

# 200-201 Prüfungsunterlagen, 200-201 Fragen&Antworten



Übrigens, Sie können die vollständige Version der Zertprüfung 200-201 Prüfungsfragen aus dem Cloud-Speicher herunterladen:  
<https://drive.google.com/open?id=1OfjcGGGSs3jwogh9UY9JOQRQogrOBhlXB>

Wenn Sie sich noch anstrengend bemühen, die Cisco 200-201 Prüfung zu bestehen, kann Zertprüfung Ihren Traum verwirklichen. Die Schulungsunterlagen zur Cisco 200-201 Zertifizierung von Zertprüfung sind die besten und bieten Ihnen auch eine gute Plattform zum Lernen. Die Frage lautet, wie Sie sich auf die Prüfung vorbereiten sollen, um die 200-201 Prüfung 100% zu bestehen. Die Antwort ist ganz einfach. Sie sollen die Fragenkataloge zur Cisco 200-201 Zertifizierung von Zertprüfung wählen. Mit ihr können Sie sich ganz entspannt auf die 200-201 Prüfung vorbereiten.

Die Cisco 200-201-Zertifizierungsprüfung soll Kenntnisse und Fähigkeiten der Kandidaten im Bereich der Cybersicherheitsoperationen testen. Es ist eine grundlegende Zertifizierung auf der Ebene, die die Grundlagen von Cybersicherheitsoperationen und die damit verbundenen Technologien, Tools und Verfahren abdeckt. Die Prüfung richtet sich an Fachleute, die daran interessiert sind, ihre Karriere im Bereich Cybersicherheit zu starten oder voranzutreiben.

Die CISCO 200-201-Zertifizierungsprüfung ist eine grundlegende Prüfung für Personen, die an einer Karriere in Cybersecurity-Operationen interessiert sind. Die Prüfung soll das Wissen eines Individuums über grundlegende Cybersicherheitskonzepte und -operationen testen. Es soll auch Kandidaten helfen, die Fähigkeiten und das Wissen zu verstehen, die für die Arbeit als Cybersicherheitsanalyst erforderlich sind.

>> 200-201 Prüfungsunterlagen <<

## Cisco 200-201 Fragen&Antworten - 200-201 Vorbereitungsfragen

Wenn Sie Dumps zur Cisco 200-201 Zertifizierungsprüfung von Zertprüfung kaufen, versprechen wir Ihnen, dass Sie 100% die Cisco 200-201 Zertifizierungsprüfung bestehen können. Sonst zahlen wir Ihnen die gesamte Summe zurück.

Das Bestehen der Cisco 200-201 Prüfung ist ein wesentlicher Schritt für jeden Cybersecurity-Enthusiasten, der seine Karriere in den Bereichen Cybersecurity-Operationen vorantreiben möchte. Das Zertifizierungsprogramm ermöglicht es den Kandidaten, grundlegende Fähigkeiten zu erwerben, die notwendig sind, um die aktuelle Cybersecurity-Landschaft zu verstehen, auf Vorfälle zu reagieren und Risiken zu mindern sowie die Sicherheitslage ihrer Organisation zu verbessern. Das Zertifizierungsprogramm validiert auch die Fähigkeit des Kandidaten, Cybersecurity-Terminologie und Konzepte zu verstehen, was die Kompetenz des Kandidaten in IT-Risiken und der Einhaltung von Industriestandards erhöhen kann.

# Cisco Understanding Cisco Cybersecurity Operations Fundamentals 200-201

## Prüfungsfragen mit Lösungen (Q343-Q348):

### 343. Frage

Refer to the exhibit.

An attacker gained initial access to the company's network and ran an Nmap scan to advance with the lateral movement technique and to search the sensitive data. Which two elements can an attacker identify from the scan? (Choose two.)

- A. number of users and requests that the server is handling
- B. functionality and purpose of the server
- C. user accounts and SID
- D. workload and the configuration details
- E. running services

**Antwort:** B,E

Begründung:

An Nmap scan can provide detailed information about a network including the functionality and purpose of servers on that network as well as any services that are currently running on those servers. This information can be used by an attacker to identify potential vulnerabilities or targets for exploitation during a cyber attack.

References := Cisco Cybersecurity Training

### 344. Frage

What is an example of social engineering attacks?

- A. sending a verbal request to an administrator who knows how to change an account password
- B. receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company
- C. receiving an email from human resources requesting a visit to their secure website to update contact information
- D. receiving an invitation to the department's weekly WebEx meeting

**Antwort:** C

### 345. Frage

A company recently encountered a breach. Critical services went through a disturbance and the integrity of the data was altered. An engineer is investigating the issue and searching through the logs in the SIEM. Which phase of the incident response is an engineer working on?

- A. detection and analysis
- B. containment and eradication
- C. post-incident and lessons learned
- D. recovery and restoration

**Antwort:** A

### 346. Frage

What is rule-based detection when compared to statistical detection?

- A. likelihood of user's action
- B. proof of a user's identity
- C. falsification of a user's identity
- D. proof of a user's action

**Antwort:** D

Begründung:

Rule-based detection is a type of intrusion detection system (IDS) that uses predefined rules or signatures to identify malicious or suspicious activity. Rule-based detection can provide proof of a user's action, such as an attempt to exploit a known vulnerability or execute a malicious command. Rule-based detection can also provide a high level of accuracy and specificity, but it requires constant updates and maintenance of the rules or signatures. References:

<https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fund> (Module 4: Attack Methods, Lesson 4.2: Attack Techniques)

### 347. Frage

Refer to the exhibit.

- A company's user HTTP connection to a malicious site was blocked according to configured policy. What is the source technology used for this measure?

- A. web proxy
  - B. network application control
  - C. firewall
  - D. IPS

Antwort: A

## Begründung:

A web proxy is the technology used to block a user's HTTP connection to a malicious site according to configured policy. It acts as an intermediary between users and the internet, enforcing security policies and preventing access to harmful sites by inspecting and managing web traffic.

### 348. Frage

• • • •

**200-201 Fragen&Antworten:** [https://www.zertpruefung.de/200-201\\_exam.html](https://www.zertpruefung.de/200-201_exam.html)

vapes

P.S. Kostenlose und neue 200-201 Prüfungsfragen sind auf Google Drive freigegeben von Zertpruefung verfügbar:  
<https://drive.google.com/open?id=1OfjcGGGSs3jwogh9UY9JOQROgrOBhlXB>