# Question 1 – Memory Injection Attacks

1. Array Index
   * There has to be an array, and an index variable with the index variable able to be reached from external input.
   * There can’t be bounds checking the array
2. Pointer Subterfuge
   * There has to be a pointer
   * The attacker has to be able to overwrite the pointer
   * After the pointer is overwritten it has to be used
3. ARC Injection
   * Function pointer in code
   * The attacker has to be able to overwrite the pointer
   * After the pointer is overwritten it has to be used
4. V-Table Smashing
   * Polymorphic class
   * Buffer as a member variable
   * Attacker can overwrite parts of the V-Table. A pointer gets overwritten, then the pointer is used
5. Stack Smashing
   * Array on the stack that you can set from input
   * There can’t be bounds checking the array
   * Buffer overrun
6. Heap Smashing
   * Two adjacent heap buffers, first can be set w/ input
   * There can’t be bounds checking the array
   * Second buffer deleted first
   * First buffer overrun
7. Integer Overflow
   * Security check
   * Expression has potential overflow (I.E. an integer set to more then the max int size)
   * Something comes from external input
8. ANSI-Unicode Conversion
   * Buffer
   * Buffer must check size rather then number of elements.
9. VAR-ARG
   * Specific function
   * Ability to pass in arguments
   * Use can specify different number of parameters then program can accept

# Question 2 – OSI Levels

1. Physical Layer
   1. Electrical Impulse
   2. Electrical interference, or snipping a ethernet wire
2. Data Link Layer
   1. MAC address
   2. Mac address spoofing
3. Network Layer
   1. Routing
   2. Rouge Access Point
4. Transport Layer
   1. Transfer of data between systems
   2. Packet Sniffing
5. Session Layer
   1. Manages and terminated connections between applications
   2. Session hijacking
6. Presentation Layer
   1. Translates from network information to computer information
   2. Script injection
7. Application Layer
   1. Applications
   2. Script injection

# Question 3 – STRIDE

* Spoofing
  + Pretending to be someone that you’re not
* Tampering
  + Modifying data in some way
* Repudiation
  + Removing logs that say you or someone else did something
* Information Disclosure
  + Exposing confidential data
* Denial
  + Make service unavailable (DOS or DDOS)
* Elevation of privilege
  + Allow an action that you’re not supposed to be able to do

# Question 4 – DREAD

* Damage Potential
  + How bad could things be?
* Reproducibility
  + How likely is the attack to succeed?
* Exploitability
  + How hard is it?
* Affected Users
  + How many people will be affected?
* Discoverability
  + How easy is it to find?

# Question 5 – Threat Mitigation

1. Prevention
   1. Increase how hard it is to attack.
   2. Reduce vulnerabilities
2. Preemption
   1. Offensive strike
3. Deterrence
   1. Discourage an attack (physical example would be fences)
4. Deflection
   1. Trick the attacker by redirecting the attack to harmless location
5. Detection
   1. Detect abnormal activities
6. Countermeasures
   1. Devices that counter an attack

# Question 6 – McCumber Model

1. Asset
   1. Confidentiality
   2. Integrity
   3. Availability
2. Information State
   1. Storage
   2. Transmission
   3. Processing
3. Vulnerability