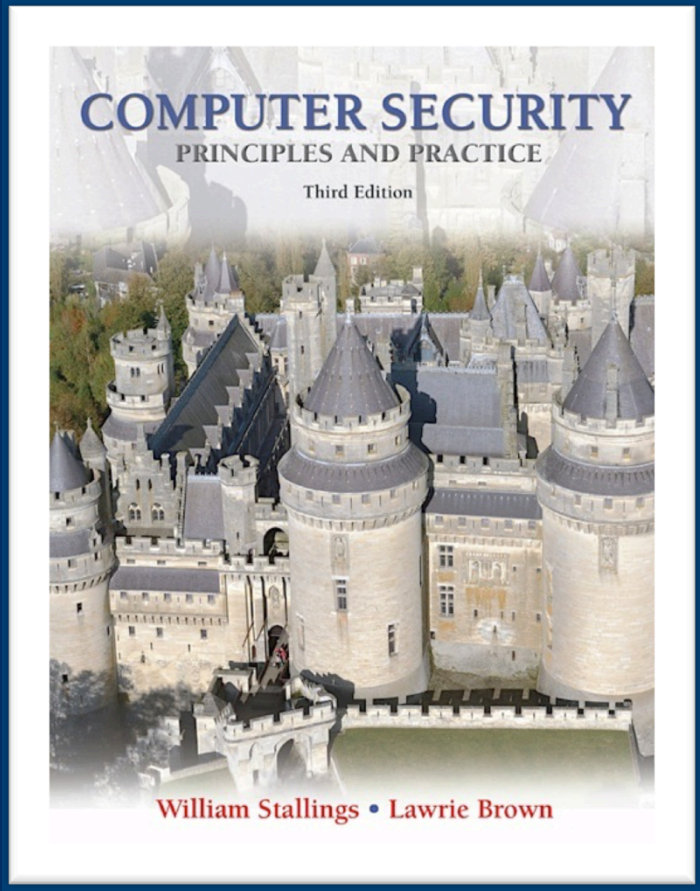
Lecture 18
Intrusion Detection



modified from slides of Lawrie Brown

Definition

- A significant security problem for networked systems; hostile, or at least unwanted, trespass by users or software
- Trespass
  - Unauthorized login (user)
  - Authorized user: acquisition of privileges beyond authorization (user)
  - Take the form of virus, worm or Trojan horse (software)

Classes of Intruders

- Cyber criminals
- Activists
- State-sponsored organizations
- Others

Classes 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
  - Data theft
  - Data ransoming
- They meet in underground forums to trade tips and data and coordinate attacks

Classes of Intruders – Activists

- Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes
- Also know as hacktivists
    - Skill level is often quite low
- Aim of their attacks is often to promote and publicize their cause typically through:
    - Website defacement
    - Denial of service attacks
    - Theft and distribution of data that results in negative publicity or compromise of their targets

Classes of Intruders – State-Sponsored

- Groups of hackers sponsored by **governments** to conduct sabotage activities

Classes of Intruders – Others

- Hackers with motivations other than those previously listed
- Include classic hackers or crackers who are motivated by technical challenge or by peer-group esteem and reputation
- Many of those responsible for discovering new categories of buffer overflow vulnerabilities could be regarded as members of this class
- Given the wide availability of attack toolkits, there is a pool of “hobby hackers” using them to explore system and network security

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 modem to access internal network
- impersonating an executive to get information
- using an unattended workstation

Intruder Behavior

Target acquisition and information gathering

Initial access

Privilege escalation

Information gathering or system exploit

Maintaining access

Covering tracks

Examples of Intruder Behavior

(a) 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 information on target network using DNS lookup tools such as dig, host, and others; and query WHOIS database.
- Map network for accessible services using tools such as NMAP.
- Send query email to customer service contact, review response for information on mail client, server, and OS used, and also details of person responding.
- Identify potentially vulnerable services, eg vulnerable web CMS.

(b) Initial Access

- Brute force (guess) a user's web content management system (CMS) password.
- Exploit vulnerability in web CMS plugin to gain system access.
- Send spear-phishing email with link to web browser exploit to key people.

(c) Privilege Escalation

- Scan system for applications with local exploit.
- Exploit any vulnerable application to gain elevated privileges.
- Install sniffers to capture administrator passwords.
- Use captured administrator password to access privileged information.

(d) Information Gathering or System Exploit

- Scan files for desired information.
- Transfer large numbers of documents to external repository.
- Use guessed or captured passwords to access other servers on network.

(e) Maintaining Access

- Install remote administration tool or rootkit with backdoor for later access.
- Use administrator password to later access network.
- Modify or disable anti-virus or IDS programs running on system.

(f) Covering Tracks

- Use rootkit to hide files installed on system.
- Edit logfiles to remove entries generated during the intrusion.

(Table can be found on pages 271-272 in textbook.)

Intrusion Detection

- **Intrusion Detection** : A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intrusion Detection Systems (IDSs)

- host-based IDS
  - monitors the characteristics of a single host suspicious activity
- network-based IDS
  - 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, in a central analyzer that is able to better identify and respond to intrusion activity

Intrusion Detection Systems (IDSs)

- comprises three logical components:
  - Sensors
    - collect data
  - analyzers
    - determine if intrusion has occurred
  - user interface
    - view output or control system behavior

IDS Principles

- assume intruder behavior differs from legitimate users
- overlap in behaviors causes problems
  - false positives
  - false negatives

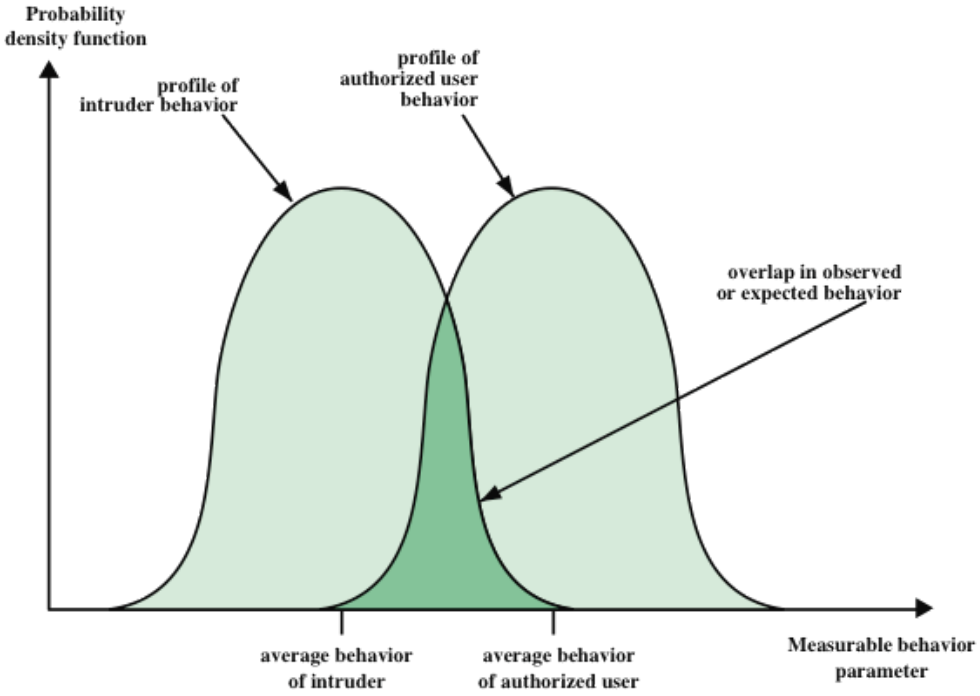


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

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 degradation of service
- allow dynamic reconfiguration

Analysis Approaches

Anomaly detection

- Involves the collection of data relating to the **behavior of legitimate users** over a period of time
- Then 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 of **known malicious data patterns** or attack rules that are compared with current behavior
- Can only identify known attacks for which it has patterns or rules

Anomaly Detection

- A variety of classification approaches are used:

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

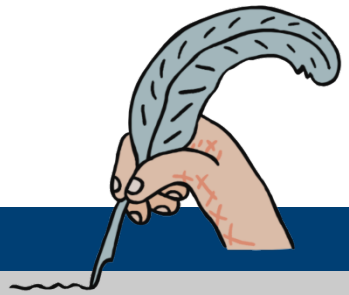
Signature or Heuristic Detection

Signature approaches

Match a large collection of known patterns of malicious data against data observed in a system or in transit over a network

The signatures need to be large enough to minimize the false alarm rate, while still detecting a sufficiently large fraction of malicious data

Widely used in anti-virus products, network traffic scanning proxies



Disadvantage?

Rule-based heuristic identification

Involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses

Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage

Typically rules used are specific

SNORT is an example of a rule-based NIDS

- Host-based intrusion detection
- Network-based intrusion detection
- Distributed/hybrid intrusion detection

Host-Based IDS

- adds a specialized layer of security software to vulnerable or sensitive systems
- Can use either anomaly or signature and heuristic approaches
- monitors activity to detect suspicious behavior
  - primary purpose is to detect intrusions, log suspicious events, and send alerts
  - can detect both external and internal intrusions

(a) Ubuntu Linux System Calls

accept, access, acct, adjtime, aiocancel, aioread, aiowait, aiowrite, alarm, async_daemon, auditsys, bind, chdir, chmod, chown, chroot, close, connect, creat, dup, dup2, execv, execve, exit, exportfs, fchdir, fchmod, fchown, fchroot, fcntl, flock, fork, fpathconf, fstat, fstat, fstatfs, fsync, ftime, ftruncate, getdents, getdirentries, getdomainname, getdopt, getdtablesize, getfh, getgid, getgroups, gethostid, gethostname, getitimer, getmsg, getpagesize, getpeername, getpgrp, getpid, getpriority, getrlimit, getrusage, getsockname, getsockopt, gettimeofday, getuid, gtty, ioctl, kill, killpg, link, listen, lseek, lstat, madvise, mctl, mincore, mkdir, mknod, mmap, mount, mount, mprotect, mpxchan, msgsys, msync, munmap, nfs_mount, nfssvc, nice, open, pathconf, pause, pcfs_mount, phys, pipe, poll, profil, ptrace, putmsg, quota, quotactl, read, readlink, readv, reboot, recv, recvfrom, recvmsg, rename, resuba, rfssys, rmdir, sbreak, sbrk, select, semsys, send, sendmsg, sendto, setdomainname, setdopt, setgid, setgroups, sethostid, sethostname, setitimer, setpgid, setpgrp, setpgrp, setpriority, setquota, setregid, setreuid, setrlimit, setsid, setsockopt, settimeofday, setuid, shmsys, shutdown, sigblock, sigpause, sigpending, sigsetmask, sigstack, sigsys, sigvec, socket, socketaddr, socketpair, sstk, stat, stat, statfs, stime, stty, swapon, symlink, sync, sysconf, time, times, truncate, umask, umount, uname, unlink, unmount, ustat, utime, utimes, vadvise, vfork, vhangup, vlimit, vpixsys, vread, vtimes, vtrace, vwrite, wait, wait3, wait4, write, writev

(b) Key Windows DLLs and Executables

comctl32
kernel32
msvcpp
msvcrt
mswsock
ntdll
ntoskrnl
user32
ws2_32

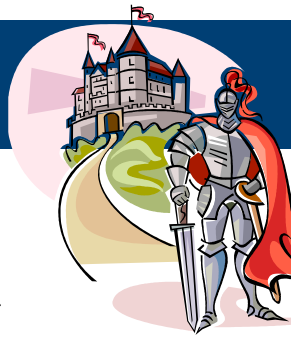
A fundamental component of intrusion detection is the sensor that collects data. One of the data sources is the system calls.

Linux System Calls and Windows DLLs Monitored

(Table can be found on page 280 in the textbook)

- Host-based intrusion detection
- Network-based intrusion detection
- Distributed/hybrid intrusion detection

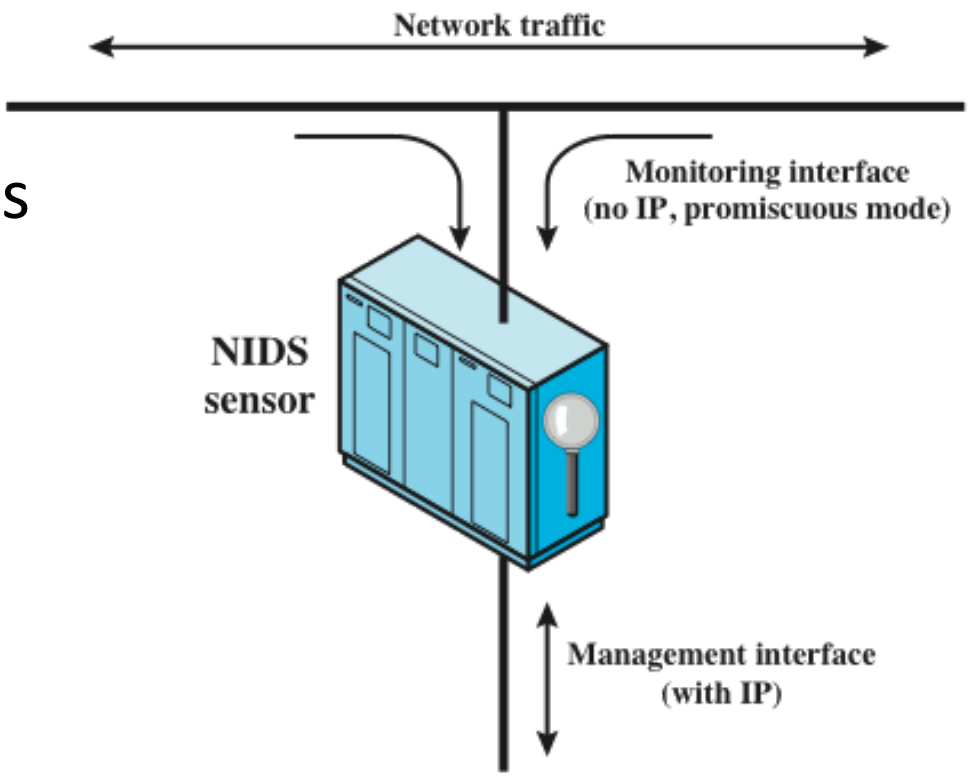
Network-Based IDS (NIDS)



- monitors traffic at selected points on a network
- examines traffic packet by packet in real or close to real time
- may examine network, transport, and/or application-level protocol activity
- comprised of a number of sensors, one or more servers for NIDS management functions, and one or more management consoles for the human interface
- analysis of traffic patterns may be done at the sensor, the management server or a combination of the two

Types of NIDS Sensor

- inline sensor
  - inserted into a network segment so that the traffic that it is monitoring must pass through the sensor
- passive sensors
  - monitors a copy of network traffic



NIDS Sensor Deployment Example