DANH SÁCH CÂU HỎI ÔN TẬP

MÔN HỌC: CƠ CHẾ HOẠT ĐỘNG CỦA MÃ ĐỘC – NT230

Ngày cập nhật: 10.06.2024

---

1. Phân biệt virus, sâu máy tính (worm), botnet, ransomware, eastern egg, salami attack, backdoor, rootkit, logic bomb, time-bomb, trojan.
2. Trình bày sự khác biệt giữa packer, cryptor và protector trong ngữ cảnh sử dụng của các phần mềm độc hại.
3. Kỹ thuật tiêm tiến trình là gì? Kỹ thuật tấn công mã độc thông qua tiến trình ma (Process Hollowing) được mã độc dùng cho mục đích gì? Nêu nguyên tắc thực hiện?
4. Kỹ thuật song trùng tiến trình (Process Doppelgänging) là gì? Nêu các nguyên lý, cách thức thực hiện trong việc lây nhiễm mã độc trên máy tính.
5. Nêu khái niệm và trình bày sự khác biệt giữa dropper và downloader trong ngữ cảnh hoạt động của các chương trình độc hại. Nhận xét về tác động gây hai của hai loại này và phương pháp phòng chống đối với vấn đề an toàn bảo mật thông tin.
6. Trong bối cảnh của các chương trình độc hại, nêu các rủi ro về bảo mật và quyền riêng tư đối với các tài liệu Microsoft Office. Trình bày cách tin tặc thực hiện tấn công mã độc thông qua các dạng tài liệu Microsoft Office.
7. Thuật ngữ Process Injection (tiêm tiến trình) dùng cho mục đích gì? Nêu tên và giải thích nguyên tắc thực hiện của 03 kỹ thuật phổ biến của Process Injection?
8. EPO virus là gì? Đặc điểm, mục đích của EPO virus. Nó bao gồm những loại nào? Trình bày chi tiết nguyên tắc của trường hợp TLS-EPO virus.
9. Trình bày mục đích của các phương pháp tạo mã độc đột biến, cho biết sự khác nhau giữa các chiến lược tạo biến thể mã độc?
10. Trình bày cấu trúc tập tin PDF, các chiến lược chèn các đoạn mã độc hại vào tập tin PDF và khả năng tấn công trên các loại kỹ thuật này.
11. Kỹ thuật Environmental Keying là gì? Nó khác gì với kỹ thuật Environmental Sensivity? Trình bày mục đích và các kỹ thuật thực hiện trong các chương trình phần mềm chứa mã độc hại?
12. Trình bày các kỹ thuật chống phân tích động trong các chương trình độc hại.
13. Để chống phân tích tĩnh, chương trình mã độc sử dụng những chiến lược nào trong mã nguồn của nó?
14. Phân biệt thuật ngữ Ransomware as a Service (RaaS) so với Ransomware? Chúng có những loại chính nào?

Gợi ý:

Easter eggs and salami attacks – what has your code eaten? | Nixu Cybersecurity.

ASVS/0x18-V10-Malicious.md at master · OWASP/ASVS · GitHub