

Performing OSINT Gathering on Corporate Targets

PREPARING TO PERFORM CORPORATE OSINT



Jerod Brennen

CISSP, INFOSEC GEEK

@slandail www.slandail.net



Overview



The what and why of OSINT

The Penetration Testing Execution Standard (PTES)

Foundational understanding of OSINT

Setting up your testing environment

Performing OSINT activities



What Is OSINT?



OSINT

Open Source Intelligence

Publicly available information about an organization



Intelligence Gathering Disciplines



HUMINT



GEOINT



SIGINT



FININT



MASINT



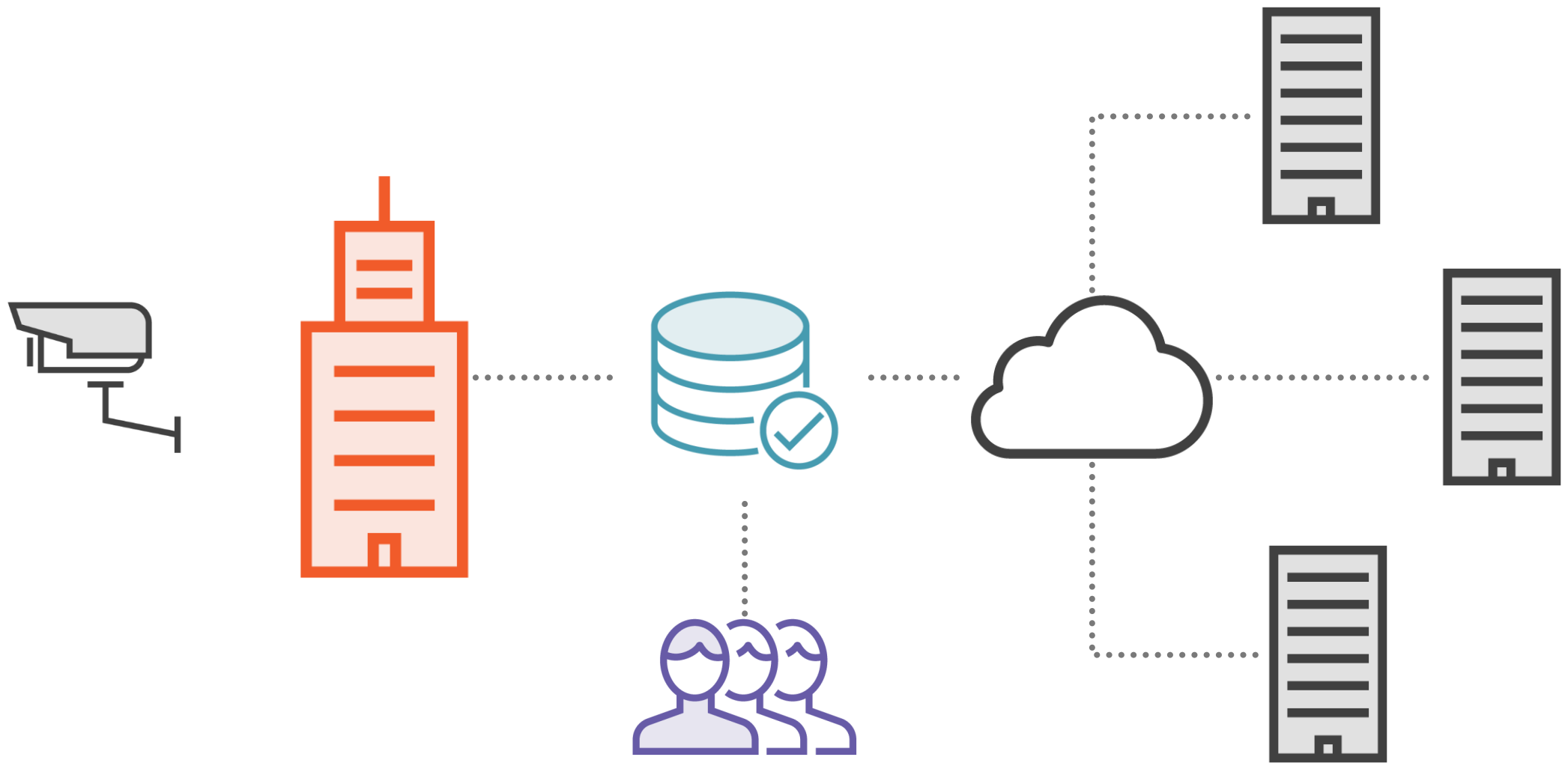
OSINT



OSINT
!=
Open Source Software



OSINT Gathering



Why Is OSINT Important?



Applications

Endpoints

Network

Servers

Data

Locations

People

Attack Surface



Information Leakage

A weakness where a system or an application reveals sensitive data that an attacker may be able to exploit



Types of Information Leakage

Necessary

IP addresses
DNS entries

???

Documents
Directories

Unnecessary

Version information
Error messages



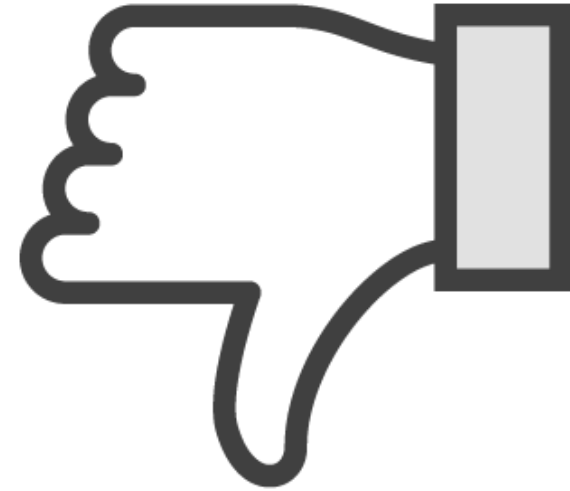
Balance risk with rewards



Pros and Cons

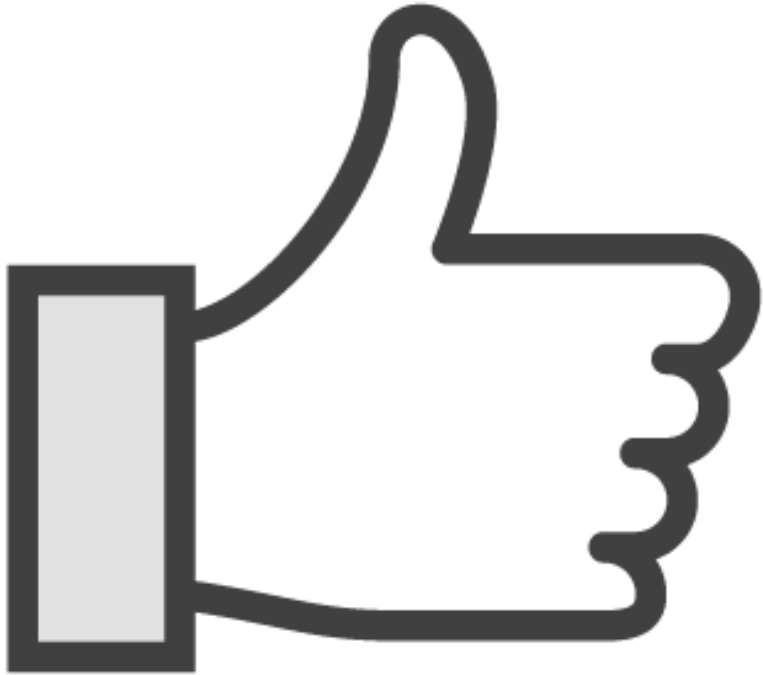


Good Stuff



Not-So-Good Stuff





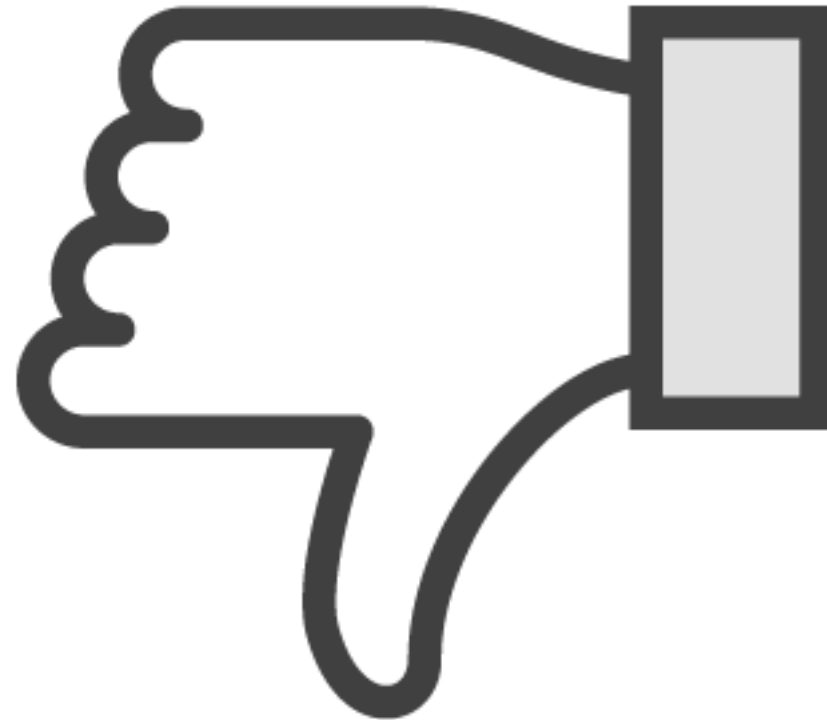
Avoid detection

Inexpensive

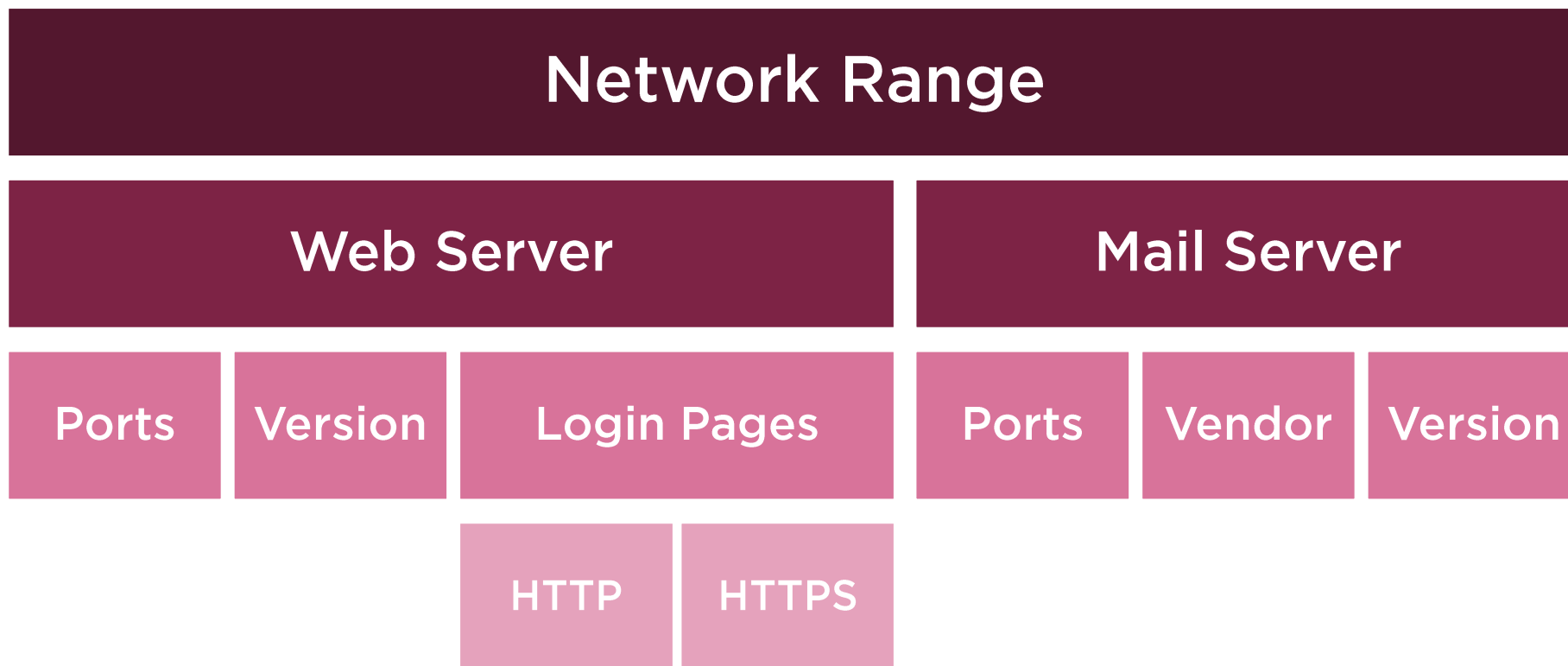
Save time



Outdated data
Inaccurate data
Potentially
overwhelming



OSINT Analysis



OSINT Gathering



How Effective Is OSINT Gathering?



“At times, we’ve had valid authentication credentials for a target environment without sending a single packet to the network.”

Tim Tomes, author of Recon-ng



The Penetration Testing Execution Standard (PTES)



Penetration
Testing
Execution
Standard
(PTES)

Pre-engagement interactions

Intelligence gathering

Threat modeling

Vulnerability analysis

Exploitation

Post exploitation

Reporting



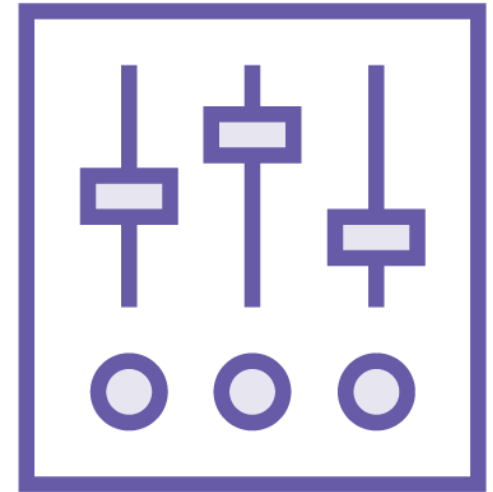
One Size Fits All?



Multiple Types



Multiple Forms



Multiple Levels

Two Types of OSINT



Corporate

Gathering information about
the organization



Individual

Gathering information about
the people
associated with the organization



Three Forms of OSINT

Passive Information Gathering

Undetectable

Semi-Passive Information Gathering

Mimic normal traffic

Active Information Gathering

Detectable



Three Levels of OSINT



Compliance Driven

PCI
FISMA



Best Practice

Mature Program
Customer Expectation



State Sponsored

Critical Infrastructure
Political Climate



Target Selection



Identification and naming of target

Rules of engagement

Time length for test

End goal of the test

How long should we spend
gathering OSINT?



It depends



What Does OSINT Entail?



Information Gathering

Gathering physical OSINT

Gathering logical OSINT

Constructing an org chart

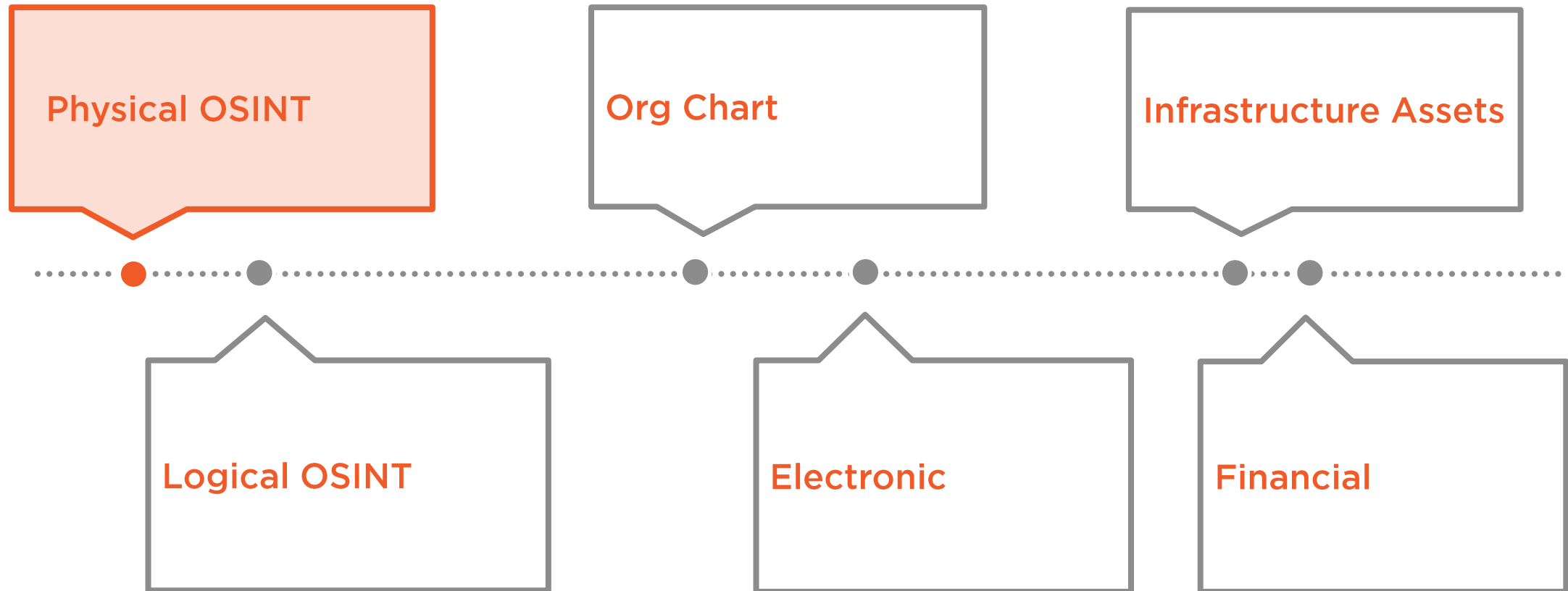
Gathering electronic OSINT

Identifying infrastructure assets

Gathering financial OSINT



OSINT Timeline



Profile the legal entity



Demo



Look for demos at the end of each module



Putting It All Together



Preparing Your Testing Environment



What Do We Do with the Data?

Data Collection

Manual processes

Automated tools

Gather data

Data Analysis

Review data

Think like an attacker

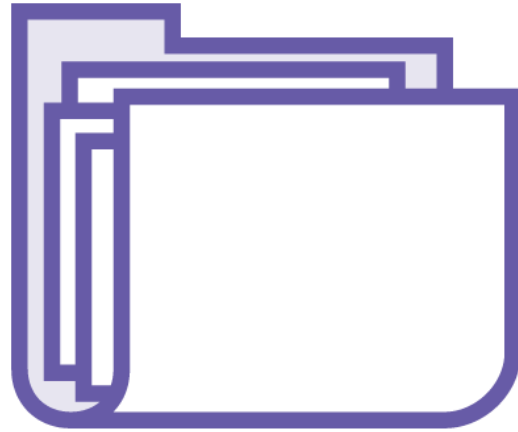
Prepare for reporting



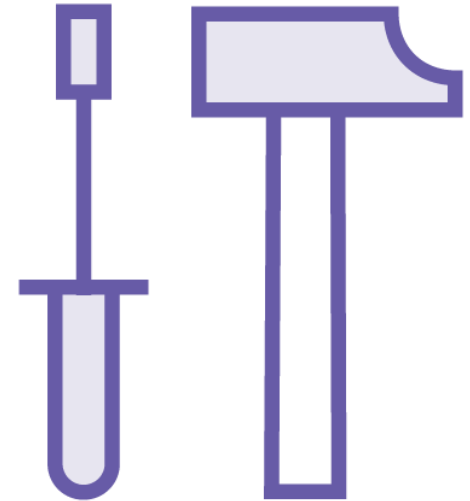
Preparing to Gather OSINT



Testing System
Virtual machine



Folder Structure
Align with PTES
one folder per module



Testing Tools
Preinstalled, add-ons,
and custom scripts



The Pen Tester's Toolbox

Your mileage may vary

Watch for this icon in each module





Mind Mapping Software

XMind

- <http://www.xmind.net/>

FreeMind

- <http://freemind.sourceforge.net/>



Virtual Machine Players

Oracle VirtualBox

- <https://www.virtualbox.org/>

VMWare Workstation Player

- <http://www.vmware.com/>



Kali Linux

- <https://www.kali.org/>

Options

- Install on disk
- Live DVD
- Virtual machine

Web Resources



Shodan

Pastebin

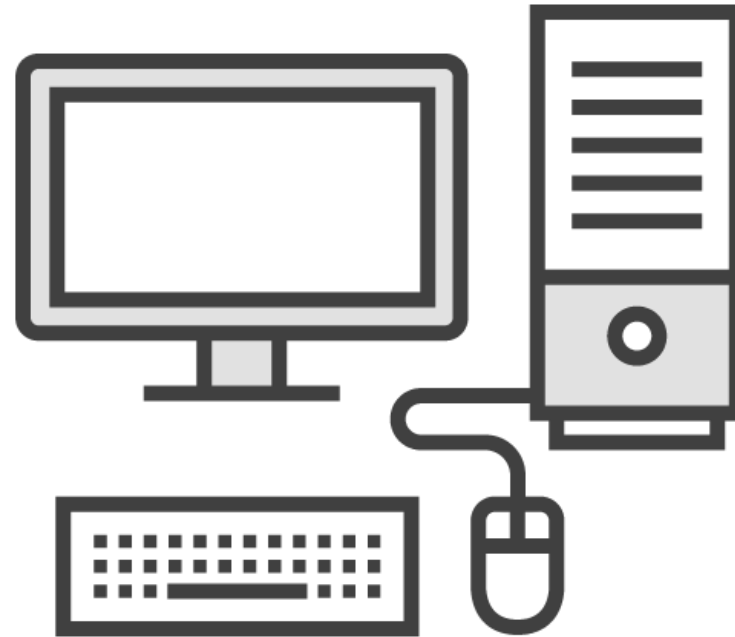
Robtex

Hurricane Electric










PunkSPIDER

Censys

Maltego CE
FOCA
Creepy
TheHarvester
Recon-ng



Course Resources

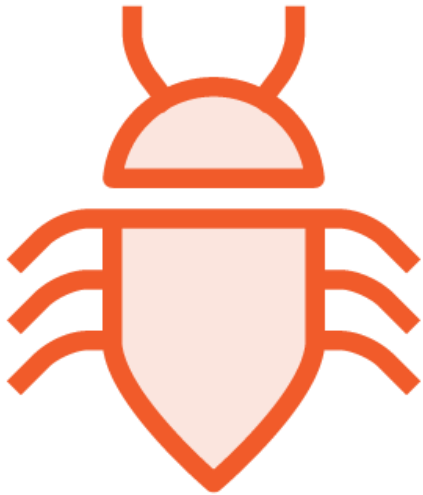
 slandail committed on GitHub
 01-preparation
 02-physical
 03-logical
 04-org-chart
 05-electronic
 06-infrastructure
 07-financial
 README.md

GitHub repository

<https://github.com/slandail/corporate-osint>

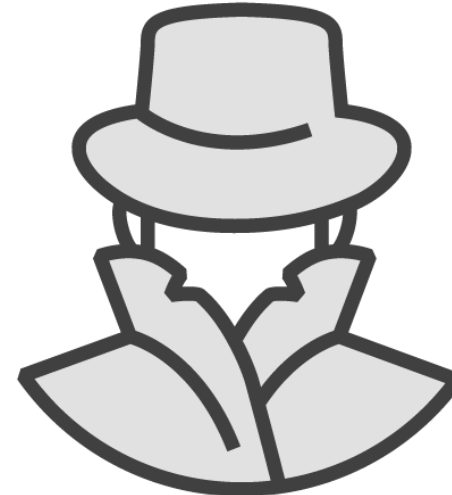


Bug Bounty Programs



Bugcrowd

<https://bugcrowd.com/>



HackerOne

<https://hackerone.com/>



Summary



OSINT definition

Importance

Effectiveness

Alignment with PTES

Process

Testing environment



Onto the next module:
Gathering Physical OSINT

