# Evil Portal and DNSMasqSpoof

Cassandra McCandless

The evil portal provides a captive portal for all clients in the Pineapple. All connections through the PineAp get redirected to the captive portal. This will happen even if the user writes the URL directly in the browser. Clients cannot reach the internet either until they accept the captive portal. The DNSMasq Spoof is needed to create a fake DNS server. This will redirect some domains and subdomains to the fake homepage, and it allows you to hijack site traffic. It only works on DNS servers that you control, and this can also mean that users can find other servers to use.

There are five areas needed to do the evil portal. They are controls, evil portal messages, white list, authorized clients, and workbench. The workbench is the most important because that is what allows you to actually create the portal. Controls allow you to start the module and activate the boot option. The evil portal messages will show some messages when a new client accepts the captive portal. The white list area allows you to input IPs, and to avoid the captive portal and reach the internet when the client connects. You can use this area to input the control device's IP. Finally, authorized clients show all IPs authorized to reach the internet. This is because they have accepted the captive portal. The first step in doing this is to create the portal. You can modify it later if need be. You will name the portal, and then you need two files inside. These files could be named index.php and MyPortal.php. The file index.php is the file that is going to contain the captive portal. It will have php and html code, and we can even paste in our own html code and create some sort of fake page. Then, you will edit MyPortal.php. This

contains the php class. It is important to change the handle authorization method and get the POST data and save it to a text file like $_POST. That's when the captive portal is complete.

To test it you can create an open network and name it something like Lewis WiFi for example. You can connect using a mobile device. When you type in a web address it should take you to the page you created.

A target for this attack would be someone that you would want to control their Internet activities. Some businesses and government agencies actually use this for this reason. This is because it is an effective monkey in the middle trick for eavesdropping and altering packets. HTTP sessions are sent and then the eavesdropper sees everything. Basically, this is used for tricking someone into getting onto the fake server you created so that you can capture and examine their traffic however you want.

Some countermeasures for this attack are using SSH and OpenVPN. This is a good measure because even though they can be vulnerable it does give a layer of protection because it takes way more expertise and  effort than just eavesdropping on traffic that does not have any encryption. SSL is also helpful in protecting against this type of attack.