-------------------- Cybersecurity Assessment Roadmap   -----------------------

1. Pre-Assessment Planning
- **Objective:** Define the scope and objectives of the assessment.
- **Actions:**
  - Identify and select systems, networks, and data for assessment.
  - Choose appropriate tools based on the assessment scope.
  - Install and configure the following tools on the assessment machine:
    - **Nmap:** Network scanner.
    - **OpenVAS:** Comprehensive network scanner.
    - **Nikto:** Web application scanner.
    - **Burp Suite:** Web application scanner.
    - **Nessus:** Vulnerability scanner.
    - **Wazuh:** Monitoring tool.
    - **Snort:** Intrusion Detection System/Intrusion Prevention System (IDS/IPS).
    - **Suricata:** IDS/IPS.
    - **OpenDLP:** Data Loss Prevention tool.
    - **ClamAV:** Malware scanner.

2. Network Vulnerability Scanning
- **Objective:** Identify potential vulnerabilities in internal and external networks.
- **Actions:**
  - Use **Nmap** for internal network scanning:
    - Command examples: `nmap -sV -oN result.txt -T4 192.168.1.0/24`, `nmap -sn -oN result.txt 192.168.1.0/24`.
  - Use **OpenVAS** for detailed network scans.

3. Web Application Scanning
- **Objective:** Discover vulnerabilities in web applications.
- **Actions:**
  - Utilize **Burp Suite** for in-depth web application scanning and analysis.
  - Deploy **Nikto** for additional web application vulnerability scanning:
    - Command example: `nikto -Format html -o report.html -h http://www.example.com/`.

4. Monitoring and Vulnerability Management
- **Objective:** Continuously monitor networks and manage vulnerabilities.
- **Actions:**
  - Implement **Wazuh** for network monitoring and compliance reporting.

5. Analysis and Reporting
- **Objective:** Analyze data collected from scans and monitoring, and compile findings.
- **Actions:**
  - Review and analyze reports from network scans, web application scans, and monitoring tools.
  - Compile findings into a comprehensive report, highlighting key vulnerabilities and providing improvement recommendations.

6. Recommendation Planning
- **Objective:** Develop a remediation plan based on the assessment findings.
- **Actions:**
  - Develop a remediation plan addressing identified vulnerabilities.
  - Prioritize actions based on the risk level of the vulnerabilities.

7. Documentation and Compliance
- **Objective:** Maintain thorough records and ensure adherence to compliance standards.
- **Actions:**
  - Keep detailed documentation of all assessments, findings, and remediation actions.
  - Regularly review security measures for compliance with relevant laws, regulations, and industry standards.

######################## TIME LINE #################################

Monthly Cybersecurity Assessment Timeline

Week 1: Planning and Preparation
- **Days 1-2:** Review and Update the Assessment Scope
  - Update the list of assets, systems, and networks to be included in this month's assessment.
- **Days 3-5:** Tool Configuration and Updates
  - Ensure all tools (Nmap, OpenVAS, Burp Suite, etc.) are updated and configured for the current assessment.

Week 2: Active Scanning and Monitoring
- **Days 1-3:** Network Vulnerability Scanning
  - Conduct scans using Nmap and OpenVAS. Focus on different segments of the network each month.
- **Days 4-5:** Web Application Scanning
  - Use Burp Suite and Nikto for targeted scanning of web applications.

Week 3: Analysis and Advanced Techniques
- **Days 1-2:** Analysis of Scanning Results
  - Analyze the results from network and web application scans.
- **Days 3-4:** Advanced Security Techniques
  - Conduct penetration testing, threat hunting, or red/blue team exercises.
- **Day 5:** Continuous Monitoring Check
  - Review alerts and logs from continuous monitoring tools like Wazuh or OSSEC.

Week 4: Reporting, Remediation Planning, and Compliance
- **Days 1-2:** Compile Reports and Develop Recommendations

  - Compile findings into a report and develop remediation recommendations.
- **Days 3-4:** Remediation Plan and Prioritization
  - Develop a remediation plan based on the findings and prioritize actions.
- **Day 5:** Compliance Review
  - Ensure that all actions and configurations comply with relevant standards and regulations.

End of Month: Review and Feedback Session
- Conduct a review meeting to discuss findings, actions taken, and gather feedback for continuous improvement.

Recurring Throughout the Month:
- **Regular Updates and Patch Management:** Continuously update and patch systems as new patches become available.
- **User Training and Awareness:** Conduct regular training sessions and updates on new threats and best practices.
- **Incident Response:** Be prepared to initiate the incident response plan in case of any detected security incidents.

NETWORK PENTEST METHODOLOGY

Step 1 : Identify live hosts

Ping
Hping
Nmap
Step 2 : Identify OS type

Nmap
Xprobe2
Banner grabbing using telnet, nc (netcat)

Step 3 : Port scan

Nmap full SYN scan with verbose mode and service detection and disabling ping scan. Export normal and greppable output for future use.

```
nmap -Pn -p- -sV X.X.X.X -v -sS -oG nmap_grepable_SYN -oN nmap_normal_SYN
```

Nmap top 1000 UDP scan with verbose mode and service detection and disabling ping scan. Export normal and greppable output for future use.

```
nmap -Pn -top-ports=1000 -sV X.X.X.X -v -sS -oG nmap_grepable_UDP -oN
nmap_normal_UDP
```

Nmap Full port scan identifying any weak algos and ciphers in SSH and SSL. Export normal and greppable output for future use.

```
nmap -Pn -A -T4 -vv --script ssh2-enum-algos --script ssl-enum-ciphers <Target List>
```

Step 4 : Use Nessus

Following things to be looked in the Nessus policy before scan is run:

DoS disabled
Enable TCP and UDP scan
Plugins are updated as per defined plugin policy
Step 5 : Use NMAP scanner on specific open ports

port 22 (SSH) is open and you want to run all scripts pertaining to SSH then use below command:

```
Nmap -Pn -sS -p22 --script ssh* -v
```

Step 6 : Audit SSL (Use testssl.sh or TestSSLMaster.exe for SSL related vulnerability mentioned here for quicker results)

Use openssl, sslyze tools to find below issues within SSL.
Self-signed certificate
SSL version 2 and 3 detection
Weak hashing algorithm
Use of RC4 and CBC ciphers
Logjam issue
Sweet32 issue
Certificate expiry
Openssl ChangeCipherSec issue
POODLE vulnerability
Openssl heartbleed issue
Lucky 13 and Beast Issue

Step 7 : Check for default passwords in server/device/service documentation

Lets say during your port scan or VA you found some services running on the server for example: cisco, brocade fabric OS, sonic firewall, apache tomcat manager. Then for these services Google what are the default configuration administrative username and password. Try those in your login and check your luck.

Step 8 : Hunting some common ports

1. DNS (53) UDP-

-Examine domain name system (DNS) using dnsenum, nslookup, dig and fierce tool

-Check for zone transfer

-Bruteforce subdomain using fierce tool

-Run all nmap scripts using following command: nmap -Pn -sU -p53 --script dns* -v

-Banner grabbing and finding publicly known exploits

-Check for DNS amplification attack

2. SMTP (25) TCP -

-Check for SMTP open relay

-Check for email spoofing

-Check for username enumeration using VRFY command

-Banner grabbing and finding publicly known exploits

-Send modified cryptors and check if SMTP gateway is enable to detect and block it?

-Run all nmap script using following command: nmap -Pn -sS -p25 --script smtp* -

3. SNMP (161) UDP -

-Check for default community strings ‘public’ & ‘private’ using snmpwalk and snmpenum.pl script.

-Banner grabbing and finding publicly known exploits

4. SSH (22) TCP-

-Banner grabbing and finding publicly known exploits

-Check if that supports sshv1 or not.

-Bruteforce password using hydra and medusa

-Check if it supports weak CBC ciphers and hmac algorithms using ssh2-enum-algos.nse nmap script.

-Run all nmap scripts using following command: nmap -Pn -sS -p22 --script ssh* -v

5. Cisco VPN (500) UDP-

-Check for aggressive and main mode enable using ikescan tool.

-Enumeration using ikeprobe tool

-Check for VPN group and try to crack PSK in order to get credentials to login into the VPN service through web panel.

6. SMB (445,137,139) TCP-

-Check SAMBA service using metasploit use auxiliary/scanner/smb/smb_version

-Get reverse shell using meterpreter reverse tcp module.

-Check for SMB related vulnerability using 'smb-check-vulns' nmap script.

7. FTP (21) TCP-

-Run all nmap script using following command: nmap -Pn -sS -p21 --script ftp* -v

-Check for cleartext password submission for ftp login

- Check for anonymous access using username and password as anonymous:anonymous

- Banner grabbing and finding publicly known exploits

- Bruteforce FTP password using hydra and medusa

8. Telnet (23) TCP-

-Banner grabbing and finding publicly known exploits

-Bruteforce telnet password

-Run following nmap scripts

- telnet-brute.nse

- telnet-encryption.nse

- telnet-ntlm-info.nse

9. NTP (123) UDP-

-Perform NTP enumeration using below commands:

- ntpdc -c monlist IP_ADDRESS
- ntpdc -c sysinfo IP_ADDRESS

-Run all nmap scripts using nmap -Pn -sS -p21 --script ntp* -v

10. SQL Server (1433,1434, 3306) TCP-

-Banner grabbing and finding publicly known exploits

-Bruteforce and perform other operation using following tools:

- Piggy
- SQLping
- SQLpoke
- SQLrecon
- SQLver

-Run following nmap scripts:

[
- ms-sql-brute.nse
- ms-sql-config.nse
- ms-sql-dac.nse
- ms-sql-dump-hashes.nse
- ms-sql-empty-password.nse
- ms-sql-hasdbaccess.nse
- ms-sql-info.nse
- ms-sql-ntlm-info.nse
- ms-sql-query.nse
- ms-sql-tables.nse
- ms-sql-xp-cmdshell.nse
- pgsql-brute.nse

]

-For MYSQL default username is root and password is

11. RDP (3389) TCP-

-Perform enumeration via connecting and checking login screen. Gather all active user’s name and domain/group name.

-Perform RDP cryptography check using RDP-sec-check.pl script.

-Run following nmap script:

- rdp-enum-encryption.nse
- rdp-vuln-ms12-020.nse

12. Oracle (1521) TCP

-Enumeration using following tools

- Tnsver [host] [port]
- Tnscmd

o perl tnscmd.pl -h ip_address

o perl tnscmd.pl version -h ip_address

o perl tnscmd.pl status -h ip_address

-Enumeration & Bruteforce using below nmap scripts:

[· oracle-brute.nse

- oracle-brute-stealth.nse
- oracle-enum-users.nse
- oracle-sid-brute.nse
- oracle-tns-version.nse]

USEFUL LINKS FOR TOOLS:

Nessus : https://www.tenable.com/products/nessus
testssl.sh : https://github.com/drwetter/testssl.sh
testsslserver.exe : https://www.bolet.org/TestSSLServer/
Nikto : https://cirt.net/Nikto2
Nmap : https://nmap.org/
Yasca : https://github.com/scovetta/yasca
John The Ripper : https://www.openwall.com/john/
masscan : https://github.com/robertdavidgraham/masscan

DNSdumpster : https://dnsdumpster.com/
Kali : https://www.kali.org/downloads/