شما به عنوان تیم مشاور امنیت شبکه وارد یک سازمان شده‌اید. مدیر فناوری اطلاعات اعلام کرده است که:

- کاربران گاهی به VLAN های غیرمجاز دسترسی پیدا می‌کنند.
- چندین بار Loop در شبکه ایجاد شده است.
- تجهیزات ناشناس به سوئیچ‌ها متصل شده‌اند.
- حملات ARP و DHCP مشکوک مشاهده شده است.
- دسترسی مدیریتی تجهیزات به درستی کنترل نمی‌شود.

هیچ مکانیزم امنیتی روی تجهیزات Cisco فعال نیست.

از شما خواسته شده وضعیت فعلی را بررسی، تهدیدها را شناسایی و راهکارهای مناسب را پیشنهاد و پیاده‌سازی کنید.

۱. این حمله در کدام لایه OSI رخ می‌دهد؟
۲. شاخص‌های شناسایی حمله چیست؟
۳. چه لاگ‌هایی تولید می‌شود؟
٤. چه ابزارهایی برای کشف آن وجود دارد؟
٥. راهکار Cisco چیست؟
٦. محدودیت‌های راهکار چیست؟
۷. آیا این حمله هنوز در شبکه‌های مدرن کاربرد دارد؟