Computer and Network Security: Intrusion Detection System (IDS)

Kameswari Chebrolu

Outline

- What is an IDS?
- Types of IDS
- Detection Mechanisms
- Problem of Evasion
- Other Aspects

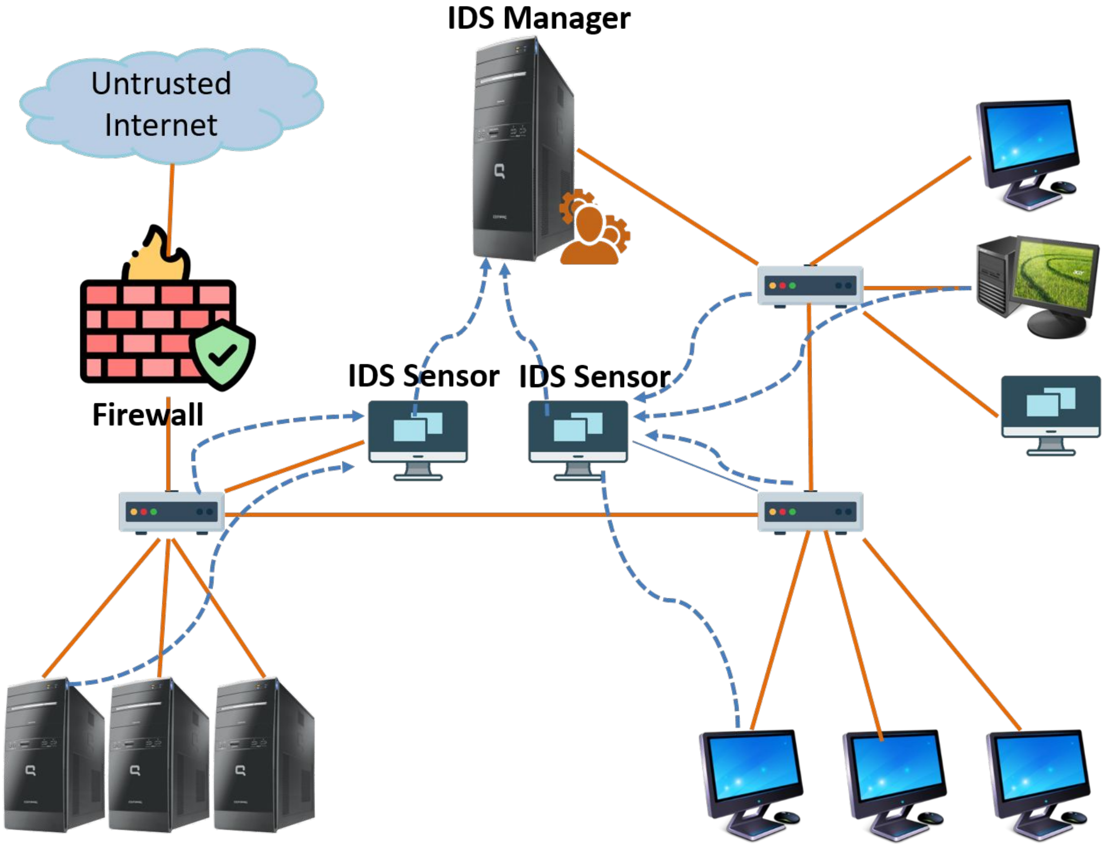
Intrusion Detection System

- Firewall is a preventive mechanism
- If a break-in happens, how to detect?
- IDS: detect signs of malicious activity
  - NIDS: detects on a network
  - HIDS: detects on a host
- Passive IDS vs Intrusion Prevention Systems (IPS)
  - Latter work with firewalls and take preemptive action
  - Example: detect DOS and update firewall

- IDS helps detect
  - Masquerader: attacker using some ones’ identity
  - Misfeasor: legitimate user performing illegal activities
  - Port scans, DOS attacks, malware, DNS pharming, ARP spoofing etc

Architecture

- Sensors: collect real-time data about component functionality
- Manager: processes data from sensors and detects intrusion



Types of IDS

- NIDS
  - deep packet inspection (e.g. character strings in packet)
  - examine correlation among multiple packets
- HIDS
  - Examine audit logs, system calls, inter-process communication

Network based IDS

- Passively observe traffic say via tcpdump
  - Unlike a firewall, it will not deny any resource
- Check for
  - unusual packet patterns
  - attack strings in packet payloads (e.g. URLs)
  - protocol violations
  - telltale sign of sniffers, port scanners etc
- Entrap attackers into revealing themselves
  - Use bogus IP addresses; username/passwords; honeypots
- Check out Snort (open source NIDS)

- Drawbacks:
  - Can’t inspect encrypted traffic
  - High overhead of processing large amount of traffic
  - Not all attacks can be caught

Host based IDS

- Based on OS monitoring mechanisms
  - Log all system events, monitor shell commands, system calls executed by applications
  - Tripwire: file integrity checker
  - Sandbox execution for selected executables
- Drawbacks:
  - Every host needs an IDS
  - An attacker with root access can tamper with logs and IDS binary

NIDS vs HIDS

- NIDS can cover lot of systems without touching end systems
- HIDS can give direct access to semantics
  - Better positioned to block attacks
  - Can detect non-network attacks
  - Can handle encrypted traffic (decrypted at host)
  - More scalable due to distributed resources

Outline

- ~~What is an IDS?~~
- ~~Types of IDS~~
- Detection Mechanisms
- Problem of Evasion
- Other Aspects

Input to IDS (Records)

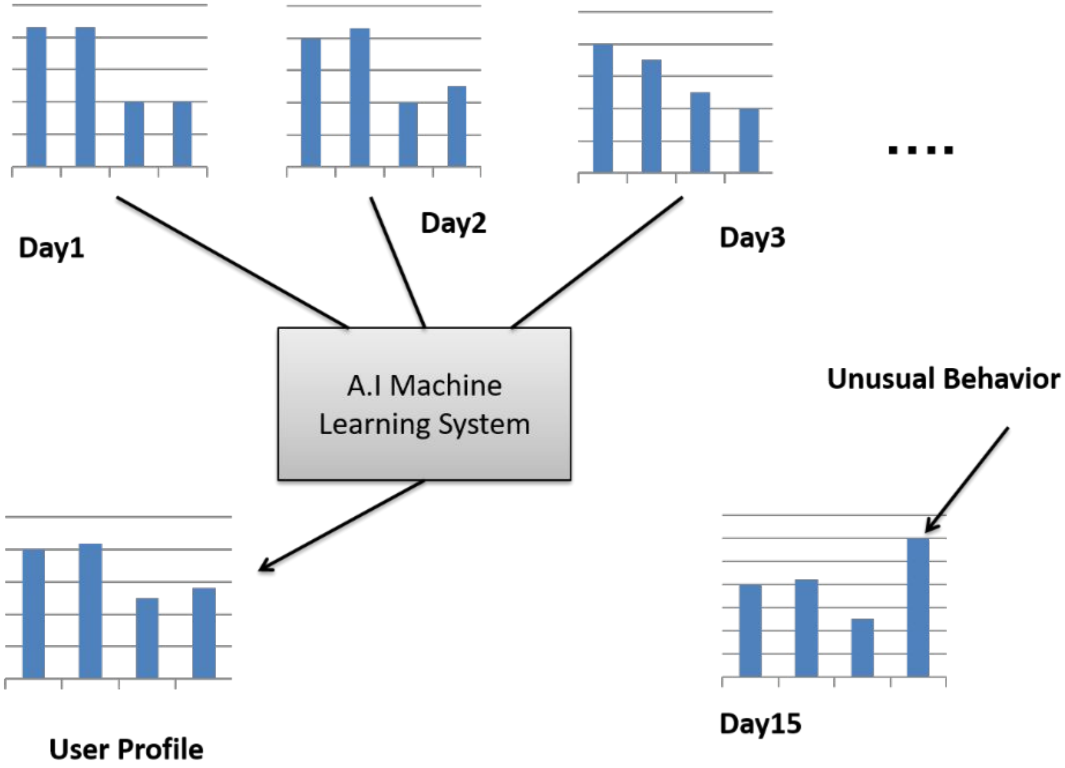
- Stream of records that identify actions for a network or host
- Several fields
  - Subject
  - Object
  - Action
  - Exception-condition
  - Resource-usage
  - Time-stamp
- Example:
  - Alice, run.exe, write, ‘no-error’, 140KB, 21/03/17-10.00am
    - Alice wrote 140KB to run.exe at the designated time without error

Signature based Detection

- Look for a pattern (invariant characteristics that translate to set of rules) that matches structure of a known attack
  - E.g. SYN flooding: Large number of SYNs and no corresponding ACKs
  - E.g. Buffer Overflow: a long argument to a string function
- Maintain a database of such signatures and process records to detect intrusions
- Disadvantages
  - Requires previous knowledge of attack (signature)
  - May miss variants of known attacks
  - May generate false alarms
  - May also get overloaded (high processing load)

Anomaly based Detection

- Develop a baseline for normal behaviour; flag activity that deviates from it
  - E.g. Distribution of characters in URL parameters
  - E.g. keystroke, log-in; mail checking patterns
- Baseline profile is statistical; built over time using ML and data mining
- Can detect new attacks
- Drawbacks:
  - Attacker can train IDS to accept activity as normal
  - Scope for false alarms
- Most IDS combine both signature and anomaly based analysis



Determine baseline (typical profile) and compare against it

Detection Accuracy

	Intrusion	No-intrusion
Alarm Sounded	True Positive	False Positive
No Alarm Sounded	False Negative	True Negative

- Detector with 0% false negatives?
  - Say it is an attack always
- Detector with 0% false positives?
  - Say no attacks always
- A good detector balances FPs and FNs

- Cost of a FP?
  - A sysad has to spend hours to check if it is an attack
- Cost of a FN?
  - Thousands of dollars in clean-up cost after an attack
- So, what is a good balance?
  - Rate of attacks an important parameter

Base Rate Fallacy

- What do you think of a detector with FP of 0.1% and FN of 1%?
- Scenario#1: 1000 audit logs /day and 1 is malicious
  - Expected FP per day = 999 * 0.1% ~ 1 (manageable)
  - Expected FN per day = 1 * 1% = 0.01 (~ 3 attacks a year)
- Scenario#2: 1000000 audit logs /day and 1 is malicious
  - Expected FP per day = 1000 (unmanageable)
  - Expected FN per day = 1 * 1% = 0.01 (~ 3 attacks a year)
- Base rate of malicious activity is very low □ FP has to be super low

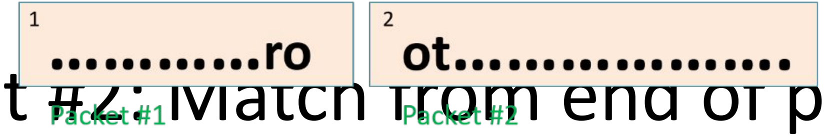
Outline

- ~~What is an IDS?~~
- ~~Types of IDS~~
- ~~Detection Mechanisms~~
- Problem of Evasion
- Other Aspects

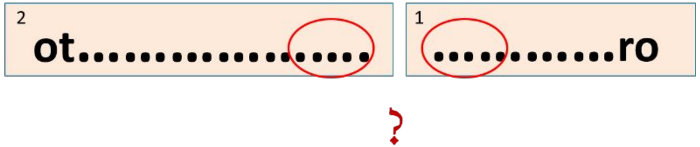
Evasion

- How can an attacker evade an IDS?
- Often possible due to imperfect observability
- Example: Detect the word “root” in a network connection
  - IDS is monitoring all packets of this connection

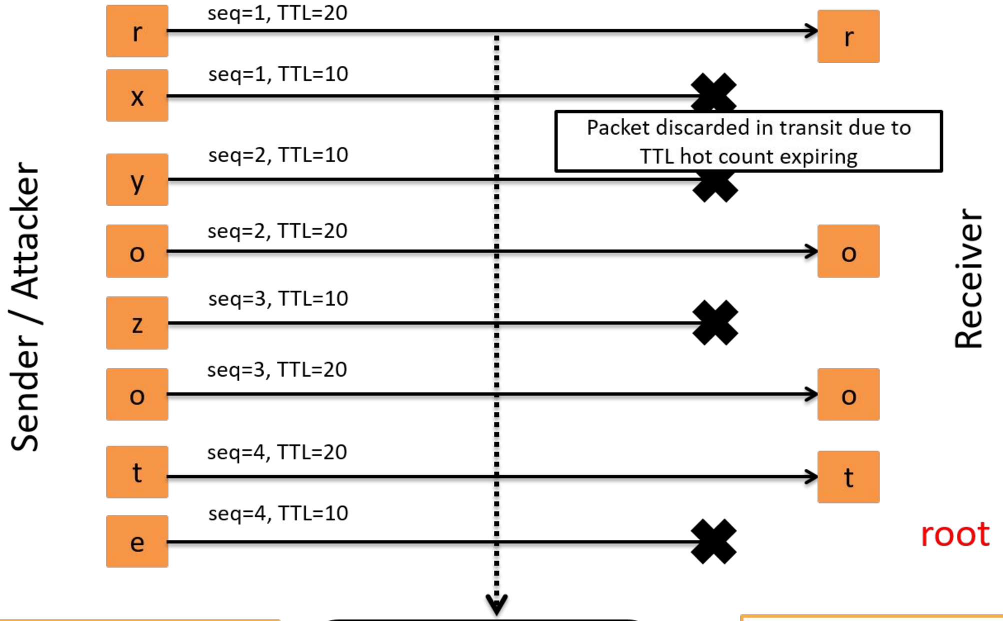
- Attempt #1: Scan each packet for the word “root”
  - TCP does not preserve text boundaries



- Attempt #2: Match from end of previous packet (requires to keep state)
  - IP can lead to packet reordering



- Attempt #3: Reassemble the entire TCP payload and scan
  - Lot of work for the IDS
  - IDS can be subject to memory exhaustion attack
  - This is also not enough



Packet discarded in transit due to TTL hot count expiring

TTL field in IP header specifies maximum forwarding hop count

Ryzt? Ryze? Xyzt? Xoze?.............

Assume the Receiver is 15 hops away

Assume the NIDS is 8 hops away

Alert odd retransmissions like this (may work for this case but not for all attacks)

IDS is hard!

Other Aspects

- Vulnerability scanning: Why wait for an attack, launch one yourself
  - Probe your system for a range of attacks and fix them
  - Widely used today
- Honeypots: Computer with ‘software vulnerabilities, seemingly important docs etc’ is used as bait for intruders
  - Any connection to honeypot □ intrusion
  - Based on how the connection is being established □ signature of attack
  - More time spent □ can detect identity of attacker
  - Can distract attacker from sensitive servers

- Forensics: Post attack, figure out nature of the attack
  - Requires rich logs and effective tools to analyze them
- IDS itself can be subject to DOS
  - Memory and processing can be targeted

Summary

- Unlike Firewalls which prevent, IDS detect malicious behavior
- Two types of IDS: Networks and Host
- Two types of detection: Signature and anomaly based
- A determined attacker can evade IDS systems