

# nmap クイックリファレンス

ポートスキャン、ホスト探索、サービス検出、NSE スクリプト

## 基本スキャン

### スキャン対象の指定

nmap 192.168.1.1	# 単一ホスト
nmap 192.168.1.0/24	# サブネット全体
nmap 192.168.1.1-50	# IPレンジ
nmap -iL targets.txt	# ファイルからホストを読み込み

### ターゲット指定

192.168.1.1	単一 IP アドレス
192.168.1.0/24	CIDR 表記 (256 ホスト)
192.168.1.1-254	IP レンジ
example.com	ホスト名 (IP に解決)
-iL file.txt	ファイルからターゲットを読み込み
--exclude 192.168.1.1	特定のホストを除外
--excludefile skip.txt	ファイルのホストを除外

## ポートスキャン

### スキャンの種類

-sS	TCP SYN スキャン (デフォルト、ステルス、root 必要)
-sT	TCP 接続スキャン (完全ハンドシェイク、root なし)
-sU	UDP スキャン (低速、フィルタリングされやすい)
-sA	TCP ACK スキャン (ファイアウォール検出)
-sN	TCP NULL スキャン (フラグなし)
-sF	TCP FIN スキャン (FIN フラグのみ)
-sX	Xmas スキャン (FIN+PSH+URG フラグ)

### ポートの選択

nmap -p 80,443 target	# 特定のポート
nmap -p 1-1000 target	# ポートレンジ
nmap -p- target	# 全65535ポート
nmap --top-ports 100 target	# よく使われる上位100ポート

### ポートの状態

open	アプリケーションが接続を受け付けている
closed	ポートは到達可能だがサービスが待機していない
filtered	ファイアウォールがブロック、状態を判定できない
unfiltered	ポートはアクセス可能だが開/閉不明
open filtered	開いているかフィルタリングされているか不明

## ホスト探索

### 探索方法

-sn	ピングスキャンのみ (ポートスキャンなし)
-Pn	ホスト探索をスキップ (全て稼働中として扱う)
-PS 80,443	ポートへの TCP SYN 探索
-PA 80	TCP ACK 探索
-PU 53	UDP 探索
-PE	ICMP エコーリクエスト
-PR	ARP 探索 (ローカルネットワーク)

### ネットワークスイープ

nmap -sn 192.168.1.0/24	# サブネットのpingスイープ
nmap -sn -n 10.0.0.0/24	# スweep、DNS解決スキップ
nmap -sn -PR 192.168.1.0/24	# ARPスキャン (最速)

## サービス検出

### バージョン検出

nmap -sV target	# サービスバージョンを検出
nmap -sV --version-intensity 5 target	# より詳細なプローブ
nmap -sV --version-all target	# 全プローブを試行 (低速)
nmap -A target	# OS+バージョン+スクリプト+トレースルート

## サービスフラグ

-sV	開いているポートのサービス/バージョンをプローブ
--version-intensity 0-9	プローブの強度 (デフォルト 7)
--version-light	軽量プローブ (強度 2)
--version-all	全プローブを試行 (強度 9)
-A	アグレッシブ: -sV -O --script=default -traceroute
-sC	デフォルト NSE スクリプトを実行

## OS 検出

### OS フィンガープリンティング

nmap -O target	# OS検出 (root必要)
nmap -O --osscan-limit target	# 有望なホストのみスキャン
nmap -O --osscan-guess target	# アグレッシブなOS推測
nmap -A target	# OS検出を含む

### OS 検出フラグ

-O	OS 検出を有効化
--osscan-limit	開放+閉鎖 TCP ポートがないホストをスキップ
--osscan-guess	よりアグレッシブに OS を推測
--max-os-tries N	ホストあたりの OS 検出最大試行回数

## スクリプト (NSE)

### スクリプトの使用

nmap --script=default target	# defaultカテゴリ
nmap --script=vuln target	# 脆弱性スクリプト
nmap --script=http-headers target	# http-headers
nmap --script="http-*" target	# ワイルドカードマッチ

### スクリプトカテゴリ

default	安全で有用なスクリプト (-sC の省略形)
vuln	既知の脆弱性をチェック
safe	非侵襲的なスクリプト
intrusive	対象をクラッシュさせたり IDS を起動する可能性あり
discovery	ネットワークとサービスの探索
auth	認証関連のチェック
brute	ブルートフォース認証テスト
exploit	積極的な悪用の試み

### 便利なスクリプト

http-title	Web ページのタイトルを取得
ssl-cert	SSL 証明書の詳細を表示
ssh-hostkey	SSH ホストキーのフィンガープリントを表示
dns-brute	DNS サブドメインを列挙
smb-os-discovery	SMB 経由で Windows OS を検出
vuln	全脆弱性チェックを実行

## 出力フォーマット

### 出力オプション

nmap -oN scan.txt target	# 通常テキスト出力
nmap -oX scan.xml target	# XML出力
nmap -oG scan.gnmap target	# grepable出力
nmap -oA scan_all target	# 全フォーマット同時出力

## 出力フラグ

-oN file	通常出力をファイルに保存
-oX file	XML 出力 (ツール/パース用)
-oG file	Grepable 出力 (1 ホスト 1 行)
-oA basename	3 つの全フォーマット (basename.nmap/xml/gnmap)
-v	冗長度を上げる (-vv でさらに詳細)
-d	デバッグ出力 (-dd でさらに詳細)
--open	開いているポートのみ表示
--reason	ポート状態の理由を表示

## タイミングとパフォーマンス

### タイミングテンプレート

-T0 (paranoid)	非常に低速、IDS 回避 (プローブ間隔 5 分)
-T1 (sneaky)	低速、IDS 回避 (プローブ間隔 15 秒)
-T2 (polite)	低速、帯域幅を抑える
-T3 (normal)	デフォルトのタイミング
-T4 (aggressive)	高速、信頼性の高いネットワークを前提
-T5 (insane)	最速、結果を見逃す可能性あり

### 細かいチューニング

--min-rate 1000	最低 1000 パケット/秒を送信
--max-rate 500	500 パケット/秒に制限
--max-retries 2	プローブの最大再送回数
--host-timeout 30m	30 分超えたらホストをスキップ
--scan-delay 1s	プローブ間の遅延
--min-parallelism 10	最小並列プローブグループ数

## ファイアウォール回避

### 回避テクニック

-f	パケットを断片化 (8 バイトチャンク)
-D RND:5	5 つのランダム IP でデコイスキャン
-S spoof_ip	送信元 IP を偽装 (raw パケットが必要)
-e eth0	特定のネットワークインターフェースを使用
--source-port 53	特定の送信元ポートを使用 (例: DNS)
--data-length 25	パケットにランダムデータを追加
--spoof-mac 0	MAC アドレスをランダム化

### 回避の例

nmap -f -D RND:3 target	# 断片化+デコイ
nmap --source-port 53 target	# DNSポート (許可されやすい)
nmap -T1 --scan-delay 5s target	# IDS回避のため低速化

## よくあるパターン

### クイック偵察

nmap -T4 -F target	# 一般的なポートの高速スキャン
nmap -T4 -A -v target	# OS+サービス検出
nmap -sV --top-ports 1000 target	# 上位1000ポート+バージョン

### 総合スキャン

# 完全TCP+サービス+OS+スクリプト	nmap -sS -sV -O -sC -p- -T4 -oA full target
# 一般的なポートのUDPスキャン	nmap -sU --top-ports 50 target

### Web サーバー監査

nmap -p 80,443 --script=http-title,http-headers,ssl-cert,http-methods target	# オープンプロキシと脆弱性のチェック
nmap -p 80,443,8080 --script=http-open-proxy,vuln target	

# nmap クイックリファレンス

---

## ネットワークインベントリ

```
# OS情報と共に稼働ホストを探索
nmap -sn 192.168.1.0/24 -oG - | grep "Up"
# サブネットのサービスインベントリ
nmap -sV -T4 192.168.1.0/24 -oX inventory.xml
```