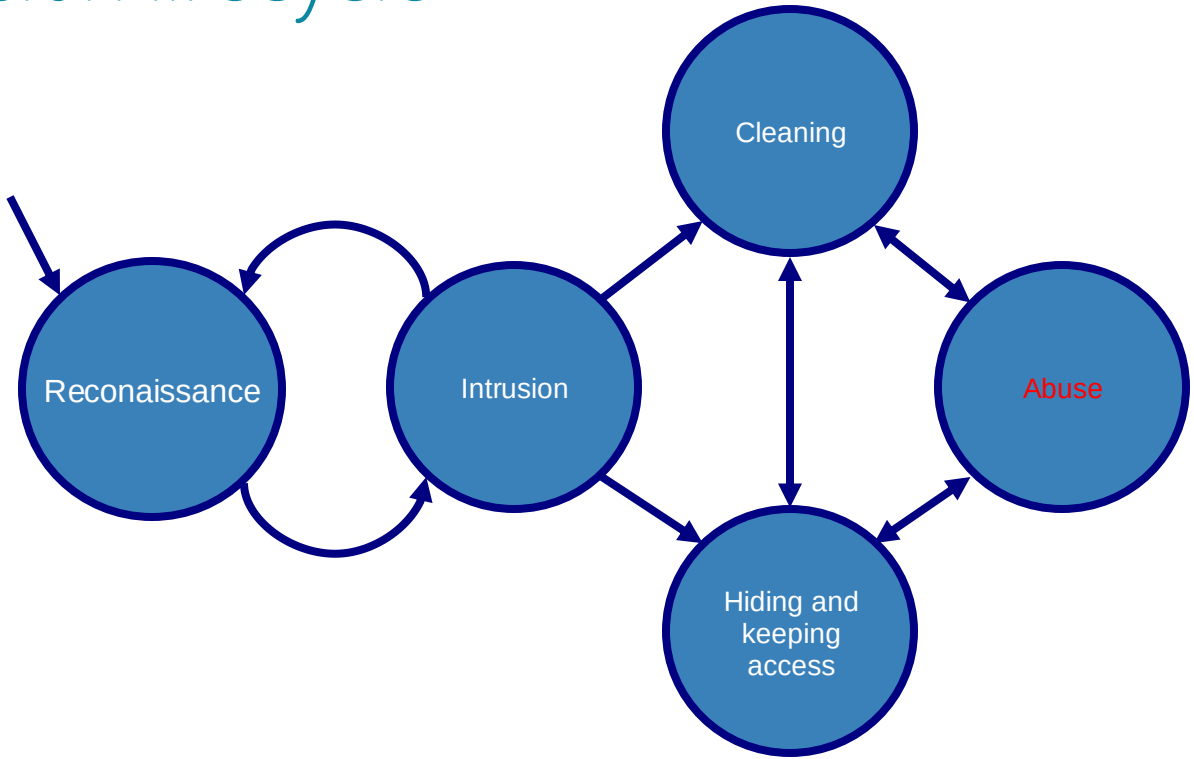
Malware Analysis

Malware (lab 3)

Intrusion lifecycle



Principles

1. To determine which operating system is to be attacked.
2. To decide how you want to distribute the virus.
3. To find the weak point that you want to attack.
4. To decide what you want the virus to do.
5. To choose a language
6. To write the code using polymorphic methodology, encrypt and obfuscate the code, etc.
7. To test the malware
8. To distribute the code

Exercices

Choose one of them

Exercice 1. Definition

- Write malware for Android 8.1.0 or python
- Make a small report

1. Estructura informe
2. Introducción
2.1 Alcance
2.2 Planificación
3. Consideraciones generales
3.1 Metodología
3.2 Software y Hardware usado
4. DESARROLLO (todo justificado)
4.1 Vulnerabilidad usada
4.2 Funcionalidades
4.3 Envio a servidor
5. Concluisiones (claras y concisas)

Exercice 2. Definition

- Analyze malware
- Make a report

1. Estructura informe
2. Introducción
2.1 Alcance
2.2 Planificación
3. Consideraciones generales
3.1 Metodología
3.2 Software y Hardware usado
4. Análisis (todo justificado)
4.1 Funcionalidades
4.2 Información que envia
4.3 Tráfico enviado (IP a donde se conecta, tramas)
5. Concluisiones (claras y concisas)

Planning

- Dec 22th december (delivery) after 20% ▼

Software

- CASE 1:

Android Studio or python

- CASE 2:

VirusTotal , Jadx1, Whois, Genymotion: application for Android emulation , Android Studio, Wireshark, PCAPdroid, Node.

THANKS!

Any questions?

You can find me at:

@jlrivas

jlrivas@det.uvigo.es

CREDITS

- Presentation template by SlidesCarnival
- Photographs by Unsplash