pwnSpoof

github.com/punk-security/pwnspoof

Realistic attack log generation for training and SIEM evaluation

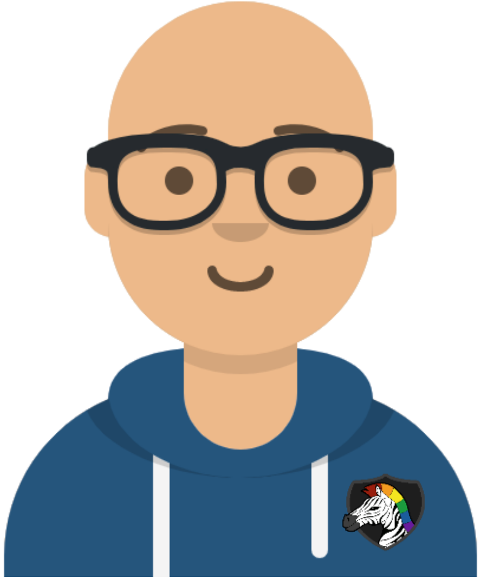
Daniel Oates-Lee

Punk Security

25+ years in IT

Cyber Security Consultant

Terraformer



Where did it come from?

Deliver a training package

How to regex and conduct search-time extraction

How to filter the mundane and find the unusual

How to leverage geo location

Make it interactive

Where do we get the logs?

Where do we get the logs?

A real attack

- ⍰ Authentic
- ▨ Full of sensitive information
- ▨ Parts of the attack missing
- ▨ Not scalable

Produce some

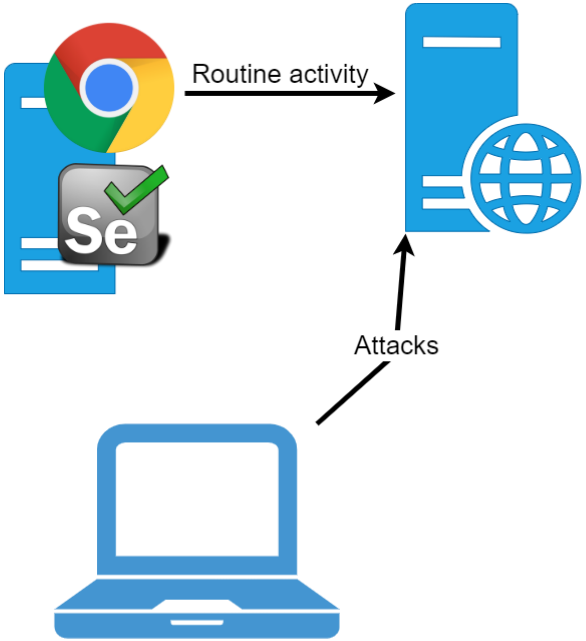
- ⍰ Authentic
- ⍰ Completely controllable content
- ⍰ Can control the attack
- ▨ Not scalable easily
- ▨ Slow to produce
- ▨ Static items, such as user agent and source IP

Spoof some

- ⍰ Completely controllable content
- ⍰ Can control the attack
- ⍰ Scales very easily
- ⍰ Can produce thousands of sessions per second
- ⍰ Not totally authentic
- ▨ Nothing out there to do it

producing real logs

- Deploy a web application
- Engineer a vulnerability into it
- Modify it to use GET parameters so they show up in the logs
- Setup a selenium hub
- Write code to drive user activity that differs a little every time
- Run the simulation for a few days
- Attack the application
- Harvest the logs



Routine activity

Attacks

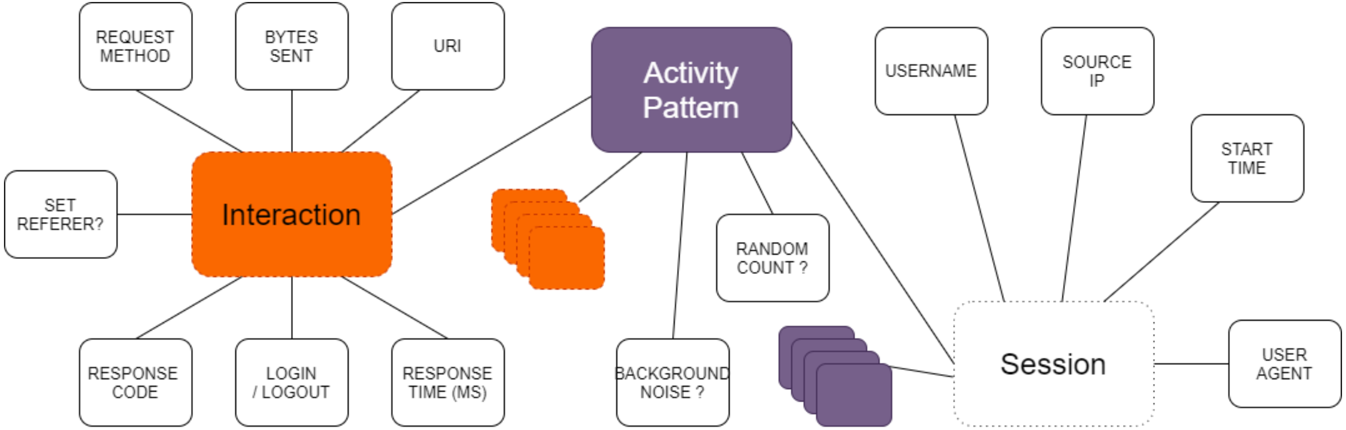
spoofing logs

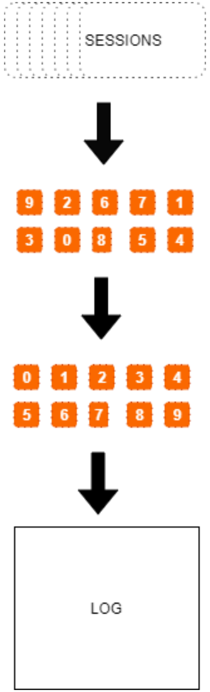
Logs file are easy, its just text

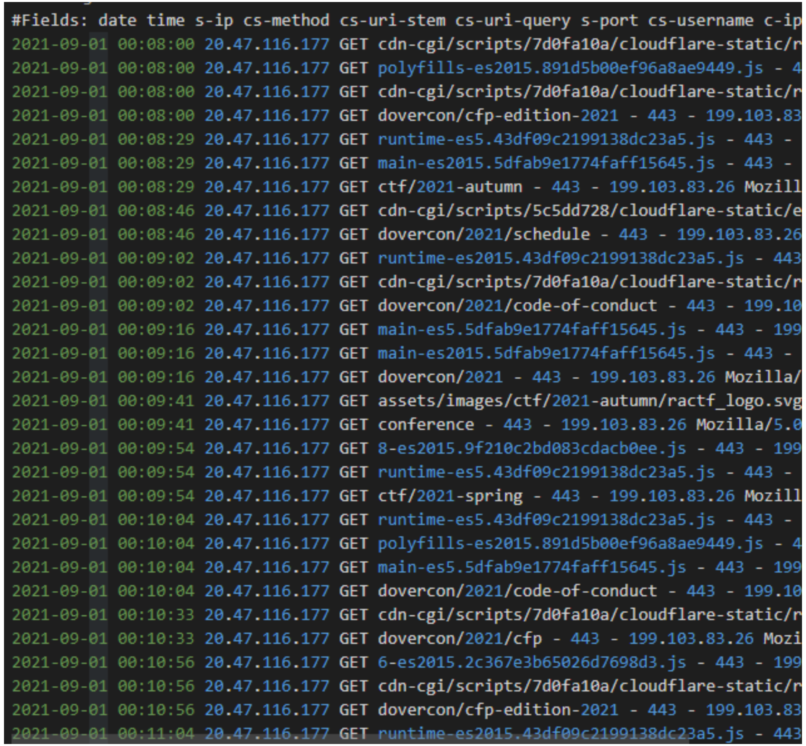
```
{source_ip} - {username} {datetime} "{method} {uri_with_query} HTTP/1.1" {status_code} {size} "{referer}" "{user_agent}“
```

Most the fields are easy, we just have to do some clever things to track the “referrer”

Each interaction with the webserver will have a purpose and we need to define these interactions.







```
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip
2021-09-01 00:08:00 20.47.116.177 GET cdn-cgi/scripts/7d0fa10a/cloudflare-static/r
2021-09-01 00:08:00 20.47.116.177 GET polyfills-es2015.891d5b00ef96a8ae9449.js - 4
2021-09-01 00:08:00 20.47.116.177 GET cdn-cgi/scripts/7d0fa10a/cloudflare-static/r
2021-09-01 00:08:00 20.47.116.177 GET dovercon/cfp-edition-2021 - 443 - 199.103.83
2021-09-01 00:08:29 20.47.116.177 GET runtime-es5.43df09c2199138dc23a5.js - 443 -
2021-09-01 00:08:29 20.47.116.177 GET main-es2015.5dfab9e1774faff15645.js - 443 -
2021-09-01 00:08:29 20.47.116.177 GET ctf/2021-autumn - 443 - 199.103.83.26 Mozill
2021-09-01 00:08:46 20.47.116.177 GET cdn-cgi/scripts/5c5dd728/cloudflare-static/e
2021-09-01 00:08:46 20.47.116.177 GET dovercon/2021/schedule - 443 - 199.103.83.26
2021-09-01 00:09:02 20.47.116.177 GET runtime-es2015.43df09c2199138dc23a5.js - 443
2021-09-01 00:09:02 20.47.116.177 GET cdn-cgi/scripts/7d0fa10a/cloudflare-static/r
2021-09-01 00:09:02 20.47.116.177 GET dovercon/2021/code-of-conduct - 443 - 199.10
2021-09-01 00:09:16 20.47.116.177 GET main-es5.5dfab9e1774faff15645.js - 443 - 199
2021-09-01 00:09:16 20.47.116.177 GET main-es2015.5dfab9e1774faff15645.js - 443 -
2021-09-01 00:09:16 20.47.116.177 GET dovercon/2021 - 443 - 199.103.83.26 Mozilla/
2021-09-01 00:09:41 20.47.116.177 GET assets/images/ctf/2021-autumn/ractf_logo.svg
2021-09-01 00:09:41 20.47.116.177 GET conference - 443 - 199.103.83.26 Mozilla/5.0
2021-09-01 00:09:54 20.47.116.177 GET 8-es2015.9f210c2bd083cdacb0ee.js - 443 - 199
2021-09-01 00:09:54 20.47.116.177 GET runtime-es5.43df09c2199138dc23a5.js - 443 -
2021-09-01 00:09:54 20.47.116.177 GET ctf/2021-spring - 443 - 199.103.83.26 Mozill
2021-09-01 00:10:04 20.47.116.177 GET runtime-es5.43df09c2199138dc23a5.js - 443 -
2021-09-01 00:10:04 20.47.116.177 GET polyfills-es2015.891d5b00ef96a8ae9449.js - 4
2021-09-01 00:10:04 20.47.116.177 GET main-es5.5dfab9e1774faff15645.js - 443 - 199
2021-09-01 00:10:04 20.47.116.177 GET dovercon/2021/code-of-conduct - 443 - 199.10
2021-09-01 00:10:33 20.47.116.177 GET cdn-cgi/scripts/7d0fa10a/cloudflare-static/r
2021-09-01 00:10:33 20.47.116.177 GET dovercon/2021/cfp - 443 - 199.103.83.26 Mozi
2021-09-01 00:10:56 20.47.116.177 GET 6-es2015.2c367e3b65026d7698d3.js - 443 - 199
2021-09-01 00:10:56 20.47.116.177 GET cdn-cgi/scripts/7d0fa10a/cloudflare-static/r
2021-09-01 00:10:56 20.47.116.177 GET dovercon/cfp-edition-2021 - 443 - 199.103.83
2021-09-01 00:11:04 20.47.116.177 GET runtime-es2015.43df09c2199138dc23a5.js - 443
```

Spoofed attack logs

- 3 different applications to spoof
- 3 different log output formats
- Background noise spoofing
- Session login state tracking
- Accurate "referrer" field
- Configurable log duration, session count and start time
- Dynamic sessions so no two are the same
- Multiple attacks, including bruteforce and command injection
- Customisable server FQDN
- Customisable web endpoints

The use cases

Training

Students have a realistic log bundle to work from, which can span weeks or months and contains millions of routine user sessions to wade through.

Attacks and scenarios can be customised quickly, or with a little effort the entire interaction can be modelled.

Product Evaluation

- How easy is it to conduct IP ASN / GEO lookups?
- Does it handle common log formats?
- Can you urldecode?
- Can you quickly see anomalous data?

CTFs

If we hide a flag in the attack, we have a reusable CTF generator that promotes blue team skills.

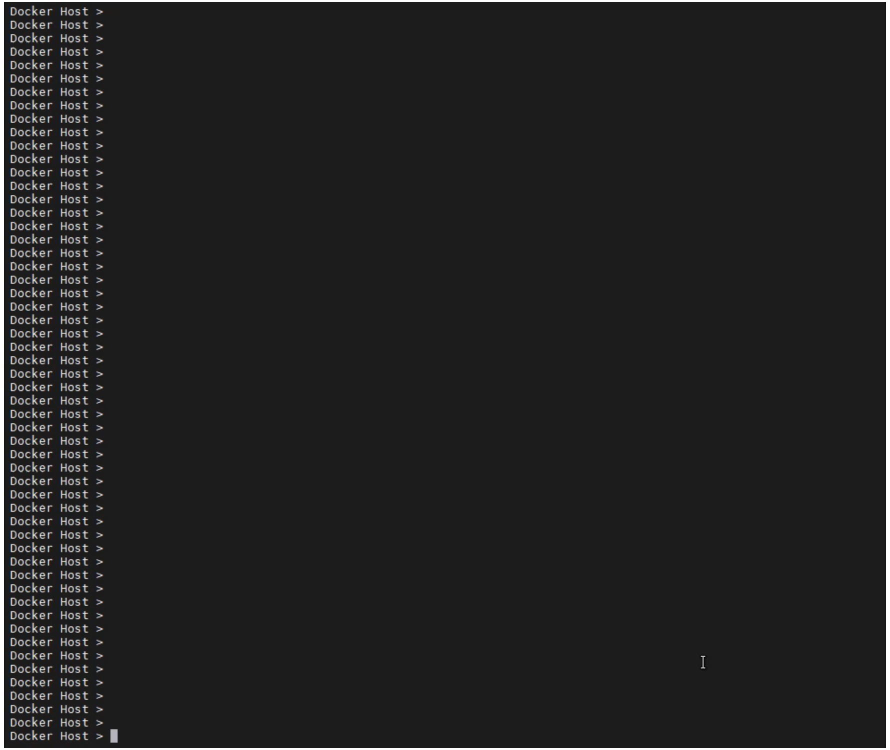
./WARGAMES CTF

BSIDES NCL

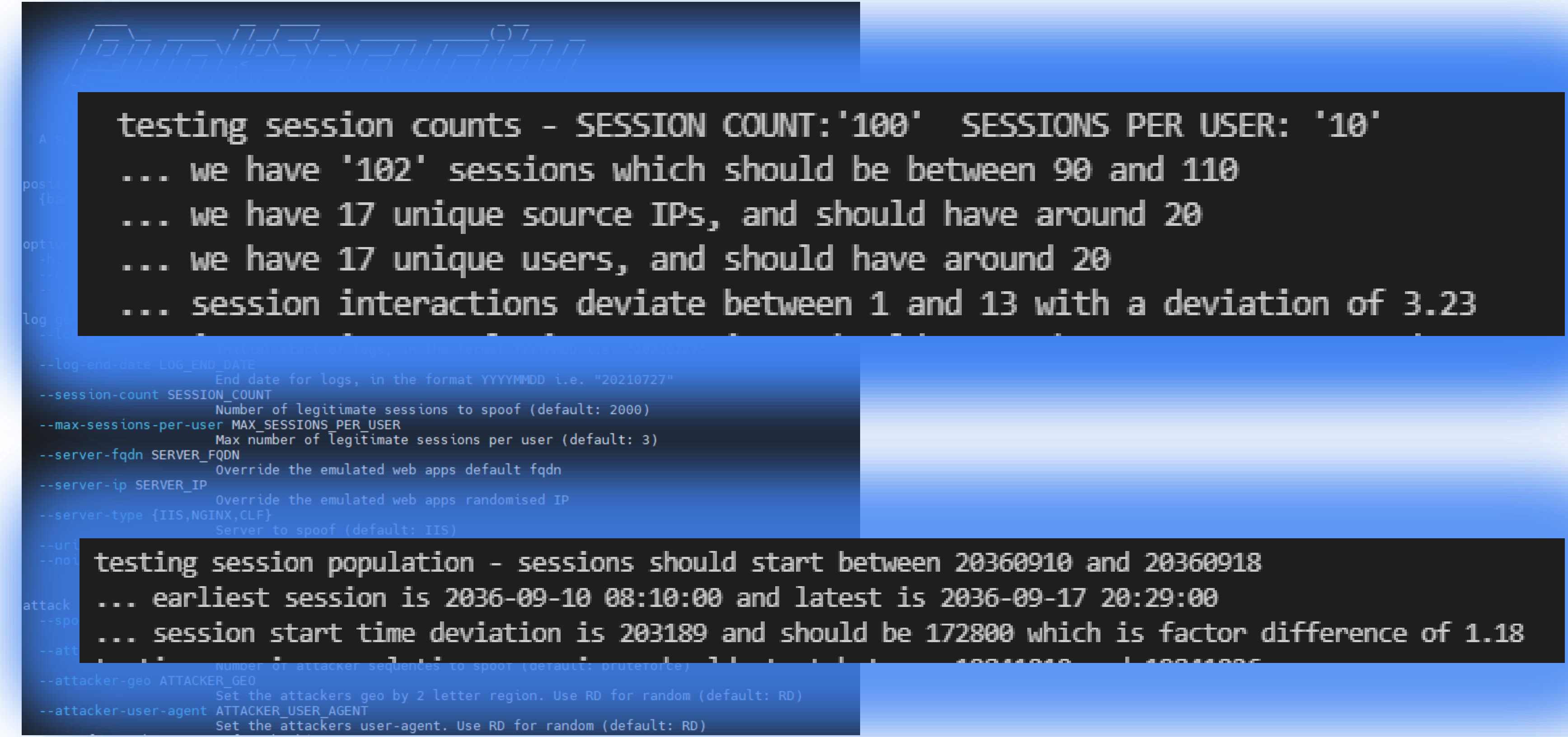
Digital Overdose CTF

Demo

Getting started



```
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
Docker Host >
```



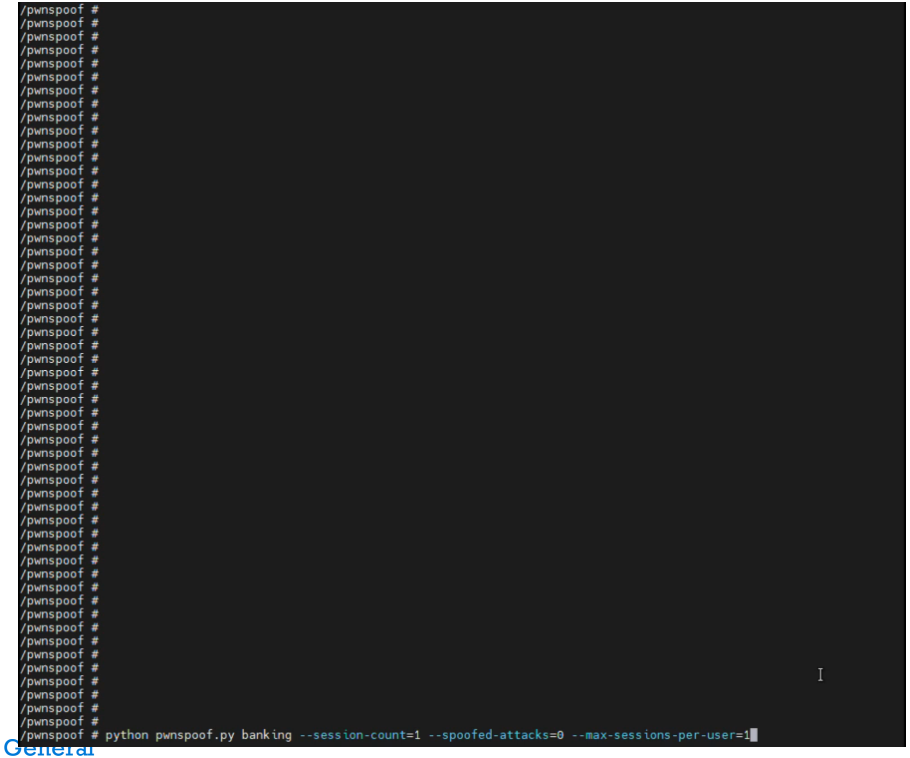
```
testing session counts - SESSION COUNT:'100'  SESSIONS PER USER: '10'
... we have '102' sessions which should be between 90 and 110
... we have 17 unique source IPs, and should have around 20
... we have 17 unique users, and should have around 20
... session interactions deviate between 1 and 13 with a deviation of 3.23
```

```
                        Initial start of logs, in the format YYYYMMDD i.e. "20210727"
  --log-end-date LOG_END_DATE
                        End date for logs, in the format YYYYMMDD i.e. "20210727"
  --session-count SESSION_COUNT
                        Number of legitimate sessions to spoof (default: 2000)
  --max-sessions-per-user MAX_SESSIONS_PER_USER
                        Max number of legitimate sessions per user (default: 3)
  --server-fqdn SERVER_FQDN
                        Override the emulated web apps default fqdn
  --server-ip SERVER_IP
                        Override the emulated web apps randomised IP
  --server-type {IIS,NGINX,CLF}
                        Server to spoof (default: IIS)
```

```
testing session population - sessions should start between 20360910 and 20360918
... earliest session is 2036-09-10 08:10:00 and latest is 2036-09-17 20:29:00
... session start time deviation is 203189 and should be 172800 which is factor difference of 1.18
```

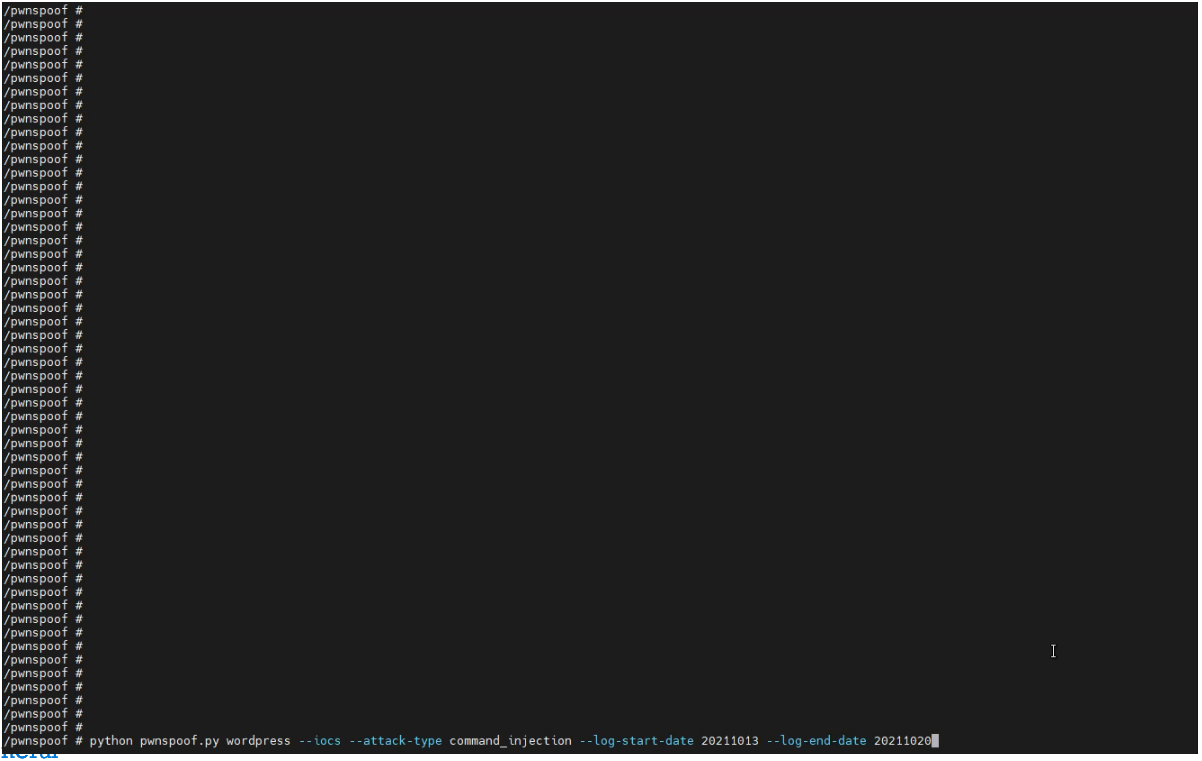
```
                        Number of attacker sequences to spoof (default: bruteforce)
  --attacker-geo ATTACKER_GEO
                        Set the attackers geo by 2 letter region. Use RD for random (default: RD)
  --attacker-user-agent ATTACKER_USER_AGENT
                        Set the attackers user-agent. Use RD for random (default: RD)
```

What does a session look like



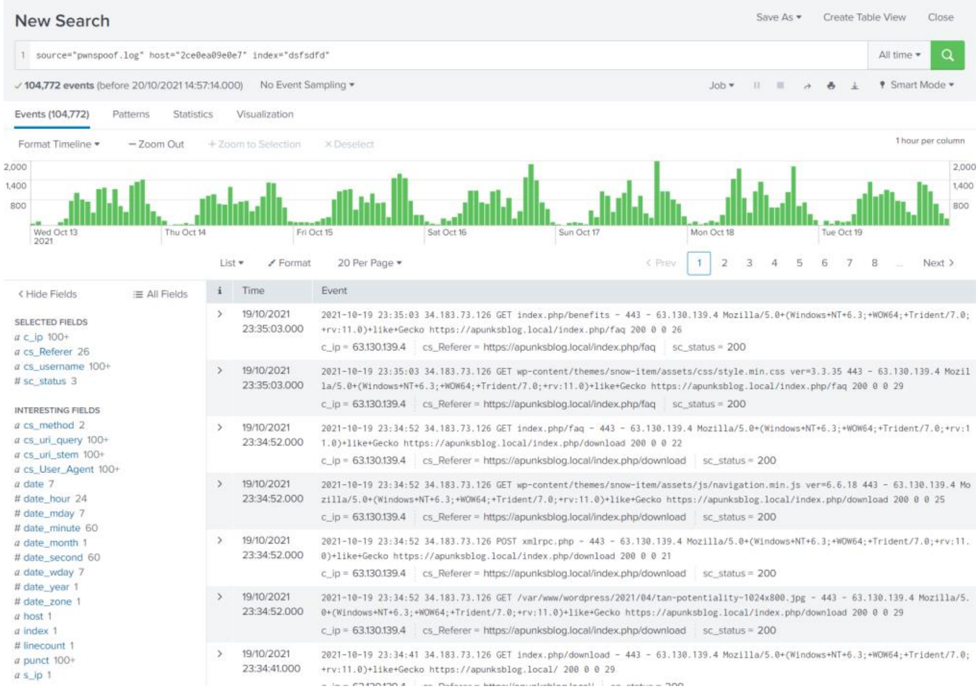
```
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof # python pwnspoof.py banking --session-count=1 --spoofed-attacks=0 --max-sessions-per-user=1
```

IOC output



```
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof #
/pwnspoof # python pwnspoof.py wordpress --iocs --attack-type command_injection --log-start-date 20211013 --log-end-date 20211020
```

Analyzing the logs



```
1  source="pwnspoof.log" host="2ce0ea09e0e7" index="dsfsdfd"
```

✓ 104,772 events (before 20/10/2021 14:57:14.000)   No Event Sampling ▾

SELECTED FIELDS

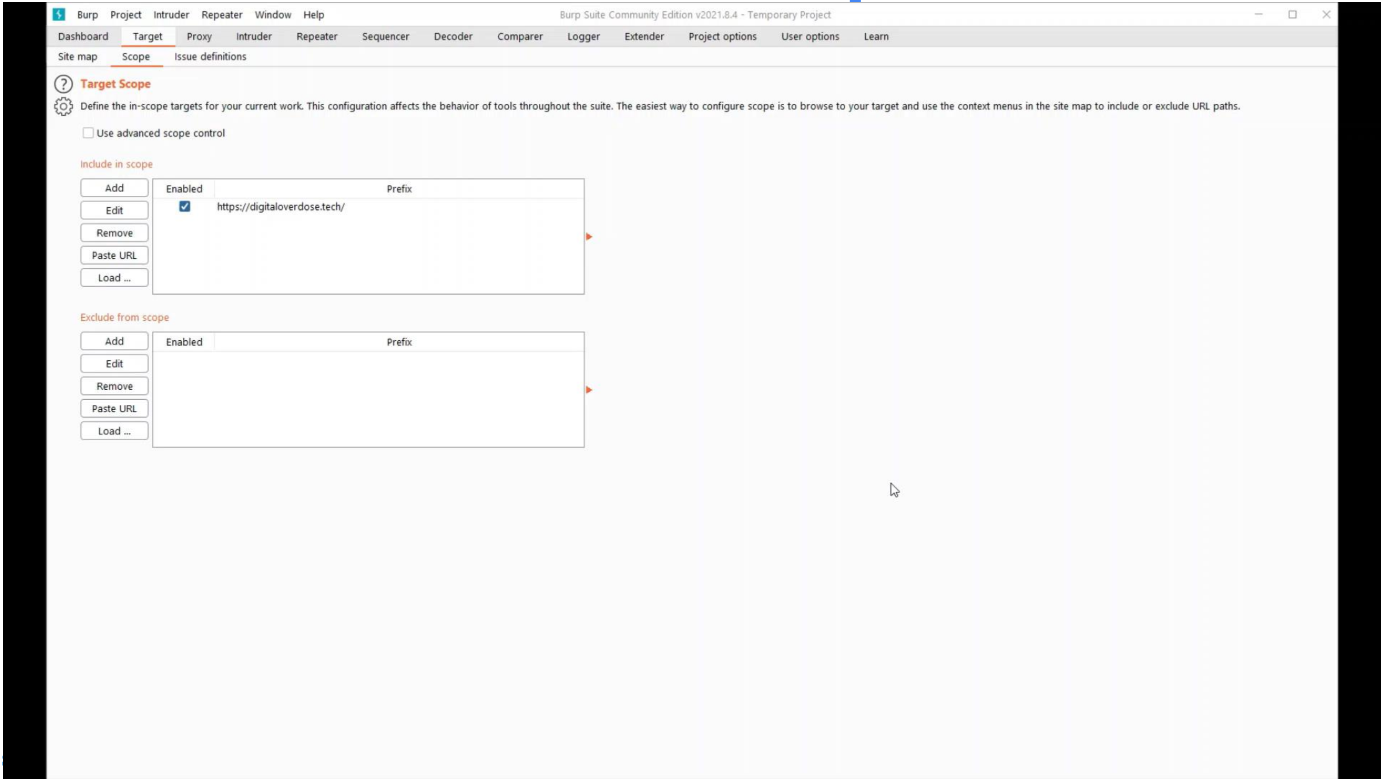
a	c_ip	100+
a	cs_Referer	26
a	cs_username	100+
#	sc_status	3

INTERESTING FIELDS

a	cs_method	2
a	cs_uri_query	100+
a	cs_uri_stem	100+
a	cs_User_Agent	100+
a	date	7
#	date_hour	24
#	date_mday	7
#	date_minute	60
a	date_month	1
#	date_second	60
a	date_wday	7
#	date_year	1
#	date_zone	1
a	host	1
a	index	1
#	linecount	1
a	punct	100+
a	s_ip	1

```
i  Time                     Event
>  19/10/2021 23:35:03.000  2021-10-19 23:35:03 34.183.73.126 GET index.php/benefits - 443 - 63.130.139.4 Mozilla/5.0+(Windows+NT+6.3;+WOW64;+Trident/7.0;
                            +rv:11.0)+like+Gecko https://apunksblog.local/index.php/faq 200 0 0 26
                            c_ip = 63.130.139.4 | cs_Referer = https://apunksblog.local/index.php/faq | sc_status = 200
>  19/10/2021 23:35:03.000  2021-10-19 23:35:03 34.183.73.126 GET wp-content/themes/snow-item/assets/css/style.min.css ver=3.3.35 443 - 63.130.139.4 Mozil
                            la/5.0+(Windows+NT+6.3;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko https://apunksblog.local/index.php/faq 200 0 0 29
                            c_ip = 63.130.139.4 | cs_Referer = https://apunksblog.local/index.php/faq | sc_status = 200
>  19/10/2021 23:34:52.000  2021-10-19 23:34:52 34.183.73.126 GET index.php/faq - 443 - 63.130.139.4 Mozilla/5.0+(Windows+NT+6.3;+WOW64;+Trident/7.0;+rv:1
                            1.0)+like+Gecko https://apunksblog.local/index.php/download 200 0 0 22
                            c_ip = 63.130.139.4 | cs_Referer = https://apunksblog.local/index.php/download | sc_status = 200
>  19/10/2021 23:34:52.000  2021-10-19 23:34:52 34.183.73.126 GET wp-content/themes/snow-item/assets/js/navigation.min.js ver=6.6.18 443 - 63.130.139.4 Mo
                            zilla/5.0+(Windows+NT+6.3;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko https://apunksblog.local/index.php/download 200 0 0 25
                            c_ip = 63.130.139.4 | cs_Referer = https://apunksblog.local/index.php/download | sc_status = 200
>  19/10/2021 23:34:52.000  2021-10-19 23:34:52 34.183.73.126 POST xmlrpc.php - 443 - 63.130.139.4 Mozilla/5.0+(Windows+NT+6.3;+WOW64;+Trident/7.0;+rv:11.
                            0)+like+Gecko https://apunksblog.local/index.php/download 200 0 0 21
                            c_ip = 63.130.139.4 | cs_Referer = https://apunksblog.local/index.php/download | sc_status = 200
>  19/10/2021 23:34:52.000  2021-10-19 23:34:52 34.183.73.126 GET /var/www/wordpress/2021/04/tan-potentiality-1024x800.jpg - 443 - 63.130.139.4 Mozilla/5.
                            0+(Windows+NT+6.3;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko https://apunksblog.local/index.php/download 200 0 0 29
                            c_ip = 63.130.139.4 | cs_Referer = https://apunksblog.local/index.php/download | sc_status = 200
>  19/10/2021 23:34:41.000  2021-10-19 23:34:41 34.183.73.126 GET index.php/download - 443 - 63.130.139.4 Mozilla/5.0+(Windows+NT+6.3;+WOW64;+Trident/7.0;
                            +rv:11.0)+like+Gecko https://apunksblog.local/ 200 0 0 29
                            c_ip = 63.130.139.4 | cs_Referer = https://apunksblog.local/ | sc_status = 200
```

Latest feature – custom endpoints



Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure scope is to browse to your target and use the context menus in the site map to include or exclude URL paths.

☐ Use advanced scope control

Include in scope

Enabled	Prefix
☑	https://digitaloverdose.tech/

Exclude from scope

Enabled	Prefix

ROADMAP

Right now

- ⍰ Functional testing
- ⍰ CI pipelines
- ◍ Be able to pip install it
- ⍰ More apps
- ⍰ More options for CTFs

This year

- ◍ Even more apps
- ◍ Even more attacks
- ⍰ Basic web scraping
- ⍰ Better GEO lookups

Future aims

- ⍰ What else can we spoof?

Q&A