قائمة الاسئلة

امتحان نهاية الفصل الدراسي الثاني - للعام الجامعي 1446 هـ - الموافق -2025/2024مـكلية الحاسوب وتكنولوجيا المعلومات :: امنية شبكات

د.عبدالرحمن الصبري

1) Which statement accurately characterizes the evolution of threats to network security?
   1) + Internal threats can cause even greater damage than external threats.
   2) - Threats have become less sophisticated while the technical knowledge needed by an attacker has grown.
   3) - Early Internet users often engaged in activities that would harm other users.
   4) - Internet architects planned for network security from the beginning.
2) What causes a buffer overflow?
   1) - launching a security countermeasure to mitigate a Trojan horse
   2) - sending repeated connections such as Telnet to a particular device, thus denying other data sources.
   3) - downloading and installing too many software updates at one time
   4) + attempting to write more data to a memory location than that location can hold*
3) Which network security solutions can be used to mitigate DoS attacks?
   1) - virus scanning
   2) + intrusion protection systems
   3) - applying user authentication
   4) - data encryption
4) What is the role of an IPS?
   1) - connecting global threat information to Cisco network security devices
   2) - authenticating and validating traffic
   3) + detecting and blocking of attacks in real time
   4) - filtering of nefarious websites
5) Which characteristic apply to role-based CLI access superviews?
   1) + A specific superview cannot have commands added to it directly.
   2) - CLI views have passwords, but superviews do not have passwords.
   3) - A single superview can be shared among multiple CLI views.
   4) - Deleting a superview deletes all associated CLI views.
6) What is the default privilege level of user accounts created on Cisco routers?
   1) - 0
   2) - 15
   3) + 1
   4) - 16
7) What is a reason to enable OSPF routing protocol authentication on a network?
   1) - to provide data security through encryption
   2) - to ensure faster network convergence
   3) - to ensure more efficient routing
   4) + to prevent data traffic from being redirected and then discarded
8) What is the Control Plane Policing (CoPP) feature designed to accomplish?
   1) - disable control plane services to reduce overall traffic
   2) + prevent unnecessary traffic from overwhelming the route processor
   3) - direct all excess traffic away from the route process
   4) - manage services provided by the control plane
9) What is the purpose of using the ip ospf message-digest-key key md5 password command and the area area-id authentication message-digest command on a router?
   1) + to configure OSPF MD5 authentication globally on the router
   2) - to enable OSPF MD5 authentication on a per-interface basis

3) - to facilitate the establishment of neighbor adjacencies
4) - to encrypt OSPF routing updates

10) A user complains about not being able to gain access to a network device configured with AAA. How would the network administrator determine if login access for the user account is disabled?
1) + Use the show aaa local user lockout command.
2) - Use the show running-configuration command.
3) - Use the show aaa sessions command.
4) - Use the show aaa user command.

11) What is a characteristic of TACACS+?
1) - TACACS+ uses UDP port 1645 or 1812 for authentication, and UDP port 1646 or 1813 for accounting.
2) - TACACS+ is backward compatible with TACACS and XTACACS.
3) - TACACS+ is an open IETF standard.
4) + TACACS+ provides authorization of router commands on a per-user or per-group basis.

12) A user complains about being locked out of a device after too many unsuccessful AAA login attempts. What could be used by the network administrator to provide a secure authentication access method without locking a user out of a device?
1) + Use the login delay command for authentication attempts.
2) - Use the login local command for authenticating user access.
3) - Use the aaa local authentication attempts max-fail global configuration mode command with a higher number of acceptable failures.
4) - None of the mentioned

13) Which server-based authentication protocol would be best for an organization that wants to apply authorization policies on a per-group basis?
1) - SSH
2) - RADIUS
3) - ACS
4) + TACACS+

14) Which authentication method stores usernames and passwords in the router and is ideal for small networks?
1) + local AAA
2) - server-based AAA
3) - server-based AAA over TACACS+
4) - local AAA over TACACS+

15) What information must an IPS track in order to detect attacks matching a composite signature?
1) - the total number of packets in the attack
2) - the attacking period used by the attacker
3) - the network bandwidth consumed by all packets
4) + the state of packets related to the attack

16) What is disadvantage of using an IDS?
1) - The IDS analyzes actual forwarded packets.
2) + The IDS does not stop malicious traffic.
3) - The IDS has no impact on traffic.
4) - The IDS works offline using copies of network traffic.

17) What is the shared characteristic of the IDS and the IPS?
1) + Both use signatures to detect malicious traffic.
2) - Both analyze copies of network traffic.
3) - Both have minimal impact on network performance.
4) - Both rely on an additional network device to respond to malicious traffic.

18) What component of Cisco NAC is responsible for performing deep inspection of device security profiles?

1) - Cisco NAC Profiler
2) + Cisco NAC Agent
3) - Cisco NAC Manager
4) - Cisco NAC Server

19) What protocol should be disabled to help mitigate VLAN hopping attacks?
1) - STP
2) - ARP
3) - CDP
4) + DTP

20) What security countermeasure is effective for preventing CAM table overflow attacks?
1) - DHCP snooping
2) - Dynamic ARP Inspection
3) - IP source guard
4) + port security

21) In what situation would a network administrator most likely implement root guard?
1) - on all switch ports (used or unused)
2) - on all switch ports that connect to host devices
3) - on all switch ports that connect to another switch
4) + on all switch ports that connect to another switch that is not the root bridge

22) Which the function is provided by Network Admission Control?
1) - protecting a switch from MAC address table overflow attacks
2) + ensuring that only authenticated hosts can access the network
3) - stopping excessive broadcasts from disrupting network traffic
4) - limiting the number of MAC addresses that can be learned on a single switch port

23) Which spanning-tree enhancement prevents the spanning-tree topology from changing by blocking a port that receives a superior BPDU?
1) - BDPU filter
2) - PortFast
3) - BPDU guard
4) + root guard

24) What additional security measure must be enabled along with IP Source Guard to protect against address spoofing?
1) - port security
2) - BPDU Guard
3) - root guard
4) + DHCP Snooping

25) Which mitigation technique would prevent rogue servers from providing false IP configuration parameters to clients?
1) + turning on DHCP snooping
2) - implementing port security
3) - implementing port-security on edge ports
4) - disabling CDP on edge ports

26) What security benefit is gained from enabling BPDU guard on PortFast enabled interfaces?
1) - enforcing the placement of root bridges
2) - preventing buffer overflow attacks
3) + preventing rogue switches from being added to the network*
4) - protecting against Layer 2 loops

27) What is one benefit of using a stateful firewall instead of a proxy server?
1) - ability to perform user authentication

2) + better performance
3) - ability to perform packet filtering
4) - prevention of Layer 7 attacks

28) An attacker is using a laptop as a rogue access point to capture all network traffic from a targeted user. Which type of attack is this?
1) - trust exploitation
2) - buffer overflow
3) + man in the middle
4) - port redirection

29) If your system sends its MAC address information without being asked for it - this is what type of ARP?
1) + Gratuitous
2) - Active
3) - Blind
4) - Proxy

30) What functional area of the Cisco Network Foundation Protection framework is responsible for device-generated packets required for network operation, such as ARP message exchanges and routing advertisements?
1) - data plane
2) - forwarding plane
3) - management plane
4) + None of the mentione

31) The single-connection keyword prevents the configuration of multiple TACACS+ servers on a AAA-enabled router.
1) + TRUE.
2) - FALSE.

32) The RADIUS protocol hides passwords during transmission but the rest of the packet is sent in plaintext.
1) + TRUE.
2) - FALSE.

33) Port security works with dynamically or statically configured trunks or access ports
1) - TRUE.
2) + FALSE.

34) The command do use to actually turn on the port security feature is switchport port-security
1) + TRUE.
2) - FALSE.

35) Rogue DHCP servers can be used to create MITM attacks.
1) + TRUE.
2) - FALSE.

36) The default state for a port in the DHCP Snooping environment is untrusted
1) + TRUE.
2) - FALSE.

37) A nontrusted port is one where no DAI needs to take place.
1) - TRUE.
2) + FALSE.

38) A firewall is a device that can separate the network.
1) + TRUE.
2) - FALSE.

39) The switchport nonegotiate disables the negotiation of trunking
1) + TRUE.
2) - FALSE.

40) Data plane - Responsible for routing data correctly
1) - TRUE.
2) + FALSE.