Honors PYQ

Sure, here is the first question and its answer:

Q1. Explain the concept of genetic algorithms and discuss their relevance in the field of information security.

Answer:

Genetic Algorithms (GAs) are optimization techniques inspired by the process of natural selection. They use operations like selection, crossover, and mutation to evolve a population of candidate solutions toward an optimal or near-optimal solution.

Components of Genetic Algorithms:

Component	Description
Population	Set of possible solutions
Fitness Function	Evaluates the quality of each solution
Selection	Chooses better-performing individuals for reproduction
Crossover	Combines two solutions to create offspring
Mutation	Randomly alters a solution to maintain diversity

Relevance in Information Security:

- **Cryptanalysis:** Breaks encryption by evolving possible keys or patterns.
- **Anomaly Detection:** Detects unusual behavior in systems by optimizing rule sets.
- **Feature Selection:** Selects best features for training intrusion detection models.
- **Access Control Optimization:** Refines user-role policies.

GAs are effective in information security due to their ability to explore large solution spaces and adapt to complex, dynamic threats.

Prompt **"next"** for the following question.

Q2. Explain the concept of a Sensor Stimuli Attack and its potential consequences in cybersecurity.

Answer:

A Sensor Stimuli Attack manipulates physical signals or environmental inputs to deceive or mislead sensors in cyber-physical systems (CPS) or IoT devices.

How It Works:

Attackers generate false stimuli (like sound, light, electromagnetic waves) that the sensor interprets as legitimate input, causing incorrect behavior or data reporting.

Potential Consequences:

Consequence	Description
False Data Injection	Misleads systems with incorrect sensor readings (e.g., temperature, motion)
Disruption of Services	Can disable alarms, cameras, or smart home systems
Unauthorized Access	Manipulates biometric sensors (like fingerprint or face recognition)
Safety Hazards	In industrial or healthcare systems, false readings can cause harm

Sensor stimuli attacks undermine the reliability of data-driven decisions and system automation.

Prompt **"next"** for the following question.

Q3. Explain Firewall architectures with suitable examples.

Answer:

Firewall architecture defines how firewalls are deployed within a network to filter traffic and enforce security policies.

Common Firewall Architectures:

Architecture Type	Description	Example Use Case
Packet Filtering Firewall	Filters packets based on IP, port, and protocol.	Basic perimeter defense for small networks.
Stateful Inspection Firewall	Tracks active connections and filters packets accordingly.	Enterprise networks needing connection context.
Proxy Firewall	Acts as an intermediary, inspecting application-layer data.	Web filtering and content control.
Dual-Homed Host Firewall	Uses a system with two NICs to separate networks.	Secure gateway between trusted and untrusted zones.
Screened Subnet (DMZ)	Creates a demilitarized zone to host public services between two firewalls.	Web servers accessible to public without LAN access.

Each architecture provides a different level of control, inspection, and isolation depending on the security needs.

Prompt **"next"** for the following question.

Q4. Distinguish between IDS vs IPS.

Answer:

Feature	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)
Function	Detects and alerts suspicious activity	Detects and actively blocks/prevents threats
Placement	Out-of-band (monitors traffic)	In-line (directly in the traffic path)
Response	Passive (alert generation)	Active (traffic blocking or modification)
Impact on Traffic	No direct impact	Can cause delays or drops during inspection
Use Case	Monitoring and forensic analysis	Real-time threat prevention

Example:

- IDS: Snort (in detection mode)
- IPS: Cisco Firepower, Suricata (in prevention mode)

Prompt **"next"** for the following question.

Q5. Discuss the goals and advantages of a Host-based Intrusion Detection System (IDS) in protecting individual endpoints and servers from security breaches and unauthorized access attempts.

Answer:

Goals of Host-based IDS (HIDS):

- **Monitor local activity:** Tracks file access, user logins, and system calls.
- **Detect unauthorized access:** Identifies suspicious behavior on a single machine.
- **Ensure system integrity:** Monitors changes in key system files and configurations.
- **Audit user actions:** Logs actions for analysis and compliance.

Advantages of HIDS:

Advantage	Description
Granular Monitoring	Offers detailed insight into system-level events
File Integrity Checking	Alerts on changes to critical files or configurations
Insider Threat Detection	Monitors legitimate users misusing privileges
Unaffected by Network Encryption	Works directly on the host, unaffected by encrypted network traffic
Customizable Policies	Tailored to specific systems or applications

HIDS complements network-level security by securing individual devices from within.

Prompt **"next"** for the following question.

Q6. What are the key components of a firewall policy, and how do they contribute to defining and enforcing security rules within a network infrastructure?

Answer:

A firewall policy is a set of rules that governs what traffic is allowed or denied in a network.

Key Components of a Firewall Policy:

Component	Description
Source/Destination IP	Specifies where the traffic originates and where it is going.
Ports and Protocols	Defines allowed or blocked communication types (e.g., HTTP, FTP).
Action (Allow/Deny)	Determines what to do with matching traffic (permit or reject).
Direction	Indicates inbound, outbound, or internal traffic.
Logging	Records rule matches for auditing and analysis.
Time-Based Rules	Enables policies to activate at specific times.

These components allow administrators to tailor traffic control, prevent unauthorized access, and ensure compliance with security standards.

Prompt **"next"** for the following question.

Q7. Provide a detailed note on how the Jerusalen Virus propagated and its effects on infected systems.

Answer:

The Jerusalem Virus (1987) was a DOS-based file infector virus that became widespread due to its stealthy propagation and destructive payload.

Propagation Mechanism:

- Infects `.COM` and `.EXE` files (except `COMMAND.COM`).
- Activates on Fridays the 13th by deleting executed programs.
- Stays resident in memory and infects files upon execution.

Effects on Infected Systems:

Effect	Description
File Re-infection	Files could be repeatedly infected, growing in size each time.
System Slowdown	Consumes memory, reducing available resources for other programs.
Destructive Payload	Deletes files on specific trigger dates (e.g., Friday the 13th).
System Instability	Causes crashes and erratic behavior due to corrupted executables.

The virus highlighted the need for proactive antivirus defenses and safe software handling practices.

Prompt **"next"** for the following question.

Q8. Compare traditional autoencoders with adversarial autoencoders in terms of training objectives and robust representation generation.

Answer:

Feature	Traditional Autoencoder	Adversarial Autoencoder (AAE)
Objective	Minimize reconstruction loss	Minimize reconstruction loss + match latent space to prior
Architecture	Encoder + Decoder	Encoder + Decoder + Discriminator
Latent Space Control	Unstructured	Structured via adversarial training
Robustness to Attacks	Limited (susceptible to noise/adversarial inputs)	More robust due to regularized latent distribution
Output Quality	Good reconstructions, poor generalization	Better generalization and sample generation

Conclusion:
AAEs combine the benefits of generative adversarial networks with autoencoders, producing more meaningful and robust feature representations for security and anomaly detection.

Prompt **"next"** for the following question.

Q9. Describe the common types of attacks targeting IoT devices, and how do these attacks exploit vulnerabilities in IoT Systems?

Answer:

IoT devices often lack strong security controls, making them easy targets.

Common IoT Attacks and Exploited Vulnerabilities:

Attack Type	Exploited Vulnerability	Description
Botnet Attacks	Weak/default credentials	Devices are hijacked into networks like Mirai for DDoS.
Man-in-the-Middle	Unencrypted communication	Intercepts and alters data between device and server.
Firmware Exploits	Lack of updates or secure boot	Attackers inject malicious code into outdated firmware.
Physical Attacks	Unsecured device access	Direct tampering with device hardware.
Data Leakage	Insecure storage or transmission	Sensitive user data is exposed or exfiltrated.

IoT security must address authentication, encryption, update mechanisms, and physical hardening.

Prompt **"next"** for the following question.

Q10. Enumerate two potential repercussions of relying on machine learning models vulnerable to adversarial attacks.

Answer:

Repercussion	Description
Security Breach via Misclassification	Adversarial inputs can fool models (e.g., image-based authentication) into incorrect outputs, leading to unauthorized access.
Loss of Trust and System Integrity	Users and stakeholders may lose confidence in ML-driven decisions due to inconsistent or unsafe behavior under attack.

These vulnerabilities highlight the importance of adversarial robustness in critical ML applications.

Prompt **"next"** for the following question.

Q11. Explain how social engineering attacks trick people into revealing sensitive information or performing actions that compromise security?

Answer:

Social engineering attacks exploit human psychology by manipulating trust, fear, or urgency.

Methods Used:

- **Pretexting:** Creating fake scenarios to gain information.
- **Phishing:** Sending deceptive emails or messages to trick users into clicking malicious links or sharing credentials.
- **Baiting:** Offering something enticing to lure victims into a trap.
- **Tailgating:** Physically following authorized personnel to gain entry.

By exploiting human error, attackers bypass technical controls and compromise sensitive data or systems.

Prompt **"next"** for the following question.

Q12. Write a Short Note on Wireless Network Hacking.

Answer:

Wireless network hacking involves exploiting vulnerabilities in Wi-Fi networks to gain unauthorized access or intercept data.

Common Techniques:

- **Packet Sniffing:** Capturing unencrypted wireless traffic.
- **Rogue Access Points:** Creating fake Wi-Fi hotspots to intercept user connections.
- **Cracking Encryption:** Breaking weak encryption like WEP or poorly configured WPA.
- **Man-in-the-Middle Attacks:** Intercepting communication between devices and access points.

Such attacks can lead to data theft, network disruption, and unauthorized resource access.

Prompt **"next"** for the following question.

Q13. Write a short Note on File Infector Virus and steps to prevent it.

Answer:

A File Infector Virus attaches itself to executable files (`.exe`, `.com`), spreading when infected files are run.

Characteristics:

- Infects and modifies executable files.
- Executes malicious code when infected file runs.
- Can corrupt or delete files, causing system instability.

Prevention Steps:

Prevention Measure	Description
Use updated antivirus software	Detects and removes infected files.
Avoid running unknown executables	Prevents accidental infection from untrusted sources.
Keep operating system patched	Fixes vulnerabilities exploited by viruses.
Use application whitelisting	Allows only approved software to run.

Prompt **"next"** for the following question.

Q14. Differentiate between Viruses, Worms, and Trojans.

Feature	Virus	Worm	Trojan
Definition	Malicious code attaching to files	Self-replicating malware spreading over networks	Malware disguised as legitimate software
Propagation	Requires user action to spread	Spreads automatically without user action	Does not self-replicate; relies on deception
Damage	Corrupts files, slows system	Consumes bandwidth, can cause network disruption	Performs malicious actions (e.g., backdoors)
Examples	Jerusalem Virus	Code Red Worm	Zeus Trojan

Prompt **"next"** for the following question.

Q15. Write a Short Note on Firewall Evaluation.

Answer:

Firewall evaluation assesses the effectiveness of firewall systems in enforcing security policies.

Key Evaluation Criteria:

Criterion	Description
Performance	Ability to handle traffic without significant latency or drops.
Security	Accuracy in blocking unauthorized traffic and preventing attacks.
Manageability	Ease of configuration, monitoring, and updating rules.
Scalability	Capability to support growing network size and complexity.
Compatibility	Integration with existing network infrastructure and systems.

Proper evaluation ensures the firewall provides reliable defense and fits organizational needs.

If you want more questions answered, just say **"next."**