Intrusion Detection Systems

Defensive Technologies

Revision 1 (2024/25)

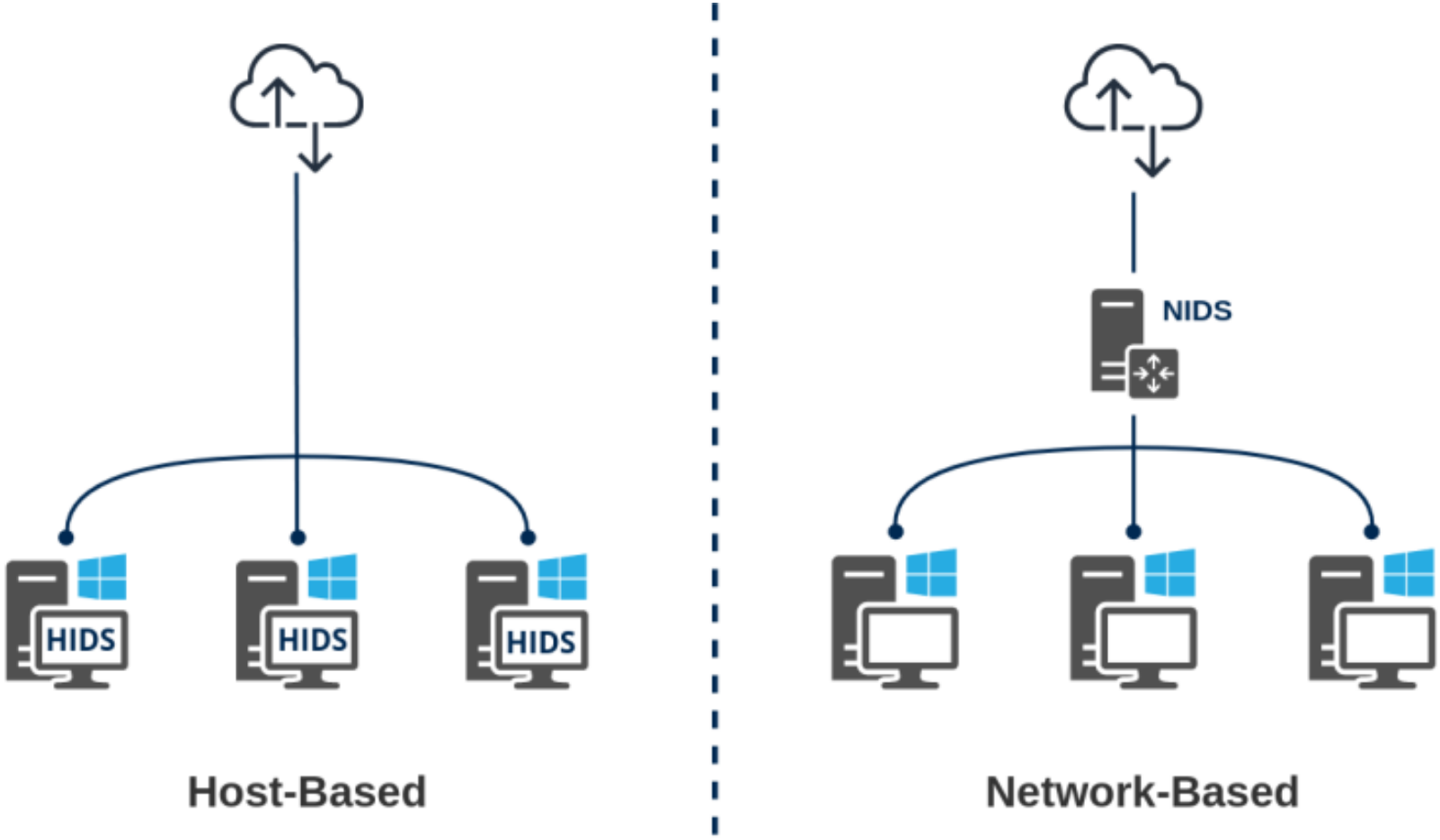
Pierre-Philipp Braun <pbraun@nethence.com>

Table of contents

Products & Use-cases

IDS / IPS

- **D**etection (passive) – *just an alert*
- **P**revention (active) – *alert* + *blocked*



// RP2/2018 IDS/IPS network evasion techniques

HIDS

- corporate HIDS fleet are generally managed by a centralized mgmt interface
- most commonly hybrid IDS/IPS by means of interactive pop-ups

Network IDS products

- Suricata (got IPS/online mode)
- Snort
- Zeek (formerly Bro)
- Wazuh (incl. UI?)
- Prelude SIEM vs. Prelude OSS (community edition)

…those essentially generate alert logs

==> need some UI (ELK/OSF/Loki)

Intrusion detection

static rule-sets

- signature-based – *character strings, binary size/checksum*
- known app-level exploit attempts – *just to catch those who try*
- protocol exploit attempts – *unprobable values in headers, known protocol attacks*
- stateful protocol analysis – *keep track of some connections*

Inference & heuristics

machine learning rule-sets

- anomaly-based – *classify what is normal or not*
- as for OSF, still somehow *stupid* tool: need to define very precisely
  - target field (e.g. status code)
  - function/feature (avg vs count …)

products

- Opensearch Anomaly Detection
- OpenUBA?
- …

Detection use-cases

During exploit attacks

- external attacker & DDoS

Persistent malware & covert channels

- malicious insider maintains access + evades network
- malware is a rootkit/backdoor

Other kinds of covert channels

- consultant (or spy) reaches his internal-network station from home
- *seen in NETWORK/VPN and OT/COVERT –> Other Tunnels*

Worms

- malware spreads around

IDS tuning

- community and commercial rules are not enough
- profile for company A doesn't fit company B
- daily tuning is required
- many false-positives by design (alert doesn't mean unsafe)
- unknown amount of false-negatives (**no alert doesn't mean safe**) – we are not aware of all the bad things in the world

Rules' limitations – detects well-known attacks

- will not detect targetted and specific attacks
- unless you **create specific**, highly effective **detection rules**

Loads of tuning… – *about 3 monthes part-time for the auditor to fine-tune*

- need to update corporate security policy
- what is NOT allowed? DropBox, ToR, Torrent, Facebook, …
- so you can get rid of false-positives

also layer 3-4 tuning…

ACL & firewall vs. fine-grained layer 3-4 IDS rules

- some kind of a passive firewall
- some kind of a firewall honey-pot

// Questions on products & use-cases?

Play Eve

- we don't necessarily get into the encrypted channels
- but still, we're sniffing, and we got a lot…

What data can we collect anyways?…

==> play Eve… *(Eavesdropping)*

1. look at the **plain-text** (first rule from some agency…)
2. network-level **meta-data** (supposedly Zeek is good for that)
3. app-level **meta-data** (cross-join with GAFAM utmost-plausible…)

Network-level meta-data

- *IP accounting, NetFlow and IPFIX are done elsewhere*
- Server Name Indication (SNI) is in clear-text
- various things e.g. who's doing SSH, …

App-level meta-data

- geo-localization (GPS vs. Wifi…)
- contact lists
- *see CCF/SURVEILLANCE*

Traffic inspection limitations

- no way to differnciate an HTTPS connection from VPN/SSL

Any idea why?…

==> OSI layer 6 – Presentation

- that’s a tunnel anyhow
- we don’t see what’s inside

// Questions on playing eve?

Where to sniff & Sensors

What's your target traffic?

monitoring floors vs. routing vs. internet

Possible locations for an IDS

- switch uplink – *attempt to catch lateral movements*
- internal router / ACL – *between network segments & VLANs*
- public gateway / firewall – *internet traffic (most important)*

==> IDS goes there – *passive only*

- port mirror *aka* SPAN/RSPAN on a switch – *monitoring the uplink*
- port mirror on an internal router? – *otherwise embedded*
- port mirror on a router/gateway? – *otherwise embedded*

BONUS QUESTION // does some Cisco switch with embedded IDS exist?

==> IPS goes there – *need to be on the path*

only routers & firewalls

- *not* on a switch – *unless the feature exists nowadays?*
- internal router / ACL
- public gateway / firewall

Consider gateway monitoring e.g. NAT

- remember we monitor only the traffic going through us

Will malicious traffic between node1 talking to node2 in the company be catched?…

==> of course not, it's not passing through the gateway

Now consider internal router monitoring

Will malicious activity within a VLAN be catched?…

==> nope, it would have to cross a VLAN to another

Now consider switch uplink monitoring

Will malicious activity between floor-neighbors be catched?…

==> also not, unless they're connected to different switches (and without stacking)

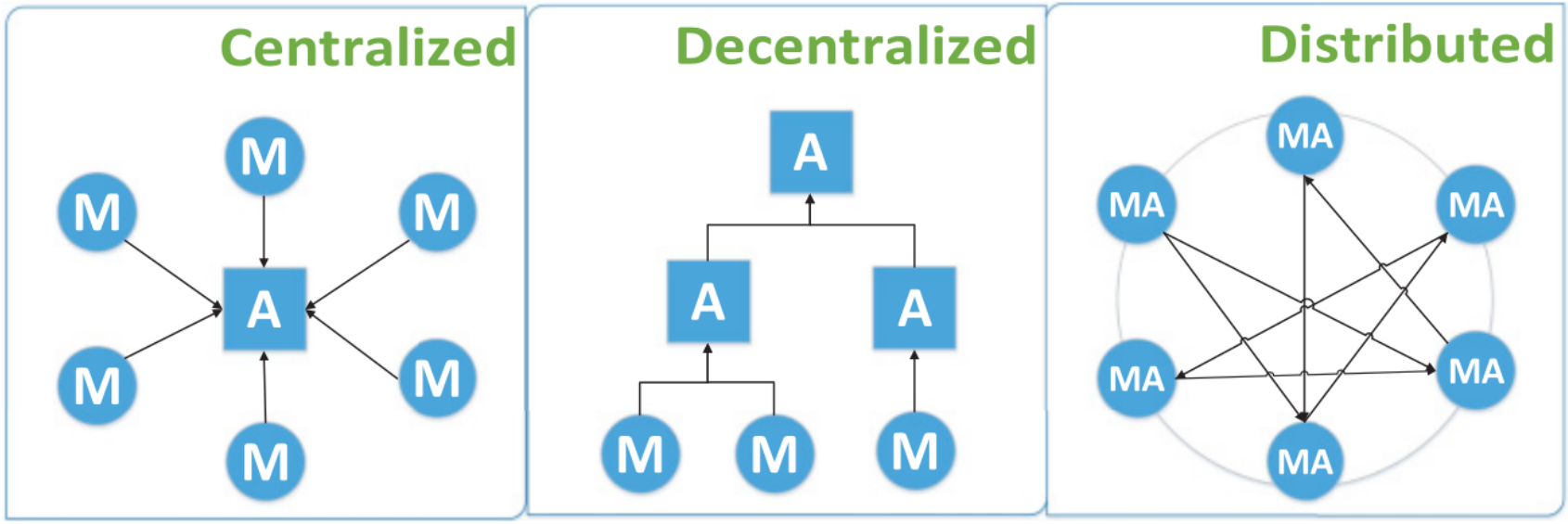
IDS architectures

- analysis unit (A) – *the main IDS instance*
- monitor (M) – *like an snmp agent…*

Note:

- we've got something similar with Zeek (cluster-capable)
- also we can do RSPAN with Cisco (remote SPAN)

Collaborative Intrusion Detection (CIDS)



BONUS QUESTION // anything concrete on that front? what products?

// Questions on where to sniff and sensors?

Evasion Techniques

- obfuscation vs. encryption
- self-modifying & polymorphic malware – *not sure there are mitigations for this*

Obfuscation e.g. tricky URLs

```
http://victim/cgi/../../winnt/system32/cmd.exe?/c+dir+
    c:\/ (root) ./ (current dir) ../ (parent of current dir)

http://victim/cgi/%252E%252E%252F%252E%252E%252Fwinnt/system32/
    cmd.exe?/c+dir+c:\

http%3A%2F%2Fvictim%2Fcgi%2F..%2F..%2Fwinnt%2Fsystem32%2F
    cmd.exe%3F%2Fc%2Bdir%2Bc%3A%5C
```

Obfuscation e.g. XOR, encoders, crypters, packers

Some packers get noticed

LAB // check the ruleset against some known *packer* and validate its detection (warning: isolate env in case this is the unmodified malware/worm)

Encryption

- Easy evasion by means of encryption
- E.g. SSL is authenticated AND end-to-end

How to work around that situation?…

==> IDS with SSL interception (next section)

// Questions on ids evasion techniques?

IDS with SSL Interception

assuming public gateway

- SSL covert channels cannot be easily identified
- the only way is to terminate the SSL tunnels

==> block anything encrypted and proxy/intercept SSL

- the only way to the public network goes through (transparent) proxy

LAB // plug the IDS to an SSL interception engine

How to SSL intercept?…

==> your PKIX CA in da place

Clients need to trust Gateway/IPS's CA which signs-on-the-fly

- deploy CA certificate in user's browsers & systems trust stores

Any idea why "on-the-fly"?…

==> remember an SSL certificate is a binding between a CN/SAN and a key pair

Hence we need to generate-and-sign certs for every requested domain

```
www.google.com
somethingelse.fr
```

E.g. some user wants to reach `www.google.com`

```
CLIENT
--> asks for www.google.com

MITM SSL PROXY intercepts (either as defined or transparent)
--> CA creates and signs www.google.com.crt

CLIENT
--> verifies the chain of trust against its CA store

MITM SSL PROXY
--> forward-proxy delivers and relays traffic
```

Idem for `somethingelse.fr`, etc.

Note: forward proxy products (& interception feature) are discussed in NETWORK/LBS-PROXY

Technology Intelligence LAB // are on-the-fly certs cached and how?

Note: there's also a blacklist feature e.g. with Squid+SquidGuard, to simply block a few websites…

// Questions on ids ssl interception?

IDS Insecurity

hints for the attacker

Avoiding the IDS

depending on where the IDS sits

exclude **routed** IP ranges from network scans e.g.

```
   nmap -T5 --exclude 10.99.99.0/24 ...
masscan -T5 --exclude 10.99.99.0/24 ...
```

Owning the IDS

Snort 2 DCE/RPC Preprocessor Buffer Overflow

```
Snort 2.6.1, 2.7 Beta 1
SourceFire IDS 4.1, 4.5 and 4.6
```

```
msf > use exploit/multi/ids/snort_dce_rpc
```

What will attacker do once the IDS is compromized?...

==>

- IDS becomes a stepping stone for lateral movements
- IDS becomes a malicious monitoring point

Attacker covers his tracks

```
if(ip.source == attacker) drop alert
```

Disowning the IDS

forging fake alerts and confuse the auditor

// Questions on ids insecurity?