How to Test an IDS?
GENESIDS: An Automated System for Generating Attack Traffic

WTMC 2018

Felix Erlacher, Falko Dressler
Network Intrusion Detection Systems (NIDS)

Analyze network traffic for malicious activity

- **Anomaly based NIDS**
  - Have a model of 'normal' traffic
  - Detect and alert deviations from 'normal' traffic

- **Signature based NIDS**
  - Have rule-set of known attacks and incidents
  - Detect rule patterns in analyzed network traffic

→ Example: Snort
How to test a NIDS?

- Real traffic?
  - hard to get
  - public traces: old, no payload
  - contains only very few attacks
How to test a NIDS?

- Real traffic?
  - hard to get
  - public traces: old, no payload
  - contains only very few attacks

- Manually creating attack traffic?
  - time intensive
  - cumbersome
How to test a NIDS?

- Real traffic?
  - hard to get
  - public traces: old, no payload
  - contains only very few attacks
- Manually creating attack traffic?
  - time intensive
  - cumbersome

SUMMARY: traces do not contain enough *unique* attacks
How to test a NIDS!

GENESIS:
Generating Events for Signature-based Intrusion Detection Systems

- **INPUT**: Set of attack descriptions
  - Snort syntax
  - HTTP attacks
- **OUTPUT**: Stateful network traffic containing attack patterns
  - One flow per attack
  - Annotated with an attack ID
Rule example:

```
alert tcp any any -> any any (msg:"This is an example rule";
content:"POST"; http_method;
uri_content:"|2F|evil.jpg";
pcre:"/AttackBody-V[0-9].*/P";
sid:1234567; rev:0;)
```
Rule example:

```plaintext
alert tcp any any -> any any ( 
msg:"This is an example rule"; 
content:"POST"; http_method; 
uricontent:"|2F|evil.jpg"; 
pcre:"/AttackBody-V[0-9].*/P"; 
sid:1234567; rev:0;)
```
Rule example:

```
alert tcp any any -> any any (  
msg:"This is an example rule";  
content:"POST"; http_method;  
uricontent:"\|2F\|evil.jpg";  
pcre:"/AttackBody-\V[0-9].*/P";  
sid:1234567; rev:0;)
```
Rule example:

```
alert tcp any any -> any any (msg:"This is an example rule";
content:"POST"; http_method;
uricontent:"\2F|evil.jpg";
pcre:"/AttackBody-V[0-9].*/P";
sid:1234567; rev:0;)
```
Rule example:

```
alert tcp any any -> any any (msg:"This is an example rule";
content:"POST"; http_method;
uricontent:"|2F|evil.jpg";
pcre:"/AttackBody-V[0-9].*/P";
side:1234567; rev:0;)
```
Rule example:

```plaintext
alert tcp any any -> any any (msg:"This is an example rule";
content:"POST"; http_method;
uricontent:"|2F|evil.jpg";
pcre:"/AttackBody-V[0-9].*/P";
sid:1234567; rev:0;)
```
Rule example:

```
alert tcp any any -> any any ( 
msg:"This is an example rule";
content:"POST"; http_method;
uri_content:"|2F|evil.jpg";
pcre:"/AttackBody-V[0-9].*/P";
sid:1234567; rev:0;)
```
Rule example:

```
alert tcp any any -> any any (    
  msg:"This is an example rule";
  content:"POST"; http_method;
  uricontent:"|2F|evil.jpg";
  pcre:"/AttackBody-V[0-9].*/P";
  sid:1234567; rev:0;)
```
Rule example:

```
alert tcp any any -> any any (  
  msg:"This is an example rule";
  content:"POST"; http_method;
  uricontent:"|2F|evil.jpg";
  pcre:"/AttackBody-V[0-9].*/P";
  sid:1234567; rev:0;)

genesids -f example.rule -s example.com
```
Example traffic in Wireshark:

```
alert tcp any any -> any any (msg:"This is an example rule";
content:"POST"; http_method;
uricontent:"|2F|evil.jpg";
pcre:"/AttackBody-V[0-9].*/P";
sid:1234567; rev:0;)
```

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
</table>
| 1   | 0.0000000 | 10.0.0.111         | 131.234.188.5      | TCP      | 74     | 56300 - 80 [SYN] Seq=0 Win=29204000
| 2   | 0.051498  | 131.234.188.5     | 10.0.0.111         | TCP      | 74     | 80 - 56300 [SYN, ACK] Seq=0 Ack=1
| 3   | 0.051561  | 131.234.188.5     | 10.0.0.111         | TCP      | 66     | 56300 - 80 [ACK] Seq=1 Ack=1 W
| 4   | 0.051747  | 10.0.0.111        | 131.234.188.5     | HTTP     | 170    | POST /evil.jpg HTTP/1.1
| 5   | 0.101175  | 131.234.188.5     | 10.0.0.111         | TCP      | 66     | 80 - 56300 [ACK] Seq=1 Ack=105
| 6   | 0.105167  | 131.234.188.5     | 131.234.188.5     | HTTP     | 597    | 1.1 301 Moved Permanently
| 7   | 0.105218  | 10.0.0.111        | 131.234.188.5     | TCP      | 66     | 56300 - 80 [ACK] Seq=105 Ack=5
| 8   | 0.105541  | 131.234.188.5     | 131.234.188.5     | TCP      | 66     | 56300 - 80 [FIN, ACK] Seq=105 Ack=5
| 9   | 0.152631  | 131.234.188.5     | 10.0.0.111         | TCP      | 66     | 80 - 56300 [FIN, ACK] Seq=532 Ack=5
| 10  | 0.152684  | 10.0.0.111        | 131.234.188.5     | TCP      | 66     | 56300 - 80 [ACK] Seq=106 Ack=5

**Hypertext Transfer Protocol**

```
POST /evil.jpg HTTP/1.1
Host: ccs-labs.org
Rulesid: 1234567
```

**Data (19 bytes)**

```
0000 e0 91 f5 79 5d 42 b6 ce 8b 47 9f 3b 08 00 45 06
0010 00 9c 84 19 40 00 00 06 6b e4 0a 00 00 6f 83 ea
0020 bc 05 db ec 00 50 f2 c4 7b cf 36 76 cb bb 80 18
0030 00 e5 4d ce 00 00 01 01 08 0a 00 29 ff e6 fc 3b
0040 dc 5f 50 4f 54 53 54 20 2f 65 76 69 6c 2e 6a 70 67
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a
0060 20 63 66 65 6d 69 6e 64 65 6e 65 6e 65 6e 74 74 3a
0070 75 6c 65 73 69 64 3a 20 31 32 33 34 35 36 37 3d
0080 0a 43 6f 6e 64 65 6c 65 6e 65 6e 65 6e 65 6e 65 6e 74 74 3a
0090 20 31 32 33 34 35 36 37 3d
```

HEINZ NIXDORF INSTITUTE
UNIVERSITÄT PADERBORN

Felix Erlacher: How to Test an IDS? GENESIDS 6
Example traffic in Wireshark:

```
alert tcp any any -> any any (msg:"This is an example rule"; content:"POST"; http_method; uricontent:"/evil.jpg"; pcre:"/AttackBody-V[0-9].*/P"; sid:1234567; rev:0;)
```

Felix Erlacher: How to Test an IDS? GENESIDS
Example traffic in Wireshark:

alert tcp any any -> any any (  
msg:"This is an example rule";  
content:"POST";  
http_method;  
uricontent:"/evil.jpg";  
pcre:"/AttackBody-V[0-9].*/P";  
sid:1234567;  
rev:0;)

Felix Erlacher: How to Test an IDS? GENESIDS
Example traffic in Wireshark:

```
alert tcp any any -> any any (
  msg:"This is an example rule";
  content:"POST"; http_method;
  uricontent:"|2F|evil.jpg";
  pcre:"/AttackBody-V[0-9].*/P";
  sid:1234567; rev:0;)
```

Felix Erlacher: How to Test an IDS? GENESIDS
Example traffic in Wireshark:

```
alert tcp any any -> any any (msg:"This is an example rule"; content:"POST"; http_method; uricontent:"|2F|evil.jpg"; pcre:"/AttackBody-V[0-9].*/P"; sid:1234567; rev:0;)
```

Felix Erlacher: How to Test an IDS? GENESIDS

---

![Image showing Wireshark traffic](image-url)
Example traffic in Wireshark:

```
alert tcp any any -> any any (msg:"This is an example rule";
content:"POST";http_method;
uricontent:"|2F|evil.jpg";
pcre:"/AttackBody~V[0-9].*/P";
 sid:1234567; rev:0;)
```

Felix Erlacher: How to Test an IDS? GENESIDS
 Ability to generate a variety of different attacks
 GENERATED attacks trigger expected event
GENESIDS Evaluation: Goals & Rules

- Ability to generate a variety of different attacks
- Generated attacks trigger expected event

All supported Snort rules from:

- Snort.org subscriber rule-set
- Snort.org community rule-set
- Emerging Threats rule-set

TOTAL 8101 different rules
GENESIDS Evaluation steps

Step 1

- Rules
- Network Trace

GENESIDS | TCP Connection | HTTP Server

Felix Erlacher: How to Test an IDS? GENESIDS
GENESIDS Evaluation steps

Step 1
- GENESIDS
- TCP Connection
- HTTP Server
- tcpdump

Step 2
- Network Trace
- Rules
- Snort
- Alerts

Felix Erlacher: How to Test an IDS? GENESIDS
Evaluation results: Generated attacks

GENESIDS: 8101 attacks generated (out of 8101 rules)
Evaluation results: True positives

Snort: 7877 (avg) true positive alerts triggered (out of 8101)
Evaluation results: False positives

Snort: 2847 (avg) false positive alerts triggered (62% triggered by 3 rules)
Evaluation results: False negatives

- Snort: 223 (avg) false negatives (generated attacks that did not trigger the corresponding alert)
- Total of 363 rules generated attack not triggering at least once (out of 100)
Conclusion

GENESIDS: Generating attack traffic for NIDS testing

- Accepting Snort syntax → thousands of up-to-date attack definitions

- 97% of generated attacks triggered corresponding alert

- Less than 3% failed to trigger corresponding alert
Software, configuration files, attack network traces:

www.ccs-labs.org/~erlacher/resources/

Reminder: GENESIDS Demo → Wednesday 14:10
Software, configuration files, attack network traces:

www.ccs-labs.org/~erlacher/resources/

Reminder: GENESIDS Demo → Wednesday 14:10

Thank you for your attention
Mixed traffic with GENESIDS and TRex
False negatives: Closer look

363 different rules not triggering corresponding event over 100 runs

1. Rules never triggering alert (179)
   - Some require non-compliant HTTP (e.g. multiple `\n\n\n`)
   - Restricting strings with ^ and $
   - ...

2. Rules failing to trigger at least once (in 100 runs) (184)
   - all of the rules contain a PCRE with random generation (.)
     random generation produced unsupported character
   - ...

Felix Erlacher: How to Test an IDS? GENESIDS
TLS interception proxy

End-to-end cryptographic service:

Interception Proxy:

libpcap format
Typical monitoring scenario
Loop through rules:
1. parse rule
2. generate patterns for HTTP request
3. init TCP connection
4. send HTTP request
5. wait for response
6. end TCP connection
repeat