xnet cheat sheet Cheat Sheet

by djtrump via cheatography.com/67354/cs/16910/

nmap Port Status

Open	Indicates that an application is listening for connections on the port. The primary goal of port scanning is to find these.
Closed	Responds to probes, but does not appear to be running a service. Commonly found on systems with no firewall in place.
Filtered	Typically protected by a firewall. Scanning tool is unable to determine if the port is open or closed.
Unfiltered	Port can be accessed, but tool is unable to determine if the port is opened or closed.
Open|Filtered	Port is believed to be open, but tool cannot definitely determine the port's state.
Closed|Filtered	Port is believe to be closed or filtered, but tool cannot definitely determine the port's state.

Nmap -- Arguments

sO	Used to discover which IP protocols are supported on the target system. Useful for deciding what type of subsequent scans to perform on the target.
sS	Performs a TCP SYN scan. It's the default scanning method when running Nmap as root. Considered to be stealthy because it does not open a full connection on the target host.
O	Similar to Xprobe2, performs OS detection. Works best where is at lease one open and one closed port on detected system.
ranodomize-hosts	Will randomize the order in which the targets are scanned. Combining this feature with other evasion techniques can decrease your chances of being detected during recon phase.
sn	Ping scan
p-	Scan all 65355 ports

File Processing

nmap -oX	For XML Output
xsltproc nmapOutput.xml -o nmapWebPage.html	Convert to HMTL
nmap-converter.py	convert to XLS

https://github.com/mrschyte/nmap-converter

By **djtrump**
cheatography.com/djtrump/

Not published yet.
Last updated 3rd September, 2018.
Page 1 of 1.