DevOps VietNam

NMAP CHEAT SHEET

VÍ DỤ VỀ NMAP (NMAP EXAMPLES)

Mục đích	Lệnh
Phát hiện phiên bản dịch vụ và hệ điều hành	`nmap -sV -O [target]`
Phát hiện máy chủ web	`nmap -sV --script http-title [target]`
Quét 10 cổng phổ biến nhất	`nmap --top-ports 10 [target]`
Khám phá host bằng ping broadcast	`nmap --script broadcast-ping`
Lấy thông tin từ bản ghi whois	`nmap --script whois [target]`
Brute force bản ghi DNS	`nmap --script dns-brute [target]`
Quét tường lửa để phát hiện giả mạo địa chỉ MAC	`nmap -v -sT -Pn --spoof-mac 0 [target]`
Chạy tất cả script trong danh mục vuln	`nmap -sV --script vuln [target]`
Chạy script trong danh mục version hoặc discovery	`nmap -sV --script=version,discovery [target]`
Phát hiện sniffer	`nmap -sP --script sniffer-detect [target]`

QUÉT CƠ BẢN (BASIC SCANNING)

Lệnh	Mô tả
`nmap [target]`	Quét cơ bản các cổng mở trên mục tiêu
`nmap -sS [target]`	Quét SYN (nhanh, ẩn, không cần kết nối đầy đủ)
`nmap -sT [target]`	Quét TCP Connect (kết nối đầy đủ)
`nmap -sU [target]`	Quét cổng UDP
`nmap -sn [target]`	Quét ping (kiểm tra host sống, không quét cổng)

QUÉT CỔNG (PORT SCANNING)

Lệnh	Mô tả
`nmap -p [port] [target]`	Quét cổng cụ thể (ví dụ: -p 80)
`nmap -p- [target]`	Quét tất cả 65535 cổng
`nmap -F [target]`	Quét nhanh 100 cổng phổ biến nhất
`nmap --top-ports [n] [target]`	Quét [n] cổng phổ biến nhất

PHÁT HIỆN HỆ ĐIỀU HÀNH VÀ DỊCH VỤ

Lệnh	Mô tả
`nmap -O [target]`	Phát hiện hệ điều hành
`nmap -sV [target]`	Phát hiện phiên bản dịch vụ
`nmap -A [target]`	Quét toàn diện (OS, dịch vụ, script, traceroute)

TÙY CHỌN THỜI GIAN (TIMING OPTIONS)

Lệnh	Mô tả
`nmap -T0 [target]`	Quét rất chậm (ẩn tối đa)
`nmap -T4 [target]`	Quét nhanh (mặc định cho mạng tốt)
`nmap -T5 [target]`	Quét cực nhanh (có thể mất chính xác)

XUẤT KẾT QUẢ (OUTPUT OPTIONS)

Lệnh	Mô tả
`nmap -oN [file] [target]`	Lưu kết quả vào tệp dạng thường
`nmap -oX [file] [target]`	Lưu kết quả vào tệp XML
`nmap -oG [file] [target]`	Lưu kết quả vào tệp Grepable
`nmap -oA [base] [target]`	Lưu kết quả tất cả định dạng (normal, XML, Grepable)

`nmap -Pn [target]`	Bỏ qua ping, giả định tất cả host sống

TÙY CHỌN CHI TIẾT VÀ GỠ LỖI

Lệnh	Mô tả
`nmap -v [target]`	Hiển thị chi tiết quá trình quét
`nmap -vv [target]`	Hiển thị chi tiết hơn
`nmap -d [target]`	Chế độ gỡ lỗi cơ bản
`nmap -dd [target]`	Chế độ gỡ lỗi chi tiết hơn

SCRIPT NMAP (NSE)

Lệnh	Mô tả
`nmap --script [script] [target]`	Chạy script cụ thể (ví dụ: http-enum)
`nmap --script [category] [target]`	Chạy tất cả script trong danh mục (ví dụ: vuln)
`nmap --script-args [key]=[value] [target]`	Truyền tham số cho script
`nmap --script-help [script]`	Hiển thị trợ giúp cho script cụ thể
