|  |  |
| --- | --- |
| 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 |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |