PKI

1. Assymetric key vs symetric key
2. how https work
3. what is hashing and encryption
4. private ip vs public ip
5. what is digital certificates and purpose of D.C
6. What is Root CA
7. CRL , Who mantaine CRL -> CA
8. Which encryption algorithm is secure -> AES
9. how many keys used by AES -> 3 -> 128,132,256
10. while storing password what is used -> salt
11. what is salt -> random value
12. why & where salt is used
13. Brute force attack & Dictionary attack
14. which hashing algo is secure
15. which attack done on hashing algorithm
16. what was the vulnerability
17. what is collision
18. extension of public key -> .cer , .pub
19. extension of private key -> .pem, .pfx
20. extension of putty -> .ppk
21. ssh-keygen
22. how ssh work
23. what known host contain & what authorized key contain in ssh
24. how authentication is provided by assymetric key

Security Concept

1. what is ethical hacking
2. what is VAPT
3. what is black box, White box , grey box in VAPT
4. what is a vulnerability
5. exploit -> method or code to gain use of vulnerability
6. payload -> program is perform something
7. steps of VAPT 8. active and passive recconations 9. port scannin tool - nmap, nessus 10. nmap -> open port (services running) 11. banner grabbing -> identify the os, versions etc 12. if nmap is not available telnet(which & what type of service) use
8. DOS attack -> make service unavailable
9. how ping is used in DOS attack
10. how ping is caused in DOS attack
11. ping flood & ping of death (increase the buffer site)
12. smurf attack
13. except dos attack -> Slowloris attack
14. DOS vs DDOS attack
15. how to prevent DOS attack -> 1. block ICMP echo request & echo reply 2.

16. Man in the Middle attack (MITM) attack
17. how arp poisoning works?
18. which tool is used for MITM
19. session hijecking
20. ransomware
21. Trojan
22. Rootkit
23. What is OWASP
24. SQL injection
25. Cross site scripting (XSS)
26. types of XSS (reflected, dom based, stored)
27. if our website is allowed to upload a file, can attacker make use of file? -> yes -> HOW?
28. How to prevent web application -> web application firewall
29. For Apache (Mode_security module)
30. security related library for security related company
31. Pythons - basic questions
32. CF - basic questions
33. what is Cyber forensics and why it done
34. what is chain of custody
35. Digital forensics
36. what are common tools and used
37. get windows registry info - reg ripper tool used
38. image formats -> dd, e01

NDC

1. What is firewall
2. What is Demiliterized zone (dmz) & why we use
3. what is Packet filter Firewall
4. What is Proxy & Proxy firewall
5. Squid & its Rules & Port number (TCP 3128)
    - squid is caching server.
6. IDS & IPS
7. why IDS is required while using firewall
8. Types of IDS (2 types)
9. how to bypass IDS -> (send encrypted traffic)
10. What is promicious Mode
11. Port mirroring
12. Snort Rule Formate
13. what is sid in snort--> Snort id , snort rule number
14. What is VPN & why use VPN & Protocols of VPN
15. IPSec Mode -> Transport mode & Tunnle mode
16. AH & ESP Protocol number (51 & 50 respectively)
17. AH vs ESP
18. why monitoring is important
19. what is nagios
20. what is required to implement monitoring in client side (NCPA)

21. what is exit status 0=green, 1=yellow, 2=red in nagios
22. $?

- if 0 = SUCCESS
- else ERROR

23. how to secure router , firewall, Switch
24. antivirus hai fir bhi virus aa jaye to kya karoge?
25. if firewall hai fir bhi infect ho jaye to kya karoge? how to isolate it (PORT change in VLAN)

Windows Admin

(most of questions from Active Directory)

1. what is forest, Domain tree, Domain
2. AD is based on which protocol & Port number
3. authentication protocol used? (kerberose)
4. what is TGS? Which server is TGS (our domain controller)
5. what is TGT
6. What is a service ticket
7. what is Group Policy
8. how many default group policy --> 2? and which are they?
9. What is Forest Fuctional level & Domain Fuctional level
10. if Domain Controller fail, How to recover it?
11. how to backup Active Directory --> system state backup
12. What is Authoritative backup &
13. What is non-Authoritative backup? --> used only for faild domain contoller

- client or server ke bich me 5 min ka time difference allowed

DevOps

1. what is diff b/w container and Virtual machine
2. what is CI/Cd
3. What is DevOps
4. What is Version Control systemm
5. What is Git ?
6. What is branch? why branches are used?
7. Docker commands
8. What is Kubernetes
9. What is Deployement , service
10. Cluster IP
11. Node port, load balancer
12. Cloud - SaaS, PaaS.....

FCN

1. IPv4 , IPv6
2. Private IP in IPv4

3. Link local, site local in IPv6
4. what eui64 in ipv6
5. what is software defined network (SDN)?
6. what is mininet

FCN mandarsir

1. IPv4 vs IPv6 (subnetting, boradcast is eliminated in ipv6, dont require DHCP,ARP)(127 series is wasted in ipv4,::1 LOOPBACK IN IPv6)
2. what is STP & use (Avoid switching loops) & how it works
3. BPDU
4. OSI Layer(devices, protocol)
5. MAC other 3 names --> Physical Address, Hardware Address, Burnt in address
6. Distance Vector Routing protocol vs Link state *****
7. what is configuration register values & use --> it is use to bypass start up configuration (Define the Booting up Sequence)
8. which command will display me IOS file name -> show flash, show version
9. which command will display me config register value - > show version
10. which functionality use router as firewall (ACL)
11. what is VTP -> it carries the VLAN database to one switch to next switch, so that we dont know to configure VLAN again on next switch, we just add the port to carrie vlan database
12. Private IP in IPv4 ->
13. APIPA series -> 169.254. x.x
14. 3 functionality of transport layer --> Flow Contorl, End-to-End Delivery Sequencing and Error correction,reliability
15. basic function's of router

- A Router is a networking device that forwards data packets between computer networks. One or more packet-switched networks or subnetworks can be connected using a router. By sending data packets to their intended IP addresses, it manages traffic between different networks and permits several devices to share an Internet connection.

16. why require router?

- A router helps you connect multiple devices to the Internet, and connect the devices to each other. Also, you can use routers to create local networks of devices. These local networks are useful if you want to share files among devices or allow employees to share software tools.
- restrict the broadcast

- connecting two different technology (LAN,WAN)
- address learning is also reduce

17. Drawback of switches

- Looping
- Broadcasting
- its learns all the addresses of all the devices is called - Flat address architecture

18. how router select the routes (Page 70 (3 criteria))

- Longest Match
- A.D (Administrative Distance) - low
- Metric - Hope count -- https://networkers-online.com/p/how-routers-select-best-routes#google_vignette

19. which entity require to backup of my driver(Router) (TFTP)
20. what CDP & Update timer of CDP (30 sec)

- cisco discovery protocol (that is used for collecting directly connected neighbor device information like hardware, software, device name details and many more.)

21. advantages of EIGRP over the OSPF(page 66)
22. VLANs & 2 methods

- single VLAN - Access port
- Multi VLAN - Trunk Port (speciality: every port is going to learn mac port, its add the vlan tag-so next switch identify vlan tag) Trunking methods - 1. ISL (inter switch link) 2. 802.1q

23. Switching

- switch is perform flood
    - Destination mac is unknown
    - broadcast mac address
- https://www.cisco.com/c/en/us/products/switches/what-is-network-switching.html#~types

24. tags of Trunks
25. what is 100 base tx (100=100 mbps, base=baseband technology,tx=twisted pair)
26. 3 Types of NAT

- static
- dynamic
- overloading (port address Translation (PAT))

27. which command is decide inside and outside

- ip nat inside
- ip nat outside

28. inside local , inside global, outside local & Global
29. complete syntax of static route

- Router(config)#ip route [destination_network][subnet_mask][next-hop_address or exitinterface] AD Permanant

30. in line conf prompt password configure but login not done what happen, what will be effect

- anyone going to telnating is given to access b/c logiing is not enabled
- it want work
- effect : teleneting not work

31. in line conf prompt login configure but password not done what happen, what will be effect

- no one able to login

32.1 hold out timer of RIP (180 sec) 32. hold out timer of EIGRP, hold in timer of EIGRP 33. update timer of EIGRP (60-5) 34. hello timer of OSPF (10-30) 35. what is election criteria of DR and BDR (OSPF topic) --> BMA(Broadcast multi access) network scenario - DR - Priority(0-255) (Default priority=1) , Highest RID

36. which process is selected for RID(router id)--> highest if lo0 or highest of an interface
37. command to see link state database command in OSPF

- show ip ospf database

38. command to see link state database command in EIGRP

- show ip eigrp topology

39. Standard ACL number = 1-99,extended ACL number=100-199
40. command access list applied on interface = show ip interface
41. command applied to ACL on vty 0 4 - access-class access-number in
42. three golder rules of access list (page 85)
43. NATing syntax

- ip nat inside source list listnumber pull pullname overrole

44. whether inside ip address or outside ip address are defined within in the ACL (outside - pull)(inside - ACL)
45. 3 diff types of modes in VTP

- Server
- client
- Transparent

46. requirement of communication across VLANs (router,Router on a stick(inter-vlan communication))
47. advantage of PPP over HDLC

- https://www.geeksforgeeks.org/difference-between-high-level-data-link-control-hdlc-and-point-to-point-protocol-ppp/

48. what is rule of username password configure in PPP

- username is hostname of remote router and password is same

49. what is the use of network command******

    - routing updates (enable) is start forwarding that
    - subnets included in routing updates

50. what is use of passive interface

- Passive interfaces allow you to include an IP subnet in the routing protocol without sending updates out of the interface.

52. what is diff RIPv1 vs RIPv2

- Page 64