

Cybersecurity Offensive and Defensive Techniques in 3 Hours

Omar Santos

 Follow @santosomar

About // Omar Ωr Santos



Omar Santos is an active member of the security community, where he leads several industry-wide initiatives and standard bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure.

Omar is the author of over 20 books and video courses; numerous white papers, articles, and security configuration guidelines and best practices. Omar is a Principal Engineer of Cisco's Product Security Incident Response Team (PSIRT) where he mentors and lead engineers and incident managers during the investigation and resolution of security vulnerabilities.

Omar is often presenting at many cybersecurity conferences and he is the co-lead of the DEF CON Red Team Village (redteamvillage.io). He is also the chair of the OASIS Common Security Vulnerability Framework (CSAF) Technical Committee and the co-chair of the Forum of Incident Response and Security Teams (FIRST) PSIRT Open Source Security Working Group.

Omar has been quoted by numerous media outlets, such as TheRegister, Wired, ZDNet, ThreatPost, CyberScoop, TechCrunch, Fortune Magazine, Ars Technica, and more.

Omar's PGP Key: 0xBe19a9d13af27edc



Learning Path: <https://h4cker.org/learning-path>

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?

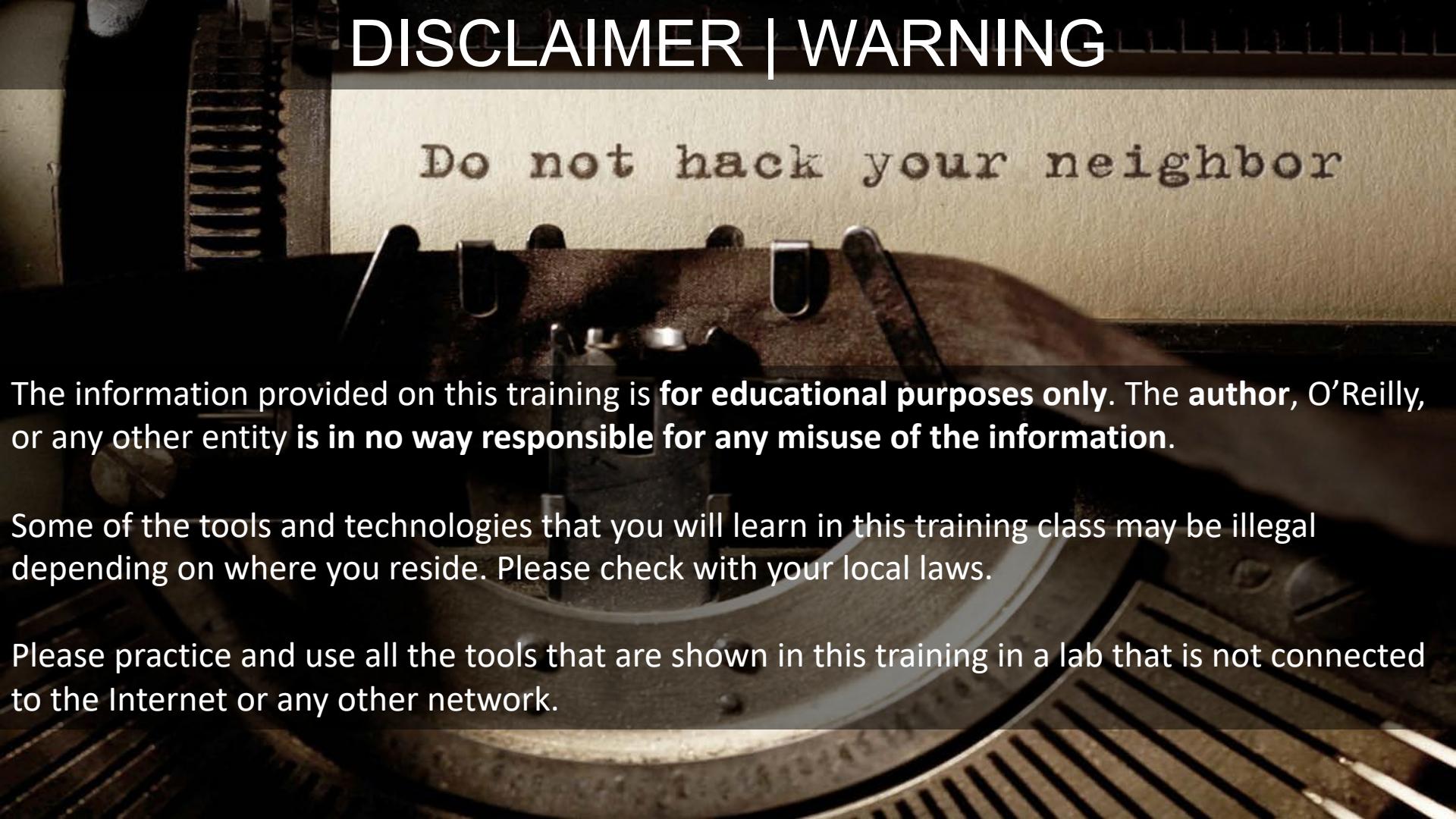
1. Beginner (less than 1 year of experience).
2. Intermediate (2-3 years of experience)
3. Expert (considerable experience).

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.

DISCLAIMER | WARNING



Do not hack your neighbor

The information provided on this training is **for educational purposes only**. The author, O'Reilly, or any other entity **is in no way responsible for any misuse of the information**.

Some of the tools and technologies that you will learn in this training class may be illegal depending on where you reside. Please check with your local laws.

Please practice and use all the tools that are shown in this training in a lab that is not connected to the Internet or any other network.

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).

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

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)).

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

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

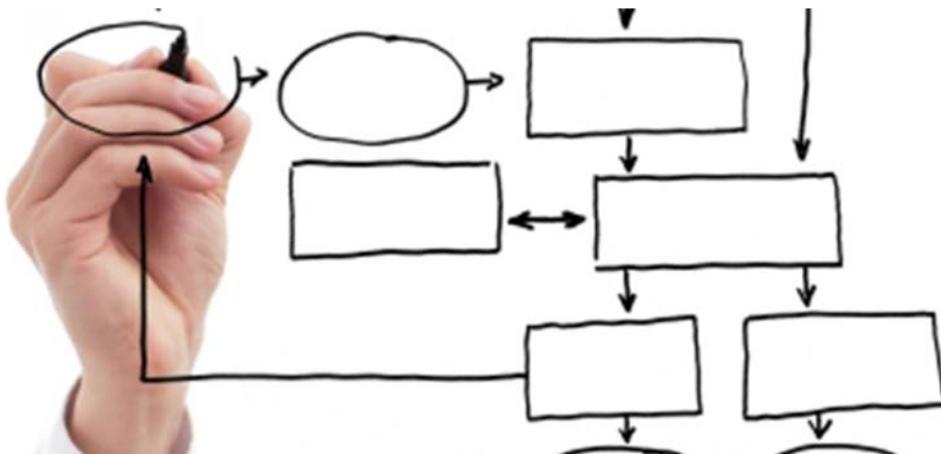
What is the goal of having the red team?

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



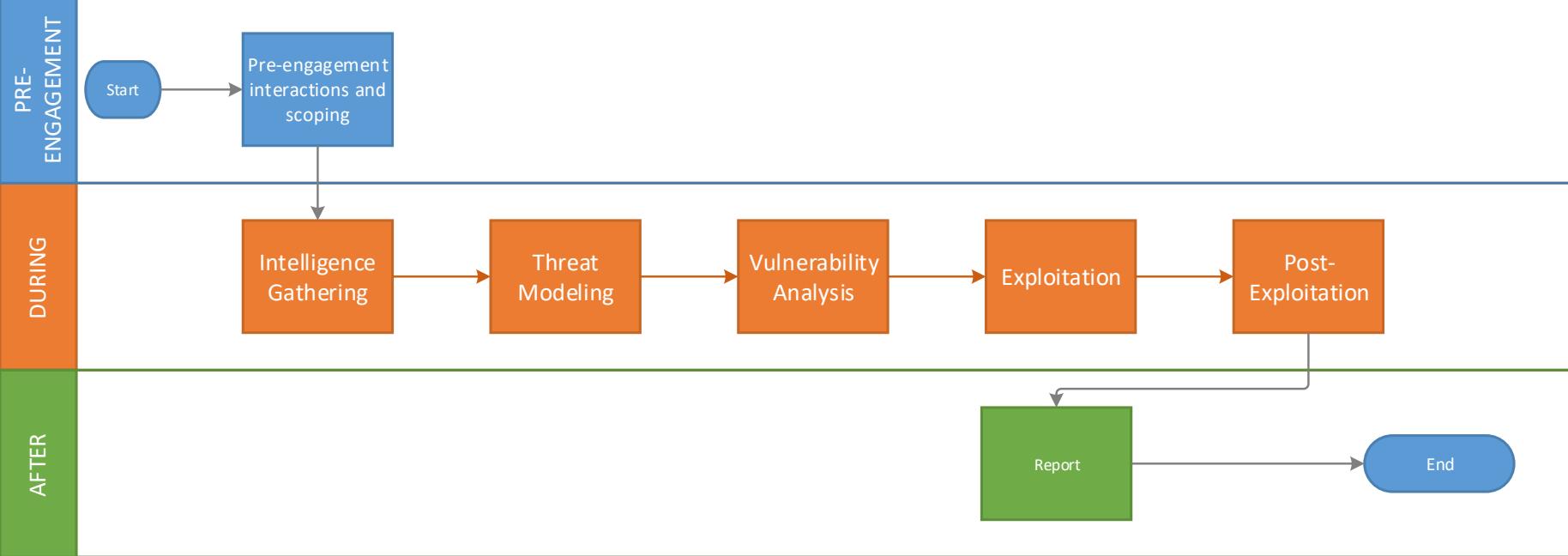
Are Red Team Methodologies the same as traditional penetration testing?

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/>

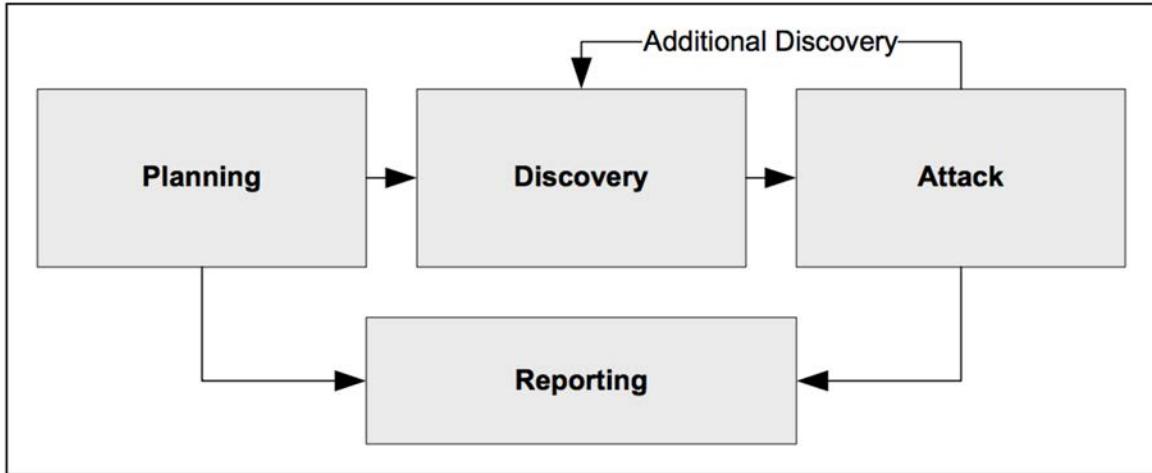


PEN TESTING LIFECYCLE



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...

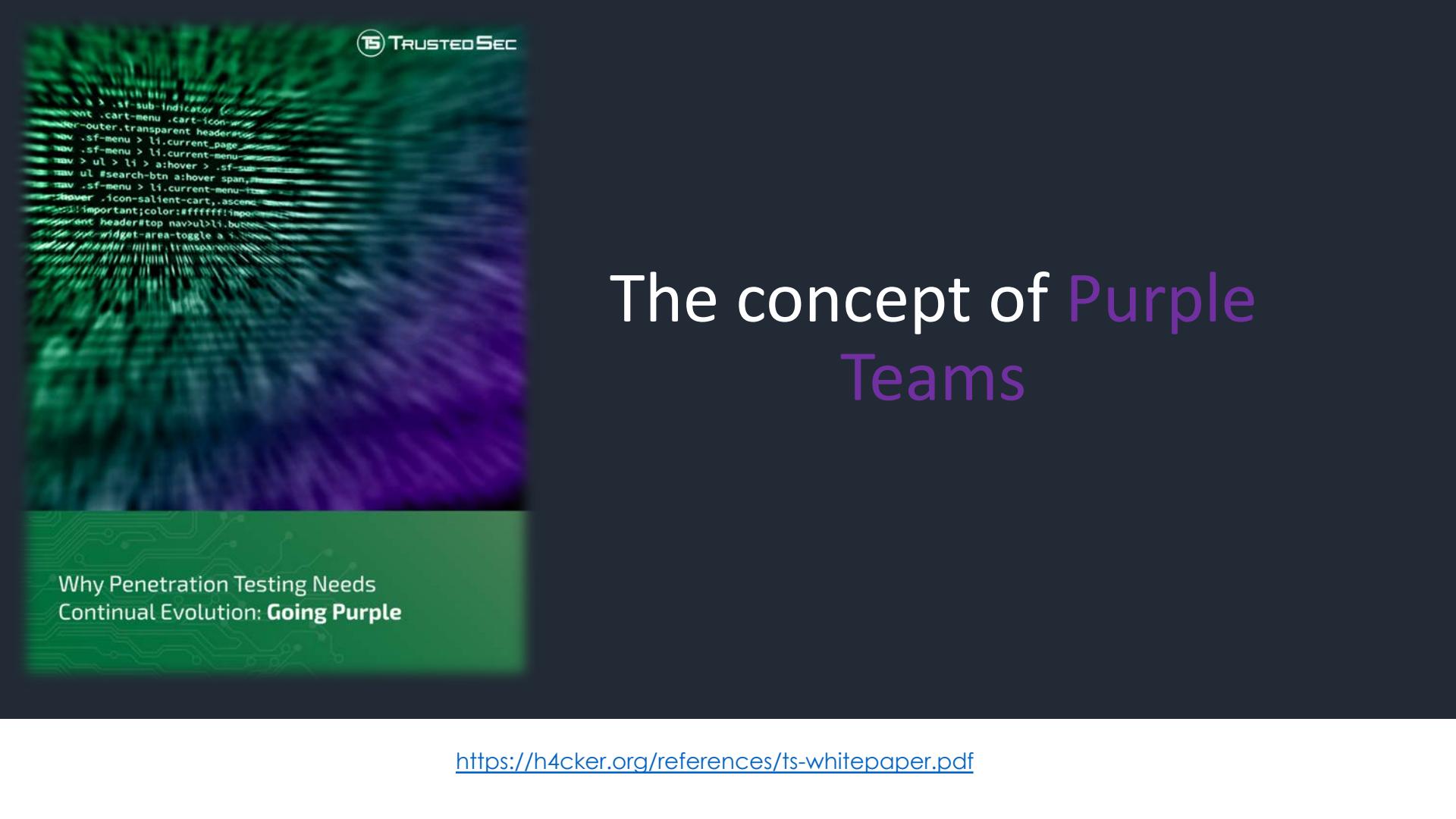
Additional Reference and Video: <http://h4cker.org/rb/2>

Persistent Access: For How Long?

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

The Hybrid Approach: Purple Teams





The concept of Purple Teams

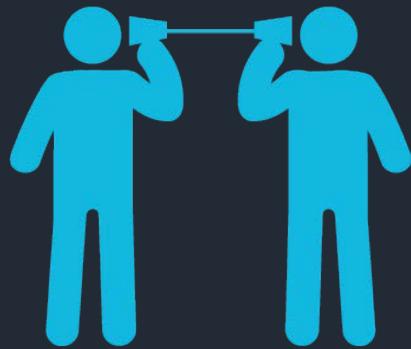
Why Penetration Testing Needs
Continual Evolution: **Going Purple**

<https://h4cker.org/references/ts-whitepaper.pdf>

```
background-color: #000000;
background-image: repeating-linear-gradient(45deg, transparent, transparent 2px, black 2px, black 4px);
background-size: 10px 10px;
background-position: center center;
background-repeat: no-repeat;
background-attachment: fixed;
```

Why Penetration Testing Needs
Continual Evolution: **Going Purple**

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.



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

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

C|EH
Certified Ethical Hacker

Master The Core Technologies Of Ethical Hacking

DOWNLOAD OUR CERTIFICATION TRACK

Download Now

Certified Ethical Hacking Certification

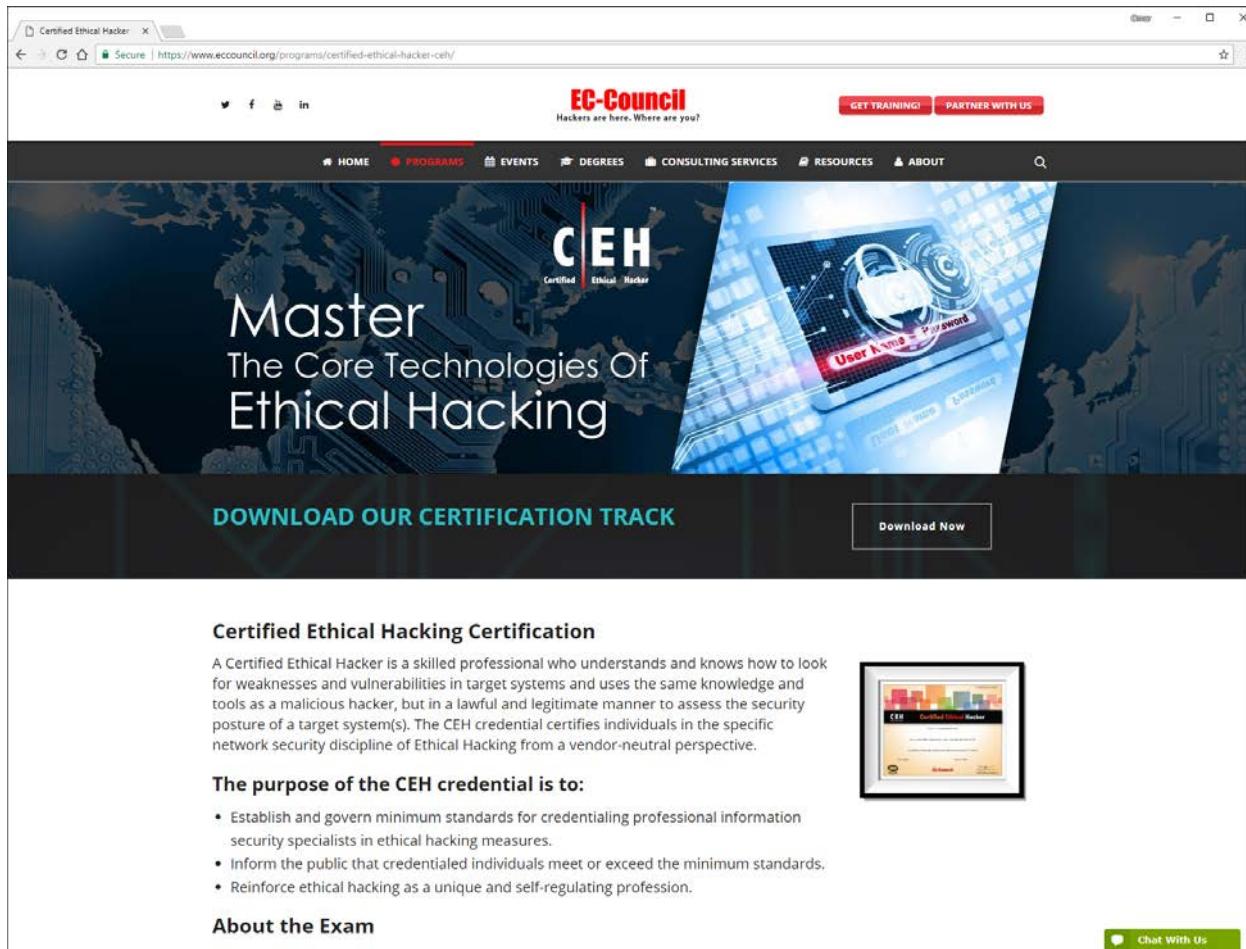
A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The 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:

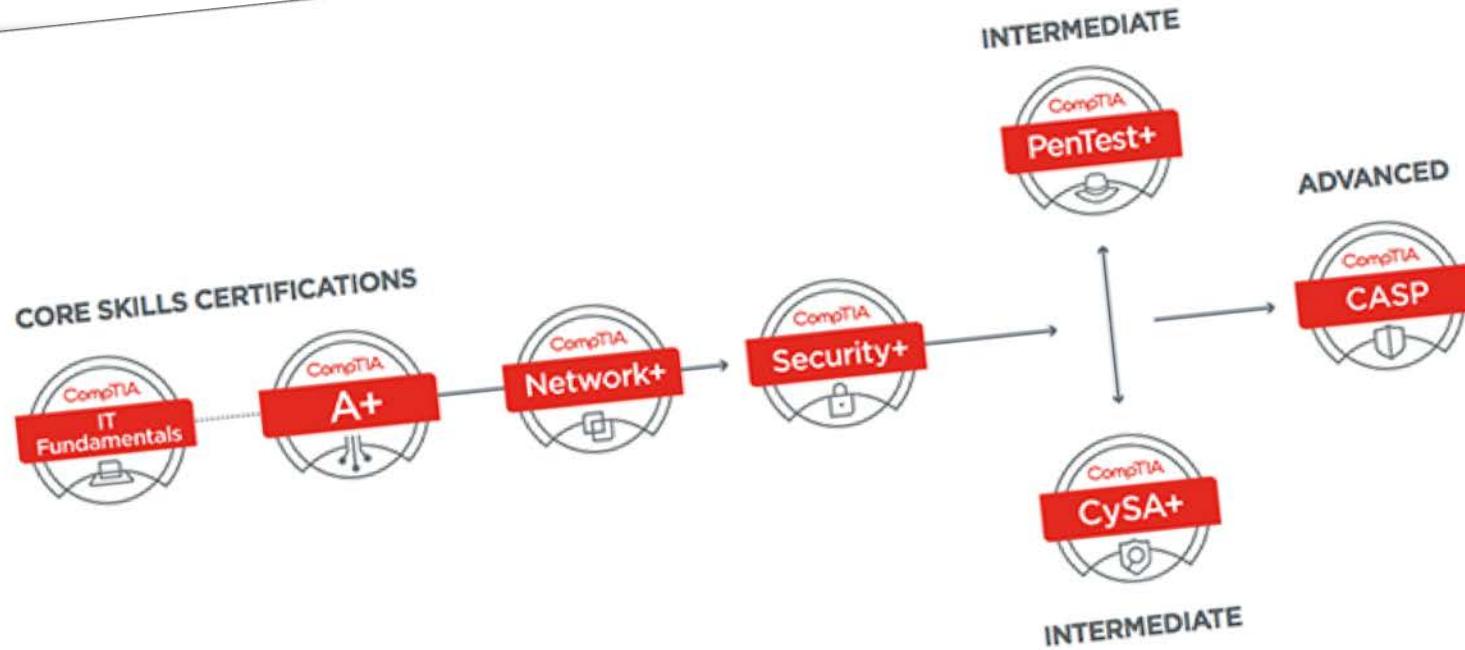
- Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures.
- Inform the public that credentialed individuals meet or exceed the minimum standards.
- Reinforce ethical hacking as a unique and self-regulating profession.

About the Exam

Chat With Us



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



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 technical excellence and repeatable methodologies. It mentions the development of GIAC Certifications to ensure ethical hackers achieve certified status. Below this, there's a table for the "Penetration Testing" certification, which includes columns for "Certification" and "Register". The first row shows the "GCIH" (Certified Incident Handler) badge, a brief description of the certification focus on managing security incidents, and a "Register Now" button. The second row shows the "GPEN" (Certified Penetration Tester) badge, a brief description of the certification focus on executing penetration testing and ethical hacking, and a "Register Now" button.

Penetration Testing		
	Certification	Register
 Certified Incident Handler	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. Affiliated Training: SEC504_Hacker Tools, Techniques, Exploits, and Incident Handling	Register Now
	GPEN holders have demonstrated their ability to execute penetration testing and ethical hacking.	Register Now

<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

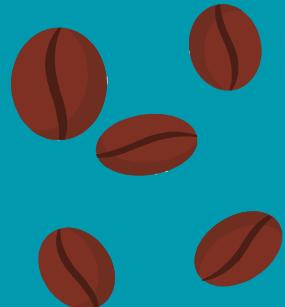


Certified
Secure
Software Lifecycle
Professional

<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	

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

3

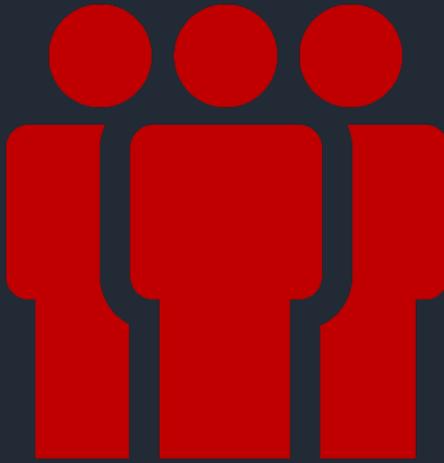


Understand the mission of the red team.

Management sponsorship.

Secure and justify funding.

Understand and create operational processes and policies for the Red Team

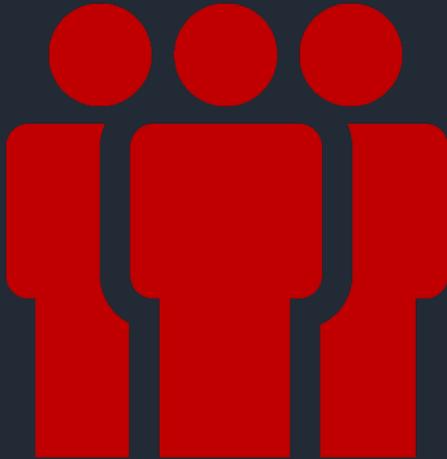


What skills?

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

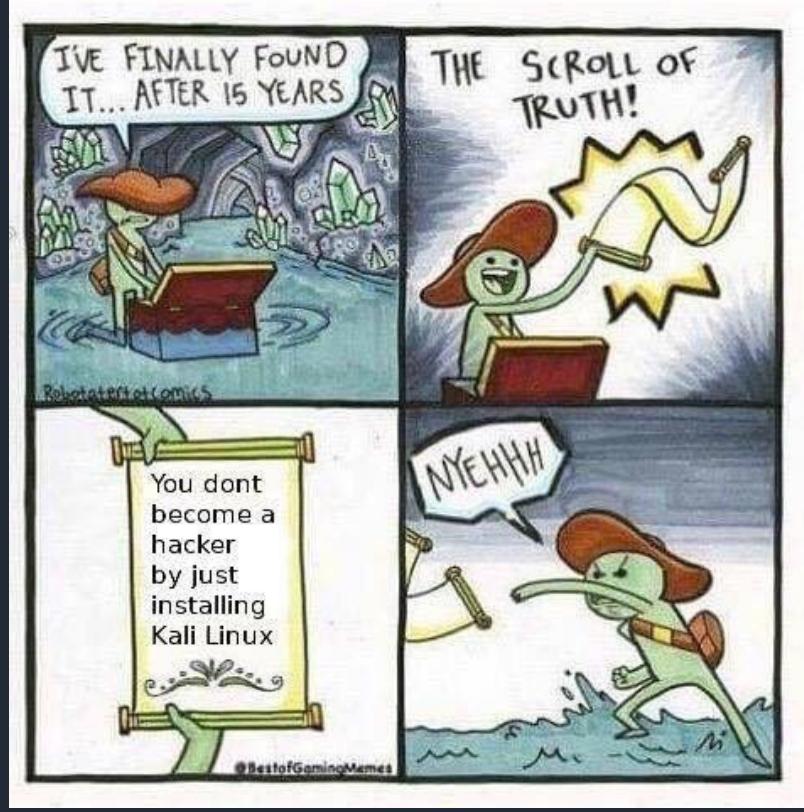
Focus on key issues and biggest risks

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: ~
File Edit View Search Terminal Help
socat(1)                                     socat(1)

NAME
    socat - Multipurpose relay (S0cket CAT)

SYNOPSIS
    socat [options] <address> <address>
    socat -V
    socat -h[h[h]] | -?/?[?]
    filan
    procanc

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.

    Filan 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.

    Procan 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>

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 sockscap / 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)

Proxychains demo



Command and Control

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

[WS]C2[

[*] 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>

```
:';' ,.MMM; ;' ;
:; ;MMMMMMMM; ;;;
:'M: ;MMMMMMMMMM; :M':
:M: MMMMMMMMMMM: :M :
.'M: MMMMMMMMMMM: :M :
;:M' :MMMMMMMMMM' 'M: :
;:M: ;"MMMMMMMM" ;: ,M: :
;:::MM; .M" :::M; ,MM: ::' :
;,: ;MMMM; :MMMMMM: ;:,
MM, ;,,MMMMMM; MMMMMM; ,; MM
M" :''':MMMMMMMM; MMMMMM: " : M
M.: ;MMMMMMMMMMMMMM; : M
::: MMMMMMMMM; MMMMMM : :M
,''; MMMMMMMMMM: MMMMMM : ' :
,' : MMMMMMMMMM: MMMMMM : ' :
;: 'MMMMMMMMMM: MMMMMM ; ' :
;,...;... MMMMMMMMMM: MMMMMM ...;...;.
:MMMMMM MMMMMMMMMMMM: MMMMMM MMMMMM:
:MM" :'" MMMMMMMMMM: MMMMMM "": "MM:
MM: : MMMMMMMMMM: MMMMMM , ' :MM
'MM: :MMMMMMMMMM: MMMM: ; :M:
;:M; : 'MMMMMMMMMMMMMM' : ;MM
;:MM: : MMMMMMMM: MMMM: : MM:
;:M: : MMMMMMMM' MMMMMM' : :MM'
'MM: :"MMMMMM: ;MMMM" , ' :M"
'M: : ""''' ;;;''' : M:
;: 'MMMMMM: ;" : "":
;: :MMMMMM: ;:
;: ,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 "stealthy Python based backdoor that uses Twitter (Direct Messages) as a command and control server. This project has been inspired by Gcat which does the same but using a Gmail account." The Setup section lists requirements and provides a command to install dependencies.

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 Latest commit bca493f on Sep 9, 2015

LICENSE Initial commit 3 years ago

README.md updated the doc 3 years ago

implant.py Initial commit 3 years ago

requirements.txt Added requirements.txt 3 years ago

twittor.py Initial commit 3 years ago

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 [Gcat](#) 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

iagox86 / dnscat2 Watch 120 Unstar 1,246 Fork 256

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

lagox86 committed on Nov 7, 2017 Merge pull request #111 from kost/envsupport Latest commit b55de42 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 Clones or download

This branch is 60 commits ahead of sensepost:master.

PaulSec Added TCP and UDP IPv6 config Latest commit 53f5f7a on Dec 18, 2017

plugins	Added IPv6 UDP exfil	5 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	5 months ago
config-sample.json	Added TCP and UDP IPv6 config	5 months ago
det.py	Update version	5 months ago
det.spec	Update README and config files	a year ago
requirements.txt	Added pygithub as a dependency	5 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>



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
- 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.

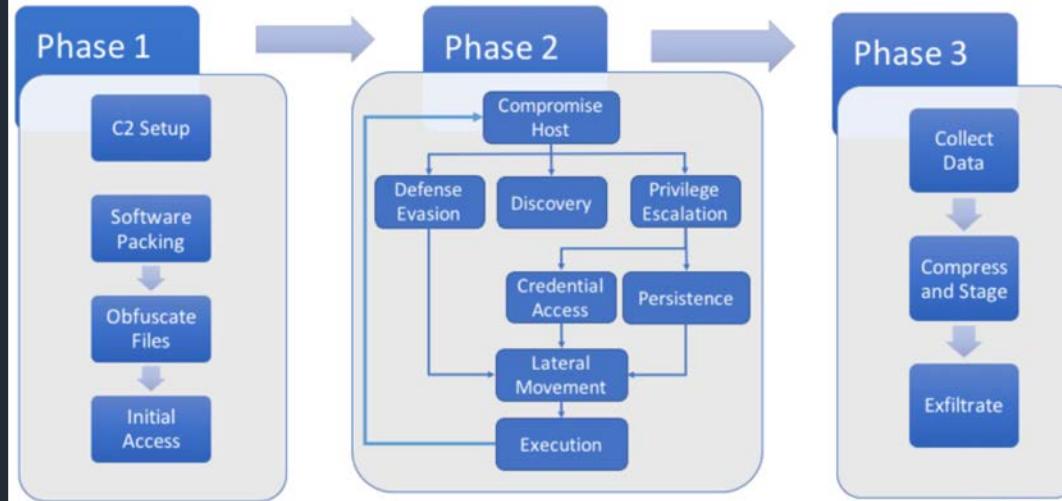
ATT&CK Matrix for Enterprise

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	CMSTP	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	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Scarebaiting 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.: I83L
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

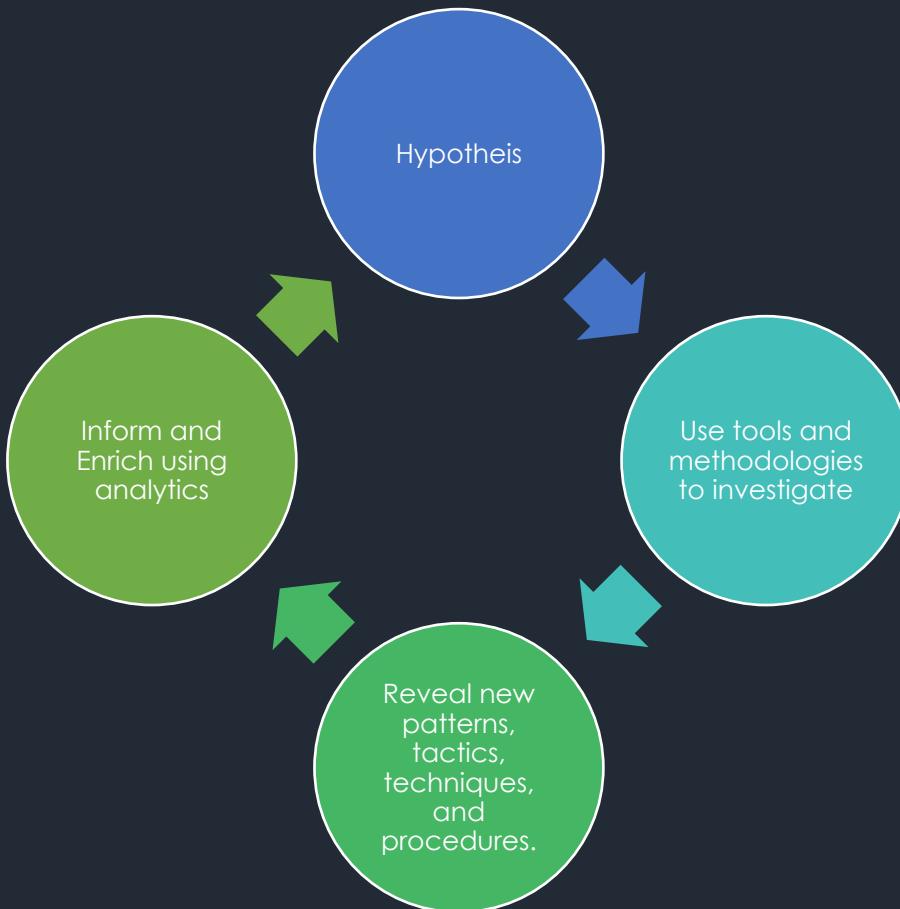
Authors: Christopher A. Korban
Douglas P. Miller
Adam Pennington
Cody B. Thomas

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

Introduction to Threat Hunting

What is Threat Hunting?

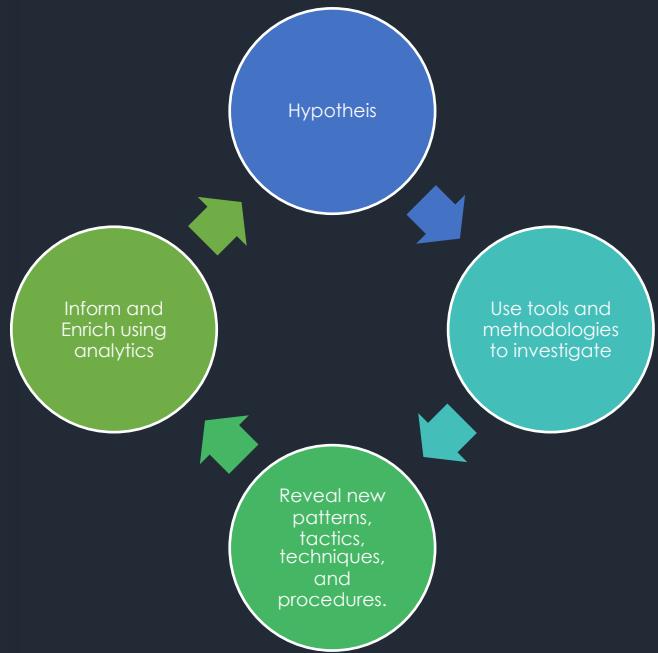
“the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.”

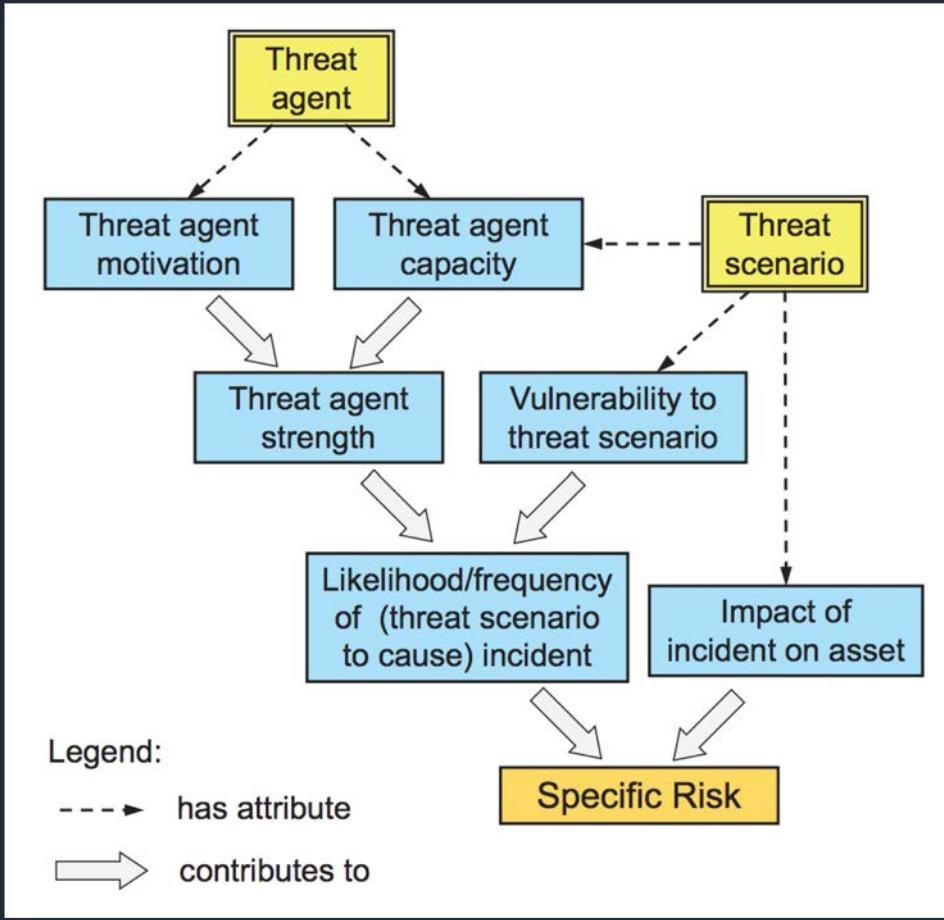


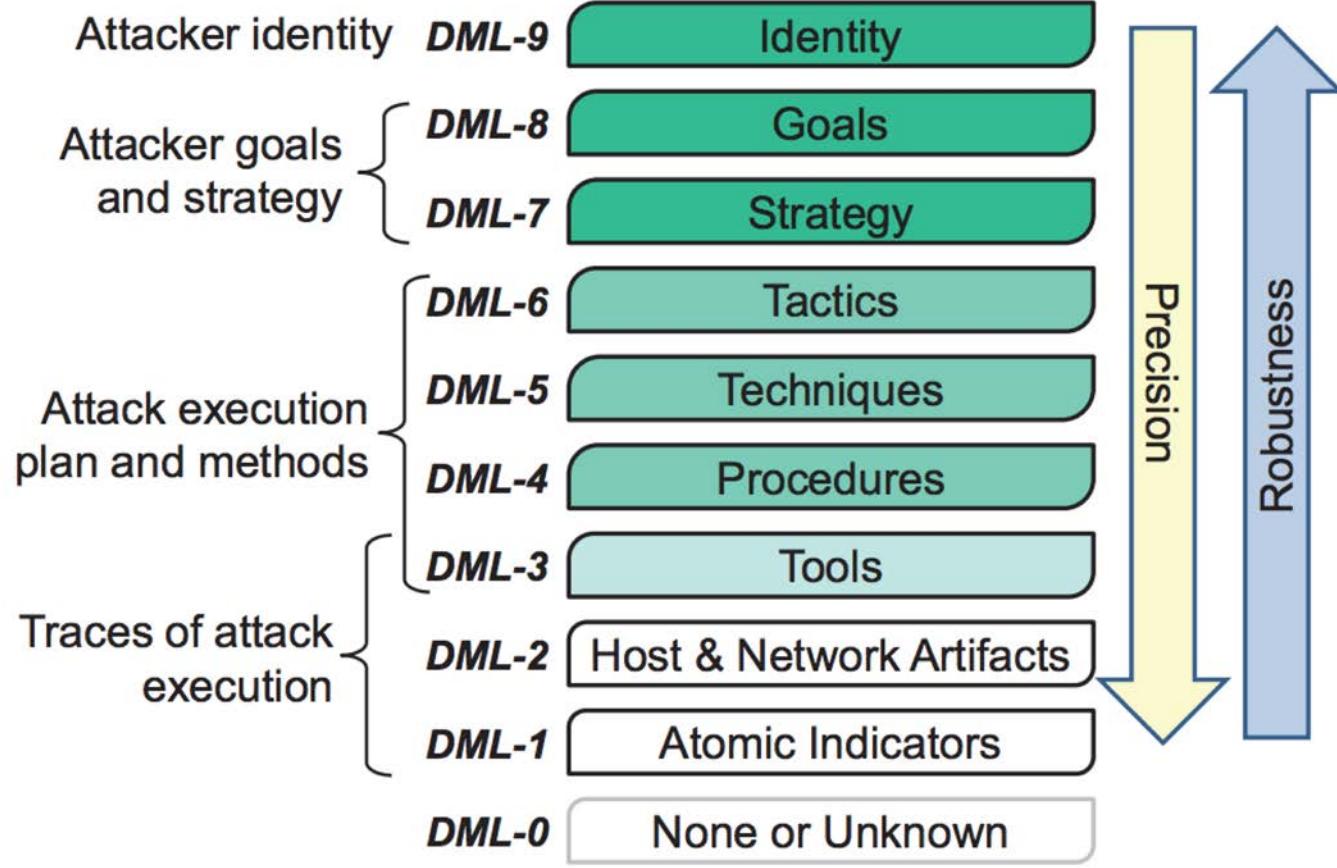
The Threat Hunting Process

HUNTING LOOP STEPS

	HMO 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)

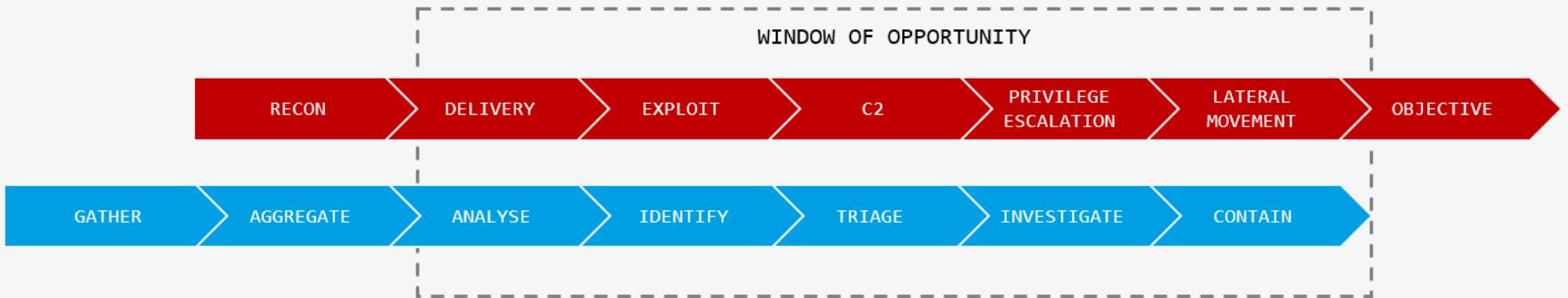






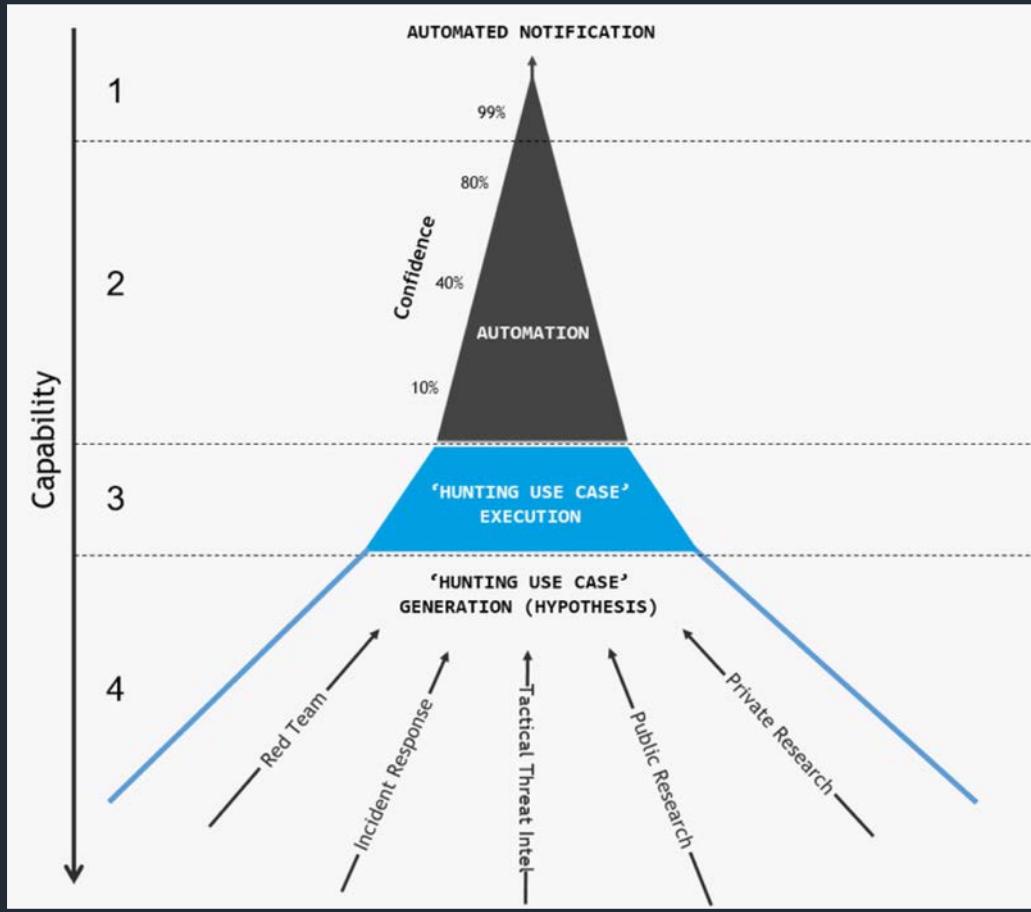
	Level 0 <i>Traditional</i> Not Considered Threat Hunting	Level 1 <i>Experimental</i> Experimenting with Threat Hunting	Level 2 <i>Intermittent</i> Part-time Threat Hunting	Level 3 <i>Proactive</i> Partial Use Case Generation / Execution	Level 4 <i>Leading</i> Complete Use Case Generation / Execution
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)	Ability to Execute 'Hunting Use Cases' (Partial) Full-Time Advanced EDR Usage Full Coverage of Network / Log Data Bespoke Configuration	Ability to Execute 'Hunting Use Cases' (Complete) 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>



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

FIRST CSIRT Case Categories and VERIS

MITRE ATT&CK

Secure | https://attack.mitre.org/wik/Main_Page

MPN MITRE PARTNERSHIP NETWORK

Log in

Main page Discussion

Last 5 Pages Viewed: AppleScript [object Object] LLMNR/NBT-NS Poisoning [object Object] Software: Pupy [object Object] Software: Responder [object Object] Adversarial Tactics, Techniques & Co...

Read View source View history Search enterprise

ATT&CK 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 @MITREatt&ck

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 known tactics, techniques, and procedures used by adversaries in their lifecycle 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.

PRE-ATT&CK | ATT&CK for Enterprise

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!

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	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Pad	

DEM0

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.

MITRE – ATT&CK



REAL-TIME BIG DATA SECURITY

[GITHUB](#)[COMMUNITY HOME](#)

Updated Documentation

[DOCS HOME](#)[WHAT IS IT?](#)[BENEFITS](#)

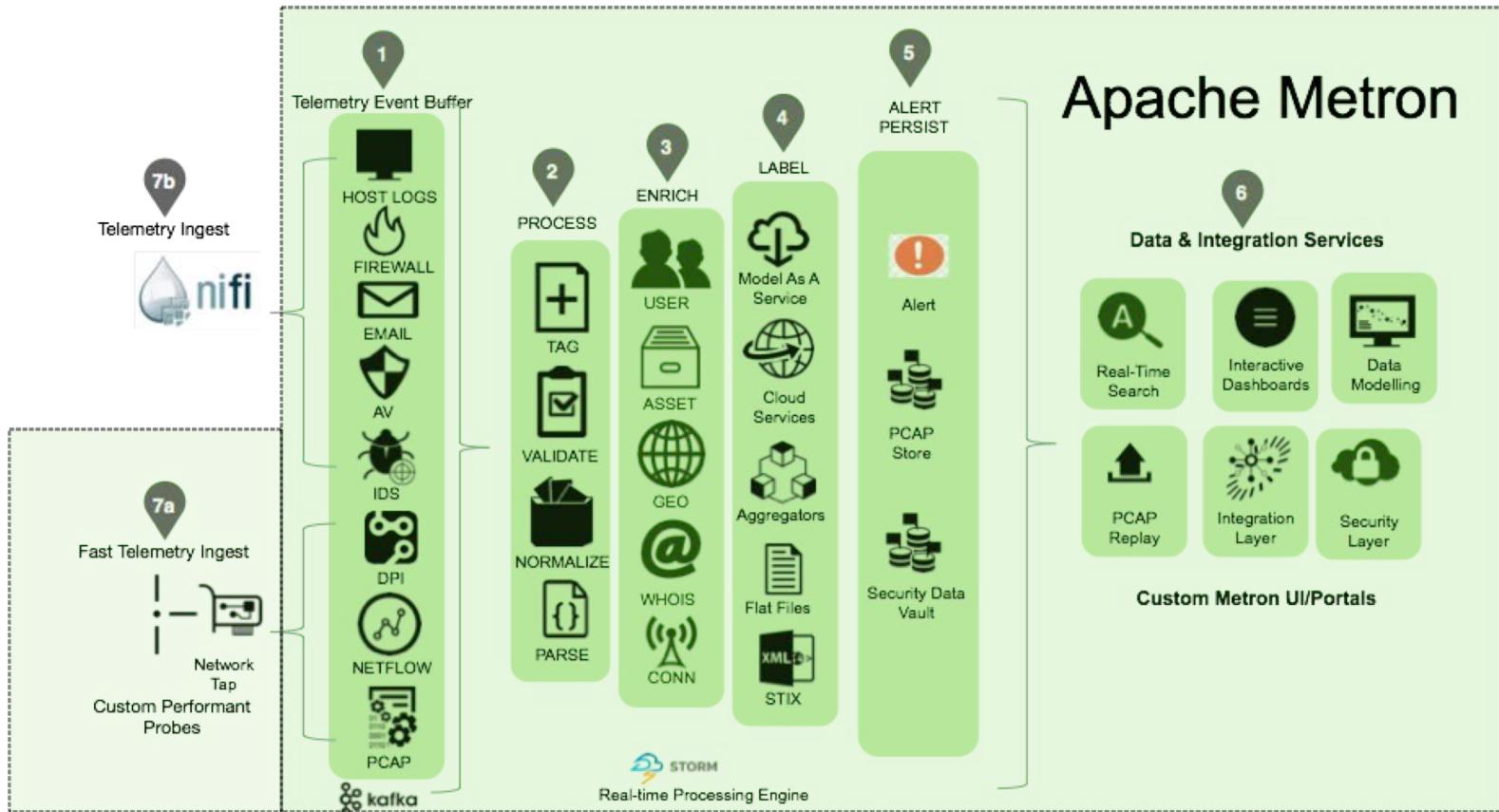
WHAT APACHE METRON DOES

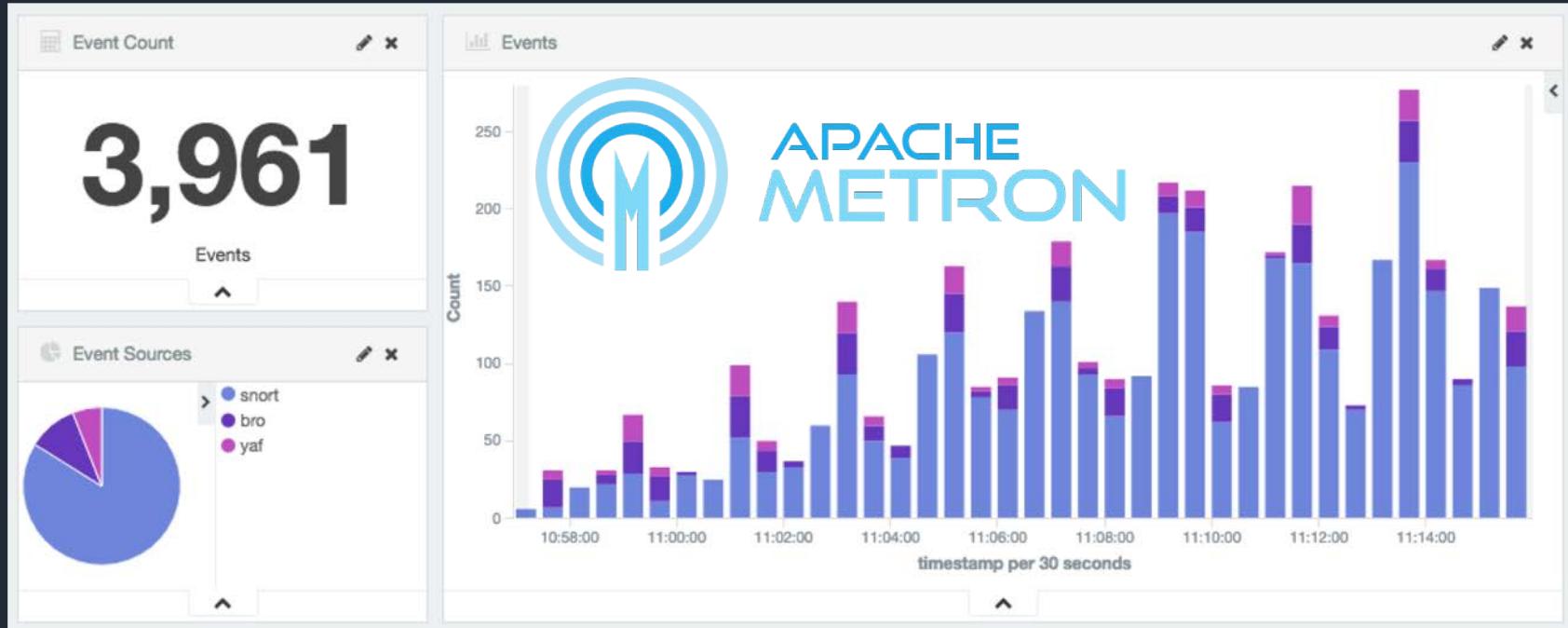
Apache Metron provides a scalable advanced security analytics framework built with the Hadoop Community evolving from the Cisco OpenSOC Project. A cyber security application framework that provides organizations the ability to detect cyber anomalies and enable organizations to rapidly respond to identified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

[MORE](#)

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

Apache Metron





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

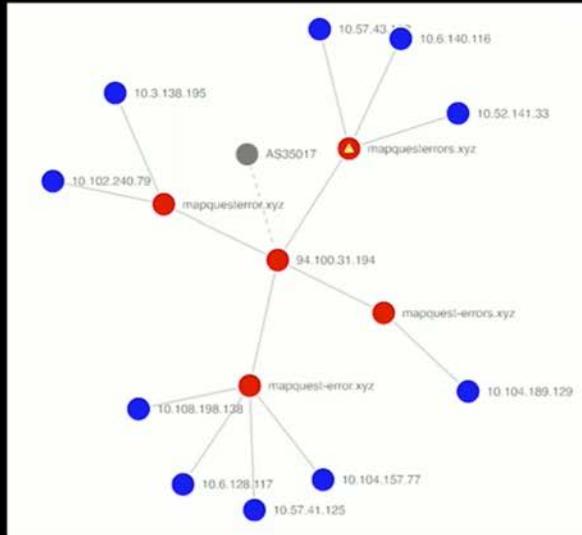
O'REILLY®
Security



OCT 29–NOV 1, 2017
NEW YORK, NY

oreillysecuritycon.com
@OReillySecurity
#OReillySecurity

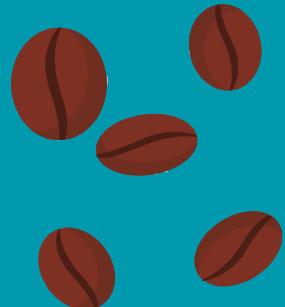
An Example (1)



Maliciousness Rating	
Country	Minimal (0.28x)
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 (4.79x)
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

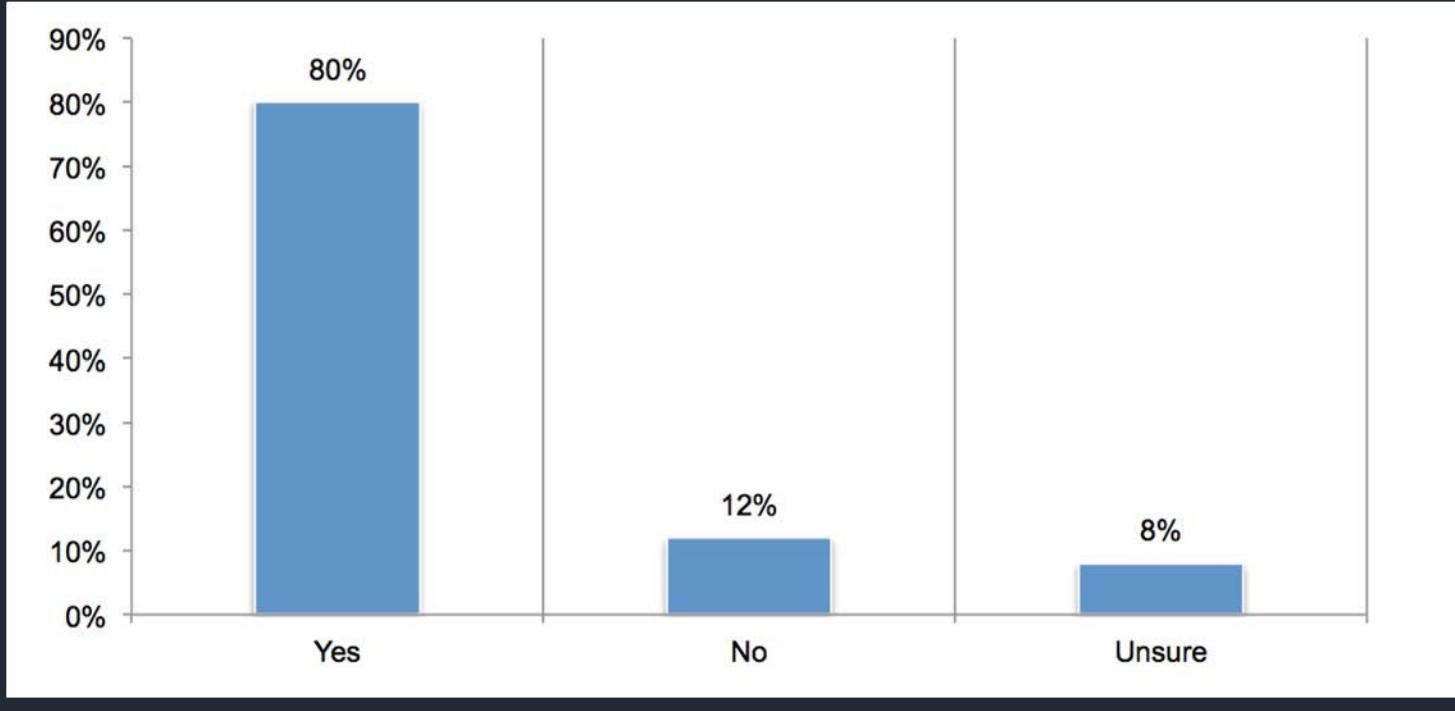
Threat Intelligence

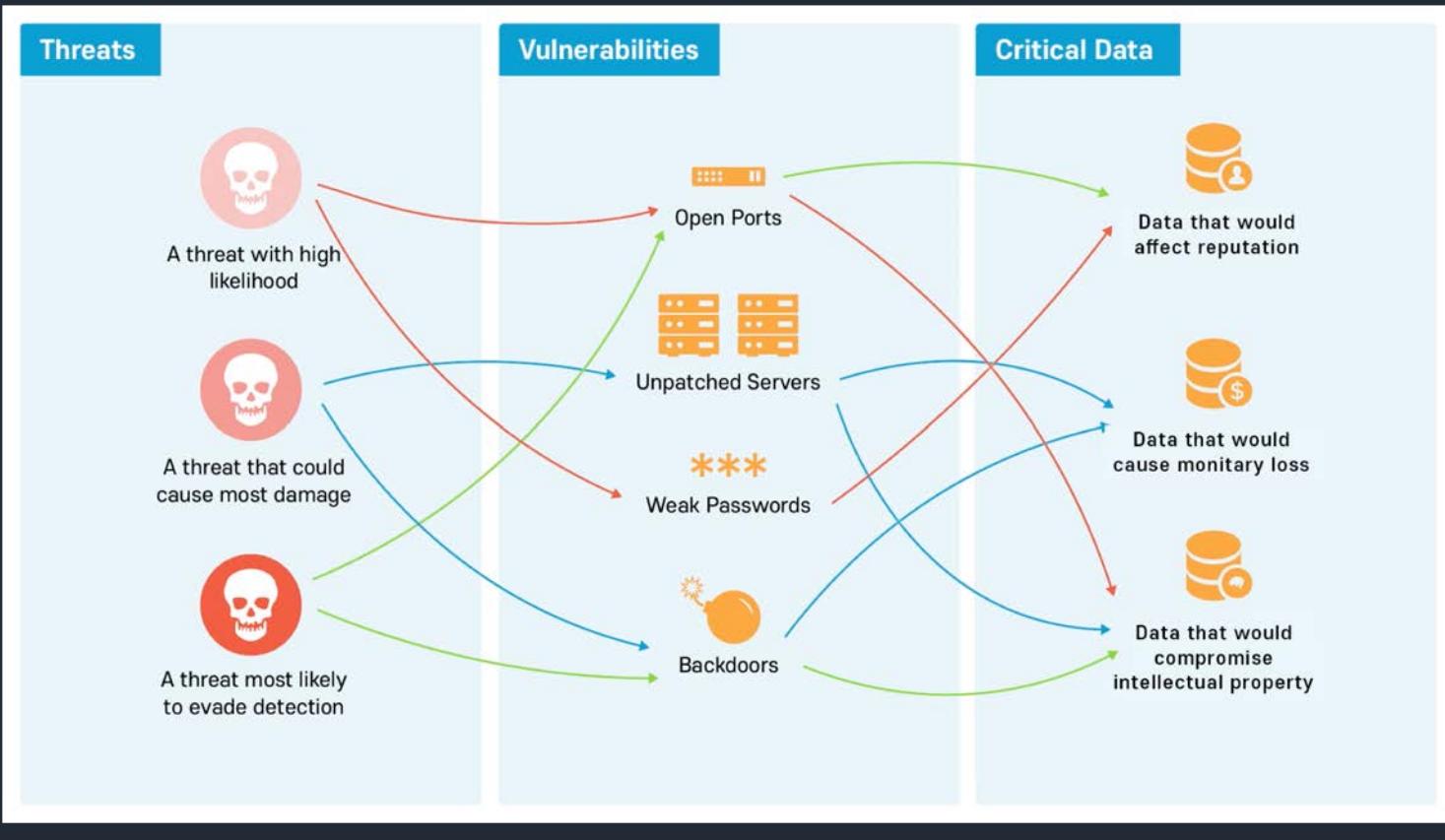
5



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/>

Cyber Threat Intelligence Tech X

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

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>

[tox.ini](#) drop python27 from testing 7 months ago

[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% [docs](#) 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>

https://crits.github.io

The screenshot shows the CRITS GitHub page. At the top, there's a navigation bar with links for Home, Getting CRITs, Documentation, and Community. The main content area has a dark background with white text. On the left, there's a section titled "EXTEND CRITS WITH SERVICES" with a sub-section about developing additional capabilities using the Services Framework. Below this is a "Get started now!" button. On the right, there's a large code block in Python. The code is related to handling PCAP files and generating XML reports. It includes imports for `os`, `tempfile`, `subprocess`, and `etree`. It defines functions for reading PCAP files and generating XML reports. The XML generation part uses `etree` to parse XML files and apply XSLT transformations.

```
pcap_html = "Could not get PCAP from CRITs: %s" % pcap_err
return {'HTML': pcap_html}

# write PCAP to disk
temp_pcaps = tempfile.NamedTemporaryFile(delete=False)
temp_pcaps.name = temp_pcaps.name
temp_pcaps.write(pcap_data)
temp_pcaps.close()

# use tshark to generate a pml file
temp_pml = tempfile.NamedTemporaryFile(delete=False)
temp_pml.name = temp_pml.name
temp_pml.write("tshark -r %s -T pml -w %s" % (temp_pcaps.name, temp_pml.name))
temp_pml.seek(0)

# transform XML into HTML
xsl_file = None
for d in settings.SERVICE_DIRS:
    try:
        file_dir = "%s/metacap_services" % d
        xsl_file = open("%s/pml2html.xsl" % file_dir, 'r')
    except IOError:
        pass
    if not xsl_file:
        return {'HTML': 'Could not find XSL.'}

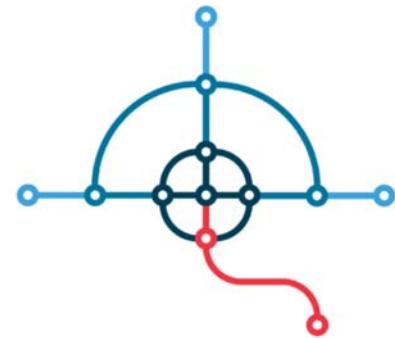
parser = etree.XMLParser()
parser.resolvers.add(file_resolver())
xslt_root = None
try:
    xsl_input = etree.parse(temp_pml, parser)
    xslt_root = etree.parse(xsl_file, parser)
    transform = etree.XSLT(xslt_root)
    ...
```

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

ANOMALI



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.

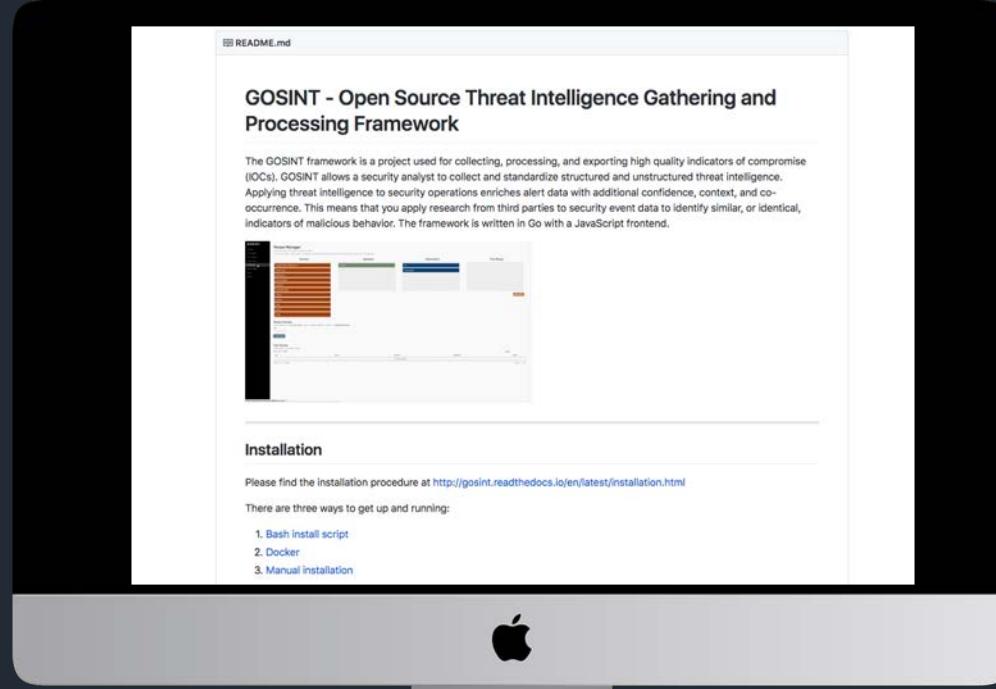
[DOWNLOAD BROCHURE ▶](#)

[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>

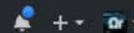
<http://s3-us-west-1.amazonaws.com/umbrella-static/index.html>



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!