1.Basic Network Scanning

Nmap Query	Nmap Command
Scan a single target	nmap [target]
Scan multiple targets	nmap [target1,target2,etc]
Scan a list of targets	nmap -iL [list.txt]
Scan a range of hosts	nmap [range of IP addresses]
Scan an entire subnet	nmap [IP address/cdir]
Scan random hosts	nmap -iR [number]
Excluding targets from a scan	nmap [targets] –exclude [targets]
Excluding targets using a list	nmap [targets] –excludefile [list.txt]
Perform an aggressive scan	nmap -A [target]
Scan an IPv6 target	nmap -6 [target]

Nmap Query	Nmap Command
Perform a ping scan only	nmap -sP [target]
Don't ping	nmap -PN [target]
TCP SYN Ping	nmap -PS [target]

Nmap Query	Nmap Command
TCP ACK ping	nmap -PA [target]
UDP ping	nmap -PU [target]
SCTP Init Ping	nmap -PY [target]
ICMP echo ping	nmap -PE [target]
ICMP Timestamp ping	nmap -PP [target]
ICMP address mask ping	nmap -PM [target]
IP protocol ping	nmap -PO [target]
ARP ping	nmap -PR [target]
Traceroute	nmap –traceroute [target]
Force reverse DNS resolution	nmap -R [target]
Disable reverse DNS resolution	nmap -n [target]
Alternative DNS lookup	nmap –system-dns [target]
Manually specify DNS servers	nmap –dns-servers [servers] [target]
Create a host list	nmap -sL [targets]
Nmap Query	Nmap Command
Operating system detection	nmap -O [target]
Attempt to guess an unknown	nmap -O –osscan-guess [target]

Nmap Query	Nmap Command
Service version detection	nmap -sV [target]
Troubleshooting version scans	nmap -sV –version-trace [target]
Perform a RPC scan	nmap -sR [target]