Possible Technical Interview Questions v1.0

HackerU

Created by ajay

1) Microsoft

a) Easy

i) What is an ISO file or ISO Image?
   (1) An **ISO image** is a disk image of an optical disc. In other words, it is an archive file that contains everything that would be written to an optical disc, sector by sector, including the optical disc file system.[1] ISO image files bear the *.iso* filename extension.
   (2) The name *ISO* is taken from the International Organization for Standardization (ISO)

ii) What does the Windows Device Manager do?
   (1) It provides a view of the hardware components connected to the computer.

iii) What does the Windows Event Viewer do?
   (1) It is an administrative tool that displays logs and system messages regarding events that occurred in the system.

iv) What is the command or program one needs to run to open a command prompt in Windows?
   (1) cmd.exe

v) What is the command in the Command prompt to display a directory?
   (1) Dir

vi) What does GUI stand for?
   (1) Graphical User Interface

vii) What is the name of the native Windows Antivirus & Anti-Malware?
   (1) Windows Defender (Windows 7) or Windows Security (Windows 10)

viii) What is the command in the Command prompt to create a directory?
   (1) Mkdir

ix) What is the command in the Command prompt to create a directory?
   (1) rmdir

x) List 2 or more physical mediums can ISO files be used to install windows Servers
   (1) CDs
   (2) DVDs
   (3) USB Flash Drives
   (4) External Hard Drives
   (5) Over the Network – Imaging – Ghosting

xi) What does OU stand for in Microsoft Windows Server?
    (1) Organizational Unit
xii) What is Microsoft PowerShell?
    (1) It is a Microsoft CLI used for automation, configuration, management and scripting.
    (2) It provides full access to the system, including Active Directory
    (3)

b) Medium

i) Is Windows Command Prompt DOS?
    (1) No, DOS or MS-DOS is a Command line operating system which is different from the Command Prompt in windows, EVEN if some of the commands are the same.
    (2) **Command Prompt** is a **Windows** program that emulates many of the **command line** abilities available in MS-**DOS** but it is not actually MS-**DOS**. **Command Prompt** is a GUI version of **command**.com in MS-**DOS**. ... In reality, **cmd**.exe is a **Windows** program that acts as a **DOS**-like **command line** interpreter.
ii) What protocol does Windows use to natively allow remote access into window via the GUI?
    (1) RDP – Remote Desktop Protocol
        (a) What is the default port that RDP operates on?
            (i) 3389
iii) What does UAC stand for in Windows?
    (1) User Access Control
iv) What does UAC do in Windows?
    (1) Limits application execution for users for basic privileges
v) What is the difference between a 32 and a 64 bit system?
    (1) 32 bit and 64 bit refer to the processor memory limit
vi) What is the difference of the user experience upgrading from a 32 bit processor to a 64 bit processor?
    (1) Faster
    (2) Better experience
vii) List 2 Roles that a Windows Server might provide. (Bonus for more)
    (1) Active Directory Domain Services
        (a) Group Policy Objects
    (2) Domain Name System
    (3) Dynamic Host Configuration Protocol
    (4) File Server
    (5) Print Server

(6) Replication Server
(7) Backup Server

viii) What is so important about the Windows Server Administrative password?
(1) It is the local administrative account on the server, having the highest privileges and the target of hackers.
(2) If hackers obtain this password they can do whatever they want to this individual system.

ix) What is Oracle Virtualbox's 'Guest Additions'?
(1) It is software that you install into a VM that provides extra features:
(a) Automatic Resizing
(b) Bidirectional Keyboard
(c) Drag and Drop
(d) Enhanced performance

x) What is Active Directory Domain Services?
(a) It is a database system that provides authentication, directory services, policy and other services in a Windows environment.

xi) What does LDAP stand for?
(a) Lightweight Directory Access Protocol

xii) What does LDAP do?
(a) It is a lightweight client-server protocol for accessing directory servers.

xiii) What does SMB stand for?
(1) Server Message Block

c) Hard

i) Name 2 Microsoft Windows Defender or Windows Security Features
(1) Exploit Guard
(2) Application Guard
(3) Advanced Threat Protection
(4) Real-Time Protection
(5) Cloud-Delivered Protection

ii) What is the main difference between Microsoft Workgroups and Domains?
(1) How resources are managed

iii) Would a large enterprise use a workgroup(s) or domains?
(1) Domains

iv) Why would a large enterprise use domains?
(1) Centralized management

v) What is a child domain?
(1) It is a separate domain created under the root domain tree.

d) What is Windows Server CORE?
   i) The Server Core option is a minimal installation option that is available when you are deploying the Standard or Datacenter edition of Windows Server. Server Core includes most but not all server roles. Server Core has a smaller disk footprint, and therefore a smaller attack surface due to a smaller code base.
e) What do OU's in Microsoft Active Directory do?
   i) An **organizational unit** (OU) provides a way of classifying objects located in directories, or names in a digital certificate hierarchy, typically used either to differentiate between objects with the same name (John Doe in OU "marketing" versus John Doe in OU "customer service"), or to parcel out authority to create and manage objects (for example: to give rights for user-creation to local technicians instead of having to manage all accounts from a single central group).
f) Does Windows Server have NFS support?
   i) Yes

2) Networks

a) Easy

i) What does LAN stand for?
   (1) Local Area Network
ii) What does WAN stand for?
   (1) Wide Area Network
iii) What does WLAN stand for?
   (1) Wireless LAN
iv) What does WWAN stand for?
   (1) Wireless WAN
v) What does Wi-Fi stand for?
   (1) Wireless Fidelity
vi) What does IP, in IP address stand for?
   (1) Internet Protocol
vii) What does DNS stand for?
   (1) Domain Name System
viii) What does DNS do?
   (1) It is a services that provides name to number (Ip addresses) mapping.
   (2) Name to IP
   (3) IP to name
ix) What is DNSSEC?

(1) A DNS extension that provides defenses against common attacks such as MITM and DNS tunneling

x) Can DNS Integrate with Active Directory?
(1) Yes

xi) What does DHCP Stand for?
(1) Dynamic Host Configuration Protocol

xii) What is the 4-letter acronym that accompany the DHCP Process?
(1) D
(2) O
(3) R
(4) A

xiii) PING and TRACEROUTE commands use what protocol?
(1) ICMP

xiv) What has replaced telnet as a secure method of accessing a shell?
(1) SSH or Secure Shell

xv) What port by default is used for SSH?
(1) 22

xvi) What port by default is used for telnet?
(1) 23

xvii) What port by default is used for RDP?
(1) 3389

xviii) What port by default is used for NTP?
(1) 1234

xix) What port by default is used for Post office protocol?
(1) 110

xx) What port by default is used for SMTP?
(1) 25

xxi) What port by default is used for IMAP?
(1)

xxii) What port by default is used for DNS?
(1) 53

xxiii) What port by default is used for HTTP?
(1) 80

xxiv) What port by default is used for HTTPS?
(1) 443

xxv) What does TCP stand for?
(1) Transmission Control Protocol

xxvi) What does UDP stand for?
(1) User Datagram Protocol

xxvii) How many ports do each network interface have? Whether Physical or virtual?
(1) 65535

b) Explain the Physical Layer:
   i) Responsible for transmission of digital data from sender to receiver through the communication media.
c) What type of information travels in the Physical Layer?
   i) Zeros and Ones
d) Explain the Data Link Layer:
   i) Handles the movement of data to and from the physical link. It is also responsible for encoding and decoding of data bits.
e) Explain the Network Layer:
   i) Responsible for packet forwarding and providing routing paths for network communication.
f) Explain the Transport Layer:
   i) Responsible for end-to-end communication over the network. It splits the data from the above layer and passes it to the Network Layer and then ensures that all the data has successfully reached at the receiver's end.
g) Explain the Session Layer:
   i) Controls connection between the sender and the receiver. It is responsible for starting, ending, and managing the session and establishing, maintaining and synchronizing interaction between the sender and the receiver.
h) Explain the Presentation Layer:
   i) It deals with presenting the data in a proper format and data structure instead of sending raw datagrams or packets.
i) Explain the Application Layer:
   (1) It provides an interface between the application and the network. It focuses on process-to-process communication and provides a communication interface.
j) What is Layer 8 of the OSI model? (Industry Inside joke)
   i) Political Layer.
   ii) This is a inside joke from the biz, where problems exist in layer 8 due to humans and politics
   iii) Layer 8 is usually considered the "office politics" layer. In most organizations, there is at least one group who is favored, at least temporarily, by management and receives "special" treatment. When it comes to networking, this may mean that this group always has the latest and/or fastest equipment and highest speed network links.
k) What is Layer 9 of the OSI model? (Industry Inside Joke)
   i) Budget Layer
   ii) Layer 9 is generally referred to as the "blinders" layer or the "BUDGET" layer. This layer applies to organizational managers who have already decided, usually with little or no current information, to dictate a previously successful network plan.
l) What is Layer 10 of the OSI model? (Industry Inside Joke)
   i) User Error Layer
   ii) Layer 10, the "user" layer, is in every organization. But users are much more than a layer. While they are one of the reasons the network exists, users can also be a big part of the need for troubleshooting. This is especially true when the users have computers at home and have

decided to “help” the network administrator or manager by making changes to the network without consulting the network staff.

iii) Equally challenging is the user who “didn’t do anything” when the network segment in his/her immediate vicinity suddenly stopped working. In these cases, the layer 10 identification coincides with layer 10 troubles (and the “ID10T” label some technicians have used).

m) What is the NTP Protocol?
   i) Network Time Protocol

n) Name 1 or 2 NTP Servers off the top of your head? (doesn’t matter, as long as they know of one)
   i) time.apple.com
   ii) pool.ntp.org
   iii) time.google.com
   iv) time.nist.gov
   v) time.clourflare.com

o) Medium

i) Recite the OSI Model?
   (1) Application Layer – Layer 7
   (2) Presentation Layer – Layer 6
   (3) Session Layer – Layer 5
   (4) Transport Layer – Layer 4
   (5) Network Layer – Layer 3
   (6) Data Link Layer – Layer 2
   (7) Physical Layer – Layer 1

ii) What does ARP stand for?
   (1) Address Resolution Protocol

   (2) What does ARP do?
      (a) **Address Resolution Protocol (ARP)**is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

      (b) When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address.
      (c) The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine.

(d) If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it.

iii) TCP and UDP operate at work Layer of the OSI model?
   (1) Layer 4 – Transport Layer
iv) When opening a browser and requesting a web page, are you using the HTML or the HTTP protocol?
   (1) HTTP
   (2) Hyper Text TRANSFER Protocol
v) Is FTP a secure protocol?
   (1) No
vi) Describe the TCP 3-way handshake as quick and dirty as possible?
   (1) SYN
   (2) SYN-ACK
   (3) ACK
vii) What is the range of privileged or low ports?
   (1) 0-1023
viii) What is the range of registered ports?
   (1) 1024-49151
ix) What is the range of Dynamic or High Ports?
   (1) 49152-65535
x) What is the difference between TCP and UDP?
   (1) TCP is a stateful protocol, UDP is not
   (2) UDP is fire and forget
   (3) UDP is best effort
xi) Explain the Client-Server model?
   (1) The Client-Server model is a distributed application structure that manages tasks and workloads by sharing them among providers of resources and services (Servers) and delivers responses to service requesters. (Clients)
xii) Name 2 DNS Record Types
   (1) Host Record
   (2) MX Record
   (3) A Record
   (4) SRV Record
   (5) CNAME Record
   (6) PTR Record
   (7) NS Record
xiii) When discussing DNS, what does SOA mean?
   (1) Start of Authority
xiv) What does LLMNR Protocol stand for?

(1) Link-Local Multicast Name Resolution

xv) What does APIPA stand for?

(1) Automatic Private IP addressing

xvi) What is a DHCP Lease?

(1) A **DHCP lease** is a temporary assignment of an IP address to a device on the network. When using **DHCP** to manage a pool of IP addresses, each client served on the network is only "renting" its IP address. Thus, IP addresses managed by a **DHCP** server are only assigned for a limited period of time.

xvii) What port by default is used for FTP? (Trick question)

(1) There are 2 ports

(a) 20

(b) 21

xviii) How many layers are there in the TCP/IP Model?

(1) 4

xix) What is a PCAP file?

(1) Packet Capture

p) What is Traceroute?

(1) **Traceroute** is a tool that shows the path of a packet. It lists all the points (mainly routers) that the packet passes through. This is used mostly when the packet is not reaching its destination. Traceroute is used to check where the connection stops or breaks to identify the point of failure.

q) What does OSPF Stand for?

i) Open Shortest Path First

r) What routing algorithm does OSPF use?

i) Shortest path First

s) What does IGP stand for?

i) Interior Gateway Protocols

t) What does EGP stand for?

i) Exterior Gateway Protocols

u) BGP stands for?

i) Border Gateway Protocol

v) Hard

i) What is a DNS Forward Lookup Zone?

(1) It maps names or aliases to IP addresses

(2) It can automatically be created when promoting a server to a domain controller

ii) What is a DNS Reverse Lookup Zone?

(1) It maps IP addresses to names and aliases

(2) Contains PTR Records

iii) Does a Secondary DNS Zone have read and write permissions?

(1) No

iv) What does SOA, in DNS do?

(1) A Start of Authority (**SOA**) resource record indicates which Domain Name Server (**DNS**) is the best source of information for the specified domain. Every domain must have an **SOA** record.

v) What file does Wireshark save its packet captures?

(1) .pcap

vi) What does LLMNR Protocol do?

(1) The Link-Local Multicast Name Resolution (**LLMNR**) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link.

vii) What is the 4 step DHCP Process?

(1) DORA

(a) Client Broadcasts the **DHCP Discovery Message**

(b) DHCP replies with a **DHCP Offer**

(c) The client broadcasts a **DHCP REQUEST**

viii) The server broadcasts a **DHCP ACK** message acknowledgement

ix) What does Software Defined Networking mean?

(1) **Software-defined networking** (**SDN**) technology is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring, making it more like cloud computing than traditional network management.

x) What is BGP?

(1) **Border Gateway Protocol or BGP** is the routing protocol of the internet that is classified as a distance path vector protocol. BGP was **designed to replace EGP** with a decentralized approach to routing.

xi) What routing algorithm does BGP use?

(1) Best Path Selection Algorithm

xii) Situational question –

(1) If you are working on a server, which is expected to be receiving some data, but it isn't, how can you prove at the network level that the server isn't getting the data, even though a server admin is telling you that they are sending it?

(a) Valid answers

(i) Packet Capture

(ii) Wireshark

(iii) TCPDUMP

(2) Follow up question

(a) What file type would you send to the network administrators to show without a doubt you are not receiving the packet?

(i) Packet Capture

(ii) .pcap

3) Cloud

a) Easy

i) What are the 3 Cloud Deployment Models
   (1) Public Cloud
   (2) Private Cloud
   (3) Hybrid Cloud

ii) What does Public Cloud mean?

iii) The public cloud refers to the cloud computing model with which the IT services are delivered across the Internet. The service may be free, freemium, or subscription-based, charged based on the computing resources consumed. The computing functionality may range from common services such as email, apps and storage to the enterprise-grade OS platform or infrastructure environments used for software development and testing.

iv) What does Private Cloud mean?
   (1) The private cloud refers to the cloud solution dedicated for use by a single organization. The data center resources may be located on-premise or operated by a third-party vendor off-site. The computing resources are isolated and delivered via a secure private network, and not shared with other customers.
   (2) Private cloud is customizable to meet the unique business and security needs of the organization. With greater visibility and control into the infrastructure, organizations can operate compliance-sensitive IT workloads without compromising on the security and performance previously only achieved with dedicated on-premise data centers.

v) What does Hybrid Cloud mean?
   (1) The hybrid cloud refers to the cloud infrastructure environment that is a mix of public and private cloud solutions. The resources are typically orchestrated as an integrated infrastructure environment. Apps and data workloads can share the resources between public and private cloud deployment based on organizational business and technical policies around security, performance, scalability, cost and efficiency, among other aspects.

vi) What does SaaS stand for?
   (1) Software as a Service

vii) What does Software as a Service mean?
   (1) Software as a Service, also known as cloud application services, represents the most commonly utilized option for businesses in the cloud market. SaaS utilizes the internet to deliver applications, which are managed by a third-party vendor, to its users. A majority of SaaS applications run directly through your web

browser, which means they do not require any downloads or installations on the client side.

viii) What is SDN stand for?
   (1) Software Defined Networking

b) Medium

i) What is a cloud workload?
   (1) Cloud Workload. The work function (application or service) processed by a remote server or instance at any given time; it generally has users or applications interacting with it through the Internet. Cloud workloads can range from a web server to a database to a container.

ii) What does PaaS stand for?
   (1) Platform as a Service

iii) What does Platform as a Service mean?
   (1) Cloud platform services, also known as **Platform as a Service (PaaS),** provide cloud components to certain software while being used mainly for applications. PaaS delivers a framework for developers that they can build upon and use to create customized applications. All servers, storage, and networking can be managed by the enterprise or a third-party provider while the developers can maintain management of the applications.

iv) What does IaaS stand for?
   (1) Infrastructure as a Service

v) What does Infrastructure as a Service mean?
   (1) Cloud infrastructure services, known as **Infrastructure as a Service (IaaS),** are made of highly scalable and automated compute resources. IaaS is fully self-service for accessing and monitoring computers, networking, storage, and other services. IaaS allows businesses to purchase resources on-demand and as-needed instead of having to buy hardware outright.
   (2)

c) Hard

i) Explain the difference

ii) What does XaaS stand for?
   (1) Everything as a Service

iii) What does Everything as a Service mean?
   (1) One term you're likely seeing more frequently in the world is XaaS, or Everything as a Service. XaaS refers to the highly-individualized, responsive, data-driven

products and offerings that are fully controlled by customers—and the data they provide via everyday IoT-powered sources like cell phones and thermostats. By using that data generated over the cloud, businesses can innovate faster, deepen their customer relationships, and sustain the sale beyond the initial product purchase. XaaS is a critical enabler of the Autonomous Digital Enterprise.

iv) What is a Cloud Availability zone?
   (1) **Availability zones** (AZs) are isolated locations within data center regions from which public **cloud** services originate and operate. Regions are geographic locations in which public **cloud** service providers' data centers reside.

4) Linux

a) Easy

i) What the 3 types of Linux standard streams?
   (1) **STDIN**
   (2) **STOUT**
   (3) **STERR**

ii) Explain STDIN
   (1) **Standard input** is a stream from which a program reads its input data. The program requests data transfers by use of the *read* operation. Not all programs require stream input.

iii) Explain STOUT
   (1) **Standard output** is a stream to which a program writes its output data. The program requests data transfer with the *write* operation. Not all programs generate output.

iv) Explain STERR
   (1) **Standard error** is another output stream typically used by programs to output error messages or diagnostics. It is a stream independent of standard output and can be redirected separately.

v) Give some examples of hardware that work with STDIN in Linux?
   (1) Mouse
   (2) Keyboard

vi) Give some examples of hardware that work with STOUT in Linux?
   (1) Computer Screen – Monitor
   (2) Printer
   (3) Speakers

vii) What does BASH stand for?
   (1) Bourne again Shell

viii) In Linux, the computer prompt says secret@secretserver:/~$, What user are you logged in with?
   (1) Secret

ix) In Linux, the computer prompt says secret@secretserver:/~$, What folder are you currently in?
   (1) Home folder for the logged in user.
x) In Linux, the computer prompt says secret@secretserver:/~$, What computer are you logged in to?
   (1) secretserver
xi) In Linux, the computer prompt says secret@secretserver:/~$, What type of user are you logged in as, a regular user or a superuser?
   (1) Regular User
xii) What is the cli command the returns your username that you are logged in with?
   (1) whoami
xiii) What is the cli command that returns the absolute path of the folder you are in?
   (1) Pwd
xiv) What is the cli command that returns the name of the computer you are logged into?
   (1) Hostname
xv) What is the cli command that shows the disk utilization and capacity of the file system?
   (1) df
xvi) What is the cli command to change folders?
   (1) cd
xvii) What does the cli command cd mean?
   (1) Change directory
xviii) What button in the linux cli auto-completes the command or filename?
   (1) TAB
xix) When using the cp command in the Linux CLI, the first argument is the file you want to copy or want to copy to?
   (1) It is the file you want to copy
xx) When using the Linux CLI, what is the command to rename a file?
   (1) Mv
xxi) What does the program vim stand for?
   (1) Vi Improved
xxii) What is vi or vim?
   (1) A terminal based text editor
xxiii) What does the SCP command stand for?
   (1) Secure Copy
xxiv) What does the head command perform in the Linux cli?
   (1) It displays the top 10 lines of a file
xxv) What does the tail command perform in the Linux cli?
   (1) It displays the last 10 lines of a file
xxvi) How is the /etc folder typically pronounced?
   (1) ETSY (ET-SEE)

xxvii) What will the following command do? chmod 777 silly.txt
(1) Make the file readable, writeable and executable by everybody

b) Medium

i) In Linux, the computer prompt says secret@secretserver:/~$, can this user use the sudo command? (Trick Question)
(1) There isn't enough information here to determine that.
(2) FOLLOW UP QUESTION
(a) Which group would you check to see if this user can use the sudo command?
(i) SUDOERS

ii) What option would I add to the df command to show the results in human readable format?
(1) -h
(2) Ex. df -h

iii) What option would I add to the ls command to show the results including hidden files?
(1) q-a

iv) When using the Linux CLI, if I wanted to change the filename from happy.txt to sad.txt what would that command be?
(1) mv happy.txt sad.txt

v) How would you copy a file securely from windows to a Linux computer via the command line?
(1) SecureCopy
(2) SCP Command
(3) WinSCP

vi) What would the command ps do?
(1) Linux provides us a utility called ps for viewing information related with the processes on a system which stands as abbreviation for "Process Status". ps command is used to list the currently running processes and their PIDs along with some other information depends on different options.
(2) It would only show you processes associated with the terminal your in or the shell that you are in.

vii) What command would you use in the linux cli to stop a process?
(1) Kill

viii) What is the redirector character used in the Linux CLI to save the standard output to a file?
(1) >

ix) What is the redirector character used in the Linux CLI to append the standard output to a file?

(1) >>

x) What would the tail -f command do?

(1) It shows the last 10 lines of a file, but also continues displaying the file so as new data enters the file it is displayed live on the screen.

xi) What keyboard command exits a file being viewed by the less command?

(1) Q

xii) What would the

xiii) What folder and file are passwords saved in Linux?

(1) /etc/shadow

xiv) What folder and file are the users that can use the sudo command located?

(1) /etc/sudoers

xv) What will the following command do? chmod 755 silly.txt

(1) Sets Read, Write, and Executable for your user

(2) Sets Readable and executable to everyone else

xvi) What will the following command do? chmod +x silly.txt

(1) Makes the file executable by everyone

xvii) Where are logs typically located in Linux?

(1) /var/log

c) Hard

i) What does GREP stand for?

(1) Globally search for a regular expression and print matching

ii) What would ps -a do?

(1) Lift the BSD-style "only yourself" restriction on selecting processes and displays it to the screen

iii) What would ps -A do?

(1) Selects and displays all processes

iv) What is the difference between ps -e and ps -a? (Trick Question) <Very hard>

(1) There isn't

v) What would the command ps -a | grep nexpose > output.txt do?

(1) It should list all processes, pipe the output to the next command which would filter for the word Nexpose and then redirect the output to a file called output.txt

(2) FOLLLOW UP

(a) Would there be any feedback on the screen that it worked successfully?

(i) Nope

vi) What would the tail -f -n 6 do?

(1) It shows the last 6 lines of a file, but also continues displaying the file so as new data enters the file it is displayed live on the screen.

vii) What is the difference of the more and less commands?

(1) The main **difference between more and less** is that **less command** is faster because it does not load the entire file at once and allows navigation though file using page up/down keys.

viii) What will the following command do? chmod 600 silly.txt
   (1) Sets Read and Write for only your account
   (2) No one can execute the file
   (3) No one else can read or write to the file

ix) What does the command iptables -L do?

5) Network Security

a) Easy

i) In Network Security, what does AAA mean?
   (1) Authentication
   (2) Authorization
   (3) Accounting

ii) What is 802.1x?
   (1) **IEEE 802.1X** is an IEEE Standard for port-based Network Access Control

iii) What are the three parties that make up 802.1x
   (1) Supplicant
   (2) Authenticator
   (3) Authentication server

iv) In Networks what does MAC stand for?
   (1) Media Access Control

v) What is another name for a MAC address?
   (1) Physical address

vi) MAC addresses are comprised of what?
   (1) 12 characters
   (2) Hexadecimal numbering 0-9 and A-F

vii) What does ARP stand for?
   (1) Address Resolution Protocol

viii) What does Network Switch Port Security do?
   (1) Restricts access to a network interface

ix) What does VLAN stand for?
   (1) Virtual LAN

b) What is a Firewall and what role does it play?
   i) A Firewall is a network security system set on the boundaries of the system/network that monitors and controls network traffic. Firewalls are mainly used to protect the system/network from viruses, worms, malware, etc. Firewalls can also be to prevent

remote access and content filtering.

ii)

c) Is 503 HTTP Error code a Client-side or Server-Side Error?
    (1) Server-Side

d) Medium

i) Are you able to identify a manufacturer via a MAC address?
    (1) Yes
ii) Name at least 2 things you can do maliciously poisoning ARP?
    (1) MiTM
    (2) DOS
    (3) Spoofing another computers identity
iii) How does Port Security work?
    (1) It limits the number of MAC addresses that a port will allow
iv) What are the three modes in Port Security?
    (1) Shutdown
    (2) Restrict
    (3) Protect
v) Explain Manual vs Sticky Port Security Configuration?
    (1) Manual
        (a) Manual is the most secure method
        (b) Requires manual configuration
    (2) Sticky
        (a) MAC addresses are learned as you plug them into the port
vi) What is VLAN?
    (1) VLAN. Stands for "Virtual Local Area Network," or "Virtual LAN." A VLAN is a custom network created from one or more existing LANs. It enables groups of devices from multiple networks (both wired and wireless) to be combined into a single logical network.

e) Is a Firewall hardware or software? (Trick Question)
    i) It can be both.
f) What does CDP stand for?
    i) Cisco Discovery Protocol
g) What does CDP do?
    i) It is a CISCO discovery protocol
    ii) It is a CISCO network discovery tool, which assists network administrators and engineers in identifying neighboring Cisco devices, particularly those running lower-layer, transparent protocols.

h) What is LLDP?
   i) Link Layer Discovery protocol
i) What does LLDP do?
   i) The **Link Layer Discovery Protocol** (**LLDP**) is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a local area network based on IEEE 802 technology, principally wired Ethernet.
j) What comprises a Hash?
   i) A hexadecimal set of characters

k) What are the three most currently common Hashing Algorithms in use today? (Use VirusTotal as an example?)
   i) MD5
   ii) Sha1
   iii) Sha256

l) What is the difference between Encoding, Hashing, and Encryption?
   i) The purpose of ***encoding*** is to transform data so that it can be properly (and safely) consumed by a different type of system, e.g. binary data being sent over email, or viewing special characters on a web page. The goal is **not** to keep information secret, but rather to ensure that it's able to be properly consumed.
   ii) ***Hashing*** serves the purpose of ensuring *integrity*, i.e. making it so that if something is changed you can know that it's changed. Technically, hashing takes arbitrary input and produce a fixed-length string.
   iii) ***Hashing*** is also used to create fingerprints for files for signature based antivirus / EDR.
   iv) The purpose of ***encryption*** is to transform data in order to keep it secret from others, e.g. sending someone a secret letter that only they should be able to read, or securely sending a password over the Internet. Rather than focusing on usability, the goal is to ensure the data cannot be consumed by anyone other than the intended recipient(s).
   v) Both ***Encryption*** and ***Hashing*** are used to convert readable data into an unreadable format. The difference is that the encrypted data can be converted back to original data by the process of decryption but the hashed data cannot be converted back to original data.

m) By decrypting Cypher text, we get _____?
   i) "Plaintext"

n) Hard

   i) What does Software Defined Security Mean?

(1) Software-defined security (SDS) is a type of security model in which the information security in a computing environment is implemented, controlled and managed by security software.
(2) It is a software-managed, policy-driven and governed security where most of the security controls such as intrusion detection, network segmentation and access controls are automated and monitored through software.

ii) Why did Cisco make CDP standard and cannot be disabled? (Trick Question)
(1) CDP can be disabled

6) Cybersecurity Infrastructure

a) Easy
b) Medium
c) Hard

7) Python

a) Easy
b) Medium
c) Hard

8) Ethical Hacking

a) Easy
i) What is Penetration Testing?
ii) **Penetration Testing** is the process of finding vulnerabilities on the target. In this case, the organization would have set up all the security measures they could think of and would want to test if there is any other way that their system/network can be hacked.
b) Medium
c) Hard

9) DFIR

a) Easy
b) Medium
c) Hard

10) Game Theory

a) Easy
b) Medium
c) Hard

-
-
-

- What is the 3 foundational pillars of Cybersecurity?
  - Confidentiality
  - Integrity
  - Availability

- What does Confidentiality provide to an organization?
  - The information should be accessible and readable only to authorized personnel. It should not be accessible by unauthorized personnel. The information should be strongly encrypted just in case someone uses hacking to access the data so that even if the data is accessed, it is not readable or understandable.

- What does Integrity provide to an organization?
  - Making sure the data has not been modified by an unauthorized entity. Integrity ensures that data is not corrupted or modified by unauthorized personnel. If an authorized individual/system is trying to modify the data and the modification wasn't successful, then the data should be reversed back and should not be corrupted.

- What does Availability provide to an organization?
  - The data should be available to the user whenever the user requires it. Maintaining of Hardware, upgrading regularly, Data Backups and Recovery, Network Bottlenecks should be taken care of.

- What does HIDS stand for?

- Host IDS

- What does NIDS stand for?
  - Network IDS

- What is the difference between a HIDS and NIDS?
  - HIDS(Host IDS) and NIDS(Network IDS) are both Intrusion Detection System and work for the same purpose i.e., to detect the intrusions. The only difference is that the HIDS is set up on a particular host/device. It monitors the traffic of a particular device and suspicious system activities. On the other hand, NIDS is set up on a network. It monitors traffic of all device of the network.

- What does SSL stand for?
  - SSL(Secure Sockets Layer) is the industry-standard security technology creating encrypted connections between Web Server and a Browser. This is used to maintain data privacy and to protect the information in online transactions.

    - What are the steps for establishing an SSL connection?
      1. A browser tries to connect to the webserver secured with SSL
      2. The browser sends a copy of its SSL certificate to the browser
      3. The browser checks if the SSL certificate is trustworthy or not. If it is trustworthy, then the browser sends a message to the web server requesting to establish an encrypted connection
      4. The web server sends an acknowledgment to start an SSL encrypted connection
      5. SSL encrypted communication takes place between the browser and the webserver

- Explain what a brute force attack is?
  - Brute Force is a way of finding out the right credentials by repetitively trying all the permutations and combinations of possible credentials. In most cases, brute force attacks are automated where the tool/software automatically tries to login with a list of credentials.

- What 3 ways one can mitigate brute force attacks?
    - Password Length: You can set a minimum length for password. The lengthier the password, the harder it is to find.
    - Password Complexity: Including different formats of characters in the password makes brute force attacks harder. Using alpha-numeric passwords along with special characters, and upper and lower case characters increase the password complexity making it difficult to be cracked.
    - Limiting Login Attempts: Set a limit on login failures. For example, you can set the limit on login failures as 3. So, when there are 3 consecutive login failures, restrict the user from logging in for some time, or send an Email or OTP to use to log in the next time. Because brute force is an automated process, limiting login attempts will break the brute force process.
    -
- What is Port Scanning?
    - Port Scanning is the technique used to identify open ports and service available on a host. Hackers use port scanning to find information that can be helpful to exploit vulnerabilities. Administrators use Port Scanning to verify the security policies of the network.
    -
- Name 2-3 Port Scanning Techniques

    1. Ping Scan
    2. TCP Half-Open
    3. TCP Connect
    4. UDP
    5. Stealth Scanning

    -

    -
- Explain the difference between Risk, Vulnerability & Threat in an organization?
    - *Threat*: Someone with the potential to harm a system or an organization
    - *Vulnerability*: Weakness in a system that can be exploited by a potential hacker
    - *Risk*: Potential for loss or damage when threat exploits a vulnerability

- Explain the difference between Vulnerability vs. Exploit vs. Payload?
    - *Vulnerability*: Weakness in a system that can be exploited by a potential hacker
    - *Exploit*: An exploit is the means by which an attacker takes advantage of a vulnerability within a system, an application, or a service. An attacker uses an exploit to attack a system in a way that results in a particular desired outcome that the developer never expected.

- *Payload*: a software tool designed to deliver a exploit that takes advantage of a flaw in a computer system, typically for malicious purposes such as installing malware

- What are the 3 different types of hackers <Think hats>?
  - Black hat hackers are known for having vast knowledge about breaking into computer networks. They can write malware which can be used to gain access to these systems. This type of hackers misuse their skills to steal information or use the hacked system for malicious purpose.
  - White hat hackers use their powers for good deeds and so they are also called Ethical Hackers. These are mostly hired by companies as a security specialist that attempts to find and fix vulnerabilities and security holes in the systems. They use their skills to help make the security better.
  - Grey hat hackers are an amalgamation of a white hat and black hat hacker. They look for system vulnerabilities without the owner's permission. If they find any vulnerabilities, they report it to the owner. Unlike Black hat hackers, they do not exploit the vulnerabilities found.
- What does MITM mean?
  - A MITM(Man-in-the-Middle) attack is a type of attack where the hacker places himself in between the communication of two parties and steal the information.
- What does DOS stand for in cybersecurity?
  - A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.
- What does a DDOS stand for in cybersecurity?
  - A DDOS(Distributed Denial of Service) attack is a distributed cyberattack that causes the servers to not be able to provide services to genuine clients by having their resources exhausted. This is achieved by using many different compromised hosts (zombies, bots) to attack the service.

- What is a botnet?
  - A Botnet is a number of devices connected to the internet where each device has one or more bots running on it. The bots on the devices and malicious scripts used to hack a victim. Botnets can be used to steal data, send spams and execute a DDOS attack.

- What are the 3 types of DDOS types?
  - Protocol
  - Volumetric
  - Application

- Explain what a Protocol DDOS attack is?
    - Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (Pps).

- Explain what a Volumetric DDOS attack is?
    - Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack's goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).

- Explain what an Application DDOS attack is?
    - Includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to exhaust the resources of the web server, and the magnitude is measured in Requests per second (Rps).

- What type of cybersecurity company prevents DDOS attacks?
    - CDN
    - Content Delivery Networks

- What does 2FA stand for?
    - 2 Factor Authentication

- What does 2FA do?
    - An extra layer of security that is known as *"multi-factor authentication".*
    - Requires not only a password and username but also something that only, and only, that user has on them, i.e. a piece of information only they should know or have immediately to hand – such as a physical token.
    - Authenticator apps replace the need to obtain a verification code via text, voice call or email.

- Explain Phishing?
    - Phishing is a Cyberattack in which a hacker disguises as a trustworthy person or business and attempt to steal sensitive financial or personal information through fraudulent email or instant message.
- What is the best defense against phishing?
    - End User Education
- Name two very popular Email Protection companies that specifically address phishing?

- Proofpoint
- MIMEcast

- One of the many fundamental things to know as a cybersecurity professional is the function and port number used by a number of common services as well as many that are typically implemented during the course of a cybersecurity professional's career.
- Memorizing the Protocol, either TCP or UDP, their port number and what the protocol does IS FAIR GAME in a cybersecurity interview.
- Life isn't fair, memorize this and GET THAT JOB!
- Students DO NOT have to memorize the IEEE RFC, but if they do, they will look like a god.

Common TCP/IP Protocols and Ports

Protocol	TCP/UDP	Port Number	Description
File Transfer Protocol (FTP) (RFC 959)	TCP	20/21	FTP is one of the most commonly used file transfer protocols on the Internet and within private networks. An FTP server can easily be set up with little networking knowledge and provides the ability to easily relocate files from one system to another. FTP control is handled on TCP port 21 and its data transfer can use TCP port 20 as well as dynamic ports depending on the specific configuration.
Secure Shell (SSH) (RFC 4250-4256)	TCP	22	SSH is the primary method used to manage network devices securely at the command level. It is typically used as a secure alternative to Telnet which does not support secure connections.
Telnet (RFC 854)	TCP	23	Telnet is the primary method used to manage network devices at the command level. Unlike SSH which provides a secure connection, Telnet does not, it simply provides a basic unsecured connection. Many lower level network devices support Telnet and not SSH as it required some additional processing. Caution should be used when connecting to a device using Telnet over a public network as the login credentials will be transmitted in the clear.

Simple Mail Transfer Protocol (SMTP) (RFC 5321)	TCP	25	SMTP is used for two primary functions, it is used to transfer mail (email) from source to destination between mail servers and it is used by end users to send email to a mail system.
Domain Name System (DNS) (RFC 1034-1035)	TCP/UDP	53	The DNS is used widely on the public internet and on private networks to translate domain names into IP addresses, typically for network routing. DNS is hieratical with main root servers that contain databases that list the managers of high level Top Level Domains (TLD) (such as .com). These different TLD managers then contain information for the second level domains that are typically used by individual users (for example, cisco.com). A DNS server can also be set up within a private network to private naming services between the hosts of the internal network without being part of the global system.
Dynamic Host Configuration Protocol (DHCP) (RFC 2131)	UDP	67/68	DHCP is used on networks that do not use static IP address assignment (almost all of them). A DHCP server can be set up by an administrator or engineer with a poll of addresses that are available for assignment. When a client device is turned on it can request an IP address from the local DHCP server, if there is an available address in the pool it can be assigned to the device. This assignment is not permanent and expires at a configurable interval; if an address renewal is not requested and the lease expires the address will be put back into the poll for assignment.
Trivial File Transfer Protocol (TFTP) (RFC 1350)	UDP	69	TFTP offers a method of file transfer without the session establishment requirements that FTP uses. Because TFTP uses UDP instead of TCP it has no way of ensuring the file has been properly transferred, the end device must be able to check the file to ensure proper transfer.

			TFTP is typically used by devices to upgrade software and firmware; this includes Cisco and other network vendors' equipment.
Hypertext Transfer Protocol (HTTP) (RFC 2616)	TCP	80	HTTP is one of the most commonly used protocols on most networks. HTTP is the main protocol that is used by web browsers and is thus used by any client that uses files located on these servers.
Post Office Protocol (POP) version 3 (RFC 1939)	TCP	110	POP version 3 is one of the two main protocols used to retrieve mail from a server. POP was designed to be very simple by allowing a client to retrieve the complete contents of a server mailbox and then deleting the contents from the server.
Network Time Protocol (NTP) (RFC 5905)	UDP	123	One of the most overlooked protocols is NTP. NTP is used to synchronize the devices on the Internet. Even most modern operating systems support NTP as a basis for keeping an accurate clock. The use of NTP is vital on networking systems as it provides an ability to easily interrelate troubles from one device to another as the clocks are precisely accurate.
NetBIOS (RFC 1001-1002)	TCP/UDP	137/138/139	NetBIOS itself is not a protocol but is typically used in combination with IP with the NetBIOS over TCP/IP (NBT) protocol. NBT has long been the central protocol used to interconnect Microsoft Windows machines.
Internet Message Access Protocol (IMAP) (RFC 3501)	TCP	143	IMAP version3 is the second of the main protocols used to retrieve mail from a server. While POP has wider support, IMAP supports a wider array of remote mailbox operations which can be helpful to users.
Simple Network Management Protocol (SNMP) (RFC 1901-1908, 3411-3418)	TCP/UDP	161/162	SNMP is used by network administrators as a method of network management. SNMP has a number of different abilities including the ability to monitor, configure and control network devices. SNMP traps

			can also be configured on network devices to notify a central server when specific actions are occurring. Typically, these are configured to be used when an alerting condition is happening. In this situation, the device will send a trap to network management stating that an event has occurred and that the device should be looked at further for a source to the event.
Border Gateway Protocol (BGP) (RFC 4271)	TCP	179	BGP version 4 is widely used on the public internet and by Internet Service Providers (ISP) to maintain very large routing tables and traffic processing. BGP is one of the few protocols that have been designed to deal with the astronomically large routing tables that must exist on the public Internet.
Lightweight Directory Access Protocol (LDAP) (RFC 4510)	TCP/UDP	389	LDAP provides a mechanism of accessing and maintaining distributed directory information. LDAP is based on the ITU-T X.500 standard but has been simplified and altered to work over TCP/IP networks.
Hypertext Transfer Protocol over SSL/TLS (HTTPS) (RFC 2818)	TCP	443	HTTPS is used in conjunction with HTTP to provide the same services but doing it using a secure connection which is provided by either SSL or TLS.
Lightweight Directory Access Protocol over TLS/SSL (LDAPS) (RFC 4513)	TCP/UDP	636	Just like HTTPS, LDAPS provides the same function as LDAP but over a secure connection which is provided by either SSL or TLS.
FTP over TLS/SSL (RFC 4217)	TCP	989/990	Again, just like the previous two entries, FTP over TLS/SSL uses the FTP protocol which is then secured using either SSL or TLS.

- What is the default port for RDP?
    - 3389
- What port is FTP? (Trick Question)

    - Its 2 ports 20 and 21

- What port does the PING command use? (Trick Question)
    - It doesn't
    - ICMP does not use a port since it does not have a place for a port. It is encapsulated with an IP datagram only.

- Is PING, UDP or TCP? (Trick Question)
    - It uses the ICMP protocol

- What does the ICMP stand for?
    - Internet Control Message Protocol

References:

https://www.edureka.co/blog/interview-questions/cybersecurity-interview-questions/

https://latesthackingnews.com/2017/07/12/difference-exploit-payload-shellcode/

https://www.us-cert.gov/ncas/tips/ST04-015

https://www.imperva.com/learn/application-security/ddos-attacks/

https://www.pearsonitcertification.com/articles/article.aspx?p=1868080

https://en.wikipedia.org/wiki/ISO_image

https://superuser.com/questions/451432/are-the-command-prompt-and-ms-dos-the-same-thing

https://docs.microsoft.com/en-us/windows-server/administration/server-core/what-is-server-core

https://support.rackspace.com/how-to/what-is-an-soa-record/

https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution

https://www.efficientip.com/glossary/dhcp-lease/

https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

https://www.geeksforgeeks.org/ps-command-in-linux-with-examples/

https://www.tecmint.com/linux-more-command-and-less-command-examples/

https://en.wikipedia.org/wiki/IEEE_802.1X