Internet-wide Scanning

Lecture & Practical

Jamie O’Hare

@TheHairyJ

Orbital Reconnaissance

Exhaustively discovers publicly accessible risk prone assets

Deloitte left their Active Directory exposed.

With RDP enabled.

A French **Hydroelectric** plant’s control panel was exposed.
Remained online despite flooding in the area.

So you want to Scan the Internet?

No, you don’t

The Scanners

The Usual Suspects

Censys

Founded in 2015, from a research project from University of Michigan

Shodan

Started in 2009 by John Matherly as a market research tool

ZoomEye

Launched in 2013, a product from Knownsec

The Unusual Suspects

BinaryEdge

Been around from 2014, recently gained prominence

Due to constraints, haven't been able to research these much…

GreyNoise

Started in 2017, tells you about what is being scanned!

Anyone have any documentation or insight on ZoomEye? What is available on their website isn’t as in depth as I am looking for

What can I do for you?

I am specifically looking for the location of the crawlers, scanning procedure, ports scanned…

There are no work documents for these issues

The With

Censys

zmap

Created by the same research group

Faster and more random than Masscan

Shodan

“Something similar but not ZMap”

ZoomEye

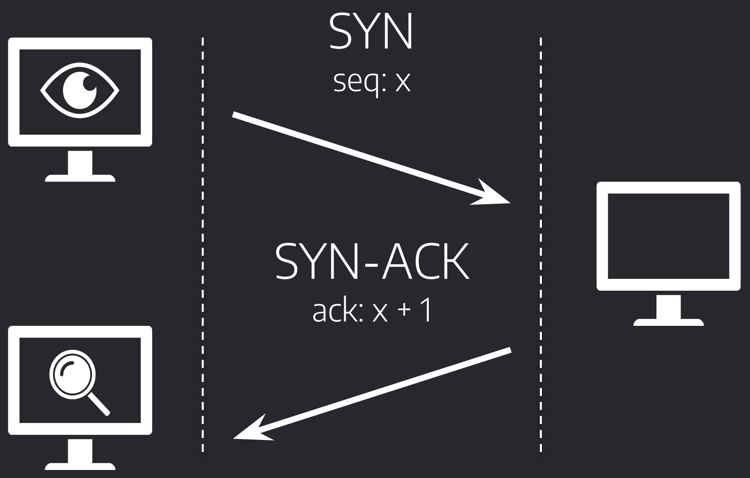
XMap & WMap

For both infrastructure and web-application scanning

Stateless Scanning

Get faster speeds by splitting the scanning process in two

Management of responses can be achieved using SYN Cookies



The What

Censys	Shodan	ZoomEye
27	512	1000
Limited additional support	Support for DBs, RDP and much more	NMap Top 1000 however, uses XMap...

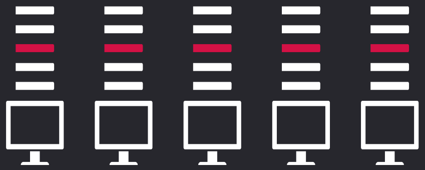
The Data

- Port 80 - HTTP
  - Apache 2.4.10
  - <!DOCTYPE html>
  - WordPress
- Port 443 - HTTPS
  - Heartbleed Check
  - Certificate Information
- Port 554 - RTSP
- Port 11211 - Memcache

49MB

The How

Horizontal



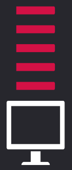
Single port across
multiple systems

ZoomEye

SHODAN

censys

Vertical



Numerous ports across
the same system

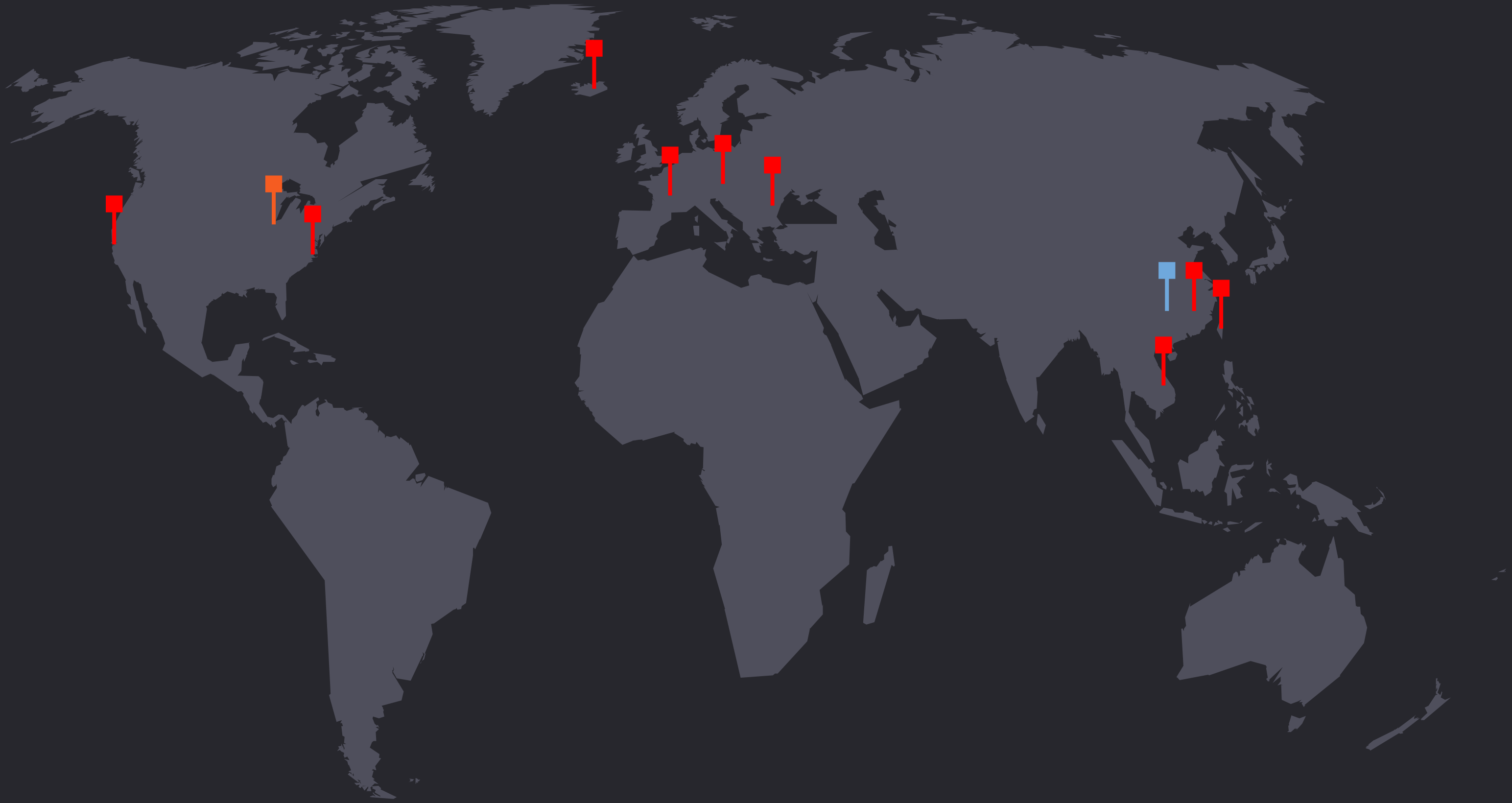
The When

Shodan and ZoomEye are 24/7

Censys uses regimented scans

- Daily, biweekly, weekly
- Take place over 24 hours

The Where



Inherent Latency

There is an inherent latency with using Internet-wide scanning data

Responses need indexed and uploaded, this varies across platforms

Summary

	Scanning	Location	Services
Censys	**Regimental Horizontal ZMap**	**USA**	**27**
Shodan	**Continuous Vertical/Horizontal ZMap-like**	**Worldwide**	**512**
ZoomEye	**Continuous Vertical/Horizontal XMap and WMap (?)**	**China(?)**	**1000(?)**

The Use Cases

Interesting Discoveries

Exposed Databases

292 Databases found within JANET

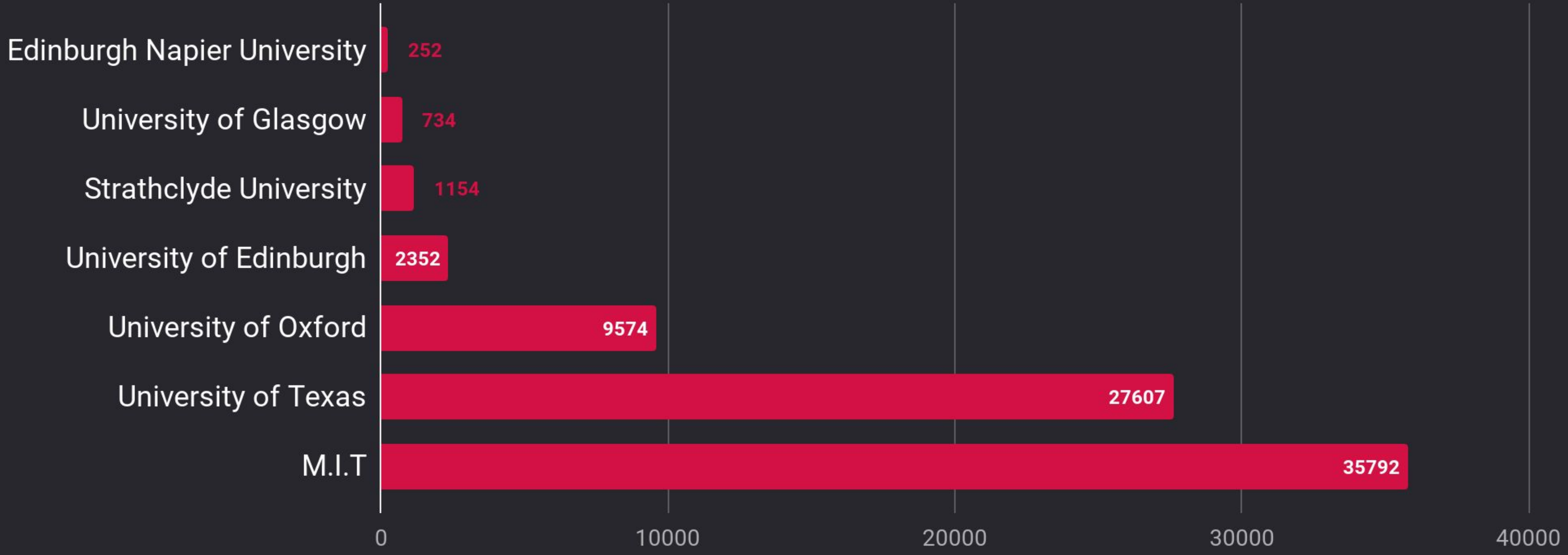
Infected Services

Watch in ‘real-time’ the spread of malware across the Internet

Scary Stuff

Crematorium, rail signal controllers and nuclear power plants

Case Study: Educational Institutes



“Universities are the most insecure organisations out there!”

John Matherly

NCSC’s Minimum Cyber Security Standard

25th June 2018

“Ensure that any infrastructure is not vulnerable to common cyber-attacks”

1st October 2018

Using Censys, one can identify a number of services vulnerable to Heartbleed on JANET

autonomous_system.asn: 786 and 443.https.heartbleed.heartbleed_vulnerable: true

NCSC’s Minimum Cyber Security Standard 2

25th June 2018

“Support TLS v1.2 for sending and receiving email securely”

1st August 2018

Using Censys, one can identify plenty of services on JANET not adhering to this

```
autonomous_system.asn: 786 and 110.pop3.starttls.tls.version: TLSv1.0
```

Identifying Services that could be used in DRDoS attacks

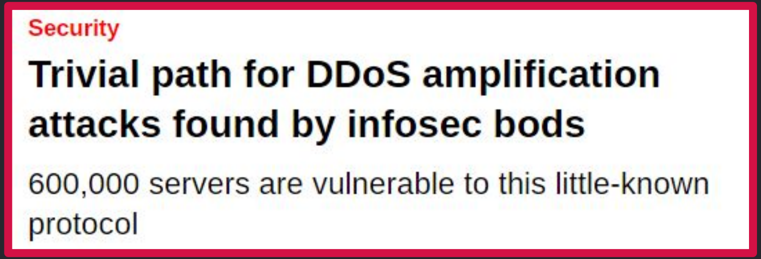
17th January 2014

US-Cert issues an alert listing the services which could be used in DRDoS

20th September 2018

I wrote a blog post, investigating said services within JANET

I found 6204 services, which collectively could amount to a 2242824 amplification factor



Security

Trivial path for DDoS amplification attacks found by infosec bods

600,000 servers are vulnerable to this little-known protocol

Bug Bounties

Twitter

$280

4 SMTP services vulnerable to POODLE via Shodan

@omespino

Grab

$5000

Analytics database exposed due to misconfigured firewall via Censys

@vinodsparrow

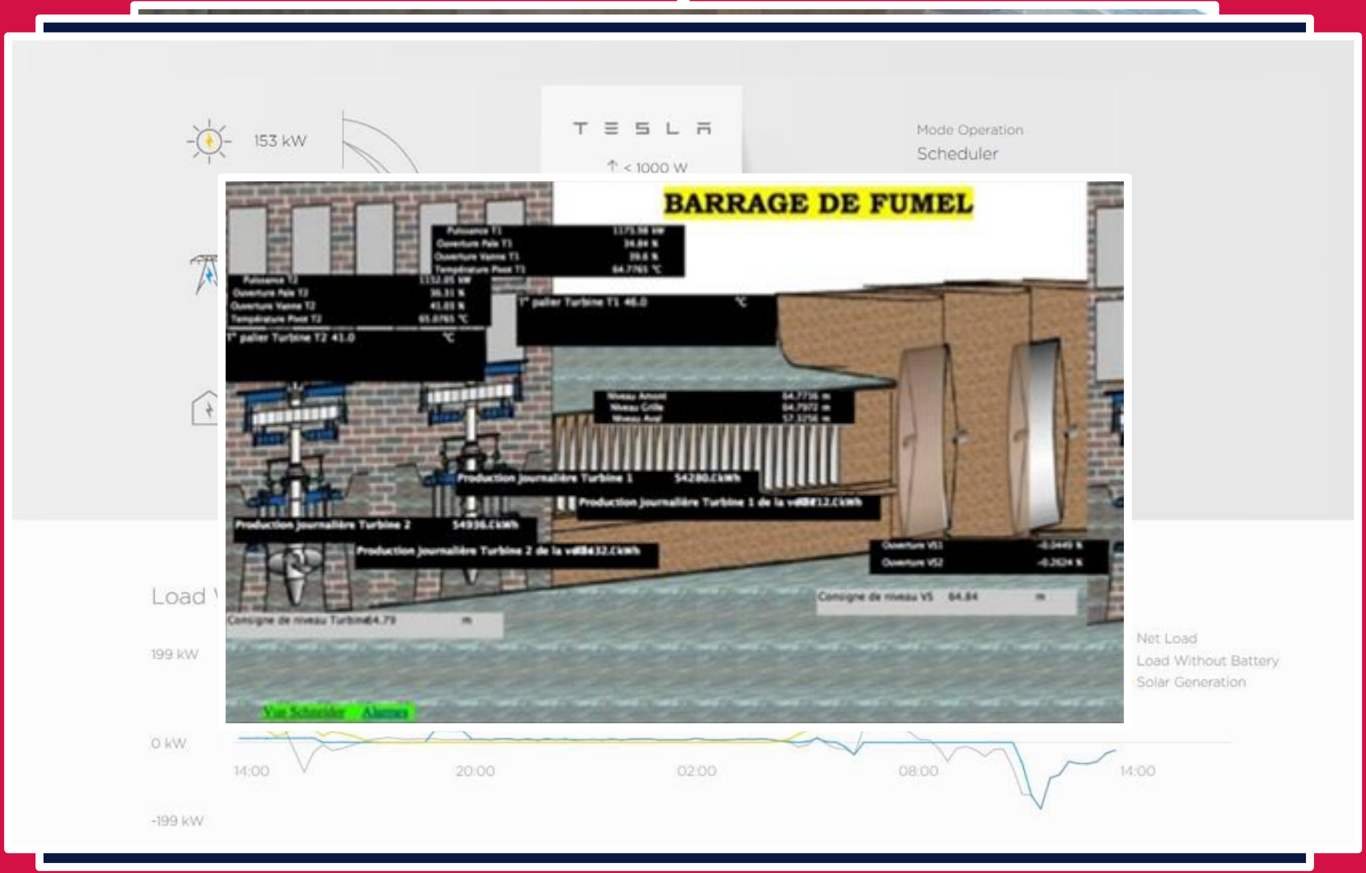
Twitter

$10080

Private Docker registry tied to Vine, hosted on AWS via Censys

@avicoder

Let’s Play A Game



Mode Operation
Scheduler

BARRAGE DE FUMEL

Puissance T1 1175.56 kW
Ouverture Pale T1 34.84 %
Ouverture Vanne T1 39.6 %
Température Pivot T1 64.7765 °C

Puissance T2 1112.05 kW
Ouverture Pale T2 36.31 %
Ouverture Vanne T2 41.03 %
Température Pivot T2 65.0765 °C

1° palier Turbine T2 41.0 °C

1° palier Turbine T1 46.0 °C

Niveau Amont 64.7716 m
Niveau Grille 64.7972 m
Niveau Aval 57.3256 m

Production journalière Turbine 1 54280.CkWh

Production journalière Turbine 1 de la veille12.CkWh

Production journalière Turbine 2 54936.CkWh

Production journalière Turbine 2 de la veille432.CkWh

Ouverture VS1 -0.0449 %
Ouverture VS2 -0.2624 %

Consigne de niveau VS 64.84 m

Consigne de niveau Turbine64.79 m

The Research

The Researchers

University of Arizona

Published multiple exceptional works all across the topic

ICS and SCADA

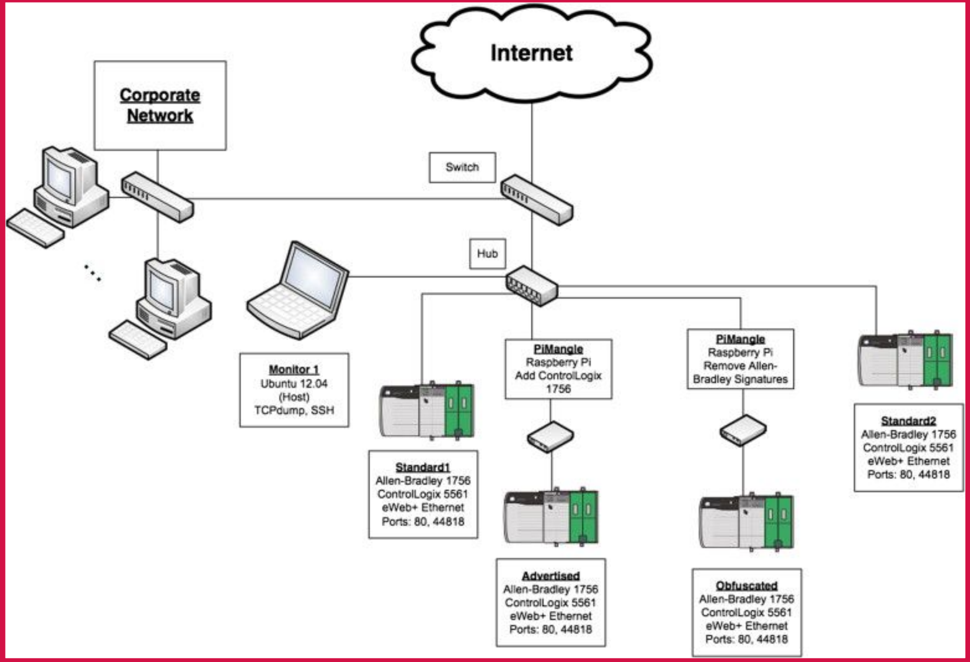
Majority of work is focused here

Vulnerability Scanning

Using the information provided to find vulnerabilities

Industrial Control Systems Identification

Due to the potential damage, ICS and SCADA research is focused quite heavily!

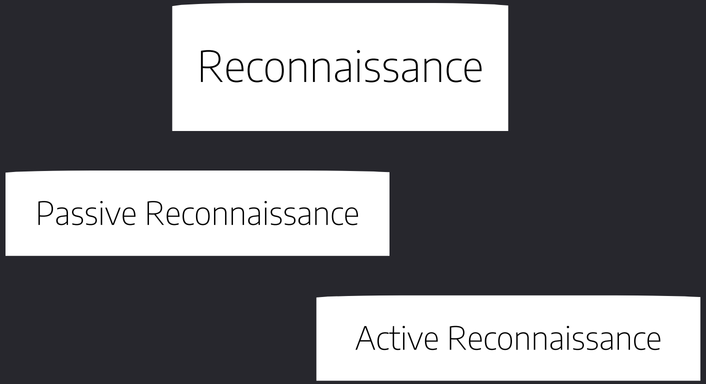


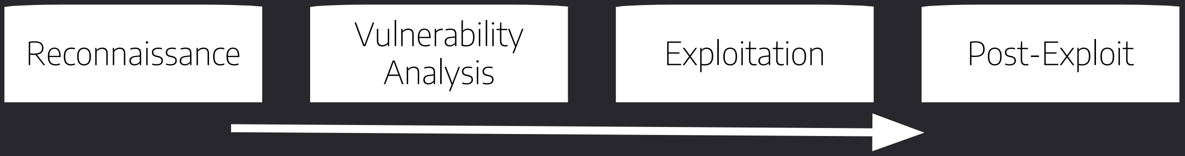
Bodenheimm et al looked at this in a paper in 2014!

The Vulnerability Scanning

It’s *different*

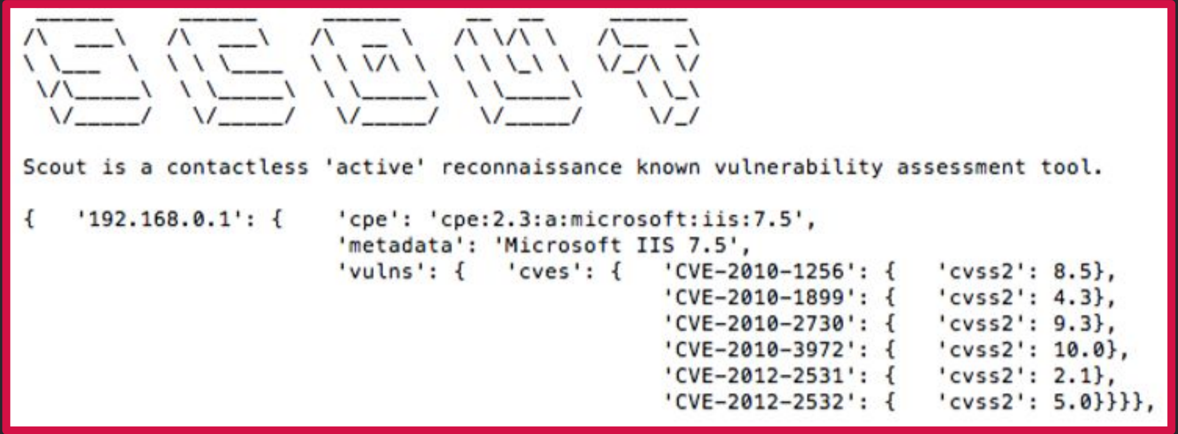
- Gaining information earlier
- Compliment with additional info
- Remember, pinch of salt





Scout: a Contactless Active Reconnaissance Tool

Using Censys data, Scout associates Internet-wide scanning results with National Vulnerability Database entries



```
 ______     ______     ______     __  __     ______  
/\  ___\   /\  ___\   /\  __ \   /\ \/\ \   /\__  _\ 
\ \___  \  \ \ \____  \ \ \/\ \  \ \ \_\ \  \/_/\ \/ 
 \/\_____\  \ \_____\  \ \_____\  \ \_____\    \ \_\ 
  \/_____/   \/_____/   \/_____/   \/_____/     \/_/ 

Scout is a contactless 'active' reconnaissance known vulnerability assessment tool.

{   '192.168.0.1': {     'cpe': 'cpe:2.3:a:microsoft:iis:7.5',
                         'metadata': 'Microsoft IIS 7.5',
                         'vulns': {   'cves': {   'CVE-2010-1256': {   'cvss2': 8.5},
                                                  'CVE-2010-1899': {   'cvss2': 4.3},
                                                  'CVE-2010-2730': {   'cvss2': 9.3},
                                                  'CVE-2010-3972': {   'cvss2': 10.0},
                                                  'CVE-2012-2531': {   'cvss2': 2.1},
                                                  'CVE-2012-2532': {   'cvss2': 5.0}}}},
```

NVD

OpenVAS

When compared to OpenVAS, Scout was able to return results with an effectiveness of 74%!

The Conclusion

There is more than Shodan

Expand your tool box

Don’t advertise your services

Make it require more effort

Use Internet-wide Scanning for good

Keep an eye on your digital footprint

THANKS!

Any Questions, feel free to ask during the practical session!

enusec.org/IWS.pdf