Laud Mills

1. E-commerce security has three main concepts: confidentiality, integrity, and availability. As well web-application security also depends on access control and certification. For each of the following scenarios, identify which security goal or set of goals have been violated. Give a short justification (two or three lines). The answer for the first scenario has been given for your reference. Follow a similar procedure for the remaining scenarios. Note that for most scenarios, Access Control seems to be a likely candidate for security goal violation. You will need to identify one or more security goals other than access control. For instance, when there is a DoS attack, it is a violation of availability.

|  |  |  |
| --- | --- | --- |
| **Scenario** | **Security Goal** | **Justification** |
| Bob crashes Alice’s computer system by sending a flood of packets | Availability | This is a classic case of a DoS attack and hence falls under the category of interruption. Alice’s computer is unavailable for her use and hence the security goal violated is Availability |
| Alice copies Bob’s credit card information by eavesdropping on traffic from his machine. | Confidentiality | This is typical of a Man-In-the-Middle attack. By this the attacker intercepts and changes information transmitted between Bob and the system Bob originally intends to transmit his information. |
| Bob copies Alice’s bank information by accessing her hard drive. | Confidentiality | This could be physical theft since Bob could be an insider with privileged access to Alice’s storage device. It is a data breach by theft or unauthorized access. |
| Alice changes the amount on Bob’s cheque when it is being transmitted. | Integrity | This amounts to information tempering and could be done by interception of transmitted information by an intermediary. It is typical of a Man-in-the Middle- Attack |
| Bob sends a property deed to the Registrar in the name of Alice by forging Alice’s signature. | Integrity | This is forgery. Physically altering a document to appear as coming from a person for gains. |
| Alice spoof’s Bob’s IP address to gain access to his office server. | Confidentiality | IP spoofing is the attack here. This occurs when message is intercepted as a result of the attacker managing to act as a legitimate network between two systems. |
|  |  |  |
| Bob installs malware on Alice’s computer. | Confidentiality  Integrity  Availability | Malware installation can be done physically or remotely due to privilege escalation. When malware is successfully installed on Alices Computer, the main issue here will be confidentiality, but the facts of system integrity and availability cannot be overruled. |
| Bob obtains Alice’s credit card information online and has the credit card company replace it with another card bearing a different account number | Integrity | This is typical of an identity theft and will result in alteration of what is originally known to Alices service providers. |
| Alice has a fake third party authenticate her server as legitimate. | Integrity | Impersonation is at play here. Once she’s authenticated successfully, the system integrity is flawed. |

1. For each of the following attacks, identify which security goal or set of goals have been violated and provide the prevention tools/techniques.

|  |  |  |
| --- | --- | --- |
| **Attacks** | **Security Goal** | **Prevention Techniques** |
| Eavesdropping | Confidentiality | End to end Encryption |
| Address spoofing | Confidentiality  Integrity | Implementing Internet Protocol Security (IPSEC) |
| Man-in-the-middle attacks | Confidentiality | TLS/SSL, HTTPS |
| Denial-of-service attacks | Availability | Firewall/WAF |
| Sniffer attacks | Confidentiality | TLS/SSL, HTTPS |

1. The following is a hypothetical story of how a group of hackers infiltrated into Company TechNet’s network and launched a variety of intrusions. Read the story carefully. The sentences in the storyline have been numbered. You must identify the name of any one tool/technique/attack type used by the hackers for each one of the numbered storylines. The answer to the first numbered sentence is given. Follow a similar procedure for the remaining ones.

Here is the story: The group of hackers, named Crackers, had been eyeing TechNet for a while.

* 1. First, they found out the IP addresses and blocks of IP addresses used by TechNet literally looking over a network administrator’s shoulder.
  2. Driving around the company premises, they used a tool to determine the SSID information of TechNet’s wireless network by sending probes.
  3. They dug through the corporate trash and pieced together bits of shredded paper. They were able to determine the names of a few employees.
  4. Using a fake email then they were able to gain access of Apache webserver.
  5. One of the hackers went to the reception area of TechNet, pretending to have a newly appointed compliance auditor and gained the access of there Financial Statements.
  6. They were able to learn the username and password of the employee by creating fake Web sites equipped with forms to capture user information, and thus infiltrated the company’s network.
  7. They sniffed traffic on the local network and captured packets.
  8. They transmitted the captured packets onto the company’s database server and got connected. From this connection, they were able to transfer funds out of the company.
  9. Finally, they repeatedly sent webpage requests to TechNet’s web server and shut it down.

|  |  |  |
| --- | --- | --- |
| **Sentence Number** | **Question** | **Name of the tool/technique/Attack** |
| 1 | What social engineering technique is this | Shoulder surfing |
| 2 | What is the name of this type of technique? | Wifi sniffing/war driving |
| 3 | What social engineering technique did they use? | Dumpster Diving/Information gathering |
| 4 | What attack did they use? | phishing |
| 5 | What social engineering technique is this? | pretexting |
| 6 | What attack did they use? | phishing |
| 7 | What tool did they use? | Packet sniffing |
| 8 | What is the name of this type of attack? | Packet injection |
| 9 | What attack did they use? | Denial of service attack |