Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

June 24-28, 2024

Murtuza Jadliwala

murtuza.jadliwala@utsa.edu

SPrITE LAB

UTSA

NSF

Introduction to Firewalls and IDSs

Intrusion and Intrusion Detection

The following definitions are from RFC 2828:

Security Intrusion: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

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 for suspicious activity.

- Network-based IDS

  Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity.

Comprises three logical components:

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

IDS Requirements

1. Run continually.
2. Fault-tolerance.
3. Resist subversion.
4. Impose minimal overhead on system.
5. Configured according to system security policies.
6. Adapt to changes in systems and users.
7. Scale to monitor large numbers of systems.
8. Provide graceful degradation of service.
9. Allow dynamic reconfiguration.

Approaches to Intrusion Detection

Anomaly detection

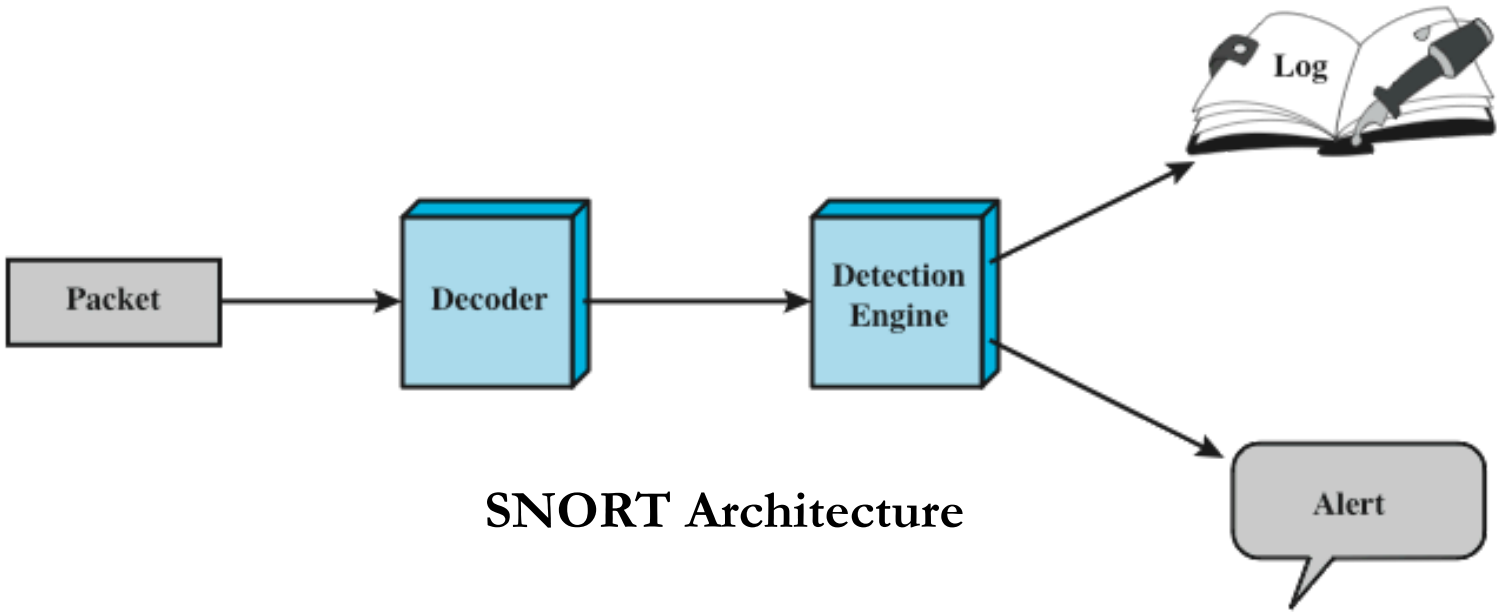
- Threshold detection
  - Involves counting the number of occurrences of a specific event type over an interval of time.
- Profile based
  - Profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

Signature detection

- Involves an attempt to define a set of rules or attack patterns that can be used to decide that a given behavior is that of an intruder.

SNORT

- Lightweight IDS
  - Open source and free!
  - Easily configurable.
  - Real-time packet capture and rule analysis.
  - Easily deployed on most nodes (host, servers, routers).
  - Uses small amount of memory and processor time.



SNORT Architecture

Action	Protocol	Source IP address	Source Port	Direction	Dest IP address	Dest Port

(a) Rule Header

Option Keyword	Option Arguments	• • •

(b) Options

SNORT Rule Formats

SNORT Rules

- Use a simple, flexible rule definition language.
- Each rule consists of a fixed header and zero or more options.

Action	Description
alert	Generate an alert using the selected alert method, and then log the packet.
log	Log the packet.
pass	Ignore the packet.
activate	Alert and then turn on another dynamic rule.
dynamic	Remain idle until activated by an activate rule , then act as a log rule.
drop	Make iptables drop the packet and log the packet.
reject	Make iptables drop the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
sdrop	Make iptables drop the packet but does not log it.

Examples of SNORT Rule Options

meta-data
msg Defines the message to be sent when a packet generates an event. **reference** Defines a link to an external attack identification system, which provides additional information. **classtype** Indicates what type of attack the packet attempted.
payload
content Enables Snort to perform a case-sensitive search for specific content (text and/or binary) in the packet payload. **depth** Specifies how far into a packet Snort should search for the specified pattern. Depth modifies the previous content keyword in the rule. **offset** Specifies where to start searching for a pattern within a packet. Offset modifies the previous content keyword in the rule. **nocase** Snort should look for the specific pattern, ignoring case. Nocase modifies the previous content keyword in the rule.
non-payload
ttl Check the IP time-to-live value. This option was intended for use in the detection of traceroute attempts. **id** Check the IP ID field for a specific value. Some tools (exploits, scanners and other odd programs) set this field specifically for various purposes, for example, the value 31337 is very popular with some hackers. **dsize** Test the packet payload size. This may be used to check for abnormally sized packets. In many cases, it is useful for detecting buffer overflows. **flags** Test the TCP flags for specified settings. **seq** Look for a specific TCP header sequence number. **icmp-id** Check for a specific ICMP ID value. This is useful because some covert channel programs use static ICMP fields when they communicate. This option was developed to detect the stacheldraht DDoS agent.
post-detection
logto Log packets matching the rule to the specified filename. **session** Extract user data from TCP Sessions. There are many cases where seeing what users are typing in telnet, rlogin, ftp, or even web sessions is very useful.

An Example SNORT Rule

Example Rule 1: alert tcp any any -> any any (msg:"This is an alert";)

Example Rule 2: alert tcp $EXTERNAL_NET any -> 192.168.10.0/24 80 (msg:"Web alert"; content:"http|3a|//www.attacker.com/execute.php"; nocase; offset:12; classtype: web-application-activity; reference:url,http://www.cs.wichita.edu/~jadliwala/details.htm; sid:2017115; rev:1;)

Firewall Design Goals

1. All traffic from inside to outside must pass through the firewall.

2. Only authorized traffic as defined by the local security policy will be allowed to pass.

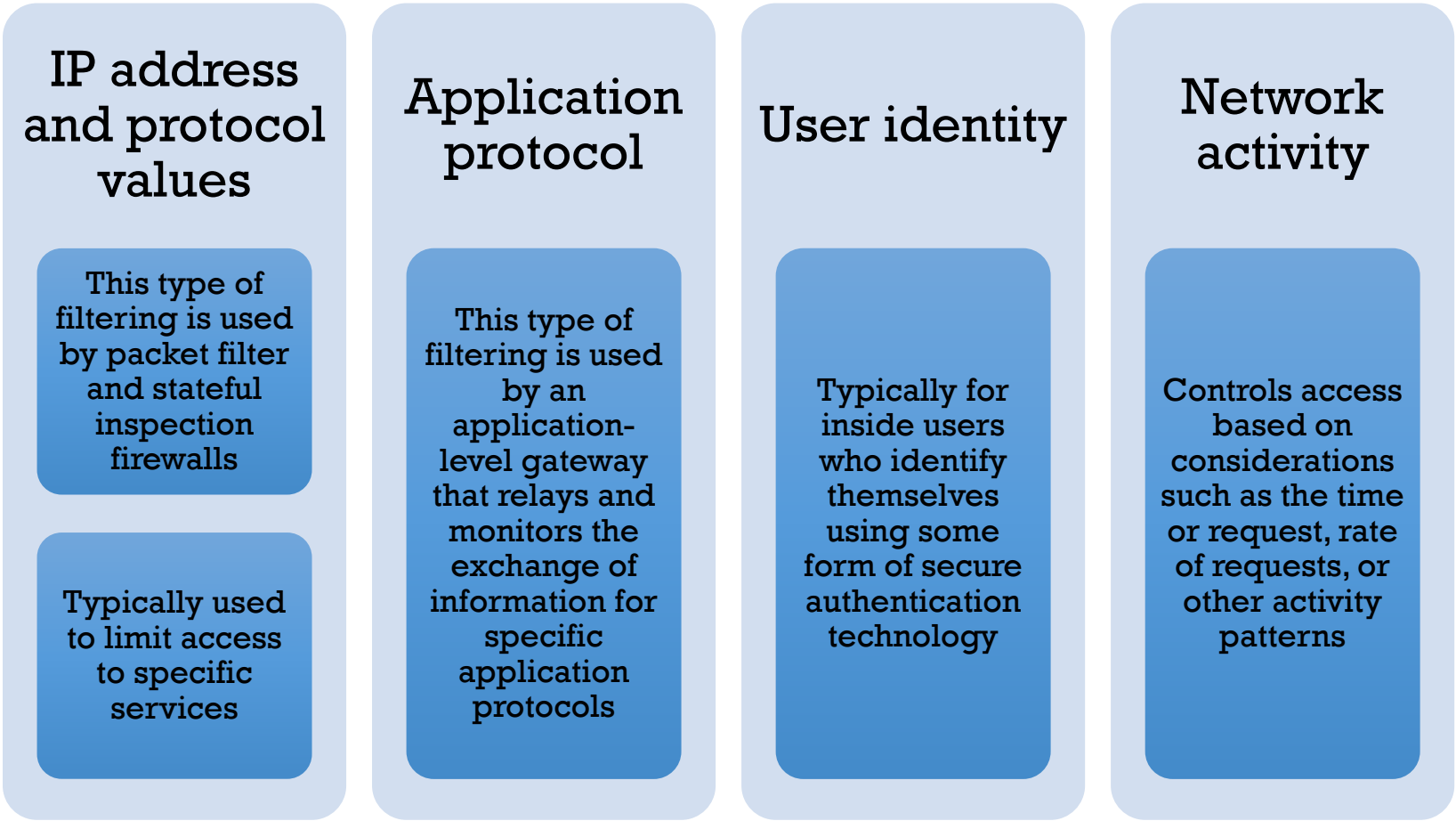
3. The firewall itself is immune to penetration.

Firewall Techniques/Control

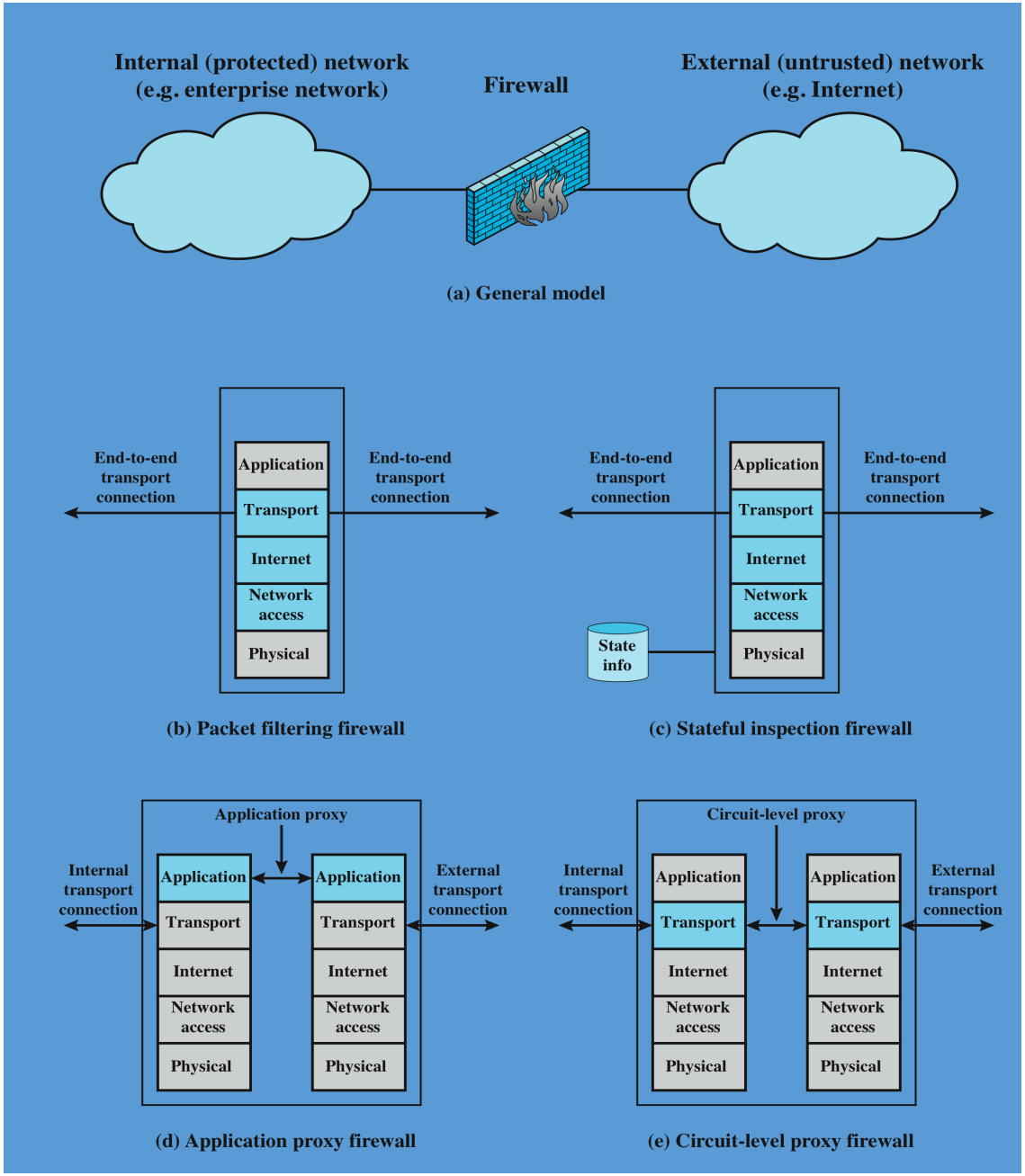
1. Service control.
2. Direction control.
3. User control.
4. Behavior control.

Firewall Filter Characteristics

- Characteristics that a firewall access policy could use to filter traffic include:

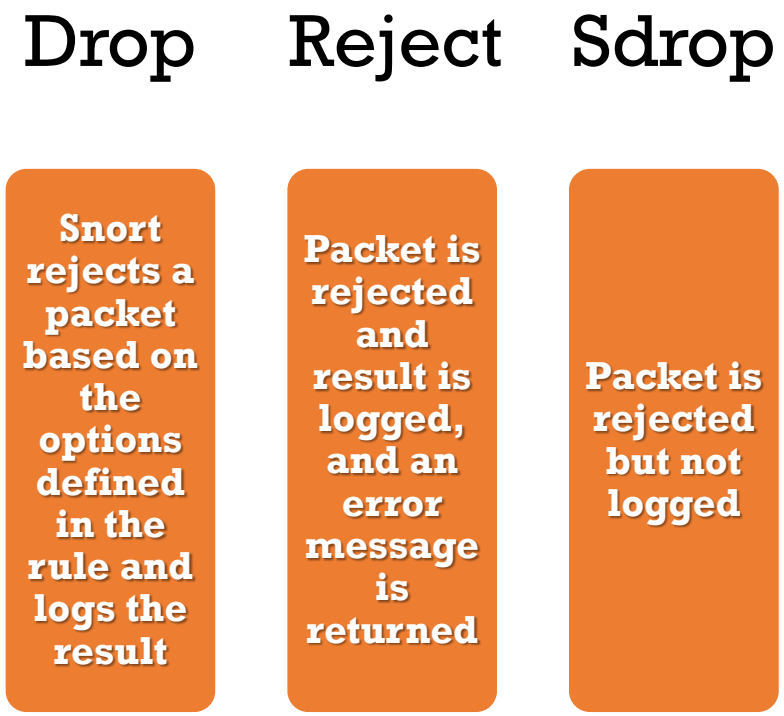


Types of Firewalls



Snort Inline

- Enables Snort to function as an intrusion prevention capability.
- Includes a replace option which allows the Snort user to modify packets rather than drop them.
  - Useful for a honeypot implementation.
  - Attackers see the failure but can't figure out why it occurred.



Questions