Computer Security – Principles and Practice (Pearson, fourth edition)

W. Stallings, L. Brown

* These slides are an adaptation of the original slides of the authors of the book

Intrusion detection

1

Learning objectives

- types of intruder behavior patterns;
- principles of and requirements for intrusion detection;
- key features of host-based intrusion detection;
- distributed host-based intrusion detection;
- key features of network-based intrusion detection;
- intrusion detection exchange format;
- honeypots;
- Snort

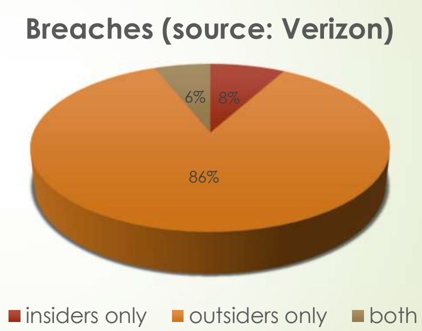
3

Intruders

4

Classes of Intruders – Cyber Criminals

- One of the key threats to security is the use of some form of hacking by an intruder (AKA hacker or cracker).
- Several reports indicate also:
  - A general increase in malicious hacking activity
  - An increase in attacks specifically targeted at individuals in organizations and the IT systems they use.



- … but insiders were responsible very large dataset compromises.

5

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
  - Corporate espionage
  - Data theft
  - Data ransoming
- Often they are young, eastern European, or southeast Asian hackers, who do business on the Web
- They meet in underground forums to trade tips and data and coordinate attacks

6

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

7

Classes of Intruders – State-Sponsored Organizations

Groups of hackers sponsored by governments to conduct espionage or sabotage activities

Also known as Advanced Persistent Threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class

Widespread nature and scope of these activities by a wide range of countries from China, Russia, USA, UK, and their intelligence allies

8

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

9

Intruder Skill Levels – Apprentice

- Hackers with minimal technical skill who primarily use existing attack toolkits
- They likely comprise the largest number of attackers, including many criminal and activist attackers
- Given their use of existing known tools, these attackers are the easiest to defend against
- Also known as "script-kiddies" due to their use of existing scripts (tools)

10

Intruder Skill Levels – Journeyman

- Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities
- They may be able to locate new vulnerabilities to exploit that are similar to some already known
- Hackers with such skills are likely found in all intruder classes
- Adapt tools for use by others

11

Intruder Skill Levels – Master

- Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities
- Write new powerful attack toolkits
- Some of the better known classical hackers are of this level
- Some are employed by state-sponsored organizations
- Defending against these attacks is of the highest difficulty

12

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

13

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

Intruder Behavior

14

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 e-mail 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, for example, 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 e-mail with link to Web browser exploit to key people.

15

Examples of Intruder Behavior

(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.

16

Intrusion detection

17

Why intrusion detection?

- Authentication facilities, access control facilities, and firewalls all play a role in countering intrusions.
- Intrusion detection is another line of defense:
  1. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised.
  2. An effective intrusion detection system can serve as a deterrent, thus acting to prevent intrusions.
  3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen intrusion prevention measures.

Assumptions:

- The behavior of the intruder differs from that of a legitimate user in ways that can be quantified.
- Not a crisp, exact distinction between an attack by an intruder and the normal use of resources by an authorized user.

18

Intrusion Detection System (IDS)

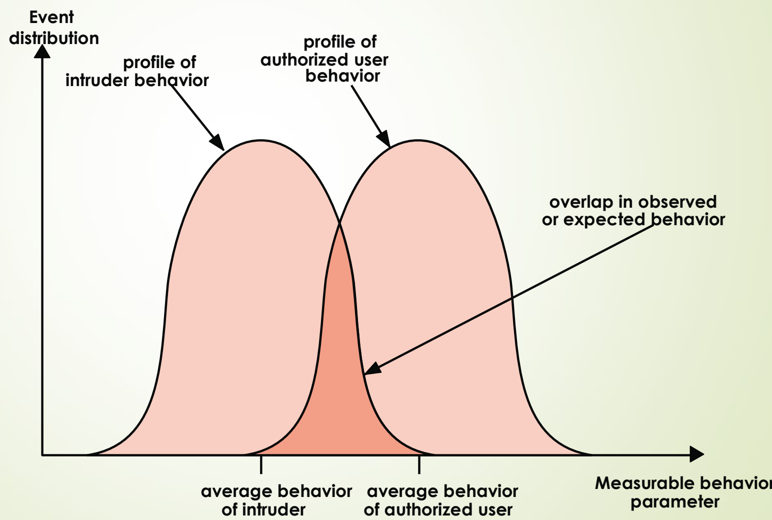
- Host-based IDS (HIDS)
  - Monitors the characteristics of a single host for suspicious activity
- Network-based IDS (NIDS)
  - Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity
- Distributed or hybrid IDS
  - Combines information from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

Comprises three logical components:

- Sensors - collect data
- Analyzers - determine if intrusion has occurred
- User interface - view output or control system behavior

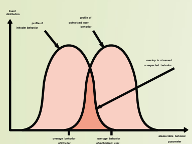
19

Profiles: intruders vs authorized users



20

Question



- Suppose there are 2 actual intrusions for every 1000 authorized users, and the overlapping area covers 1% of the authorized users and 50% of the intruders.

a) Sketch the event distribution and argue that this is not an unreasonable depiction.

b) What is the probability that an event that occurs in this region (the overlapping area) is that of an authorized user?
   - Keep in mind that 50% of all intrusions fall in this region.

21

Solution

22

Profiles of Behavior of Intruders and Authorized Users

An early study of intrusion (Anderson 1980, still valid) postulated that:

- it is possible to distinguish between an outside attacker and a legitimate user with reasonable confidence.
- Patterns of legitimate user behavior can be established by observing past history, and significant deviation from such patterns can be detected.
- Detecting an inside attacker (a legitimate user acting in an unauthorized fashion) is more difficult:
  - the distinction between abnormal and normal behavior may be small;
  - such violations would be undetectable solely through the search for anomalous behavior;
  - however, insider behavior might be detectable by an intelligent definition of the class of conditions that suggest unauthorized use.

24

The base-rate fallacy

- An IDS should detect a substantial percentage of intrusions (true positives), while keeping false alarm rate low
- If the percentage of true positives is low then the IDS may give a false sense of security
- If too many false alarms then either:
  - Lots of additional work to sort out what's happening
  - The alarms (including the real ones) will be ignored
- If the number of actual intrusions is very low, meeting this requirement becomes difficult… either:
  - IDS too discriminating
  - High false alarm rate

This is known as **base-rate fallacy**, still an open issue in current systems

25

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

26

Review question

What is an IDS in the end?

Is it a hardware appliance? A piece of software? A process? A component of an O.S. or of a firewall?

27

Analysis approaches in intrusion detection

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
- **Can detect even unknown, zero-day attacks**

Signature/heuristic detection

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior
- Also known as misuse detection
- Can only identify known attacks for which it has patterns or rules

28

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

29

Signature or Heuristic Detection

Signature approaches

- Match a large collection of known patterns of malicious data against data stored on 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, and in NIDS

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 to the machine and to the operating system
- SNORT is an example of a rule-based NIDS

30

Host-Based Intrusion Detection (HIDS)

- 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 (this is not possible with network IDS and firewalls…)

31

Data Sources and Sensors

A fundamental component of intrusion detection is the sensor that collects data

Common data sources include:

- System call traces
- Audit (log file) records
- File integrity checksums
- Registry access (Windows)

32

Anomaly HIDS

- In UNIX/Linux most effective results based on the analysis of system call traces
  - analyses sequences of system calls invoked by a process over time
  - System call traces can be produced by inserting hooks in the OS itself (e.g.BSM audit module)
  - Anomaly detection often on machine learning:
- In Windows The analysis of system calls activations does not work well:
  - Extensive use of Dynamic Link Libraries (DLL) that often hide the system calls
  - Even the analysis of the registry or of audit logs does not work very well
  - Best approaches analyze traces of DLL functions invocations (similar to Linux for the system calls)
- In all OSs: cryptographic checksums to verify integrity of files
  - Problematic that files can be legally modified (and they are many, even in the OS)

33

Linux System Calls and Windows DLLs Monitored

Ubuntu Linux system calls

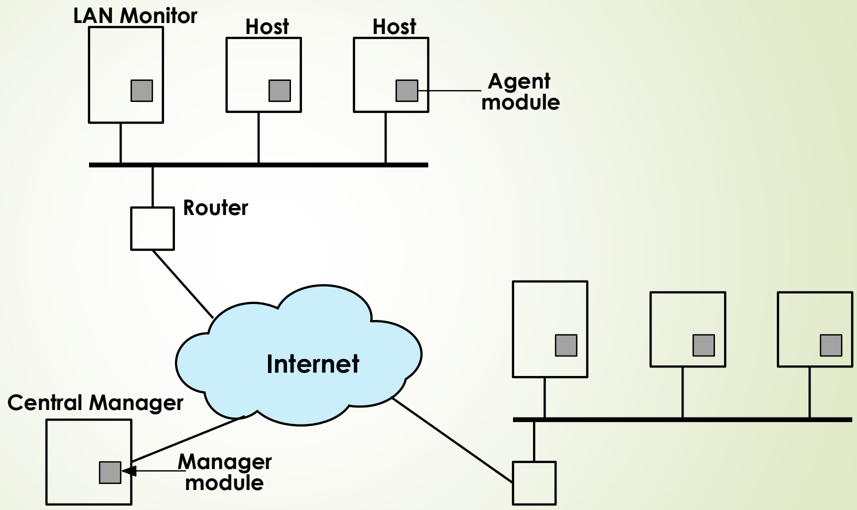
accept, access, acct, adjtime, aiocancel, aioread, aiowait, aiowrite, alarm, async_daemon, auditsys, bind, chdir, chmod, chown, chroot, close, connect, creat, dup, dup2, execv, execve, exit, exportfs, fchdir, fchmod, fchown, fchroot, fcntl, flock, fork, fpathconf, fstat, fstat, fstatfs, fsync, ftime, 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

Key Windows DLL and executables

comctl32
kernel32
msvcpp
msvcrt
mswsock
ntdll
ntoskrnl
user32
ws2_32

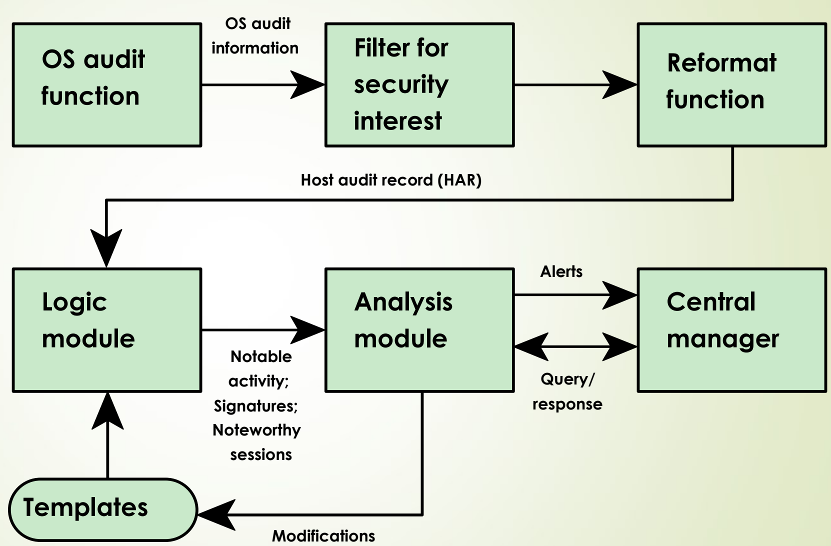
34

Architecture for distributed intrusion detection



35

Architecture for distributed intrusion detection: agent architecture



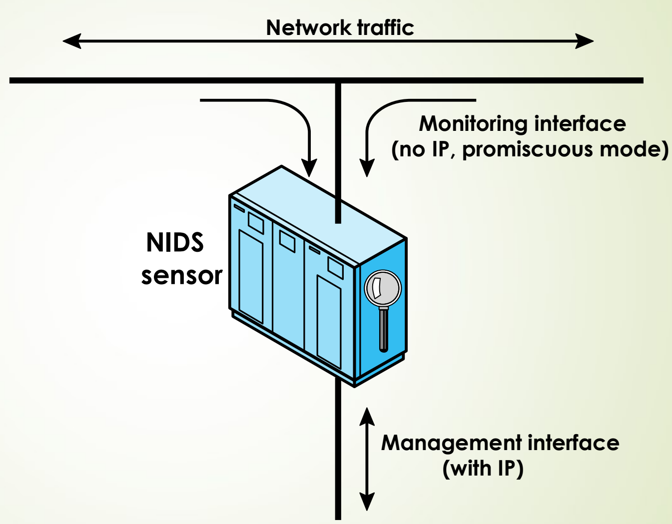
36

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
- Comprises several sensors; one or more servers for NIDS management functions; one or more management consoles for the human interface
- Analysis of traffic patterns:
  at the sensor, at the management server or a combination of the two

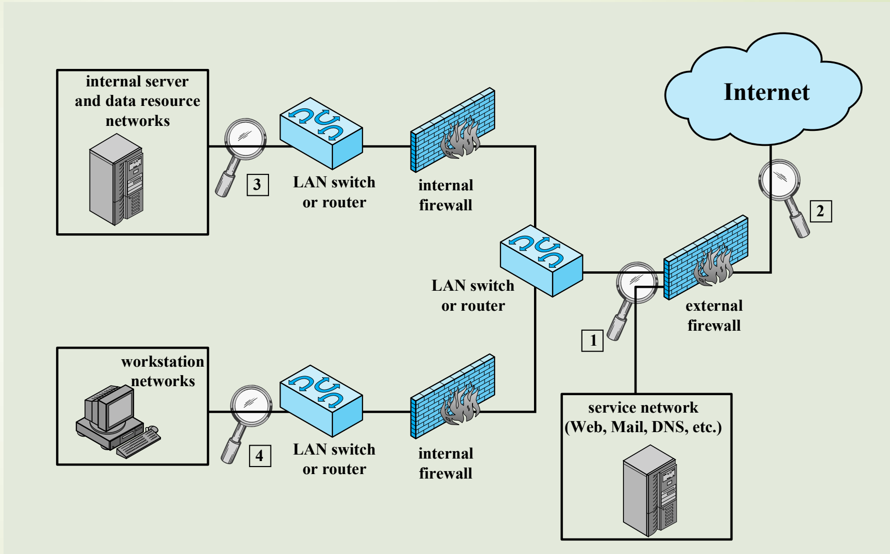
37

Passive NIDS sensors



38

Example of NIDS sensor deployment



39

Intrusion Detection Techniques (NIDS)

Attacks suitable for Signature detection

- Application layer reconnaissance and attacks
- Transport layer reconnaissance and attacks
- Network layer reconnaissance and attacks
- Unexpected application services
- Policy violations

Attacks suitable for Anomaly detection

- Denial-of-service (DoS) attacks
- Scanning
- Worms

40

Stateful Protocol Analysis (SPA)

Subset of anomaly detection:

- Compares observed network traffic against predetermined universal vendor supplied profiles of benign protocol traffic
  - Different than anomaly techniques trained with organization-specific traffic protocols
- Understands and tracks network, transport, and application protocol states to ensure they progress as expected
- A key disadvantage is the high resource use it requires

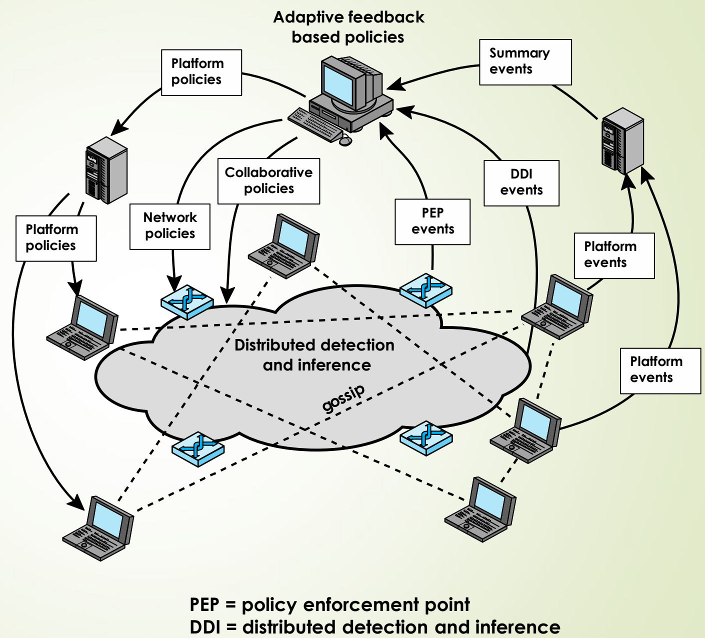
41

Logging of Alerts

- Typical information logged by a NIDS sensor includes:
  - Timestamp
  - Connection or session ID
  - Event or alert type
  - Rating (e.g., priority, severity, impact, confidence)
  - Network, transport, and application layer protocols
  - Source and destination IP addresses
  - Source and destination TCP or UDP ports, or ICMP types and codes
  - Number of bytes transmitted over the connection
  - Decoded payload data, such as application requests and responses
  - State-related information (e.g., authenticated username)

42

Overall architecture of an autonomic enterprise security system



43

IETF Intrusion Detection Working Group

- Defines data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to management systems that may need to interact with them
- The working group issued several RFCs in 2007:

Intrusion Detection Message Exchange Requirements (RFC 4766)

- defines requirements for the **Intrusion Detection Message Exchange Format** (IDMEF)
- specifies requirements for a communication protocol for communicating IDMEF

The Intrusion Detection Message Exchange Format (RFC 4765)

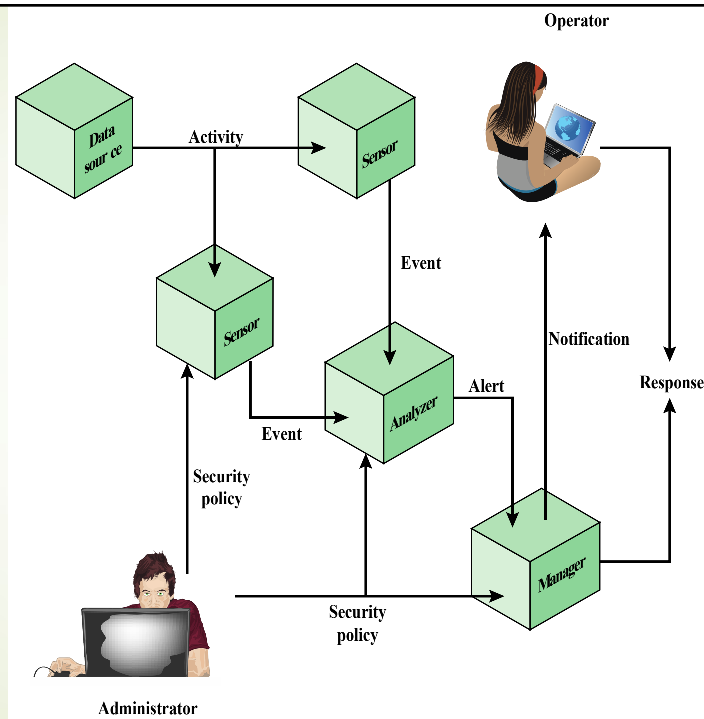
- describes a data model to represent information exported by intrusion detection systems and explains the rationale for using this model
- presents an implementation of the data model in the Extensible Markup Language (**XML**) and provides an XML Document Type Definition

The Intrusion Detection Exchange Protocol (RFC 4767)

- describes the Intrusion **Detection Exchange Protocol** (IDXP): an application-level protocol for exchanging data between intrusion detection entities
- IDXP supports mutual authentication, integrity, and confidentiality over a connection-oriented protocol

44

Model for intrusion detection message exchange



45

Review question

Do you think storing log files is important in IDS?

46

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
  - Hence any incoming communication is most likely a probe, scan, or an attack
  - Initiated outbound communication suggests that the system has probably been compromised

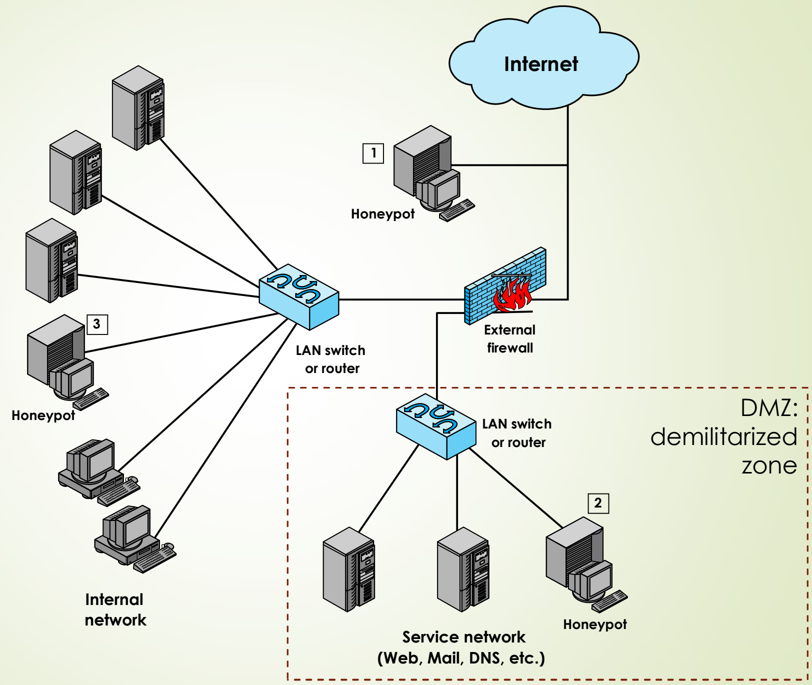
47

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
- High interaction honeypot
  - A real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers
  - Is a more realistic target that may occupy an attacker for an extended period
  - However, it requires significantly more resources
  - If compromised could be used to initiate attacks on other systems

48

Example of honeypot deployment



49

Honeywords

- Honeywords: use of several decoy accounts:
  - Each account appears legitimate and has its own password
  - Access to one of these accounts rise an alert and diverts the access to a honeypot
  - However the attacker may recognize in advance the decoy accounts…
- A possible extension consists in associating each user with multiple decoy passwords
  - If attempt to access by using a decoy password: alert and divert to honeypot
  - pseudo-passwords must be chosen in order to be easy to crack, and possibly related to the username
  - need for an external entity (Honeychecker) hosted on another OS/domain to store passwords and perform user authentication

50

The base rate fallacy

58

Conditional probability

- We often want to know a probability that is conditional on some event.
- The effect of the condition is to remove some of the outcomes from the sample space.
- Example: what is the probability of getting a sum of 8 on the roll of two dice if we know that the face of at least one die is an even number?

1. Because one die is even and the sum is even, the second die must show an even number.
2. Thus, there are three equally likely successful outcomes: (2, 6), (4, 4), and (6, 2)
3. While the total set of possibilities is [36 - (number of events with both faces odd)] = 36 - (3 * 3) = 27.
4. The resulting probability is 3/27 = 1/9.

59

Conditional probability

- the **conditional probability** of an event *A* assuming the event *B* has occurred, denoted by $\Pr[A \mid B]$, is defined as the ratio:

$$\Pr[A \mid B] = \frac{\Pr[AB]}{\Pr[B]}$$

- where we assume $\Pr[B]$ is not zero.
- In our example:
  - *A* = {sum of 8}
  - *B* = {at least one die even}.
- The quantity $\Pr[A \mid B]$ encompasses all outcomes in which the sum is 8 **and** at least one die is even.
  - As we have seen, there are three such outcomes.
- Thus, $\Pr[AB] = 3/36 = 1/12$.
- A moment's thought should convince you that $\Pr[B] = 3/4$.
- Follows that

$$\Pr[A \mid B] = \frac{1/12}{3/4} = \frac{1}{9}$$

- Which confirms the previous reasoning.

60

Conditional probability

- Two events *A* and *B* are called **independent** if

$$\Pr[AB] = \Pr[A] \cdot \Pr[B]$$

- Recall that if *A* and *B* are independent,

$$\Pr[A \mid B] = \Pr[A]$$

and

$$\Pr[B \mid A] = \Pr[B]$$

61

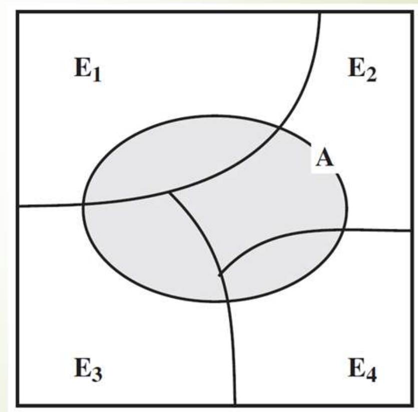
Conditional probability – Total probability

Total probability

- given a set of mutually exclusive events $E_1, E_2, \dots, E_n$,
- such that the union of these events covers all possible outcomes,
- and given an arbitrary event *A*, then it can be shown that:

$$\Pr[A] = \sum_{i=1}^{n} (\Pr[A \mid E_i] \cdot \Pr[E_i])$$

Total probability theorem illustrated



62

Conditional probability – Bayes theorem

Bayes' theorem:

- it is used to calculate "posterior odds"…
- … the probability that something really is the case, given evidence in favor of it.

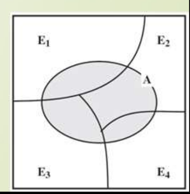
Example:

- if A happens,
- what is the probability that a given E_i is true?

The theorem may also be stated as follows:

$$\Pr[E_i \mid A] = \frac{\Pr[A \mid E_i] \cdot \Pr[E_i]}{\Pr[A]} =$$

$$= \frac{\Pr[A \mid E_i] \cdot \Pr[E_i]}{\sum_{i=1}^{n} (\Pr[A \mid E_i] \cdot \Pr[E_i])}$$



63

Conditional probability – Bayes theorem

Example:

- Suppose we are transmitting a sequence of zeroes and ones over a noisy transmission line.
  - Let S0 and S1 be, at a given time, the events a 0 is sent and a 1 is sent, respectively,
  - Let R0 and R1 be the events that a 0 is received and a 1 is received.
- Suppose we know the probabilities of the source:

$$\Pr[S1] = p \text{ and } \Pr[S0] = 1 - p$$

- … and we observe the line to determine how frequently an error occurs when a one is sent and when a zero is sent, so that the following probabilities are calculated:

$$\Pr[R0 \mid S1] = p_A \text{ and } \Pr[R1 \mid S0] = p_B$$

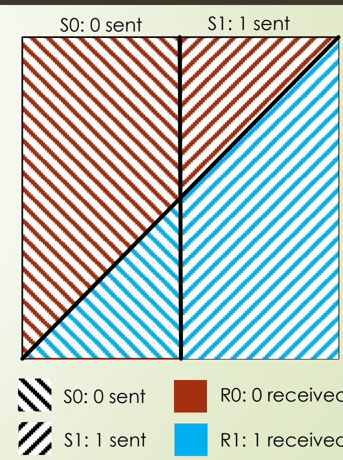
64

Conditional probability – Bayes theorem

- If a zero is received (R0), we can then calculate the conditional probability of an error, namely the conditional probability that a one was sent (S1) given that a zero was received, using Bayes' theorem:

$$\Pr[S1 \mid R0] = \frac{\Pr[R0 \mid S1] \cdot \Pr[S1]}{\Pr[R0 \mid S1] \cdot \Pr[S1] + \Pr[R0 \mid S0] \cdot \Pr[S0]} =$$

$$= \frac{p_A \cdot p}{p_A \cdot p + (1 - p_B) \cdot (1 - p)}$$



Bayes: $\Pr[E_i \mid A] = \frac{\Pr[A \mid E_i] \cdot \Pr[E_i]}{\sum_{i=1}^{n}(\Pr[A \mid E_i] \cdot \Pr[E_i])}$

65

The base rate fallacy

Consider a patient that has a test for some disease that comes back positive (indicating he has the disease). You know that:

- The accuracy of the test is 87% :
  - if a patient has the disease, 87% of the time, the test yields the correct result,
  - if the patient does not have the disease, 87% of the time, the test yields the correct result.
- The incidence of the disease in the population is 1%.

Given that the test is positive, how probable is it that the patient does not have the disease?

- That is, what is the probability that this is a false alarm?

66

The base rate fallacy

- The accuracy of the test is 87%
- The incidence of the disease in the population is 1%.

- We need Bayes' theorem to get the correct answer:

$$\Pr[well \mid positive] = \frac{\Pr[positive \mid well] \cdot \Pr[well]}{\Pr[positive \mid disease] \cdot \Pr[disease] + \Pr[positive \mid well] \cdot \Pr[well]} =$$

$$= \frac{0.13 \ \cdot 0.99}{0.87 \ \cdot 0.01 + 0.13 \ \cdot 0.99} = 0.937$$

- Which means that in most cases it's a false alarm

67

The base rate fallacy

The problem is that, when proposed to people, the answer is:

- Many subjects gave the answer 13%.
- The vast majority, including many physicians, gave a number below 50%.
- Many physicians who guessed wrong lamented,

  "If you are right, there is no point in making clinical tests!"
- The reason most people get it wrong is that they do not consider the basic rate of incidence (the base rate) when intuitively solving the problem.
- This error is known as the ***base rate fallacy***.

68

The base rate fallacy

- What happens when probabilities change?

accuracy	0,87	0,99	0,999	0,99
incidence	0,01	0,01	0,01	0,001
$Pr[well \mid positive]$ **(false alarm rate)**	0,94	**0,5**	**0,09**	0,91

- In actual situations it was found that the probabilities associated with IDSs were such that the false alarm rate was unsatisfactory.

69

Summary

- Intruders
  - Intruder behavior
- Intrusion detection
  - Basic principles
  - The base-rate fallacy
  - Requirements
- Analysis approaches
  - Anomaly detection
  - Signature or heuristic detection
- Host-based intrusion detection
  - Data sources and sensors
  - Anomaly HIDS
  - Signature or heuristic HIDS
  - Distributed HIDS
- Network-based intrusion detection
  - Types of network sensors
  - NIDS sensor deployment
  - Intrusion detection techniques
  - Logging of alerts
- Distributed or hybrid intrusion detection
- Intrusion detection exchange format
- Honeypots
- Example system: Snort
  - Snort architecture
  - Snort rules
- Base rate fallacy

70

Threat Level	Signature
Low	1 P1 + 1 P2
Medium	1 P3 + 1 P4
High	2 P4

Exercise

- A decentralized NIDS is operating with two nodes in the network monitoring anomalous inflows of traffic. In addition, a central node is present, to generate an alarm signal upon receiving input signals from the two distributed nodes.
- The signatures of traffic inflow into the two IDS nodes follow one of four patterns: P1, P2, P3, and P4 (all equiprobable).
- The threat levels are classified by the central node based upon the observed traffic by the two NIDS at a given time and are given by the above table
- If, at a given time instance, at least one distributed node generates an alarm signal P4, what is the probability that the observed traffic in the network will be classified at threat level "Medium" or "High"?

71

Solution

- The signatures of traffic inflow into the two IDS nodes follow one of four patterns: P1, …, P4.
- If,at least one node generates an alarm P4, what is the probability that the observed traffic will be classified at threat level "Medium" or "High"?

Threat Level	Signature
Low	1 P1 + 1 P2
Medium	1 P3 + 1 P4
High	2 P4

72

Exercise

- The network of an organization has two intrusion detection sensors aimed at detecting cyberattacks in real-time by means of anomaly detection. The two sensors are based on a different technology, and they have the following accuracy in the detection of DoS, worms or scan attacks:

Accuracy	DoS	Scan	Worm
Sensor1	-	0.75	0.82
Sensor2	0.79	0.91	-

- Assume that, from historical records, 10% of the attacks are DoS, 50% are Scan and 40% are worms.
- If Sensor 2 raises an alarm for a DoS attack. What is the probability this is a false positive?

74

Solution

Accuracy	DoS	Scan	Worm
Sensor1	-	0.75	0.82
Sensor2	0.79	0.91	-

10% of the attacks are DoS, 50% are Scan and 40% are worms.

If Sensor 2 raises an alarm for a DoS attack, what is the probability that it is a false positive?

75

Exercise

- The network of an organization has two intrusion detection sensors aimed at detecting cyberattacks in real-time by means of anomaly detection. The two sensors are based on a different technology, and they have the following accuracy in the detection of DoS, worms or scan attacks:

Accuracy	DoS	Scan	Worm
Sensor1	-	0.75	0.82
Sensor2	0.79	0.91	-

- Assume that, from historical records, 10% of the attacks are DoS, 50% are Scan and 40% are worms.
- If Sensor 1 raises an alarm for a worm attack, what is the probability that it is a false positive?

77

Solution

Accuracy	DoS	Scan	Worm
Sensor1	-	0.75	0.82
Sensor2	0.79	0.91	-

10% of the attacks are DoS, 50% are Scan and 40% are worms.

If Sensor 1 raises an alarm for a worm attack, what is the probability that it is a false positive?

78

Exercise

A taxicab was involved in a fatal hit-and-run accident at night. Two cab companies, the Green and the Blue, operate in the city. You are told that:

- 85% of the cabs in the city are Green and 15% are Blue.
- A witness identified the cab as Blue.

The court tested the reliability of the witness under the same circumstances that existed on the night of the accident and concluded that the witness was correct in identifying the color of the cab 80% of the time. What is the probability that the cab involved in the incident was Blue rather than Green?

80

Solution

- 85% of the cabs are Green; 15% are Blue.
- A witness identified the cab as Blue.
- the witness was correct 80% of the times.
- What is the probability that the cab involved in the incident was Blue rather than Green?

81