

Attack Surface Management



Winning the battle against Cyber Criminals
i.e., kicking ass

WHO AM I?

PRINCIPAL AND FOUNDER AT RIVER SECURITY
CERTIFIED SANS INSTRUCTOR

SHORT SUMMARY:

I SHOW HOW CRIMINALS BREAK-IN,
AND I HELP THROW THEM BACK OUT...

GCIH	GIAC Certified Incident Handler
GPEN	GIAC Certified Penetration Tester
GSLC	GIAC Security Leadership
GIAC	Mobile Device Security Analyst
GDAT	GIAC Defending Advanced Adversaries
GCTI	GIAC Cyber Threat Intelligence
GCFA	GIAC Certified Forensic Analyst



WHY DO WE DO PENTESTING?

WHAT IS THE GOAL OF A PENETRATION TEST?

High Level Pentest Methodology



Common problems with traditional pentests...

**Receiving a
Pentest**

**Providing a
Pentest**

Procuring and Receiving a Penetration Test

As a client

- What is the scope of the pentest?
 - You might have some idea
 - Very often clients doesn't have the full idea of their own attack surface
- Very often wants a single application pentest
 - Testing one application vs. Testing the organizations resilience against attacks
- The client doesn't know how hackers operate!
- Once a year approach

Providing a Penetration Test

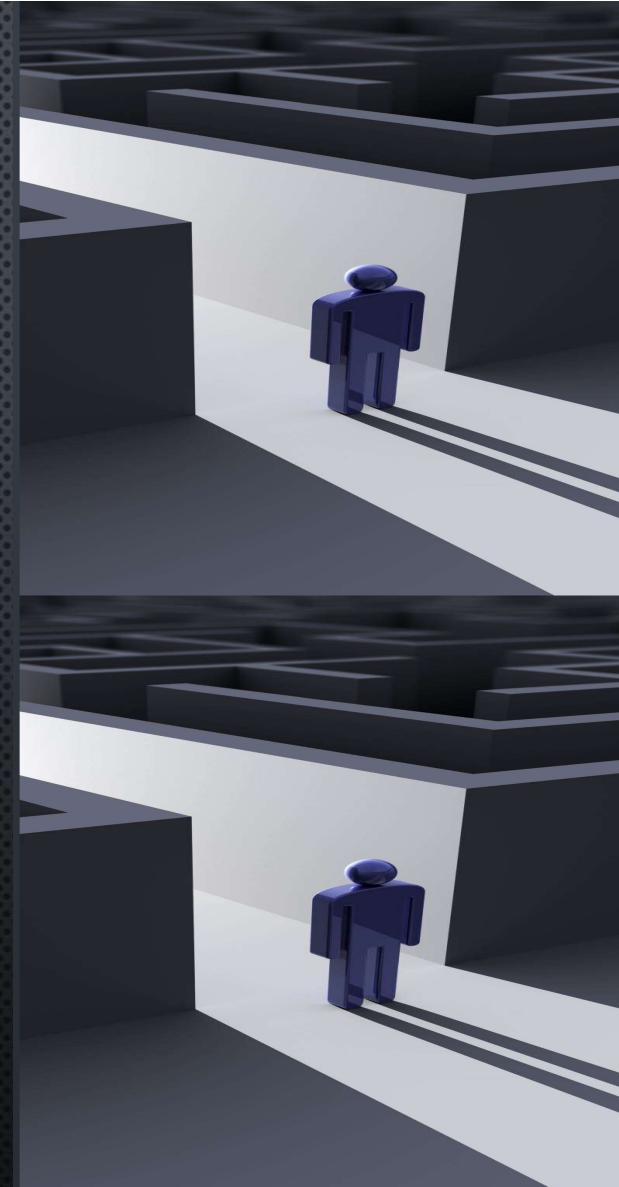
As a Provider

- What is the scope?
 - How do you find out?
 - The customer is likely not to know what their attack surface is
 - Scoping and planning meetings delay the process
- How much is the customer willing to invest?
- Focus on an individual application instead of real-world scenarios
- You start your work, only to be surprised by scope creep

WHAT IS ATTACK SURFACE MANAGEMENT?

ATTACK SURFACE MANAGEMENT

- DISCOVERING OPPORTUNITIES AS COMPANIES INNOVATE AND CHANGE
- RECONNAISSANCE, SCANNING AND DISCOVERY, CONTINUOUSLY
- IDENTIFYING DARK DATA AND SHADOW IT
- FINDING THE PATH LEAST TRAVELLED TO
- KNOWING THE TARGET BETTER THAN THEY KNOW THEMSELVES
- DISCOVERING CHANGES AND OPPORTUNITIES TO ATTACK SURFACE
- WHAT ABOUT THAT DOOR WE LEFT OPEN?





Attackers often get in via the road-less travelled

- How to find the roads less travelled?
- Have the best recon
 - The best recon process
 - The best wordlists
 - Continuous and always-on
- Be inspired by bug-bounty hunters

WHAT IS ALWAYS-ON PENETRATION TESTING

- ASSESSING RISK, CONTINUOUSLY AND ALWAYS PRYING ON OPPORTUNITIES WHICH ARISE
- WEAPONIZATION OF CVE'S
- HIGH FIDELITY ALERTS; ONLY ALERTING ON WHAT MATTERS
- MICRO ENGAGEMENTS INSTEAD OF WEEKLONG ENGAGEMENTS
- DEVSECOPS HAS BEEN A THING FOR A WHILE NOW
- SUCCESSFUL BUG BOUNTY HUNTERS WIN BECAUSE THEY FIND OPPORTUNITIES



The high-level Penetration Test methodology



Some clear benefits



- Client knows what has been left out of scope
- Easier for client to commit on having work done
- Easier to guarantee that the entire scope has been tested
- Immediate value from
 - Things the customer can start working on now
- Customer gets an 3rd party understanding of their attack surface
- Easier on the Penetration Testers while they're doing work

OODA LOOPS

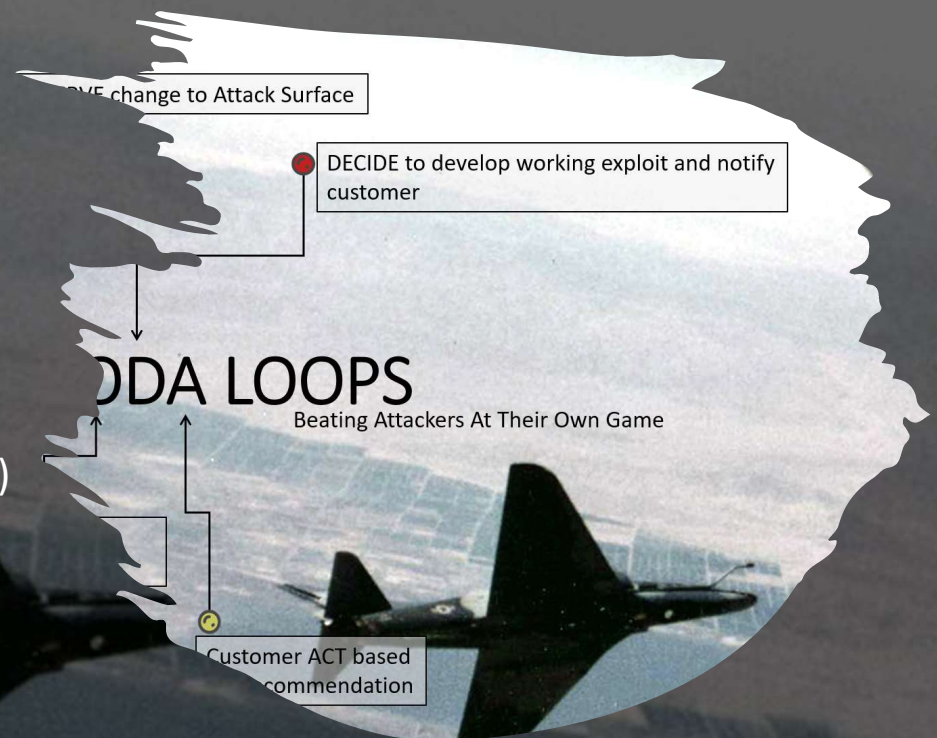
Beat Attackers At Their Own Game!!

Cannot be stressed enough.

How does attackers work?

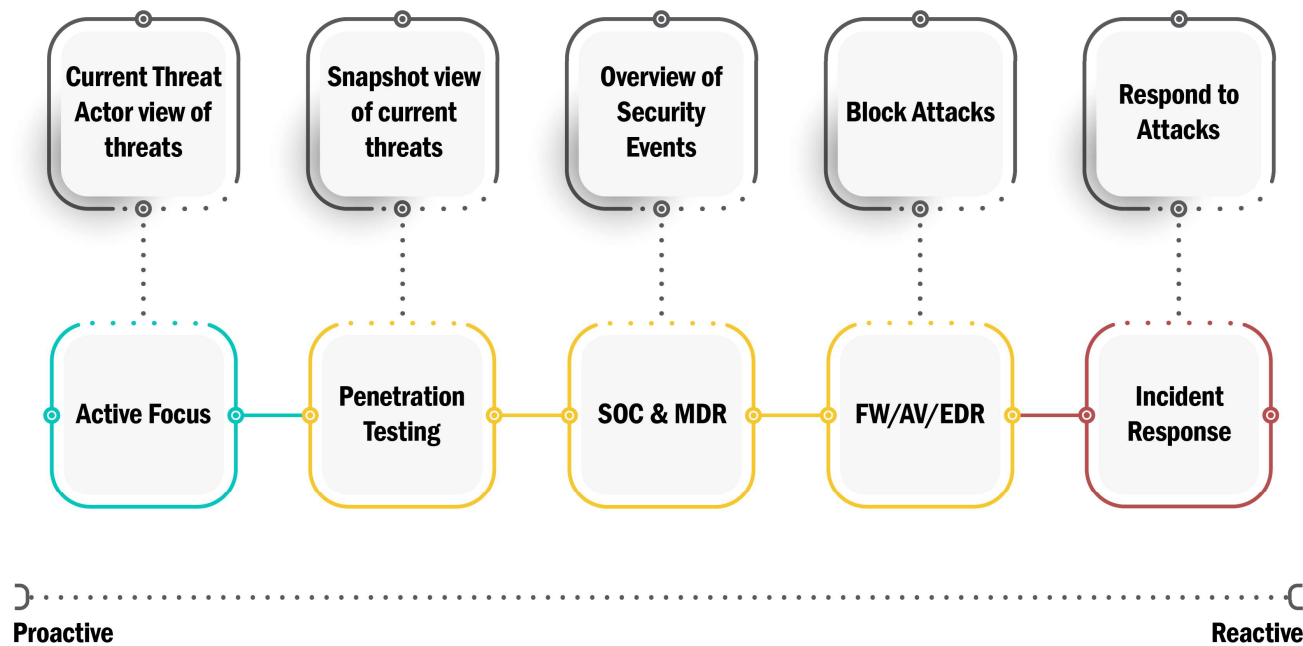
Why is penetration testing in-futile?

Penetration testing must adapt (a long time ago!)





Proactive vs. Reactive



From the outside – threat actors are always-on



HOW WE OPERATE



Certificate Transparency Log

<https://transparencyreport.google.com/https/certificates>
<https://certstream.calidog.io>
<https://crt.sh>

crt.sh
Identity Search
❗
Group by issuer

Criteria
Identity LIKE *.vg.no

Certificates	crt.sh ID	Logged At	Not Before	Not After	Identity	Issuer Name
	1023453909	2018-12-12	2018-12-12	2019-03-12	pay-api.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1023452961	2018-12-12	2018-12-12	2019-03-12	pay-api.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1006659669	2018-12-06	2018-10-26	2019-11-26	id.vg.no	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	993417246	2018-12-03	2018-12-03	2020-01-03	id-pre.vg.no	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	993756380	2018-12-01	2018-12-01	2019-03-01	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	993755638	2018-12-01	2018-12-01	2019-03-01	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	993247873	2018-12-01	2018-12-01	2019-03-01	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	993247240	2018-12-01	2018-12-01	2019-03-01	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	985230465	2018-11-29	2018-11-28	2019-02-26	darkweb.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	985231858	2018-11-29	2018-11-28	2019-02-26	darkweb.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	968838490	2018-11-22	2018-11-22	2019-02-20	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	968837981	2018-11-22	2018-11-22	2019-02-20	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	952503237	2018-11-17	2018-11-16	2019-02-14	es1.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	952500105	2018-11-17	2018-11-16	2019-02-14	es1.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	952508902	2018-11-17	2018-11-16	2019-02-14	phpmyadmin.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	952500254	2018-11-17	2018-11-16	2019-02-14	phpmyadmin.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	947076169	2018-11-15	2018-11-14	2019-02-12	front.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	947075330	2018-11-15	2018-11-14	2019-02-12	front.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	947074392	2018-11-15	2018-11-14	2019-02-12	es1.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	938970872	2018-11-12	2018-11-11	2019-02-09	store.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	938971437	2018-11-12	2018-11-11	2019-02-09	store.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	938967925	2018-11-12	2018-11-11	2019-02-09	einoros.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	938966886	2018-11-12	2018-11-11	2019-02-09	einoros.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	938968059	2018-11-12	2018-11-11	2019-02-09	host.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	938969732	2018-11-12	2018-11-11	2019-02-09	host.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	930604731	2018-11-08	2018-11-08	2019-02-06	chess.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	930604731	2018-11-08	2018-11-08	2019-02-06	sjakk.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	930604802	2018-11-08	2018-11-08	2019-02-06	chess.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	930604802	2018-11-08	2018-11-08	2019-02-06	sjakk.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	929738697	2018-11-08	2018-11-08	2019-02-06	sjakk.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	929738719	2018-11-08	2018-11-08	2019-02-06	sjakk.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	929634844	2018-11-08	2018-11-08	2019-02-06	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

<https://transparencyreport.google.com/https/certificates>

<https://certstream.calidog.io>

<https://crt.sh>

Paying Attention to Changes and Opportunities == Rewards

24 hours from domain was provisioned until compromise


```
chris@DESKTOP-8UENK1V: /mnt/c/Users/chris/Downloads
chris@DESKTOP-8UENK1V:/mnt/c/Users/chris/Downloads$ zcat nodomains.gz | cut -d "|" -f 3 | cut -d "/" -f 3 | sort | uniq
| rev | cut -d "." -f 1,2 | rev | sort | uniq
rev: stdin: Invalid or incomplete multibyte or wide character

123hjemmeside.no
129.132
138wan.com
169.104
17mma.com
183.104
187.68
187.70
187.72
1890.no
1bakuganworld.ru
1kel.no
2009
230.17
230.26
235.104
24blogg.no
39.104
3tblogg.no
40.177
40.180
42.no
44.75
44.98
730.no
77.132
```

URL SHORTENERES MIGHT LEAK INFORMATION

URLTeam over at ArchiveTeam has been doing a brute force against URL Shorteners

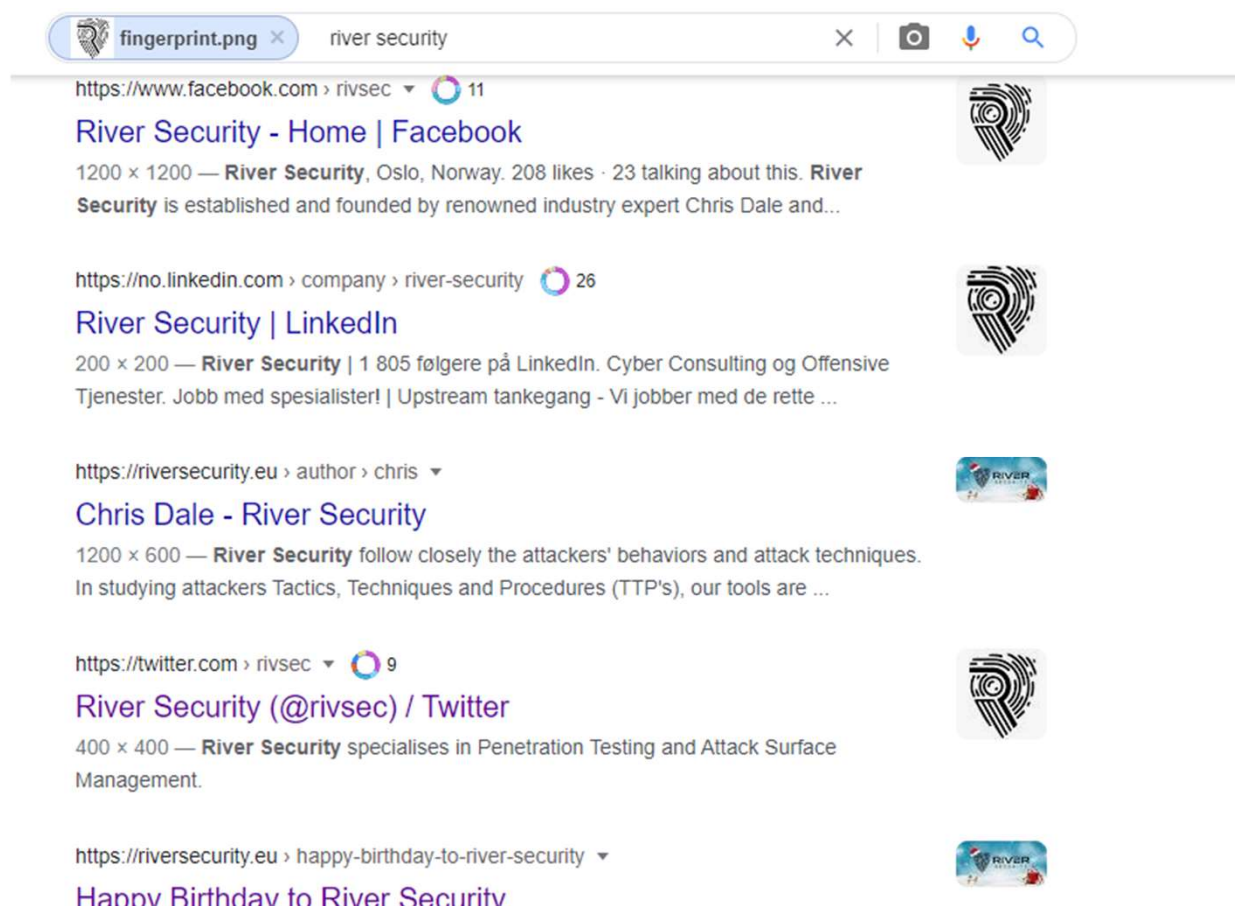
Backup data

Next up in line of examples is backed up data. Many developers and IT-operators make temporary backups available online. While sharing these, it is evident that some of them have used URL shorteners to make life more convenient. This vulnerability classifies as a information leak.

Search term	Example data
<pre>{"wildcard": {"uri_path.keyword": "*.bak"}}</pre>	<pre>uri_path / [REDACTED] ca_20140924_1515.bak /mp/ [REDACTED] moon/415.bak /blog/tag/welcome-0.bak /zh/scanresult/file/[REDACTED] 8adcd350958547e7.bak</pre>
<pre>{"wildcard": {"uri_path.keyword": "*.sql"}}</pre>	<pre>uri_path /[REDACTED] ata-trade.sql /decibel/variant/blob/master/sql/variant.sql /dbdump.sql /[REDACTED] rp_main.sql /[REDACTED] usi.sql /[REDACTED] %20tempdb.sql</pre>

<https://www.sans.org/blog/the-secrets-in-url-shortening-services/>

Reverse Image Searching



The screenshot shows a web browser window with a search bar containing 'fingerprint.png' and 'river security'. The search results are displayed on the left, and a column of image thumbnails is on the right. The results include:

- <https://www.facebook.com/rivsec> 11
River Security - Home | Facebook
1200 x 1200 — **River Security**, Oslo, Norway. 208 likes · 23 talking about this. **River Security** is established and founded by renowned industry expert Chris Dale and...
- <https://no.linkedin.com/company/river-security> 26
River Security | LinkedIn
200 x 200 — **River Security** | 1 805 følgere på LinkedIn. Cyber Consulting og Offensive Tjenester. Jobb med spesialister! | Upstream tankegang - Vi jobber med de rette ...
- <https://riversecurity.eu/author/chris> ▼
Chris Dale - River Security
1200 x 600 — **River Security** follow closely the attackers' behaviors and attack techniques. In studying attackers Tactics, Techniques and Procedures (TTP's), our tools are ...
- <https://twitter.com/rivsec> 9
River Security (@rivsec) / Twitter
400 x 400 — **River Security** specialises in Penetration Testing and Attack Surface Management.
- <https://riversecurity.eu/happy-birthday-to-river-security> ▼
Hannv Birthday to River Security

The image thumbnails on the right correspond to the search results, showing the River Security logo and various profile pictures.

Using trackers to expand the attack surface

```
nmap --script http-tracker_tracking.nse -p 80 -T 4 zonetransfer.me digininja.org -oA tracking
```

```
Starting Nmap 6.00 ( http://nmap.org ) at 2013-03-01 13:46 GMT
```

```
Nmap scan report for zonetransfer.me (217.147.180.162)
```

```
Host is up (0.024s latency).
```

```
PORT      STATE SERVICE
```

```
80/tcp    open  http
```

```
| http-tracker_tracking:
```

```
|   Tracking code: 7503551
```

```
|_  Page title: ZoneTransfer.me - DigiNinja
```

```
Nmap scan report for digininja.org (217.147.180.164)
```

```
Host is up (0.025s latency).
```

```
rDNS record for 217.147.180.164: www.digininja.org
```

```
PORT      STATE SERVICE
```

```
80/tcp    open  http
```

```
| http-tracker_tracking:
```






```
|   Tracking code: 7503551
```

```
|_  Page title: DigiNinja
```

```
Nmap done: 2 IP addresses (2 hosts up) scanned in 0.30 seconds
```


Mobile Applications

MOBILE APPLICATIONS [edit]

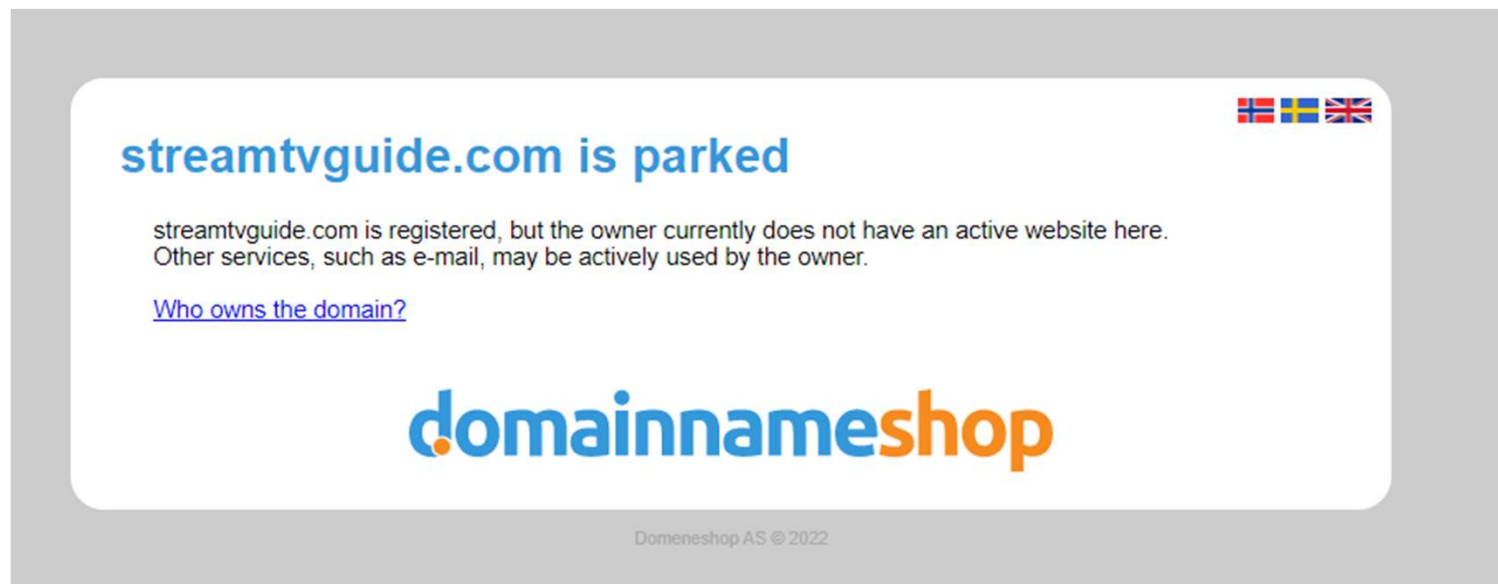
- <https://theappstore.org/> 
- <https://play.google.com/store/search> 
- <https://appworld.blackberry.com/webstore/?countrycode=NO&lang=en> 
- <https://www.microsoft.com> 
- <https://android.fallible.co/> 

403/404/Splash-Pages

- Building great wordlists
 - CEWL is extremely useful
- DNS enumeration
- Content enumeration
- Indexed information in search engines
- VHOST enumeration
- IIS short name scanning
 - Bug bountry tip #1!



Parked Domains





Cyber Warfare vs. Traditional Warfare

"Know yourself, know your enemy, you will not fear the
result of a hundred battles"
Sun Tzu, The Art of War



Defend Forward

Thank You For Your Attention!



<https://into.bio/chrisdale>



Twitter – <https://twitter.com/ChrisADale>



LinkedIn – <https://www.linkedin.com/in/chrisad/>



YouTube – <https://www.youtube.com/c/chrisdale>



SANS Profile – <https://www.sans.org/profiles/chris-dale/>



River Security – <https://riversecurity.eu>

Do attackers care about scope?

- Threat Actors target everything, everyone, and most importantly the low hang fruits.
- CVSS is a problem because not everything is publicly exploitable
- CVSS often rely on a local or authenticated user
- No proof-of-concept is acceptable
- How does criminals operate?
 - Do they weaponize their own CVE's based on CVSS?