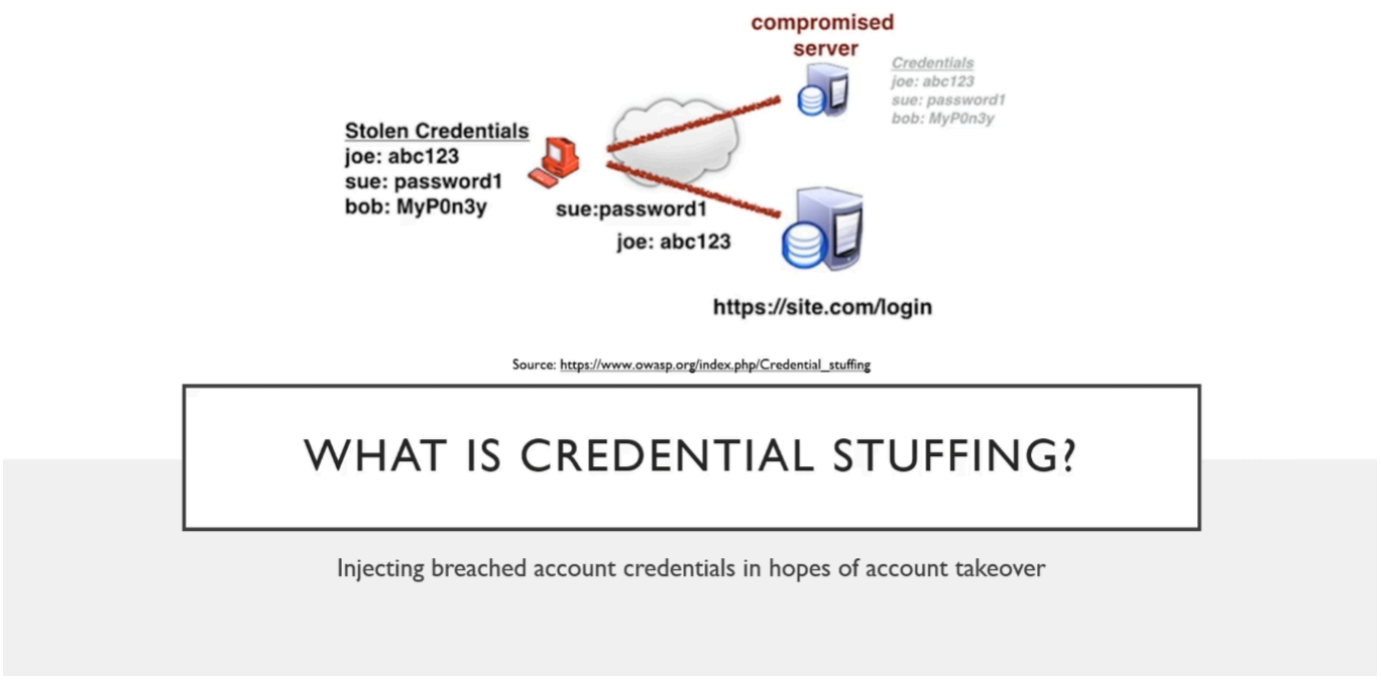
Credential Stuffing and Password Spraying



Pretty much "throwing" the breached credentials found at a website login, and hoping for a successful authentication.

We can search for those credentials in sites discusses in the "Information Gathering" notebook. There are specific websites, but we can also google it.

Credential Stuffing is when we try to use known login credentials against a website authentication mechanism hoping for a successful authentication. For this, Heath demonstrated the technique using Burp, and the type of attack is "pitchfork", which means the first item of the first list goes with the first item of the second list, and then the second item of first list with second item of second list, and so on. Because it will usually be short lists, this could be done in Burp in feasible time. But, there should be other tools we can use for this. Maybe even Hydra. Furthermore, Heath show how to Grep for a specific string on the login attempt requests, so it is easier see which ones authenticate, and which ones doesn't. Also, always keep a look for the length of the response, and the status code.

Password Spraying is when we have known usernames, but do not have a password. So, we run that username list against a big password list. Depending on the username list, and the password list, this method could take quite some time. This can be accomplished using Burp as well, but Hydra is going to iterate through the lists much much faster than Burp, if you are using community edition like I am. We can also try a single password, and a list of usernames.

These, according to Heath, are by far the most common way to get initial access in external assessments. The next most common way according to him are default credentials. Chances are very

low to find a known exploit for the external assessments.