

# ECCouncil 212-82자격증참고서 & 212-82높은통과율인 기덤프문제



## ECCouncil

212-82  
Certified Cybersecurity Technician (CCT)

- Up to Date products, reliable and verified.
- Questions and Answers in PDF Format.

### Full Version Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24 Hours Live Chat Support

### For More Information:

<https://www.testsexpert.com/>

### • Product Version

Visit us at <https://www.testsexpert.com/212-82/>

그리고 KoreaDumps 212-82 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다:  
<https://drive.google.com/open?id=1KHcH3qiX8sZM1byDMC750NitdLJIOWAZ>

ECCouncil인증 212-82시험패스 공부방법을 찾고 있다면 제일 먼저KoreaDumps를 추천해드리고 싶습니다. ECCouncil인증 212-82시험이 많이 어렵다는것은 모두 알고 있는 것입니다. KoreaDumps에서 출시한 ECCouncil인증 212-82덤프는 실제시험을 대비하여 연구제작된 멋진 작품으로서 ECCouncil인증 212-82시험적중율이 최고입니다. ECCouncil인증 212-82시험패스를 원하신다면KoreaDumps의 제품이 고객님의 소원을 들어줄것입니다.

CCT (Certified Cybersecurity Technician) 시험은 사이버 보안과 관련된 광범위한 주제를 다룹니다. 여기에는 네트워크 보안, 암호화, 맬웨어 분석, 사고 대응 및 취약성 평가가 포함됩니다. 이 시험은 또한 윤리적 해킹 기술과 사이버 보안을 둘러싼 법적 및 윤리적 문제를 다룹니다.

>> ECCouncil 212-82자격증참고서 <<

## 212-82자격증참고서 시험 최신 덤프자료

ECCouncil 212-82 덤프의 PDF 버전과 Software 버전의 내용은 동일합니다. PDF버전은 프린트 가능한 버전으로서 단독구매하셔도 됩니다. Software 버전은 테스트용으로 PDF 버전 공부를 마친후 시험전에 실력테스트 가능합니다. Software 버전은 PDF버전의 보조용이기에 단독 판매하지 않습니다. 소프트웨어버전까지 필요하신 분은 PDF버전

을 구입하실때 공동구매하셔야 합니다.

ECCouncil 212-82 인증 시험을 치르려면 개인은 네트워킹 개념 및 프로토콜에 대한 기본적인 이해를 가져야합니다. 시험은 50 개의 객관식 질문으로 구성되며 통과 점수는 70%입니다. 인증은 3 년간 유효하며 최신 버전의 시험을 취하거나 평생 교육 크레딧을 통해 갱신 할 수 있습니다. ECCOUNCIL 212-82 인증을 얻으면 사이버 보안 분야에서 개인의 신뢰성을 높이고 경력 기회를 높일 수 있습니다.

ECCouncil 212-82 시험은 인증된 사이버 보안 기술자 자격증으로 알려져 있으며, 사이버 보안 분야에서 경력을 쌓고자 하는 개인들을 위해 설계된 광범위하게 인정받는 자격증 프로그램입니다. 이 시험은 네트워크 및 시스템 보안, 사고 대응, 위협 분석 및 취약점 평가 분야에서 후보자의 지식과 기술을 검증하기 위해 설계되었습니다. 이 자격증은 사이버 보안 개념과 실천에 대한 기본적인 이해를 얻고자 하는 입문자 수준의 사이버 보안 전문가들에게 이상적입니다.

## 최신 Cyber Technician (CCT) 212-82 무료샘플문제 (Q104-Q109):

### 질문 # 104

Grace, an online shopping freak, has purchased a smart TV using her debit card. During online payment, Grace's browser redirected her from ecommerce website to a third-party payment gateway, where she provided her debit card details and OTP received on her registered mobile phone. After completing the transaction, Grace navigated to her online bank account and verified the current balance in her savings account.

Identify the state of data when it is being processed between the ecommerce website and the payment gateway in the above scenario.

- A. Data in use
- B. Data in inactive
- C. Data at rest
- **D. Data in transit**

정답: D

설명:

Data in transit is the state of data when it is being processed between the ecommerce website and the payment gateway in the above scenario. Data in transit is data that is moving from one location to another over a network, such as the internet, a LAN, or a WAN. Data in transit can be vulnerable to interception, modification, or theft by unauthorized parties, so it needs to be protected by encryption, authentication, and other security measures. Data at rest is data that is stored on a device or a media, such as a hard drive, a flash drive, or a cloud storage. Data in active is data that is currently being accessed or modified by an application or a user. Data in use is data that is loaded into the memory of a device or a system for processing or computation.

### 질문 # 105

Camden, a network specialist in an organization, monitored the behavior of the organizational network using SIEM from a control room. The SIEM detected suspicious activity and sent an alert to the camer a. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers. Which of the following SIEM functions allowed Camden to view suspicious behavior and make correct decisions during a security incident?

- A. Application log monitoring
- **B. Dashboard**
- C. Log Retention
- D. Data aggregation

정답: B

설명:

Dashboard is the SIEM function that allowed Camden to view suspicious behavior and make correct decisions during a security incident. SIEM (Security Information and Event Management) is a system or software that collects, analyzes, and correlates security data from various sources, such as logs, alerts, events, etc., and provides a centralized view and management of the security posture of a network or system. SIEM can be used to detect, prevent, or respond to security incidents or threats. SIEM consists of various functions or components that perform different tasks or roles. Dashboard is a SIEM function that provides a graphical user interface (GUI) that displays various security metrics, indicators, alerts, reports, etc., in an organized and interactive manner. Dashboard can be used to view suspicious behavior and make correct decisions during a security incident. In the scenario, Camden monitored the

behavior of the organizational network using SIEM from a control room. The SIEM detected suspicious activity and sent an alert to Camden. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers. This means that he used the dashboard function of SIEM for this purpose. Application log monitoring is a SIEM function that collects and analyzes application logs, which are records of events or activities that occur within an application or software. Log retention is an SIEM function that stores and preserves logs for a certain period of time or indefinitely for future reference or analysis. Data aggregation is an SIEM function that combines and normalizes data from different sources into a common format or structure.

#### 질문 # 106

Warren, a member of IH&R team at an organization, was tasked with handling a malware attack launched on one of servers connected to the organization's network. He immediately implemented appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization.

Identify the IH&R step performed by Warren in the above scenario.

- A. Incident triage
- B. Eradication
- C. Recovery
- **D. Containment**

**정답: D**

**설명:**

Containment is the IH&R step performed by Warren in the above scenario. IH&R (Incident Handling and Response) is a process that involves identifying, analyzing, containing, eradicating, recovering from, and reporting on security incidents that affect an organization's network or system. Containment is the IH&R step that involves implementing appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization. Containment can be done by isolating the affected system or network, blocking malicious traffic or communication, disabling or removing malicious accounts or processes, etc.

Recovery is the IH&R step that involves restoring the normal operation of the system or network after eradicating the incident.

Eradication is the IH&R step that involves removing all traces of the incident from the system or network, such as malware, backdoors, compromised files, etc.

Incident triage is the IH&R step that involves prioritizing incidents based on their severity, impact, and urgency.

#### 질문 # 107

As a cybersecurity technician, you were assigned to analyze the file system of a Linux image captured from a device that has been attacked recently. Study the forensic image 'Evidenced.img' in the Documents folder of the "Attacker Machine-1" and identify a user from the image file. (Practical Question)

- A. john
- **B. attacker**
- C. roger
- D. smith

**정답: B**

**설명:**

The attacker is a user from the image file in the above scenario. A file system is a method or structure that organizes and stores files and data on a storage device, such as a hard disk, a flash drive, etc. A file system can have different types based on its format or features, such as FAT, NTFS, ext4, etc. A file system can be analyzed to extract various information, such as file names, sizes, dates, contents, etc. A Linux image is an image file that contains a copy or a snapshot of a Linux-based file system. A Linux image can be analyzed to extract various information about a Linux-based system or device. To analyze the file system of a Linux image captured from a device that has been attacked recently and identify a user from the image file, one has to follow these steps:

Navigate to Documents folder of Attacker Machine-1.

Right-click on Evidenced.img file and select Mount option.

Wait for the image file to be mounted and assigned a drive letter.

Open File Explorer and navigate to the mounted drive.

Open etc folder and open passwd file with a text editor.

Observe the user accounts listed in the file.

The user accounts listed in the file are:

```

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:systemd-network:x:systemd-resolve:x:
systemd-bus-proxy:x:syslog:x:_apt:x:messagebus:x:uidd:x:lightdm:x:whoopsie:x:avahi-autoipd:x:avahi:x:dnsmasq:x:colord:x:
speech-dispatcher:x:hplip:x:kernoops:x:saned:x:nm-openvpn:x:nm-openconnect:x:pulse:x:rtkit:x:sshd:x:attacker::1000 The user
account that is not a system or service account is attacker, which is a user from the image file.

```

**질문 # 108**

Maisie, a new employee at an organization, was given an access badge with access to only the first and third floors of the organizational premises. Maisie Hied scanning her access badge against the badge reader at the second-floor entrance but was unsuccessful. Identify the short- range wireless communication technology used by the organization in this scenario.

- A. Li-Fi
- B. Wi-Fi
- C. Bluetooth
- **D. RFID**

**정답: D**

**설명:**

RFID (Radio Frequency Identification) is a short-range wireless communication technology that uses radio waves to identify and track objects. RFID tags are attached to objects and RFID readers scan the tags to obtain the information stored in them. RFID is commonly used for access control, inventory management, and identification.

**질문 # 109**

.....

**212-82높은 통과율 인기 덤프문제**: [https://www.koreadumps.com/212-82\\_exam-braindumps.html](https://www.koreadumps.com/212-82_exam-braindumps.html)

- 100% 유효한 212-82자격증참고서 시험덤프  ➡ [www.exampassdump.com](http://www.exampassdump.com) 에서  212-82 를 검색하고 무료로 다운로드하세요212-82덤프샘플문제 체험
- 212-82최신 업데이트 덤프문제  212-82최신 인증시험 대비자료  212-82완벽한 시험덤프공부  [[www.itdumpskr.com](http://www.itdumpskr.com)]에서 검색만 하면“212-82”를 무료로 다운로드할 수 있습니다212-82퍼펙트 덤프 최신 샘플
- 212-82자격증참고서 인기자격증 시험덤프 ☆ 지금▷ [www.dumptop.com](http://www.dumptop.com)◁에서  212-82 를 검색하고 무료로 다운로드하세요212-82완벽한 시험덤프공부
- 212-82최신 업데이트 덤프문제  212-82퍼펙트 최신 덤프공부  212-82최고합격덤프  무료 다운로드를 위해[ 212-82 ]를 검색하려면 「 [www.itdumpskr.com](http://www.itdumpskr.com) 」을(를) 입력하십시오212-82덤프샘플문제 체험
- 시험패스 가능한 212-82자격증참고서 덤프 최신 데모  《 [kr.fast2test.com](http://kr.fast2test.com) 》에서“212-82”를 검색하고 무료로 다운로드하세요212-82최고품질 덤프데모 다운로드
- 212-82자격증참고서 인기자격증 시험덤프  ▶ [www.itdumpskr.com](http://www.itdumpskr.com) ◀을(를) 열고[ 212-82 ]를 입력하고 무료로 다운로드를 받으십시오212-82자격증공부
- 212-82최신 덤프공부자료  212-82퍼펙트 최신 덤프공부  212-82시험대비 최신버전 공부자료  「 [www.dumptop.com](http://www.dumptop.com) 」의 무료 다운로드  212-82 페이지가 지금 열립니다212-82덤프샘플문제 체험
- 212-82시험유효덤프  212-82시험대비 공부하기  212-82최신 인증시험 덤프데모  검색만 하면{ [www.itdumpskr.com](http://www.itdumpskr.com) }에서[ 212-82 ]무료 다운로드212-82최신 인증시험 덤프데모
- 212-82덤프샘플문제 체험  212-82최고합격덤프  212-82최고품질 덤프데모 다운로드  ⇒ 212-82 ⇐를 무료로 다운로드하려면  [kr.fast2test.com](http://kr.fast2test.com) 웹사이트를 입력하세요212-82자격증공부
- 212-82최신 덤프문제모음집  212-82자격증공부  212-82퍼펙트 덤프 최신 샘플  지금▶ [www.itdumpskr.com](http://www.itdumpskr.com) 에서 ⇒ 212-82 를 검색하고 무료로 다운로드하세요212-82시험대비 최신버전 공부자료
- 212-82자격증참고서 완벽한 시험 최신버전 자료  시험 자료를 무료로 다운로드하려면⇒ [www.koreadumps.com](http://www.koreadumps.com) 을 통해 ( 212-82 ) 를 검색하십시오212-82최신버전 인기 덤프자료
- [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [lms.digitalmantraacademy.com](http://lms.digitalmantraacademy.com), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [www.callcentersindia.co.in](http://www.callcentersindia.co.in), [rasnir.com](http://rasnir.com),

helpingmummiesanddaddiesagencytt.com, hhi.instructure.com, www.52tikong.com, academy.frenchrealm.com,  
dl.instructure.com, Disposable vapes

BONUS!!! KoreaDumps 212-82 시험 문제집 전체 버전을 무료로 다운로드하세요: <https://drive.google.com/open?id=1KHcH3qiX8sZM1byDMC750NitdLJOWAZ>