TRAP AND TRACE SYSTEMS

An extension of the attractant -based technologies in the preceding section, trap and trace applications are growing in popularity. These systems, often simply referred to as trap and trace, use a combination of techniques to detect an intrusion and then to trace incidents back to their sources. The trap usually consists of a honey pot or padded cell and an alarm.

While the intruders are distracted, or trapped, by what they perceive to be successful intrusions, the system notifies the administrator of their presence. The trace feature is an extension to the honey pot or padded cell approach. Similar in concept to caller ID, the trace is a process by which the organization attempts to determine the identity of someone discovered in unauthorized areas of the network or systems. If this individual turns out to be someone inside the organization, the administrators are completely within their power to track the individual down and turn them over to internal or external authorities. If the individual is outside the security perimeter of the organization, then numerous legal issues arise.

It includes a companion product, ManTrap, which is the honey pot application and thus presents a virtual network running from a single server. ManHunt is an intrusion detection system with the capability of initiating a track back function that can trace a detected intruder *as* far as the administrator wishes. Although administrators usually trace an intruder back to their organization's information security boundary, it is possible, with this technology, for them to coordinate with an ISP that has similar technology and thus hand off a trace to an upstream neighbor.

On the surface, trap and trace systems seem like an ideal solution. Security is no longer limited to defense. Now the security administrators can go on the offense. They can track down

the perpetrators and turn them over to the appropriate authorities. Under the guise of justice, some less scrupulous administrators may even be tempted to back-hack, or hack into a hacker's system to find out as much as possible about the hacker. Vigilante justice would be a more appropriate term for these activities, which are in fact deemed unethical by most codes of professional conduct. In tracking the hacker, administrators may end up wandering through other organizations' systems, especially when the wily hacker may have used IP spoofing, compromised systems, or a myriad of other techniques to throw trackers off the trail. The result is that the administrator becomes a hacker himself, and therefore defeats the purpose of catching hackers.

There are more legal drawbacks to trap and trace. The trap portion frequently involves the use of honey pots or honey nets. When using *honey* pots and honey nets, administrators should be careful not to cross the line between enticement and entrapment. **Enticement** is the process of attracting attention to a system by placing tantalizing bits of information in key locations. **Entrapment** is the action of luring an individual into committing a crime to get a conviction. Enticement is legal and ethical, whereas entrapment is not. It is difficult to gauge the effect such a system can have on the average user, especially if the individual has been nudged into looking at the information. Administrators should also be wary of the *wasp trap syndrome.* In this syndrome, a concerned homeowner installs a wasp trap in his back yard to trap the few insects he sees flying about. Because these traps use scented bait, however, they wind up attracting far more wasps than were originally present. Security administrators should keep the wasp trap syndrome in mind before implementing honey pots, honey nets, padded cells, or trap and trace systems.

Active Intrusion Prevention

Some organizations would like to do more than simply wait for the next attack and implement active countermeasures to stop attacks. One tool that provides active intrusion prevention is known as LaBrea *(http://www.labreatechnologies.com).* LaBrea works by taking up the unused IP address space within a network. When LaBrea notes an ARP request, it checks to see if the IP address requested is actually valid on the network. If the address is not currently being used by a real computer or network device, LaBrea will pretend to be a computer at that IP address and allow the attacker to complete the TCP/IP connection request, known as the three-way handshake. Once the handshake is complete, LaBrea will change the TCP sliding window size down to a low number to hold the TCP connection from the attacker open for many hours, days, or even months. Holding the connection open but inactive greatly slows down network-based worms and other attacks. It allows the LaBrea *system* time then to notify the system and network administrators about the anomalous behavior on the network.

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf