Was sind Exploits?
Ins deutsche übersetzt, heisst "exploit" soviel wie ausnutzen oder ausbeuten. Die hack-technische Bedeutung bezieht sich auf das Ausnutzen von Schwachstellen eines spezifischen Programms.
In der Regel bezeichnet ein Exploit nur ein Programm, dass einen Fehler der verwendeten Software auf einem Server ausnutzt, um unberechtigt Zugang auf diesem System zu erlangen.
Wie funktionieren Exploits?
Es sind schon viele verschiedene Verfahrensweisen nötig, um die Schwachstellen eines Systems ausfindig zu machen und entsprechend zu verwerten. Zudem versuchen Administratoren ihr möglichstes selbst die Schwachstellen Ihres Netzwerkes und der darauf laufenden Software aufzuspüren und durch entsprechende Einstellungen und Patches diese Sicherheitslöcher zu stopfen.

Es wird immer eine theoretische Möglichkeit geben, ein Programm zu nicht vorgesehene Aktionen zu bewegen. Bisher wird dies auch durch fast endlose Anzahl an Exploits, die auf diversen Sites für jedes Betriebssystem erhältlich sind unterstützt.

Im Beispiel des Unix-Betriebssystems, können Programme bestimmte Prozesse nur verarbeiten, wenn diese unter Root-Rechten (UID 0) laufen. Deswegen verfährt man in vielen Fällen so, dass entsprechende Programm das mit Root-Rechten läuft zu "crashen", um selbst an seiner Stelle die Root-Privilegien entgegen zu nehmen.
Die meisten Exploits basieren auf dem Buffer Overflow. Das bedeutet Pufferüberlauf, das Exploit startet meistens ein Programm, übergibt diesem Daten die das Programm nicht richtig verarbeiten kann und schreibt darauf hin einen neuen Code in den Arbeitsspeicher. Dieser neue Code ruft dabei meistens eine Shell mit den Benutzerrechten des Programms auf.

Arten von Exploits
Es gibt 2 Arten von exploits:

1. Local-Exploits: Das bedeutet das man schon einen Account auf diesem Rechner haben muss und dann dort den Exploit ausführt.

2. Remote-Exploits Mit dieser Sorte bekommt man von seinem eigenen Rechner Zugriff auf den anderen ohne einen Account auf auf dem Zielrechner zu haben.

Wie kommen Exploits zum Einsatz?
Das Programm wird ausgeführt und versucht das Ziel selbstständig anzugreifen, indem Sicherheitslücken ausgenutzt werden. Da vorzugsweise Exploits in der Programmsprache C vorliegen, muss zuvor noch der zugrunde liegende Quellcode kompiliert werden, um daraus ein lauffähiges Programm zu machen.
Je nach angewandter Verfahrensweise, wird ein Exploit direkt auf dem Zielrechner zur Anwendung gebracht, oder man benutzt einen anderen fremden Rechner, der den Angriff auf den Zielrechner durchführt. In der Regel wird ein fremder, schlecht gesicherter Rechner für einen Hack-Angriff verwendet, da hier Erfolgswahrscheinlichkeit grösser ist, seine Spuren so zu verwischen, dass man nicht mehr zurückverfolgt (traced) werden kann.
Und wie kompiliert man ein Exploit?

Da die meisten Exploits für *nix Systeme sind, werden sie auch unter *nix in C geschrieben. Also um ein Exploit zu kompilieren gibt in eurer *nix Shell: "gcc -o name quellcode.c" oder alternativ "cc -o name quellcode.c"

gcc -> das ist der Gnu-C-Compiler; cc ist der "normale"; -o -> ist eine Compileroption; name -> der gewünschte Programmname. Nach dem Kompilieren müssen wir das Programm nur noch ausführen also in die Shell eintippen: "./name" und das Programm wird ausgeführt. Oft steht im Quelltext eine

Anleitung und die entsprechenden Parameter die man benutzen sollte. Also unbedingt reinschauen und auch versuchen zu verstehen (manche Programmierer bauen sogar Fehler ein damit Unerfahrene sie nicht ausführen können). Also C Kenntnisse könnten nicht schaden.

Viele Exploits sind Versionsbezogen d.h. man sollte wissen welches OS läuft gibt es verschiedene Möglichkeiten:

1. Man verbindet sich über Telnet mit dem Server (falls Telnet läuft), man wartet auf den Login und liest die obere Zeile ab, da steht es meistens, einige Admins unterdrücken diese Zeile aber das man nicht sehen kann welches OS läuft.

2. Wenn der Port 21 (ftp) offen ist, verbindet man sich mit diesem und liest wieder diese Zeilen ab.

3. Unter z.B. Linux gibt es einen Scanner namens "nmap", dieser Scanner ist ziemlich beliebt und hat auch viele Funktionen. Mit nmap kann man auch feststellen welches OS auf dem Server läuft und man erfährt auch noch die offenen Ports. Diese ganzen Informationen muss man haben um evtl. Bugs auszunutzen.

Zu empfehlen ist vor allem ein Computer mit einem installierten Linux.

Wo finde ich Exploits?
Exploits gibt's auf:

http://packetstorm.securify.com/

http://www.rootshell.com/

http://www.rootsecure.de/inside/archive/exploits/exploits.html

http://www.rootshell.com/

http://www.secureroot.com/

http://hackersprimeclub.tsx.org/