Họ tên: Trần Trí Dũng

MSSV: HE190680

Lớp: IA1901

10.1 – Scanning kernel parameters with Lynis.

kernel.dmesg\_restrict = 1

* Hạn chế quyền truy cập vào kernel log (dmesg) chỉ cho người dùng root
* Ngăn người dùng thông thường xem các thông tin nhạy cảm trong log kernel

kernel.kptr\_restrict = 2

* Ẩn các kernel pointer trong /proc và các interface khác
* Tăng cường bảo mật bằng cách ngăn leak thông tin về địa chỉ bộ nhớ kernel

kernel.modules\_disabled = 1

* Vô hiệu hóa việc load module kernel
* Ngăn chặn việc load các module kernel độc hại

kernel.perf\_event\_paranoid = 3

* Hạn chế quyền truy cập vào performance events
* Ngăn việc thu thập thông tin hiệu năng hệ thống

kernel.sysrq = 0

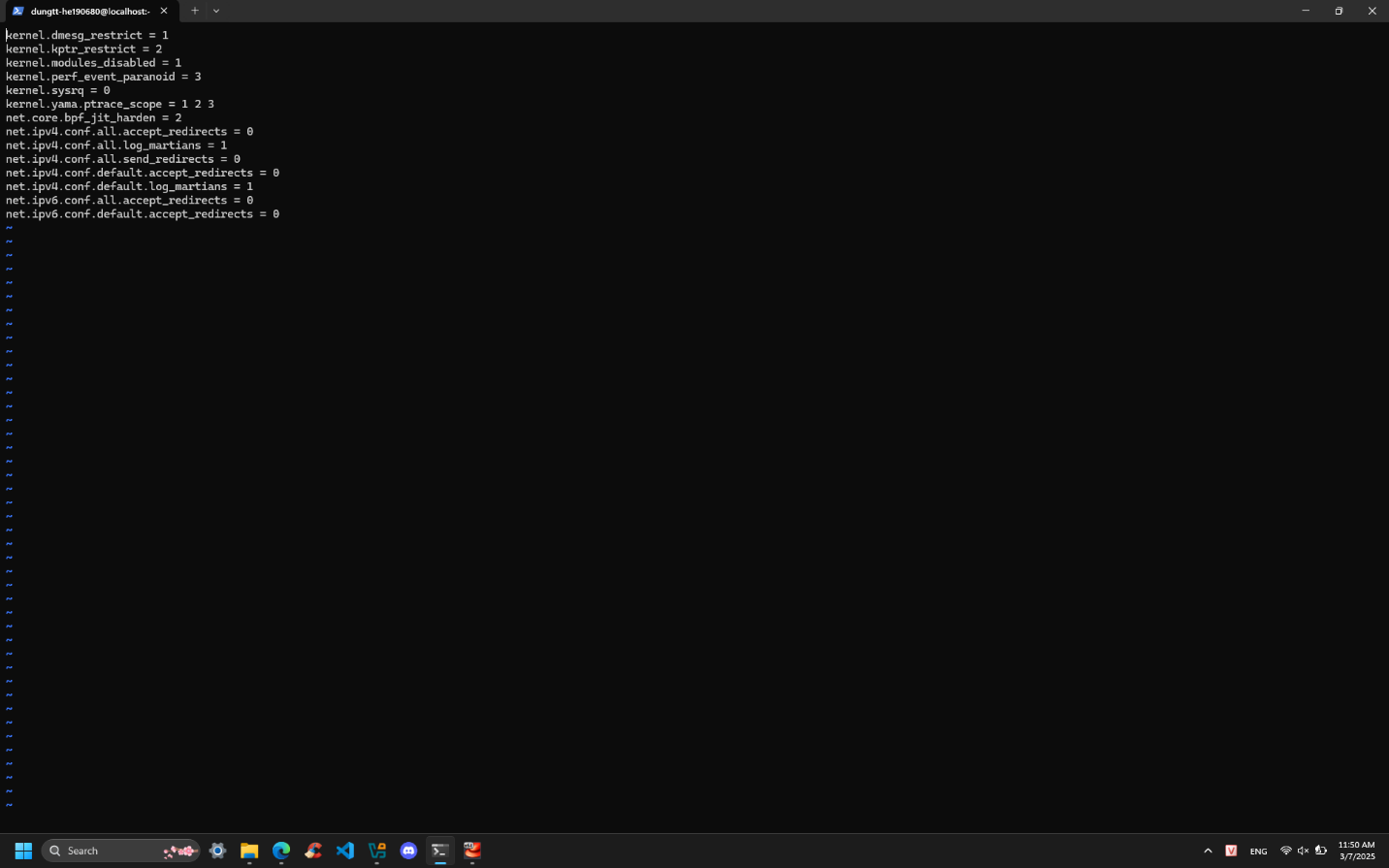
* Vô hiệu hóa SysRq key
* Ngăn việc thực thi các lệnh hệ thống nguy hiểm thông qua phím tắt

kernel.yama.ptrace\_scope = 1 2 3

* Hạn chế khả năng debug process
* Ngăn việc process này theo dõi process khác

Các thiết lập về network:

* Vô hiệu hóa việc chấp nhận ICMP redirects (ngăn tấn công MITM)
* Bật logging cho các gói tin "martian" (có địa chỉ nguồn/đích không hợp lệ)
* Áp dụng cho cả IPv4 và IPv6



10.2 – Setting a kernel capability

cap\_net\_raw: Đây là một capability cho phép chương trình:

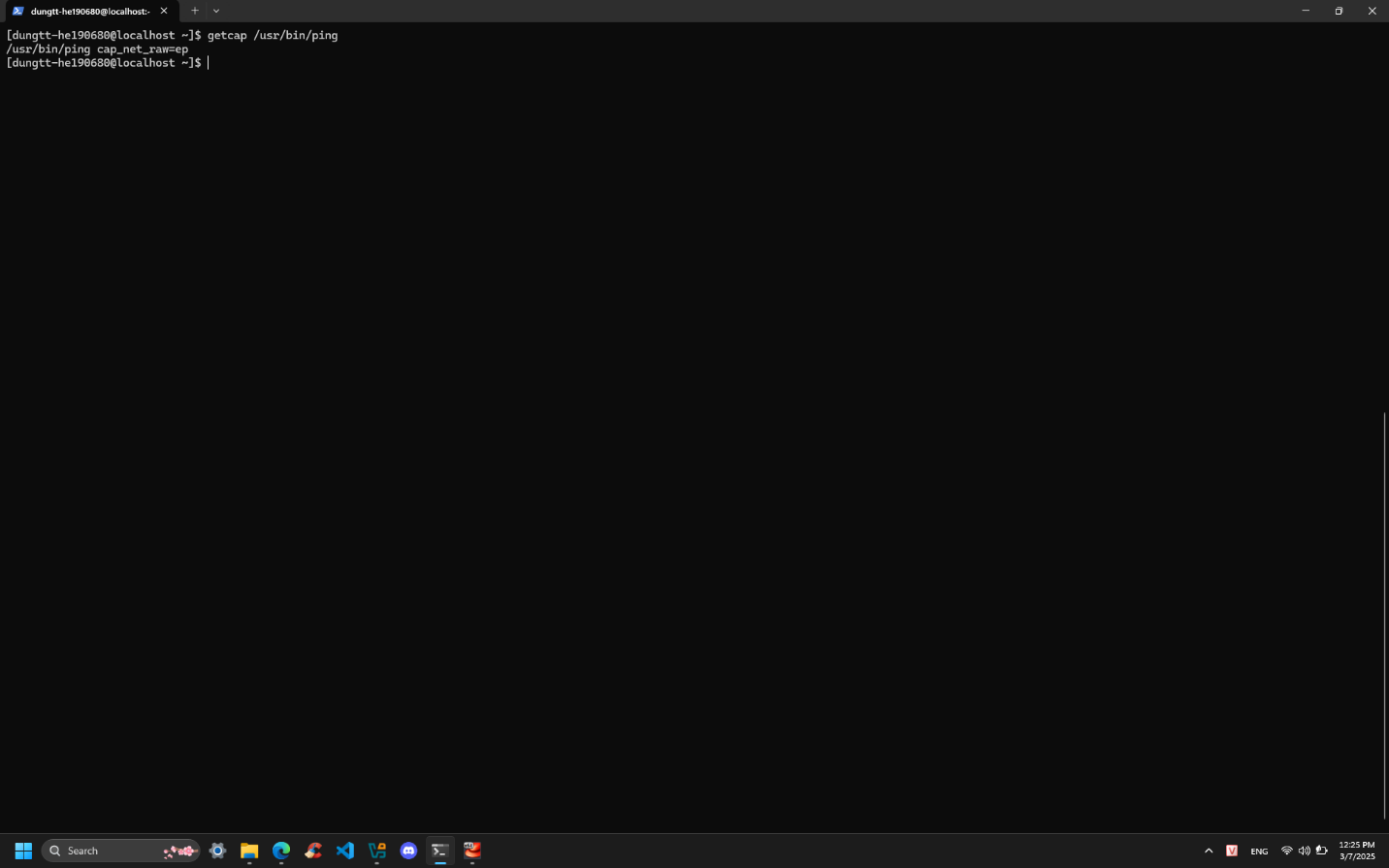
* Tạo và thao tác với các raw network sockets
* Truy cập trực tiếp vào giao thức mạng cấp thấp
* Cho phép ping gửi và nhận các gói tin ICMP (Internet Control Message Protocol)

Ký hiệu ep có ý nghĩa:

* e (Effective): capability được kích hoạt khi chương trình chạy
* p (Permitted): capability được cho phép sử dụng

Capability này rất quan trọng đối với lệnh ping vì:

* Nó cho phép ping hoạt động mà không cần quyền root
* Đảm bảo an toàn hơn vì chỉ cấp đúng quyền cần thiết (principle of least privilege)
* Người dùng thường có thể sử dụng lệnh ping mà không cần sudo



10.3 – Using Firejail

Khi chạy sudo firecfg, Firejail sẽ:

* Tạo các symbolic links trong thư mục /usr/local/bin cho tất cả các ứng dụng có thể được sandbox
* Các symbolic links này sẽ trỏ đến binary của Firejail (/usr/bin/firejail)

Khi liệt kê bằng lệnh ls -l sẽ thấy danh sách các symbolic links

Điều này có nghĩa là:

* Mỗi khi khởi động một ứng dụng từ menu Start hoặc command line, nó sẽ đi qua symbolic link này
* Symbolic link sẽ chuyển hướng việc thực thi qua Firejail
* Firejail sau đó sẽ tự động chạy ứng dụng trong môi trường sandbox

