Recall:
1. A remote exploit allows you to gain access to another machine by attacking a network service.
2. A local exploit allows you to elevate privileges on a machine you already have unprivileged access to.
3. We often represent a host diagramatically as two concentric circles. The inner circle represents privileged access (i.e. you can execute commands as the root/admin user — Note: in class we included executing commands as our “target” user as privileged access, but we will not look at it that way for this assignment!). The area between the inner and outer circles represents unprivileged access (i.e. you can execute commands, but only as a regular user). Outside of both circles represents no local access. Several hosts diagrams may be contained within a large circle which represents a firewall.

Mark each diagram below with the letter of the attack scenario it best represents. Note: there will be leftover letters!

a. Their apache webserver was vulnerable to a remote exploit, which I used to get a shell on the webserver ... but it wasn't an admin shell, just a regular user. So I used a local exploit against the Windows JVM to elevate to Administrator privileges.

b. I used my botnet to carry out a DDoS on their webserver.

c. I used a remote exploit to get access to the webserver, and in the webserver access log I found the password a user named “charlie” used for the password-protected part of the website. I figured he might use the same password for his account on his Windows workstation. Their firewall lets rdesktop through, so I rdesktop'd into the Windows workstation with username charlie and the password I found, and it got me in!

d. I had discovered that “charlie” was a username for some of these systems, and I had already done a little recon and determined some likely passwords for him from some social media sites --- he thinks we went to high school together :). So I tried rdesktop'ing to the Windows workstation over and over again with all the different password possibilities I had, and finally one worked: funkalicious. So I was in!

e. The firewall lets DNS traffic through, and the DNS server software they were using had a vulnerability. So I used a remote exploit on the DNS server and was able to get a shell ... and wouldn't you know it, the DNS server was running as a root/admin processes, so I got a root/admin shell!

f. I used a remote exploit to get access to the DHCP server and got a remote shell. Then I found a buffer overflow command that allowed me to elevate privileges to the root/admin user. This allowed me to view the password hashes, and a dictionary attack gave me the password to the root/admin account. I figured the same password might be used for the root/admin accounts of other machines, so I ssh'd to the DNS server and logged in as root using the same password, and I was in. Now I had root/admin access on both the DHCP server and the DNS server.

g. I used a remote exploit against the DNS server that got me a root/admin shell on that machine. That gave me access to the password file, so I used a dictionary attack and managed to crack the password hash for a user named charlie. Then I ssh'd from the DNS server to the fileserver with username charlie and tried the password I'd cracked from the DNS server. Of course charlie used the same password for his account on the fileserver, so I was in!