NETVÆRKS- OG KOMMUNIKATIONSSIKKERHED

IDS intro

Agenda

- Hand-inn exercise
- IDS

News

- Kaspersky and the NSA
  - https://www.kaspersky.com/blog/internal-investigation-preliminary-results/19894/
  - https://arstechnica.com/information-technology/2017/10/worker-who-snuck-nsa-secrets-home-had-a-backdoor-on-his-pc-kaspersky-says/

Hand-inn start-up

A midsize company requires a redesign of their network

Start with a clean slate, and create a network consisting of the following:

- 1 web server facing the www
- 1 web server for internal tools
- 2 database servers (for each webserver)
- 1 file server

- 1 sales team (~50 hosts) requiring internet access and access to local file server
- 1 technical support team (~10 hosts) requiring access to internal tools and web
- 1 development team (~10 hosts) they should have access to all systems, and have their own dev environment, consisting of a clone of the 5 servers above.
- Wifi setup for company access requiring only internet access

Hand-inn start-up

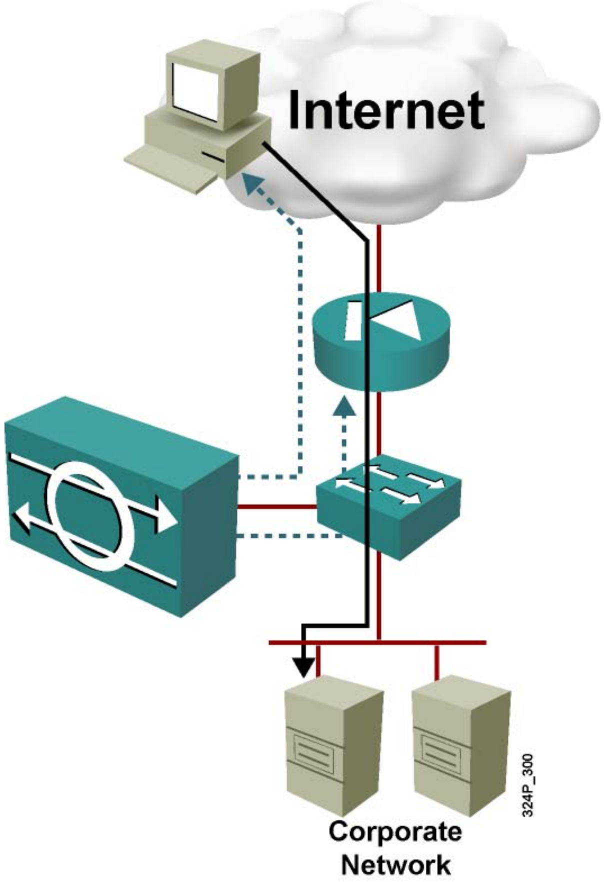
- Create a network diagram with all the components that you need (not vendor specific)
- Define the IPs for the subnets and devices
- Add the security devices you find necessary (firewalls, sensors, vpns)
- Write about your considerations (~ 1 page)

- Consider limited resources, and that we do not have all the storage in the world for storing full packet capture

- Preferably work in groups (2-3 persons)

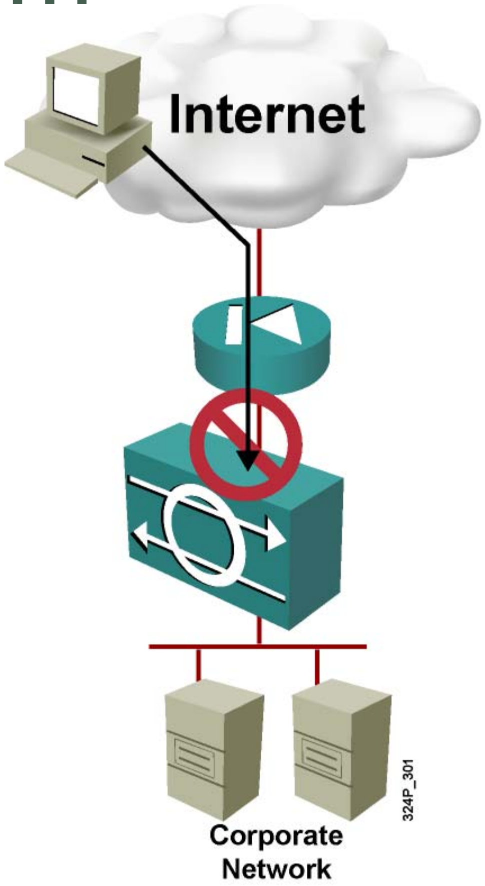
Intrusion Detection System

- IDS is a passive device:
  - Traffic does not pass through the IDS device.
  - Typically uses only one promiscuous interface.
- IDS is reactive:
  - IDS generates an alert to notify the manager of malicious traffic.
- Optional active response:
  - Further malicious traffic can be denied with a security appliance or router.
  - TCP resets can be sent to the source device.



Intrusion Protection System

- IPS is an active device:
  - All traffic passes through IPS.
  - IPS uses multiple interfaces.
- Proactive prevention:
  - IPS denies all malicious traffic.
  - IPS sends an alert to the management station.



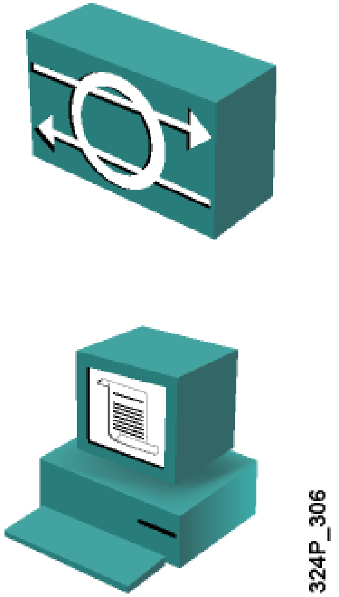
Combining IDS and IPS

- IPS actively blocks offending traffic:
  - Should not block legitimate data
  - Only stops “known malicious traffic”
  - Requires focused tuning to avoid connectivity disruption
- IDS complements IPS:
  - Verifies that IPS is still operational
  - Alerts you about any suspicious data except “known good traffic”
  - Covers the “gray area” of possibly malicious traffic that IPS did not stop

IDS and IPS Types and Options

Criteria	Type	Description
Deployment Options	Network-based	Network sensors scan traffic that is destined to many hosts.
	Host-based	Host agent monitors all operations within an operating system.
Approaches to Identifying Malicious Traffic	Signature-based	A vendor provides a customizable signature database.
	Policy-based	Policy definition and description is created.
	Anomaly-based	“Normal” and “abnormal” traffic is defined.
	Honeypot-based	Sacrificial host is set up to lure the attacker.

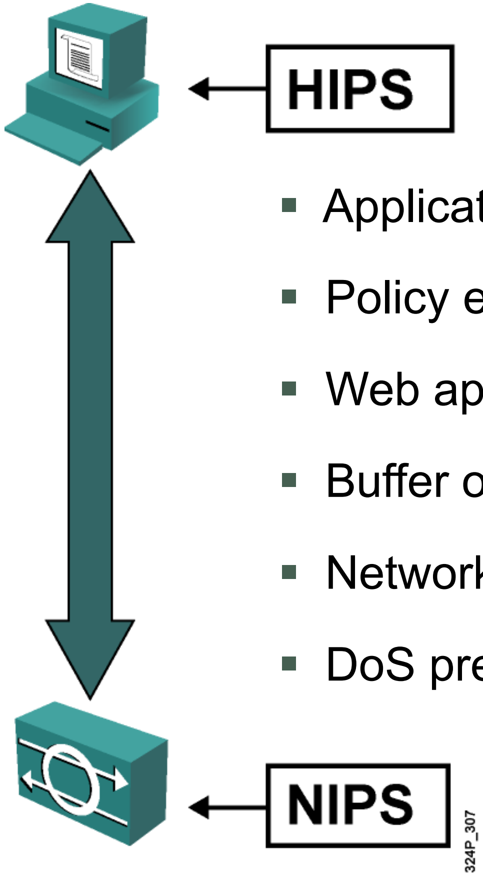
Network-Based and Host-Based IPS



- NIPS: Sensor appliances are connected to network segments to monitor many hosts.

- HIPS: Centrally managed software agents are installed on each host.
  - CSAs defend the protected hosts and report to the central management console.
  - HIPS provides individual host detection and protection.
  - HIPS does not require special hardware.

Comparing HIPS and NIPS

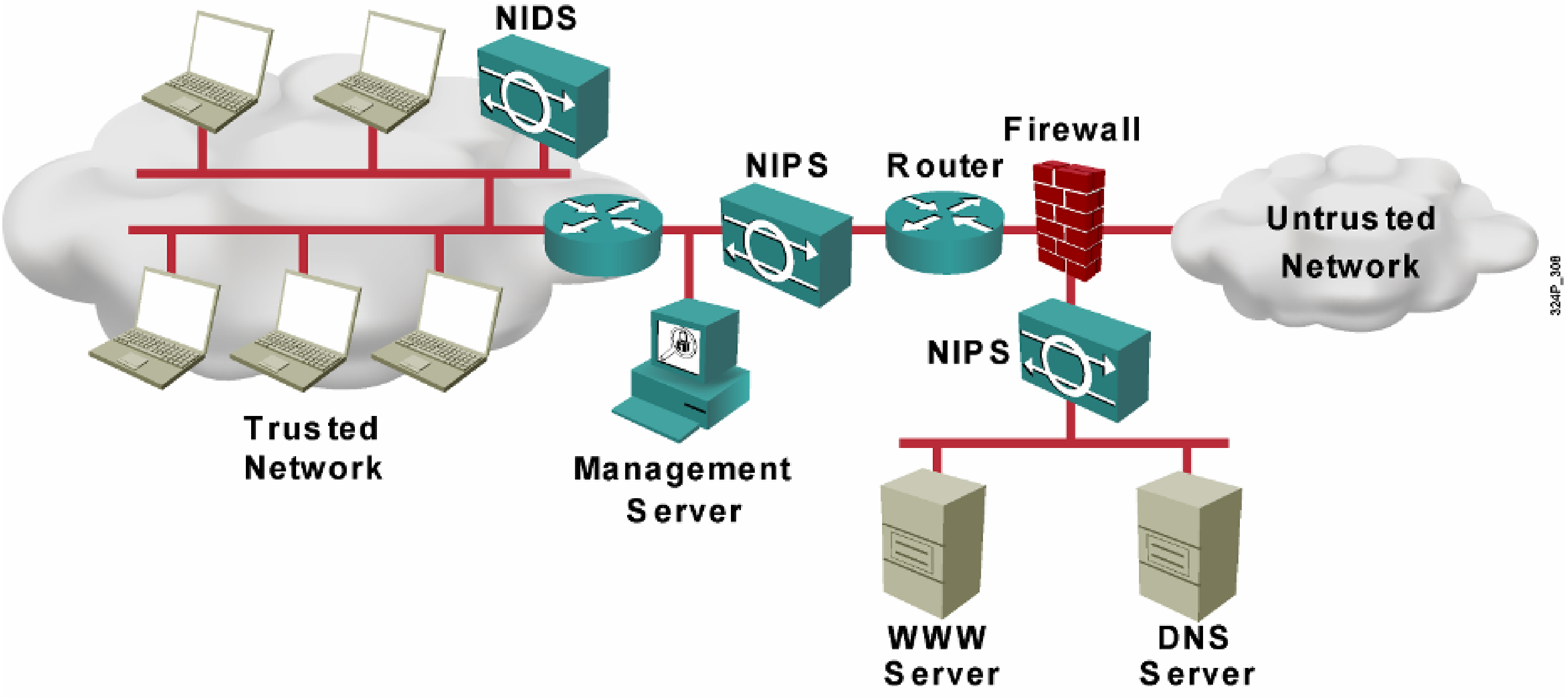


- Application-level encryption protection
- Policy enhancement (resource control)
- Web application protection
- Buffer overflow
- Network attack and reconnaissance prevention
- DoS prevention

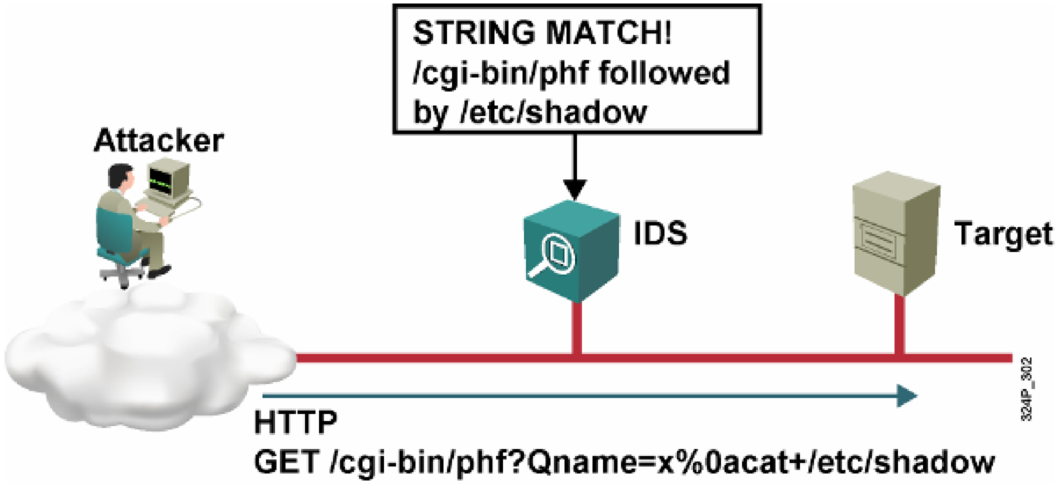
NIPS Features

- Sensors are network appliances that you tune for intrusion detection analysis:
    - The operating system is “hardened.”
    - The hardware is dedicated to intrusion detection analysis.
- Sensors are connected to network segments. A single sensor can monitor many hosts.
- Growing networks are easily protected:
    - New hosts and devices can be added without adding sensors.
    - New sensors can be easily added to new networks.

NIDS and NIPS Deployment

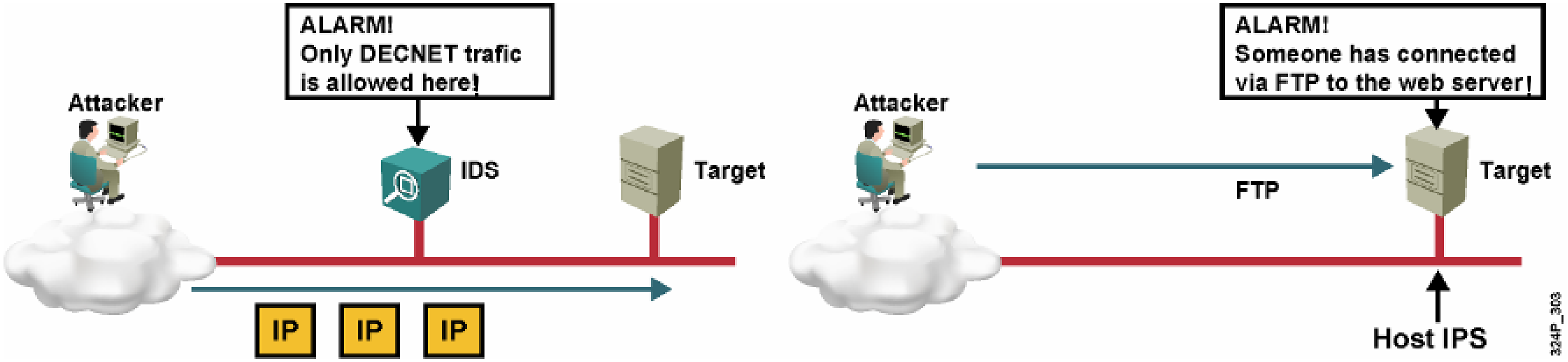


Signature-Based IDS and IPS



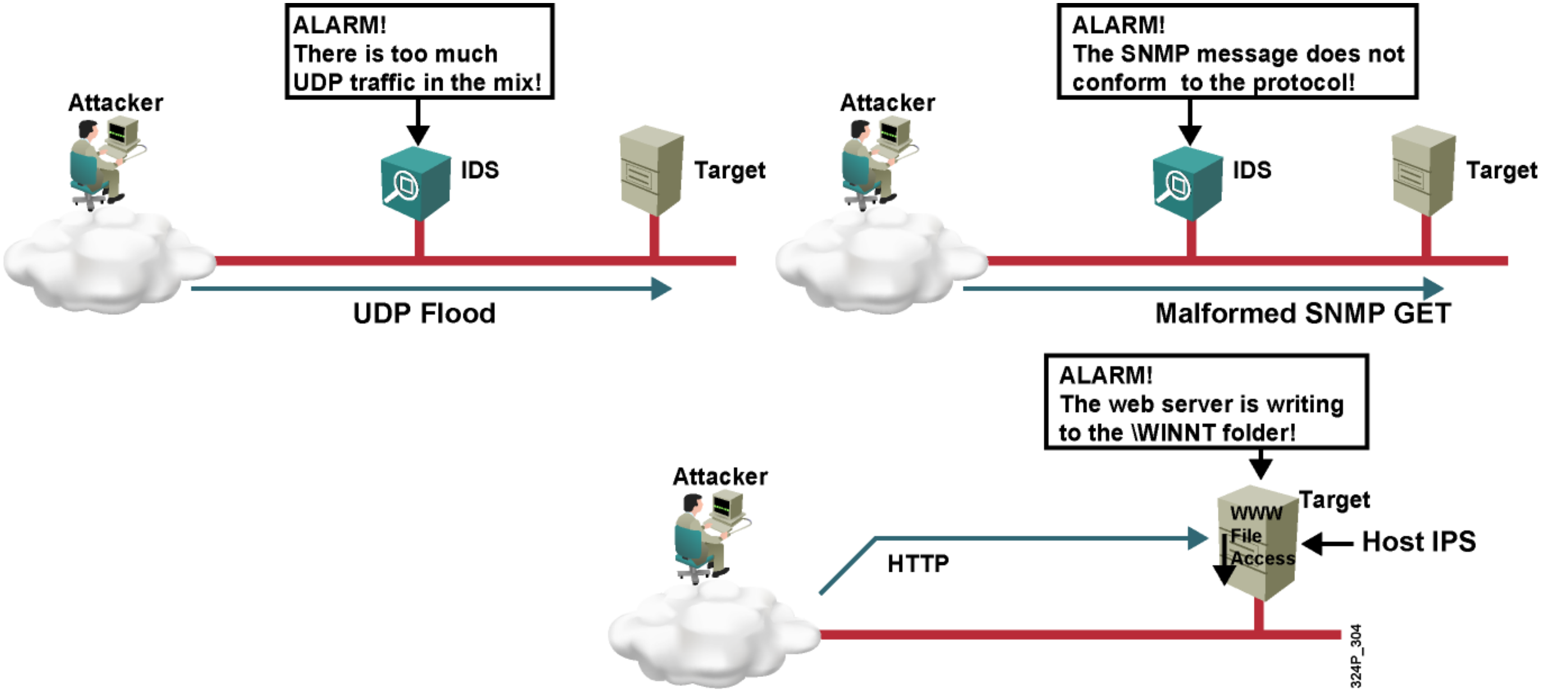
- Observes and blocks or alarms if a known malicious event is detected:
  - Requires a database of known malicious patterns.
  - The database must be continuously updated.

Policy-Based IDS and IPS


ALARM!
Only DECNET trafic is allowed here!
Attacker
IDS
Target
IP
IP
IP
ALARM!
Someone has connected via FTP to the web server!
Attacker
FTP
Target
Host IPS
324P_303

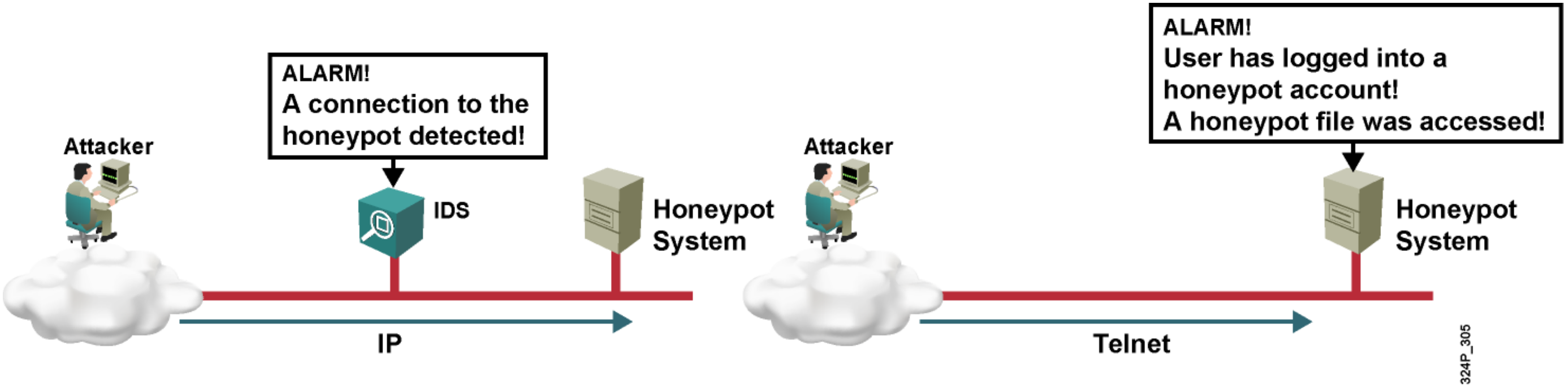
- Observes and blocks or alarms if an event outside the configured policy is detected
- Requires a policy database

Anomaly-Based IDS and IPS



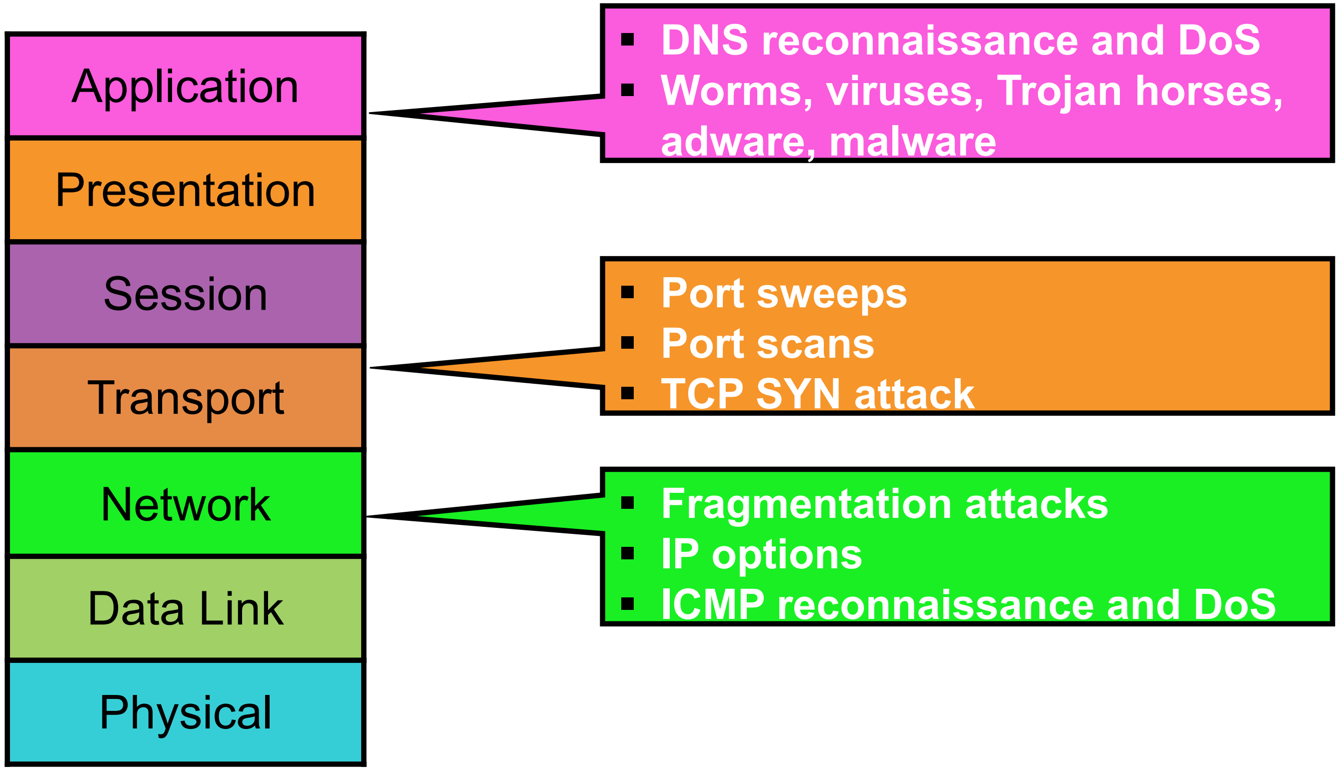
- **Observes and blocks or alarms if an event outside known normal behavior is detected:**
  - **Statistical versus nonstatistical anomaly detection**
  - **Requires a definition of “normal”**

Honeypot-Based IDS and IPS


ALARM!
A connection to the honeypot detected!
Attacker
IDS
Honeypot System
IP
ALARM!
User has logged into a honeypot account!
A honeypot file was accessed!
Attacker
Honeypot System
Telnet
324P_305

- Observes a special system and alarms if any activity is directed at the system:
  - The special system is a trap for attackers and not used for anything else.
  - The special system is well-isolated from the system’s environment.
  - The system is typically used as IDS, not IPS.

Exploit Signatures



- DNS reconnaissance and DoS
- Worms, viruses, Trojan horses, adware, malware

- Port sweeps
- Port scans
- TCP SYN attack

- Fragmentation attacks
- IP options
- ICMP reconnaissance and DoS

Signature Examples

ID	Name	Description
1101	Unknown IP Protocol	This signature triggers when an IP datagram is received with the protocol field set to 134 or greater.
1307	TCP Window Size Variation	This signature will fire when the TCP window varies in a suspect manner.
3002	TCP SYN Port Sweep	This signature triggers when a series of TCP SYN packets have been sent to a number of different destination ports on a specific host.
3227	WWW HTML Script Bug	This signature triggers when an attempt is made to view files above the HTML root directory.

Security onion

Collection of tools built on top of Ubuntu distribution

IDS/IPS

- Snort
- Suricata

Analysis

- Squert
- ELSA
- Sguil

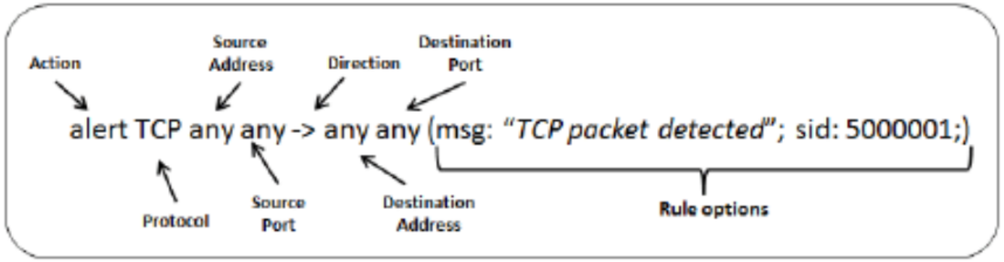
Logging

- Bro
- netsniff-ng

HIDS

- OSSEC

Snort rules



```
alert TCP any any -> any any (msg: "TCP packet detected"; sid: 5000001;)
```

Trying out the IDS

- Make sure that your security onion is fully configured.
- Try to run some of the previous commands (like nmap scans, arp poisoning etc), and see which ones it can discover.
- You can also try to run some of the sample attacks that are already there. But it is very important that you disable internet access to security onion first. (configure it to run host-only in vmware)
- `sudo tcpreplay -i eth0 -M10 /opt/samples/*.pcap`