

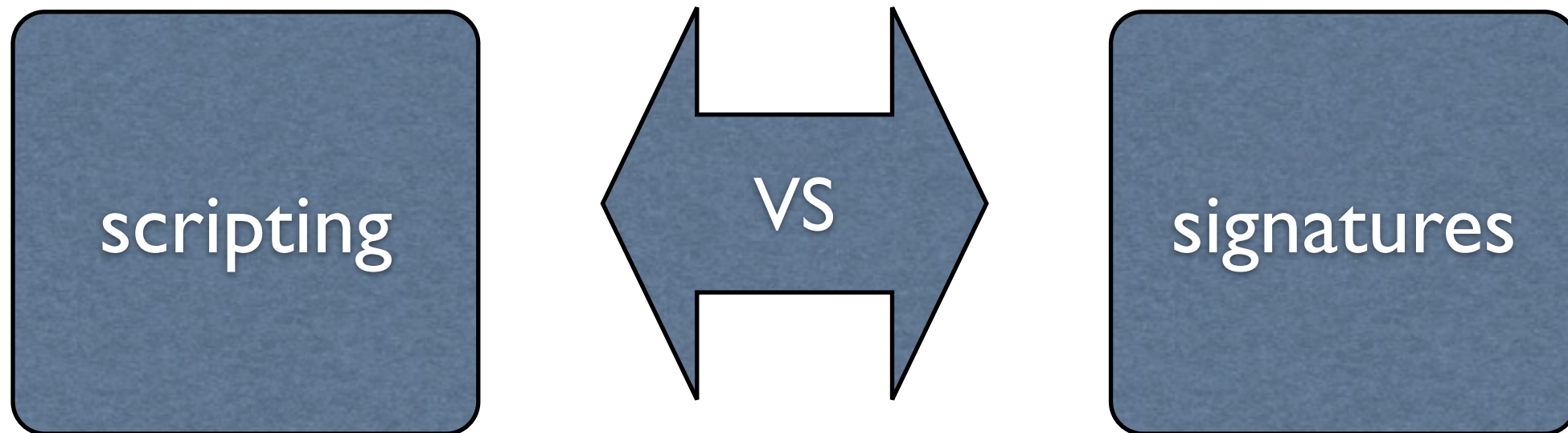


# Signature Framework

Bro 2.3 Training 2014



# Detection Mechanisms



- Low level, Snort-style pattern matching
- Not preferred detection methodology
- Familiar

# Example Signature

```
signature my-first-sig {  
    ip-proto == tcp  
    dst-port == 80  
    payload /. *root/  
    event "Found root!"  
}
```

# Matches

```
signature my-first-sig {  
    ip-proto == tcp  
    dst-port == 80  
    payload /. *root /  
    event "Found root!"  
}
```



Match **. \*root** on all  
TCP connections on  
Port 80

# Ports vs. Protocols

```
signature my-first-sig {  
    ip-proto == tcp  
    dst-port == 80  
    payload /. *root/  
    event "Found root!"  
}
```

# On Match

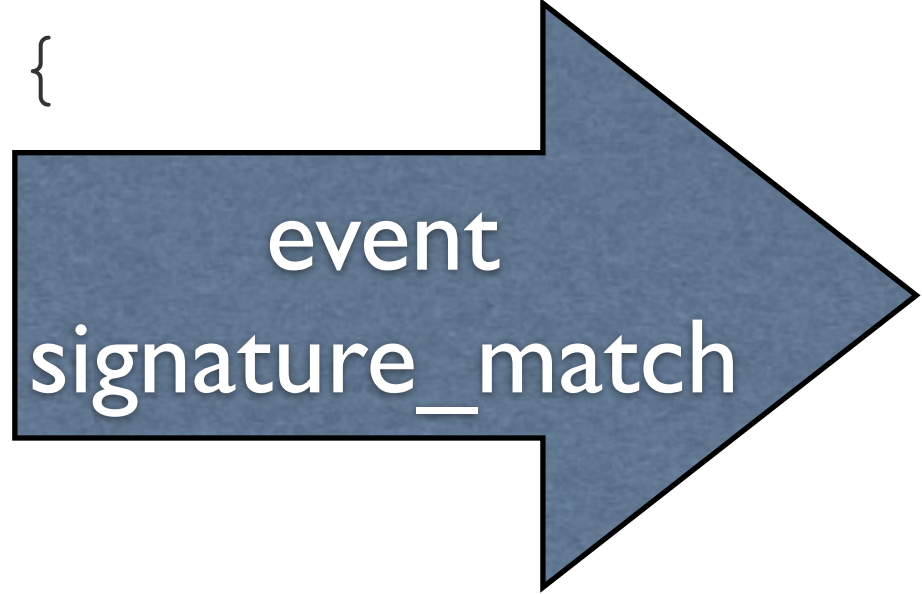
```
signature my-first-sig {  
    ip-proto == tcp  
    dst-port == 80  
    payload /. *root /  
    event "Found root!"  
}
```



event  
signature\_match

# signature\_match

```
signature my-first-sig {  
    ip-proto == tcp  
    dst-port == 80  
    payload /.*/root/  
    event "Found root!"  
}
```



event  
signature\_match

event signature\_match(state: signature\_state, msg: string, data: string)

state: Connection Information

msg: "Found root!"

data: last piece of the payload that generated the match

# Signature Components

```
signature <id> {  
  
    <attributes>  
  
}
```



# Signature Components

```
signature <id> {  
    <attributes>  
  
}
```

<id>

Must be unique

# Signature Components

```
signature <id> {  
    <attributes>  
  
}
```

*conditions*

When to Match

*actions*

What to Do

# Conditions

Condition	Usage
header	Limit to subset of traffic
content	regular expression (~flex)
dependency	requires-signature [!] <id> requires-reverse-signature [!] <id>
context	pass decision to other part of bro

# Condition: Header

`<keyword> <cmp> <value-list>`

`<cmp> ==, !=, <, <=, >, >=`

Keyword	Compare	Details
src-ip / dst-ip	<code>&lt;cmp&gt;</code>	IPv4 or IPv6
src-port / dst-port	<code>&lt;cmp&gt;</code>	source/dest port #
ip-proto	<code>&lt;cmp&gt;</code>	ip, tcp, udp, icmp icmp6, ip6

# Condition: Header 2

```
header <proto>[<offset>:<size>] [& <integer>] <cmp> <value-list>
```

Keyword	Compare	Details
proto	<cmp>	ip, tcp, udp, icmp ip6, icmp6
offset		defines position of the value
size		1 2 4 value size in bytes
integer		mask of 0-32 ( CIDR )

```
header ip[16:4] == 1.2.3.4/16, 5.6.7.8/24
```

# Condition: Content

`payload /<regular expression>/`

- Matches raw payload of connection
- TCP: Matched against reassembled TCP stream
- ICMP, UDP: each packet (& non-reassembled TCP)

# Condition: Content HTTP Specific

- Only fire if Analyzer is attached
- On HTTP Pipelining match any transaction

Protocol	Matched Against
http-request	decoded URIs of HTTP requests
http-request-header	client-side HTTP headers
http-request-body	client-side bodys of HTTP requests
http-reply-header	server-side HTTP headers
http-reply-body	server-side bodys of HTTP replys

# Condition: Content Other

- Only fire if Analyzer is attached
- Data extracted by analyzers

Protocol	Matched Against
ftp	command line input of FTP session
finger	only check finger requests



# Condition: Dependency

- define dependencies between signatures
- can negate with [!] <id>

requires-signature	requires-reverse-signature
<ul style="list-style-type: none"><li>• current sig only matches if previous &lt;id&gt;</li><li>• !&lt;id&gt; negating defers match until connection terminates</li></ul>	<ul style="list-style-type: none"><li>• match for opposite direction of SAME connection</li><li>• Allows notion of requests &amp; replies</li></ul>

# Condition: Context

- pass match to other part of Bro
- evaluated last after other matches

function	detail
eval	boolean function
payload-size	compare integer to size of packet payload
same-ip	true if source = dest
tcp-state	established   originator   responder

# Actions

action	Usage
event	Raise an event
enable	Dynamically enable Protocol Analyzer

# Exercises

Documentation:

[http://www.bro.org/sphinx-git/frameworks/  
signatures.html](http://www.bro.org/sphinx-git/frameworks/signatures.html)

Time for Exercises