

**Exploitation | Vulnerability Assessment | Linux**

Linux Service	Purpose
Apache Web Server {80/443}	Web Server
SSH {22}	Remote Access Protocol
FTP {21}	File Transfer Protocol
SAMBA {445}	Linux equivalent of SMB - File sharing protocol between PCs on a LAN

Tool	Purpose	How to use
Nessus	Vuln Scanner	DL Nessus Essentials
NMAP	Vuln Scanner Scripts	<code>nmap --script vuln -p 21 demo.ine.local</code>

Vulnerability Assessment | Web App

Tool	Purpose	How to use
WMap	Web App Vuln Scanner	In MSF: load wmap wmap_sites -a {IP} wmap_targets -t {Service://IP} wmap_run -t / -e

Extra Notes:

- To spawn a bash session: `/bin/bash -i`
- Webshells: `/usr/share/webshells/`