

# People Information Gathering with the Social Engineering Toolkit (SET)

---



**Rishalin Pillay**

OFFENSIVE CYBER SECURITY AUTHOR & SPECIALIST

@r1shal1n







**Creator: David Kennedy (ReL1K) @HackingDave**

<https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/>

---

**Open source penetration testing framework designed for social engineering. Encompasses built-in attacks which are designed to be focused on a person or organization.**





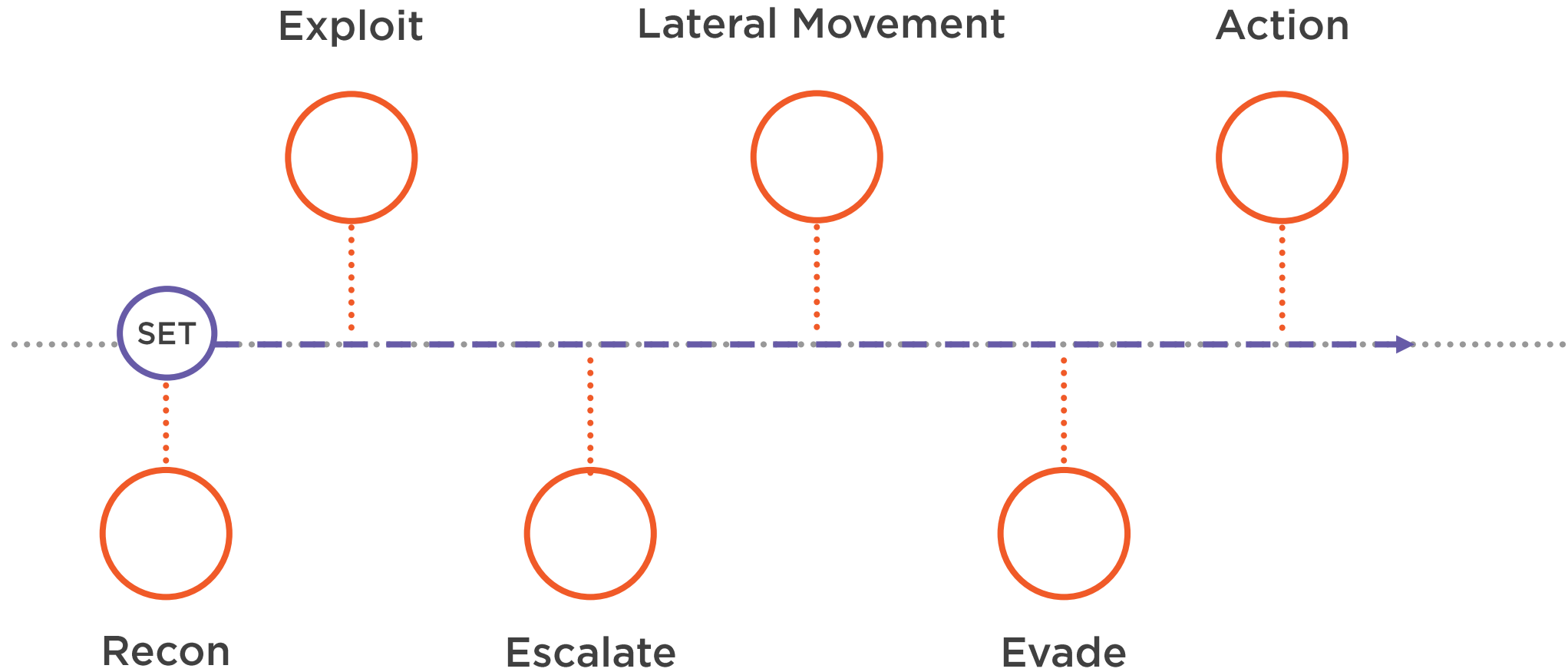
Open source tool

MacOS, Linux, Windows 10 (WSL)

Multiple attack vectors

- Spear-Phishing attacks
- Website attacks
- Infectious media creation
- And more..

# Kill Chain



# MITRE PRE-ATT&CK

## Tactics

Technical Information Gathering  
People Information Gathering  
Organizational Information Gathering  
Technical Weakness Identification  
People Weakness Identification  
Organization Weakness Identification  
Adversary Opsec  
Establish and Maintain Infrastructure  
Persona Development  
Build Capabilities  
Test Capabilities  
Stage Capabilities



# MITRE PRE-ATT&CK

## Tactics

### Technical Information Gathering

People Information Gathering

Organizational Information Gathering

Technical Weakness Identification

People Weakness Identification

Organization Weakness Identification

Adversary Opsec

Establish and Maintain Infrastructure

Persona Development

Build Capabilities

Test Capabilities

Stage Capabilities

T1249:

Conduct Social Engineering

T1397:

Spearphishing for  
information



# MITRE PRE-ATT&CK

## Tactics

Technical Information Gathering

**People Information Gathering**

Organizational Information Gathering

Technical Weakness Identification

People Weakness Identification

Organization Weakness Identification

Adversary Opsec

Establish and Maintain Infrastructure

Persona Development

Build Capabilities

Test Capabilities

Stage Capabilities

T1268:

Conduct Social Engineering





Kali Linux 2020.2

Up to date:

`apt-get update`

`apt-get upgrade`



# Social Engineering Attacks

**Spearphishing Attacks**

**Website Attacks**

**Infectious Media Attacks**

**Wireless AP Attacks**

**Powershell Attacks**

**..and more**



# Demo



## Spearphishing attack



# Demo



## Credential Harvesting attack



# Demo



**Infectious Media attack**

**QR Code attack**



# Demo



## Google Analytics attack



# More Information

## Documentation

SET User Manual

<https://github.com/trustedsec/social-engineer-toolkit>

## Related Information

Learn Penetration Testing

Chapter 4: Mastering Social Engineering

<https://amzn.to/3frIPCn>



# Thank you!



**Rishalin Pillay**  
Cybersecurity Author &  
Specialist

