About the Course Project

Estimated duration: 2 minutes

Welcome to the final project for the course, Penetration Testing, Threat Hunting, and Cryptography. In this project, you will apply the knowledge and skills learned in this course to a real-world-inspired scenario.

The tasks in this hands-on project correspond to the activities performed by a pen tester or ethical hacker as part of their critical organizational responsibilities.

Imagine yourself as an ethical hacker hired by SecureBank, a mid-sized financial institution, while you complete this project. You'll perform tasks related to protecting the organization from vulnerabilities and enhancing its security posture.

This final project, which will take you about 60 minutes to complete, will be completed in two parts:
Part 1: Perform vulnerability analysis and penetration testing (30 minutes)
Part 2: Secure information using symmetric encryption (30 minutes)

Here are the individual tasks you'll perform in each part:

Peer-Graded Final Project: Part 1 - Perform Vulnerability Analysis and Penetration Testing

In this final project, you will demonstrate your ability to protect SecureBank from vulnerabilities and enhance its security posture.

Part 1 will consist of three tasks:

- **Task 1:** Identifying a vulnerability using IBM X-Force Exchange
- **Task 2:** Investigating the chosen vulnerability using Google Dorking
- **Task 3**: Creating a penetration testing plan

You will first provide screenshots that identify a vulnerability using IBM X-Force Exchange and investigate it further using Google Dorking. Next, you will make decisions that influence the outcome of the penetration testing plan. You should plan to complete Part 1 in about 30 minutes.

Step-by-step instructions

Project scenario

Imagine you've recently been hired as an ethical hacker by SecureBank, a mid-sized financial institution known for its rapidly growing digital services. In the wake of recent incidents in the banking sector, the management has become increasingly anxious about potential vulnerabilities in SecureBank's online banking platform. Preliminary investigations have highlighted weak security measures. To address these risks, the bank has tasked you with identifying vulnerabilities and investigating potential threats.

Completing project tasks

Submitting a complete assignment by adhering to the instructions will facilitate a thorough review.

For successful project submission:

- **Task 1:**
  - Complete the task and upload the required screenshot to the platform.
- **Task 2:**
  - Complete the three steps in this task and upload the corresponding screenshot for each step to the platform.
- **Task 3:**
  - Go through the six scenario-based questions and type the response that best suits the scenario in the designated area for each step. Then, provide a 1–2 line justification for your selection in the space provided.

Task 1: Identify a vulnerability using IBM X-Force Exchange
Your first task will be to identify any vulnerabilities that might expose the bank's systems to cyber threats. You will use IBM X-Force Exchange to gather threat intelligence.

The following are the steps to complete this task:

1. Visit https://exchange.xforce.ibmcloud.com/.
2. **Note:** You would have created a login in IBM X-Force Exchange when you worked on the corresponding lab.
3. Use the search bar to find a recent vulnerability that has been assigned a common vulnerabilities and exposures (CVE) number.

Submission: Capture a screenshot of the recently identified vulnerability. Ensure that the CVE number is visible.

Task 2: Investigate the selected vulnerability using Google Dorking commands
Your second task will be to further investigate the identified vulnerability using Google Dorking commands. You will use specific search queries to uncover any exposed or

publicly available sensitive information that could potentially compromise the bank's systems.

Here are the steps to use Google Dorking commands for investigating your selected vulnerability:

Step 1: Use the "site" command to find information specific to your CVE number

- **Hint:** site: CVE-2024-XXXX
- **Submission:** Capture a screenshot of the search results and upload it to the designated area. Ensure that the search command and CVE number are visible in the screenshot.

Step 2: Refine the "site" command to limit the results to gov websites

- **Hint:** site: gov CVE-2024-XXXX
- **Submission:** Capture a screenshot of the search results and upload it to the designated area. Ensure that the search command, CVE numbers, and .gov sites are all included in the screenshot.

Step 3: Use the "filetype" command to find any PDF formatted reports related to the selected vulnerability

- **Hint:** site: gov CVE-2024-XXXX filetype: pdf
- **Submission:** Capture a screenshot of the identified PDF formatted vulnerability report on a .gov website and upload it to the designated area. Ensure that the CVE number, .gov site, and the PDF file are visible in the screenshot.

Task 3: Create a penetration testing plan

Scenario: SecureBank's management wants you to conduct a penetration test on their network. Once you have identified the vulnerabilities, you will need to create a penetration testing plan. This plan will outline your strategy for simulating cyberattacks to test the network's defenses and detect weak points. In this task, you will make decisions that will affect the outcome of the penetration test.

This task consists of six steps, each with three options. You need to select the correct answer and provide a justification in the designated space.

Submission:
In the text box provided for each step:

- Enter the best answer for the scenario-based question.

- Enter a 1–2 sentence justification for your selection.

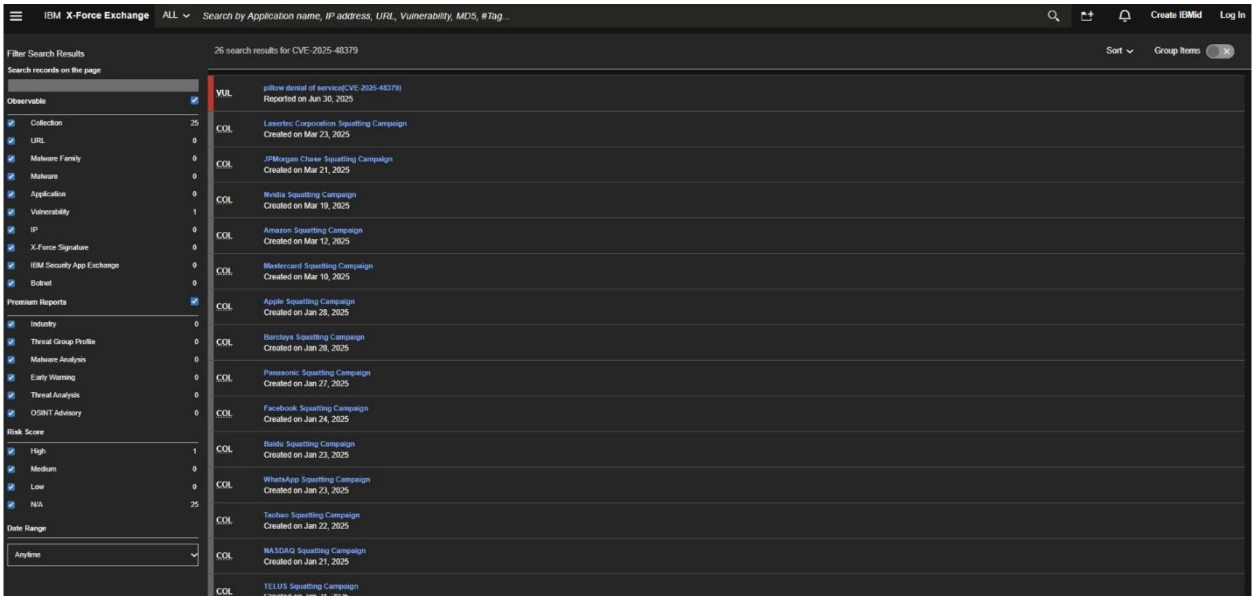
Review criteria

A total of fifty (50) points are allotted for Part 1 of this final project.

Your grade will be based on the following distribution of points:

Part 1:

- ***Task 1:*** Identify a vulnerability using IBM X-Force Exchange


IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
Create IBMid
Log In
Sort
Group Items

Filter Search Results

Search records on the page

Observable	☑
☑ Collection	25
☑ URL	0
☑ Malware Family	0
☑ Malware	0
☑ Application	0
☑ Vulnerability	1
☑ IP	0
☑ X-Force Signature	0
☑ IBM Security App Exchange	0
☑ Botnet	0
Premium Reports	☑
☑ Industry	0
☑ Threat Group Profile	0
☑ Malware Analysis	0
☑ Early Warning	0
☑ Threat Analysis	0
☑ OSINT Advisory	0
Risk Score	
☑ High	1
☑ Medium	0
☑ Low	0
☑ N/A	25

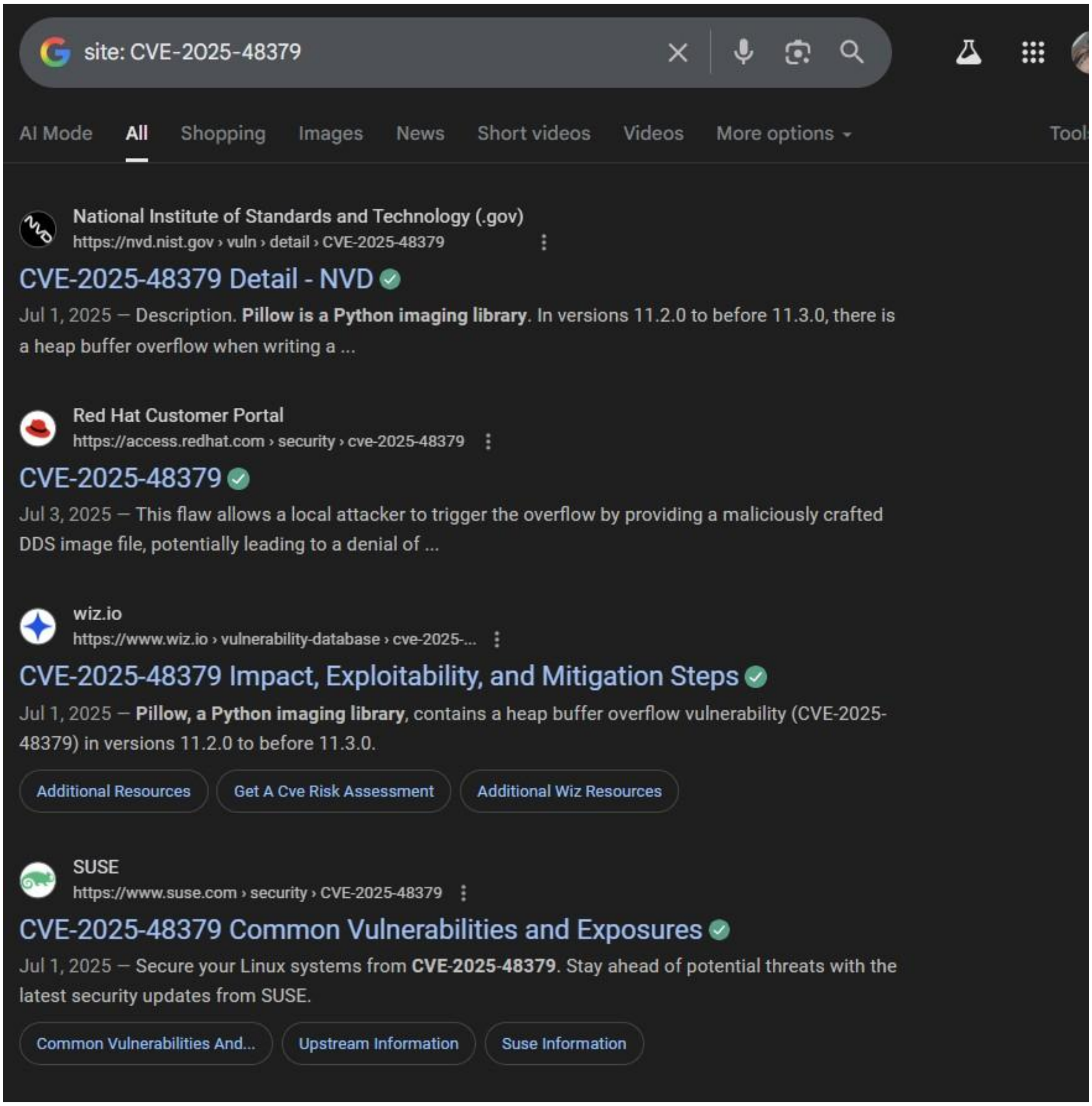
Date Range: Anytime

26 search results for CVE-2025-48379

VUL	pillow denial of service(CVE-2025-48379) Reported on Jun 30, 2025
COL	Lasertec Corporation Squatting Campaign Created on Mar 23, 2025
COL	JPMorgan Chase Squatting Campaign Created on Mar 21, 2025
COL	Nvidia Squatting Campaign Created on Mar 19, 2025
COL	Amazon Squatting Campaign Created on Mar 12, 2025
COL	Mastercard Squatting Campaign Created on Mar 10, 2025
COL	Apple Squatting Campaign Created on Jan 28, 2025
COL	Barclays Squatting Campaign Created on Jan 28, 2025
COL	Panasonic Squatting Campaign Created on Jan 27, 2025
COL	Facebook Squatting Campaign Created on Jan 24, 2025
COL	Baidu Squatting Campaign Created on Jan 23, 2025
COL	WhatsApp Squatting Campaign Created on Jan 23, 2025
COL	Taobao Squatting Campaign Created on Jan 22, 2025
COL	NASDAQ Squatting Campaign Created on Jan 21, 2025
COL	TELUS Squatting Campaign

I originally submitted CVE-2025-43300 but it was rejected due to lack of metadata/tags in the IBM X-Force Exchange. For resubmission, I've chosen CVE-2025-48379, which is fully indexed in IBM's exchange with observable and timestamped metadata. It meets the requirements of being a recent vulnerability (June 2025) and appears directly in IBM X-Force's vulnerability listings.

- ***Task 2:*** Investigate the selected vulnerability using Google Dorking commands



site: CVE-2025-48379

National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › vuln › detail › CVE-2025-48379

CVE-2025-48379 Detail - NVD

Jul 1, 2025 — Description. **Pillow is a Python imaging library**. In versions 11.2.0 to before 11.3.0, there is a heap buffer overflow when writing a ...

Red Hat Customer Portal
https://access.redhat.com › security › cve-2025-48379

CVE-2025-48379

Jul 3, 2025 — This flaw allows a local attacker to trigger the overflow by providing a maliciously crafted DDS image file, potentially leading to a denial of ...

wiz.io
https://www.wiz.io › vulnerability-database › cve-2025-...

CVE-2025-48379 Impact, Exploitability, and Mitigation Steps

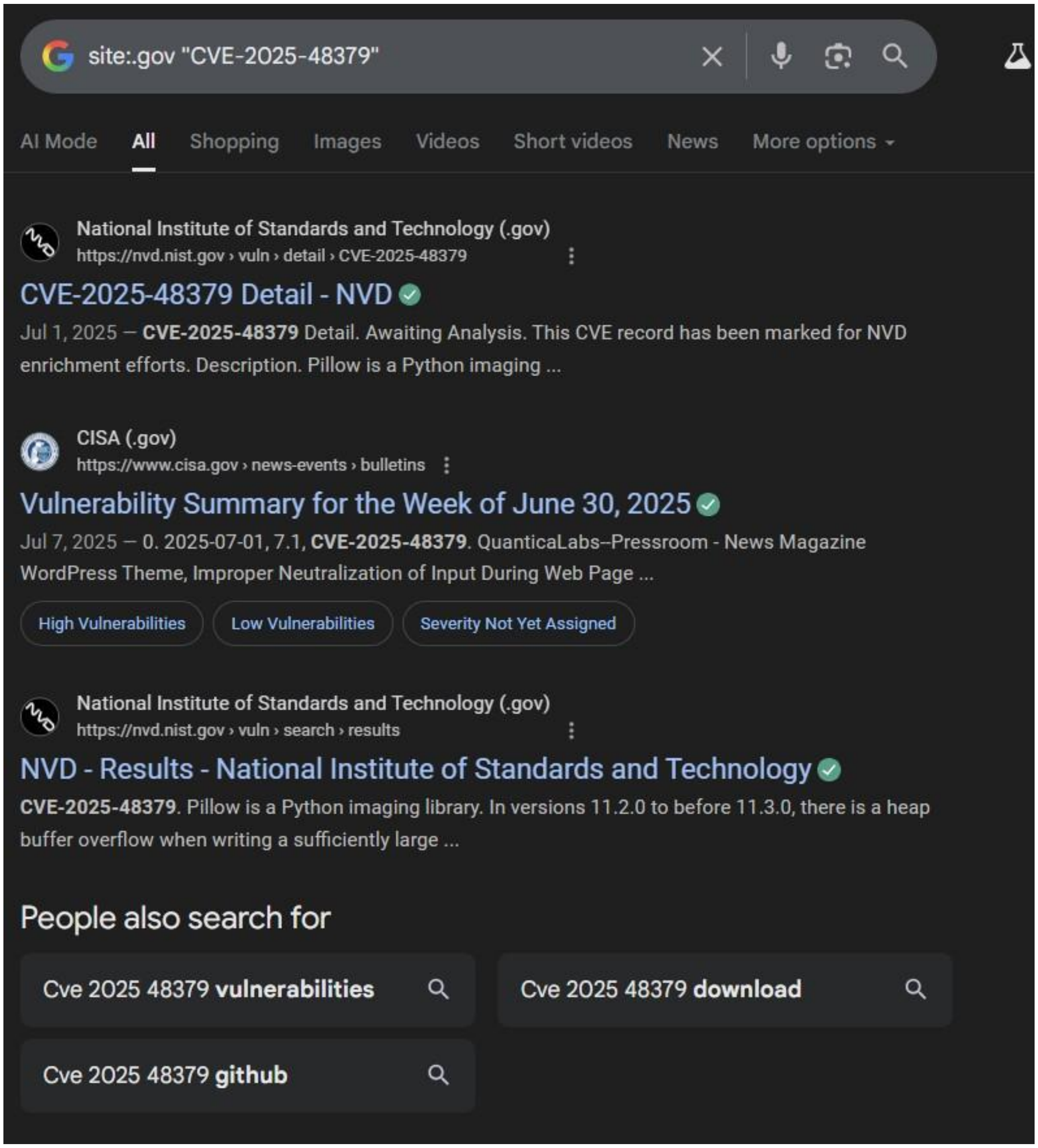
Jul 1, 2025 — **Pillow, a Python imaging library**, contains a heap buffer overflow vulnerability (CVE-2025-48379) in versions 11.2.0 to before 11.3.0.

SUSE
https://www.suse.com › security › CVE-2025-48379

CVE-2025-48379 Common Vulnerabilities and Exposures

Jul 1, 2025 — Secure your Linux systems from **CVE-2025-48379**. Stay ahead of potential threats with the latest security updates from SUSE.

Google Dorking search using the site: operator to investigate CVE-2025-48379. The search command site: CVE-2025-48379 returns relevant vulnerability details from trusted domains, including NVD, Red Hat, Wiz.io, and SUSE. This confirms that the CVE is actively documented and tracked across multiple platforms.



site:.gov "CVE-2025-48379"

National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › vuln › detail › CVE-2025-48379

CVE-2025-48379 Detail - NVD

Jul 1, 2025 — **CVE-2025-48379** Detail. Awaiting Analysis. This CVE record has been marked for NVD enrichment efforts. Description. Pillow is a Python imaging ...

CISA (.gov)
https://www.cisa.gov › news-events › bulletins

Vulnerability Summary for the Week of June 30, 2025

Jul 7, 2025 — 0. 2025-07-01, 7.1, **CVE-2025-48379**. QuanticaLabs--Pressroom - News Magazine WordPress Theme, Improper Neutralization of Input During Web Page ...

National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › vuln › search › results

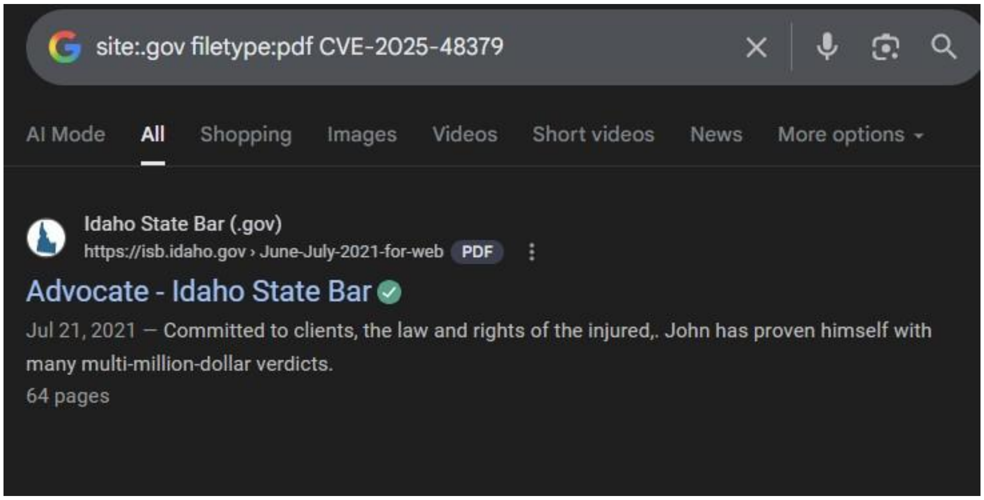
NVD - Results - National Institute of Standards and Technology

CVE-2025-48379. Pillow is a Python imaging library. In versions 11.2.0 to before 11.3.0, there is a heap buffer overflow when writing a sufficiently large ...

People also search for

Cve 2025 48379 **vulnerabilities**
Cve 2025 48379 **download**
Cve 2025 48379 **github**

The screenshot displays a refined Google Dorking search using the command site:.gov "CVE-2025-48379" to limit the results strictly to U.S. government websites. The search successfully identifies CVE-2025-48379 within official .gov resources, such as the National Vulnerability Database (NVD) maintained by the NIST. This ensures the information comes from authoritative and trusted cybersecurity sources.



site:.gov filetype:pdf CVE-2025-48379

Idaho State Bar (.gov)
https://isb.idaho.gov › June-July-2021-for-web PDF

Advocate - Idaho State Bar

Jul 21, 2021 — Committed to clients, the law and rights of the injured,. John has proven himself with many multi-million-dollar verdicts.
64 pages

This screenshot shows a refined search using site:.gov filetype:pdf CVE-48379 to locate a PDF-formatted report for the selected vulnerability on a U.S. government website. The result from the Idaho State Bar is the only .gov domain result retrieved; however, it does not appear to relate to the CVE in question, indicating that no relevant PDF vulnerability report is currently available from official .gov sources for this CVE.

- ***Task 3:*** Create a penetration testing plan

Task 3/4: Create a penetration testing plan

Step 1

Scenario: You are in a meeting with SecureBank's IT team to discuss the penetration test. The team includes the IT manager, the network administrator, and a security officer. They provide you with an overview of their infrastructure, which includes external web applications, internal databases, and a mix of on-premises and cloud-based services.

Question: What should you include in the scope?

Options:

A: Include all systems, networks, and applications

B: Focus only on the external-facing systems and applications

C: Include only the internal network and critical applications

Prompt: From the options provided, identify the correct answer. Then, provide a 1–2 line justification for your selection. In the textbox provided, type your responses in the format provided below.

Format:

Correct answer: < >

Justification: < >

Correct Answer: <A) Include all systems, network, and applications>

Justification: <Including all systems, networks and applications ensures a comprehensive assessment of SecureBanks's full infrastructure, including external web applications, internal databases, and both on-premises and cloud-based systems, allowing for the identification of vulnerabilities across all layers. This aligns with the best practices for a full scope pen test when permitted by the organization.>

Prompt

Task 3/4: Create a penetration testing plan

Step 2

Scenario: You are required to define the primary objectives of the penetration test. The IT team has expressed concerns about recent phishing attacks and regulatory compliance requirements.

Question: Which objective should be prioritized for the penetration test based on the IT team's concerns?

Options:

A: Identify all possible vulnerabilities

B: Test incident response capabilities

C: Focus on compliance with industry standards

Prompt: From the options provided, identify the correct answer. Then, provide a 1–2 line justification for your selection. In the textbox provided, type your responses in the format provided below.

Format:

Correct answer: < >

Justification: < >

Correct answer: <C.) Focus on compliance with industry standards.>

Justification: <Since the IT team is concerned about phishing attacks and regulatory compliance, the penetration test should prioritize assessing adherence to industry standards and identifying weaknesses related to compliance, especially those exploited in social engineering attacks.>

Prompt

Task 3/4: Create a penetration testing plan

Step 3

Scenario: You have to establish the rules of engagement for the penetration test. However, the IT team is concerned about potential disruptions to business operations.

Question: What approach will you take to minimize disruptions while conducting the penetration test?

Options:

A: Notify staff that the test will be conducted during business hours

B: Notify staff that the test will be conducted after business hours

C: Conduct the test without notifying the IT team

Prompt: From the options provided, identify the correct answer. Then, provide a 1–2 line justification for your selection. In the textbox provided, type your responses in the format provided below.

Format:

Correct answer: < >

Justification: < >

Correct Answer: <B.) Notify staff that the test will be conducted after business hours.

Justification: <Notifying staff that the test will be conducted after business hours helps minimize business disruptions while still keeping the team informed and engaged.>

Prompt

Task 3/4: Create a penetration testing plan

Step 4

Scenario: You begin the Discovery phase to gather information about the target systems. However, the IT team has provided you with limited information about their network topology.

Question: Which approach will be most effective for gathering information?

Options:

A: Use automated tools like Nmap and Nessus

B: Use manual techniques like social engineering

C: Use a combination of automated and manual techniques

Prompt: From the options provided, identify the correct answer. Then, provide a 1–2 line justification for your selection. In the textbox provided, type your responses in the format provided below.

Format:

Correct answer: < >

Justification: < >

Correct answer: <C) Use a combination of automation and manual techniques.>

Justification: <Using both automated tools and manual techniques ensures a more thorough discovery process, especially when internal documentation is limited. Automated tools can scan for vulnerabilities while manual methods like observation and inquiry uncover gaps the tools might miss.>

Prompt

Task 3/4: Create a penetration testing plan

Step 5

Scenario: You have identified several vulnerabilities and are ready to exploit them. The vulnerabilities include an outdated web server, weak passwords, and an unpatched database.

Question: Which approach will you take to exploit the identified vulnerabilities?

Options:

A: Exploit the easiest vulnerabilities first

B: Exploit the highest severity vulnerabilities first

C: Exploit a mix of high-severity and easy vulnerabilities

Prompt: From the options provided, identify the correct answer. Then, provide a 1–2 line justification for your selection. In the textbox provided, type your responses in the format provided below.

Format:

Correct answer: < >

Justification: < >

Correct Answer:<B.) Exploit the highest severity vulnerabilities first.>

Justification: <Exploiting the highest severity vulnerabilities first reduces the most critical risks to the system and aligns with the best practices in pen testing. Prioritizing these helps organizations address the most impactful threats immediately.>

Prompt

Task 3/4: Create a penetration testing plan

Step 6

Scenario: You now have to compile your findings and provide recommendations. Your audience includes technical staff and the executive leadership.

Question: What is the most effective way to present your findings?

Options:

A: Create a detailed technical report

B: Create a high-level executive summary

C: Create a detailed technical report and an executive summary

Prompt: From the options provided, identify the correct answer. Then, provide a 1–2 line justification for your selection. In the textbox provided, type your responses in the format provided below.

Format:

Correct answer: < >

Justification: < >

Correct Answer: <C.) Create a detailed technical report and executive summary.>

Justification: <Providing both a detailed technical report and executive summary ensures that all stakeholders receive the information in a format suited for their needs. Technical staff can act on detailed findings, while leadership can understand the strategic implications. >