MSF Community Post Exploitation a11y.text MSF Community Post Exploitation A number of penetration testers stop at this point since they have obtained obtained a shell with administrative access on the target machine. This is a huge mistake since post-exploitation is just as important as getting that initial shell. Information gathered at this stage can be used to gain access to an organizationâ€™s crown jewels. With a session already established with the target machine, we simply click on the Session #, which is 3 in this case. Clicking on the Session 3 presents us with several options, but we are only interested in the â€˜Post-Exploitation Modulesâ€™ at this point, so we simply click on it and select our desired post-exploitation module. For purposes of this illustration, we will be using the â€˜Linux Gather Dump Password Hashes for Linux Systemsâ€™ post-exploitation module, so we just click on it: General information about the module is presented to us. If the session information is correct, we simply click on â€˜Run Moduleâ€™ Module is run and the desired output is presented to us. We can then attempt to crack some of those passwords, which may have been re-used on other critical pieces of the infrastructure. This marks the end of our post-exploitation section. There are more powerful post-exploitation modules than the one that was illustrated on this page, so we encourage you to some try of them on your own! Next Armitage Prev MSF Community: Exploitation