Assignment 7
Gunnar Yonker

1.

Automated Incident Response		Manual Incident Response	
Pros	Cons	Pros	Cons
Shuts down the "attacker"	More false positives, may automatically shut off something that doesn't need to be	Human looking at it may lead to more accurate actions	Takes more time, more employees needed
Sets off an alarm – Notifies system admin	To many alarms, system admin may start ignoring them as false positives	Human investigates it and either dismisses it or takes proper action	Slower which can potentially let the attacker damage the system more
Automatic logging	Logging doesn't lead to any action	Expensive due to more time needed/employees needed	
Faster response, analyzes the traffic faster			

2.

There are a few different methods that can be used to contain an attack, one of the most common would be that of shutting down a system. If the attack is being conducted on that system, simply shutting it down will halt the attack. It will not fix the issue, but will stop it for the moment. The system can also be disconnected from the network to ensure that the attack cannot keep spreading through to other systems connected to the same network. Depending on the attack, it can also be contained by changing the firewall rules to either stop the inflow of packets to the victim machine, or the firewall could also be set to block any traffic that is coming out of the infected system. If the infected accounts are known, they can be disabled or deleted. An example of this would be a user falling victim to an email phishing attempt where they entered their username and password that the attacker then used to gain access to a database. That user's account could be disabled until it could be recovered, or it could be deleted to contain the attack. All of these methods help to limit access to valuable resources on the network/systems and can be used at different times depending on the attack taking place.

3. Honeypot deployments

Outside of External Firewall		DMZ (network of externally available services)		Fully Internal	
Pros	Cons	Pros	Cons	Pros	Cons
Does not increase risk for the internal network	Little to no ability to trap internal attackers	False positives are drastically reduced	Firewall must open up the traffic beyond what is permissible – incurs risk but makes honeypot more effective	Catches internal attacks, detects a misconfigured firewall that forwards traffic to the internal network	If honeypot is compromised the attackers can attack other internal systems
Reduces the alerts issued by the firewall		Connection from Internet to honeypot indicates probing the DMZ systems			Firewall must be adjusted to allow traffic into the honeypot – more complicated firewall rules
Attracts potential attacks					

4. The monitoring of the communications of another party are regulated by the ECPA and in this situation section 2 provides the exceptions for what situations can legally have monitoring. It says that system operators and their employees can monitor, disclose, or use the communications of other users in the normal course of performing system administration or protecting the rights of the service providers. This is the part of the ECPA that allows the use of an IDS on a system without being in a violation of privacy. It becomes illegal if an unauthorized party is monitoring the traffic and it is not the system operators and their employees doing the monitoring. Since the traffic of the system is protected through the ECPA if any Federal law enforcement entities wanted to also monitor the traffic, they would need to obtain a search warrant to do so. If the monitoring is being conducted by a system operator or the employees of the organization's system, it is legally justified.