ANATOMY OF A HACK

The Objective	The Methodology	The Techniques	The Tools
Target address range, namespace acquisition, and information gathering are essential to a surgical attack. The key here is to not miss any details.	Footprinting	Open Source search whois Web interface to whois ARIN whois DNS zone transfer	UseNet, search engines, Edgar Any UNIX client http://www.networksolutions.com/whois http://www.arin.net/whois/ dig, nslookup ls -d, Sam Spade
Bulk target assessment and identification of listening services focuses the attacker's attention on the most promising avenues of entry	Scanning	Ping sweep TCP/UDP port scan OS Detection	fping, icmpenum WS_Ping ProPack nmap, Superscan, fscan nmap, queso, siphon
More intrusive probing now begins as attackers begin identifying valid user accounts or poorly protected resources.	Enumeration	List user accounts List file shares Identify applications	null sessions, DumpACL, sid2user, Onsite showmount, NAT, Legion banner grabbing with telnet or ncat
Enough data is gathered at this point to make an informed attempt to access the target.	Gaining Access	Password eavesdropping File share bruteforcing password file grab Buffer overflows	tcpdump, L0phtcrack readsmb NAT, Legion tftp, pwdump2 (NT) ttdb, bind, IIS
If only user-level access was obtained in the last step, the attacker will now seek to gain complete control of the system.	Escalating privilege	Password cracking Known exploits	john, L0phtcrack lc_messages, getadmin, sechole
The information gathering process begins again to identify mechanisms to gain access to trusted systems	Pilfering	Evaluate trusts Search for cleartext passwords	rhosts, LSA Secrets user data, config files, Registry
Once total ownership of the target is secured, hiding this fact from system administrators becomes paramount, lest they quickly end the romp.	Covering Tracks	Clear Logs Hide tools	zap, Event log GUI rootkits, file streaming
Trap doors will be laid in various parts of the system to ensure that privileged access is easily regained at the whim of the intruder.	Creating back doors	Create rogue user accounts Schedule batch jobs Infect startup files Plant remote control services install monitoring services replace apps with trojans	members of wheel, Administrators cron, AT rc, Startup folder, Registry keys netcat, remote.exe, VNC, BO2k keyloggers, addact, secadmin login, ftp, ps, ls, lsof, etc.
If the attacker is unsuccessful in gaining access, they may use readily available exploit code to disable the target as a last resort.	Denial of Service	SYN Flood ICMP techniques Identical src/dst SYN requests Overlapping fragment.offset bugs Out of bounds (OOB) DDoS	synk4 ping of death, smurf land, latierra teardrop, bonk, newtear supernuke.exe trinoo/TFN/stacheldraht