

Check if manually mapped

cat /etc/hosts

Try DNS resolution

dig +short <hostname>

nslookup <hostname>

Simple ping

ping -c 1 <hostname>

Windows-style NetBIOS name lookup

nmblookup <hostname>

DNS brute-force (if DNS known)

dnsrecon -d <domain> -n <DNS_SERVER_IP>

Bash loop brute-force

for h in \$(cat names.txt); do ping -c 1 \$h.domain.local | grep "PING"; done