

Cybersecurity **Offensive** and Defensive Techniques in 3 Hours

Omar Santos



AGENDA

- Understanding **Offensive** and **Defensive** Security Methodologies
- So, You Want to Be a Hacker? What are the cybersecurity skills that are necessary in today's environment?
- How to Build, Manage, and Operate Cybersecurity Teams
- Introduction to Threat Hunting
- Effective Threat Intelligence
- Enterprise-wide Ethical Hacking and Continuous Monitoring

POLL 1

What is your level of familiarity with Cybersecurity?

1. Beginner (less than 1 year of experience).
2. Intermediate (2-3 years of experience)
3. Expert (considerable DFIR experience).

POLL 2

Why are you interested in this course?

1. Just curious and want to learn more about Cybersecurity Red/Blue Teams.
2. I am preparing for a cybersecurity certification.
3. I am part of a Red Team.
4. I am part of a Blue Team.

Understanding Offensive and Defensive Security Methodologies



What is a Red Team?

An **offensive security** team that will perform an organizational assessment beyond a traditional penetration testing engagement.

A **red team** can be comprised of full-time employees of an organization or it can be contracted (outsourced).

What is a Blue Team?

A dedicated defensive security team (or teams) that will monitor and defend the organization against cybersecurity incidents.

A blue team can also be comprised of full-time employees (often different teams) of an organization or it can be contracted (outsourced to a managed security service provider (MSSP)).

Why Red Teaming?

Adversarial testing process (mimicking a real-life threat actor).

Red teams focus on organizational assessments vs. testing a specific target (depending on the organization's objective).

Red teams can also target humans and use social engineering.

Red teams often create custom exploits for specific vulnerable systems.

Additional Reference: <http://h4cker.org/rb/1>

Incorporate Business Processes

Red Teams often incorporate business processes such as:

- Evaluating new vendors and their products get incorporated into the corporation
- Evaluating how new employees get onboarded.

Tradecraft:

“...within the intelligence community, refers to the techniques, methods and technologies used in modern espionage (spying) and generally, as part of the activity of intelligence. This includes general topics or techniques (dead drops, for example), or the specific techniques of a nation or organization”.

Understanding the **Red Team** Environment

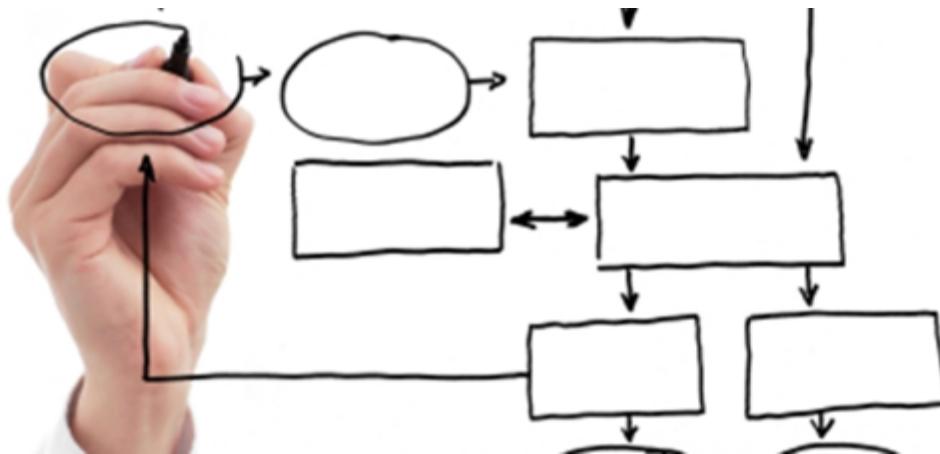
What is the goal of having the red team?

Who do they report to?

How is it structured?

Hacking is a lot
more than cool
tools...

- Methodologies
- Research
- Think like an attacker
- Combine social engineering with technical capabilities



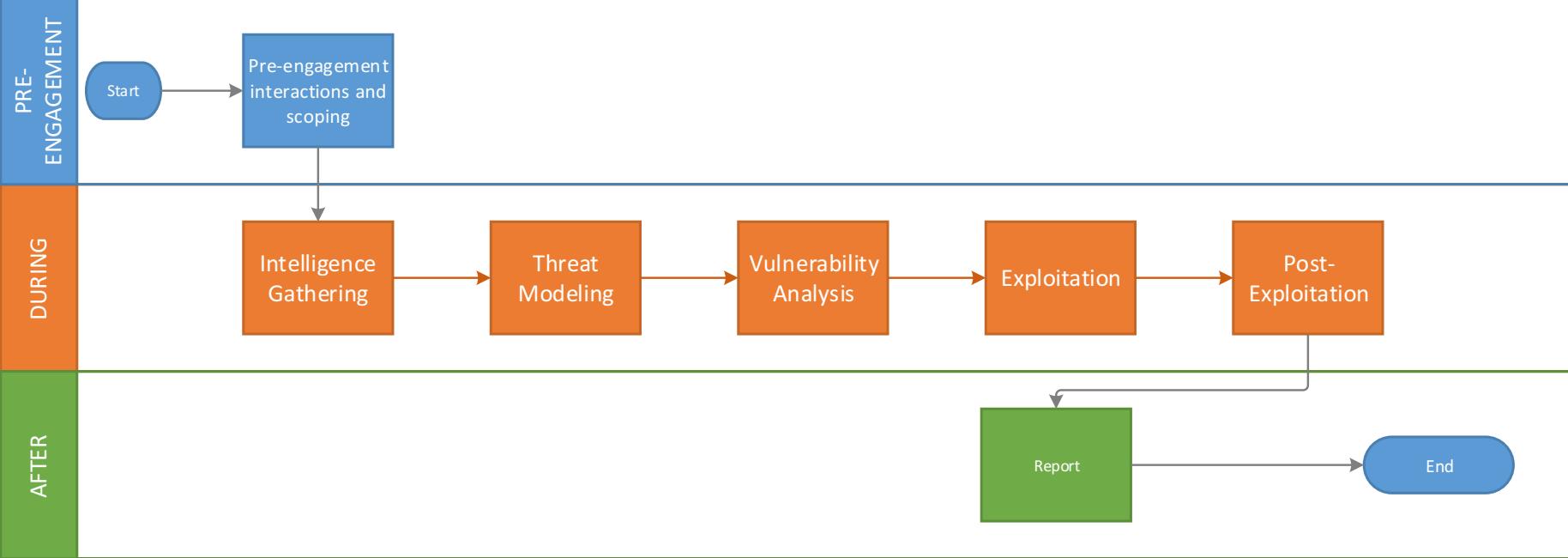
Are **Red Team** Methodologies the same as traditional
penetration testing?

PEN TESTING METHODOLOGIES

- Penetration Testing Execution Standard
<http://www.pentest-standard.org>
- OWASP Testing Guide
https://www.owasp.org/index.php/OWASP_Testing_Project
- NIST 800-115: Technical Guide to Information Security Testing and Assessment
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
- Open Source Security Testing Methodology Manual (OSSTMM)
<http://www.isecom.org/research/>

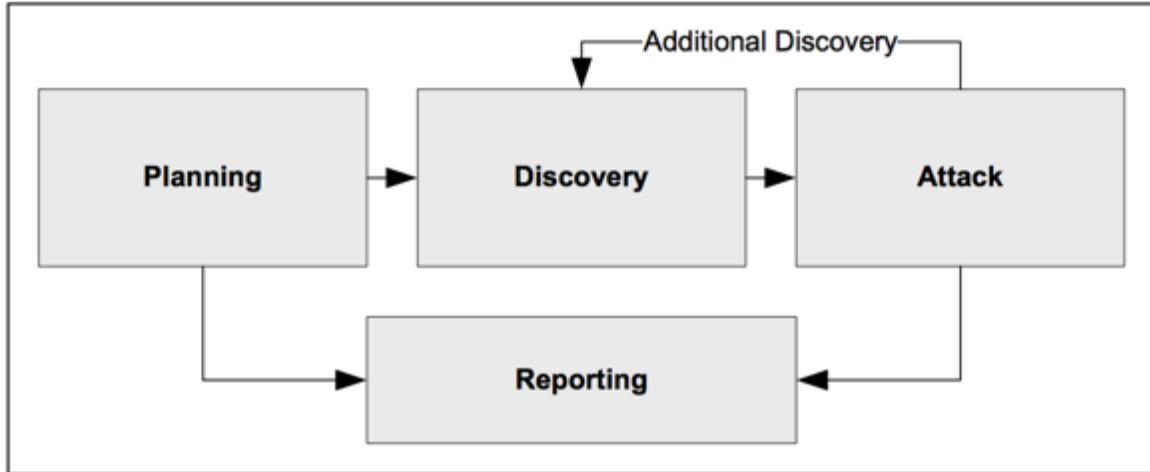


PEN TESTING LIFECYCLE



Aligned with: <http://www.pentest-standard.org>

NIST 800-115



<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>

Scope

Scope in Traditional Penetration Testing vs. Red Teams Engagements

Additional Reference and Video: <http://h4cker.org/rb/2>

Social Engineering and How to Target Employees

Additional Reference and Video: <http://h4cker.org/rb/3>

Internal and External Recon

Internal and external recon in red teams include the elements of passive and active recon in traditional pen testing; however, it also entails additional enterprise-wide methodologies.

For example, a red team member could already have access to internal email archives, forums, bug databases, code repositories, etc.

Reports are different...

Additional Reference and Video: <http://h4cker.org/rb/2>

Persistent Access: For How Long?

Additional Reference and Video: <http://h4cker.org/rb/5>

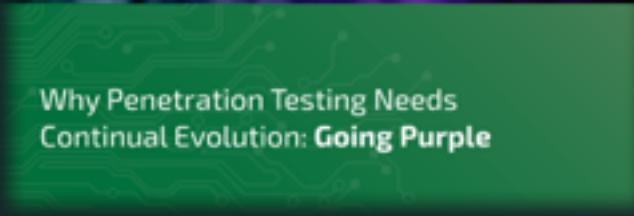
The Hybrid Approach: Purple Teams



The concept of Purple Teams

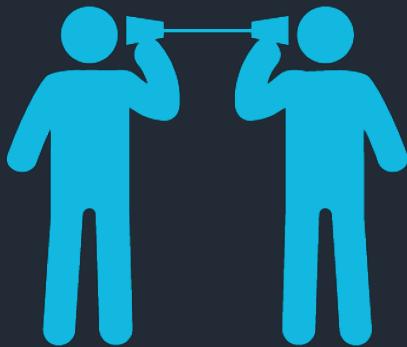
Why Penetration Testing Needs
Continual Evolution: Going Purple

<https://github.com/The-Art-of-Hacking/web/blob/master/references/ts-whitepaper.pdf>



Regardless of the terminology or what is being used, the Purple Team concept can be applied to each of these based on the level of maturity of the organization.

Why Penetration Testing Needs
Continual Evolution: Going Purple



Communication Among All Cybersecurity Teams

Additional Reference and Video: <http://h4cker.org/rb/2>

So, You Want to Be a Hacker?
What are the cybersecurity
skills that are necessary in
today's environment?

How are you planning to continue learning and enhancing your cybersecurity skills?

- A. Not planning to continue to develop cybersecurity skills
- B. Industry certifications
- C. Two-year college degree
- D. University / bachelors degree
- E. Post-graduate degree

The Art of Hacking

To all to whom these presents shall come, Greeting
Be it known that

Omar Santos

having honorably fulfilled all the requirements imposed by the authorities of this
Institution, the President and the trustees of The Art of Hacking, upon
recommendation of the faculty, do therefore confer the degree of

Doctor of Nothing

with all the Honors, Rights, and Privileges to that degree appertaining.



Clark Kent
University President

Bruce Wayne
Vice President

CYBERSECURITY AND ETHICAL HACKING CERTIFICATIONS

Certified Ethical Hacker X

Secure | https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

EC-Council
Hackers are here. Where are you?

GET TRAINING! PARTNER WITH US

HOME PROGRAMS EVENTS DEGREES CONSULTING SERVICES RESOURCES ABOUT

Master
The Core Technologies Of
Ethical Hacking

DOWNLOAD OUR CERTIFICATION TRACK

Download Now

Certified Ethical Hacking Certification

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

The purpose of the CEH credential is to:

- Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures.
- Inform the public that credentialed individuals meet or exceed the minimum standards.
- Reinforce ethical hacking as a unique and self-regulating profession.

About the Exam

Chat With Us

<https://www.eccouncil.org/programs/certified-ethical-hacker-ceh>



CORE SKILLS CERTIFICATIONS



INTERMEDIATE



INTERMEDIATE

ADVANCED



Information Security Certifications

Hands-on information security certifications training by Offensive Security.

Information Security Certifications

For Pen Testers and IT Security Professionals

In-demand **Information Security Certifications** and hands-on ethical hacking courses for pen testers and IT security professionals. These ethical hacking certifications are provided by Offensive Security, the creators of Kali Linux.

Accompanying our **hands-on security training** programs are a set of industry leading **Information Security Certifications**, which are considered the most rigorous tests of skill available in the computer security field. These **performance-based certifications** rely entirely on **demonstrated ability and merit**. Instead of relying on outdated multiple choice questions, candidates are presented with a series of **real-world hacking challenges** which they must complete in a limited amount of time. Pass or fail is **based on your actual performance**. From the best penetration testing training comes the **best information security certifications**.



BECOME CERTIFIED NOW!
REGISTER TODAY

<https://www.offensive-security.com>

GIAC Penetration Testing Certification

The screenshot shows a web browser displaying the GIAC Certifications website at <https://www.giac.org/certifications/pen-testing>. The page title is "GIAC Certifications: Penetration Testing". The main content area describes penetration testing as a craft focused on improving security through methodology. It highlights GIAC Certifications developed with these principles in mind to ensure ethical hackers achieve certified status. A table lists two certifications: GCIH (Certified Incident Handler) and GPEN (Certified Penetration Tester). The GCIH row includes a "Register Now" button. The right sidebar lists categories: Cyber Defense, Penetration Testing, Incident Response and Forensics, Management, Audit, Legal, Developer, Industrial Control Systems, and GSE.

Penetration Testing		
	Certification	Register
	<p>GCIH holders have demonstrated their ability to manage security incidents by understanding common attack techniques, vectors and tools as well as defending against and/or responding to such attacks when they occur. The GCIH certification focuses on methods used to detect, respond, and resolve computer security incidents.</p> <p>Affiliated Training:</p> <p>SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling</p>	Register Now
	<p>GPEN holders have demonstrated their ability to execute penetration testing and ethical hacking.</p>	

Categories

- Cyber Defense*
- Penetration Testing*
- Incident Response and Forensics*
- Management, Audit, Legal*
- Developer*
- Industrial Control Systems*
- GSE*

<https://www.giac.org/certifications/pen-testing>

ISC² CERTIFICATIONS



Certified
Information
Systems Security
Professional



Certified
Cloud
Security
Professional



Certified
Cyber
Forensics
Professional



Systems
Security
Certified
Practitioner



Certified
Authorization
Professional



HealthCare
Information
Security
and Privacy
Practitioner



Certified
Secure
Software Lifecycle
Professional

<https://www.isc2.org>

Certification Tracks	Entry	Associate	Professional	Expert	Architect
Cloud	CCNA Cloud	CCNP Cloud			
Collaboration	CCNA Collaboration	CCNP Collaboration	CCIE Collaboration		
Cybersecurity Operations	CCNA Cyber Ops				
Data Center	CCNA Data Center	CCNP Data Center	CCIE Data Center		
Design	CCENT	CCDA	CCDP	CCDE	CCAr
Industrial		CCNA Industrial			
Routing and Switching	CCENT	CCNA Routing and Switching	CCNP Routing and Switching	CCIE Routing and Switching	
Security	CCENT	CCNA Security	CCNP Security	CCIE Security	
Service Provider		CCNA Service Provider	CCNP Service Provider	CCIE Service Provider	
Wireless	CCENT	CCNA Wireless	CCNP Wireless	CCIE Wireless	

The concept of Purple Teams

<https://github.com/The-Art-of-Hacking/web/blob/master/references/ts-whitepaper.pdf>

BREAK



REMEMBER TO CHECK OUT THE RESOURCES AT:

<https://theartofhacking.org>

<https://theartofhacking.org/training>

<https://theartofhacking.org/github>

https://theartofhacking.org/go/training_resources.pdf

How to Build, Manage, and Operate Cybersecurity Teams





Understand the mission of the red team.

Management sponsorship.

Secure and justify funding.

Understand and create operational processes and policies for the Red Team



What skills?

Who should you hire?

Technical skills across all your technologies. Is it feasible?

What about administrative skills?



Set clear objectives

Get the right tools

Support the team

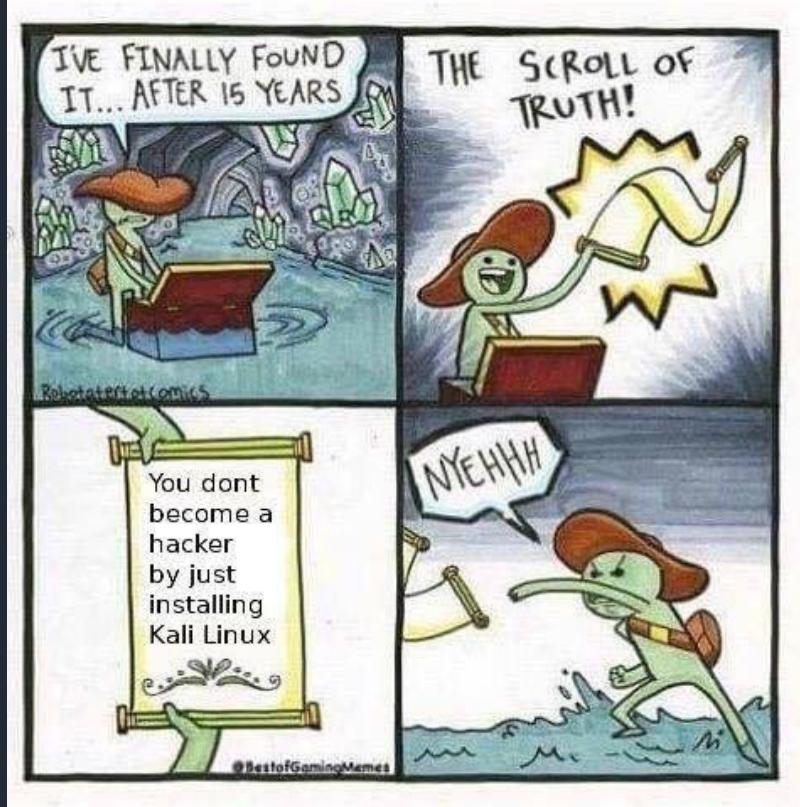
Focus on key issues and biggest risks

How can you measure success? Qualitative and quantitative metrics?

Red Team Tools



Toolz of the trade



Of course, the penetration testing tools will apply:

<https://theartofhacking.org/github>

Consider segregating these functions on different assets:

- Phishing SMTP
- Phishing payloads
- Long-term command and control (C2)
- Short-term C2

Using Redirectors

Common redirector types:

- SMTP
- Payloads
- Web Traffic
- C2 (HTTP(S), DNS, etc)

```
root@kali: ~ socat(1) socat(1)

File Edit View Search Terminal Help
socat(1)

NAME
    socat - Multipurpose relay (S)ocket CAT

SYNOPSIS
    socat [options] <address> <address>
    socat -V
    socat -h[h[h]] | -?/?[?]
    filam
    procam

DESCRIPTION
    Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them. Because the streams can be constructed from a large set of different types of data sinks and sources (see address types), and because lots of address options may be applied to the streams, socat can be used for many different purposes.

    Filam is a utility that prints information about its active file descriptors to stdout. It has been written for debugging socat, but might be useful for other purposes too. Use the -h option to find more infos.

    Procam is a utility that prints information about process parameters to stdout. It has been written to better understand some UNIX process properties and for debugging socat, but might be useful for other purposes too.

    The life cycle of a socat instance typically consists of four phases.

    In the init phase, the command line options are parsed and logging is initialized.

    During the open phase, socat opens the first address and afterwards the second address. These steps are usually blocking; thus, especially for complex address types like socks, connection requests or authentication dialogs must be completed before the next step is started.

    In the transfer phase, socat watches both streams' read and write file descriptors via select() , and, when data is available on one side and can be written to the other side, socat reads it, performs newline character conversions if required, and writes the data to the write file descriptor of the other stream, then continues waiting for more data in both directions.

    When one of the streams effectively reaches EOF, the closing phase begins. Socat transfers the EOF condition to the other stream, i.e. tries to shutdown only its write stream, giving it a chance to terminate gracefully. For a defined time socat continues to transfer data in the other direction, but then closes all remaining channels and terminates.

OPTIONS
    Manual page socat(1) line 1 (press h for help or q to quit)
```

<http://www.dest-unreach.org/socat>

```
root@kali: ~
File Edit View Search Terminal Help
proxychains(1)                               proxychains(1)

NAME
    ProxyChains - redirect connections through proxy servers

SYNTAX
    proxychains <program>

DESCRIPTION
    This program forces any tcp connection made by any given tcp client to follow through proxy
    (or proxy chain). It is a kind of proxifier.

    It acts like sockscape / premeo / eborder driver (intercepts TCP calls).

    This version (2.0) supports SOCKS4, SOCKS5 and HTTP CONNECT proxy servers. Auth-types: socks
    - "user/pass", http - "basic".

    When to use it ?

    1) When the only way to get "outside" from your LAN is through proxy server.

    2) When you are behind restrictive firewall which filters outgoing connections to some ports.

    3) When you want to use two (or more) proxies in chain:
    like: your_host <-> proxy1 <-> proxy2 <-> target_host

    4) When you want to "proxyfy" some programs with no proxy support built-in (like telnet).

    5) When you don't want to pay for eBorder / premeo socks driver :)

    Some cool features:
    * This program can mix different proxy types in the same chain

    like: your_host <->socks5 <-> http <-> socks4 <-> http <-> target_host

    * Different chaining options supported      like: take random proxy from the list.      or
    : chain proxies in exact order      or : chain proxies in dynamic order (smart exclude
    dead proxies from chain)

    * You can use it with any TCP client application, even network scanners.. yes, yes - you can
    make portscan via proxy (or chained proxies) for example with Nmap scanner by fyodor
    (www.insecure.org/nmap).

    proxychains nmap -sT -PO -p 80 -iR (find some webservers through proxy)

    NOTE: to run suid/sgid programs(like ssh) through proxychains you have to be root
Manual page proxychains(1) line 1 (press h for help or q to quit)
```

<http://proxychains.sourceforge.net>

Proxychains demo



Command and Control

```
root@kali:~/Tools/WSC2# ./wsc2.py

[!] WSC2 controller - Author: Arno0x0x - https://twitter.com/Arno0x0x - Version 0.1
[+] Trying to clone website [https://www.google.com]
[+] HTML stager created as [./static/index.html]
[no agent]#> genStager jscript2
[+] Stager created as [./stagers/wsc2Agent2.js]
[no agent]#> [+] New agent connected: [192.168.52.1:51835]
[+] New agent connected: [192.168.52.1:51836]

[no agent]#> list
      Agent list
-----
[192.168.52.1:51835]
[192.168.52.1:51836]
[no agent]#> use 192.168.52.1:51836
[192.168.52.1:51836]#> cli
[*] Switching to CLI mode
[*] Use the command 'back' to exit CLI mode
[192.168.52.1:51836-cli]#> notepad
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
c:\Temp\SecurityResearch\WSC2>notepad

[192.168.52.1:51836-cli]#>
```

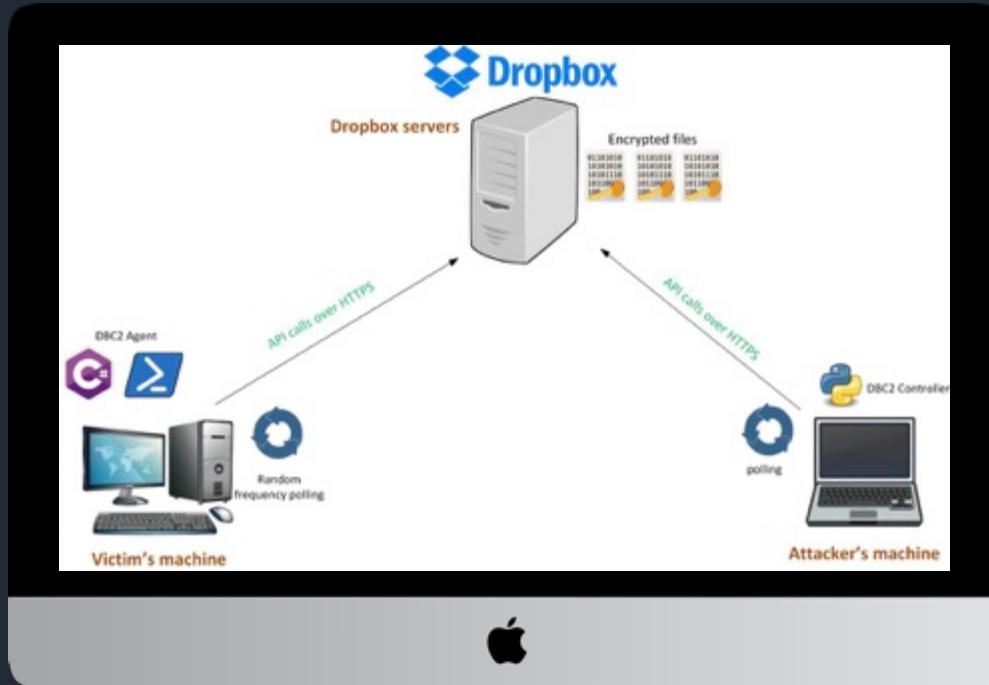
<https://github.com/Arno0x/WSC2>

WMIImplant

PowerShell based tool that leverages WMI to both perform actions against targeted machines, but also as the C2 channel for issuing commands and receiving results.

<https://github.com/ChrisTruncer/WMIImplant>

DropboxC2 from Arno0x0x



<https://github.com/santosomar/DBC2>

```
":' . ,MM; ;' . ;
:: :M-----: ; ;
:'M: ;M-----: ; ;M:
: M: M-----: ; M:
: 'M: M-----: ; M:
: ;M: 'M-----: 'M:
: ;M: ;"M-----: ; ,M:
: ::M: ;M: ;M: ;M:
: , ;M-----: ;M-----: ;
MM: , ,M-----: ;M-----: , ,MM:
M: ;'-----: ;M-----: " : M
M: ;M-----: ;M-----: ; M
:: :M-----: ;M-----: ;M
;"-----: ;M-----: ;" :
: ;M-----: ;M-----: ;
: "M-----: ;M-----: ;
....: ;M-----: ;M-----: ;
:MM-----: M-----: MM-----: MM-----: MM-----:
:MM-----: " : M-----: MM-----: " : "MM:
:MM: ;M-----: ;M-----: ; MM:
:MM: ;'-----: ;M-----: ; M:
:MM: ;M-----: ;M-----: ; MM:
:MM: ;M-----: MM-----: ; MM:
:MM: "M-----: ;M-----: ; M"
:M: "-----: ; M:
;"-----: ;M-----: ;
: ;M-----: ;
: ,MM-----: ;M:
: ;M: MM: ; ;;
```

TrevorC2 by Dave Kennedy

<https://github.com/trustedsec/trevorc2>

Trevor Demo



This screenshot shows the GitHub repository page for `PaulSec/twittor`. The repository has 62 stars and 167 forks. It contains 5 commits, 1 branch, 0 releases, and 1 contributor. The latest commit was made on Sep 9, 2015. The repository uses the MIT license. The README.md file describes the project as a fully featured backdoor that uses Twitter as a C&C server, inspired by `Goat`.

A fully featured backdoor that uses Twitter as a C&C server

5 commits 1 branch 0 releases 1 contributor MIT

Branch: master New pull request Create new file Upload files Find file Clone or download

PaulSec updated the doc

LICENSE README.md implant.py requirements.txt twittor.py

Initial commit updated the doc Initial commit Added requirements.txt Initial commit

3 years ago 3 years ago 3 years ago 3 years ago 3 years ago

Latest commit bca481f on Sep 9, 2015

README.md

Twittor

A stealthy Python based backdoor that uses Twitter (Direct Messages) as a command and control server. This project has been inspired by [Goat](#) which does the same but using a Gmail account.

Setup

For this to work you need:

- A Twitter account (Use a dedicated account! Do not use your personal one!)
- [Register an app](#) on Twitter with Read, write, and direct messages Access levels.

Install the dependencies:

```
$ pip install -r requirements.txt
```

<https://github.com/PaulSec/twittor>

This repository Search Pull requests Issues Marketplace Explore

Watch 120 Unstar 1,246 Fork 266

iagox86 / dnscat2

Code Issues 44 Pull requests 0 Projects 0 Wiki Insights

No description, website, or topics provided.

985 commits 7 branches 6 releases 11 contributors BSD-3-Clause

Branch: master New pull request Create new file Upload files Find file Clone or download

lager86 committed on Nov 7, 2017 Merge pull request #111 from kost/ensupport

Latest commit b5d4e42 on Nov 7, 2017

client	Implement basic environment support	6 months ago
data	Crypto: Added short-authentication strings to the client and the serv...	3 years ago
doc	Update CHANGELOG and CONTRIBUTORS	2 years ago
img	Updated the logo	3 years ago
server	Caching is controlled via a command line option	a year ago
tools	Mastermind: Fixed a bug where strings that have every character wrong...	2 years ago
LICENSE.md	Changed LICENSE.txt to LICENSE.md throughout	3 years ago
Makefile	Build: Some updates to the release build	2 years ago
README.md	Tunnels/docs: Documented the new tunnels stuff	2 years ago
contributors.md	Update CHANGELOG and CONTRIBUTORS	2 years ago
package.sh	Fixed the .zip version, and the 'bin' folder is no longer zipped as p...	3 years ago

README.md

Introduction

Welcome to dnscat2, a DNS tunnel that WON'T make you sick and kill you!

This tool is designed to create an encrypted command-and-control (C&C) channel over the DNS protocol, which is an effective tunnel out of almost every network.

This README file should contain everything you need to get up and running! If you're interested in digging deeper into the protocol, how the code is structured, future plans, or other esoteric stuff, check out the doc/ folder.

<https://github.com/iagox86/dnscat2>

This repository Search Pull requests Issues Marketplace Explore

Watch 6 Star 63 Fork 139

Code Pull requests Projects Wiki Insights

(extensible) Data Exfiltration Toolkit (DET)

91 commits 3 branches 0 releases 5 contributors MIT

Branch: master New pull request Create new file Upload files Find file Clone or download

This branch is 60 commits ahead of sensepost:master.

PaulSec Added TCP and UDP IPv6 config Latest commit `53H5f7a` on Dec 18, 2017

plugins	Added IPv6 UDP exfil	6 months ago
powershell	Restore Powershell plugins	6 months ago
.gitignore	Update README and config files	a year ago
LICENSE	Changed License to MIT License	2 years ago
README.md	Fixed the layout	6 months ago
config-sample.json	Added TCP and UDP IPv6 config	6 months ago
det.py	Update version	6 months ago
det.spec	Update README and config files	a year ago
requirements.txt	Added pygithub as a dependency	6 months ago

README.md

BlackHat Arsenal 2016 Black Hat Arsenal EU 2017

DET (extensible) Data Exfiltration Toolkit

DET (is provided AS IS), is a proof of concept to perform Data Exfiltration using either single or multiple channel(s) at the same time.

The idea was to create a generic toolkit to plug any kind of protocol/service to test implemented Network Monitoring and Data Leakage Prevention (DLP) solutions configuration, against different data exfiltration techniques.

<https://github.com/PaulSec/DET>



Adversarial Tactics, Techniques & Common Knowledge

[Main page](#)
[Help](#)
[Contribute](#)
[References](#)
[Using the API](#)
[Tactics](#)
[Initial Access](#)
[Persistence](#)
[Privilege Escalation](#)
[Defense Evasion](#)
[Credential Access](#)
[Discovery](#)
[Lateral Movement](#)
[Execution](#)
[Collection](#)
[Exfiltration](#)
[Command and Control](#)
[Techniques](#)
[Technique Matrix](#)
[All Techniques](#)
[Windows](#)
[Linux](#)
[macOS](#)
[Groups](#)
[All Groups](#)
[Software](#)
[All Software](#)
[Tools](#)
[Printable version](#)
[Permanent link](#)
 Follow @MITREattack

[Main page](#) [Discussion](#)

Last 5 Pages Viewed: Adversarial Tactics, Techniques & Co...

[Read](#) [View source](#) [View history](#) [Search enterprise](#)

Adversarial Tactics, Techniques & Common Knowledge

Welcome to ATT&CK

MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.

Note: A MITRE Partnership Network (MPN) account is not required to view and use the ATT&CK site.

[PRE-ATT&CK](#) | [ATT&CK for Enterprise](#) | [ATT&CK Mobile Profile](#)

ATT&CK for Enterprise

ATT&CK for Enterprise is an adversary behavior model that describes the actions an adversary may take to compromise and operate within an enterprise network.

- [Introduction and Overview](#)
- [All Techniques](#)
- [ATT&CK Navigator](#)
- [Adversary Emulation Plans](#)
- [Cyber Analytics Repository](#)
- [ATT&CK expressed in STIX&JSON](#)
- [Related Efforts](#)
- [Using the API](#)
- [Contribute or contact us](#)

Enterprise Platform Coverage

The MITRE ATT&CK Matrix™ is a visualization of the tactics and techniques. It aligns individual techniques under the tactics in which they can be applied.

- [Windows Technique Matrix](#)
- [Mac Technique Matrix](#)
- [Linux Technique Matrix](#)

News and Updates

News and Blogs

- [ATT&CK 101](#)
- [PRE-ATT&CK and ATT&CK Integration](#)
- [ATT&CK Navigator](#)
- [What's Next for ATT&CK](#)

[See Past Blogs](#) for previous posts.

Updates

- [April 2018](#)
- [January 2018](#)
- [July 2017](#)

[See Past Updates](#) for previous changes.

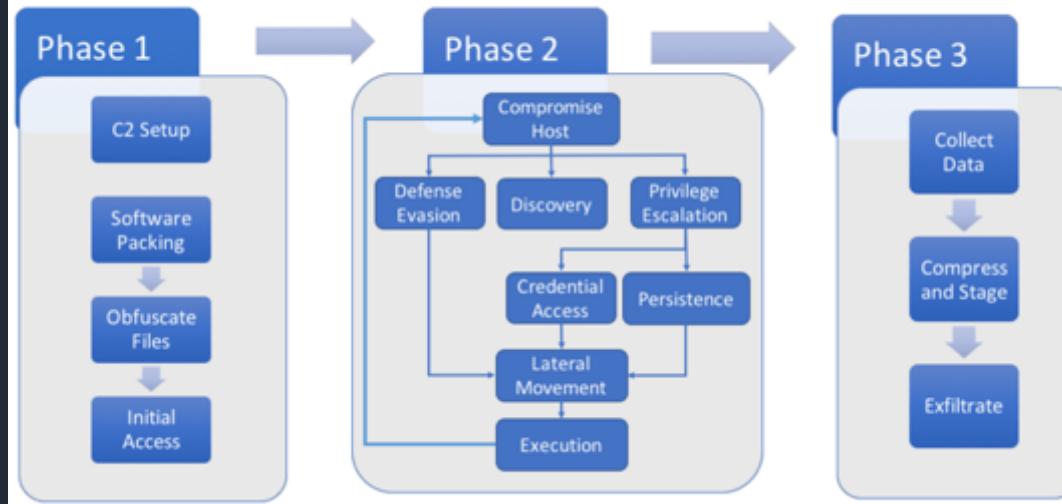
ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSIPT	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSIPT	Credentials in Files	Network Service Scanning	Logon Script	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Responding Link	Execution through API	Authentication	Bypass User Account	Clear Command	Credentials in Registry	Network Share	Pass the Hash	Data from Local	Exfiltration Over Command and Control	Data Encoding

<https://attack.mitre.org>

APT 3 Emulation Plan



https://attack.mitre.org/wiki/Adversary_Emulation_Plans



MTR170446
MITRE TECHNICAL REPORT

APT3 Adversary Emulation Plan

Dept. No.: IKL
Project No.: 0717MM09-AA

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release;
Distribution Unlimited. Case Number 17-
3569. ©2018 The MITRE Corporation. All
Rights Reserved.

Annapolis Junction, MD

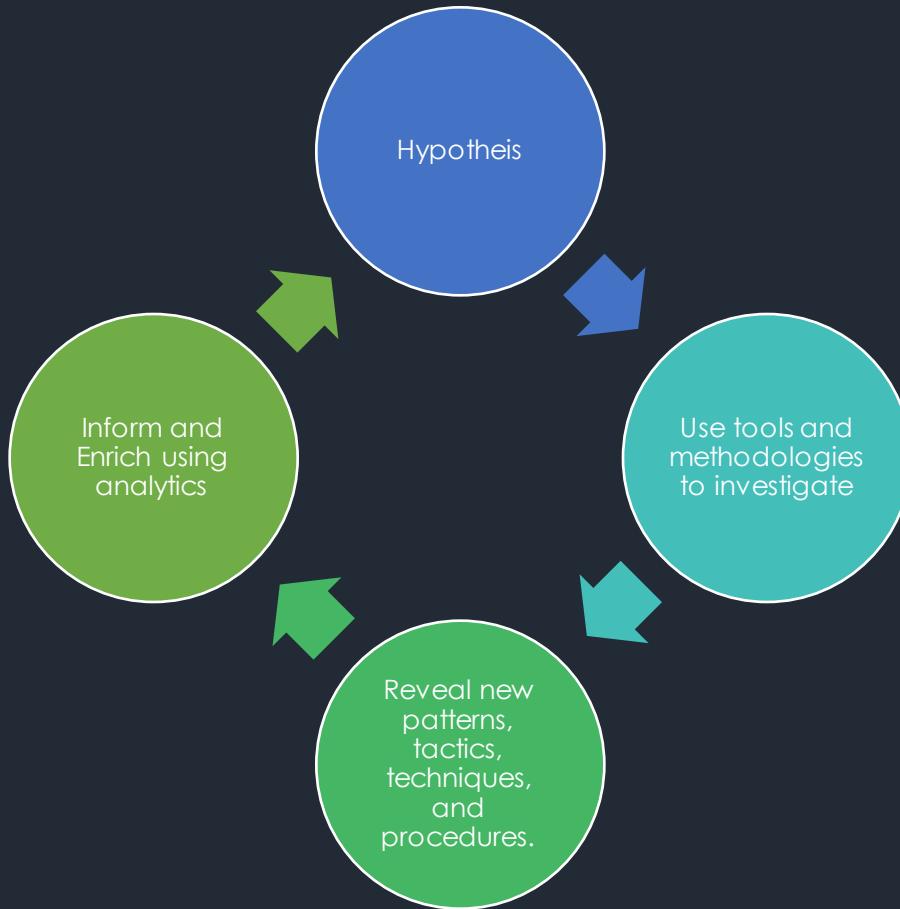
Authors: Christopher A. Korban
Douglas P. Miller
Adam Pennington
Cody B. Thomas

https://attack.mitre.org/w/img_auth.php/6/6c/APT3_Adversary_Emulation_Plan.pdf

Introduction to Threat Hunting

What is Threat Hunting?

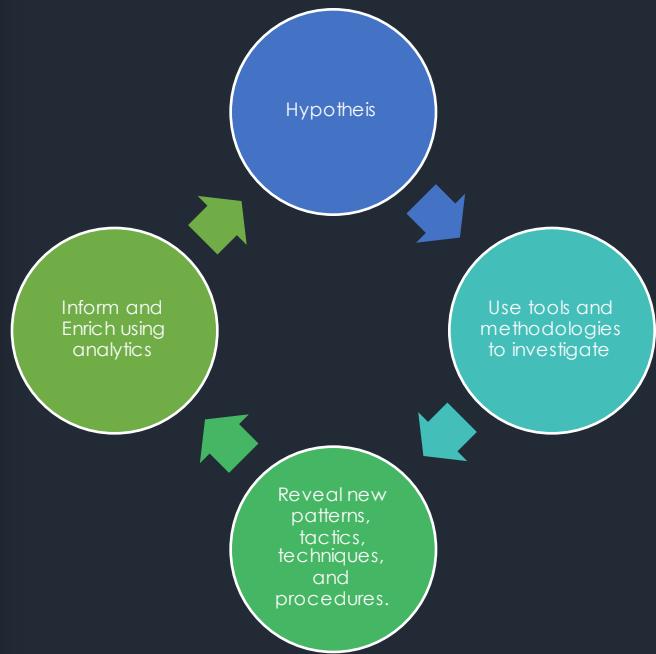
“the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.”

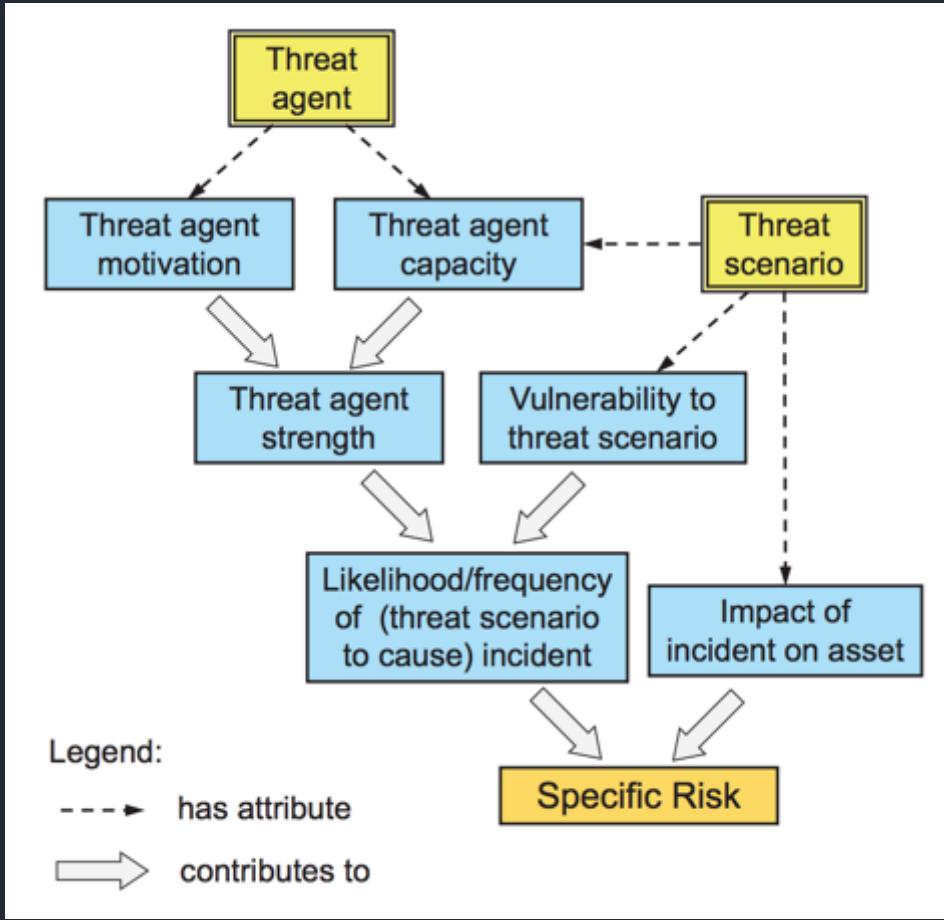


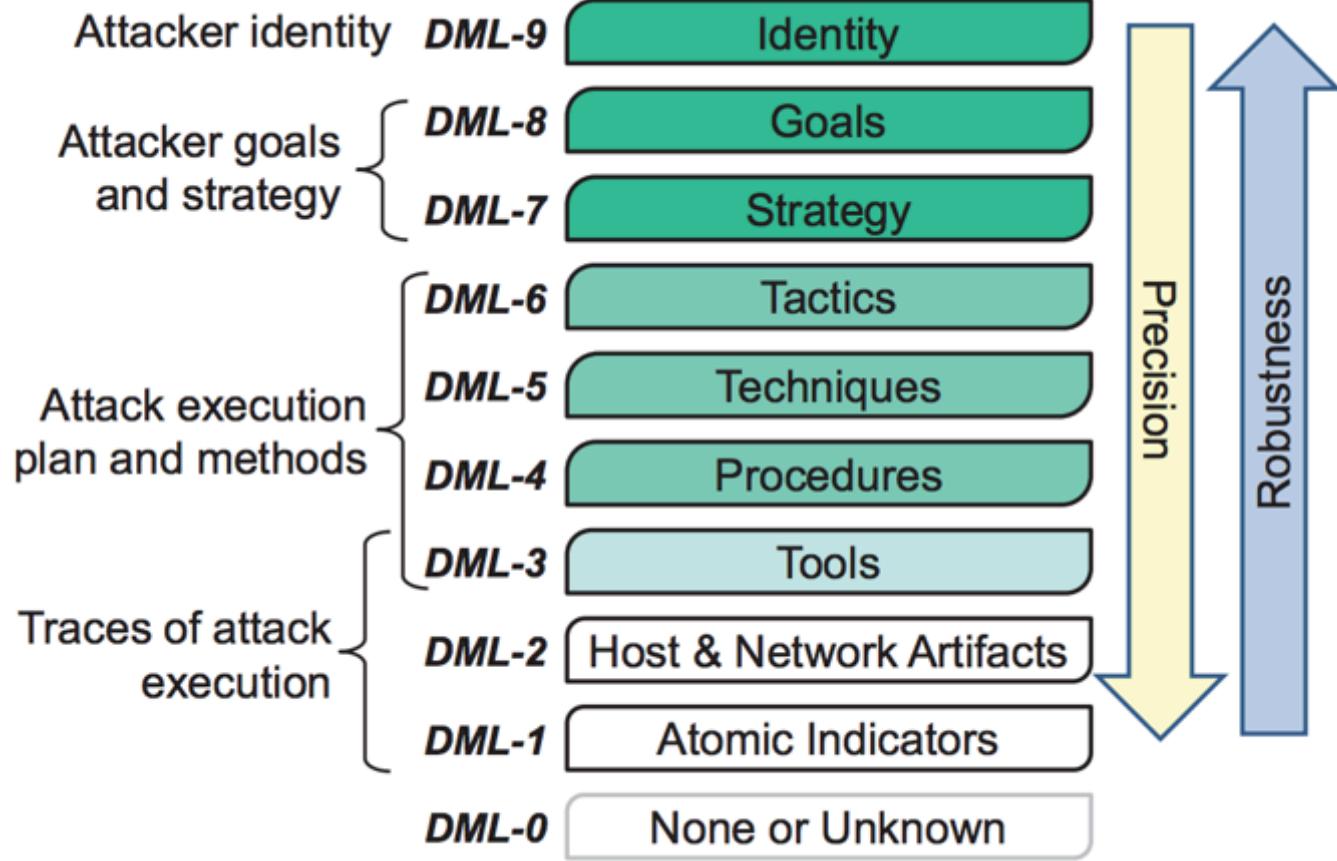
The Threat Hunting Process

HUNTING LOOP STEPS

	HM0 Initial	HM1 Minimal	HM2 Procedural	HM3 Innovative	HM4 Leading
DATA COLLECTION 	Little or no data collection	Moderate collection of some types of data from a few key points in the IT environment	High collection of certain types of data throughout the IT environment	High collection of certain types of data throughout the IT environment	High collection of many types of data throughout the IT environment
HYPOTHESIS CREATION 	Respond to existing automated alerts from SIEM, IDS, Firewall, etc.	Review threat intelligence to develop new hypotheses	Review threat intelligence and "friendly intelligence" to develop new hypotheses	Review threat intelligence, "friendly intelligence", and manual cyber risk scoring (i.e. "crown jewel analysis") to develop new hypotheses	Review threat intelligence, "friendly intelligence", and automated cyber risk scoring to develop new hypotheses
TOOLS & TECHNIQUES FOR HYPOTHESIS TESTING 	Alert consoles, SIEM searches; No proactive investigation	Utilize SIEM or log analysis tools to conduct basic search via full-text or SQL-like queries	Utilize simple tools and histograms to search and analyze data based on existing hunting procedures	Leverage visualizations and graph searches. Develop new hunting procedures	Advanced visualizations and graph searches. Publish, and automate new hunting procedures
PATTERN & TTP DETECTION 	None; Only SIEM/IDS alerts	Identifying IOCs at bottom of PoP like domains, URLs, and hashes	Identification of IOCs at bottom and middle of PoP and mapping trends of those IOCs over time	Able to detect adversary TTPs and other IOCs at the top of the PoP	Automatic complex TTP discovery and campaign tracking; Active sharing of IOCs with information sharing organization
ANALYTICS AUTOMATION 	None	Integrates threat intel feeds into automated alerting for basic matching	Build a library of effective hunting procedures and performs them on a regular schedule	Build a library of effective hunting procedures and performs them frequently; basic data science (standard deviation, outlier detection)	Automate effective hunting procedures to continuously improve alerting capabilities; advanced data science (machine learning)

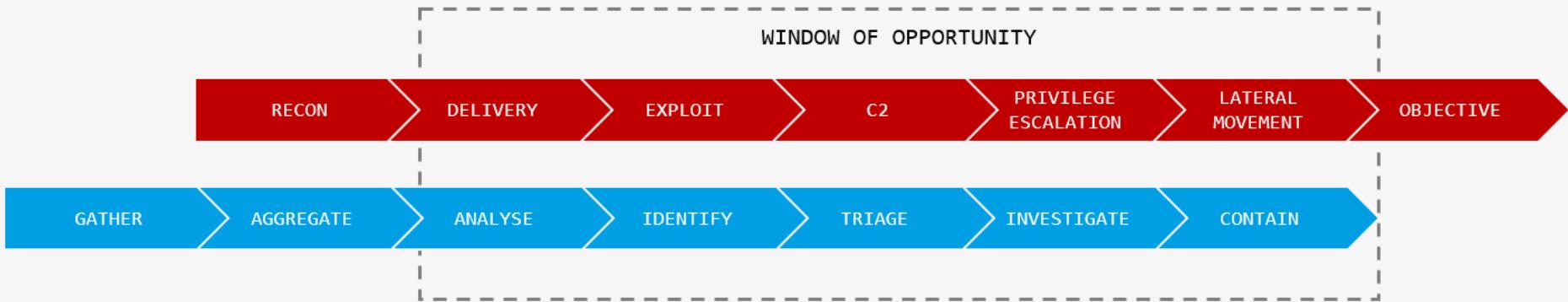






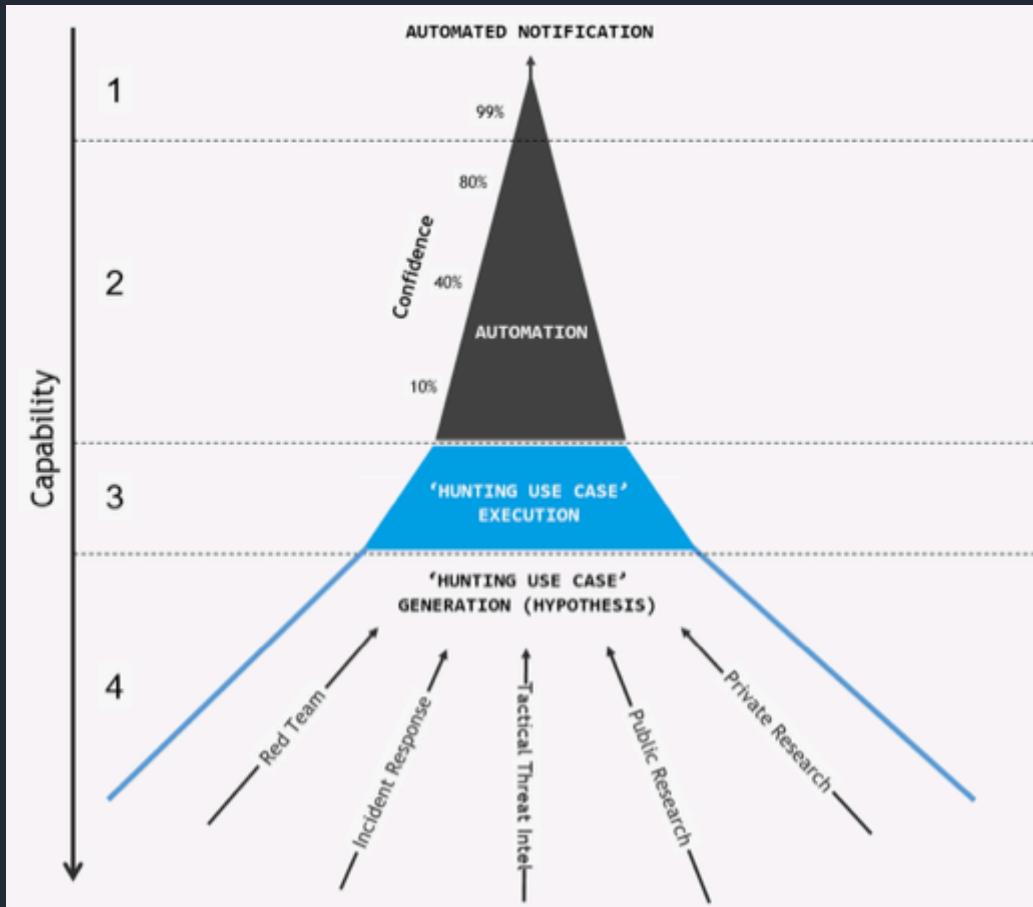
	Level 0 <i>Traditional</i> Not Considered Threat Hunting	Level 1 <i>Experimental</i> Experimenting with Threat Hunting	Level 2 <i>Intermittent</i> Part-time Threat Hunting	Level 3 <i>Proactive</i> Partial Use Case Generation / Execution	Level 4 <i>Leading</i> Complete Use Case Generation / Execution
PEOPLE	SOC Analysts Alert Driven mind set Basic alert triaging	SOC Analysts Basic understanding of forensics Good Endpoint / Network knowledge	Part Time Threat Hunter Intermediate forensics knowledge Strong Endpoint / Network knowledge	Dedicated Hunt Team Strong Forensics / Malware knowledge Strong Offensive Knowledge	Dedicated Hunt Team Level 3 capabilities plus research capability
PROCESS	24/7 Passive Monitoring	Ad Hoc Threat Hunting IOC search	"Hunt Sprints" - e.g. 1 Week per Month Regular Threat Hunting	24/7 Proactive Threat Hunting Partial Use Case Generation	24/7 Proactive Threat Hunting Complete Use Case Generation Use Case verification Use Case Automation
TECHNOLOGY	Traditional Tooling e.g. SIEM Network IDS Network IPS Anti-Virus Alternative Automated Technology (i.e. Sandboxing) Based on "Known Bad" e.g. Signature-based Threat Intel Feeds	Endpoint Detection & Response (EDR) Partial Network Data Coverage Partial Deployment	Endpoint Detection & Response (EDR) Full Deployment Full-Time Automated EDR Usage (IOC Matching, Threat Feeds etc.) Part-Time Advanced EDR Usage (During Hunt Sprints)	<u>Ability to Execute 'Hunting Use Cases' (Partial)</u> Full-Time Advanced EDR Usage Full Coverage of Network / Log Data Bespoke Configuration	<u>Ability to Execute 'Hunting Use Cases' (Complete)</u> Level 3 Technology, plus: Tight Integration Between Data Sources Bespoke Development and Custom Use of APIs

Threat Hunting Maturity Model



Microsoft's BlueHat conference introduced the concept of a blue team cyber kill chain, as a defender-centric version of the standard attack focussed cyber kill chain. This described the chain of actions a defender needs to go through to find and evict attackers.

<https://youtu.be/aZxtCKHhAUE?t=160>



Map of FIRST CSIRT Case Classification criteria to VERIS

Information on VERIS can be found at veriscommunity.net

Information on CSIRT Case Classification can be found at [http://www.Fist.org/_events/resources/guides/csirt_case_classification.html](http://www.First.org/_events/resources/guides/csirt_case_classification.html)

Point of contact: VERIS@veriscommunity.com

Map of FIRST CSIRT Case Classification criteria to VERIS

#	Source variable	Notes from CSIRT Case Classification	Notes and questions from Veris	Veris_Incident	Action_Internal variety; vector, notes	Action_Partner variety; vector, notes	Action_Malware variety; vector, notes	Action_Hacking variety; vector, notes	Action_Social variety; vector, notes	Action_Mouse variety; vector, notes	Action_Physical variety; vector, notes	Action_Emer variety; vector, notes	Action_Envir variety; notes	Asset_Variety variety [and]; notes	Asset_Governance owns, mgr, hosting, cloud, monitoring	Attribute_data
1	Denial of service	Denial or Denials attack	Assuming this actually results in availability issues. If just an attack, there would be no attribute. Assuming no particular asset is sheep implied.	Confirmed	Unknown											Unknown
2	Forensics	Any forensic work to be done by CSIRT	This isn't an incident as defined by VERIS (doesn't imply specific actions that compromise security attributes of assets).	No												
3	Compromised information	Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or intellectual property	The only thing that can be directly inferred is loss of sensitive information, assets, or assets implied. Data variety unknown. If known, they'd need to be recorded on a per-incident basis.	Confirmed												Unknown
4	Compromised Asset	Compromised host (just account, Trojans, malware), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.	The only thing that can be directly inferred is loss of confidentiality and integrity attributes. Don't be afraid to infer other malware varieties since each incident may be different. Hosts cannot be inferred because it may or may not involve an actor attempting to gain access. Assuming external actor control implies migration. If known, these need to be recorded on a per-incident basis.	Confirmed	Unknown											Unknown
5	Unfulfilled activity	Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving the use of computers, insider investigations, or crime prevention.	The only thing that can be directly inferred is that this is a suspected incident.	Suspected												
6	Internal Hacking	Reconnaissance or suspicious activity originating from inside the Company corporate networks, excluding malware.	Can't infer actor since this could be an internal actor moving laterally inside the networks or an insider behaving badly. Can't infer action in hacking footprinting. Can't infer any particular asset.	Suspected												
7	External Hacking	Reconnaissance or suspicious activity originating from outside the Company corporate networks (partner networks, vendors, etc.)	Can directly infer actor to external. Assume action is hacking footprinting. Can't infer any particular asset.	Suspected	Unknown											
8	Malware	A virus or worm that is affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojans (See Compromised Asset).	Assuming confirmed infection. Assuming external actor. Can't infer any particular variety of malware.	Confirmed												Unknown
9	Email	Spammed email, SPAM, and other email security-related events.	Assuming this didn't actually compromise attributes of an asset. If so, these details will need to be recorded on the incident basis.	Unknown												
10	Gathering	Security-relevant information to any confirmed incident. Sharing offensive material, sharing/gross invasion of copyrighted material. Deliberate violation of laws, policies, regulations, standards, or norms. Unauthorized access to computer, network, or application. Unauthorized escalation of privileges or deliberate attempt to subvert access controls.	This isn't an incident as defined by VERIS. It's specific actions implied.	Confirmed	Unknown											
11	Policy Violations	Security-relevant violations to any confirmed incident.	Can directly infer incident. Assumption is that this can't have a specific variety of incident. The assumption can be applied to many of them.	Confirmed	Unknown											

DEMO

<http://veriscommunity.net/veris-mapping.html>

FIRST CSIRT Case Categories and VERIS

Welcome to ATT&CK

ATT&CK is a curated knowledge base and model for cyber adversary behavior, reflecting the latest in threat research and analysis. It provides a detailed understanding of the tactics and techniques used by adversaries, their interactions, and the platforms they are known to target.

Note: A MITRE Partnership Network (MPN) account is not required to view and use the ATT&CK site.

ATT&CK for Enterprise

ATT&CK for Enterprise is an adversary behavior model that describes the actions an adversary may take to compromise and operate within an enterprise network.

- Introduction and Overview
- All Techniques
- ATT&CK Navigator
- Adversary Emulation Plans
- Cyber Analytics Reports
- ATT&CK expressed in...
- Related Efforts
- Using the API
- Contribute or contact us!

News and Updates

News and Blogs

- ATT&CK 101
- PRE-ATT&CK and ATT&CK Integration
- ATT&CK Navigator
- What's Next for ATT&CK

See Past Blogs for previous posts.

Updates

- April 2018
- January 2018
- July 2017

See Past Updates for previous changes.

ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	bash_profile and	Access Token	Access Token	Account Manipulation	Account Discovery	Asclepius	Audio Creation	Automated Exfiltration	Previously Used Port

MITRE – ATT&CK



REAL-TIME BIG DATA SECURITY

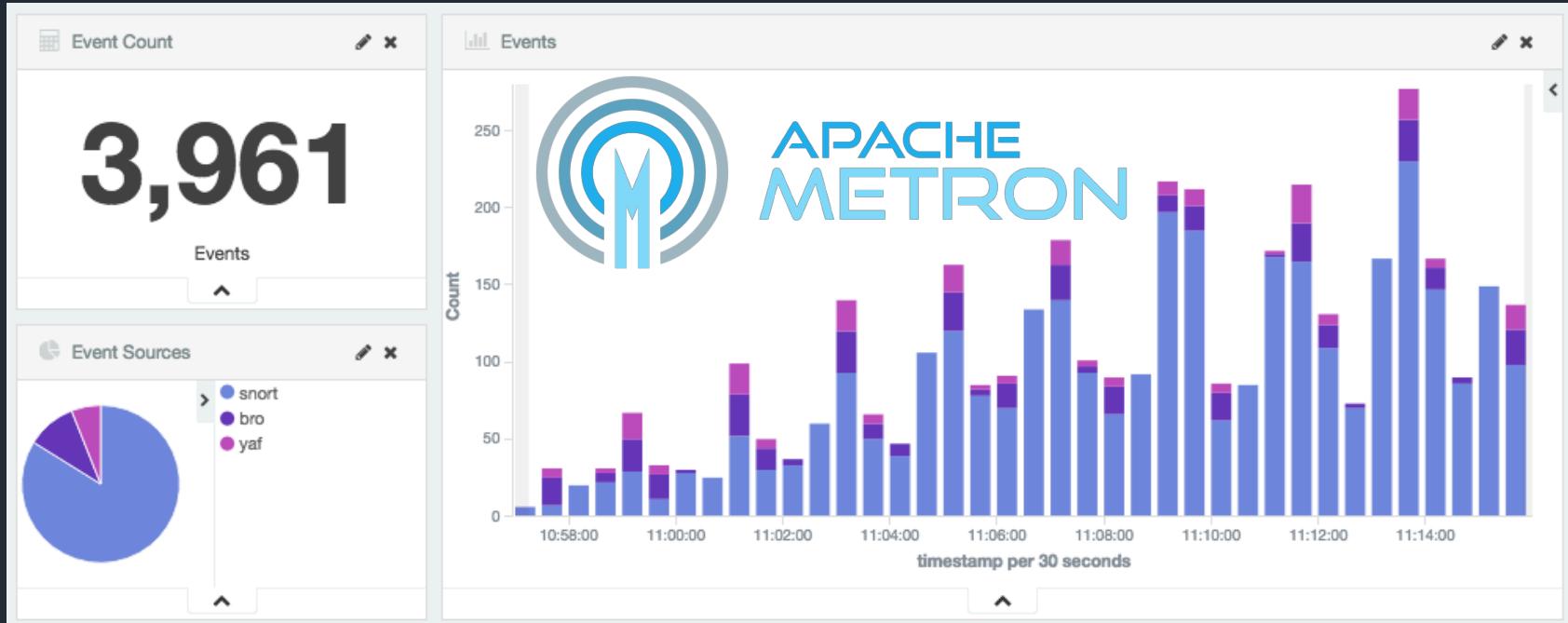
[GITHUB](#)[COMMUNITY HOME](#)[Updated Documentation](#)[DOCS HOME](#)[WHAT IS IT?](#)[BENEFITS](#)

WHAT APACHE METRON DOES

Apache Metron provides a scalable advanced security analytics framework built with the Hadoop Community evolving from the Cisco OpenSOC Project. A cyber security application framework that provides organizations the ability to detect cyber anomalies and enable organizations to rapidly respond to identified anomalies.

[MORE](#)

<https://metron.apache.org/>



<https://github.com/apache/metron>

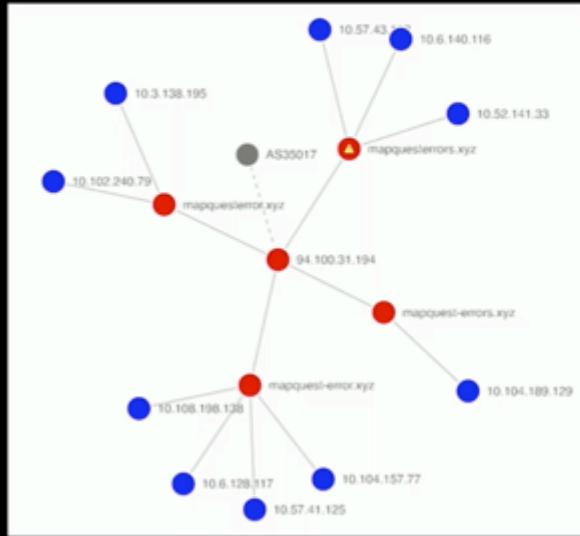
O'REILLY®
Security



OCT 29–NOV 1, 2017
NEW YORK, NY

oreillysecuritycon.com
@OReillySecurity
#OReillySecurity

An Example (1)



Maliciousness Rating	
Country	Minimal (0.38x)
AS	Very High (42.80x)
BGP prefix	Very High (156.74x)
Dst. Host Public Suffix	Very High (15.30x)
Dst. Reverse Host Public Suffix	Very High (4.78x)
Dst. Reverse Host Org. Suffix	Minimal (0.00x)
Dst. Host SOA Authority	Minimal (0.00x)
Dst. Host SOA E-mail	Minimal (0.00x)
Dst. Host SOA NS	Minimal (0.00x)
Dst. Host WHOIS Registrar	Low (3.65x)
Dst. Host WHOIS Registrant	Low (4.41x)
Dst. Host WHOIS Registrant E-mail	Minimal (0.00x)
Dst. Host WHOIS NS	Very High (75.15x)

Matches			
Source	Category	Campaign	Entity
malwaredomains	scam; private	MalwareDomains · scam · 2016-10-05	mapquesterrors.xyz

BREAK



REMEMBER TO CHECK OUT THE RESOURCES AT:

<https://theartofhacking.org>

<https://theartofhacking.org/training>

<https://theartofhacking.org/github>

https://theartofhacking.org/go/training_resources.pdf

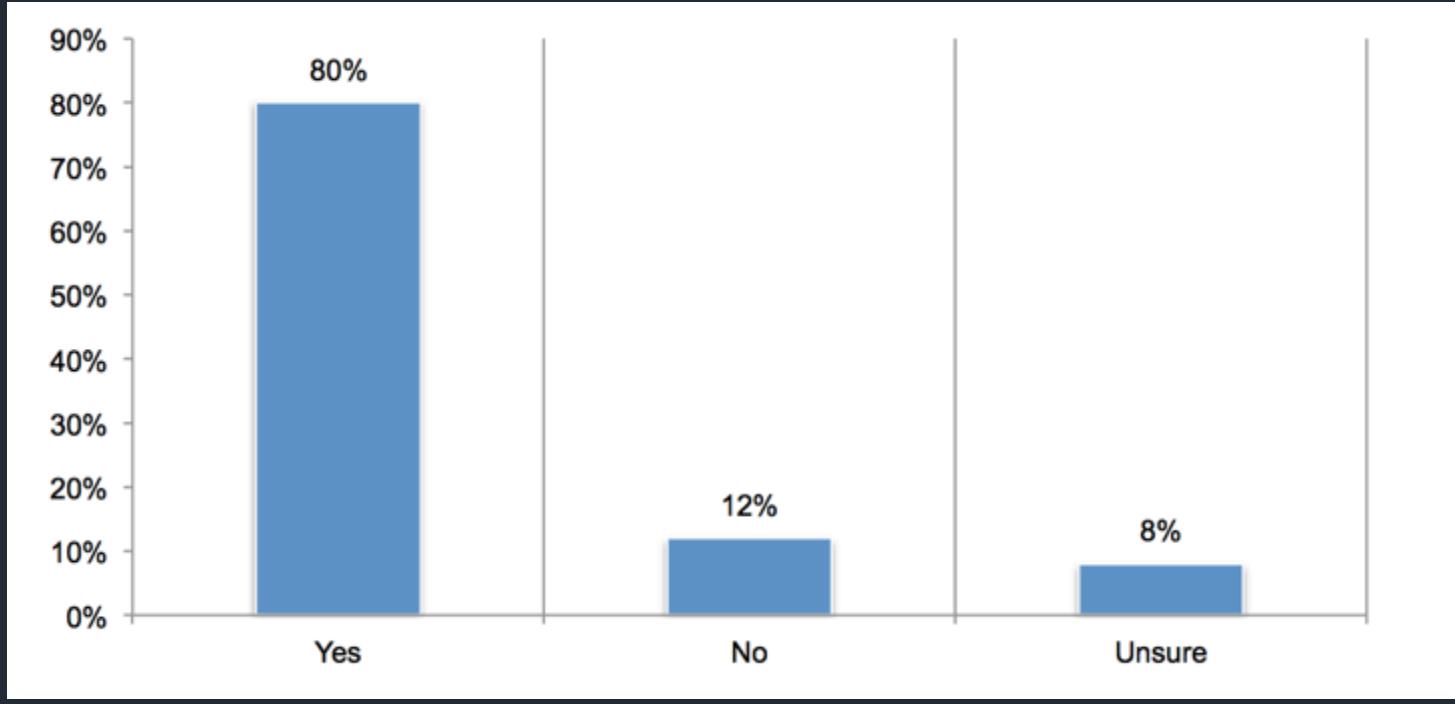
Threat Intelligence

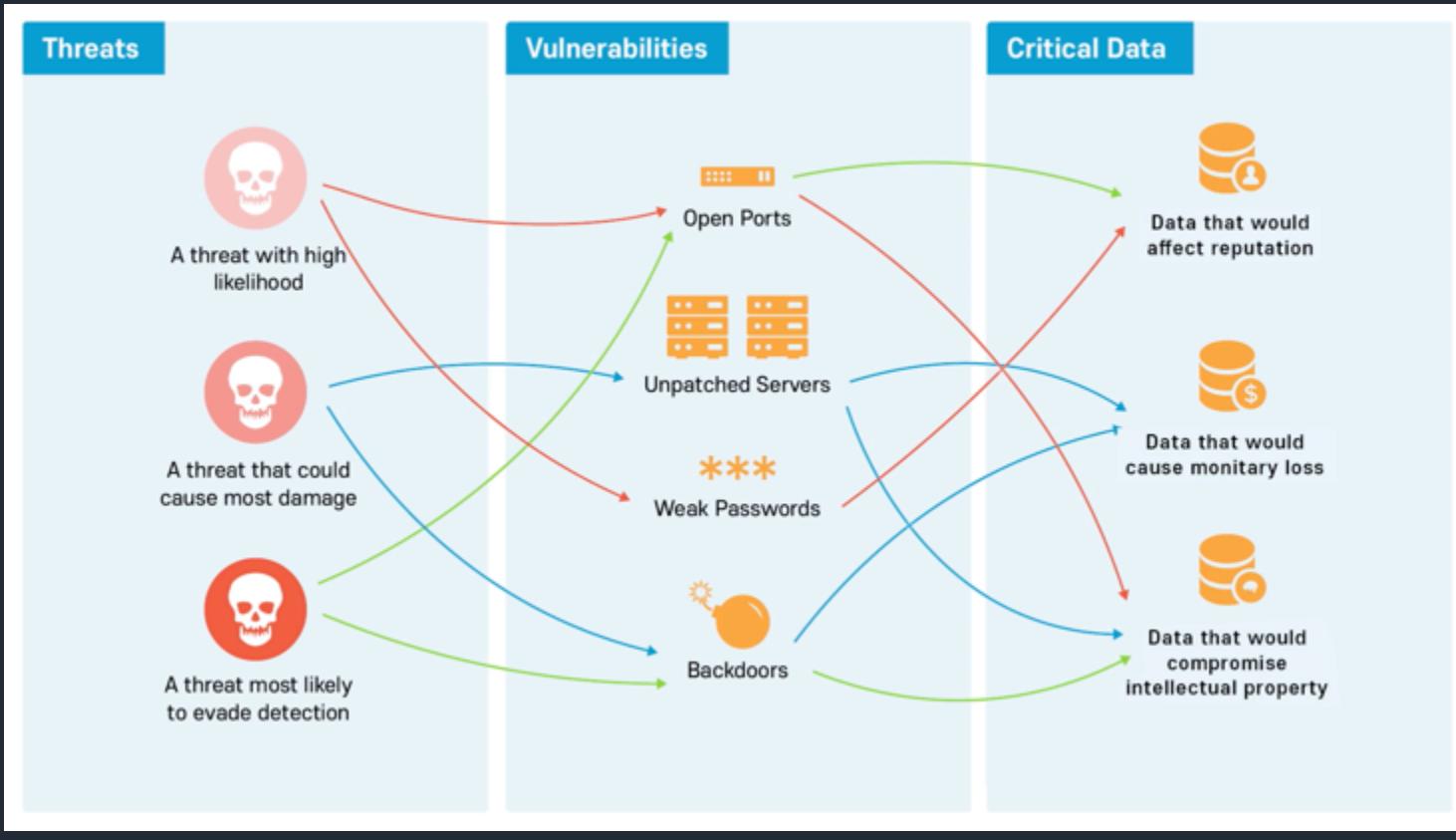
5



Why Threat Intelligence is Important?

Would threat intelligence have helped prevent or minimize the consequences of an attack?





Threat Intelligence and Hunting

```
1  /*
2  This is a Yara Rule Example by Omar
3  */
4 rule Super_Bad_Malware
5 {
6     meta:
7         author = "OmarOmar"
8         threat = "MalWare.Gen0"
9     strings:
10        HASH = 60844f93dba8f5197f748b3012cd14654a107053
11    condition:
12        any of them
13 }
14 |
```



<https://virustotal.github.io/yara/>

OmarOmar
Online

YaraEditor Web Edition

Version 0.8

Files 11

Rules 12343

Best Uploaders

- tigzy 12343 rules
- direnje 2 rules

Tags

PEiD

Last Comments

Tigzy on Rule : SmartServiceDriver (#12324)
This file is the driver from SmartService infection 2017-10-20 17:00:25

Tigzy on Rule : PureBasic (#3960)
Is this a packer? 2017-10-20 12:27:15

Last Rules						
Rule	Author	File	Threat	Tags	Last Modified	Created
AdwAudioService (#12340)	Tigzy	Adware	AdwAudioService	adware	2018-04-05 16:11:17	2017-10-30 08:39:45
APT_malware_1 (#12343)	Tigzy	TA18-074A	TA18-074A		2018-03-16 17:52:39	2018-03-16 17:51:53
testrule (#12342)	direnje	Antidebug_AntVM			2017-11-11 10:11:05	2017-11-11 10:11:05
churascronle (#12341)	direnje	Antidebug_AntVM			2017-11-10 09:18:52	2017-11-10 09:18:52
Mimikatz (#12339)	Tigzy	HackTool	HackTool_Mimikatz		2017-10-27 10:49:32	2017-10-27 10:35:17
RansomwareWCry (#12338)	Tigzy	Ransomware	Ransom.WCry		2017-10-26 12:08:28	2017-10-26 11:58:13
RansomwareBadRabbit (#12337)	Tigzy	Ransomware	Ransom.BadRabbit		2017-10-25 09:23:42	2017-10-25 09:09:11
Trojan/Backdoor (#12336)	Tigzy	Malware	TCVBA.Gen		2017-10-24 16:34:50	2017-10-24 16:30:00
ImpHash_UPX_Packed_Malware_1_TA17_293A (#12333)	Tigzy	Malware			2017-10-24 14:56:25	2017-10-21 20:41:12
Trojan/Downloader (#12335)	Tigzy	Malware	TcDownloader		2017-10-23 14:43:35	2017-10-23 14:42:19
TA17_293A_Hacktool_Touch_MAC_modification (#12331)	Tigzy	Malware			2017-10-21 20:46:06	2017-10-21 20:41:12
TA17_293A_malware_1 (#12325)	Tigzy	Malware			2017-10-21 20:41:32	2017-10-21 20:41:12
TA17_293A_malware_2 (#12326)	Tigzy	Malware			2017-10-21 20:41:32	2017-10-21 20:41:12
TA17_293A_Query_XML_Code_MAIL_DOC_PT_2 (#12327)	Tigzy	Malware			2017-10-21 20:41:32	2017-10-21 20:41:12
TA17_293A_Query_XML_Code_MAIL_DOC (#12328)	Tigzy	Malware			2017-10-21 20:41:32	2017-10-21 20:41:12
TA17_293A_Query_Javascript_Decode_Function (#12329)	Tigzy	Malware			2017-10-21 20:41:32	2017-10-21 20:41:12

<https://yara.adlice.com/>

Yara Share

OmarOmar
Online

Rule creation

Private Global Make public

File Malware

Rule name: Omar's rule

Tags: APT super_bad_horrible_hacker

Author: OmarOmar

Threat.name: SuperBad.threat

Comment: This is a comment.

Metas

Strings

+ Edit Delete Search: []

Name	Value
HASH	68844f93db0ff5297f740b3812cd14654a187853

Showing 1 to 2 of 2 entries Previous Next

Condition: any of them

Preview

```
1 /*  
2 This is a comment  
3 */  
4 rule Omar's_rule  
5 {  
6   meta:  
7     author = "OmarOmar"  
8     threat = "SuperBad.threat"  
9   strings:  
10    HASH = 68844f93db0ff5297f740b3812cd14654a187853  
11    condition:  
12      any of them  
13 }  
14
```

Home Files Unknown New

<https://yara.adlice.com/>

Cyber Threat Intelligence Tech X

Secure | <https://oasis-open.github.io/cti-documentation/>

Home STIX TAXII Contribute FAQ Resources Looking for... STIX 1.x? TAXII 1.x?

Sharing threat intelligence just got a lot easier!

STIX™

A structured language for cyber threat intelligence

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI). STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively. STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

STIX Relationship Example

[Learn More](#)

TAXII™

A transport mechanism for sharing cyber threat intelligence

Trusted Automated Exchange of Intelligence Information (TAXII™) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner. TAXII is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models. TAXII is specifically designed to support the exchange of CTI represented in STIX.

TAXII Collections

[Learn More](#)

<https://oasis-open.github.io/cti-documentation/>

[taxii](#) [Issues](#) [Pull Requests](#) [Commits](#) [Commits \(raw\)](#) [Raw](#) [Logos](#)

[README.md](#)

OpenTAXII

TAXII server implementation in Python from EclecticIQ.

OpenTAXII is a robust Python implementation of TAXII Services that delivers rich feature set and friendly pythonic API built on top of well designed application.

OpenTAXII is guaranteed to be compatible with [Cabby](#), TAXII client library.

[Source](#) | [Documentation](#) | [Information](#) | [Download](#)

[build](#) unknown [health](#) 96% [coverage](#) 86% [dock](#) passing [Requirements Status](#)

Getting started

See [the documentation](#).

Getting started with OpenTAXII using Docker

OpenTAXII can also be run using docker. This guide assumes that you have access to a local or remote docker server, and won't go into the setup of docker.

To get a default (development) instance using docker

```
$ docker run -d -p 9000:9000 eclecticiq/opentaxii
```

NOTE: OpenTAXII is now accessible through port 9000, with data stored locally in a SQLite database, and no authentication, using services defined in [services.yml](#) and collections from [collections.yml](#)

More documentation on running OpenTAXII in a container is found in the [OpenTAXII Docker Documentation](#).

Feedback

You are encouraged to provide feedback by commenting on open issues or sending us email at opentaxii@eclecticiq.com

<https://github.com/EclecticIQ/OpenTAXII>

The screenshot shows a GitHub repository page for CRITs. At the top, there's a navigation bar with links for Home, Getting CRITs, Documentation, and Community. The main content area has a dark header "EXTEND CRITs WITH SERVICES". Below it, a text block says "Develop additional capabilities using the Services Framework to combine CRITs with third-party and home-grown intelligence systems." A "Get started now!" button is present. The central part of the page displays a large block of Python code. The code is annotated with comments explaining its purpose: it uses tshark to capture network traffic, writes it to a temporary file, and then uses etree to parse the XML output into a PCAP file. It also handles configuration settings for services like metasploit.

```
1  #!/usr/bin/python
2
3  # This file is part of CRITs, a framework for threat hunting and
4  # incident response. It is maintained by the Security Engineering
5  # Research Group at the University of Michigan. For more information,
6  # see https://crits.github.io/crits/
7  #
8  # SPDX-License-Identifier: Apache-2.0
9  #
10 # Copyright 2010-2023 University of Michigan
11 #
12 # Licensed under the Apache License, Version 2.0 (the "License");
13 # you may not use this file except in compliance with the License.
14 # You may obtain a copy of the License at
15 #
16 #     http://www.apache.org/licenses/LICENSE-2.0
17 #
18 # Unless required by applicable law or agreed to in writing, software
19 # distributed under the License is distributed on an "AS IS" BASIS,
20 # WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
21 # See the License for the specific language governing permissions and
22 # limitations under the License.
23
24
25  import os
26  import sys
27
28  from lib.crits.services import Service
29
30
31  class MetasploitService(Service):
32
33      def __init__(self):
34          Service.__init__(self)
35
36      def run(self, args):
37
38          # use tshark to generate a pcap file
39          temp_pcap = tempfile.NamedTemporaryFile(delete=False, suffix=".pcap")
40          tshark_name = temp_pcap.name
41          temp_pcap.write(tshark_data)
42          temp_pcap.close()
43
44          # use tshark to generate a xml file
45          temp_xml = tempfile.NamedTemporaryFile(delete=False, suffix=".xml")
46          tshark = Popen(["tshark", "-w", temp_pcap.name, "storage:off"])
47          tshark_out, tshark_err = tshark.communicate()
48          if tshark.returncode != 0:
49              return ("Metasploit: %s" % (tshark_out, tshark_err))
50
51          # use etree to parse the xml file
52          etree = ET.parse(temp_xml.name)
53          temp_pcap.seek(0)
54
55          # transform XML into HTML
56          xml_file = None
57          for d in settings.SERVICE_DIRS:
58              try:
59                  file_dir = "%s/metasploit_service" % d
60                  xml_file = open("%s/parsedxml.xml" % file_dir, "r")
61              except IOError:
62                  pass
63          if not xml_file:
64              return ("Metasploit: Could not find XML...")
65
66          parser = etree.XMLParser()
67          parser.resolve_references.add(resolveReference)
68          namespaces = False
69          try:
70              # XML input = etree.parse(temp_pcap, parser)
71              # XML root = etree.parse(xml_file, parser)
72              # transforms = etree.XSLT(xml_root)
73
74              # XML input = ...
75              # XML root = ...
76              # transforms = ...
77
78          except Exception as e:
79              return ("Metasploit: %s" % str(e))
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
```

OF THE COMMUNITY. BY THE COMMUNITY. FOR THE COMMUNITY.

CRITs is an open source malware and threat repository that leverages other open source software to create a unified tool for analysts and security experts engaged in threat defense. It has been in development since 2010 with one goal in mind: give the security community a flexible and open platform for analyzing and collaborating on threat data. In making CRITs free and open source, we can provide organizations around the world with the capability to quickly adapt to an ever-changing threat landscape. CRITs can be installed locally for a private isolated instance or shared among other trusted organizations as a collaborative defense mechanism.



<https://crits.github.io>



<https://github.com/certtools/intelmq>



A Search Engine for Threats

SEARCH NOW >

Search by Domain, IP, Email or Organization

Try [tibet](#) - [wellpoint](#) - [aoldaily.com](#) - [188.40.75.132](#) - [plugx](#)



ThreatCrowd is now powered by [AlienVault](#)®
Learn more about [AlienVault's Open Threat Exchange \(OTX\)](#) today!



<https://www.threatcrowd.org/>

STAXX

Your Free STIX / TAXII Solution

DOWNLOAD NOW



Access any STIX / TAXII feed

<https://www.anomali.com/platform/staxx>



SOLTRA EDGE®

Soltra Edge® is an industry-driven software that automates processes to share, receive, validate and act on cyber threat intelligence. It enables an end-to-end community defense model and changes the posture of cybersecurity defenders from reactive to proactive. Soltra Edge is the most widely used Cyber Threat Communications Platform for two-way sharing of cybersecurity information among peers, trust groups, communities and government.

NEW RELEASE AVAILABLE: Check out the latest 2.11.3 release by starting with a FREE 90-day trial.

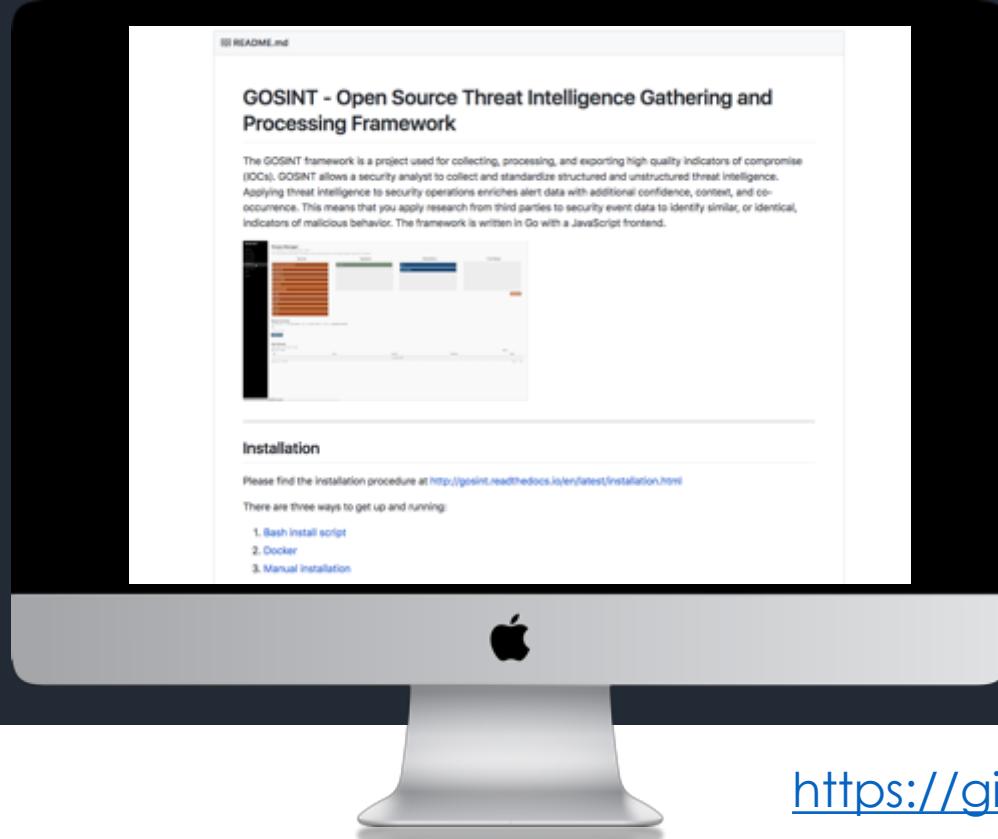
[DOWNLOAD BROCHURE ▶](#)

[DOWNLOAD FAQ ▶](#)

[DOWNLOAD TRIAL ▶](#)



GOSINT



<https://github.com/ciscocsirt/gosint>



Umbrella Popularity List

The popularity list contains our most queried domains based on passive DNS usage across our Umbrella global network of more than 100 Billion requests per day with 65 million unique active users, in more than 165 countries. Unlike Alexa, the metric is not based on only browser based 'http' requests from users but rather takes in to account the number of unique client IPs invoking this domain relative to the sum of all requests to all domains. In other words, our popularity ranking reflects the domain's relative internet activity agnostic to the invocation protocols and applications where as 'site ranking' models (such as Alexa) focus on the web activity over port 80 mainly from browsers.

As for Alexa, the site's rank is based on combined measure of unique visitors (Alexa users who visit the site per day) and page views (total URL requests from Alexa users for a site). Umbrella popularity lists are generated on a daily basis reflecting the actual world-wide usage of domains by Umbrella global network users and includes root domains, subdomains in addition to TLDs (Alexa list has only this). In addition, Umbrella popularity algorithm also applies data normalization methodologies to smoothen potential biases that may occur in the data due to sampling of the DNS usage data.

Top 1 million

<http://s3-us-west-1.amazonaws.com/umbrella-static/top-1m.csv.zip>

Top TLDs

<http://s3-us-west-1.amazonaws.com/umbrella-static/top-1m-TLD.csv.zip>

<http://s3-us-west-1.amazonaws.com/umbrella-static/index.html>



This repository

Search

Pull requests Issues Marketplace Explore

[The-Art-of-Hacking / art-of-hacking](#)[Unwatch](#) 20[Unstar](#) 66[Fork](#) 24[Code](#)[Issues 0](#)[Pull requests 0](#)[Projects 0](#)[Wiki](#)[Insights](#)[Settings](#)

Branch: master

art-of-hacking / osint /

[Create new file](#)[Upload files](#)[Find file](#)[History](#)

santosomar adding OSINT resources

Latest commit 7bed5b4 on Jan 17

..

README.md

adding OSINT resources

4 months ago

README.md

Open Source

Open-source intelligence (OSINT) is data collected from open source and publicly available sources. The following are a few OSINT resources and references:

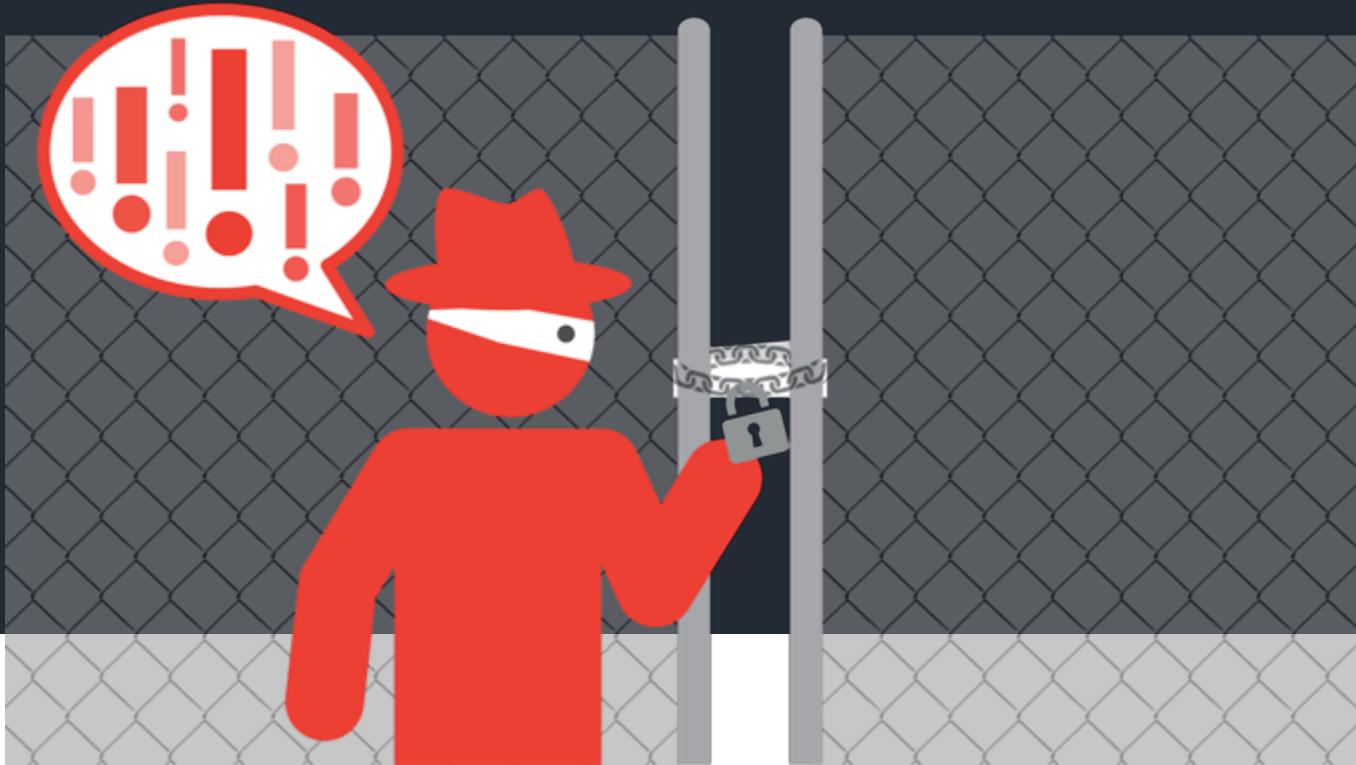
- [GOSINT](#) - a project used for collecting, processing, and exporting high quality indicators of compromise (IOCs). GOSINT allows a security analyst to collect and standardize structured and unstructured threat intelligence.
- [Awesome Threat Intelligence](#) - A curated list of awesome Threat Intelligence resources. This is a great resource and I try to contribute to it.
- [Umbrella \(OpenDNS\) Popularity List](#) - most queried domains based on passive DNS usage across our Umbrella global network of more than 100 Billion requests per day with 65 million unique active users, in more than 165 countries.

<https://github.com/The-Art-of-Hacking/art-of-hacking/tree/master/osint>

Enterprise-wide Ethical Hacking and Continuous Monitoring

Before we proceed...

Question: What is the difference between a major breach and a minor breach?



Know where's your critical data!

Monitor and protect it!

Segment your environment!

Penetration Testing

VS

Red Teaming

VS

Vulnerability Management

VS

Continuous Monitoring

CCNA CYBER OPS

- [CCNA Cyber Ops SECFND 210-250 Video Course](#)
- [CCNA Cyber Ops SECOPS 210-255 Video Course](#)
- [Learning Path: CCNA Cyber Ops SECFND \(210-250\) and SECOPS \(210-255\)](#)
- [CCNA Cyber Ops SECFND 210-250 Official Cert Guide](#)
- [CCNA Cyber Ops SECOPS 210-255 Official Cert Guide](#)
- [Cisco NetFlow for Cyber Security Big Data Analytics](#)

CCNA SECURITY

- [CCNA Security Video Course](#)
- [CCNA Security 210-260 Official Cert Guide](#)
- [Cisco Firepower and Advanced Malware Protection LiveLessons](#)
- [Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP](#)
- [Cisco NetFlow for Cyber Security Big Data Analytics](#)

ETHICAL HACKING

- [Security Penetration Testing \(The Art of Hacking Series\) LiveLessons](#)
- [Wireless Networks, IoT, and Mobile Devices Hacking \(The Art of Hacking Series\)](#)
- [Enterprise Penetration Testing and Continuous Monitoring The Art of Hacking](#)

OTHER SAFARI CYBERSECURITY LIVE TRAINING

- [Ethical Hacking - Penetration Testing](#)
- [Cybersecurity Blue Teams vs Red Teams](#)
- [Introduction to Digital Forensics and Incident Response \(DFIR\)](#)
- [Introduction to Cybersecurity](#)



https://theartofhacking.org/go/training_resources.pdf

QUESTIONS?

THANK YOU!