**Capture the flag #5: Preparations**

Rules: no firewalls or defense; no social engineering. The only machines that can be exploited are Windows Server 2003 VM’s (Where your DNS and Web servers are hosted). You must make sure you don’t turn on firewalls or anything like that. One person per team should be responsible for documentation. Doesn’t matter who, and they can do other things as well.

1. Both teams need to create a web server that hosts a page that says the teams name (red team or blue team, no decoys at this point).
2. Both teams need to designate one of their dns servers as their team’s dns server. (no decoys at this point)
3. This DNS server should host an A record that points to their web server (e.g. redteam.localtarget.com or blueteam.localtarget.com)
4. Both teams will create a user called “Redroot” or “Blueroot” on their designated DNS server and assign it a 5-letter dictionary word for a password.