Cyber Network Security Midterm Cheat Sheet 1 Page Double Sided with Professor’s Permission

Focus Points:

Basic Concepts: (There relationship and the differences)

1. Vulnerability: A weakness in a system that can be exploited to cause loss and or harm.
2. Attacks: The execution of a plan (Threat) to cause loss and or harm.
3. Threats: A set of circumstances that have the potential to cause loss and or harm.

IP packets with spoofed source IP addresses: (And its relationship with other attacks/vulnerabilities)

* Attacker can impersonate another client that is on the same server the attacker is on.
* Attackers can access IP-based authenticated services.

DNS poisoning attacks

* Client sends a request to the DNS server, and if an attack can send a response back to the server before the client can, then the attacker can see all data that the server sends to the client but it is sent to the attacker first and the attacker can choose what is sent back to the client.

TCP session hijacking attacks

* For a TCP

Virus and Worm: (Permutation-based scanning)

* Both are able to permutate and self-replicate when attacking and infecting the system but each happen in different ways.
* The Worm can self-replicate and permutate on its own.
* The Virus can only do the same thing but with the user interactions giving direction.

XSS attacks:

* XSS Attack: A scripting vulnerability that enables attackers to bypass the same origin policy of browsers.
* Two Types of XSS Attacks:
  + Persistent XSS Attacks
    - Saved persistently in the database
    - Damage large number of users
  + Non-Persistent XSS Attacks
    - Targeted victims
* Same-Origin Policy:
  + One webpage can only read properties of another webpage if they share the same server, protocol, and port.
  + If the same server hosts unrelated sites, scripts from one site can access document properties on the other.

SQL injection attacks

* Exploit a security vulnerability in an SQL application (e.g., web application)
  + It is a specific case of “incomplete mediation”

RST injection for censorship

* Send an RST packet to a client with spoofed IP to terminate connection with whatever the client was connected to.

DNS hijacking

* An attack to trick victim to connecting to a normal website but it is just a fake copy that looks real. Giving the attacker the ability to view all the client’s information.