Firewalls and Intrusion Detection Systems: Part 6

Gaurav S. Kasbekar

Dept. of Electrical Engineering

IIT Bombay

References

- J. Kurose, K. Ross, “*Computer Networking: A Top Down Approach*”, Sixth Edition, Pearson Education, 2012
- B.L. Menezes, R. Kumar, “*Cryptography, Network Security, and Cyber Laws*”, Cengage Learning India Pvt. Ltd., 2018
- C. Kaufman, R. Perlman, M. Speciner, “*Network Security: Private Communication in a Public World*”, Pearson Education, 2nd edition, 2002

Types of IDS

Classification Based on Detection Method:

1) Signature-Based Systems
2) Anomaly-Based Systems

Classification Based on Where Detection Takes Place:

1) Host-Based Systems
2) Network-Based Systems

Signature-Based IDS

- Maintains an extensive database of *attack signatures*
- Each signature is a set of rules used to match a packet, or series of packets, with a known intrusion activity
- E.g.:
  - ❑ Snort is a public-domain, open source IDS
  - ❑ An example of a Snort signature is as follows
  - ❑ alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg: “ICMP PING NMAP”; dsize: 0; itype: 8;)
  - ❑ This signature is matched by any ICMP packet that enters the organization’s network ($HOME_NET) from external network ($EXTERNAL_NET), is of type 8 (ICMP ping packet) and has an empty payload (dsize = 0)
  - ❑ Since nmap generates ping packets with these specific characteristics, this signature is designed to detect nmap ping sweeps
- In general, a signature:
  - ❑ may be a list of characteristics about a single packet (e.g., source and destination port numbers, protocol type, and a specific string of bits in the packet payload)
  - ❑ or may relate to a series of packets
- Signatures are normally created by skilled network security engineers who research known attacks

Signature-Based IDS (contd.)

- A signature-based IDS operates as follows:
  - ❑ Sniffs each packet passing by it, comparing it with each signature in its database
  - ❑ If a packet (or series of packets) matches a signature in the database, the IDS generates an alert
- Examples of detection by a signature-based IDS:
  1) If attempt to establish a TCP connection is made from an external host to an internal host at unused destination port:
     - o It may indicate attempt to find which services are open
  2) If a specific byte sequence is present in the application payload of an incoming packet:
     - o It may indicate attempt to inject specific malware (e.g., virus, worm)

Signature-Based IDS (contd.)

- An attack that is undetected by a signature-based IDS is called a “false negative”
- An IDS is said to generate a “false positive” if it raises an alarm even when there is no ongoing attack
- Clearly, both false positives and false negatives should be minimized
  - however, a trade-off is involved in doing so
- E.g.:
  - Suppose packets containing a certain worm need to be filtered out by a signature-based IDS
  - The worm accesses a file called “*run.exe*”. The worm payload includes this filename
  - The IDS could be configured to filter out packets containing the string “run.exe”
  - Disadvantage of doing this:
    - Innocuous packets containing strings such as “xrun.exe”, “rerun.exe”, “newrun.exe” will be filtered out, resulting in false positives
  - Such false positives can be eliminated by making the search string more specific and changing it to: “/winXP/system32/run.exe”
  - However, now the attacker can cause a false negative to occur by:
    - using the following equivalent pathname in the body of the worm: “/winXP/system32/../system32/run.exe”

Signature-Based IDS (contd.)

- Limitations of signature-based IDS:
  - ❑They require previous knowledge of the attack to generate a signature
    - o They are unable to detect attacks that have not yet been recorded
  - ❑since each packet needs to be compared with an extensive collection of signatures, the IDS can become overwhelmed with processing and fail to detect some malicious packets in a timely manner

Anomaly-Based IDS

- Stores the statistics of traffic observed during normal operation
- Looks for packet streams that are statistically unusual, e.g.,
  - ❑ a large percentage of ICMP packets
- Advantage of anomaly-based IDS:
  - ❑ they don’t rely on previous knowledge about existing attacks
  - ❑ they can potentially detect new, undocumented attacks
- Examples of anomalous packet streams:
  1) If there is a tenfold increase over the norm in the number of accesses to a specific file:
     - o It may indicate a DoS attack
  2) If the login frequency to a particular account is unusually high:
     - o It may indicate an attempted break-in
  3) If the number of distinct source IP addresses of packets arriving into organization’s network from outside is very high:
     - o It may indicate a DDoS attack
  4) If the ratio of the number of TCP SYN packets to number of TCP FIN packets in a time interval is $\gg 1$:
     - o It may indicate a SYN flooding attack

Anomaly-Based IDS (contd.)

- Disadvantage of anomaly-based IDS:
  - ❑challenging to distinguish between normal traffic and statistically unusual traffic
- Some challenges are as follows:
  - ❑the IDS will have to learn, over time, what constitutes normal activity
  - ❑also, the definition of what is normal may vary as a function of time of day or day of the week
  - ❑what is normal may also vary from one host to another
- Hence, to date, most IDS deployments are signature-based
  - ❑however, some also include anomaly-based features

Host-Based versus Network-Based IDS

- IDS that captures information about packets flowing through the network referred to as network-based IDS
- For reasons of performance, common to have *stand-alone appliances* that perform network-based intrusion detection
    - ❑these typically run only the IDS and hence are not vulnerable to malware attacks
- Network-based IDS typically deployed at multiple points in a large organization

Host-Based versus Network-Based IDS (contd.)

- Host-based IDS:
  - ❑ typically implemented in software
  - ❑ runs as an application on a host
- Monitors the internal behavior of the host:
  - ❑ e.g., sequence of system calls made, files accessed, etc.
- Makes use of the following to identify events related to an intrusion:
  - ❑ operating system logs, application logs, etc.
- Operating system logs keep track of:
  - ❑ when users log in, number of unsuccessful login attempts, commands executed, network connections made, etc.
- Application logs keep track of:
  - ❑ the events that are logged by an application during its execution, e.g., which files it opened, which system calls it made and when
- Keeping track of modified files can play a key role in host-based intrusion detection
  - ❑ e.g., a change in the contents of core system libraries should cause suspicion since these are rarely modified, if ever
- File system integrity checkers compute a cryptographic hash on the contents of each file
  - ❑ they compare the computed hash of a file to its stored hash