**Encryption Is Now a Trojan Horse: Ignore It at Your Peril**

**Question 1**

**What is Encryption? How does it work?**

Encryption is a process that encodes a message or file so that it can be only be read by certain people. Encryption uses an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble, or decrypt, the information. The message contained in an encrypted message is referred to as plaintext. In its encrypted, unreadable form it is referred to as ciphertext.

Encryption uses algorithms to scramble your information. It is then transmitted to the receiving party, who is able to decode the message with a key. There are many types of algorithms, which all involve different ways of scrambling and then decrypting information.

**Question 2**

Write an algorithm through which we can design a Encryptor ?

* The main processing of this project is we provide a original text file in to an encryptor module.
* The encryptor module provides the facility of encrypting the original text file, i.e. converting it into a non-readable form.
* Then after each character of the given data is extracted and if further converted into ASCII codes.
* These codes are then subjected to FFT algorithm for further encryption.
* Then we convert the ASCII code to frequency domain while performing the encryption process which requires a particular key i.e. a password or a code or a pin to be entered to perform the remaining process.
* A series of complex numbers are produced as the result
* Then after the encrypted data is converted into a file which is the required encrypted output.
* The encrypted output is saved and stored in a new file location where it is possible.

**Question 3**

Explain briefly about SSL Protocol ?

1. Secure Sockets Layer (SSL) is a standard protocol used for the secure transmission of documents over a network.
2. SSL technology creates a secure link between a Web server and browser to ensure private and integral data transmission.
3. SSL uses Transport Control Protocol (TCP) for communication.
4. SSL, the word socket refers to the mechanism of transferring data between a client and server over a network.
5. When using SSL for secure Internet transactions, a Web server needs an SSL certificate to establish a secure SSL connection. SSL encrypts network connection segments above the transport layer, which is a network connection component above the program layer.

**Question 4**

What is IDS ? Explain briefly.

1. An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.
2. Some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses.
3. Although intrusion detection systems monitor networks for potentially malicious activity, they are also prone to false alarms. Consequently, organizations need to fine-tune their IDS products when they first install them.
4. That means properly configuring their intrusion detection systems to recognize what normal traffic on their network looks like compared to potentially malicious activity.

**Question 5**

Differentiate between HTTP and HTTPS?

HTTP URL in your browser’s address bar is http:// and the HTTPS URL is https://.

1. HTTP is unsecured while HTTPS is secured.
2. HTTP sends data over port 80 while HTTPS uses port 443.
3. HTTP operates at application layer, while HTTPS operates at transport layer.
4. No SSL certificates are required for HTTP, with HTTPS it is required that you have an SSL certificate and it is signed by a CA.
5. HTTP doesn’t require domain validation, where as HTTPS requires at least domain validation and certain certificates even require legal document validation.
6. No encryption in HTTP, with HTTPS the data is encrypted before sending

**Comprehensive Email Protection**

**Question 1**

**What is spear Phishing? How does it work ?**

Ans.

**Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. It is often used to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user’s computer.**  An email arrives, apparently from a trustworthy source, but instead it leads the unknowing recipient to a bogus website full of malware. These emails often use clever tactics to get victims' attention. For example, the FBI has warned of spear phishing scams where the emails appeared to be from the National Center for Missing and Exploited Children. These emails don’t display any obvious characteristics (such as infected attachments or suspicious URLs) that would flag their malicious intent to gateway security controls. Many times, government-sponsored hackers and hacktivists are behind these attacks. Cybercriminals do the same with the intention to resell confidential data to governments and private companies. These cybercriminals employ individually designed approaches and social engineering techniques to effectively personalize messages and websites. As a result, even high-ranking targets within organizations, like top executives, can find themselves opening emails they thought were safe. That slip-up enables cybercriminals to steal the data they need in order to attack their networks.

**Question 2**

How to protect ourselves from being attacked? Suggest some methods.

Traditional security often doesn't stop these attacks because they are so cleverly customized. As a result, they're becoming more difficult to detect.

Some of the methods are:

1. Inbound protection from advanced threats

Incoming attacks with zero-hour malware should be blocked and prevented from entering the organization, and users should be protected from malicious URLs embedded within messages and attachments.

1. Outbound protection to prevent data leakage

Outbound email should be monitored to prevent the leakage of sensitive content, and messages encrypted if needed to secure sensitive communications.

1. Business and Email Continuity

Organizations should be able to restore production email data quickly and accurately in the event of accidental deletion or data loss. In addition, users should be able continue email communications if their primary email server becomes temporarily unavailable.

1. Spear Phishing and Business Fraud protection

Zero-payload spear phishing emails should be proactively detected, and quarantined from email inboxes, and attempts to compromise user email accounts should be prevented. Organizations should also be able to identify and protect against domain spoofing and business fraud activities.

1. User Awareness Training

End users should be enabled as the last line of defense against spear phishing and other targeted attacks, by providing them with tools and training to proactively identify and avoid these threats.

**Question 3**

What is Barracuda Email Protection?

Ans.

Barracuda provides the most comprehensive, cloud-based, multi-layered solution to secure your entire email infrastructure. The Barracuda Email Security Gateway includes spam and virus blocking, data protection, email continuity, DoS prevention, encryption, and policy management—combined to deliver a complete solution. As new requirements emerge, it is automatically updated with new capabilities to ensure continuous protection. The Barracuda Email Security Gateway provides multi-layer security, email continuity, and data leakage prevention. Advanced Threat Protection1 combines behavioral, heuristic, and sandboxing technologies to protect against zerohour, targeted attacks and ransomware.It also provides Advanced Threat Protection1 to protect against ransomware and other advanced threats

**Question 4**

# What are the advantages of Barracuda Cloud Protection Layer ?

# Ans.

CPL receives inbound email on behalf of the organization, insulating your organization's mail server from receiving direct Internet connections and associated threats. ‘This layer does not apply to outbound mail.’ Here are some of the benefits of using CPL together with your Barracuda Email Security Gateway:

* Spooling – CPL polls your inbound mail server regularly and, if the mail server goes down, the service spools your inbound mail for up to 4 days. As soon as the mail server comes back up, email is released in a steady stream, resuming consistent inbound mail flow.
* Advanced Threat Protection (ATP) – The optional, subscription-based ATP service analyzes inbound email attachments in a separate, secured cloud environment, detecting new threats and determining whether to block such messages. ATP offers protection against advanced malware, zero-day exploits, and targeted attacks not detected by the Barracuda Email Security Gateway virus scanning features.
* Link Protection – Rewrites a deceptive URL in an email message to a safe Barracuda URL, and delivers that message to the user.
* Email Burst Handling – Email surge suppression during peak traffic and spam spikes, which offloads a significant volume of spam email from your Barracuda Email Security Gateway to be filtered via the cloud.
* Immediate Response – Automatic updates in real time, leveraging threat intelligence from Barracuda Labs and Barracuda Central to continuously stay ahead of quickly morphing threats.

# Question 5

# What are the different layers that Burracuda implement to ensure the email security?

# Ans.

# Barracuda Essentials

# Inbound email filtering protects against spam, viruses and phishing attacks, and enforces policy controls.

# Email Continuity Service ensures users can continue working through email server and service disruptions.

# Outbound email filtering prevents data leakage and automatically encrypts sensitive data.

# Cloud Archiving Service provides comprehensive email archiving, with granular retention policies ensuring compliance, e-discovery searches and mobile access for end users.

# Barracuda Sentinel

1. AI-based real time identification and protection against targeted spear phishing attacks.
2. Detection, prevention and remediation of email account takeover. •
3. DMARC Reporting and Management guards against domain spoofing and business fraud activities
4. Barracuda PhishLine
5. Multi-Vector and Multi-Variable attack simulations to train users and turn them into a strong last line of defense against email threats.
6. Customizable simulation scenarios including pre-built email templates and landing pages.
7. Rich, elegant and engaging training content including quizzes and risk assessment surveys, in easy to use online catalogs.

**WIFI 6**

**Question 1**

What is WiFi 6 ?

1. Wi-Fi 6 is the next generation standard in WiFi technology. Wi-Fi 6 also known as “AX WiFi" or "802.11ax WiFi” builds and improves on the current 802.11ac WiFi standard.
2. Wi-Fi 6 was originally built in response to the growing number of devices in the world.
3. If you own a VR device, multiple smart home devices, or simply have a large number of devices in your household, then a Wi-Fi 6 router might just be the best WiFi router for you.
4. WiFi 6 will be up to four times faster in device-dense areas and offer much greater bandwidth than its predecessor. With internet service getting faster than ever, WiFi 6 will allow wireless devices to take full advantage of these new speeds.

**Question 2**

**How Wifi 6 and 5 G network used in IoT devices?**

Both Wi-Fi 6 and 5G offer exciting opportunities to connect more devices reliably via wireless. This is important for mission-critical IoT devices being used in manufacturing automation, healthcare, energy, and many other industries.

Wi-Fi 6 and 5G will also offer enhanced mobile broadband for immersive experience via augmented and virtual reality. Although many industries will benefit from the enhanced mobile experience, industries such as hospitality, retail, and education will drive immersive experiences for their business.

Both Wi-Fi 6 and 5G offer exciting opportunities to connect more devices reliably via wireless. This is important for mission-critical IoT devices being used in manufacturing automation, healthcare, energy, and many other industries.

Wi-Fi 6 and 5G will also offer enhanced mobile broadband for immersive experience via augmented and virtual reality. Although many industries will benefit from the enhanced mobile experience, industries such as hospitality, retail, and education will drive immersive experiences for their business.

**Question 3**

**What are the advantages and disadvantages of WiFi 6?**

It has been developed to deliver 40% high peak data rates using single client device. Average throughput per user is improved by at least 4 times in dense environments.

1. It offers four times increase in network efficiency compare to 802.11ac.
2. It is backward compatible with 802.11n and 802.11ac devices.
3. It uses OFDMA and hence multiple users can transmit at the same. The OFDMA based scheduling helps in reducing overhead and latency both.

Disadvantages:

1. OFDM subcarrier spacing is narrower at 78.125 KHz. This means good phase noise oscillators and highly linear RF front ends are essential.
2. As 1024-QAM is used to achieve higher data rates, EVM specification is tight.
3. Tight frequency synchronization and clock offset correction are required to achieve better performance.
4. Moreover WiFi 6 stations maintain frame timing based on their clocks. This is essential as their transmissions should be as per trigger frames and scheduling.

**Question 4**

**What is MU-MIMO ? How it is used in WiFi 6?**

MU-MIMO stands for Multi-User, Multiple Input, Multiple Output.Before MU-MIMO, imagine your Wi-Fi as a single lane road, along which cars must pass in both directions to receive and send information. You can easily imagine how slow this would be, having to stop periodically to allow traffic in the opposite direction to pass. With MU-MIMO, extra lanes are added to the road, so that you now have dedicated lanes for transferring information in both directions.

Wifi 6 uses this to dramatically increases efficiencies by doubling the number of downstream and increasing the number of upstreams that can be handled by a factor of eight with the potential to deliver four simultaneous streams to a single device. Orthogonal Frequency Division Multiple Access improves numerous aspects of Wi-Fi delivery by making it more efficient by lowering latency and improving the overall quality of service in congested, high-demand areas such as conference halls and stadiums.

**Question 5**

**What is OFDMA ?**

Orthogonal frequency division multiple access – OFDMA

1. OFDMA takes a Wi-Fi channel and divides it into smaller frequency allocations known as resource units (RUs).
2. This enables an AP to communicate with multiple clients by assigning them to specific RUs.
3. By subdividing the channel, applications that use small frames, such as video or audio streaming, can be transmitted to multiple endpoints simultaneously, which cuts down on overhead and congestion at layer two, improving application performance.
4. OFDMA is highly flexible and can allocate the entire channel to a single client or sub-divide, depending on traffic.