**1.(50 points) Select a target domain and use Nmap for the following tasks.**

(a) host discovery on the selected domain,

(b) port scanning on a selected host,

(c) active stack fingerprinting on the selected host,

(d) version scanning on a selected port,

(e) vulnerability scanning on the selected port.

**2.(20 points) List and compare nmap-os-fingerprints**

**Used in Nmap and osprints.conf used in Siphon. Discuss how and why they differ.**

**3.(20 points) List and compare nmap-services**

**and nmap-service-probe. Discuss how and why they differ.**

**4.(10 points) On a UNIX/Linux host, list**

**/etd/inetd.conf. Discuss what services are being**

**offered.**

**5.(30 points) Select a target domain,**

**Run metaexploit with Nmap scans and**

**import Nmap results into the database. Show found hosts and available ports.**

**6.(30 points) Select a website to do banner grabbing with telnet, netcat, and grendel-scan, respectively. Show and compare their results.**

**7.(20 points) Select a target domain to do automatic DNS enumeration by dnsenum to find subdomains, servers, and their IP addresses.**