# **Ubuntu 20.04**

#include <stdio.h> #include <stdlib.h> #include <unistd.h> int main(){

while (1){

fork();

system("ps -e| wc -l >> process.txt"); system("sleep 2");

}

return 0;

}

Команда ps -e выведет все процессы, включая те, которые не привязаны к текущему терминалу.

Команда wc -l подсчитает количество строк в выводе первой команды.

Цикл while будет выполняться бесконечно.(Vòng lặp while sẽ lặp vô hạn.)

Функция fork() создаст дочерний процесс.(Hàm fork() sẽ tạo ra một tiến trình con.)

Функция system() выполнит системную команду. В этом случае необходимо выполнить команду ps -aux | wc -l >> процесс.txt. Эта команда подсчитает количество запущенных процессов и запишет результаты в файл process.txt.

Hàm system() sẽ thực thi một lệnh hệ thống. Trong trường hợp này, lệnh được thực thi là ps -aux | wc -l >> process.txt. Lệnh này sẽ đếm số lượng tiến trình đang chạy và ghi kết quả vào file process.txt.

Функция Sleep() приостановит текущий процесс на 2 секунды. Hàm sleep() sẽ tạm dừng tiến trình hiện tại trong 2 giây.

gcc fork.c -o fork : используется для компиляции программ на языке C (и других языках).

./fork : это команда для запуска исполняемого файла, созданного на предыдущем шаге

# **Windows 10**

@echo off

:start

rem Запускает текущую программу с теми же параметрами.

start %0 %0

rem выводит список всех запущенных процессов

tasklist | find /v /n /c ""

rem Запишите результаты в файл C:\process\output.txt.

echo. > C:\process\output.txt

tasklist | find /v /n /c "" >> C:\process\output.txt

rem Возврат к исходной точке

goto start

Это язык Batch программирования, язык программирования, используемый для создания файлов сценариев, которые могут выполняться в операционных системах Windows. Эти файлы обычно имеют расширение \*.bat или \*.cmd.

Đây là ngôn ngữ lập trình Batch, một ngôn ngữ lập trình được sử dụng để tạo các tập tin kịch bản có thể thực thi trên hệ điều hành Windows. Các tập tin này thường có đuôi \*.bat hoặc \*.cmd.

Код работает следующим образом:

Эта программа работает следующим образом:

Строка @echo off отключает вывод сообщений на экран.

Строка :start определяет точку перехода.

Строка start %0 %0 запускает текущую программу с теми же параметрами.

Строка tasklist | find /v /n /c "" перечисляет все запущенные процессы.

Строка echo. > C:\process\output.txt удаляет содержимое файла C:\process\output.txt.

Строка tasklist | find /v /n /c "" >> C:\process\output.txt записывает результаты команды списка задач в файл C:\process\output.txt.

строка goto start перехода в начальную точку.

Chương trình này hoạt động như sau:

* Dòng @echo off tắt thông báo xuất ra màn hình.
* Dòng :start định nghĩa một điểm nhảy.
* Dòng start %0 %0 khởi chạy chương trình hiện tại với các tham số giống nhau.
* Dòng tasklist | find /v /n /c "" liệt kê tất cả các tiến trình đang chạy.
* Dòng echo. > C:\process\output.txt xóa nội dung của tệp C:\process\output.txt.
* Dòng tasklist | find /v /n /c "" >> C:\process\output.txt ghi kết quả của lệnh tasklist vào tệp C:\process\output.txt.
* Dòng goto start quay lại điểm bắt đầu.

Результатом работы этой программы будет файл C:\process\output.txt, содержащий список всех запущенных процессов. Kết quả của chương trình này sẽ là một file C:\process\output.txt chứa danh sách tất cả các tiến trình đang chạy.

Sau khi thực hiện lab này, làm thế nào đẻ bảo vệ máy tính khỏi những chương trình như vậy?

В Windows включите брандмауэр, не загружайте приложения со странными расширениями типа .bat, перед запуском любой программы неизвестного происхождения сначала запускайте ее на виртуальной машине.

При написании программы помните условия, избегайте случаев бесконечного выполнения, родительская программа и дочерние программы приводят к тому, что программа съедает всю память и приводит к выходу компьютера из строя.

Forkbomb — это атака типа **«отказ в обслуживании»**, при которой процесс постоянно воспроизводит себя, чтобы **истощить доступные системные ресурсы, замедляя или приводя к сбою системы** из-за нехватки ресурсов.

Forkbomb là một loại phần mềm độc hại hoặc tấn công vào hệ thống máy tính nhằm mục đích làm cạn kiệt tài nguyên hệ thống, dẫn đến việc từ chối dịch vụ. Forkbomb tạo ra nhiều tiến trình con, từ đó sinh ra nhiều tiến trình hơn cho đến khi tất cả các tài nguyên có sẵn, chẳng hạn như RAM và thời gian CPU, cạn kiệt.

Компьютерная программа, намеренно или из-за ошибки в коде создающая бесконечные копии, которые тоже могут начать бесконтрольно размножаться. Названа по имени функции fork(), присутствующей во многих языках программирования

Một chương trình máy tính cố ý hoặc do lỗi mã tạo ra vô số bản sao, bản sao này cũng có thể bắt đầu nhân lên một cách không kiểm soát. Được đặt tên theo hàm fork(), có mặt trong nhiều ngôn ngữ lập trình.

Membomb (Memory Bomb) — это атака или программа, направленная на истощение **оперативной памяти компьютера** (RAM), что приводит к снижению производительности или полному зависанию системы. В отличие от форкбомб, которая порождает процессы для исчерпания процессорных ресурсов, мембомба сосредоточена на создании или заполнении памяти так, чтобы все доступные ресурсы оперативной памяти оказались заняты.

Membomb (Memory Bomb) là một cuộc tấn công hoặc chương trình nhằm làm cạn kiệt bộ nhớ truy cập ngẫu nhiên (RAM) của máy tính, dẫn đến hiệu suất kém hoặc đóng băng toàn bộ hệ thống. Không giống như forkbomb, tạo ra các tiến trình làm cạn kiệt tài nguyên CPU, membomb tập trung vào việc tạo hoặc lấp đầy bộ nhớ để tất cả tài nguyên RAM có sẵn đều bị chiếm dụng.

После открытия файла forkbomb нагрузка на ЦП резко возрастает, поскольку система вынуждена создавать и управлять слишком большим количеством процессов за короткий период времени, что приводит к высокой загрузке ЦП и, возможно, к сбою.

sau khi mở file forkbomb, CPU tăng đột biến vì hệ thống đang bị ép phải tạo và quản lý quá nhiều tiến trình trong một thời gian ngắn, gây ra tình trạng sử dụng CPU cao và có thể dẫn đến treo máy.

Как защитить компьютер от этого?

Ограничение количества процессов:

Ограничение прав пользователей:

Мониторинг и завершение процессов:

Использование антивирусов и систем безопасности:

Làm thế nào để bảo vệ máy tính của bạn khỏi điều này?

Giới hạn số lượng tiến trình:

Hạn chế quyền của người dùng:

Giám sát và tắt các quy trình:

Sử dụng hệ thống chống virus và bảo mật:

Sự khác nhau của đồ thị forkbomb giữa linux và windows: do kiến trúc hệ điều hành và cách quản lý tiến trình của mỗi hệ thống.

Различия в графике работы **fork bomb** на Linux и Windows обусловлены архитектурой операционных систем и методами управления процессами в каждой системе.

1. **Управление процессами**:

+)linux

График количества процессов на Linux будет иметь форму **экспоненциального роста**, так как fork() постоянно порождает дочерние процессы, и каждый из этих процессов может вызывать fork(), что быстро увеличивает число процессов.

Когда количество процессов превышает лимит, система начнет отклонять новые запросы на создание процессов, и в конечном итоге это приведет к блокировке системы из-за нехватки ресурсов.

Đồ thị thể hiện số lượng tiến trình trên Linux sẽ có dạng tăng theo cấp số nhân do fork() liên tục tạo ra nhiều tiến trình con, và mỗi tiến trình con lại có thể gọi fork(), làm tăng nhanh số lượng tiến trình.

Khi số lượng tiến trình vượt quá giới hạn, hệ thống có thể bắt đầu từ chối các lệnh tạo tiến trình mới và cuối cùng sẽ bị "nghẽn" khi đạt giới hạn tài nguyên.

+) windows

Создание нового процесса в Windows требует больше ресурсов и времени, чем в Linux. Следовательно, fork bomb на Windows увеличивает количество процессов медленнее.

Windows также имеет более строгие механизмы защиты системы, что может привести к тому, что график количества процессов **растет медленнее и стабилизируется** быстрее, чем в Linux.

Tạo một tiến trình mới trên Windows tốn tài nguyên và thời gian hơn so với Linux. Do đó, fork bomb trên Windows có thể tăng tiến trình chậm hơn.

Windows cũng có các cơ chế bảo vệ hệ thống mạnh mẽ hơn (ví dụ: **Job Objects** và giới hạn tài nguyên cho tiến trình) để ngăn chặn số lượng tiến trình vượt quá một giới hạn nào đó. Điều này có thể khiến đồ thị số lượng tiến trình của fork bomb trên Windows **tăng chậm hơn và có xu hướng ổn định sớm hơn** so với Linux.

**2) Механизмы защиты операционной системы**

**+) linux**

Хотя Linux может быть уязвим для fork bomb без соответствующих защит, большинство современных версий Linux имеют встроенные механизмы защиты, такие как ограничение количества процессов для каждого пользователя и системы мониторинга, которые могут остановить fork bomb до того, как система будет полностью перегружена.

Mặc dù Linux có thể dễ bị ảnh hưởng bởi fork bomb nếu không có biện pháp bảo vệ trước, nhưng hầu hết các phiên bản hiện đại của Linux có cơ chế bảo vệ như giới hạn số tiến trình cho mỗi người dùng và các công cụ giám sát hệ thống để dừng fork bomb trước khi hệ thống bị quá tải hoàn toàn.

**+) windows**

В Windows существуют более строгие механизмы защиты процессов. Кроме того, современные версии Windows способны обнаруживать и предотвращать подозрительное поведение, такое как fork bomb.

Windows có các cơ chế bảo vệ tiến trình chặt chẽ hơn. Ngoài ra, các phiên bản Windows hiện đại cũng có khả năng phát hiện và ngăn chặn hành vi bất thường, bao gồm cả fork bomb.