1. **The HTML reports from your scans.**

   ➔ The HTML reports for scans on the four machines/IPs are included in the folder. Details given below will help in recognizing the same
   a. 10.0.0.113 -> Scan_113
   b. 10.0.0.124 -> Scan_124
   c. Windows VM 10.0.100.2 -> Scan_windowsVM
   d. Linux VM -> Scan_linuxVM

2. **Analyze any one high or medium risk vulnerability that you found in your reports. What could have caused this vulnerability? What are some of the steps you can take to remediate the vulnerability?**

   ➔ A high vulnerability risk was found in the scan of 10.0.0.124(chicago.nslab)

   Here is the export list of chicago.nslab :
   /export *
   Please check the permissions of this exports.

   nfs (2049/udp)

   This implies that the Network File System is running but does not import/export any files and can impact the confidentiality and the integrity of the file system.
   There can be chances of complete information leak and also since the port used by NFS is 2049 which is used by most of the installations by default, the intruders will have chance of accessing this port directly without any authentication required. NFS gives complete information about system-critical data to any user.

   Steps to remediate this vulnerability:
   - Never specify /export * which gives permission to anyone connected to the NFS server to access the shared data
   - Use wildcards while using exports in NFS .
   - Firewall rules can be setup in the iptables and the access can be restricted to the portmap service

   A medium vulnerability: One of the scan showed medium vulnerability for using weak ciphers protocols like

```
Weak ciphers offered by this service:
SSL3_RSA_RC4_128_MD5
SSL3_RSA_RC4_128_SHA
SSL3_RSA_WITH_SEED_SHA
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
```

   Steps to remediate :
   Use better cipher suites which includes a combination for encryption, authentication and Message authentication codes. (AES,RSA,Diffie-hellman,etc)

3. **Are vulnerability scanners efficient in finding all the vulnerabilities of a system? Explain some situations where vulnerability scanners may not work efficiently.**

   ➔ No the vulnerability scanners are not efficient in finding all the vulnerabilities of a system.
   The scanners fail to scan the customized applications and also use a predefined set of vulnerabilities of the scanner to generate the scan report.

   Few scanners like Nessus doesn't detect SQL injection on the web application. They generate false negatives and positives which would require a human to authenticate. If the scanner can't find the SQL injection, the attacker can turn it into an XSS exploit, or bypass authentication, or disclose the data stored in the database server, modify or delete the data in the database.
   Also , the scanners maintain a list of version numbers of the softwares or OS which are prone to certain kinds of vulnerabilities. Few OS releases like Linux distributions provide security fixes on the older version and may or

may not change the version number where some string may be appended to the version number. This creates false positives and will be vulnerable.