NETVÆRKS- OG KOMMUNIKATIONSSIKKERHED

IDS intro

Agenda

- Hand-inn exercise
- Netflow
- Subnets
- IDS

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)

Full capture vs. netflow compromise

- Combining full packet captures with netflow data can be considered a optimal solution
- F.ex. Rotating Full packet capture after 1 week and netflow data after 365 days
- Setting up netflow sensors on all routers, but only full packet capture on critical segments

Components needed

- fprobe
  - This is the **exporter** that generates the netflow updates
- nfcapd
  - This is the **collector** that, accepts the updates from the exporter
- nfdump
  - This is the **analysis** tool, that enables up to query the netflow data

Setting up Netflow

- Install fprobe and nfdump

```
apt-get update
apt-get install fprobe
apt-get install nfdump
```

- Make fprobe export all traffic on eth0 as netflow to collector (running localy on port 555)

```
fprobe -i eth0 localhost:555
```

- Collect the netflow data on port 555 and write it to the disk

```
Mkdir netflow
nfcapd -D -p 555 -S 1 -z -I Linux-Host-1-eth0 -l /root/netflow/
```

Netflow from pcap

- Netflow traffic can be extracted from full packet capture using nfpcapd

```
nfpcapd –r dmp.pcap –S 1 –z –l /root/netflow/
```

Looking into Netflow

- To read the content of a specific nfdump file:

```
nfdump -r nfcapd.xxxxxxxxxx
```

- Or you could have nfdump read a whole directory

```
nfdump -R /root/netflow/*
```

- You can apply filters on the netflow output

```
nfdump -R /root/netflow/* 'host 192.168.65.133'
```

Looking into Netflow

- You can have netflow combine the unidirectional flow

```
nfdump -R netflow/* -B
```

- You can also have netflow provide you with statistical aggregation
- The following will for example give the ip address consuming most traffic in the flow

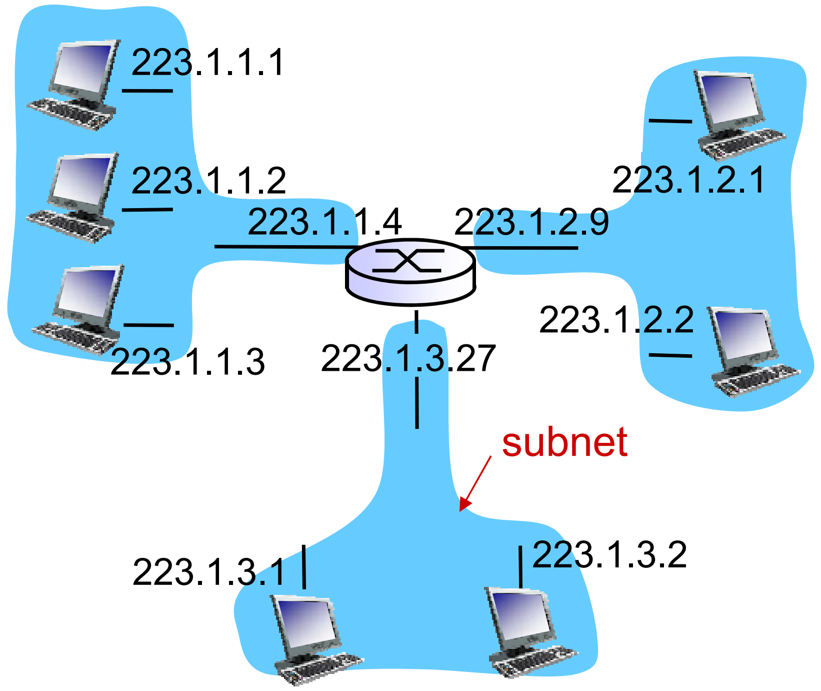
```
nfdump -R netflow/* -s ip/bytes
```

- The following will aggregate the flows by source ip, order by bytes and limit the flows displayed to 10

```
nfdump -R netflow/* -A srcip -O bytes -c 10
```

Subnets

- IP address:
  - subnet part - high order bits
  - host part - low order bits
- *what's a subnet ?*
  - device interfaces with same subnet part of IP address
  - can physically reach each other *without intervening router*

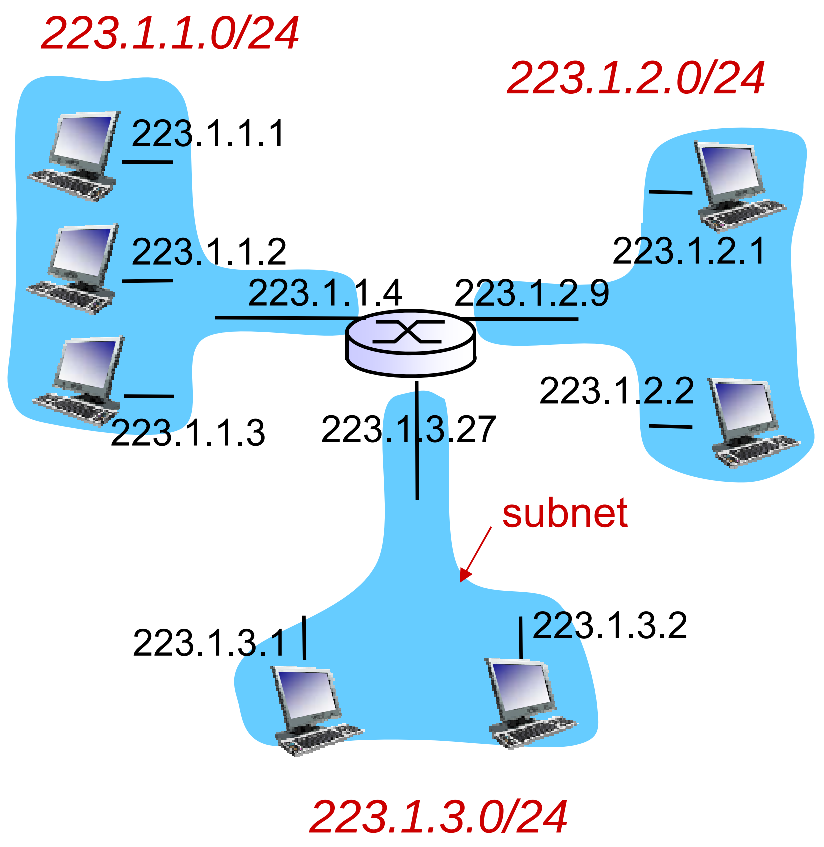


network consisting of 3 subnets

Subnets

recipe

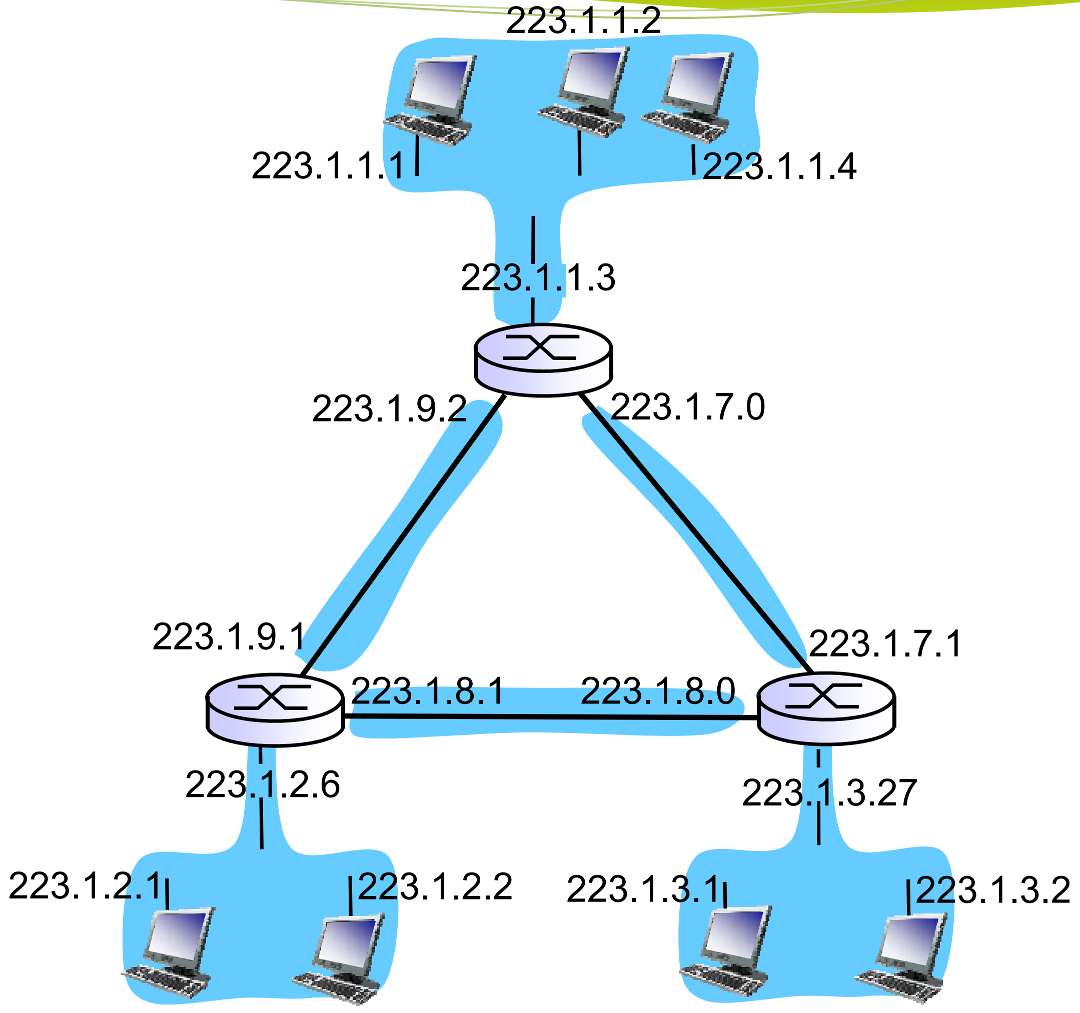
- to determine the subnets, detach each interface from its host or router, creating islands of isolated networks
- each isolated network is called a *subnet*



subnet mask: /24

Subnets

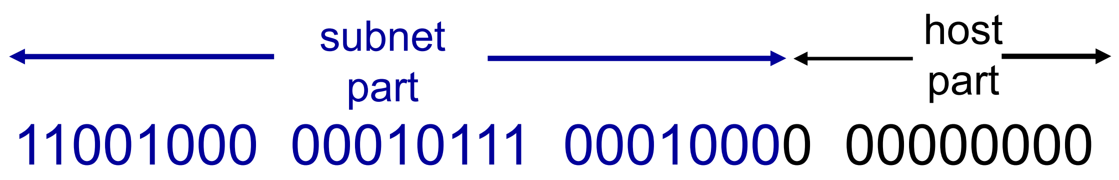
how many?



IP addressing: CIDR

CIDR: Classless InterDomain Routing

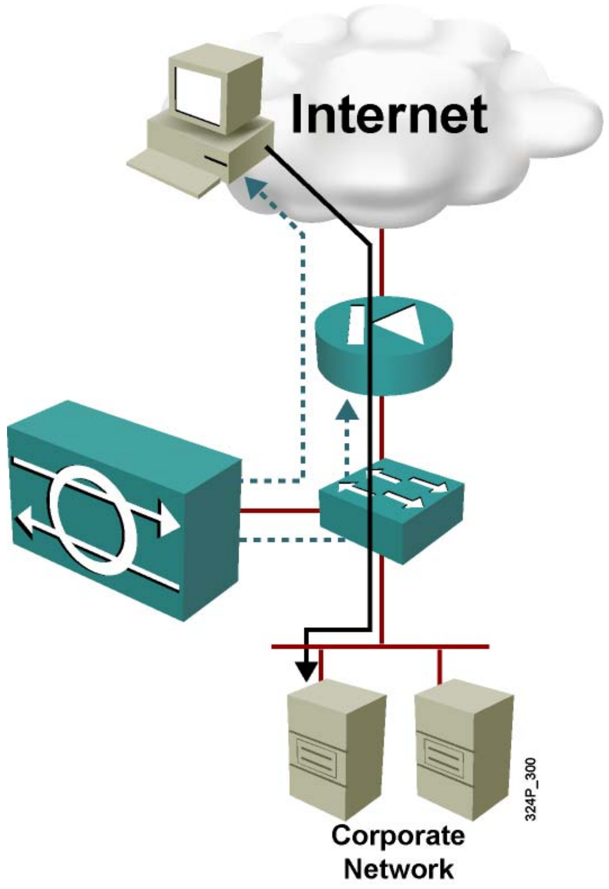
- subnet portion of address of arbitrary length
- address format: a.b.c.d/x, where x is # bits in subnet portion of address



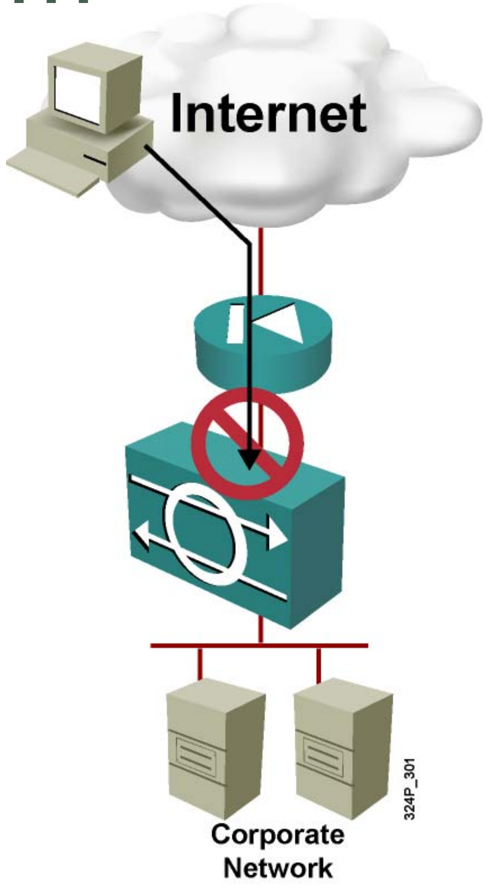
200.23.16.0/23

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.

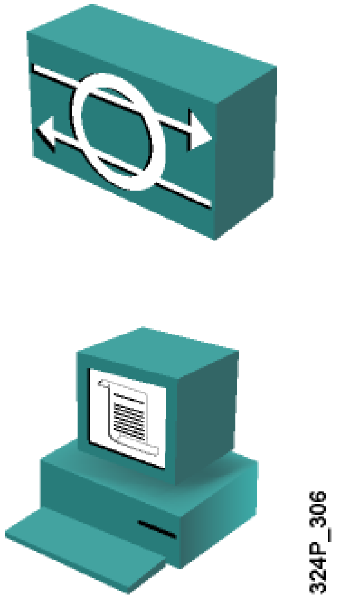
Combining IDS and IPS

- 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

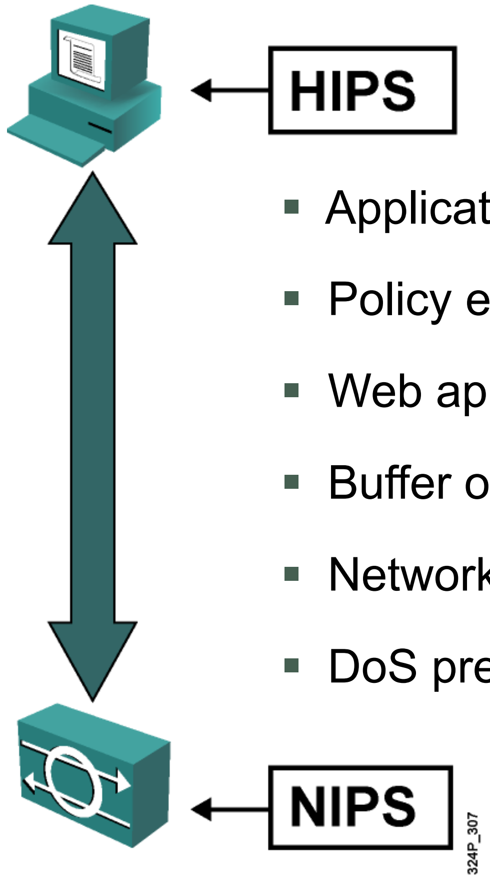
Criteria	Type	Description
Deployment Options	Network-based	Network sensors scan traffic that is destined to many hosts.
	Host-based	Host agent monitors all operations within an operating system.
Approaches to Identifying Malicious Traffic	Signature-based	A vendor provides a customizable signature database.
	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.
  - HIPS provides individual host detection and protection.
  - HIPS does not require special hardware.

Comparing HIPS and NIPS

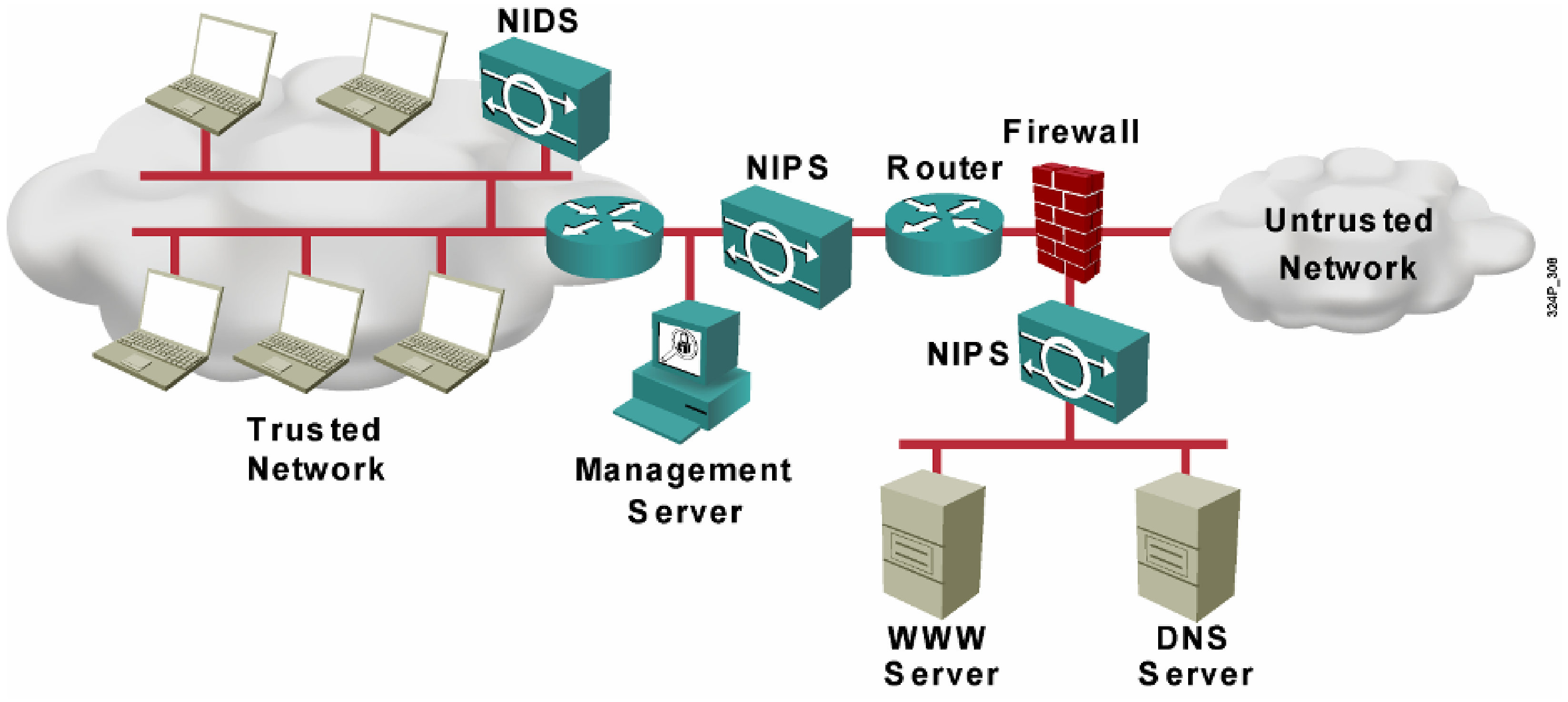


- Application-level encryption protection
- Policy enhancement (resource control)
- Web application protection
- Buffer overflow
- Network attack and reconnaissance prevention
- DoS prevention

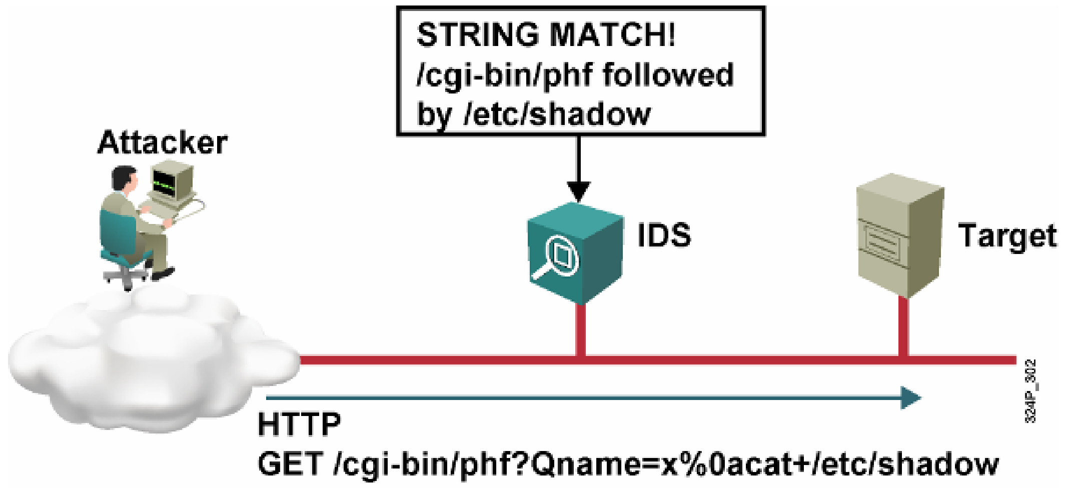
NIPS Features

- 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

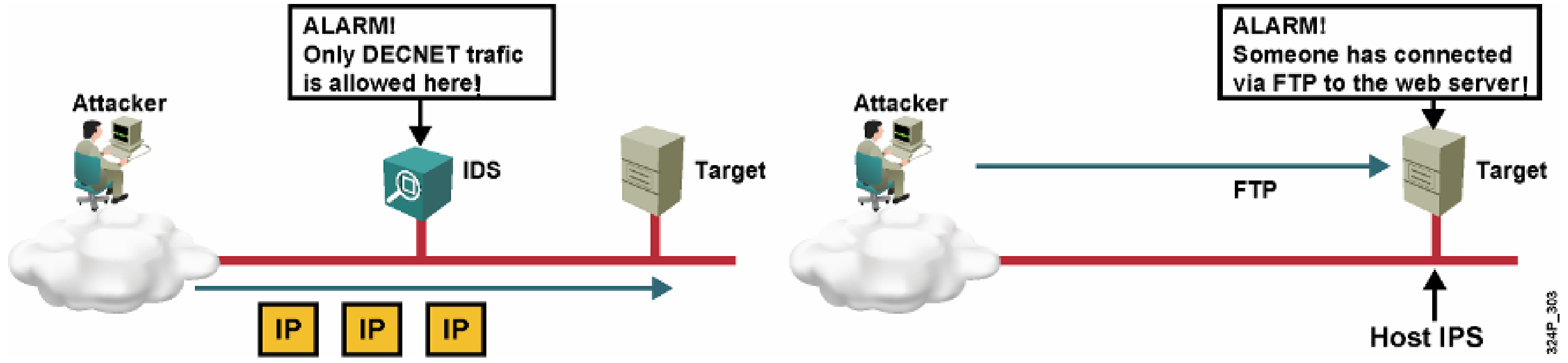


Signature-Based IDS and IPS



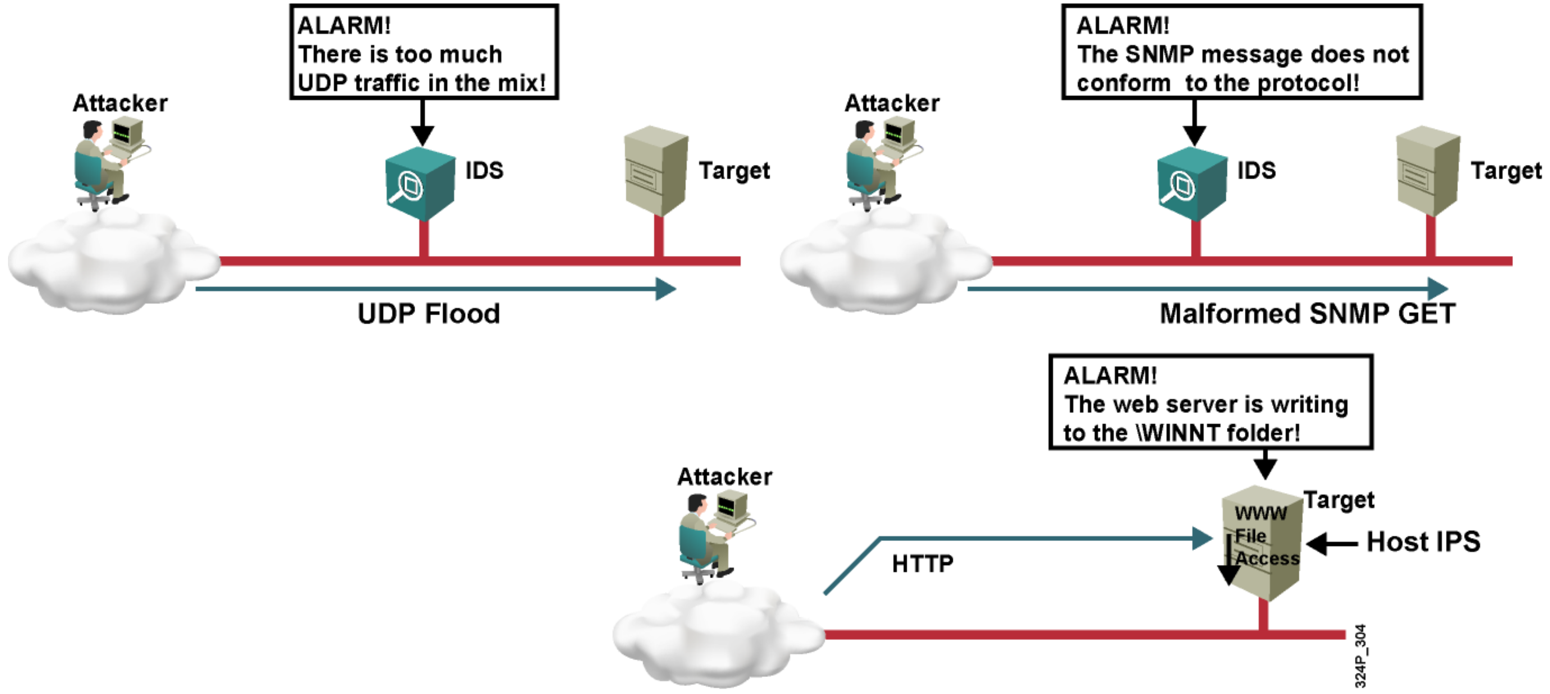
- Observes and blocks or alarms if a known malicious event is detected:
  - Requires a database of known malicious patterns.
  - The database must be continuously updated.

Policy-Based IDS and IPS



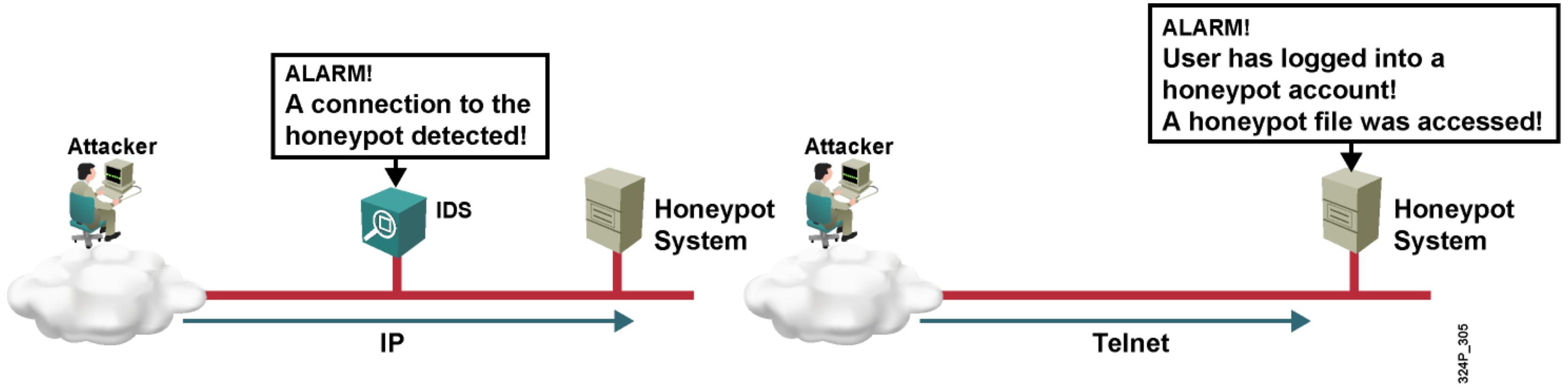
- Observes and blocks or alarms if an event outside the configured policy is detected
- Requires a policy database

Anomaly-Based IDS and IPS



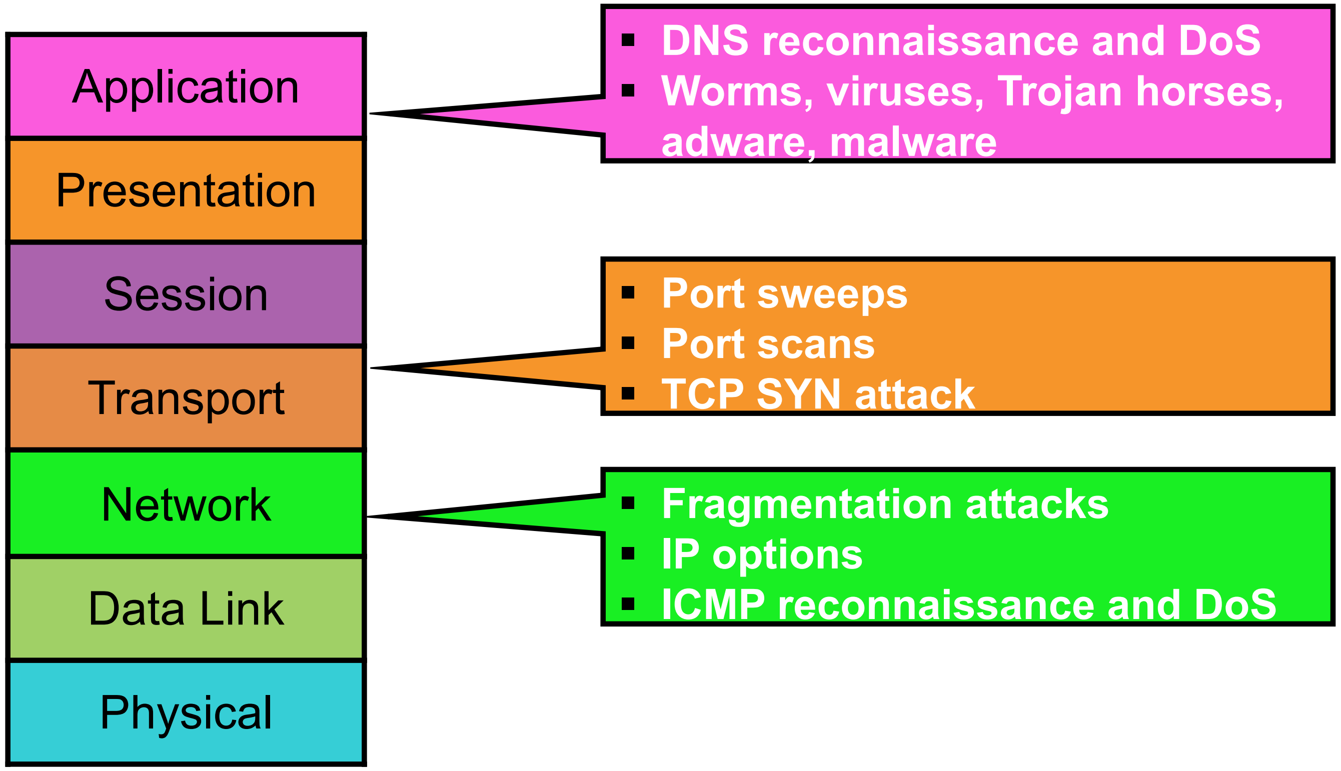
- **Observes and blocks or alarms if an event outside known normal behavior is detected:**
  - **Statistical versus nonstatistical anomaly detection**
  - **Requires a definition of "normal"**

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

Security onlion services

- You can see the services running:

```
sudo service nsm status
```

- To restart all services

  Sudo service nsm restart

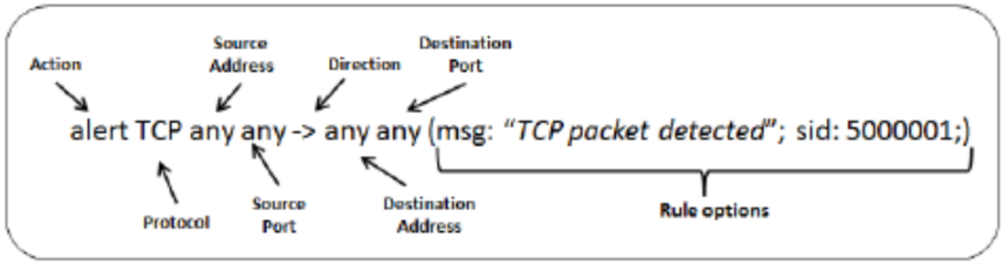
- To restart a single sensor service for instance Snort after a config change:

```
sudo nsm_sensor_ps-restart --only-snort-alert
```

Snort rules

- Several sources can be used for rules
- Most updated rules costs some money.
- ET
- GPL

Snort rules



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

- Address can also be $HOME_NET or $EXTERNAL_NET

Trying out the IDS

- Make sure that your security onion is fully configured.
- Try to run some of the previous commands (like nmap scans, flooding, 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`

Updating rules

- Rules can be written in

```
less etc/nsm/rules/local.rules
```

- The automatically downloaded rules are in

```
less etc/nsm/rules/downloaded.rules
```

- To update the rules to the most up to date, you can use

```
sudo rule-update
```

- It will create a copy of your old rules and place it in

```
ll etc/nsm/rules/backup/
```

Updating rules

- In some cases you would like to disable some alerts, and make sure that they will not be reapplied with the next rule-update request, you can disable them in
```
/etc/nsm/pulledpork/disablesid.conf
```
- In our case we need to do that to the downloaded rule on line 5123, in downloaded.rules, because it crashes our snort.
- We find the sid of that rule, and then we add it to our disablesid.conf file
```
sudo nano /etc/nsm/pulledpork/disablesid.conf
```
- At the bottom of that file we add
```
1:2002802
```
- Then we update the rules again
```
sudo rule-update
```
- If snort is not running
```
sudo nsm_sensor_ps-status --only-snort-alert
```
- Then restart it
```
sudo nsm_sensor_ps-restart --only-snort-alert
```

Creating custom rules

- Lets create a rule that will detect if someone is trying to retrieve something containing putty.exe (http://kallasoft.dk/putty.exe)
- Go to your local.rules and add the rule

  sudo nano /etc/nsm/rules/local.rules
- Add the following to the file (its 1 line):

```
alert tcp any any -> any any (msg:"test"; uricontent:“putty.exe"; sid:90005238;
rev:1;)
```
- Then update the rules

```
sudo rule-update
```
- Now try to download the file http://kallasoft.dk/putty.exe from the kali linux

Detecting flooding

- We can also create rules to test for tcp flooding

```
alert tcp any any -> 192.168.65.1 any (msg:"TCP SYN
flood attack detected"; flags:S; threshold: type
threshold, track by_dst, count 20 , seconds 60;
classtype=denial-of-service;priority:5 ;sid: 5000001;
rev:1;)
```

- Then try to do the flooding from scapy.

Exercise 1

- Now try to create a rule that will trigger on someone doing ping on the internal network.
- Find the correct classification for the attack and put it on the rule. You can find all classifications in:

```
less /etc/nsm/rules/classification.config
```

Then set the class type in the rule

```
… classtype=xxx; …
```

Exercise 2

- You find that kallasoft webpage is considered malicious.
- Create a rules that will alert when someone from the internal network is trying to access it using http, https or ftp/ssh.

References

Chapter on Squil and NSM

- http://ptgmedia.pearsoncmg.com/images/0321246772/samplechapter/bejtlich_chs.pdf

Snort rules infographic

- https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/116/original/Snort_rule_infographic.pdf?

Snort manual

- http://manual-snort-org.s3-website-us-east-1.amazonaws.com/