

200-201^{Q&As}

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/200-201.html

100% Passing Guarantee 100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

Instant Download After Purchase

- 100% Money Back Guarantee
- 😳 365 Days Free Update
- 800,000+ Satisfied Customers





QUESTION 1

Refer to the exhibit.

Top Alarming Hosts	- 2	Alarms by Type	Today's Alarms	
HOST	CATEGORY	1		
10.201.3.51 💮 Ent Usar Devices	20	§2	Suspect Data Hoarding: 17	Crypto Compliance Violation - TLS 1.0: 9
10.201.3.149 () Kind User Devices	DH RC CI EX	t teet to	Data Hoarding: 4	High Target Index: 11 High Total Traffic: 15
10.201.3.18 💮 Int Unit Onders	RC DH	0 0 0 0 0 0 0 4/10 5/1 5/2 5/3 5/4 5/5 5/0	Policy Vidance:2	New Flows Initiated: 2
10.150.1.200 🖯 Web-cated/acc	RC DH RC C	4/30 5/1 5/2 5/3 5/4 5/5 5/6 © Crypto Compliance Violation - TLS L0 © Packet Flood @ High Target Index @ High Total Traffic @ Nam Rove Initiated @ S1%b Received	Suspend Date Loss. 5 Max Flows Served: 2	High Traffic 5 High Concern Index: 13
10.201.0.23 💮 Territal Derena	DH	High File Sharing Index. Relationship High Total Traffic. High Concern Index. Europed Long Flow High Concern Index. Warn Procession Mar Flows Honored	Worm Propagation: 57	Suspect Long Flow: 11 Relationship SYN Floor: 2
10.10.101.24 🗇 End Uter Devices	E	New Rows Served Suspectifiers Press © Data Extension ® Dolby Violation Suspect Durit Leng How Roles © Data Hearing High DDoD Target Index ® Part Sus Target Lenger Index ® Part Sus Target Index ® Part Sus		Worm Activity: 3
10.201.3.83 () End Liter Deukes		Deselect All Select All		
	Wein All Hosts >			

What is the potential threat identified in this Stealthwatch dashboard?

- A. A policy violation is active for host 10.10.101.24.
- B. A host on the network is sending a DDoS attack to another inside host.
- C. There are two active data exfiltration alerts.
- D. A policy violation is active for host 10.201.3.149.

Correct Answer: C

QUESTION 2

An information security analyst inspects the .pcap file and observes encrypted unusual SSH traffic flow over nonstandard ports. Which technology makes this behavior feasible?

- A. NAT
- B. tunneling
- C. P2P
- D. TOR
- Correct Answer: B

QUESTION 3

Which security model assumes an attacker within and outside of the network and enforces strict verification before



connecting to any system or resource within the organization?

A. Biba

- B. Object-capability
- C. Take-Grant
- D. Zero Trust
- Correct Answer: D

Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

QUESTION 4

An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?

- A. nmap --top-ports 192.168.1.0/24
- B. nmap P 192.168.1.0/24
- C. nmap -sL 192.168.1.0/24
- D. nmap -sV 192.168.1.0/24

Correct Answer: B

https://explainshell.com/explain?cmd=nmap+-sP

QUESTION 5

Which attack method intercepts traffic on a switched network?

- A. denial of service
- B. ARP cache poisoning
- C. DHCP snooping
- D. command and control

Correct Answer: B

An ARP-based MITM attack is achieved when an attacker poisons the ARP cache of two devices with the MAC address of the attacker\\'s network interface card (NIC). Once the ARP caches have been successfully poisoned, each victim device sends all its packets to the attacker when communicating to the other device and puts the attacker in the middle of the communications path between the two victim devices. It allows an attacker to easily monitor all communication between victim devices. The intent is to intercept and view the information being passed between the two victim devices and potentially introduce sessions and traffic between the two victim devices



200-201 VCE Dumps

200-201 Practice Test

200-201 Exam Questions