**Cybersecurity**

**Final Exam Study Guide**

**Unit 1:**

* List and define each part of the cybersecurity lifecycle? (Activity 1.3.1)
  + Detects: Try to find 6he problem
  + Respond: Find the solution
  + Recover: Fix anything regular that’s missing
  + Identify the assets, or whats in the data
  + Protect the data to make sure this never happens again.
* What is your digital footprint?
  + Everything you’ve done online, and what have you left behind
* Define brute force attack.
  + attackers systematically test characters over and over hoping to match a password
* What system is used to distinguish between a human and an automated program?
  + CAPTCHAs
* Define vulnerability.
  + or weaknesses in a system,
* What are the 5 types of malware? Give a definition of each.
  + Virus
  + Venom
  + Backdoor
  + Spyware
  + Trojan Horse
* Where are firewall applications typically installed...on what devices?
  + SMS, Image-Sharing, Streaming Media Services, VoIP, Emails, Forums, IRC, Mailing Lists, FTP.
* What are wildcard characters? Give one example.
  + A wildcard is a special character that represents other characters. There are many different wildcard characters, but a common one is the asterisk (\*). This wildcard stands for any number of letters, numbers, and symbols.
* What is the purpose of a site certificate?
  + Without an HTTPS in the address, a lock icon, and a valid site certificate, a website is not guaranteed to be using encrypted, secure communication.

**Unit 2:**

* What is the CIA Triad? Define each part of the Triad.
  + The CIA triad is a common model that forms the basis for the development of security systems. The parts are Confidentiality, Integrity, & Availability.
  + Confidentiality is more professional and try to make it safe. Example: Government secrets
  + Integrity keeps it more correct and more statistical, Example: Hospital data
  + Availability just shows availability basically. Example: Movie dates & time
* How would the whois, traceroute, and netstat commands help you investigate a website?
  + A Whois record contains all of the contact information associated with the person, group, or company that registers a particular domain name.
  + Traceroute is more seen to be used to trace data around the internet to confirm all is well, to trace malware, or to find evidence.
  + The tool netstat l shows network statistics, specifically the portsand IP addresses on your computer that are busy communicating with other hosts on the network.
* What does DDOS stand for and what is the purpose of a DDOS attack? List 2 types of a DDOS attack.
  + If one host is involved in the attack, the attack is considered to be a DoS attack. If multiple hosts are involved, it is a DDoS attack.
* How are log files and forceful browsing used to hack websites?
  + Hackers can use their knowledge of a web server’s directory structure to craft URL addresses and navigate to locations that are unreferenced and unlinked in a website.List 3 examples of client-side software and 3 examples of server-side software.
* What is XSS and how is it used?
  + XSS is a type of exploit in which the attacker takes advantage of an interactive web page to insert malicious client-side code into it. XSS can be used to steal data, take control over a computer, run malicious code, or initiate a phishing scam.
* How is Wireshark used?
  + Wireshark helps you organize and manage data packets so you can monitor and analyze network traffic.
* What is a MAC address? Provide 1 example of a MAC Address.
  + A MAC address uniquely identifies any device that uses a network. **00:00:5e:00:53:af**
* What does IEEE stand for and what does the organization do?
  + Institute of Electrical and Electronics Engineers is an organization that, in part, develops global standards in a broad range of industries, including information technology.

**Unit 3:**

* What is the purpose of a permission matrix? Define each part of the matrix.
  + Additionally, the first notation preceding these permissions denotes whether the item is a directory or not. A notation of “d” indicates a directory; a notation of “-” indicates it’s not a directory, for example, a file.
* Why is it necessary to have a security baseline?
  + To recognize what is suspicious, they must first understand what’s normal.
* What is the purpose of iptables?
  + the iptables utility allows for many arguments or flags.
* List the 3 guiding principles of ethical hacking.
  + Keep confidential all private information and intellectual property discovered.
  + Disclose all potential hazards or risks.
  + Use only legally obtained software and legal processes.
* List the 4 phases of ethical hacking and define each phase.
  + Reconnaissance
  + Scanning
  + Compromise
  + Remediation
* Explain the process of ARP poisoning.
  + a malicious user changes and corrupts the MAC to IP address information on a target computer, changing them to other addresses, usually to hosts they control. ARP poisoning attacks also corrupt a device’s ARP cache and wreak havoc on the hosts trying to communicate with each other.
* What is the connection between ICMP and TTL?
  + In trying to find a destination IP address, traceroute sends multiple ICMP echo request packets with increasing TTL values.

**Unit 4:**

* Explain the difference between Symmetric and Asymmetric Encryption.
  + Unlike symmetric key encryption where the shared key could be a password or passphrase, the keys in asymmetric key encryption are very large prime numbers.
* What is steganography?
  + Steganography is the practice of hiding data inside of other data, such as hiding text inside of media files.
* What is the purpose of a chain of custody form and a subpoena?
  + The form is used to record the transfer of evidence to new owners and the date and time of the transfer. a court order to produce records, or show up to a place at a certain time
* What are the 5 main properties of a hash function?
  + It is *deterministic*, meaning the same message always results in the same hash.
  + It is quick to compute the hash value for any given message. In other words, the execution time of the hash function should be fast.
  + It is infeasible to reverse the hash and obtain the original message from its hash value. All you can do is guess the original message using a brute-force method like a rainbow table to try all possible messages.
  + A small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value.
  + It generates unique hash values for unique data. It is extremely unlikely that two different messages will result in the same hash value (a collision).