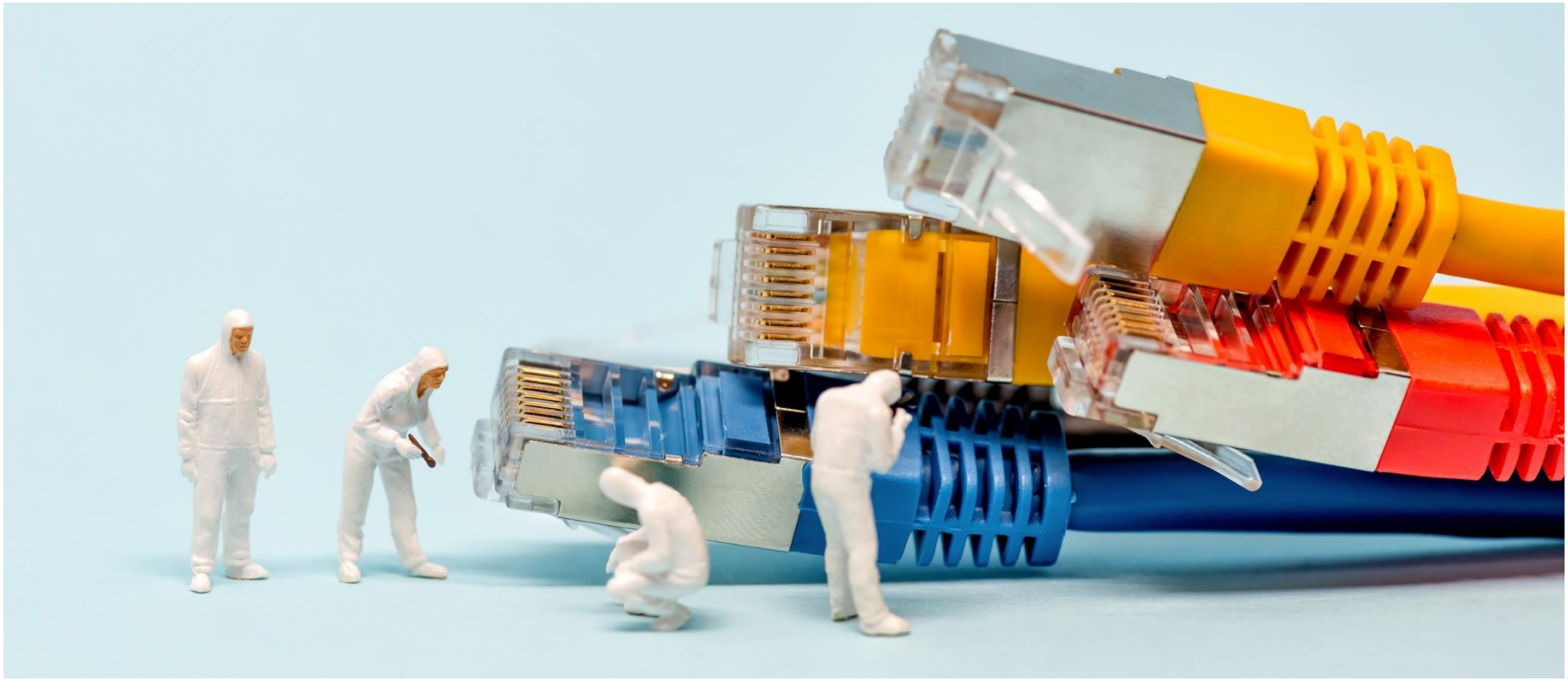
Computer Network Security

COMP 178 | Spring 2025 | University of the Pacific | Jeff Shafer



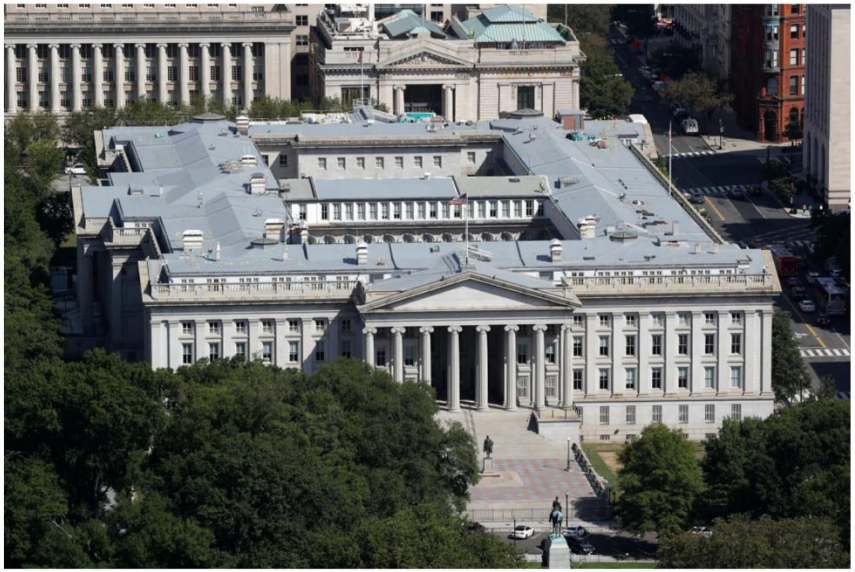

WE HOPE YOU HAD A NICE WINTER BREAK
WELCOME BACK. EVERYTHING IS FINE.
imgflip.com

“Worst” Security Disasters

Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect

In one of the most sophisticated and perhaps largest hacks in more than five years, email systems were breached at the Treasury and Commerce Departments. Other breaches are under investigation.

482



The Treasury Department was one of the agencies targeted by the hackers. Patrick Semansky/Associated Press

By David E. Sanger

Published Dec. 13, 2020 Updated Jan. 2, 2021

As Understanding of Russian Hacking Grows, So Does Alarm

Those behind the widespread intrusion into government and corporate networks exploited seams in U.S. defenses and gave away nothing to American monitoring of their systems.

1135

Legal prohibitions on the National Security Agency bar it from surveilling networks inside the United States. T.J. Kirkpatrick for The New York Times

By David E. Sanger, Nicole Perlroth and Julian E. Barnes

Jan. 2, 2021

SolarWinds

SolarWinds

Company

- **Software vendor** of products for system monitoring and management (systems, databases, networks, etc…)

https://www.solarwinds.com/

SolarWinds Orion

- Management Platform
  - Network configuration manager
  - Network performance monitor
  - Traffic analyzer
  - Server & application monitor
- Used by 33,000+ organizations
  - 425 of Fortune 500
  - US Military, State Dept, White House, etc…

FireEye

- **Cybersecurity company**
- Consulting services include
  - Vulnerability testing
  - Incident response
- Well known for investigations into major hacking groups (private and nation-state)

https://www.fireeye.com/

Approximate Timeline of Events

- **March 2020**
  - Legitimate updates for SolarWinds Orion project were replaced by copies that included malware
  - *Signed with legitimate certificate*
- **Supply Chain Attack**
  - Customers downloaded what was supposed to be legitimate code and received malware as a “bonus”
    - Updates could be automatic, or manually installed by administrators (after testing, verification, …)
  - These infected downloads were present for MONTHS!

- This malware has been given the name **SUNBURST**

SolarWinds: Attack Chain

Symantec. A Division of Broadcom

Example of attack chain on one computer infected by attackers. Note that while there may be some commonalities in post-compromise activity, each victim is likely to see different patterns in activity.

Trojanized SolarWinds Orion Update

Sunburst Backdoo

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds

Sunburst Backdoor

- Waits 12-14 days before execution
- Checks if it is running on a domain it wants to skip (e.g. domains with the name 'test', swdev.local, etc.)
- Returns without doing anything more if sees certain security tools/software
- Attempts to disable security software
- Checks if it can resolve api.solarwinds.com properly
- Collects system information to generate a DGA domain
- DNS resolves that DGA
- Depending on the value of the IP field (A NAME), the threat will:
  - start the
  - or updat

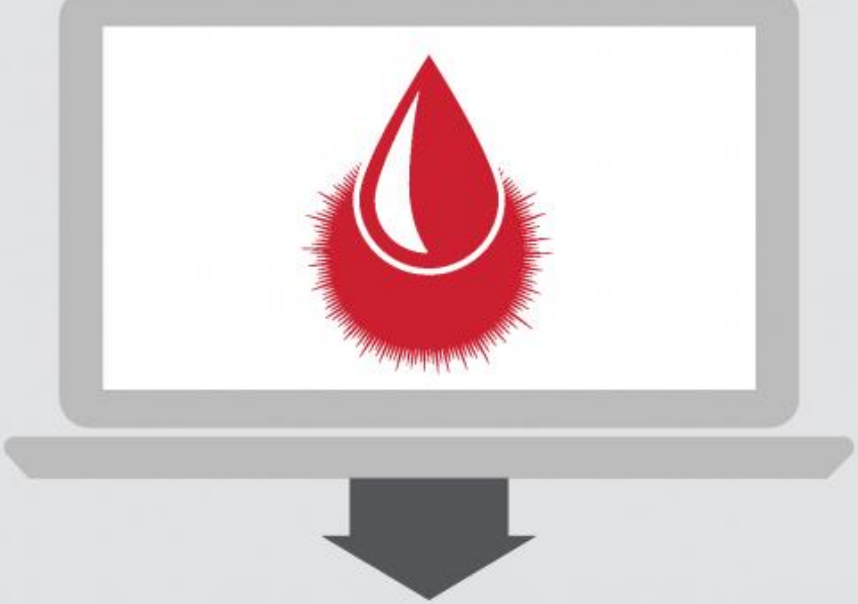
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds

- Waits 12-14 days before execution
- Checks if it is running on a domain it wants to skip (e.g. domains with the name 'test', swdev.local, etc.)
- Returns without doing anything more if sees certain security tools/software
- Attempts to disable security software
- Checks if it can resolve api.solarwinds.com properly
- Collects system information to generate a DGA domain
- DNS resolves that DGA
- Depending on the value of the IP field (A NAME), the threat will:
  - start the HTTPS backdoor
  - or update process listing
- The domain for the HTTPS backdoor will be in the CNAME record
- Contacts command and control server (C&C) (HTTPS)
- Opens backdoor
- Delivers secondary payload

Teardrop

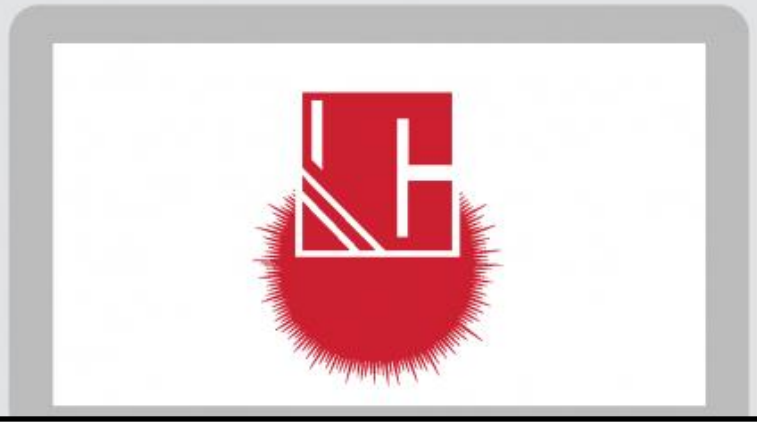
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds

Teardrop Backdoor



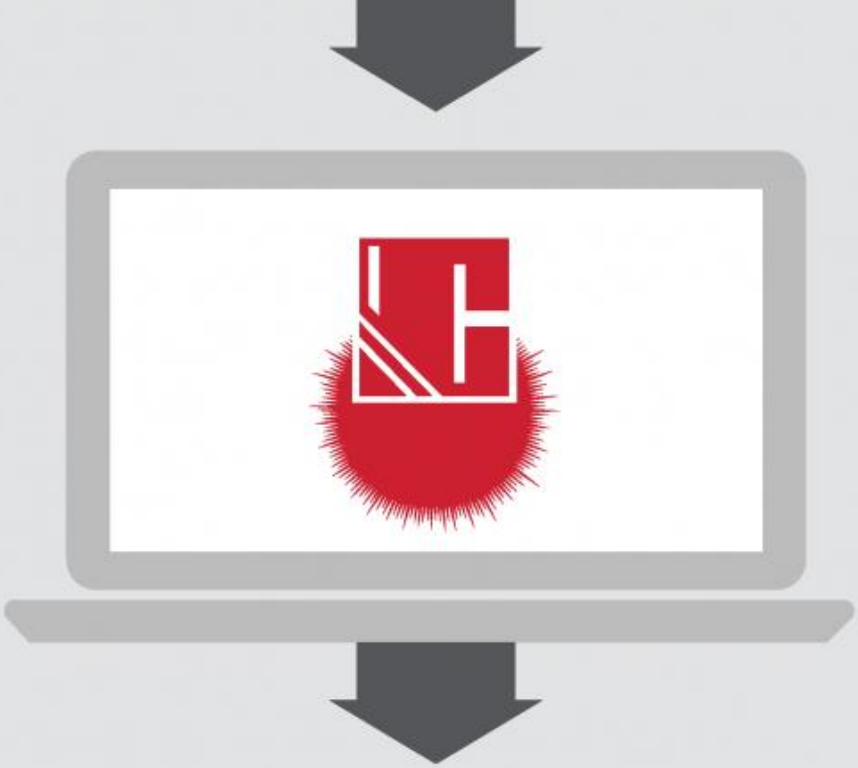
- Extract and installs embedded copy of Cobalt Strike Beacon

Cobalt Strike



https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds

Cobalt Strike



- Contacts C&C server
- Launches WMI to load malicious DLL
- Attempts to steal credentials
- Queries active directory
- Attempts to elevate privileges
- Likely lateral movement, SAML token minting, or email theft

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds

Supply Chain Attack

- ~18,000(?) organizations installed the infected update
  - Malware would wait 10-14 days before contacting C&C server – more than long enough to fool an organization testing new software in a monitored sandbox first
  - SolarWinds SEC filing [12/17/2020 report] says malware was "only" available "in updates to the Orion Platform products delivered between March and June 2020"
    - https://investors.solarwinds.com/financials/sec-filings/default.aspx
- ~250(?) government and private organizations got a secondary payload from the C&C server
  - High priority targets for attacker? (Were others not worth attacking, or was threat actor resource constrained?)

Approximate Timeline of Events

- **December 8th 2020** – FireEye
  - **We were hacked!**
    - Our own highly proprietary "Red Team" (*hacking*) tools were taken
    - Responsibly disclosed - Signatures provided on GitHub to detect and neuter stolen toolset
- https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

Threat Research

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

FIREEYE EVASION SUPPLY CHAIN

Executive Summary

- We have discovered a global intrusion campaign. We are tracking the actors behind this campaign as UNC2452.
- FireEye discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute malware we call SUNBURST.
- The attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, but these efforts also offer some opportunities for detection.
- The campaign is widespread, affecting public and private organizations around the world.
- FireEye is releasing signatures to detect this threat actor and supply chain attack in the wild. These are found on our public GitHub page. FireEye products and services can help customers detect and block this attack.

Approximate Timeline of Events

- **Dec 13th, 2020** – FireEye
  - **The attackers gained access via SolarWinds!**
  - **The threat is global!**
  - **Public and private organizations are at risk!**
  - Specifically named SolarWinds Orion as the threat vector, labeled the malware SUNBURST, and provided detection signatures
  - https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Emergency Directive 21-01

December 13, 2020

Mitigate SolarWinds Orion Code Compromise

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Emergency Directive 21-01, "*Mitigate SolarWinds Orion Code Compromise*".

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat." 44 U.S.C. § 3553(h)(1)–(2)

Section 2205(3) of the Homeland Security Act of 2002, as amended, delegates this authority to the Director of the Cybersecurity and Infrastructure Security Agency. 6 U.S.C. § 655(3).

Federal agencies are required to comply with these directives. 44 U.S.C. § 3554 (a)(1)(B)(v)


2020

- And legions of IT workers had a terrible holiday, because where do you even start when you suspect attackers have been in your network for *months?*

"Worst" Security Disasters

Log4j / Log4Shell

- CVE-2021-44228 *(Common Vuln & Exposures)*
- CVSS *(Common Vuln Scoring System)* severity rating of 10/10 🔥🧨💀
- Public disclosure: December 9th, 2021
- Log4j – Open-source Java **logging library** from Apache

Log4j

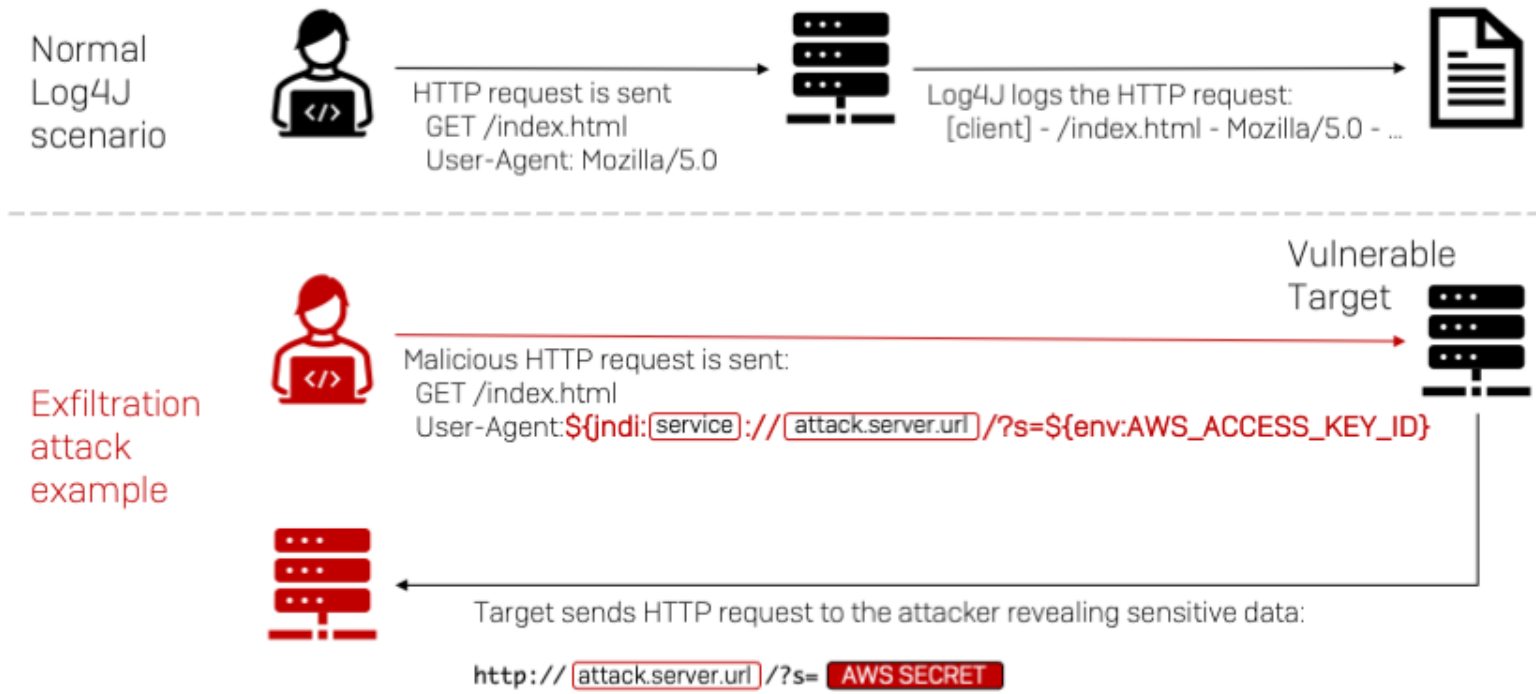
- Log4j – Open-source Java **logging library** from Apache
- Very popular / commonly used in Java software
  - Consumer apps: Minecraft, Steam
  - Enterprise apps: *Practically everywhere!*
    - *Akamai, Amazon, Apache, Apereo, Apple, Atlassian, Broadcom, Cisco, Cloudera, ConnectWise, Debian, Docker, Fortinet, Google, IBM, Intel, Juniper Networks, Microsoft, Okta, Oracle, Red Hat, SolarWinds, SonicWall, Splunk, Ubuntu, VMware, Zscaler, Zoho*

Log4j Vulnerability

- "It's not a bug, it's a **feature**"
- Log4j can do more than just *blindly save some strings to a text file*
  - It can **interpreter those strings** (to substitute in variables like Java version, environment variables, thread name, etc…)
  - It can also **make network requests to remote JNDI servers** based on content inside the log message, **retrieve remote classfiles** (i.e. code), and **execute it**


SECURITY BY
OBSCURITY
Spongebob Squarepants vector trace by
memegenerator.net

Log4j Vulnerability – Exfiltration

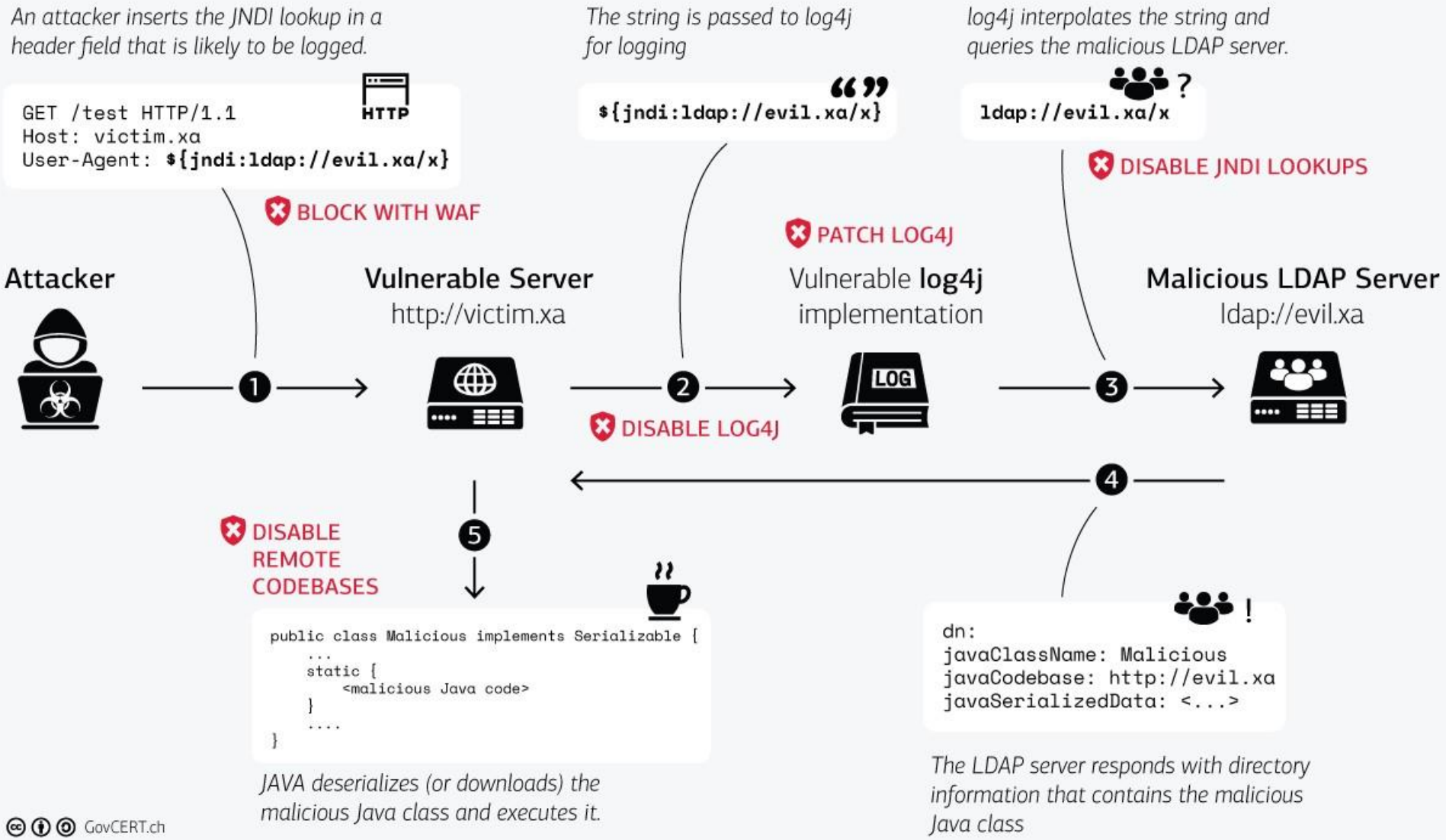


SOPHOSlabs

https://news.sophos.com/en-us/2021/12/12/log4shell-hell-anatomy-of-an-exploit-outbreak/

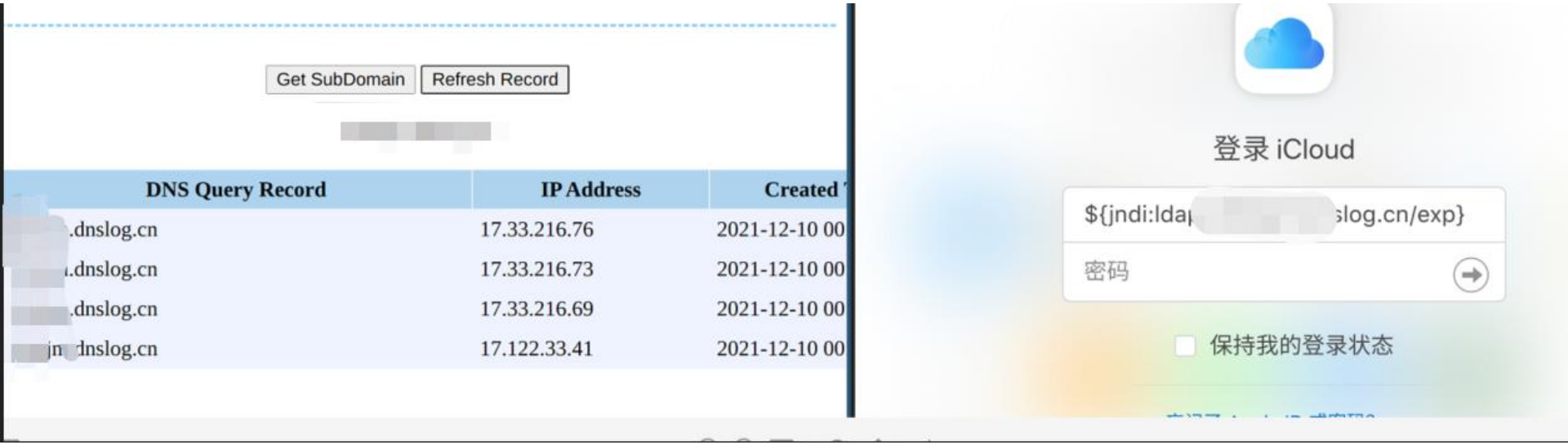
The log4j JNDI Attack

and how to prevent it



https://www.govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/

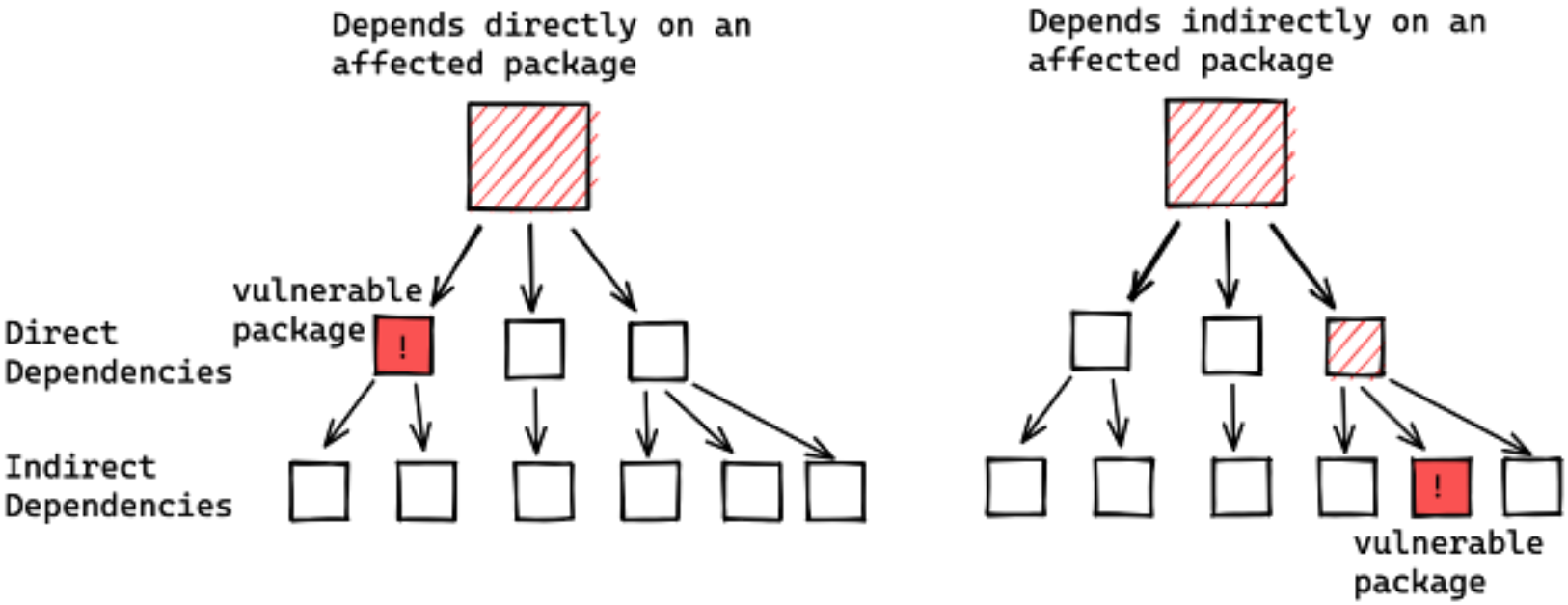
Log4j Vulnerability in Action



- Attacker enters malicious string as “username”
  - Username is logged via vulnerable Log4j
  - Formatting string -> lookup jndi -> deserialize class -> pwned
- Evidence in DNS record that Apple servers did a DNS lookup for attacker-controlled domain

Log4j Remediation

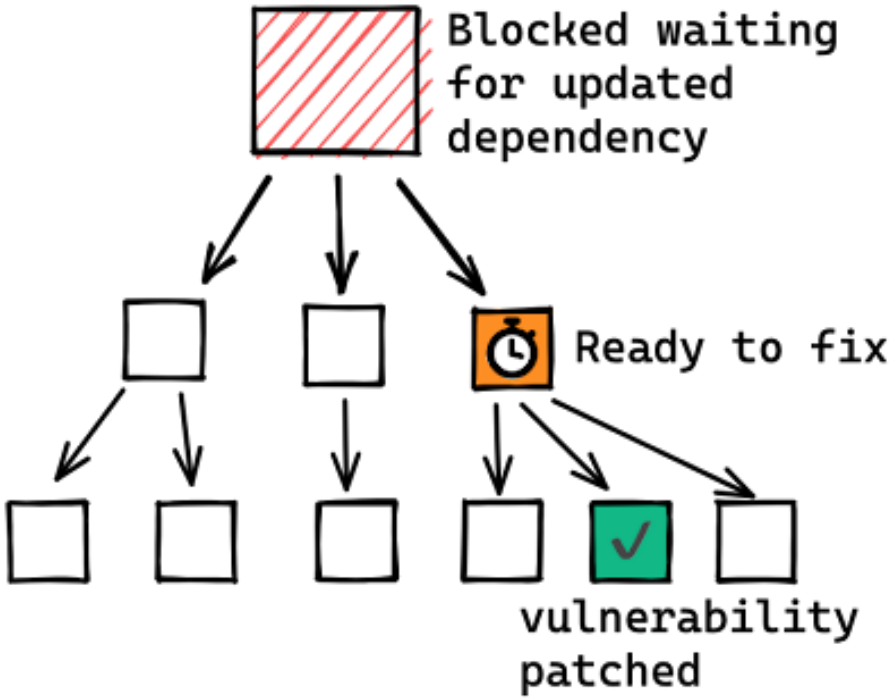
- *Just update your software, right?*



https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html

Log4j Remediation

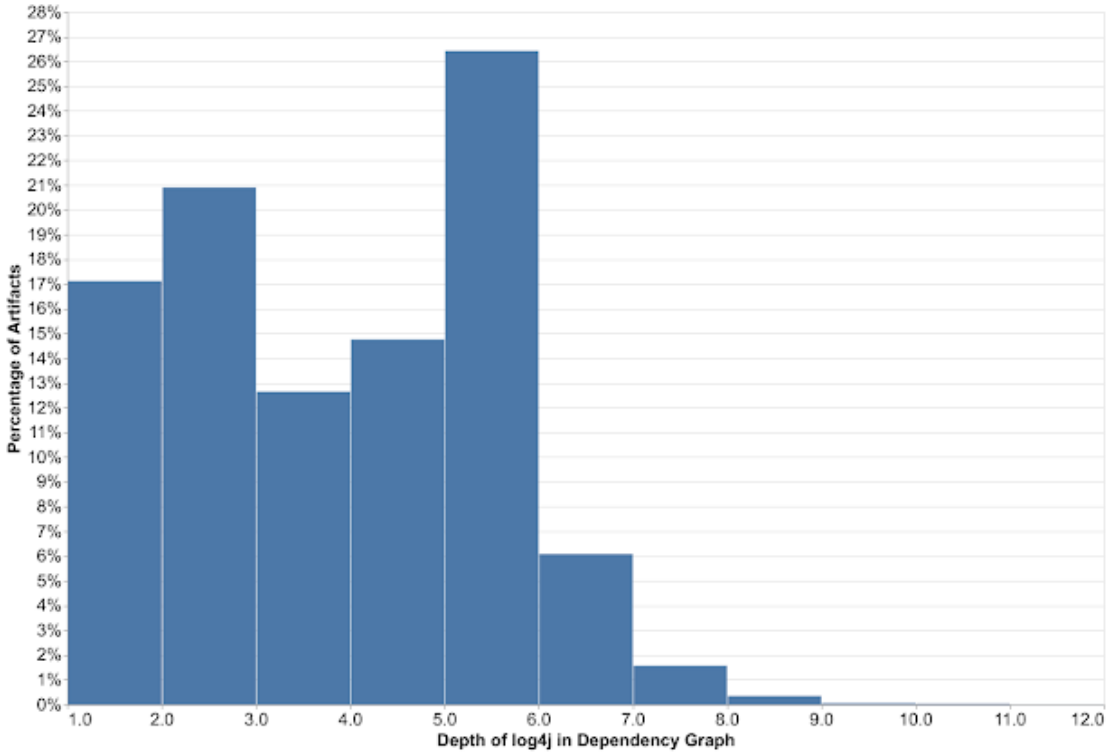
- *Just update your software, right?*



https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html

Log4j Remediation

- *Just update your software, right?*



For greater than 80% of the packages, the vulnerability is more than one level deep, with a majority affected five levels down (and some as many as nine levels down). These packages will require fixes throughout all parts of the tree, starting from the deepest dependencies first.

https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html


2020
2021

Why Study Cybersecurity?

Motivating Question for Class

- **What do you, as a security professional, need to know to detect, prevent, and analyze computer attacks?**
- Emphasis on *network* related attacks, given course title

Course Overview

Class Survey

- **Have you taken ECPE 170?**
  (Computer Systems & Networking)
- **Have you taken COMP 175?**
  (System Administration & Security)
- **Have you taken COMP 177?**
  (Computer Networking)

Websites

Main website

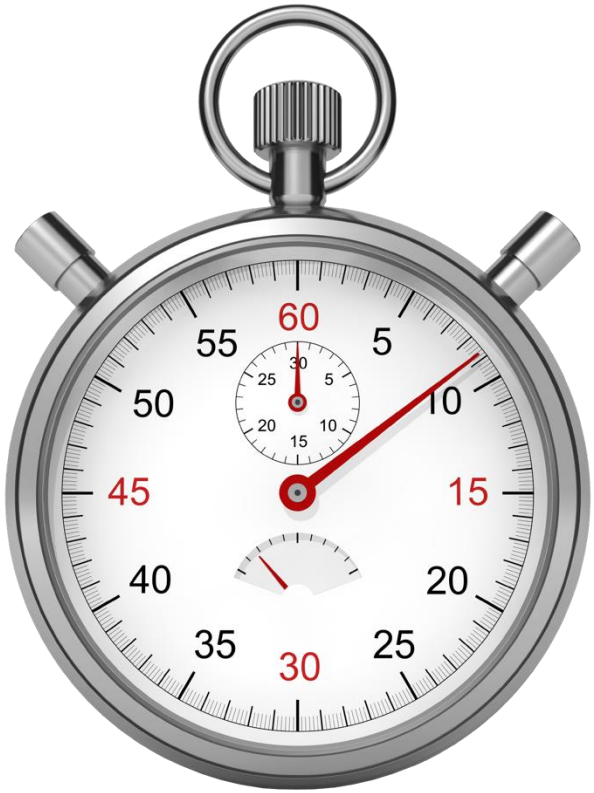
- https://cyberlab.pacific.edu/

Canvas CMS (gradebook, labs, …)

- http://canvas.pacific.edu

Course Topics

- Only 15 weeks in a semester
- 29 classes, including today
  - **The clock is ticking now!**
- What to cover?



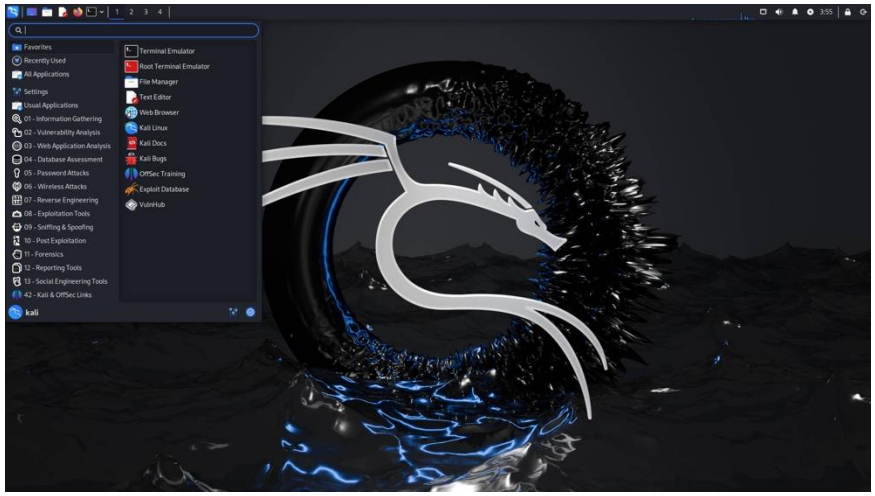
Lecture Topics

- **Penetration Testing**
  - Reconnaissance
  - Scanning
  - Vulnerability Scanning
  - Exploitation
- **Cryptography**
- Honeypots
- Social Engineering
- Physical Security
- **Other topics you would like to learn about?**

Lab Topics

- **Penetration Testing**
  - Reconnaissance
  - Scanning
  - Vulnerability Scanning
  - Exploitation
- **Network Security Devices**
  - Firewalls
  - Intrusion Detection Systems
- **Cryptography**
- Social Engineering

Lab Tools – Kali Linux



- Debian-based Linux distribution
- Several hundred tools pre-installed
  - Penetration Testing
  - Forensics
  - Reverse engineering
  - https://www.kali.org/tools/

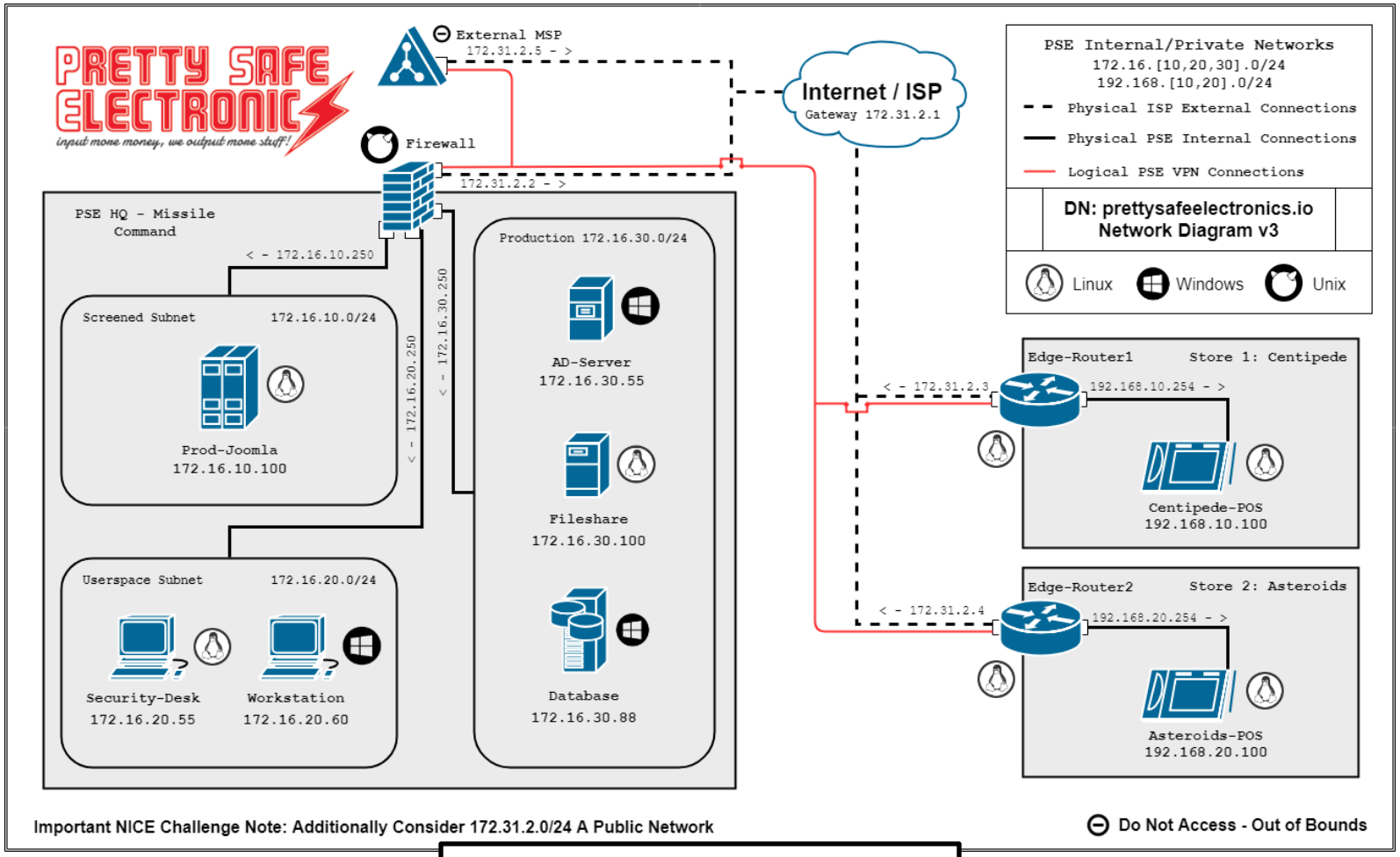
https://www.kali.org/

Lab Tools – XP Cyber

- **Real-world cybersecurity challenges**
  - Narrative scenarios
  - Full business environments (servers, services, workstations, networks)
- No installation required (web portal)

https://www.xpcyber.com/

Lab Tools – XP Cyber

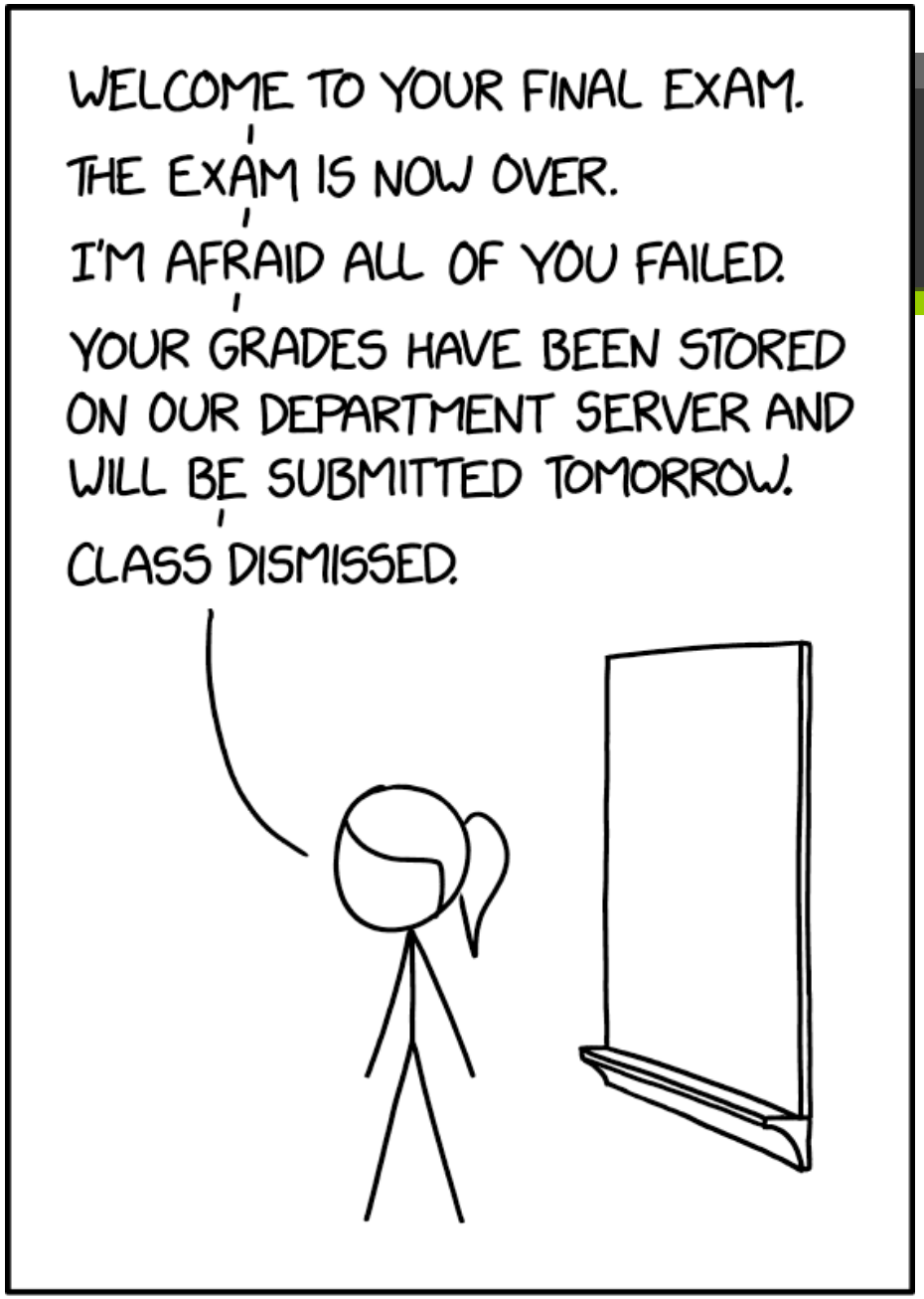


https://www.xpcyber.com/

Course Components

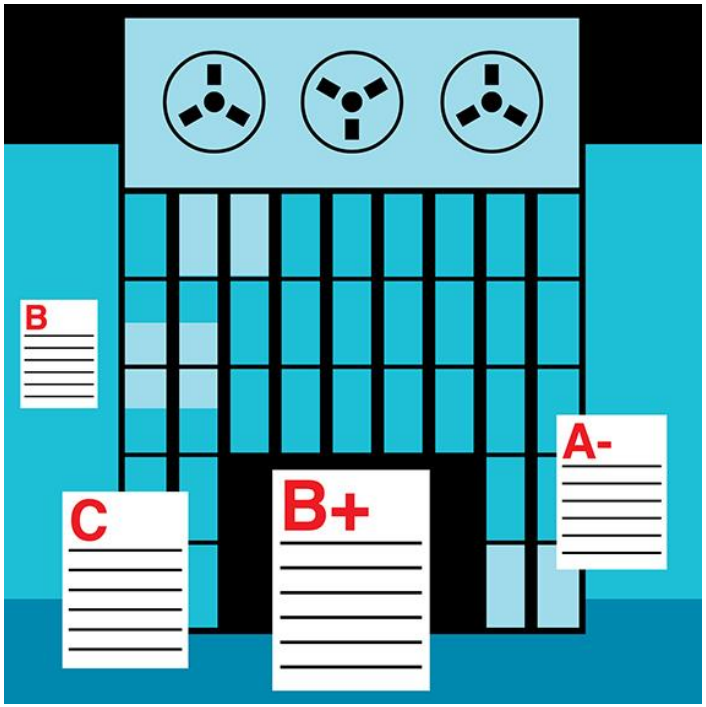
- **70%** - **Labs**
  - Begin in-class, finish at home
  - Hands-on experience using real tools and systems
- **20%** - **Projects**
  - Open-ended assignments
- **10%** - **Presentations**

Final Exam



https://xkcd.com/2385/

Lab Auto-Grader



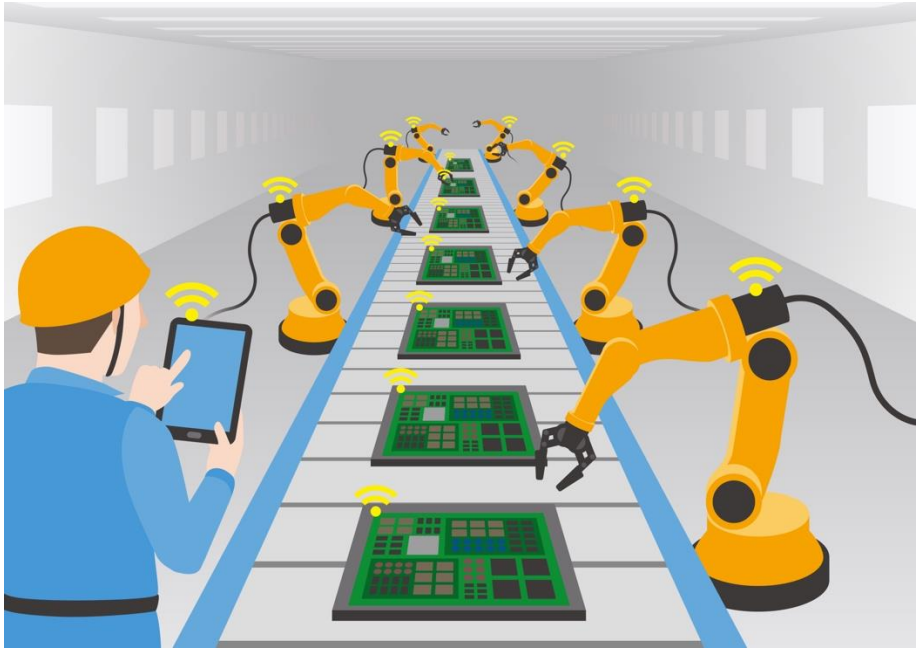
- Canvas will immediately auto-grade the fill-in-the-blank lab questions upon submission
- Problems with this…
  1. Computer is very picky
  2. The correct answer may have changed between 2024 and 2025
- **Don't Worry! A human will review all answers that are marked "wrong"**

Course Support

- **TA**
  - Vivek Kumar Maheshwari
- **Instructor Canvas messages or email**
  - **See syllabus**
- **Instructor Office Hours**
  - **See syllabus**

Next Class

- Recap of computer networking
- Lab 1: Kali and Metasploitable2 Setup



Questions?

- Questions?
- Concerns?