|  |  |
| --- | --- |
| Security Testing Essential Testing | |
|  | |
| 1. Risk Assessment 2. Security Control Assessment 3. Compliance Assessment 4. Vulnerability Assessment 5. Penetration test |  |
| **RISK ASSESSMENT** – Goal to find threats and vulnerability (NIST)  Example – malware, impact, inflicted by a threat.  -Make sure you do your research | **Security Control Assessment** – Determine whether or not your security program meets the specific requirements outlined by some external authority.  Example: you pick up a framework.  2 popular frameworks   1. ISO – International Organization for standardization 2. NIST Cybersecurity framework |
| **Compliance Assessment –** determine whether or not your security program meets the specific requirements outlined by some external authority.  Example: PCI DSS – payment card industry | **Vulnerability Assessment** – validates that technical vulnerabilities are being identified and remediated on a regular basis.  Example: looking for exploitable, like security patches, SQL injection, Endpoint and network   1. Authenticated scans of all host system 2. Unauthenticated scans of internet-facing web applications 3. Authenticate scans of nonproduction instances of those same applications 4. Security configuration scans of those same systems and application. |
| **Penetration Testing** –   1. White box testing – given full information 2. Black box testing – treated as unauthorized outsider, focus on finding exploiting weaknesses 3. Gray box testing – some internal knowledge   Goals: domain admin, email access, intellectual property, customer information | |

|  |  |
| --- | --- |
| Security Tester Toolkit | |
| 1. Kali Linux 2. NMAP 3. NESSUS 4. WIRESHARK 5. LYNIS – for linux 6. CIS-CAT lite 7. Aircrack-ng 8. Hashcat – cracking password or john the ripper 9. OWASP ZAP – open web application security project |  |
|  |  |

|  |  |
| --- | --- |
| Planning Your Assessment | |
| Don’t take unnecessary risk – GET IT WRITING |  |
| NIST  SP-800-30 REV 4 | ISO |
| Vulnerability Assessment   1. Nessus 2. Qualys Cloud Platfom 3. Nexpose 4. OpenVAS | Basic Assessment Tools |

|  |  |
| --- | --- |
| Review Documentation | |
| ISACA   1. Policies 2. Standard 3. Guidelines 4. Procedures | **Logging and Monitoring** – examine logging configuration.   1. Failed Authentication 2. Sensitive Authentications 3. Privilege use 4. Service modification 5. Source, destination, date, time |
| **Log management tool** –   1. Endpoint activity 2. Centralized log storage 3. Time synchronization 4. Log Retention | Log management tool – Commercial Solutions   1. Splunk 2. QRadar 3. LogRythm 4. Alien Vault 5. Syslog 6. Syslog-ng 7. Graylog 8. ELK Stack   Critical Log Review Checklist for Security Incidents |
| **Ruleset Review** – Router, Firewall, IDS, IPS  Deny rules, use by defaults  Least privilege (do open port and close unnecessary ports)  IDS/IPS Review – disable/delete unnecessary signatures  Testing firewall – user NMAP or manually review | **System Configuration Review** –  -Enable Service  -Privileged accounts  -Encryption requirements  Use Tools:  -LYNIS  -CIS-CAT |
| **Network Sniffer** – check what’s the normal time for users.  -Active devices and identifying information  -Unencrypted data  -Unencrypted credentials  Sniffer Location  -At the perimeter  -Behind firewalls – IDP/IPS | **File integrity Checking** –  -To make sure they’re same  -Add hash (MD5, Hash value)  Tripwire.com – Commercial  OSSEC – OPEN-SOURCE SOLUTION |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| Passive Scanning | Active Scanning |
|  |  |
|  |  |
| Vulnerability Scanning   1. Upgrade hardware 2. Software   Authenticate vs Unauthenticate Scan   1. Host 2. Web 3. Mobile | Varies on severity   1. Full-host compromise – high   CVSS – Common Vulnerability Scoring System |
|  |  |
|  |  |
|  |  |
|  |  |