

OSINTを活用した データ収集の方法

ムンジェウン(2017.12.5)

目次

- OSINTとは？
- Maltego活用とデモ
- Shodan活用とデモ
- Google検索活用とデモ
- Q & A

1. OSINTとは?

OSINT概要

- OpenSource Intelligenceの略語
- 「オシント」と発音
- 諜報活動分野の一つ
- ヒューミント(HUMINT) - 人間情報
- シギント(SIGINT) - 信号情報
- テキント(TECHINT) - 技術情報



出所: <http://www.pentesteracademy.com/course?id=29>

OSINT概要

ジェームズ・ウルシ元CIA局長

“すべての情報の95%は公開されたソースで、
残りの5%だけが秘密の情報源から出てくる。”



出所: <https://www.voakorea.com/a/4127320.html>

OSINT登場の背景

- インターネットの普及によりインターネット上の公開情報 (Open Source) が爆発的に増加
- あふれる情報の中から、現在の主要な問題に対し、適切かつ有益な情報を抽出することが重要になる。
- 2001年9月11日のテロ以降に急速に適用
- 事前に無数の情報があったにもかかわらず、措置を取れずにテロ攻撃を受けたため



OSINT登場の背景

- 2002年に米国国土安全保障省が設立
(現在の規模は20万人以上)
- 日本の場合、内閣情報調査室や公安調査庁で
当該業務をすることが知られている



出所: https://en.wikipedia.org/wiki/United_States_Department_of_Homeland_Security

OSINTその他

- インターネットがなかった時代にも存在していた概念
- 昔は報道機関や大学などがその役割を担うが、現在では、インターネットがその役割を果たす
- インターネット上の世界最大の民間OSINTサイトはウィキペディア



出所: <http://www.bloter.net/archives/179278>

2. Maltego活用とデモ



Maltegoとは？

- データ・マイニングツール
- インターネット上に存在する公開データ (Open Source) を収集し、そのデータ間の関係を可視化する。
- Written in JAVA
- 今回は無料(コミュニティ)バージョンであるMaltego CEを使用
- KaliLinuxには、デフォルトでインストールされている。



デモ1

- ある組織の公開された電子メールアドレスを収集する

デモ2

- ある人が主に使用するWebサイトを調査する

デモ3

- ある組織のインフラストラクチャーとネットワーク構造を把握する

3. Shodan活用とデモ

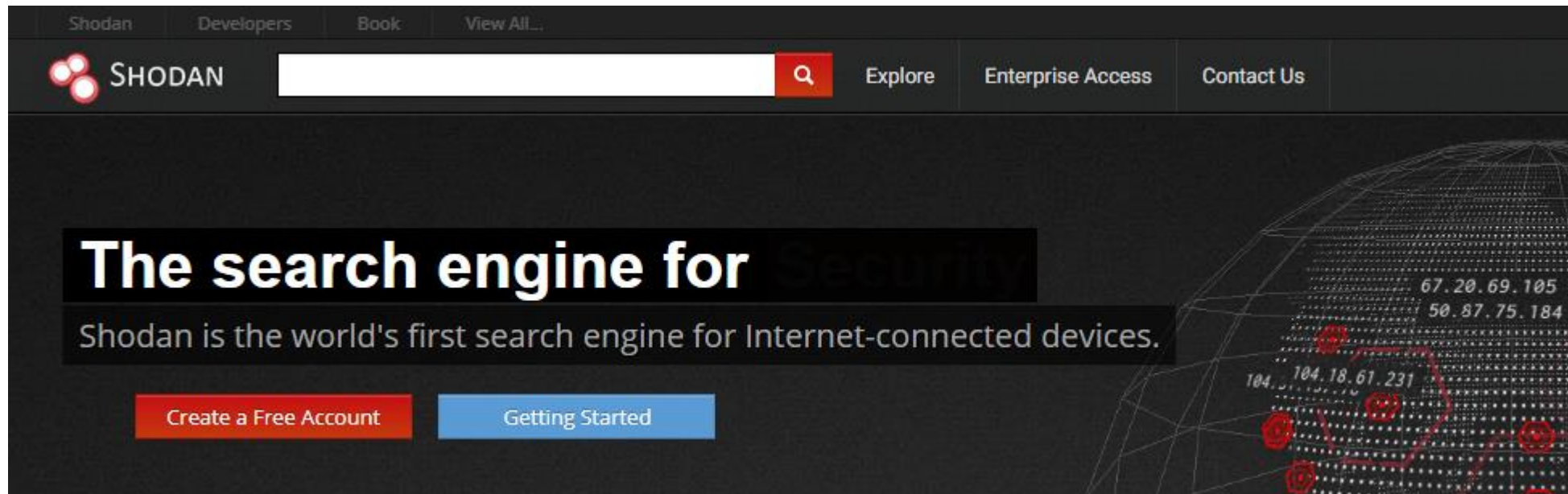
Shodanとは?

- 公開されたIOT機器を検索してくれるエンジン
- バックドアが露出されたルータ、安全でないウェブカメラ、産業用制御システムなどを探す
- 最も人気のあるのは、世界中のウェブカメラ
- 有料でAPIを使用したデータ取得もできる
- www.shodan.io



使い方

- 使い方は簡単
- 検索ウィンドウに検索文字列を入力
- 国別、プロトコル別、製品別に検索件数を知らせる。



デモ1

- パスワードなしで公開されたウェブカメラの検索
- webcamxp
- より詳しく検索したい場合は、演算子を使って検索
- 演算子検索はログインが必要
- `webcamxp country:"KR" city:"Seoul"`

デモ2

- デフォルトのパスワード(admin/ admin)になっているウェブカメラを検索
- linux upnp **avtech** country:JP

公開されているデフォルトパスワード

ACTi: admin/123456 or Admin/123456

Axis (traditional): root/pass,

Axis (new): requires password creation during first login

Cisco: No default password, requires creation during first login

Grandstream: admin/admin

IQinVision: root/system

Mobotix: admin/meinsm

Panasonic: admin/12345

Samsung Electronics: root/root or admin/4321

Samsung Techwin (old): admin/1111111

Samsung Techwin (new): admin/4321

Sony: admin/admin

TRENDnet: admin/admin

Toshiba: root/ikwd

Vivotek: root/<blank>

WebcamXP: admin/ <blank>

出処: <https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-webcams-across-globe-using-shodan-0154830/>

デモ3

- 公開されたスクリーンショットを検索

has_screenshot: -port:3389 -port:3388 -port:5900 -port:5901 -
port:6000 country:"RU"

4. Google Search










検索演算子

- site : 該当サイトのみ検索
- intitle : タイトルに含まれている文字列を検索
- "" : 完全一致検索
- * : すべて検索

デモ

- 日本のサイトの中でディレクトリが公開されている管理者関連ページを検索
- すべての日本のサイト=> **site:*.jp**
- ディレクトリインデックス=> **intitle:"index of"**
- 管理者関連=> **admin** キーワード

Index of /typo3conf/ext

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 automaketemplate/	23-Nov-2011 21:07	-	
 introduction/	23-Nov-2011 21:07	-	
 jquerycolorbox/	23-Nov-2011 21:07	-	
 realurl/	23-Nov-2011 21:07	-	
 tt_news/	23-Nov-2011 21:07	-	
 wt_spamshield/	23-Nov-2011 21:07	-	

Apache/2 Server at example.org Port 80

要約

- 近年OSINTの重要性が高まっており、支援するツールが幾つか存在する。
- Maltegoを使用して公開情報を可視化することができる。
- Shodanを使用してIOT機器を検索することができる。
- Google検索演算子を使用して、高度な検索を行うことができる。
- このようなツールの登場で、個人でもかつて国家機関で行っていた水準で情報収集を行うことができるようになった。

An aerial photograph of a city skyline, likely New York City, is shown in a dark blue, semi-transparent overlay. The skyline features numerous skyscrapers, including the Empire State Building and the Chrysler Building. The text "Q & A" is centered over the image in a white, serif font.

Q & A

ありがとうございます！