1. Malware: software ce da aka tsara don to kawo cutarwa , misali virus, worms, trojans, ransomware, ko spyware.
2. Phishing: wani kutsen na’ura ne da me kutse yake yaudarar wanda zaiwa kutse ya bashi bayanansa kamar:Kalmar sirri (password) ko bayanan katin cirar kudi (pin), ta hanyar nunawa shi abun yarda ne. yana faruwa ta email, ko sakon karta kwana (message), ko website.
3. Firewall: Na’ura ce da take lura da sarrafa yadda zirga-zirga (traffic) ke fita da shiga akan tsarin da aka seta ta. Tana kasancewa shinge tsakanin cibiyar sadawarwa na ciki (internal network) da cibiyar sadarwa na waje (external network ) don ta kare wanda bashi da izini shiga ko yin barna a cikin hanyar sadarwa (network).
4. Encryption: hanya ce ta canja bayani zuwa amintacce (secure) da tsari mara karantuwa (unreadable format), ta hanyar amfanin da algorithm. Yana tabbatar da cewa iya mai izini ne kawai zai iya shiga ko yaga bayanan da aka tsare.
5. Vulnerability: Yana nufin Rauni ko matsala a cikin tsari (system) ko software ko hanyar sadarwa (network), da masu kutse zasu iya amfani dashi don shiga ciki su samar da matsala ko suyi abunda bai dace ba.
6. Patch: sabuntawa (software update) ne da developers suke gyara vulnerability ko bugs a cikin application ko operating system. Yin patch yana taimakawa wajan gano matsala da kara karfin tsaro a system.
7. Two-Factor Authentication (2FA): Yana kara layer akan process din authentication ta hanyar bukatar user ya bada sheda guda biyu. Yawanci, yana nufin hada password da wani abu da user kadai yake dashi. Kamar lamba na musamman da application ko website yake baka a matsayin token.
8. Intrusion Detection System(IDS): security tool ne da ake amfani dashi don bibiyar hanyar sadawar don gano wani hali na tuhuma (suspicious behaviour) ko alama of potential attacks. Yana alert din administrators yayin da yaga sabon al’amari a network.
9. Social Engineering: Hanya ce da masu kutse suke amfani dashi don manipulating mutum don ya divulging sensitive information ko yin wani abu da zai compromise din tsaro. Suna amfani da ilimin sanin halayyar dan adam don manipulating kuma suna amfanin da impesonation, deception, ko persuation.
10. Denial-of-Service (DoS) Attack: kutse ne da yake distrupt ko ya lalata normal function na network ko system ko website, ta hanyar overwhelming dinsa da excessive amount of traffic ko resource request. Takamai man abunda yasa ake yinsa shine a hana masu amfani da system din amfani dashi.
11. Penetration Testing: Ana kiransa da ethical hacking ko kuma pen testing, hanya ce da masanan cybersecurity suke gano Rauni da kuma gano karfin security na system ko network. Suna gwada yin kutse irin yadda masu kutse sukeyi don gano matsalolin da raunin da mai kutsen zai iya ganowa.
12. Zero-day Exploit: yana nufin Rauni a software ko hardware da company bai sani ba ko bashi da patch dinsa. Masu kutse suna amfani da wannan ne su gudanar da kutse kafin masu kamfani sus ani (zero-day yana nufin ranar da aka san da matsalar)