KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

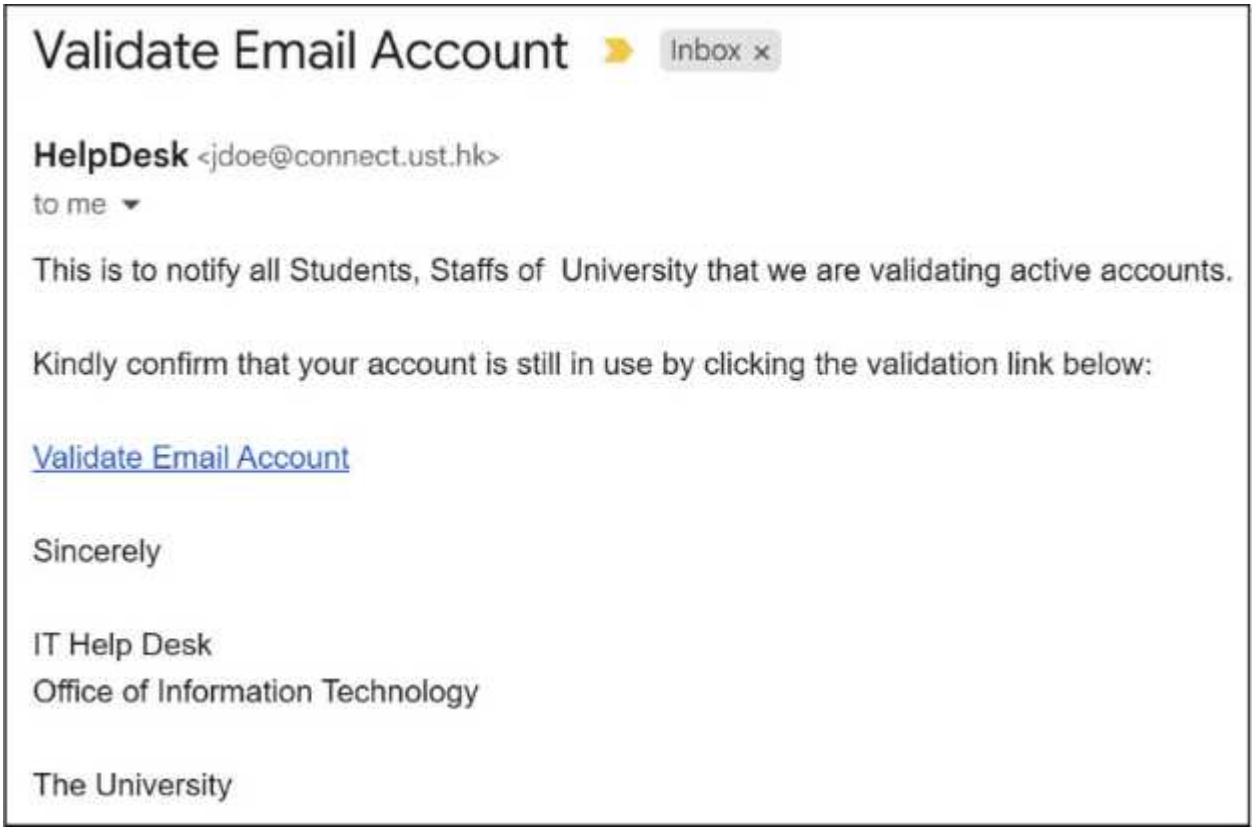
Exam : **PPAN01**

Title : Certified Threat Protection Analyst Exam

Version : DEMO

1.Refer to Exhibit:
X-Proofpoint-Banner-Trigger: inbound
MIM-version: 1.0
Content-Type: multipart/mixed; boundary="boundary-1698346305"
X-CLX-Shades: MLX
X-Proofpoint-Virus-Version: vendor=baseguard
engine=ICAP:2.0.272,Aquarius:18.0.987,Hydra:6.0.619,FMLib:17.11.176.26 definitions=2023-10-26_22,2023-10-26_01,2023-05-22_02
X-Proofpoint-Spam-Details: rule=spam policy=default score=89 bulkscore=0 phishscore=0 mlxlogscore=-91 suspectscore=0 malwarescore=0 adultscore=0 spamscore=89 classifier=spam adjust=0 reason=mlx scancount=l engine=8.12.0-2310240000 definitions=main-2310260209
In the process of reviewing a false positive, you see the following email header.
What was the reason the message was quarantined by the Proofpoint Protection Server?
A. A custom spam rule caused the message to be quarantined.
B. An anti-virus rule forced the message to be quarantined.
C. The recipient's personal block list forced quarantine of the message.
D. A content policy rule (DLP/compliance) forced quarantine of the message.
Answer: A
Explanation:
The header contains X-Proofpoint-Spam-Details: rule=spam policy=default ... spamscore=89 ... reason=mlx, which is the Proofpoint spam engine verdict (MLX classifier) and indicates quarantine was driven by the spam policy evaluation, not by anti-virus or a user block list. In Proofpoint PPS/PoD, quarantine decisions frequently include an “X-Proofpoint-*Details” header that records the policy, rule family, and scoring components used to reach the final disposition. Here, the high spamscore=89 is decisive, and there is also an MLX log score entry supporting the ML-based spam classification. Antivirus-related quarantines typically show explicit malware/virus condemnation outcomes (e.g., malware score, “virus” rule, or attachment verdicts), while personal block list actions would be reflected as user-specific allow/block triggers, not the spam classifier rule. For IR triage, this header is the fastest way to validate why a message was quarantined and whether a false positive should be addressed by tuning spam thresholds, allow lists, or MLX-related settings rather than malware policies.

2.A college student receives the email shown in the exhibit.

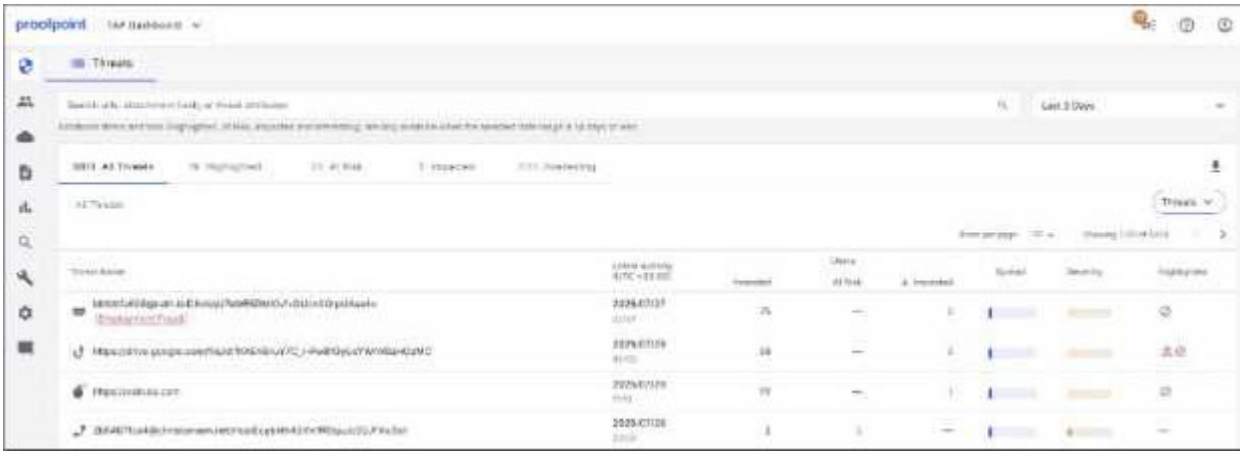


What type of attack is being performed?
A. Domain Hijacking
B. Display Name Spoofing
C. Lookalike Domain
D. Reply-To Spoofing
Answer: B
Explanation:
This is a classic phishing lure ("Validate Email Account") where the attacker aims to create trust by presenting a familiar-looking sender identity to the recipient. In many real phishing waves, attackers manipulate what the user visually trusts first: the friendly name (display name) shown by mail clients. "Display Name Spoofing" is specifically when the attacker sets the From display name to something authoritative (e.g., "HelpDesk", "IT Support", "University Admin") while the underlying sender address may not be an approved helpdesk identity, or may be a compromised mailbox that is not actually the IT department. Proofpoint IR review commonly verifies this by comparing: (1) the displayed name, (2) the RFC5322.From address, and (3) authentication results (SPF/DKIM/DMARC) plus "Header From vs Envelope From" alignment. Lookalike domain focuses on deceptive domains (e.g., great-c0mpany.com) rather than the visible name; Reply-To spoofing requires a mismatched Reply-To field, which is not the primary indicator shown in the exhibit. For response, analysts prioritize user notification, link detonation/URL Defense verdicts, and retroactive search-and-pull (TRAP/CTR) if delivered.

3.An analyst has been tasked with providing a report that can be used to prioritise investigations based on a user's Attack Index score.
Which report would be most suitable for this purpose?
A. VIP Activity

B. Top 10 Recipients
C. Very Attacked People
D. Top 10 Clickers
Answer: C
Explanation:
Attack Index is a user-level risk/burden metric intended to help SOC teams prioritize which people to investigate first based on the amount and severity/diversity of threat activity directed at them (and often their exposure/interaction, depending on module). The report that directly supports that workflow is “Very Attacked People,” which is designed to surface users with the highest Attack Index and concentration of targeted threats. Operationally, this aligns with IR queue management: instead of treating all alerts equally, analysts use user-centric risk ranking to focus on likely compromise candidates (e.g., frequent recipients of credential phishing, repeated exposure to the same campaign, or elevated threat severity). “Top 10 Recipients” is volume-oriented and may include benign bulk mail; “Top 10 Clickers” is behavior-oriented but does not necessarily reflect overall threat burden; and “VIP Activity” is scoped to a subset (VIPs) rather than the complete organization’s risk ranking. In Proofpoint-led IR best practice, this report is commonly used to drive daily standups, assign investigations, and justify proactive account checks (MFA posture, suspicious logins, mailbox rules) for the highest-risk users.

4.An analyst is reviewing the Threats page in the TAP Dashboard.



Which of the top four threats seen in the exhibit should be prioritised for investigation?
A. The Malware Delivery threat
B. The TOAD (Telephone-Oriented Attack Delivery) threat
C. The Credential Phishing threat
D. The BEC (Business Email Compromise) threat
Answer: C
Explanation:
In Proofpoint-driven triage, threats are prioritized by likelihood of immediate compromise and blast radius. Credential phishing typically ranks highest because a single successful credential submission can lead to account takeover (ATO), which then enables follow-on attacks: internal phishing, mailbox rule abuse, OAuth consent abuse, wire-fraud/BEC escalation, and data access. Proofpoint TAP surfaces credential phishing with strong indicators (URL defense verdicts, rewritten URL clicks, campaign clustering, and known phishing kits/landing pages), making it actionable for containment. Compared to malware delivery, credential theft often bypasses endpoint controls and produces fewer immediate

artifacts, so rapid response is critical: password reset, token revocation, MFA enforcement, and mailbox audit. TOAD and BEC can be high impact, but in many environments they require human interaction outside email controls (phone/social steps) and may not always show definitive technical IOCs early. The TAP “Threats” view is designed for quick pivoting (Intended/At Risk/Impacted) and credential phishing typically correlates strongly with “Impacted” activity (clicks/submissions), which is why it should be investigated first when competing items are present.

5.What is the first action a security analyst should take when beginning to review and prioritize alerts from Targeted Attack Protection (TAP)?
A. Use filtering options on the TAP Threats page to organize and prioritize threat alerts.
B. Assess claims of false positives by analyzing forensic details and threat indicators.
C. Open and examine the contents of an email using the associated .eml file.
D. Investigate false negatives by identifying root causes in source policy configurations.
Answer: A
Explanation:
The first step in a scalable TAP-driven workflow is to reduce the alert set into an actionable queue using built-in filtering on the Threats page (time range, severity, threat type, campaign grouping, Intended/At Risk/Impacted, VIP targeting, and “Highlighted” categories). This aligns with SOC operational procedures: triage is a funnel, and TAP’s dashboards are optimized for sorting by risk and user impact so analysts can quickly identify what is most likely to represent an active incident. Jumping straight into .eml review or false-positive adjudication is inefficient before you know which threats have user interaction (clicks), broad distribution, or high severity. Likewise, false-negative root cause analysis is a later-stage improvement activity, typically triggered after an incident or quality review. In Proofpoint IR practice, you filter first to find: (1) threats with “Impacted” users (clicks/interaction), (2) high severity (credential theft/malware), (3) VIP targeting, and (4) campaign clusters. Only then do you pivot into forensic details, message artifacts, URL/attachment detonation results, and—if necessary—remediation actions (blocklists, TRAP pulls, user resets).