Internal Penetration Test Process/Checklist

* [ ] Map the Internal Network
* [ ] Scan the Network for Live Hosts
* [ ] Port-scan individual machines
* [ ] Try to gain access using known vulnerabilities
* [ ] Attempt to establish null sessions
* [ ] Enumerate users/identify domains on the network
* [ ] Sniff the network using Wireshark
* [ ] Sniff POP3/FTP/Telnet Passwords
* [ ] Attempt Replay Attacks
* [ ] Attempt ARP Poisoning
* [ ] Attempt MAC Flooding
* [ ] Conduct Man-In-The-Middle Attacks
* [ ] Attempt DNS Poisoning
* [ ] Try logging in to a console machine
* [ ] Boot the PC Using an Alternate OS and Steal the SAM File
* [ ] Bypass the OS to Obtain Information
* [ ] Attempt to plant a software keylogger to steal passwords.
* [ ] Attempt to plant a hardware keylogger to steal passwords.
* [ ] Attempt to plant spyware on the target machine
* [ ] Attempt to plant a Trojan on the target machine
* [ ] Attempt to to bypass antivirus software installed on the target machine
* [ ] Attempt to send a virus using the target machine.
* [ ] Attempt to to plant rootkits on the target machine
* [ ] Hide sensitive data on target machine
* [ ] Hide hacking tools and other data on target machines
* [ ] Use various steganography techniques to hide files on target machines.
* [ ] Escalate user privileges
* [ ] Capture POP3 Traffic
* [ ] Capture SMTP Traffic
* [ ] Capture IMAP E-mail traffic
* [ ] Capture the communications between FTP client and FTP Server
* [ ] Capture HTTP Traffic
* [ ] Capture RDP Traffic
* [ ] Capture VoIP Traffic
* [ ] Run Wireshark with the filter -ip.src == ip\_address
* [ ] Run Wireshark with the filter -ip.dst == ip\_address
* [ ] Run Wireshark with the filter -tcp.dstport == port\_no
* [ ] Run Wireshark with the filter -ip.addr == ip\_address
* [ ] Spoof the MAC Address
* [ ] Attempt Session Hijacking on telnet traffic.
* [ ] Attempt Session Hijacking on FTP traffic.
* [ ] Attempt Session Hijacking on HTTP traffic.
* [ ] Document Everything