**Pre-Lab**

Kali 192.168.56.105

Windows Host 192.168.56.1

**Part 1**

**Q.1:**

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

**Part 2**

**Q.2:**

**Graphical user interface

Description automatically generated**

**Text

Description automatically generated**

**Part 3**

**Q.3:**

Text

Description automatically generated

**Part 4**

**Q.4:**

* **Identify**
  + <https://whois.domaintools.com/>
  + Nmap (NSE)
  + Wireshark – Packet Sniffing
  + Nikto – Comprehensive Tests against a Web Server
  + OWASP ZAP – Scan Web Services
  + Netcat – Banner Grabbing and Port Scan
  + Lynis – Audit Linux System for Security, Hardening, and Compliance Testing
  + Wfuzz – Provides Invalid, Unexpected, or Random Data Inputs
  + Legion – Penetration Testing Tool
  + Burp Suite – Mapping and Exploiting Security Vulnerabilities
  + SSL Certificate – Digital Certificate for Authentication, provides information
* **Protect**
  + DVWA – Practice with different levels of Security
  + Remote Desktop Connection via UDP/SNMP – Remote Access to a System
    - Keeping systems up to date, patched
  + Steganographic Tool – Hide a Message in Spam
    - <https://www.spammimic.com/index.cgi>
  + PGP – Encryption Program, signing, encrypting, and decrypting
* **Detect**
  + Nmap
  + Wireshark – Real Time Monitoring
  + Legion
  + Burp Suite – Mapping and Exploiting Security Vulnerabilities
* **Response**
  + Legion
  + Scapy – Packet Manipulation and DoS
  + Fixing any found vulnerabilities would be a key part of the Response Function
* **Recover**
  + I don’t think any tools specifically that we learned fit into Recover, however I know that we have talked about tools that can schedule routine backups of the system. We have also discussed how an organization should handle an attack by having a pre-existing Recovery Plan.