Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

Факультет безопасности информационных технологий

Дисциплина:

«Операционные систеимы»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

«Forkbomb»

Выполнил:

студент группы N3246,

Бардышев Артём Антонович

(подпись)

Проверил: Савков Сергей Витальевич,

(отметка о выполнении)

(подпись)

Санкт-Петербург

2024г.

Реакция Windows на Форкбомбу:

1) Замедление системы: Форкбомба создает множество процессов, что приводит к сильной нагрузке на процессор и оперативную память. Это замедляет работу системы, делает её неотзывчивой.
2) Замораживание системы: Если ресурсы системы полностью исчерпаны, она может "заморозиться", перестать реагировать на ввод с клавиатуры и мыши. В таких случаях поможет только перезагрузка.
3) Защита от отказа в обслуживании: Современные версии Windows имеют встроенные механизмы для предотвращения подобных атак, например, с помощью системы контроля ресурсов (Resource Control System). Она может ограничить количество создаваемых процессов для одного пользователя или программы, что может уменьшить эффективность форкбомбы.
4) Перезагрузка системы: В некоторых случаях, если системные ресурсы полностью исчерпаны, может понадобиться принудительная перезагрузка через физическое отключение питания или аппаратную перезагрузку.

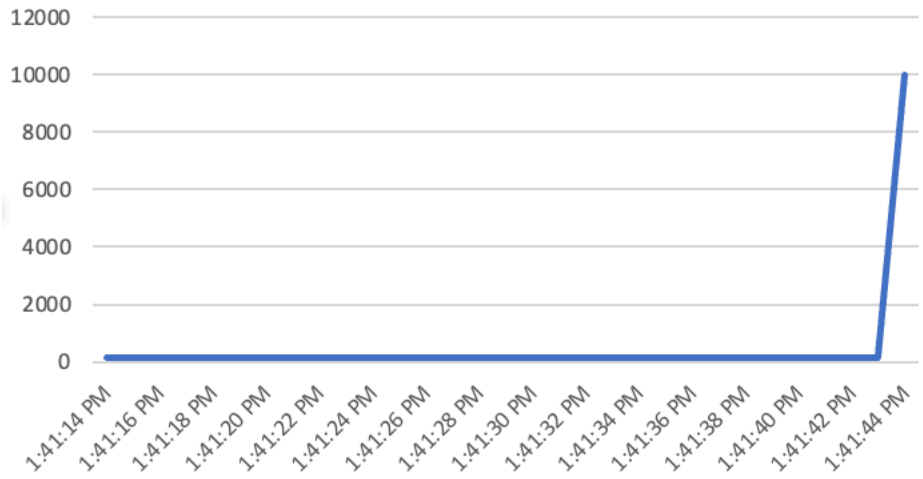
Реакция Linux на Форкбомбу:

1) Захват всех ресурсов: Форкбомба создает множество дочерних процессов, каждый из которых пытается захватить ресурсы (CPU, память). В итоге система становится очень медленной и может перестать реагировать на команды. Это проявляется как отказ в обслуживании (DoS).
2) Использование ulimit: В большинстве дистрибутивов Linux существует утилита ulimit, которая позволяет ограничивать количество процессов, которое может создать каждый пользователь.
3) OOM-killer: Linux включает механизм под названием OOM (Out-Of-Memory) Killer. Когда оперативная память исчерпывается, OOM-killer автоматически завершает процессы, чтобы освободить ресурсы. Форкбомба может вызвать срабатывание этого механизма, который может завершить злоумышленные процессы, но иногда завершает критически важные процессы, что может привести к краху системы.
4) Cgroups (Control Groups): Linux поддерживает механизм cgroups, который позволяет более точно управлять ресурсами на уровне групп процессов. Администраторы могут ограничивать использование CPU, памяти и количество процессов для определенных пользователей или приложений. Это эффективный способ защиты от форкбомб и других атак на ресурсы.
5) Перезагрузка системы: В случае, если механизмы защиты не настроены или не работают эффективно, форкбомба может потребовать физической перезагрузки системы, так как интерфейс может полностью перестать отвечать.

Linux:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat fork.c
#include<stdio.h>
#include<unistd.h> //for fork
#include<stdlib.h> //for system

int main(){
while(1){
fork();
system("ps -e | wc -l >> count.txt");
}
return 0;
}
```



Windows:
Forkbomb:

```
$MaxCount = 9
$Count = 0
while ($Count -lt $MaxCount) {
Start-Process powershell -ArgumentList "& { Start-Sleep -Seconds 0.3;

Start-Process powershell -ArgumentList '& { Start-Sleep -Seconds 0.3; Start-Process powershell -ArgumentList " }' }"

$Count++
Start-Sleep -Seconds 0.3
}
```

Counter:

```
$outputFile = "process_count.txt"
"Time,Count_processes" | Out-File -FilePath $outputFile -Encoding utf8
$startTime = Get-Date
while ($true) {
$currentTime = Get-Date -Format "HH:mm:ss"
$processCount = (Get-Process).Count
"$currentTime,$processCount" | Out-File -FilePath $outputFile -Append -Encoding utf8
$elapsedTime = (Get-Date) - $startTime
if ($elapsedTime.TotalSeconds -ge 60) {
break
}
```

```
Start-Sleep -Seconds 1
}
```