Module 10: LAN Security Concepts Switching, Routing and Wireless Essentials v7.0 (SRWE) Module Objectives Module Title: LAN Security Concepts Module Objective: Explain how vulnerabilities compromise LAN security Topic Title Topic Objective Endpoint Security Explain how to use endpoint security to mitigate attacks Access Control Explain how AAA and 802.1x are used to authenticate LAN endpoints and devices Layer 2 Security Threats Identify Layer 2 vulnerabilities MAC Address Table Attack Explain how a MAC address table attack compromised LAN security LAN Attacks Explain how LAN attacks compromise LAN security .2 10.1 Endpoint Security .3 Network Attacks Today The news media commonly covers attacks on enterprise networks.Now the threat actor sends unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway.o To conduct an STP manipulation attack, the attacking host broadcasts STP bridge protocol data units (BPDUs) containing configuration and topology changes that will force spanning-tree recalculations.o The IEEE 802.1X standard is a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports.The first step in mitigating attacks on the Layer 2 infrastructure is to understand the underlying operation of Layer 2 and the Layer 2 solutions: Port Security, DHCP Snooping, DAI, and IPSG.o VLAN hopping and VLAN double-tagging attacks can be prevented by implementing the following trunk security guidelines: o Disable trunking on all access ports.In a typical attack, a threat actor sends unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway, effectively setting up a man-in-the-middle attack.IPv6 includes strategies to mitigate Neighbor Advertisement spoofing, similar to the way IPv6 prevents a spoofed ARP Reply.gratuitous ARP: o Check IP duplication o Change gateway data o IP address spoofing is when a threat actor hijacks a valid IP address of another device on the subnet or uses a random IP address.CDP information includes the IP address of the device, IOS software version, platform, capabilities, and the native VLAN.o Endpoints are particularly susceptible to malware-related attacks that originate through email or web browsing, such as DDOS, date breaches, and malware.These endpoints have typically used traditional host-based security features, such as antivirus/antimalware, host- based firewalls, and host-based intrusion prevention systems (HIPSs).o AAA controls who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting).CDP information includes the IP address of the device, IOS software version, platform, capabilities, and the native VLAN.o ARP spoofing and ARP poisoning are mitigated by implementing Dynamic ARP Inspection (DAI).o Network attackers can manipulate the Spanning Tree Protocol (STP) to conduct an attack by spoofing the root bridge and changing the topology of a network.o An attacker can send a gratuitous ARP message containing a spoofed MAC address to a switch, and the switch would update its MAC table accordingly.CDP information is sent out CDP-enabled ports in periodic, unencrypted, unauthenticated broadcasts.Endpoints are best protected by a combination of NAC, host-based AMP software, an email security appliance (ESA), and a web security appliance (WSA).o Disable auto trunking on trunk links so that trunks must be manually enabled.o CDP Reconnaissance: CDP information is sent out CDP-enabled ports in periodic, unencrypted broadcasts.Other hosts on the subnet store the MAC address

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي

and IP address contained in the gratuitous ARP in their ARP tables.o There is no security mechanism at Layer 2 that allows a switch to verify the source of MAC addresses, which is what makes it so vulnerable to spoofing.CDP Reconnaissance The Cisco Discovery Protocol (CDP) is a proprietary Layer 2 link discovery protocol.o To disable CDP globally on a device, use the no cdp run global configuration mode command.o ARP Attack: A threat actor sends a gratuitous ARP message containing a spoofed MAC address to a switch, and the switch updates its MAC table accordingly.ARP spoofing and ARP poisoning are mitigated by implementing DAI.o STP Attack: Threat actors manipulate STP to conduct an attack by spoofing the root bridge and changing the topology of a network.o IPv6 uses ICMPv6 Neighbor Discovery Protocol for Layer 2 address resolution.o MAC address spoofing attacks occur when the threat actors alter the MAC address of their host to match another known MAC address of a target host.It then inadvertently forwards frames destined for the target host to the attacking host.o IP and MAC address spoofing can be mitigated by implementing IP Source Guard (IPSG).o This STP attack is mitigated by implementing BPDU Guard on all access ports.Network administrators also use CDP to help configure and troubleshoot network devices.To mitigate the exploitation of CDP, limit the use of CDP on devices or ports.For example, disable CDP on edge ports that connect to untrusted devices.To enable CDP globally, use the cdp run global configuration command.o To disable CDP on a port, use the no cdp enable interface configuration command.Note: Link Layer Discovery Protocol (LLDP) is also vulnerable to reconnaissance attacks.To disable LLDP on the interface, configure no lldp transmit and no lldp receive.o A VLAN double-tagging attack is unidirectional and works only when the threat actor is connected to a port residing in the same VLAN as the native VLAN of the trunk port.Both attacks are mitigated by implementing DHCP snooping.o Address Spoofing Attack: IP address spoofing is when a threat actor hijacks a valid IP address of another device on the subnet or uses a random IP address.MAC address spoofing attacks occur when the threat actors alter the MAC address of their host to match another known MAC address of a target host.IP and MAC address spoofing can be mitigated by implementing IPSG.Threat actors make their hosts appear as root bridges; therefore, capturing all traffic for the immediate switched domain.This STP attack is mitigated by implementing BPDU Guard on all access ports.To mitigate the exploitation of CDP, limit the use of CDP on devices or ports.IP address spoofing is difficult to mitigate, especially when it is used inside a subnet in which the IP belongs.To stop the switch from returning the port assignment to its correct state, the threat actor can create a program or script that will constantly send frames to the switch so that the switch maintains the incorrect or spoofed information.It is enabled on all Cisco devices by default.The device receiving the CDP message updates its CDP database.To enable CDP on a port, use the cdp enable interface configuration command.Configure no lldp run to disable LLDP globally.o MAC address flooding attacks bombard the switch with fake source MAC addresses until the switch MAC address table is full.o A VLAN hopping attack enables traffic from one VLAN to be seen by another VLAN without the aid of a router.o Two types of DHCP attacks are DHCP starvation and DHCP spoofing.The device receiving the CDP message updates its CDP database.the information provided by CDP can also be used by a threat actor to discover network infrastructure vulnerabilities.The switch overwrites the current MAC table entry and assigns the MAC address to the new port.Attackers can then capture all traffic for the immediate

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي

switched domain.The BPDUs sent by the attacking host announce a lower bridge priority in an attempt to be elected as the root bridge.Summary 10.6 Module Practice and Quiz .43 What Did I Learn In This Module?o If Layer 2 is compromised, then all layers above it are also affected.o Be sure that the native VLAN is only used for trunk links.o There are many tools available on the internet to create ARP man-in-the-middle attacks.These won't work unless management protocols are secured.o When the target host sends traffic, the switch will correct the error, realigning the MAC address to the original port.BPDU ?.Guard is discussed in more detail later in the course

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي