Nmap コマンドライン 参考シート

2013/03/20
http://www.checksite.jp/
Check!Site

- nmapコマンドラインオプションを簡単にまとめた参考シート
- 初級者向け

ホスト発見
- -sP Pingスキャン(default)
- -P0 Pingしない
- -n DNS解決しない

ポート指定/順序
- -p <port> ポート指定
- -F 高速スキャン
- -r ポート番号順

出力
- default 標準出力 (stdout)
- -oN <file> 通常出力
- -oX <file> XML出力
- -v 冗長出力

 # nmap [ホスト発見] [スキャンタイプ] [ポート指定/順序] [バージョン/OS検出] [出力] [ターゲット指定]

スキャンタイプ
- -sS TCP SYN スキャン(default)
- -sT TCP connectスキャン
- -sU UDPスキャン

バージョン/OS検出
- -sV バージョン検出
- -O OS検出
- -A バージョン検出とOS検出

ターゲット指定
- 例：192.168.0.100
- 例：192.168.0.0/24
- 例：192.168.0.1-100
- -iL <file> ファイルから読み込み

nmap -n -F -r -O 192.168.1.5
DNS解決を行わないで、高速スキャンをポート番号順に実施する。

nmap -p 1-100 -sV -oN nmap_result.log 192.168.1.10
ポート1～100 に対してスキャンを行い、開いているポートに対してバージョン検出を行い、結果をファイルに書き込む。

nmap -sS -sU 192.168.2.100-102
TCP SYN スキャン、UDPスキャンを、3つのIPアドレスに対して実施する。