ESIROI
ÉCOLE D'INGÉNIEURS
UNIVERSITÉ DE LA RÉUNION

DEPARTMENT : *IT*
SEMESTER : *S8*

IDENTIFICATION

Course code :	ESI-SPI-CI-IN4-S8-UE4-EC1
ECTS :	1

DURATION

Lectures :	4
Tutorial classes :	8
Labs :	12
Total :	24

Project :
Personnal work :

ASSESSMENT

Continuous assessments and evaluated practical work.

TEACHING MATERIALS

Slides, guided and practical work sheets.

LANGUAGE

English

CONTACT

Tahiry RAZAFINDRALAMBO
tahiry.razafindralambo@univ-reunion.fr

Modifié le : 14 juillet 2026

UE : UE8-CYBER

COURSE : Cybersecurity : Exfiltration, Evasion and Malware

SCOPE OF THE COURSE

OBJECTIVES

Understand offensive mechanisms of data exfiltration, evasion of defenses, and malware operation to enable malware analysis, detection of suspicious behaviors, and strengthening of an information system's defensive posture.

COMPETENCE AND SKILLS

- Statically and dynamically analyze malware to understand its behavior and indicators of compromise
- Identify and counter data exfiltration techniques (hidden channels, DNS tunneling, C2) and evasion of detection mechanisms
- Design, develop, and implement mechanisms to protect data, software, networks, and cloud environments
- Select and administer tools for detecting and correlating security incidents in response to malware threats
- Write a technical analysis report in French and English, including indicators of compromise (IoC) and remediation recommendations

PROGRAM

- **Malware taxonomy :** viruses, worms, Trojans, ransomware, spyware, rootkits, bootkits — infection and propagation mechanisms
- **Data exfiltration techniques :** hidden channels, DNS tunneling, exfiltration via HTTP/HTTPS, command and control (C2) protocols, *beaconing*
- **Defense evasion techniques :** obfuscation, *packing*, payload encryption, antivirus and EDR bypass, *living off the land* (LOLBins)
- **Static malware analysis :** metadata extraction, disassembly (Ghidra, IDA Free), string extraction, analysis of imports/exports
- **Dynamic malware analysis :** sandboxing, system call monitoring, network analysis (Wireshark, FakeNet-NG), *hooking*
- **Countermeasures and remediation :** containment, eradication, restoration, system hardening, threat intelligence
- **Report writing :** structure, IoC, criticality scoring, technical and organizational recommendations

BIBLIOGRAPHY

- Michael Sikorski & Andrew Honig - *Practical Malware Analysis* - No Starch Press, 2012
- Chris Eagle - *The IDA Pro Book* - No Starch Press, 2^(nd) ed., 2011
- Bruce Dang et al. - *Practical Reverse Engineering* - Wiley, 2014
- Solange Ghernaouti - *Sécurité informatique et réseaux* - Éditions Dunod
- MITRE ATT&CK - Exfiltration and evasion tactics : `https://attack.mitre.org`
- ANY.RUN - Dynamic analysis sandbox : `https://any.run`
- VirusTotal - File and URL analysis : `https://www.virustotal.com`

— MalwareBazaar - Malware sample database : `https://bazaar.abuse.ch`
— ANSSI - Guides and recommendations : `https://www.ssi.gouv.fr/guide/`
— NIST SP 800-83 - *Guide to Malware Incident Prevention and Handling* : `https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final`

REQUIREMENTS

— **SEC502 - Cybersecurity : Principles, Practices and Threats :** CIA model, threat classification, malware introduction and defenses
— **SEC602 - Cryptography and Applications :** encryption, PKI, TLS/SSL — necessary to understand obfuscation techniques and encrypted C2 channels
— **SEC702 - Cybersecurity : Offensive Security Methodologies :** pentest phases, vulnerability exploitation, post-exploitation — direct basis for understanding malicious behaviors
— **SEC701 - Secure Architecture and Infrastructure :** networks, firewalls, DMZ, segmentation — essential for analyzing malicious communications
— **SYSRES 501 - Network and IoT Principles :** TCP/IP protocols, DNS, HTTP — essential for analyzing malicious network traffic
— **SYSRES 502 - Operating Systems and Command Languages :** Linux/Windows administration, processes, registry, file systems — foundation for behavioral analysis
— **Expected cross-disciplinary skills :**

  — Linux terminal and Windows environment proficiency
  — Scripting basics (Bash, Python)
  — Ability to read technical documentation in English
  — Use of virtual machines and isolated environments