

Nmap OS Fingerprint Cheatsheet

Test	Options	Explanation
A		Ack
	Z	Ack response is zero.
	S	Ack response = sequence number
	S+	Ack # equals sequence number +1
	O	Acknowledgment number is something else (Other).
CC		Explicit congestion control notification.
	Y	Only the ECE bit is set (not CWR). This host supports ECN.
	N	Neither of these two bits is set. The target does not support ECN.
	S	Both bits are set.
	O	Other
CD		ICMP response code.
	Z	Both code values are zero.
	S	Both code values are equal (Same).
	<NN>	When they both use the same non-zero number, it is shown here.
	O	Any other combination
CI		TCP closed port sequence generation (Z=zero, RD=random, HEX=same, RI=random positive increments, BI=Broken increment, I=incremental.)
CT		Closed TCP port used for scan
CU		Closed port for UDP, usually blank
D		Date in Month/Day
DC		Distance Calculation, how the Network Distance was calculated
	L	Localhost
	D	Direct subnet connection
	I	ICMP response to the U1 probe
DF		Don't Fragment, (Yes or No) (from the IP header)
DFI		Don't Fragment, (Yes or No) (from the IMCP header)
	N	Neither of the ping responses have the DF bit set.
	S	Both responses echo the DF value of the probe.
	Y	Both of the response DF bits are set.
	O	Both responses have the DF bit toggled.
DS		Hop distance
F		Flags
	E	ECN Echo (ECE): [64]
	U	Urgent Data (URG): [32]
	A	Acknowledgment (ACK): [16]
	P	Push (PSH): [8]
	R	Reset (RST): [4]
	S	Synchronize (SYN): [2]
	F	Final (FIN): [1]
G		Good results (Yes or No) If Yes the fingerprint can be submitted to nmap.
GCD		Greatest Common Divisor, A difference calculation between the packets.
II		ICMP port sequence generation (Z=zero, RD=random, HEX=same, RI=random positive increments, BI=Broken increment, I=incremental.)
IPL		IP Total Length (in octets)
ISR		TCP Counter Rate
M		Mac Prefix (1st 6 hex digits or vendor name)
O		TCP Options (See the OPS= Field below)
OT		Open TCP Port used for scan
P		Platform Nmap was compiled on.
PV		Shows if the target is on a private network (Yes or No)
Q		Quirks (R= reserved field in non-zero, U= urgent field is set)
R		Response(yes or no)
RD		TCP RST data checksum
RID		Returned IP ID value, (results G= good, or exact value)
RIPCK		Returned IP Checksum value, (results G= good, Z= zero, I= invalid)
RIPL		Returned IP length, (results G= good, or exact value)
RUCK		Returned IP Checksum , (results G= good, or exact value)
RUD		Integrity of returned UDP data, (results G= good, I= invalid)
S		SYN
	Z	Sequence number is zero.
	A	Sequence number = acknowledgment number
	A+	Sequence number = acknowledgment number+1
	O	Sequence number is something else (Other).
SP		Sequence Predictability, an estimate of how difficult it would be to predict.
SS		Shared Sequence (results S=shared O= other)
T		TTL setting
TG		TTL start value guess
TI		TCP open port sequence generation (Z=zero, RD=random, HEX=same, RI=random positive increments, BI=Broken increment, I=incremental.)
TM		Time, Unix time format (in hex)
TS		Time Stamp(0=zero, 1=2Hz, 7=100Hz, 8=200Hz, A=1000Hz, U=unsupported)
UN		Gives the value of the last four bytes in an ICMP response (if not zero)
V		Nmap version
W		Window size (in HEX)

Scan	Nmap Data
	V
	D
	OT
	CT
	CU
	PV
	DS
	DC
	G
	M
	TM
	P
Seq	Sequence
	GCD
	SP
	ISR
	TI
	CI
	II
	SS
	TS
Ops	TCP Options
Win	Window Size
ECN	Explicit Congestion
	R
	DF
	T
	TG
	W
	O
	CC
	Q
T1-T7	Test #
	R
	DF
	T
	TG
	W
	S
	A
	F
	O
	RD
	Q
U1	UDP
	R
	DF
	T
	TG
	IPL
	UN
	RIPL
	RID
	RIPCK
	RUCK
	RUD
IE	ICMP
	R
	DFI
	T
	TG
	CD

nmap-os-db format:
Fingerprint= 'Fingerprint' token and text description of the OS
class= Class vendor | OS family | OS generation | device type

Prepared by:
Smithpaul60

ops=	The TCP options recieved from the probes.
	End of Options List (EOL)
	No operation (NOP)
	Maximum Segment Size (MSS) : The value is appended.
	Window Scale (WS) : The value is appended.
	Timestamp (TS) : The value is appended.
	Selective ACK permitted (SACK)