Notes Nov 15 2018

Intrusion Detection Systems

Detection: Alert------------IDS

Prevention: Stopping------IPS

Network Intrusion Detection System- Detects intrusion and monitors traffic on a Network.

Host Intrusion Detection System – Detects intrusion and monitors the Host device.

From: a,b,c,d:1792 From w,x,y,z,53

To: w,x,y,z,53 To: a,b,c,d:1792

Normal User 🡪 DNS Server (IP: w,x,y,z) 🡪 IP:

Figure 7.7 Amplified Attack

* Attacker 🡪 Zombies

DNS Amplification Attacks

* Use packets directed at a legitimate DNS server as the intermediary system.

DoS Attack Defenses

* Four lines of defense against DDoS attacks
  + Attack prevention and preemption
    - Before attack
  + Attack detection and filtering
    - During the attack
  + Attack source traceback and identification
    - During and after the attack
  + Attack reaction
    - After the attack
* These attacks cannot be prevented entirely
* High traffic volumes may be legitimate
  + High publicity about a specific site
  + Activity on a very popular site
  + Described as slash dotted, flash crowd, or flash event.

Class of Intruders – Cyber Criminals

* Individuals or members of an organized crime group with a goal of financial reward
* Their activities may include
  + Identity theft
  + Theft of financial credentials
  + Corporate espionage
  + Data theft

Classes of Intruders – Activists

* Are either individuals usually working as insiders or members of a larger group of outsiders attackers, who are motivated

Classes of Intruders – State-Sponsored Organizations

* Groups of hackers sponsored by govern

Class of intruders – Others

* Hackers with motivations other than those previously listed
* Include classic hackers or

Intruder Skill Levels – Apprentice

* Hackers with minimal technical skill who primarily use existing attack toolkits
* They likely comprise

Intruder Skill Levels – Journeyman

Examples of Intrusion

* Remote root compromise
* Web server defacement
* Guessing/cracking passwords
* Copying databases containing credit card numbers
* Viewing sensitive data without authorization
* Running a packet sniffer
* Distributing pirated software
* Using an unsecured

Intruder Behavior

* Target acquisition and information gathering
* Initial access
* Privilege escalation
* Information gathering or system exploit
* Maintaining access
* Covering tracks

Table 8.1 Examples of Intruder Behavior

* Target acquisition and information gathering
  + Explore corporate website for information on corporate structure, personnel, key systems, as well as details of specific web server and OS used.
  + Gather

Definitions

* Security Intrusion:
  + Unauthorized act of bypassing the security mechanisms of a system

Intrusion Detection System (IDS)

* Host-based IDS (HIDS)
  + Monitors the characteristics of a single host for suspicious activity
* Network-based IDS (NIDS)
  + Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity
* Distributed or hybrid IDS
  + Combines information from a number of sensors, often both host and network based, in a central analyzer

Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

* Probability density function
* Profile of intruder behavior
* Profile of authorized user behavior

IDS Requirements

* Run continually
* Be fault tolerant
* Resist subversion
* Impose a minimal overhead on system
* Configured according to system security policies
* Adapt to changes in systems and users
* Scale to monitor large numbers of systems
* Provide graceful

Analysis Approaches

* Anomaly detection
  + Involves the collection of data relating to the behavior of legitimate users over a period of time.
  + Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder
* Signature/Heuristic detection
  + Uses a set

Anomaly Detection

* A variety of classification approaches are used:
  + Statistical
    - Analysis of the observed behavior using univariate multivariate, or time-series models of observed metrics
  + Knowledge based
    - Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior
  + Machine-learning
    - Approaches automatically determine a suitable classification model from the training data using data mining techniques.

Table 8.2

Honeypots

* Decoy systems designed to:
  + Lure a potential attacker away from critical systems
  + Collect information about the attacker’s activity
  + Encourage the attacker to stay on the system long enough for administrators to respond
  + Systems are filled with fabricated information that a legitimate user of the system wouldn’t access.
* Resources that have no production value
  + Therefore, incoming communication is most likely a probe, scan, or attack.
  + Initiated outbound communication suggests that the system has probably been compromised.

Honeypot Classifications

* Low interaction honeypot
  + Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems
  + Provides a less realistic target
  + Often sufficient for use as a component of a distributed IDS to warn of imminent attack.

Figure 8.8 Example of Honeypot Deployment

* Internet 🡪HoneyPot or External Firewall 🡪 LAN Switch 🡪

Figure 8.9 Snort Architecture

* Packet 🡪 Decoder 🡪 Detection Engine 🡪

Figure 8.10

* Action,

Table 8.3 Snort Rule Actions

* Action

Table 8.4 Examples

Summary

* Intruders