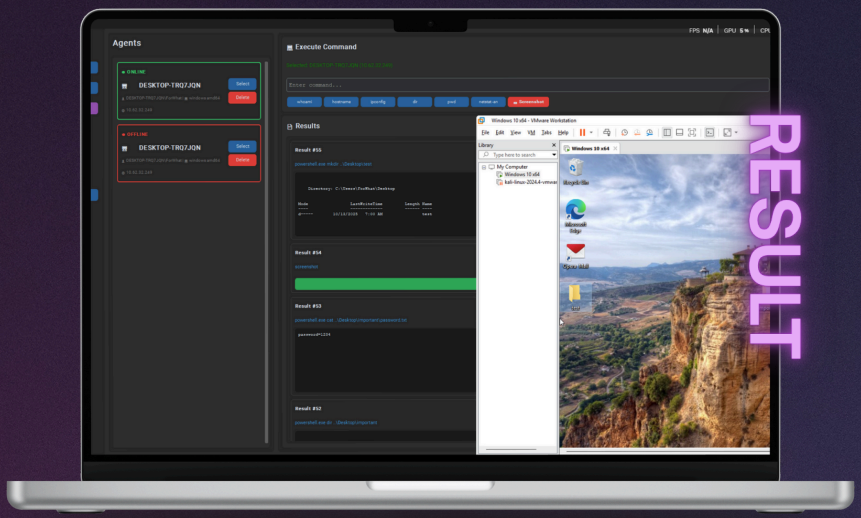
CP422011 SEC.1
INTRODUCTION TO
COMPUTER NETWORKING

chakchai so-in
Phet Imtongkhum

AustenC2

What is AustenC2 ?

AustenC2 เป็นตัวอย่างเครื่องมือ C2 (Command & Control) ที่แสดงให้เห็นว่าการรันโปรแกรมบางชนิดอาจเปิดช่องให้ผู้โจมตีสั่งงานเครื่องจากระยะไกล



หลักการและเหตุผล

- **Attack** มัลแวร์ที่สามารถควบคุมเครื่อง (RATs / botnets) สร้างความเสี่ยงต่อความมั่นคงและความต่อเนื่องของระบบ
- **Learning** เพื่อเข้าใจช่องทางการโจมตี ผลกระทบ และพัฒนามาตรการป้องกันที่เหมาะสม
- **Protect** เสนอวิธีป้องกันและแผนรับมือเมื่อเกิดเหตุ

วัตถุประสงค์

- เข้าใจประเภทและการทำงานของมัลแวร์ควบคุมเครื่อง
- วิเคราะห์ช่องทางแพร่กระจายและช่องโหว่ในเครือข่าย
- เสนอวิธีป้องกันและแผนรับมือเมื่อเกิดเหตุ
- สาธิตแนวคิดในสภาพแวดล้อมที่ปลอดภัย (VM หรือวิดีโอ)

HOW TO USE OUR PRODUCT?

1. ติดตั้ง golang และ python
2. ติดตั้ง dependencies ที่ต้องใช้ใน project
3. start server ด้วยคำสั่ง python server.py
4. start Austen ด้วย python austen.py
5. Build Agent
6. Agent delivery ด้วย Web-based app.py
7. เมื่อเหยื่อรันไฟล์ agent รอรับ request จากเหยื่อ

References

- howto.thec2matrix.com
- the-beginners-guide-to-command-and-control-part-1-how-c2-frameworks-operate
- AdaptixC2
- 0xrick.github.io/misc/c2
- mitre attack | TA0011

เครื่องมือและซอฟต์แวร์ที่ใช้

GO Python CustomTkinter

github.com/AustenC2

SECTION 1
GROUP 3

MEMBER

Kittithat Sihawong	673380147-4
Phanukon Kaeokan	673380179-1
Napassakorn marasri	673380165-2
Tanadol Langputeh	673380008-8
Chanachai Rachawong	673380155-5
Suphawong Saiprasert	673380189-8