MULTIPLE CHOICE QUESTION ON CYBER SECURITY

SIFAT JAHAN

ALIGARH MUSLIM UNIVERSITY

Collected from IBM course on cyber security

Question: What was shown in the movie war Games that concerned President Regan

- Answer: A teenager hacked into a Pentagon Computer that was capable of launching nuclear weapons

Question: In addition to the movie war Games, what other event made the need for advance cyber security

- Answer: 9/11

Question: what were the three main cybersecurity concerns arising from the 9/11

- Answer
- Could an attack like this happen in the virtual world too?
- Could this happen again?
- How did this happen

Question: "A defined way to breach the security of an IT system through a vulnerability" is the definition of which key cybersecurity term?

Answer: Exploit

Question: "A situation involving exposure to a danger." Is the definition of which key cybersecurity term?

Answer: Risk

Question: Which aspect of a comprehensive approach to cybersecurity includes these items: evaluate, create teams, establish baselines, identify and model threats, identify use cases, identify risks, establish monitoring and control requirements?

Answer: Security Program

Question: Alice sends an unencrypted message to Bob but it is intercepted by Trudy. Trudy reads the message but does not in any way interfere with its content or delivery. What precept of the CIA triad would have been violated.

Answer: Confidentiality

Question: Alice sends an encrypted message to Bob but it is intercepted by Trudy. Trudy cannot reads it so, in anger, she deletes it without allowing its delivery to Bob. What precept of the CIA triad would have been violated

Answer: Availability

Question: Alice sends an encrypted message to Bob but it is intercepted by Trudy. Trudy cannot read it but forward it on Bob from an anonymous address she controls . What precept of the CIA triad would have been violated

Answer: Integrity

Question A major Metropolitan police department gets a warrant from a judge to hack into the computer of a suspected crime boss. A skilled penetration tester working for the department conducts the hack and retrieves incriminating evidence. What color hat does this officer wear

Answer: A White Hat

Question: Which three are resources that are available to help guide penetration testing efforts by cybersecurity specialist?

- Answer:
- NIST SP 800-42 Guidelines on Network Security Testing
- Open source security testing Methodology Manual (OSSTMM)
- Federal Financial institutions examination council(EFIEC) information technology Examination.

Question: which hacker organization hacked into the Democratic National Convension and released Hillery Clinton's Email?

- Answer: Fancy Bears

Question: which challenges are expected in the future?

- Answer:
- Enhanced espionage from more countries
- Far more advanced malware
- New consumer technology to exploit

Question:
why are cyber-attacks using SWIFT so dangerous?

- Answer: SWIFT is the protocol used by all banks to transfer money.

Question: Authentication?

- Answer: Assurance that the communicating entity is the one claimed

Question: Trusted functionality, security audits trails and security recovery are all examples of which type of security mechanism?

Answer: Passive security mechanism

Question: An attack that is developed particularly for a specific customer and occurs over a long period of time is a form of what type of attack?

- Answer: Advanced Persistent Threat

Question: A political motivation is often attributed to which type of actor?

- Answer: Hactivist

Question: Which Type of actor hacked the 2016 US Presidential elections?

- Answer: Government

Question: True or False: Passive attacks are easy to detect because the original message are usually altered or undelivered?

- Answer: False

Question: Trusted functionality, security labels, event detection and security audits trails are all considered which?

- Answer: Pervasive security mechanism

Question: Cryptography, digital signatures, access controls and routing controls considered which?

- Answer: Security Specific Mechanism

Question: Traffic flow analysis is classified as which?

- Answer: A Passive Attack

Question: Police and training can be classified as which form of threat control?

- Answer: Administrative controls

Question: Which type of attack can be addresses using a switched Ethernet gateway and software on every host on your network that makes sure their NICs is not running in promiscuous mode?

- Answer: Packet Sniffing

Question: A flood of maliciously generated packets swamp a receiver's network interference preventing it from responding to legitimate traffic. This is characteristic of which form of attack?

- Answer: A denial of Service attack (DOS)

Question: A person calls you at work and tells you he is a lawyer for your company and that you need to send him specific confidential company documents right away, or else! Assuming the caller is not really a lawyer for your company but a bad actor, what kind of attack is this?

Answer: A social Engineering attack

Question: True or False: An individual hacks into a military computer and uses it to launch an attack on a target he personally dislikes. This is considered an act of cyberwarfare ?

- Answer: False

Question: What are the three types of modern encryption?

- Answer:
- 1. Hash
- 2. Symmetric
- 3. Asymmetric

Question: What is Locard's exchange possible

- Answer: The perpetrator of a crime will bring something into the crime scene and leave with something from it, and both can be used as forensic evidence.

Question: Types of firewall?

- Answer:
- Application firewall
- Packet-filtering

Question: Which type of data does a packet-filtering firewall inspect when it decides whether to forward or drop a packet?

- Answer:
- Source an destination IP addresses
- TCP/UDP source and destination port numbers.
- ICMP message type
- TCP SYN and ACK bits

Question: Limitations of Application gateways?

- Answer:
- Client software must be “smart” and know to contact the gateway.
- Application gateway are susceptible to IP spoofing
- Each application to be managed needs its own gateway.

Question: Which type of firewall inspects XML packet payload for things like executable code, a target IP address that make sense and a known source IP address?

- Answer: An XML Gateway.

Question: Stateful firewalls

- Answer: They have state tables that allow them to compare current packets with previous packets.

Question: True or False: Most antivirus/ Antimalware software works by comparing a hash of every file encountered on your system against a table of hashs of known virus and malware previously made by antivirus/ antimalware vendor.

- Answer: True

Question: Which type of cryptographic attack is characterized by comparing a captured hashed password against a table of many millions of previously hashed words or strings?

- Answer: Rainbow tables