



MITRA INTEGRASI INFORMATIKA

Cyber Sec

Python-Assisted Red Teaming Operation

Pycon Indonesia 2019

About Us

Hi!

Satria Ady Pradana

- **Cyber Security Consultant** of **Mitra Integrasi Informatika**
- Penetration Tester, Red Team
- IoT / OT Cyber Security Special Interest Group
- Community Leader of **Reversing.ID**

- Love **Low-Level** Stuffs



 xathrya

 xathrya

 @xathrya

About Us

Hi!

M. **Dzikri** Ramdhani

- **Cyber Security Consultant** of **Mitra Integrasi Informatika**
- Penetration Tester, Red Team
- Reverse Engineering addict
- Python Lover

- Love **Low-Level** Stuffs



@mr_dzikri



HadrianCorbett



MITRA INTEGRASI INFORMATIKA

Cyber Sec

“

We are not going to teach you Python programming.

We are going to show you the power of python! ❤️

Agenda

Introduction to Red-Teaming

What is Red-Teaming? What it need?
How effective can it be?

01



02



Tactics, Techniques, and Procedures

Successful attack comes from strategic plan.



Offensive Python

How to train your Python .. For doing dirty job.

04



03



Security loves Python

Python bytes, but we still love.

First, A Story

It's fictive, of course!



This is **Budi**

Own a **store** in marketplace.

Trusted store with **hundred transactions** each day.

Marketplace is secure, **comply** to various security standards.

Budi activated 2 Factor Authorization (**2FA**).

OTP will be sent to his mobile phone each time he login.

This morning, an OTP Is coming when he was sleeping.

Budi's account got hacked!!

Money got stolen from his account.

What possibly can be **wrong**?

Introduction to Red Teaming

“Attack is the secret of defence; defence is the planning of an attack”

- Sun Tzu

Red Teaming

- Originate from **military** practices.
- Evaluate security posture by **playing as aggressor**.
- **Full-scope, multi-layered** attack simulation designed to measure how well organization's security controls can withstand attack from real-life adversaries.

Requirements

- Deep knowledge of **systems** (computer system, protocols, libraries, etc).
- Ability to think **outside the box**.
- Software **development** skills.
- **Penetration** testing skills
- Social engineering.

Red Team vs Pentest

Red Team

- Act as **enemy**
- **Entire environment** is within scope.
- Goal is to penetrate (as deep as possible), maintain persistence, pivot, exfiltrate assets.

Penetration Test

- No special act.
- Scope is **limited** to certain extent.
- Goal is to prove exploitation can happen.

Tactics, Techniques, Procedures

Inside the mind of Threat Actor

- **Tactics**

Outline the way adversary choose to carry out attack from beginning to the end. Describing the way threat actor operate during different steps of operation / campaign.

- **Techniques**

Technological approach of achieving intermediate results during campaign.

- **Procedures**

Special sequence of actions used.

Highly detailed description in the context of techniques.

The Cyber Kill Chain



Highlight on Infrastructure

- Provide **reliable** communication for long term campaign.
- **Obfuscate** and **masquerade** to sufficiently avoid detection.
- **Flexible**, adapt to priority or goals.

Packet crafting reverse engineering

Penetration testing machine learning

Cyber Security Forensic

Automation Exploit Development

Fuzzing

-
-
-

Cyber Security Python

“Python bytes!”

Why Python for cyber security?

1. Designed for **rapid prototyping**
2. **Simple** and **clean structure**, improve readability and ease of use.
3. **Extensive library**, also **ease of interfacing**
4. **Widely adopted**, most linux distro ship it by default *

Which makes it ideal language for scripting and rapid development.

Tools? Use Python!

- Many essential tools are written in Python.
- Many tools scriptable with Python.
- Not satisfied? Write your own tools.

Case: Basic Networking

Server

- Host some files
- Collect data
- Relay information

- Common: HTTP, FTP, SMB

Client

- Create (malicious) requests
- Scraping
- Probing

Case: Basic Cryptography

- Encrypt & Decrypt
- Compute hash value
- Some stuffs on digital certificate

Offensive Python

Using Python for Red-Team Operations.

Where is Python?

Infrastructure Preparation

Good infrastructure for long-term and series of attacks.

Attack & Exploitation

Conducting or supporting the attack.

Miscellaneous

Not-directly used for attack but still useful.



Infrastructure Preparation

- Deliver payloads
 - Active Exploitation
 - Controlling nodes
 - Receive results
-
- Every part of campaign might need **infrastructure**.
 - Programmatically deploy infrastructure for engagements.

Common Infrastructures

- Command & Control Servers
 - Payload Server
 - Phishing Servers
 - Redirectors
-
- Should we create dedicate infrastructure?
 - Server or serverless?

Phishing Servers

- Orchestrate **SMTP servers** with good reputations
 - **Scheduling** mail deliveries, coordinated with multiple available SMTP servers.
 - **DKIM, DMARC, SPF**, etc... etc...
-
- Python way?

Redirectors

- Achieve resilience and concealment by having set of “**proxy**” in front of assets.
- Common types:
 - **SMTP**
 - **Payloads**
 - Web traffic
 - C2 (HTTP/HTTPS, DNS, etc)
- Python way?

Infrastructure Setup

- **DomainHunter** (<https://github.com/threatexpress/domainhunter>)
 - Hunt expired domains for categorization / reputation

Attack & Exploitation

- Attack **machine** and **human**.
- Deliver malicious code to potential victims:
 - Reconnaissance
 - Weaponization
 - Delivery
 - Command & Control
 - Lateral Movement
- Network penetration:
 - Reconnaissance
 - Exploitation
- Red-Team **iterate** these over and over.

Reconnaissance

- **Active** or **passive** intelligence gathering.
- Gathering:
 - Assets (machine, application).
 - Identity.
 - Document.
 - Metadata.
- Map and classify.

Scanning, Probing, Enumerating

- **Scapy** (<https://scapy.net/>)
 - Packet manipulation and decoder.
 - Send, sniff, dissect, and forge network packets.
- **OpenDoor** (<https://github.com/stanislaw-web/OpenDoor>)
 - Directory scanner

Make it async?! Sure!

- **Wfuzz** (<https://github.com/xmendez/wfuzz/>)
 - Web fuzzer framework
- **Pyfuzz** (<https://github.com/AyoobAli/pyfuzz>)
 - URL fuzzing tool
 - Fuzzing to discover hidden files/directories

OSINT with Python

- **Recon-NG** (<https://github.com/lanmaster53/recon-ng>)
 - Reconnaissance framework for powerful environment to conduct open source web-based reconnaissance.
- **Belati** (<https://github.com/aancw/Belati>)
 - Collecting public data & public document from website and other services.
- **Pwndb** (<https://github.com/davidtavarez/pwndb>)
 - Search leaked credentials.
- Python + Shodan API

With Machine Learning? Sounds good

Weaponization

- There are many CVEs
- Create python script for generate payload based on public disclosure.

Delivery

- **CredSniper** (<https://github.com/ustayready/CredSniper>)
 - Phishing framework on top of micro-framework.
 - Supports capturing 2FA tokens.

Command & Control – Remote Access

- **Empire** (<https://github.com/EmpireProject/Empire>)
 - Post exploitation framework.
 - Pure-PowerShell 2.0 agent for Windows
 - Pure **Python 2.6 / 2.7** agent for Linux / OS X
- **SILENTTRINITY** (<https://github.com/byt3bl33d3r/SILENTTRINITY>)
 - Asynchronous collaborative post-exploitation agent.
 - Python and .NET DLR

Exploitation

- Web application?
- Web service?
- Network services?
- Cloud environment?

- **Pacu** (<https://github.com/RhinoSecurityLabs/pacu>)
 - AWS exploitation framework
- **AWS Pwn** (https://github.com/dagrz/aws_pwn)
 - Collection of AWS penetration testing scripts

- **CrackMapExec** (<https://github.com/byt3bl33d3r/CrackMapExec>)
 - Map SMB network, crack credentials, and execute command.
- **DeathStar** (<https://github.com/byt3bl33d3r/DeathStar>)
 - Using Empire's RESTful API to automate gaining Domain Admin in Active Directory.
- **Responder** (<https://github.com/SpiderLabs/Responder>)
 - LLMNR, NBT-NS, MDNS poisoner
 - Built-in HTTP/SMB/MSSQL/FTP/LFAP rogue authentication server.
 - Answer queries to specific names

- **Winpayloads** (<https://github.com/nccgroup/Winpayloads>)
 - Undetectable windows payload generation.
- **Cloak** (<https://github.com/s0md3v/Cloak>)
 - Python backdoor framework
 - Generate payload and inject into python scripts.

Data Exfiltration

- **PyExfil** (<https://github.com/ytisf/PyExfil>)
 - Python package for data exfiltration.

Miscellaneous

- **RedELK** (<https://github.com/outflanknl/RedELK>)
 - Red-Team's SIEM tool for tracking and alarming Blue Team activities.

Miscellaneous

- Debugging
 - ImmunityDbg + [mona.py](#)
- Binary Analysis
 - [Angr](https://github.com/angr/angr) (<https://github.com/angr/angr>)



ASK
A
QUESTION



FINALLY



MITRA INTEGRASI INFORMATIKA

Cyber Sec

Thank You

-  Satria Ady Pradana
-  +62 89 774 239 35
-  Satria.Pradana@mii.co.id
-  @xathrya (telegram)