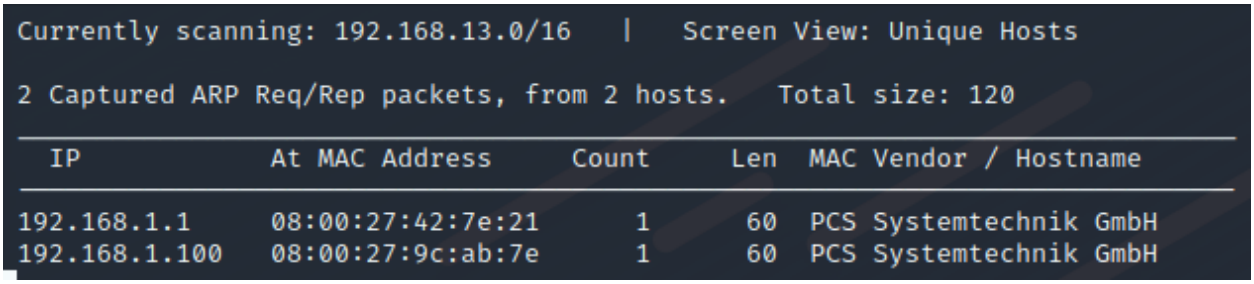
Writeup: Metasploitable vsftp exploit

This exploit uses a backdoor in version 2.3.4 of vsftp. This backdoor allows for an attacker to the terminal on the vulnerable machine. All the attacker needs to do is enter a username ending in :) and invalid as the password.

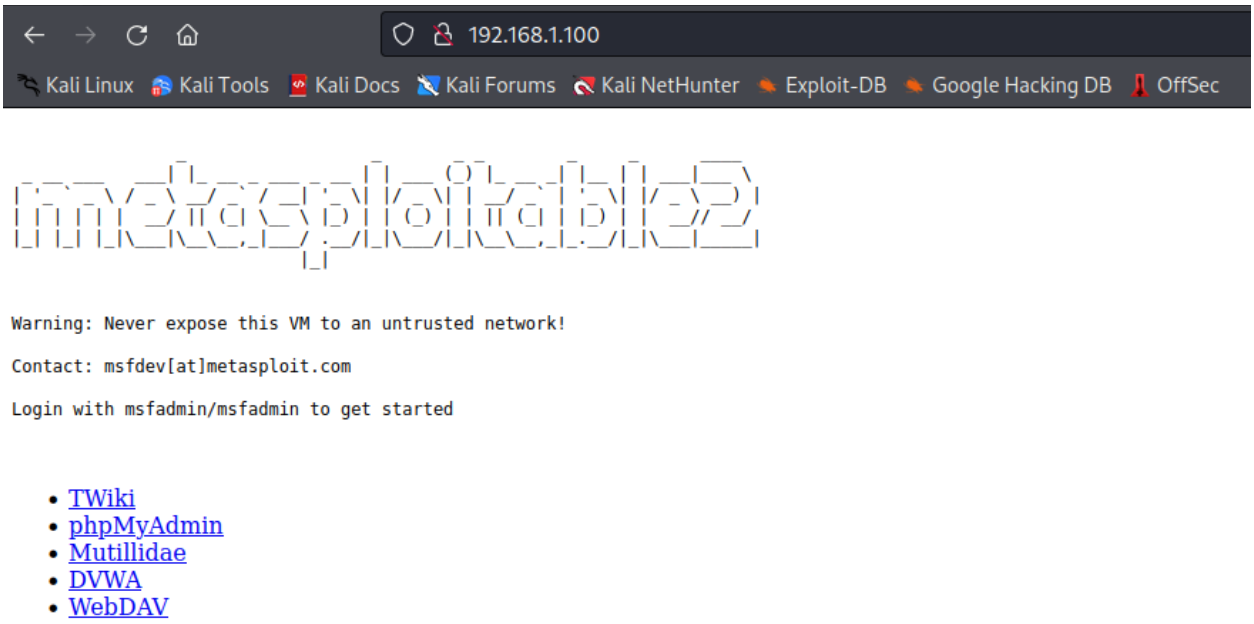
Once the attack is activated, it opens a shell on port 6200.

Initial recon

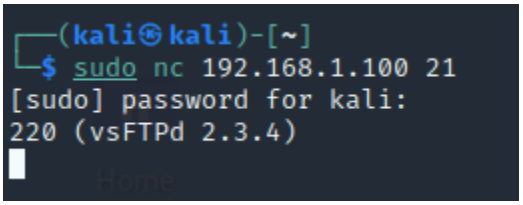
First, I scan the network to find the IP address of the Metasploitable server. I used the terminal command netdiscover to access this information. My results have my firewall, the result with the lower IP address, and the IP address of the Metasploitable server.



Navigating to 192.168.1.100 in my web browser confirms that I have the correct IP address.



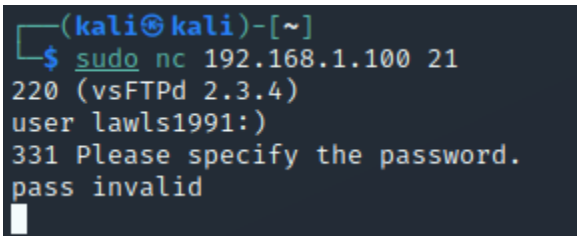
Next, I use Netcat (nc) to open a TCP socket to the server. I'll be opening port 21.



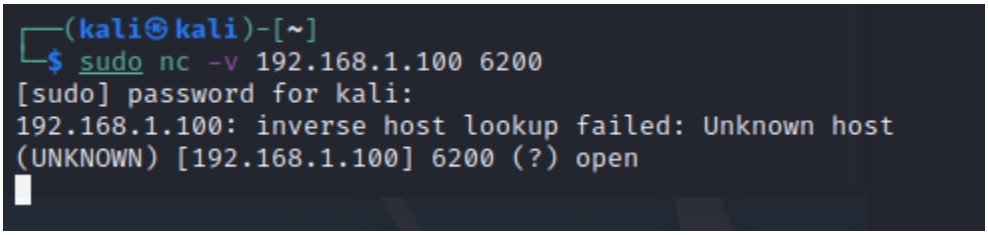
Here we see the version of vsftp is 2.3.4. A quick search on google for this version brings me to the Rapid7 page giving a description of the exploit.

Exploit

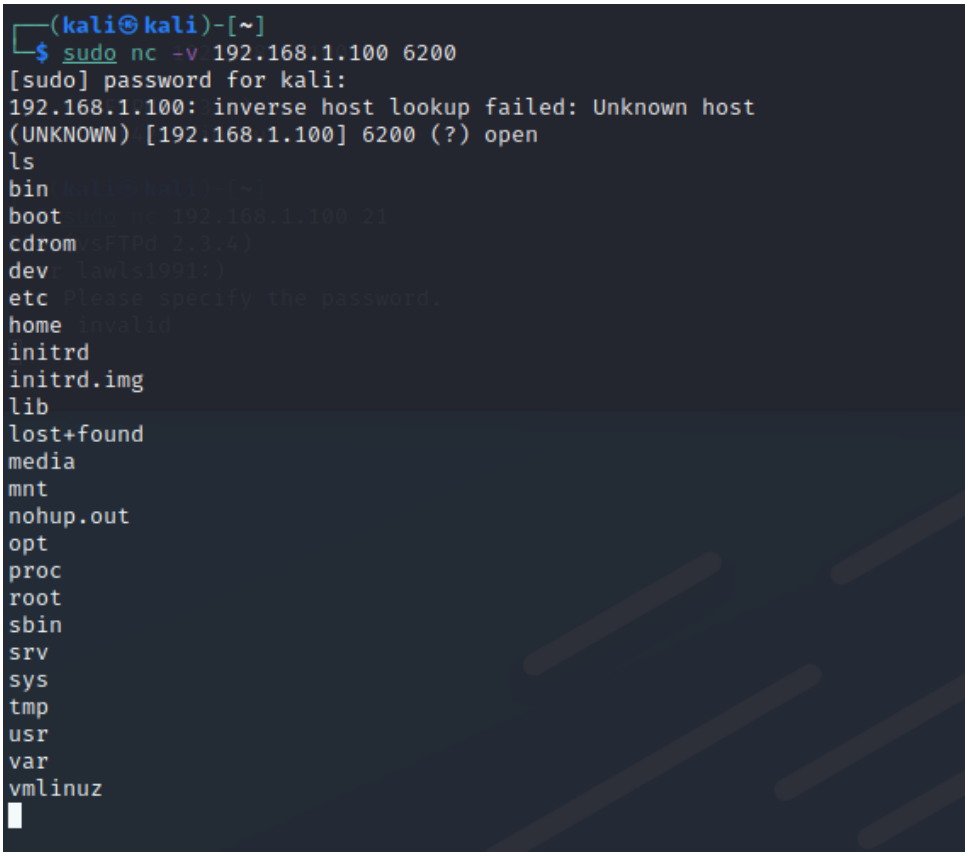
Now that I've confirmed the version, I can enter anything I want as a username as long as it ends with :) and invalid as the password.



In a new terminal window, I use Netcat again with the -v (verbose) command and feed it port 6200.



I get what looks like an error, inverse host lookup failed: Unknown Host. But entering the ls command will verify that I have access to the server.



Now that I have control, I can go as far as deleting all the information on the server to cause chaos, but as I'd have to reconfigure my server, I'll settle for just rebooting the server to cause minimal havoc.

Conclusion

This exploit can be patched by updating to the latest version of vsftp, however this machine will remain not updated as it is meant to be exploitable. This was a fun and quick little hack, and a good way to break in my home lab. I am reading through Ethical Hacking: A Hands-on Introduction to Breaking In by Daniel G. Graham, which has been an extremely helpful look into ethical hacking. This is also my first writeup, so if you've made it this far thanks for the support.

See You Space Cowboy…