Q1.

ICMP: Benefit:

1. ICMP can be used by C&C for network scanning

2. AN ICMP flood attack causing DoS or DDoS can be made easily with the botnet having multiple IPs is more advantageous where in the conventional way of a single attacker uDsing spoofed IPs linearly.

Drawback:

When the C&C uses the ICMP for communication between victim and bots/itself, if in a victim network, the ICMP echo messages are disabled then the botnet/ or communication between the victim machine to C&C may be lost.

DNS: Benefit:

1. **In Fast-flux network, dns is used as multiplexer and load balancer**

1. It is possible to assign multiple IP addresses to the same domain name enabling the use of multiple hosts for a single web page. This mechanism is used in a fast-flux network, where multiple bots register for one DNS host record. Upon resolving the record, one or several of these bots are returned. Instead of connecting directly to the C&C server these bots are used as intermediate hosts which in turn relay the data to the C&C server. Therefore, only these so called proxy bots know the real C&C server. Since registering and de-registering servers can be done at any time, this method can be used to cycle through multiple servers quickly. This increases the effort needed to shut down the botnet.

DNS: Drawback:

1. Registering expired domain names either for C&C or bots, make the C&C vulnerable to debugging by IDC.

2. When all the bots of a C&C are registered for the same DNS, blocking or de-registering that DNS can shutdown the entire botnet of that C&C

Q2.

Off-path:

Blind packet injection: must guess the proper values in the forged response fields(like tx id, port num etc) according to the query

Race condition: forged response must arrive before the real one

On-path:

Race condition: forged response must arrive before the real one

In-path:

I guess no conditions

Q3.

Database server

Q4.

9999

Q5.

HTTPS provides end-to-end encryption whereas SMTPS doesn’t provide end-to-end encryption. SMTPS in fact provides encryption between only Mail Transfer Agents (MTAs)

Q6. EXAM BROWSER

1. **Phishing**
2. **SSL Stripping using arp spoofing -**

Malicious attackers can perform arp spoofing between the victim machine(web page on victim browser) and the server. After this whenever the victim types the url name(www.blackboard.com) then the browser connects to the server machine and waits for the server response. Since an attacker can intercept packets from both victim/server, now it forwards the victim’s request to the server and receives the secure HTTPS page. At this point, the attacker has complete control over the secure web page. He downgrades it from HTTPS to HTTP and sends it back to the victim’s browser. Next, the victim browser is now redirected to http://www.blackboard.com. From now onward, all the victim’s data will be transferred in plain text format, and the attacker will be able to intercept it. Meanwhile, the website’s server will think that it has successfully established the secure connection, which indeed it has—but with the attacker’s machine, not the victim’s.

3. **Shoulder surfing.**

Q7. ON-PATH

1. **DNS spoofing: if victim sends a dns request to a dns server and attacker sniffs the dns request packet. After this with the matching txid attacker creates a forged dns response packet and sends it to the victim machine before the victim machine receives the actual dns response from the server, then the victim rejects the actual dns response considering it as a duplicate packet.**

2. Unprotected wifi network: any client that joins the network can mount it right away

//airpwn

Q8. SYN COOKIES

No, SYN cookies does not completely solve the problem of DOS attacks. SYN cookies places extra load on server resources, thus doesn't reduce the traffic completely making it ineffective against DOS attacks.

Q9. PGP SMTPS

Yes we still need to use SMTPS because PGP doesn't encrypt metadata, whereas SMTPS encrypts metadata as well.

Q10.

Defences against man in the middle
---
(1)Use a VPN
it masks the IP address by bouncing it through a private server. VPNs also encrypt the data as it's being transmitted over the Internet.

(2) Encryption

End-to-end encryption:
End-to-end encryption is primarily a communication encryption system that works best against email hijacking and similar types of man-in-the-middle attacks. The encryption makes it impossible for parties other than the sender and the recipient to read a message.
Device encryption:
Device encryption covers endpoint security weaknesses and provides more robust security against man-in-the-middle attacks.
TLS/SSL encryption:
TSL/SSL encryption secures HTTP network connection thereby protecting against HTTP interception and web-reliant man-in-the-middle attacks.

(3) Malware Protection:
Most antivirus software detect the malware and provides additional network security and firewall protection, which should further reinforce the protection against attacks.

4) Use firewall

5) Use HTTPS websites only

6) Authentication

7) Tamper detection

Q11.

HSTS and MTA-STS

Q12. GOALS OF DNS

Both protocols use end-to-end encryption between the client and the DoH/DoT-based DNS resolver. They provide:

They aim to secure DNS by adding confidentiality, integrity and server authenticity•

DoT: DNS queries and responses are tunneled over TLS (RFC7858)

- DoH: DNS resolution is performed over HTTPS, inheriting all security benefits of the HTTPS protocol (RFC8484)

Q13.

The adversary can follow an attack similar to stuxnet. The only way is to add a new machine to the router's network which is injected with malware or somehow we need to enter our malware into some system of that network. Now the malware code can be propagated to other machines in the network and whenever the request to the web interface is sent, the malware code can run and attack the setup.

Q14.

HMAC-SHA256

Q15.

Please enter your name correctly

Q16.

Two-factor authentication
Single Sign On
Forcing users to pick long passphrases
Force users to pick strong passwords

Q17. NAT and STATEFUL FIREWALL

NAT performs address/port translation while statefull firewall doesnt. Also NAT doesnt fully track the TCP 3-way handshake.

Q18. TCP PORT 5544

Read below answer and try to summerize
Using the connectionless UDP instead of the connection-oriented TCP is crucial for a successful DDoS amplification attack. Here we are using tcp, so doesnt work.

Q19.XSS

Client

Q20.
Denial of Service attack (users cannot access the e-banking website).
Redirect visitors into a phishing website to intercept their passwords.
Intercept email messages sent to any @vulnbank.com email address.
Send valid SPF-allowed messages from any @vulnbank.com email address.
Send valid DKIM-signed email messages from any @vulnbank.com email address.

Q21. CENSOR
DNS Tampering: **In countries where authorities have control over domain name servers, censors can "deregister" a domain or website**
IP Blocking: Censors with control over internet service providers can blacklist certain IP addresses of websites
Keyword filtering: For a more powerful censoring technique, censors may use URL filtering. This mechanism scans the requested string for target words
Packet filtering: The process of deep packet inspection examines packet contents for banned keywords. Communication identified as containing forbidden content can be disrupted by dropping the connection. Users may receive one of a number of error messages on their browsers, none indicating explicitly that they are being censored.

Q22. MOUNT MITM

SSL Stripping :

1. **MitM attack to prevent redirection to HTTPS**
2. **Watch for HTTPS redirects and links, and map them to HTTP links**

Rogue certificates:

Rogue certificates allow attackers to create illegitimate sites that are indistinguishable from real sites like eBay, Google or PNC because their certificate hierarchy can be

validated. Users then will be redirected to such sites through '"man in the middle" attacks where a compromised host in-between the user and a legitimate site sends traffic to an illegitimate site instead.

Self Signed Certificates:

Self-Signed Certificate is a security certificate that is not signed by a certificate authority (CA). However, they do not provide all of the security properties that certificates signed by a CA aim to provide. For instance, when a website owner uses a self-signed certificate to provide HTTPS services, people who visit that website will see a warning in their browser. Website visitors who bypass such warnings are exposed to a risk that a third party could intercept traffic to the website using the third-party's own self-signed certificate. This is a type of man-in-the-middle (MitM) attack, and it allows the third party to read and modify all data sent to or from the website by the target user.

Q23. CRYPTO HASH

A hash is a fixed-length string of letters and numbers generated by an algorithm. The digital signature creator's private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature.

The reason for encrypting the hash instead of the entire message or document is a hash function can convert an arbitrary input into a fixed-length value, which is usually much shorter. This saves time as hashing is much faster than signing.

Q24. Switched Local network

Arp Spoofing:

1. Arp reply to victim, mapping gateway's ip to attackers MAC

2. Arp reply to gateway, mapping victim's ip to attacker's mac

3. Just forward back and forth.

Q25. HIJACK BOTNET

No. Because, it is less accurate. Below are the reasons:

NAT => underestimation: many bots behind the same IP address
DHCP => overestimation: the same bot uses many IP addresses

Q26.

Only Tor exit nodes can identify the full URL of the websites anonymous user visited.

In case of foo.com exit node, can identify the URL and content of the message.
In case of bar.com exit node, can identify the URL from SNI (Server name Indication) used field during TCP handshake.

Https - domain name --- sub web page link not visible
Http - all are visible...