MSF Community Exploitation a11y.text MSF Community Exploitation So here it is, the exploitation phase! Now that a number of vulnerabilities have been discovered, we can proceed to the fun part, exploitation. Let us explore how this can be accomplished: First, let us browse to the list of vulnerabilities and click on our desired exploit module. In this case, we will be using exploit/multi/samba/usermap_script as follows: We are then taken to the exploit module page. We can now specify our Target Addresses, Target Settings, Payload and Evasion Options, and so forth. When ready, we can click on â€˜Run Moduleâ€™ to exploit the target system(s). Exploit is now sent to the target(s) and if successful, a corresponding session is opened. Notice how we have (1) active session by looking at the â€˜Sessionsâ€™ tab. Clicking on â€˜Sessionsâ€™ provides us with more information about the active sessions to the target(s) as seen below: Clicking on â€˜Session 3â€™ allows us to interact with the current session. Please note that the number â€˜3â€™ corresponds to our current session, so you may have a different session ID. Clicking on â€˜Command Shellâ€™ allows us to interact with our target. We have now successfully exploited our target machine. As can be clearly seen below, we have a shell and can execute system commands. Now that we have successfully exploited our target machine, letâ€™s take a look at post-exploitation in more detail! Next MSF Community: Post Exploitation Prev MSF Community: Scanning