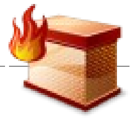
TUXCEPTION cheat-sheet

nmap basics

How it will scan	
-sA	ACK scan – it will not determine open ports, but firewall rules used.
-sF	FIN scan, sends FIN packet, can show some false-positives, but it may be not discovered by some IDS programs.
-sI	IDLE scan – bounce packet from external host – used for attacks.
-sL	DNS scan (a.k.a. list scan)
-sN	NULL scan sends FIN packet, usefull to fool a firewall. Don't use it to scan Windows – it will not understand null scan.
-sO	Protocol scan
-sP	Ping scan – it will show what servers, devices are up and running
-sR	RPC scan (Remote Procedure Call)
-sS	SYN scan -default, half-open, probably not visible in simple logs, half-open means that tcp handshake is not completed.
-sT	TCP connect scan – connection is estabilished during scan – full TCP handshake. It is noisy.
-sW	Windows scan
-sX	XMAS scan, sends FIN packet, but all flags will be enabled. Windows machine will not respond to this.
-sZ	SCTP scan – silent and effective, not so eassy to discover by IDS.

What will be scanned	
-iL [file]	Scan hosts listed in file
--exclude [ip] --excludefile [file]	Exclude one ip Exclude hosts listed in file
nmap -sL [targets]	Create host list
Nmap 192.168.0.101,102	scan multiple host with different last octet of ip
--script-help "ssh-*"	Get help.

Scripts	
-sC	Run all default scripts, safe scripts.
A, auth, default, discovery, external, intrusive, malware, safe, vuln, brute, dos, version, fuzzer, broadcast, exploit,	This is list of nmap script categories. You can specify also --script "not vuln", "default of broadcast"
nmap –script [script|category]	Run with specified script/scripts

nmap 192.168.1.1 --script "not intrusive"	Run only non intrusive scripts.
Timing	
-T0	Timing options, where number is from 0 (slowest) to 4 (fastest, parallel)
Oh no! Firewall!	
-f	Fragment packets to bypass firewall 
--open	To show only open and possibly open ports
--data-length	append random data to sent packets
-PS, -PA	Try it when ICMP pings are blockeds.
To hide scanning	
-D[decoy_ip],[decoy_ip]	if you want to hide your scan with decoys (it will looks like several hosts are scanning target.
--proxies	connect through http/socks4
-S	spoof source address
--spoof-mac	Spoof mac address
Discover services/system/interfaces/protocols	
-sV	Service/Version Detection
--iflist	showing host interfaces and routes
--osscan-guess	Guess os
-s0	to determine if TCP, ICMP, IGMP or other ip protocols are supported by target
Other	
--top-ports [number]	Scan most popular ports (argument is number of most popular ports)
ndiff [scan1.xml] [scan2.xml]	Compare results
nmap -p80 10.0.1.0/24 -oG - | nikto.pl -h -	Use nikto to scan what nmap discovered
nmap -iR 10 -n -oX out.xml | grep "Nmap" | cut -d " " -f5 > live_hosts.txt	Generate list of live ip addreses