SANS-GCIA 503 Intrusion Detection(PDFs)

by analyzing these attack paths and generating false and valid responses, the security professional can create a comprehensive security policy to protect against the majority of attacks. more importantly, an audit is able to objectively identify a range of vulnerabilities and priorities for remediation. this paper illustrates how unix system administration tools can be used by a penetration tester to perform both functional and security audits. two types of unix audit are illustrated here: general and enhanced. audit results are presented for each type of audit and included are descriptions of the kinds of data required for each type of audit and examples of successful and unsuccessful audit results. this paper studies the targeted adaptive filtering and intrusion detection frameworks. the authors discuss the challenges of this field in terms of function and performance, which are evaluated with the following tools: ida pro, lookout, snort, and surbl, that implement different algorithms for tcp stream filtering. based on the work of snort, surbl, and lookout, this paper explores the real-time detection of "java deserialization" attacks and presents a framework of several practical building blocks for delivering highly efficient and accurate real-time detection of java deserialization attacks. analysis is conducted on two actual java deserialization attacks, using surbl. many protocols share the same format of data packets, including the udp, tcp, and http protocols. so, a workable solution must be able to identify the protocol from a packet that is being analyzed. this paper presents a method for classifying a packet, and provides information for selecting an appropriate solution depending on the type of packet being analyzed.

SANS-GCIA 503 Intrusion Detection(PDFs)

a side effect of this intrusion is that many hosts or computers on the internal network now think they are using or being addressed by a domain name that is not on this host. because of this, we recommend that you ask your internet service provider if the problem is on their end. this attack type requires an attacker to identify weaknesses in security settings on the firewall or other system which reduces the effectiveness of the firewall. administrators should make sure to check system time settings and closely monitor log files. if any access to the network is allowed to databases, web servers, or other systems on the internal network, update log files or host security settings. the command-line interface accepts input from file, stdin, and command-line parameters. administrators should make sure that the command-line is disabled and that no syslog running on the host is receiving log messages from this host. a side effect of this attack is that many hosts or computers on the internal network now think they are using or being addressed by a domain name that is not on this host. because of this, we recommend that you ask your internet service provider if the problem is on their end. an attacker can leverage an already compromised host to gain access to another host through a man-in-the-middle attack, or send a crafted email message to be delivered to the victim's intended destination. administrators should log any suspicious email messages and take appropriate remedial measures. 2009 sans institute, the publisher of the sans magazines and books, is the leading provider of information security training and information assurance software. sans institute, with headquarters at 283 municipal drive, fairfax, va 22030, conducts the majority of its training programs in florida at the sans training center in lake mary. opened in 2005, the sans training center is accredited by the acsp. 5ec8ef588b