Southern New Hampshire University

CYB 220 Project Three Technology Evaluation

Evaluation Factor	Evaluation Criteria	Network-Based Intrusion Prevention System (NIPS)	Network-Based Intrusion Detection System (NIDS)	Host-Based Intrusion Prevention System (HIPS)	Host-Based Intrusion Detection System (HIDS)
Effectiveness	Ability to identify network-connected systems	Good for many different types of systems in network	Good for many different types of systems in network	Very good for computer host that HIPS software is installed on Cannot analyze other network-connected systems	Very good for computer host that HIDS software is installed on Cannot analyze other network-connected systems
	Ability to discern operating systems of network-connected systems	Good for many different types of systems in network	Good for many different types of systems in network	Very good for computer host that HIPS software is installed on Cannot analyze other network-connected systems	Very good for computer host that HIDS software is installed on Cannot analyze other network-connected systems
	Ability to discern specific software applications based on their unique data flows	Good for many different types of systems in network	Good for many different types of systems in network	Very good for computer host that HIPS software is installed on Cannot analyze other network-connected systems	Very good for computer host that HIDS software is installed on Cannot analyze other network-connected systems
	Ability to handle encrypted data flows	Cannot step inside and analyze encrypted communications of systems in monitored network segment	Cannot step inside and analyze encrypted communications of systems in monitored network segment	Able to analyze encrypted traffic passing to and from computer that HIPS software is installed on	Able to analyze encrypted traffic passing to and from computer that HIDS software is installed on

	Reliability under stress	Somewhat reliable under stress; will lose track of individual data flows under extreme conditions	Somewhat reliable under stress; will lose track of individual data flows under extreme conditions	Somewhat reliable under stress; will lose track of individual data flows under extreme conditions	Somewhat reliable under stress; will lose track of individual data flows under extreme conditions
	Potential to cause individual network-connected system outage	Unlikely, since the NIPS acts at the network level	Unlikely, since the NIDS acts at the network level; does not interact with data flows at all	Extremely likely if HIPS software crashes and affects the computer operating system	Extremely likely if HIDS software crashes and affects the computer operating system
	Potential to cause individual network-connected system disruption/slowdown	Likely for suspicious traffic flows, or when the network is congested	Unlikely, since the NIDS software is not designed to interact directly with network traffic flows	Extremely likely if HIPS software crashes or becomes stressed, since it directly interacts with computer traffic flows	Unlikely, since the HIDS software is not designed to interact directly with computer traffic flows
	Potential cause of network outage	Extremely likely if the NIPS software crashes or mistakenly blocks important network flows because of faulty analysis or misconfiguration	Extremely unlikely, since the NIDS software is not designed to interact directly with network traffic flows	Extremely unlikely, since the HIPS software only affects the system it is installed on	Extremely unlikely, since the HIDS software only affects the system it is installed on
	Potential cause of network disruption/slowdown	Extremely likely if the NIPS software crashes or mistakenly blocks important network flows because of faulty analysis or misconfiguration	Extremely unlikely, since the NIDS software is not designed to interact directly with network traffic flows	Extremely unlikely, since the HIPS software only affects the system it is installed on	Extremely unlikely, since the HIDS software only affects the system it is installed on
	Potential cause of excessive alerts	Extremely likely with large networks or if regular tweaking or tuning isn't practiced	Extremely likely with large networks or if regular tweaking or tuning isn't practiced	Extremely unlikely, since the HIPS software only affects the system it is installed on	Extremely unlikely, since the HIDS software only affects the system it is installed on

Cost	Software	High cost for large or complex networks	Low to moderate cost for large or complex networks	High cost for environments with large numbers of computers	Low to moderate cost for environments with large numbers of computers
	Personnel (training)	Moderate skill development required for both detection and prevention technologies	Moderate skill development required for detection technologies	Moderate skill development required for both detection and prevention technologies	Moderate skill development required for detection technologies
	Deployment (time to implement)	Significant time needed for large or complex networks	Moderate time needed for large or complex networks	Significant time needed for environments with large numbers of computers	Significant time needed for environments with large numbers of computers
	Deployment (complexity)	High complexity for large or complex networks	Moderate complexity for large or complex networks	High complexity if there is a need for centralized monitoring	High complexity if there is a need for centralized monitoring