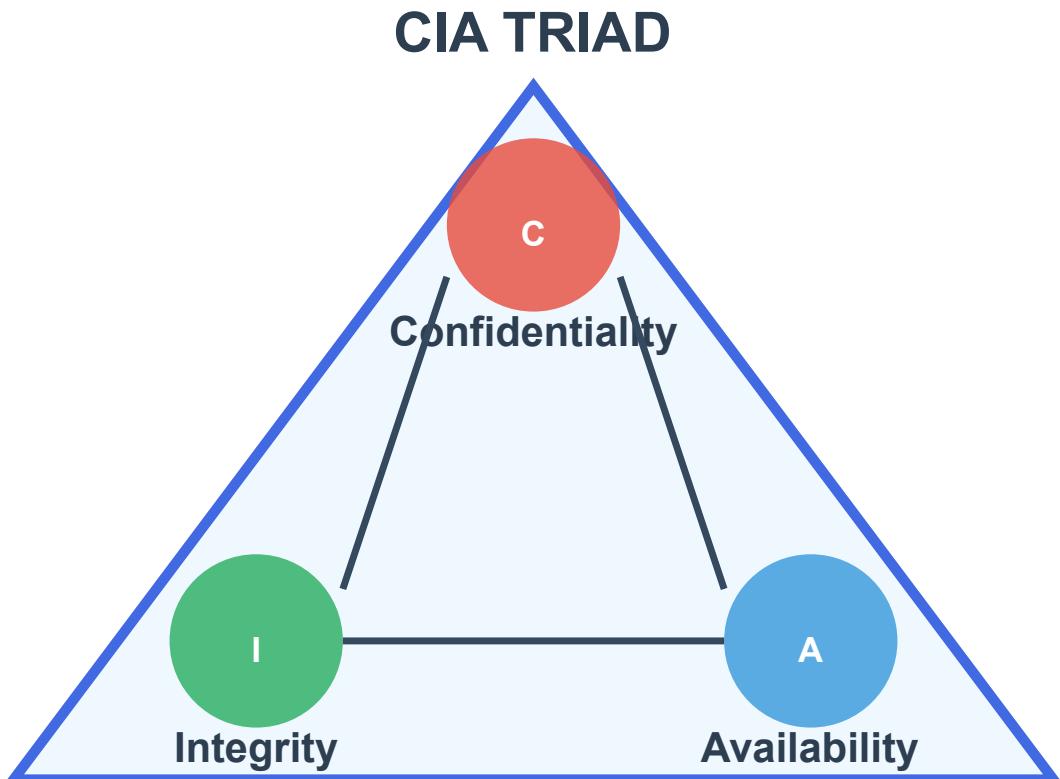


પ્રશ્ન 1(અ) [૩ ગુણા]

ઉદાહરણ સાથે CIA ત્રિપુટીનું વર્ણન કરો.

જવાબ:

CIA ત્રિપુટીના ઘટકો:



ઘટક	વ્યાખ્યા	ઉદાહરણ
કન્ફિડેન્શિયાલિટી	અનધિકૃત એક્સેસથી ડેટાનું રક્ષણ	બેંક એકાઉન્ટ પર પાસવર્ડ પ્રોટોકોલ
ઇન્ટેગ્રિટી	ડેટાની ચોકસાઈ અને સંપૂર્ણતા	ડોક્યુમેન્ટ પર ડિજિટલ સહી
એવેઇલેબિલિટી	જરિયાત મુજબ સિસ્ટમની ઉપલબ્ધતા	24/7 ઓનલાઇન બેંકિંગ સેવાઓ

- કન્ફિડેન્શિયાલિટી:** માત્ર અધિકૃત વપરાશકર્તાઓ જ સંવેદનશીલ માહિતી એક્સેસ કરી શકે
- ઇન્ટેગ્રિટી:** ટ્રાન્સફર દરમિયાન ડેટા ચોકસ અને અપરિવર્તિત રહે
- એવેઇલેબિલિટી:** સિસ્ટમો કાયદેસર વપરાશકર્તાઓ માટે કાર્યરત અને સુલભ રહે

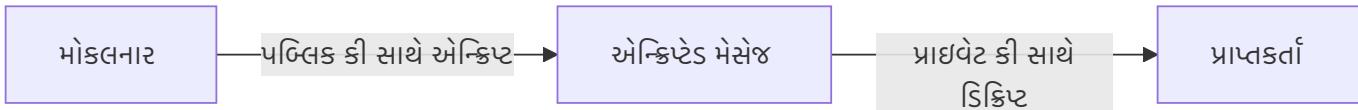
મેમરી ટ્રીક: "CIA માહિતી ને સુરક્ષિત રાખો"

પ્રથન 1(બ) [4 ગુણા]

પદ્ધિલક કી અને પ્રાઇવેટ કી કિષ્ટોગ્રાફી સમજાવો.

જવાબ:

પદ્ધિલક કી કિષ્ટોગ્રાફી (એસિમેટ્રિક):



મુખ્ય લક્ષણો:

વિશેષતા	પદ્ધિલક કી	પ્રાઇવેટ કી
વિતરણ	મુક્તપણે શોર કરાય	ગુપ્ત રાખાય
ઉપયોગ	એન્કિપણ/વેરિફિકેશન	ડિક્રિપ્શન/સાઈનિંગ
સુરક્ષા	જાહેર હોઈ શકે	સુરક્ષિત રાખવી જરૂરી

- પદ્ધિલક કી:** એન્કિપણ અને સિગનેચર વેરિફિકેશન માટે
- પ્રાઇવેટ કી:** ડિક્રિપ્શન અને ડિજિટલ સાઈનિંગ માટે
- સુરક્ષા:** ગાણિતિક જટિલતા પર આધારિત (RSA, ECC અલ્ગોરિદમ)

મેમરી ટ્રીક: "પદ્ધિલક એન્કિપ કરે, પ્રાઇવેટ ડિકિપ કરે"

પ્રથન 1(સ) [7 ગુણા]

OSI મોડેલના દરેક સ્તર સાથે સંકળાયેલ વિવિધ સુરક્ષા હુમલાઓ, પદ્ધતિઓ અને સેવાઓ સમજાવો.

જવાબ:

OSI સુરક્ષા ફેમવર્ક:

સ્તર	હુમલાઓ	પદ્ધતિઓ	સેવાઓ
ફિઝિકલ	વાયરેપિંગ, જોમિંગ	ફિઝિકલ સિક્યોરિટી, શિલ્ડિંગ	એક્સેસ કંટ્રોલ
ડેટા લિંક	MAC ફલડિંગ, ARP પોઇઝનિંગ	એન્જિનિયરિંગ, આથેન્ટિકેશન	ફેમ ઇન્ટેગ્રિટી
નેટવર્ક	IP સ્પૂફિંગ, રાઉટિંગ એટેક	IPSec, ફાયરવોલ	પોકેટ ફિલ્ટરિંગ
ટ્રાન્સપોર્ટ	સેચાન હાઇજોકિંગ, SYN ફલડિંગ	SSL/TLS, પોર્ટ સિક્યોરિટી	અન્ડ-ટુ-અન્ડ સિક્યોરિટી
સેચાન	સેચાન રિપ્લે, હાઇજોકિંગ	સેચાન ટોકન, ટાઇમઆઉટ	સેચાન મેનેજમેન્ટ
પ્રોઝન્ટેશન	ડેટા કરપણ, ફોર્મેટ એટેક	એન્જિનિયરિંગ, કમ્પ્રોશન	ડેટા ટ્રાન્સફોર્મેશન
અેપ્લિકેશન	મેલવેર, સોશિયલ એન્જિનિયરિંગ	અન્ટિવાયરસ, યુઝર ટ્રેનિંગ	અેપ્લિકેશન સિક્યોરિટી

મુખ્ય સુરક્ષા સેવાઓ:

- અથેન્ટિકેશન: યુઝર આઇડન્ટિટી વેરિફિકેશન
- અોથોરાઇઝેશન: એક્સેસ પરમિશન કંટ્રોલ
- નોન-રિપ્યુટિઅન: કિયાઅંનો ઇનકાર અટકાવવો
- ડેટા ઇન્ટેગ્રિટી: ડેટાની થોકસાઈ સુનિશ્ચિત કરવી

મેમરી ટ્રીક: "બધા લોકોને ડેટા પ્રોટોકોલનાની જરૂર છે"

પ્રથમ 1(ક અથવા) [7 ગુણ]

MD5 હેશિંગ અને સિક્યોર હેશ ફંક્શન (SHA) અલાર્મિંગ સમજાવો.

જવાબ:

હેશ ફંક્શન સરખામણી:

વિશેષતા	MD5	SHA-1	SHA-256
આઉટપુટ સાઇઝ	128 બિટ્સ	160 બિટ્સ	256 બિટ્સ
સુરક્ષા સ્તર	નબળું	નબળું	મજબૂત
જડપ	જડપી	મદ્યમ	ધીમું
વર્તમાન સ્થિતિ	અપ્રયાલિત	અપ્રયાલિત	ભલામણ કરેલ



હેશ ગુણધર્મો:

- ડિટર્મિનિસ્ટિક: સમાન ઇનપુટ સમાન હેશ આપે

- અંગેલાન્ચ ઈફેક્ટ: નાનો ઇનપુટ ફેરફાર મોટો હેશ ફેરફાર લાવે
- વન-વે ફંક્શન: હેશથી મૂળ ડેટા મેળવી શકતો નથી
- કોલિજન રેઝિસ્ટ્રેન્ચ: બે અલગ ઇનપુટ માટે સમાન હેશ મળવો મુશ્કેલ

અંગેલાન્ચ ફંક્શન:

- પાસવર્ડ સ્ટોરેજ અને વેરિફિકેશન
- ડિજિટલ સિગનેચર અને સર્ટિફિકેટ
- ડેટા ઇન્ટેગ્રેશન યેકિંગ

મેમરી ટ્રીક: "હેશ હંમેશા સમાન આઉટપુટ આપે"

પ્રથન 2(અ) [3 ગુણા]

ફાયરવોલ થું છે? તેના પ્રકારોની યાદી આપો.

જવાબ:

ફાયરવોલ વ્યાખ્યા:

નેટવર્ક સિક્યુરિટી ડિવાઇસ જે સુરક્ષા નિયમોના આધારે આવતા-જતા ટ્રાફિકને મોનિટર અને કંટ્રોલ કરે છે.

ફાયરવોલના પ્રકારો:

પ્રકાર	ફંક્શન	સ્તર
પેકેટ ફિલ્ટર	પેકેટ હોડર તપાસે	નેટવર્ક લેયર
સ્ટેટકુલ	કનેક્શન સ્ટેટ ટ્રેક કરે	ટ્રાન્સપોર્ટ લેયર
અંગેલાન્ચ પ્રોક્સી	અંગેલાન્ચ ડેટા તપાસે	અંગેલાન્ચ લેયર
પર્સનલ ફાયરવોલ	વ્યક્તિગત ડિવાઇસ સુરક્ષા	હોસ્ટ-બેસ્ડ

- હાર્ડવેર ફાયરવોલ: સમર્પિત નેટવર્ક ઉપકરણ
- સોફ્ટવેર ફાયરવોલ: વ્યક્તિગત કમ્પ્યુટર પર ઇન્સ્ટોલ
- કલાઉડ ફાયરવોલ: સેવા તરીકે પૂરો પાડવામાં આવે (FWaaS)

મેમરી ટ્રીક: "ફાયરવોલ હંમેશા નેટવર્કનું રક્ષણ કરે"

પ્રથન 2(બ) [4 ગુણા]

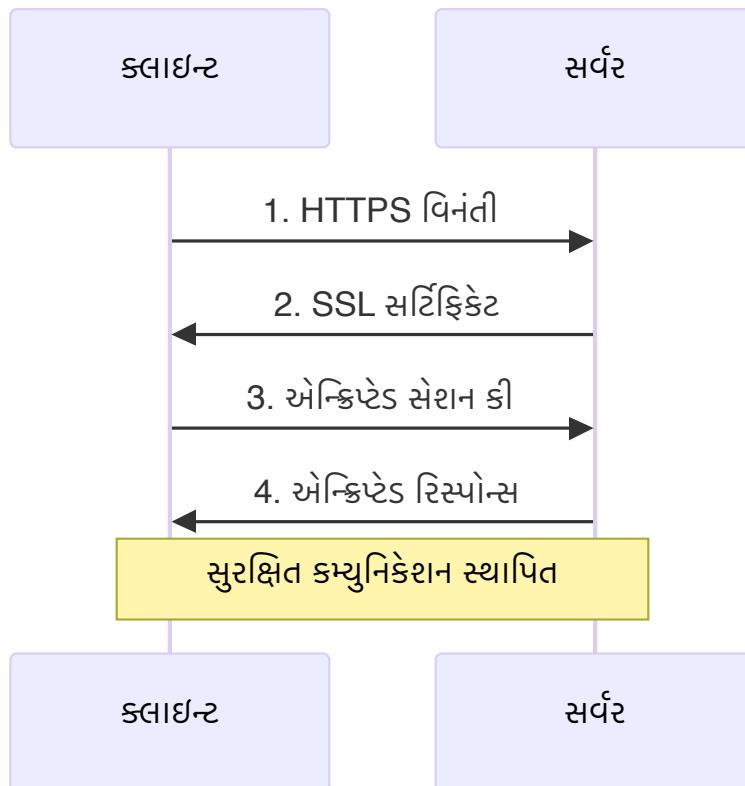
વ્યાખ્યાચિત કરો: HTTPS અને HTTPS ના કાર્યનું વર્ણન કરો.

જવાબ:

HTTPS વ્યાખ્યા:

Hypertext Transfer Protocol Secure - SSL/TLS એન્ક્રિપ્શન પર HTTP.

HTTPS કાર્ય પ્રક્રિયા:



HTTPS ઘટકો:

- પોર્ટ 443: સ્ટાન્ડર્ડ HTTPS પોર્ટ
- SSL/TLS: એન્ક્રિપ્શન પ્રોટોકોલ
- ડિજિટલ સર્ટિફિકેટ: સર્વર ઓથેન્ટિકેશન
- સિમેટ્રિક એન્ક્રિપ્શન: ડેટા ટ્રાન્સમિશન

ફાયદાઓ:

- ટ્રાન્સમિશન દરમિયાન ડેટા એન્ક્રિપ્શન
- સર્વર ઓથેન્ટિકેશન વેરિફિકેશન
- ડેટા ઇન્ટેગ્રિટી પ્રોટોકોલ
- SEO રેંકિંગ સુધારો

મેમરી ટ્રીક: "HTTPS વેબ ટ્રાફિકને સુરક્ષિત કરે"

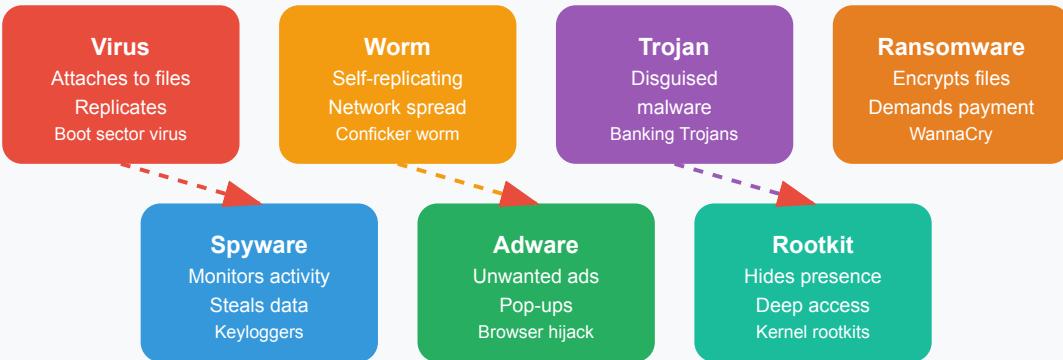
પ્રશ્ન 2(સ) [7 ગુણ]

વિવિધ પ્રકારના દુર્ભાવનાપૂર્ણ સોફ્ટવેર અને તેમની અસર સમજાવો.

જવાબ:

મેલવેર વર્કિંગ્ઝેડ:

Malware Classification



Effects on Systems



Prevention Methods

- Regular antivirus updates
- Safe browsing practices
- Email attachment caution
- System security patches

Malware Infection Chain

પ્રકાર	વર્તન	અસર	ઉદાહરણ
વાયરસ	ફાઈલો સાથે જોડાય	ફાઈલ કરાયાન	બૂટ સેક્ટર વાયરસ
વોર્મ	સ્વ-પ્રતિકૂટિ	નેટવર્ક ભીડ	કન્ફિકર વોર્મ
ટ્રોજન	ઇભવેશી મેલવેર	ડેટા ચોરી	બોંકિંગ ટ્રોજન
રેન્સમ્વેર	ફાઈલો ઓન્ફિલ કરે	ડેટા બંધક	WannaCry
સ્પાયવેર	પ્રવૃત્તિ મોનિટર કરે	ગોપનીયતા લંગ	કીલોગાર
એડવેર	અનચાહેલી જાહેરાતો	પ્રદર્શન ઘટાડો	પોપ-અપ જાહેરાતો
રૂટકિટ	હાજરી છુપાવે	સિસ્ટમ સમાધાન	કર્નલ રૂટકિટ

સિસ્ટમ પર અસરો:

- પ્રદર્શન:** ધીમી સિસ્ટમ પ્રતિક્રિયા
- ડેટા:** નુકસાન, કરાયાન અથવા ચોરી
- ગોપનીયતા:** અનધિકૃત મોનિટરિંગ
- નાણાકીય:** પ્રત્યક્ષ નાણાકીય નુકસાન

રોકથામના પદ્ધતિઓ:

- નિયમિત એન્ટિવાયરસ અપડેટે
 - સુરક્ષિત બ્રાઉઝિંગ પ્રેક્ટિસ
 - ઇમેઇલ એટોયમેન્ટમાં સાવધાની
 - સિસ્ટમ સિક્યુરિટી પેચ

ਮੇਮਰੀ ਡ੍ਰੀਕ: "ਵਾਧਰਸ ਵੋਰਮ ਟ੍ਰੋਜਨ ਖੋਲ੍ਹੇ ਬਦਾ ਸੰਸਾਧਨੋ ਚੋਠੇ"

પ્રશ્ન 2(અ અથવા) [3 ગુણ]

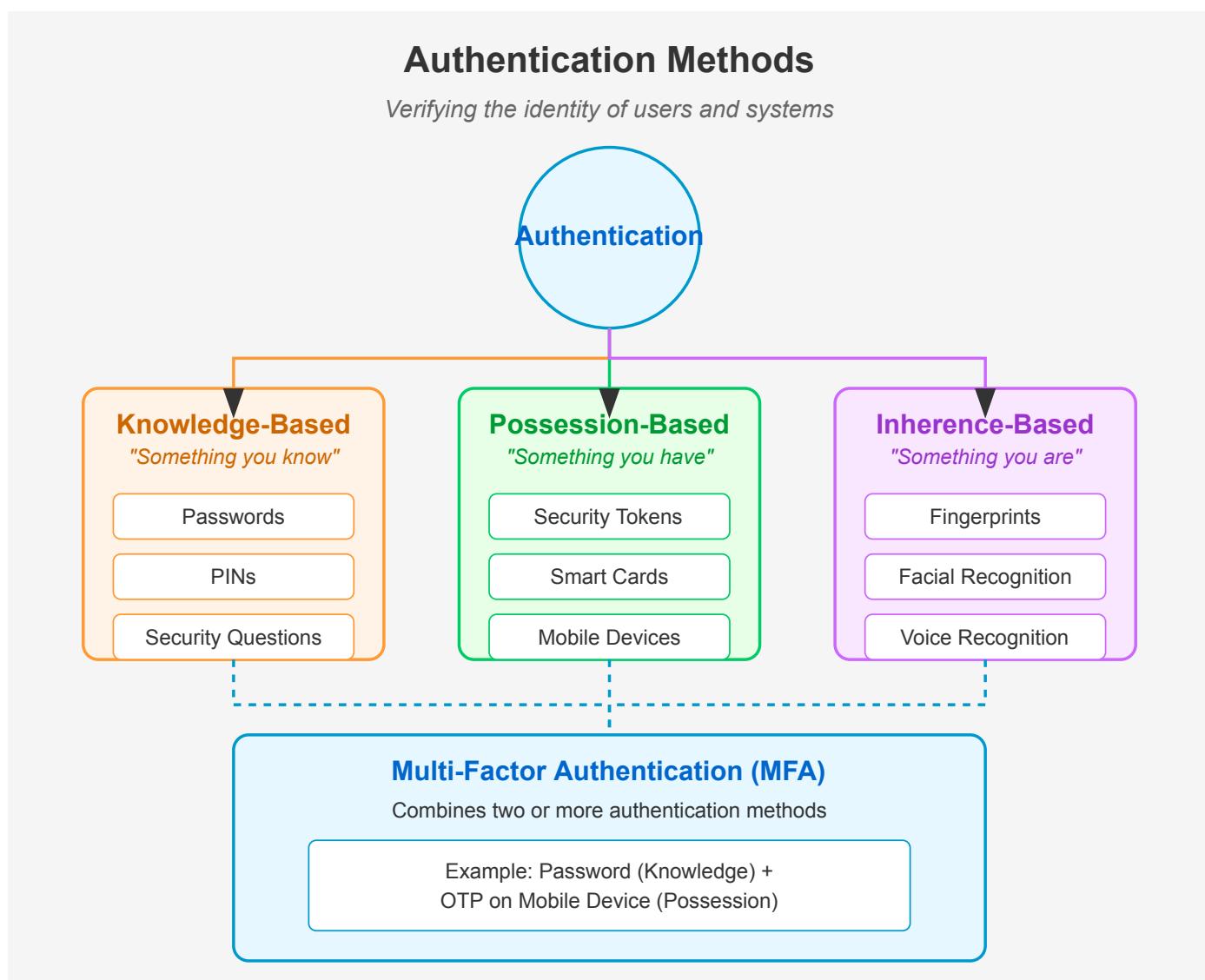
પ્રમાણીકરણ(ઓયેન્ટિકેશન) શું છે? પ્રમાણીકરણ(ઓયેન્ટિકેશન) ની વિવિધ પદ્ધતિઓ સમજવો.

ੴ ਪ੍ਰਾਣੀ

ઓથેન્ટિકેશન વ્યાખ્યા:

સિસ્ટમ એકસેસ આપતા પહેલા યાર આઇડેન્ટિટી વેરિફાઇ કરવાની પ્રક્રિયા.

ઓથેન્ટિકેશન પદ્ધતિઓ:



પદ્ધતિ	વર્ણન	ઉદાહરણ
પાસવર્ડ	તમે જે જાણો છો	PIN, પાસવર્ડ
બાયોમેટ્રિક	તમે જે છો	ફિંગરપ્રિન્ટ, આઇરિસ
ટોકન	તમારી પાસે જે છે	સ્માર્ટ કાર્ડ, USB કી

- સિંગલ-ફેક્ટર:** અંક ઓથેન્ટિકેશન પદ્ધતિ વાપરે
- મલ્ટિ-ફેક્ટર:** અનેક પદ્ધતિઓ જોડે
- કુ-ફેક્ટર (2FA):** બરાબર બે ફેક્ટર વાપરે

મેમરી ટ્રીક: "પાસવર્ડ બાયોમેટ્રિક ટોકન ઓથેન્ટિકેશન"

પ્રથન 2(બ અથવા) [4 ગુણ]

વ્યાખ્યાયિત કરો: ટ્રોજન્સ, રૂટકિટ, બેકડોર્સ, કીલોગર

જવાબ:

મેલવેર વ્યાખ્યાઓ:

શાદી	વ્યાખ્યા	લક્ષણો
ટ્રોજન્સ	કાયદેસર સોફ્ટવેરના છઘવેશમાં મેલવેર	હાનિકારક દેખાય, છુપાયેલ પેલોડ
રૂટકિટ	મેલવેરની હાજરી છુપાવતો સોફ્ટવેર	ઉંડી સિસ્ટમ એક્સેસ, સ્ટેલ્ટ્ય ઓપરેશન
બેકડોર્સ	અનધિકૃત એક્સેસ પદ્ધતિ	સામાન્ય ઓથેન્ટિકેશન બાયપાસ કરે
કીલોગર	કીબોર્ડ ઇનપુટ રેકોર્ડ કરે	પાસવર્ડ, સંવેદનશીલ ડેટા કેચર કરે

- ટ્રોજન્સ:** ગ્રીક ટ્રોજન હોર્સ પરથી નામ
- રૂટકિટ:** કર્નલ લેવલ પર કામ કરે
- બેકડોર્સ:** હાર્ડવેર અથવા સોફ્ટવેર આધારિત હોઈ શકે
- કીલોગર:** સોફ્ટવેર અથવા હાર્ડવેર ડિવાઇસ હોઈ શકે

મેમરી ટ્રીક: "ટ્રોજન રૂટ બેકડોર કીલોગ"

પ્રથન 2(ક અથવા) [7 ગુણ]

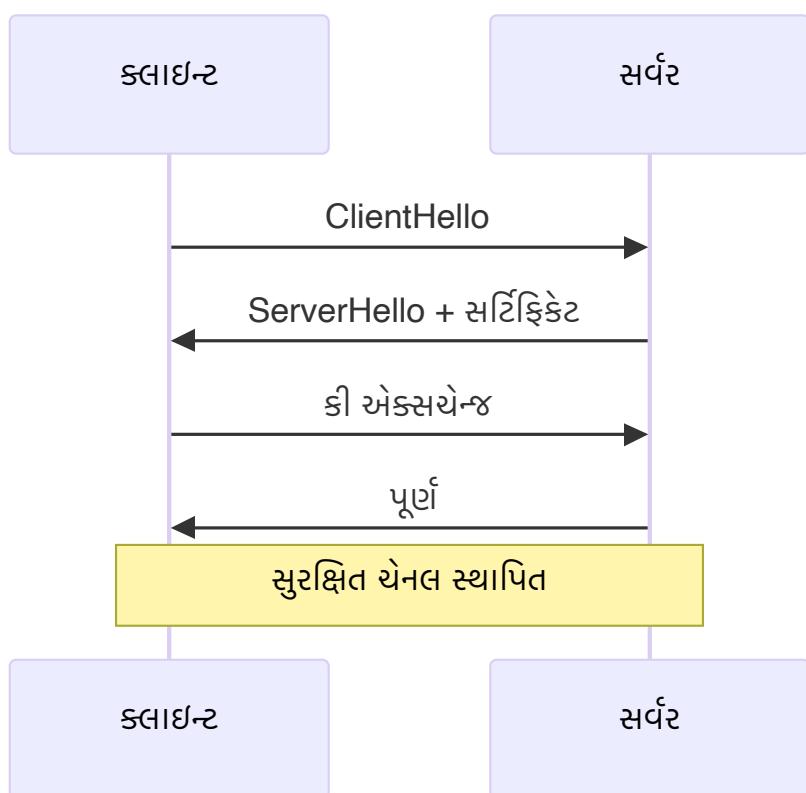
સિક્યોર સોકેટ લેયર (SSL) અને ટ્રાન્સપોર્ટ લેયર સિક્યોરિટી (TLS) મ્રોટોકોલ સમજાવો.

જવાબ:

SSL/TLS મ્રોટોકોલ ઉત્કાંતિ:

વર્ગન	વર્ષ	સ્થિતિ	સુરક્ષા સ્તર
SSL 2.0	1995	અપ્રયાલિત	નબળું
SSL 3.0	1996	અપ્રયાલિત	સંવેદનશીલ
TLS 1.0	1999	લેગસી	મયાર્દિત
TLS 1.2	2008	વ્યાપક ઉપયોગ	સાંચું
TLS 1.3	2018	વર્તમાન	મજબૂત

TLS હેન્ડશેક પ્રક્રિયા:



મુખ્ય વિશેષતાઓ:

- અનિક્રિપ્શન: સિમેટ્રિક અને એસિમેટ્રિક અલ્ગોરિદમ
- ઓથેરિન્કેશન: સર્વર અને કલાયન્ટ વેરિફિકેશન
- ઇન્ટેગ્રિટી: મેસેજ ઓથેરિન્કેશન કોડ
- ફોરવર્ડ સિકેસી: સેશન કી પ્રોટોકોલ

અપ્લિકેશન:

- HTTPS વેબ બ્રાઉઝિંગ
- ઇમેઇલ સિક્યુરિટી (SMTPS)
- VPN કનેક્શન
- સુરક્ષિત ફાઇલ ટ્રાન્સફર

મેમરી ટ્રીક: "TLS બધા નેટવર્ક ટ્રાફિકને એન્ક્રિપ્ટ કરો"

પ્રથન 3(અ) [૩ ગુણ]

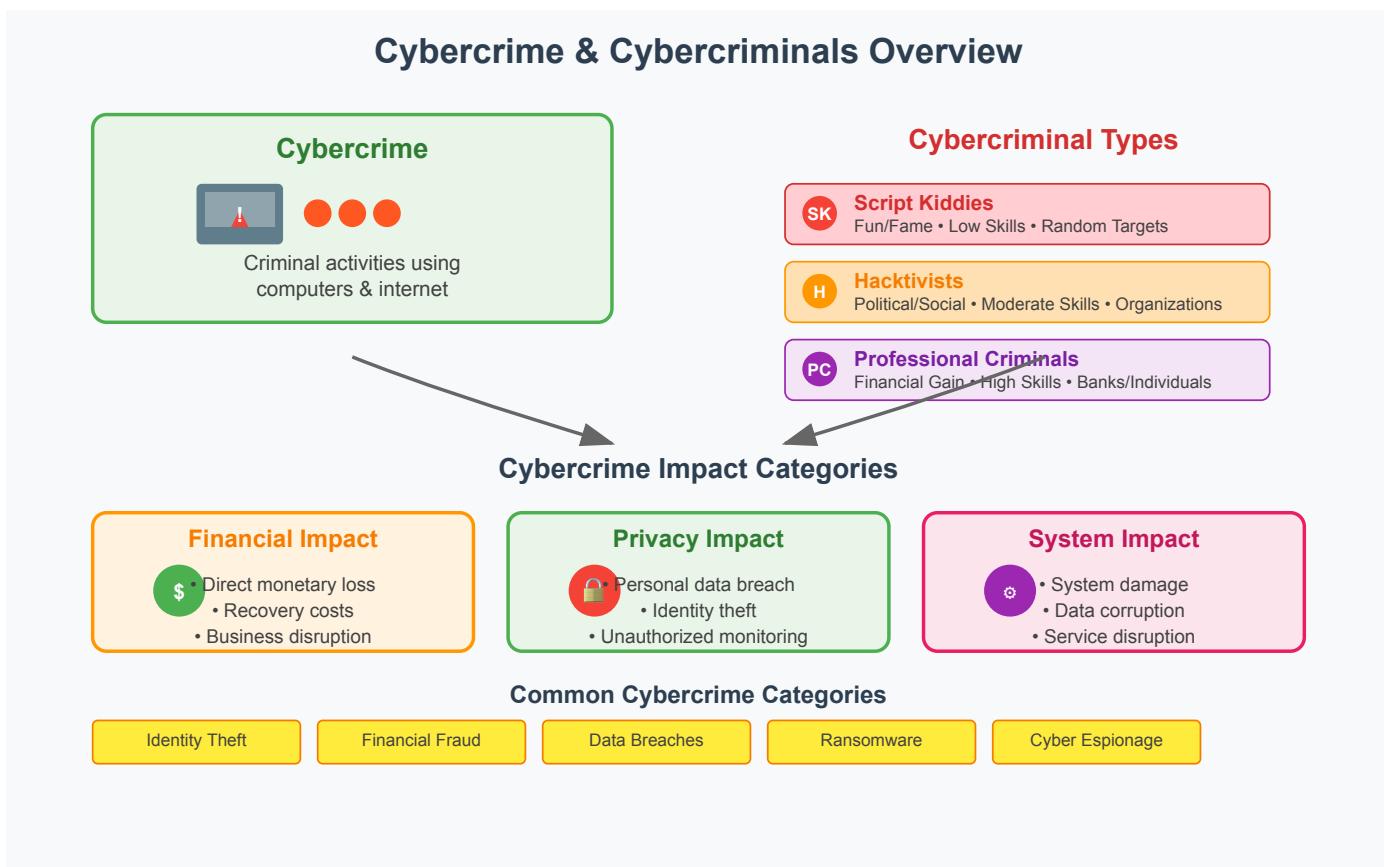
સાયબર કાઇમ અને સાયબરકિલ્ડિનિલ ને વિગતવાર સમજાવો.

જવાબ:

સાયબર કાઇમ વ્યાખ્યા:

કમચુટ્ટર અથવા ઇન્ટરનેટ નેટવર્ક દ્વારા કરવામાં આવતી ગુનાહિત પ્રવૃત્તિઓ.

ડાયાગ્રામ:



સાયબરકિલ્ડિનિલ પ્રકારો:

પ્રકાર	પ્રેરણા	કુશળતા	લક્ષ્ય
સ્ક્રિપ્ટ કિડીઝ	મજા/પ્રસિદ્ધિ	અોછી	અવ્યવસ્થિત
હેક્ટિવિસ્ટ	રાજકીય/સામાજિક	મદ્યમ	સંસ્થાઓ
સાયબરકિલ્ડિનિલ	નાણાકીય લાભ	ઉચ્ચ	વ્યક્તિઓ/બેંકો

- સાયબર કાઇમ:** ડિજિટલ ટેકનોલોજીનો ઉપયોગ કરીને ગોરકાયદેસર પ્રવૃત્તિઓ
- સાયબરકિલ્ડિનિલ:** સાયબર કાઇમ કરનાર વ્યક્તિ
- અસર:** નાણાકીય નુકસાન, ગોપનીયતા ભંગ, સિસ્ટમ નુકસાન

મેમરી ટ્રીક: "સાયબર કિલ્ડિનિલો અરાજકતા સર્જે છે"

પ્રશ્ન 3(બ) [4 ગુણા]

સાયબર સ્ટોકિંગ અને સાયબર બુલીંગ નું વર્ણન કરો.

જવાબ:

ડિજિટલ પજવણી સરખામણી:

પાસું	સાયબર સ્ટોકિંગ	સાયબર બુલીંગ
લક્ષ્ય	વિશિષ્ટ વ્યક્તિ	મોટેભાગે નાભાલિંગાં
અવધિ	સતત, લાંબા ગાળાની	એપિસોડિક હોઇ શકે
હેતુ	ભીતિ, નિયંત્રણ	પજવણી, અપમાન
પ્લેટફોર્મ	સોશિયલ મીડિયા, ઇમેઇલ	શાળાઓ, ગોમિંગ પ્લેટફોર્મ

સાયબર સ્ટોકિંગ લક્ષણો:

- સતત અનયાહેલ સંપર્ક
- પીડિતની આોનલાઈન પ્રવૃત્તિનું મોનિટરિંગ
- ધમકીલર્યા સંદેશાઓ અથવા વર્તન
- આોટખની થોડી અથવા ઢોંગા

સાયબર બુલીંગ સ્વરૂપો:

- આોનલાઈન જાહેર અપમાન
- ડિજિટલ જૂથોમાંથી બાકાત
- ખોટી માહિતી ફેલાવવી
- સંમતિ વિના ખાનગી સામગ્રી શેર કરવી

રોકથામના પગલાં:

- સોશિયલ મીડિયા પર ગોપનીયતા સેટિંગ્સ
- પ્લેટફોર્મને પજવણીની જાણ કરવી
- જરૂર પડે ત્યારે કાયદેસીની કાર્યવાહી
- ડિજિટલ સાક્ષરતા શિક્ષણ

મેમરી ટ્રીક: "બુલીંગ બંધ કરો, સ્ટોકિંગની જાણ કરો"

પ્રશ્ન 3(સ) [7 ગુણા]

સાયબર કાઇમમાં પ્રોપટી બેઝિઝડ કલાસિફિકેશન સમજાવો.

જવાબ:

પ્રોપટી-આધારિત સાયબર કાઇમ શ્રેણીઓ:

Cybercrime & Cybercriminal Classification

Cybercrime Definition

Criminal activities conducted through computers or internet networks

Script Kiddies

Motivation: Fun/Fame
Skills: Low
Target: Random
Use pre-made tools

Hacktivists

Motivation: Political/Social
Skills: Moderate
Target: Organizations
Ideological goals

Cybercriminals

Motivation: Financial
Skills: High
Target: Banks/Individuals
Profit-driven

Impact of Cybercrime

Financial Loss

Direct monetary damage

Privacy Breach

Personal data exposure

System Damage

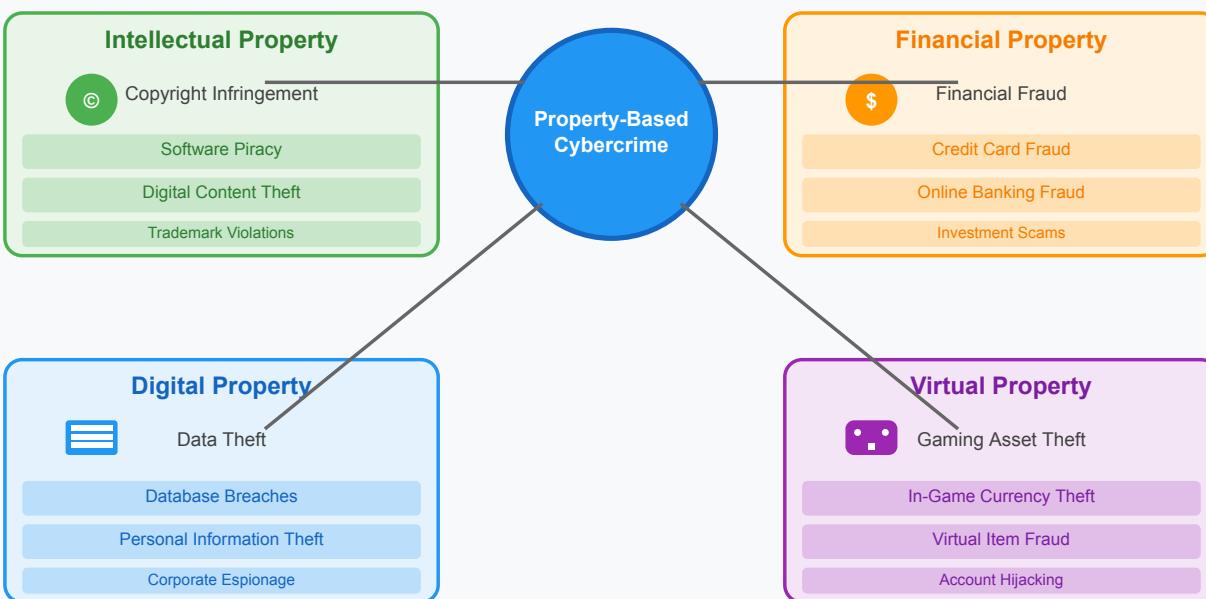
Infrastructure disruption

Skill Level & Threat Sophistication Increases →

શ્રેણી	કાઇમ પ્રકાર	વર્ણન	ઉદાહરણ
બૌદ્ધિક સંપત્તિ	કોપીરાઇટ ઉલ્લંઘન	કોપીરાઇટ સામગ્રીનો અનધિકૃત ઉપયોગ	સોફ્ટવેર પાયરેસી
નાણાકીય સંપત્તિ	કેડિટ કાર્ડ ફોડ	નાણાકીય માહિતીનો અનધિકૃત ઉપયોગ	અંનલાઈન શોપિંગ ફોડ
ડિજિટલ સંપત્તિ	ડેટા ચોરી	ડિજિટલ માહિતીની ચોરી	ડેટાબેસ ભ્રીચ
વર્ષ્યુઅલ સંપત્તિ	ગોમિંગ એસેટ ચોરી	વર્ષ્યુઅલ વસ્તુઓની ચોરી	અંનલાઈન ગોમ કરન્સી ચોરી

ડાયાગ્રામ:

Property-Based Cybercrime Classification



Economic Impact on Industries

Software Industry \$90B+ annually

Banking Sector \$18B+ annually

Gaming Industry \$3B+ annually

Media & Entertainment \$52B+ annually

Copyright Laws

Trademark Laws

Patent Laws

Trade Secret Laws

Cyber Crime Laws

કાયદેસરના પાસાઓ:

- કોપીરાઇટ કાયદાઓ: સર્જનાત્મક કાર્યોનું રક્ષણ
- ટ્રેડમાર્ક કાયદાઓ: બ્રાન્ડ અ૱ન્ડિન્ગનું રક્ષણ
- પેટ-ન કાયદાઓ: આવિજ્ઞારોનું રક્ષણ
- ટ્રેડ સિકેટ કાયદાઓ: ગોપનીય માહિતીનું રક્ષણ

અર્થતંત્ર પર અસર:

- કાયદેસર વ્યવસાયો માટે આવકનું નુકસાન
- નવીનતાની પ્રેરણામાં ઘટાડો
- ગ્રાહક વિશ્વાસનું ધોવાળા
- કાયદેસર અમલીકરણના ખર્ચ

રોકથામ વ્યૂહરચનાઓ:

- ડિજિટલ રાઇટ્સ મેનેજમેન્ટ (DRM)
- વોટરમાર્કિંગ અને ટ્રેકિંગ
- કાયદેસર અમલીકરણ મિકેનિક્ઝમ
- જાહેર જાગૃતિ ચૂંબેશા

મેમરી ટ્રીક: "પ્રોપર્ટી પ્રોટેક્શન પાયરેસી અટકાવે"

પ્રશ્ન 3(અ અથવા) [3 ગુણ]

ડેટા ડિડલિંગ સમજાવો.

જવાબ:

ડેટા ડિડલિંગ વ્યાખ્યા:

કમ્પ્યુટર સિસ્ટમમાં ડેટા દાખલ કરતા પહેલા અથવા દરમિયાન અનધિકૃત ફેરફાર.

લક્ષણો:

પાસું	વર્ણન
પદ્ધતિ	ડેટા વેલ્યુમાં ફેરફાર
સમય	સિસ્ટમ પ્રોસેસિંગ પહેલા
શોધ	ઘણીવાર ઓળખવું મુશ્કેલ

- ઉદાહરણો:** સેલેરી આંકડાઓમાં ફેરફાર, પરીક્ષાના સ્કોરમાં ફેરફાર
- લક્ષ્ય:** એન્ટ્રી પ્રક્રિયા દરમિયાન ઇનપુટ ડેટા
- અસર:** નાણાકીય નુકસાન, ખોટા રેકૉર્ડ

મેમરી ટ્રીક: "ડેટા ડિડલિંગ ડેટાબેસને નુકસાન પહોંચાડે"

પ્રશ્ન 3(બ અથવા) [4 ગુણ]

સાયબર સ્પાઇંગ અને સાયબર ટેરરીઝમ સમજાવો.

જવાબ:

સાયબર ધમકીઓની સરખામણી:

Cyber Spying vs. Cyber Terrorism

Cyber Spying



Purpose:

- Information gathering
- Intelligence collection
- Competitive advantage
- Strategic planning

Targets:

- Government agencies
- Military organizations
- Corporations
- Research institutions

Methods:

- Stealth infiltration
- Social engineering
- Malware implantation
- Network monitoring

Impact:

- Intelligence loss

Cyber Terrorism



Purpose:

- Causing fear and panic
- Mass disruption
- Political influence
- Ideological agenda

Targets:

- Critical infrastructure
- Power grids
- Financial systems
- Transportation networks

Methods:

- Destructive attacks
- DDoS campaigns
- System sabotage
- Psychological warfare

Impact:

- Public safety risk

Stealth & Secrecy

VS

Visibility & Fear

પાસું	સાયબર સ્પાઈંગ	સાયબર ટેરરીઝમ
હેતુ	માહિતી અંકત્રીકરણ	ભય/વિકષેપ સર્જવો
લક્ષ્ય	સરકાર, કોર્પોરેશન	નિર્ધારક ઇન્ફાસ્ટ્રક્ચર
પદ્ધતિઓ	છુપી ઘૂસણાખોરી	વિનાશક હુમલાઓ
અસર	ગુપ્ત માહિતીનું નુકસાન	જાહેર સુરક્ષા જોખમ

સાયબર સ્પાઈંગ પ્રવૃત્તિઓ:

- કોર્પોરેટ જાસ્તુસી
- સરકારી દેખરેખ
- ડ્રેસ સિકેટ થોરી
- વ્યક્તિગત માહિતી અંકત્રીકરણ

સાયબર ટેરરીઝમ પદ્ધતિઓ:

- ઇન્ફાસ્ટ્રક્ચર હુમલાઓ
- મોટા પાયે વિકષેપ જુબેશ
- મનોવૈજ્ઞાનિક યુદ્ધ

- આર્થિક નુકસાન

ચોકથામના પગલાં:

- નેટવર્ક સિક્યુરિટી મોનિટરિંગ
- ઘટના પ્રતિક્રિયા આયોજન
- અંતરરાજ્યીય સહયોગ
- જાહેર-ખાનગી ભાગીદારી

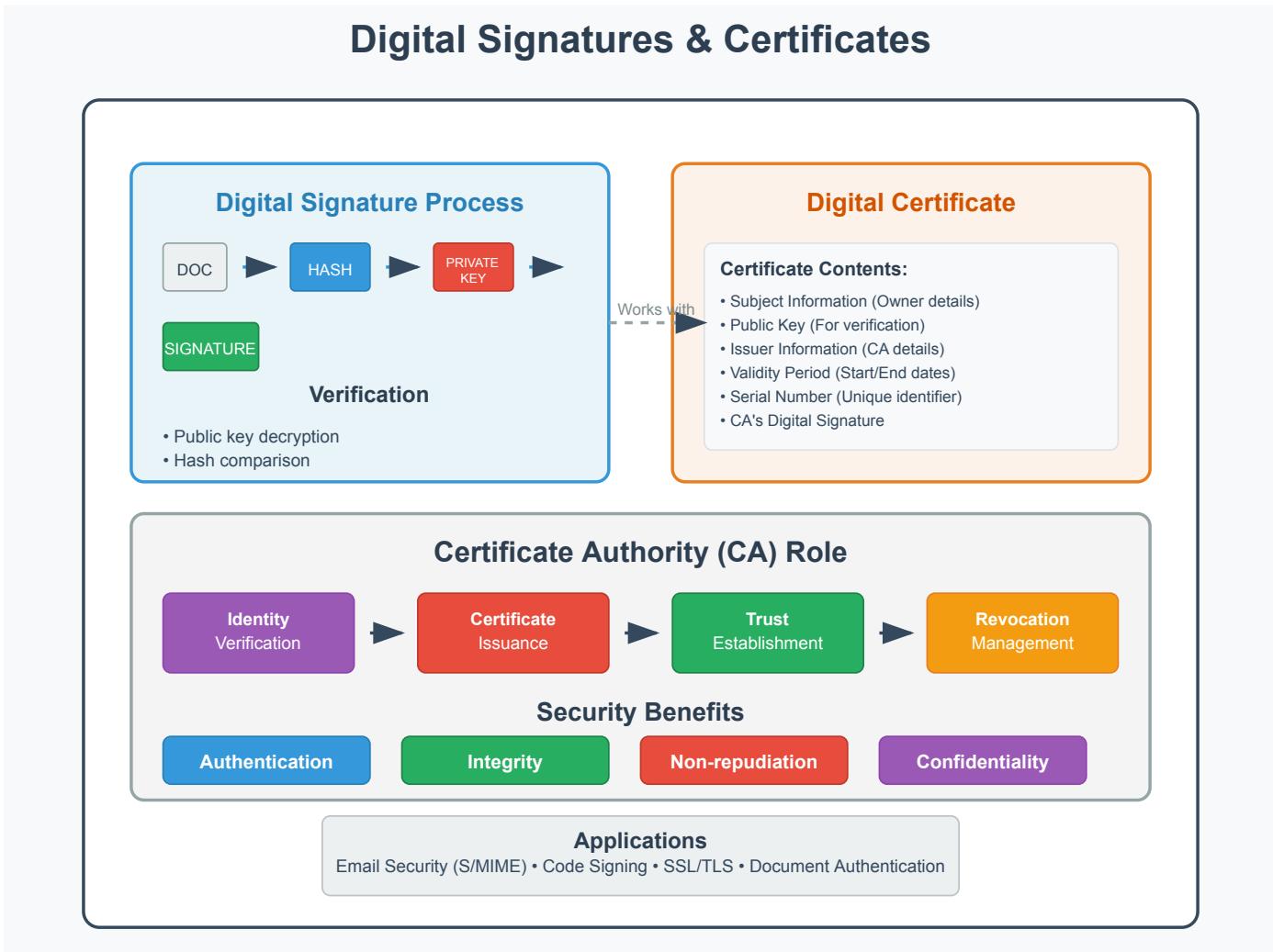
મેમરી ટ્રીક: "જાસૂસો થોરે, આતંકવાદીઓ આતંક"

પ્રથન 3(ક) અથવા) [7 ગુણ]

સાયબર સુરક્ષામાં ડિજિટલ સહીઓ અને ડિજિટલ પ્રમાણપત્રોની લૂભિકા સમજવો.

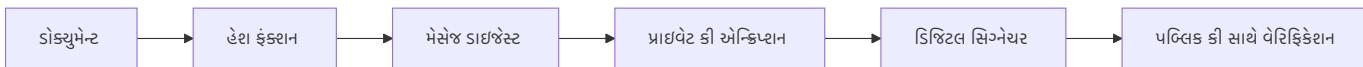
જવાબ:

ડિજિટલ સુરક્ષા ઘટકો:



ઘટક	હેતુ	ફંકશન	ફાયદો
ડિજિટલ સિગનેચર	અંદેન્ટેક્ચેન	મોકલનારની ઓળખ સાબિત કરે	નોન-રિપ્યુટાશન
ડિજિટલ સર્ટિફિકેટ	વેરિફિકેશન	પરિલક કીની માન્યતા	વિશ્વાસ સ્થાપના

ડિજિટલ સિગનેચર પ્રક્રિયા:



ડિજિટલ સર્ટિફિકેટ ઘટકો:

- વિષય માહિતી: સર્ટિફિકેટ માલિકની વિગતો
- પબ્લિક કી: એન્ક્રિપ્શન/વેરિફિકેશન માટે
- ડિજિટલ સિગનેચર: CA ની સહી
- માન્યતા અવધિ: સર્ટિફિકેટની સમાપ્તિ તારીખ

સર્ટિફિકેટ ઓથોરિટી (CA) લૂભિકા:

- ડિજિટલ સર્ટિફિકેટ જારી કરે
- જારી કરતા પહેલા ઓળખ ચકાસે
- સર્ટિફિકેટ રદ કરવાની યાદીઓ જાળવે
- વિશ્વાસ ઇન્ફાસ્ટ્રક્ચર પૂરું પાડે

સાયબર સિક્યોરિટીમાં એપ્લિકેશન:

- ઇમેઇલ સિક્યોરિટી (S/MIME)
- સોફ્ટવેર માટે કોડ સાઇનિંગ
- વેબસાઈટો માટે SSL/TLS સર્ટિફિકેટ
- ડોક્યુમેન્ટ ઓથેન્ટિકેશન

સુરક્ષા ફાયદાઓ:

- ઓથેન્ટિકેશન: મોકલનારની ઓળખ ચકાસે
- ઇન્સ્ટ્રીટી: ડેટામાં ફેરફાર થયો નથી તેની ખાતરી
- નોન-રિપ્યુટેશન: કિયાઅંનો ઇનકાર અટકાવે
- ગોપનીયતા: સુરક્ષિત કમ્પ્યુનિકેશન સક્ષમ કરે

મેમરી ટ્રીક: "ડિજિટલ સિગનેચર ડોક્યુમેન્ટને સુરક્ષિત રીતે પ્રમાણિત કરે"

પ્રદાન 4(અ) [૩ ગુણા]

હેકિંગ શું છે? હેકર્સના પ્રકારોની યાદી બનાવો.

જવાબ:

હેકિંગ વ્યાખ્યા:

નબળાઈઅંગોનો ફાયદો ઉઠાવવા માટે કમ્પ્યુટર સિસ્ટમ અથવા નેટવર્કમાં અનધિકૃત એક્સેસ.

હેકર વર્ગીકરણ:

Types of Hackers

Hacker Classification by Intent

White Hat	Black Hat	Gray Hat
Ethical Hackers Intent: Security improvement Legal Status: Authorized Examples: <ul style="list-style-type: none">Penetration testersSecurity researchers	Malicious Hackers Intent: Malicious activities Legal Status: Illegal Examples: <ul style="list-style-type: none">CybercriminalsData thieves	Ambiguous Hackers Intent: Mixed motivations Legal Status: Questionable Examples: <ul style="list-style-type: none">Unauthorized researchersVigilante hackers

Additional Hacker Categories

Script Kiddie	Hacktivist	State-Sponsored	Insider Threat
• Uses existing tools • Limited technical skills • Motivated by attention • Often young/inexperienced	• Political motivations • Social activism • Protest through hacking • Groups like Anonymous	• Government backed • Advanced capabilities • National security goals • APT groups	• Internal access • Legitimate credentials • Abuse of trust • Hardest to detect

Motivation Spectrum

Ethical Financial Political Malicious Espionage

Legal Gray Area Illegal

પ્રકાર	હેતુ	કાયદેસર સ્થિતિ
ધાઈટ હેઠ	સુરક્ષા સુધારણા	કાયદેસર
જ્લેક હેઠ	દુર્ભાવનાપૂર્ણ પ્રવૃત્તિઓ	ગોરકાયદેસર
ગ્રે હેઠ	મિશ્ર પ્રેરણા	શંકાસ્પદ

- ધાઈટ હેઠ: નૈતિક હેકર, સુરક્ષા સંશોધકો
- જ્લેક હેઠ: સાયબરક્રિમિનલ, દુર્ભાવનાપૂર્ણ હેતુ
- ગ્રે હેઠ: કેટલીકવાર કાયદેસર, કેટલીકવાર નહીં

મેમરી ટ્રીક: "સફેદ સારું, કાળું ખરાબ, ગ્રે શંકાસ્પદ"

પ્રથન 4(બ) [4 ગુણા]

હેકિંગની વલન્રેબિલિટી અને 0-દિવસની પરિલાખા સમજાવો.

જવાબ:

સુરક્ષા પરિલાખા:

શાબ્દ	વ્યાખ્યા	જોખમ સ્તર	ઉદાહરણ
વલનરેબિલિટી	સિસ્ટમની નબળાઈ	વિવિધ	અનપેચ સોફ્ટવેર
0-દિવસ	અજાણી નબળાઈ	ગંભીર	અશોધાયેલી ખામી

વલનરેબિલિટી લક્ષણો:

- શોધ: સુરક્ષા પરીક્ષણ દ્વારા મળે
- જાહેરાત: વેન્ડરને જવાબદાર રિપોર્ટિંગ
- પેચિંગ: વેન્ડર સુરક્ષા અપડેટ પૂરું પાડે
- વિંડો: શોધ અને પેચ વચ્ચેનો સમય

0-દિવસ હુમલો પ્રક્રિયા:

- ઠેકર અજાણી નબળાઈ શોધે
- વેન્ડરની જાણકારી પહેલા ખામીનો ફાયદો ઉઠાવે
- કોઈ ઉપલબ્ધ પેચ અથવા સંરક્ષણ નથી
- આશ્વર્યના કારણે ઉચ્ચ સફળતા દર

સંરક્ષણ વ્યૂહરચના:

- નિયમિત સુરક્ષા અપડેટ
- ઇન્ટ્રોડ્યુક્શન ડિટેક્શન સિસ્ટમ
- વર્તાણૂકીય વિશ્લેષણ સાધનો
- ઝીરો-ટ્રસ્ટ સુરક્ષા મોડેલ

મેમરી ટ્રીક: "નબળાઈઓને પેચની જરૂર, ઝીરો-કેને સાવયેતીની જરૂર"

પ્રથન 4(ક) [7 ગુણ]

ઠેકિંગના પાંચ સ્ટેપ્સ સમજાવો.

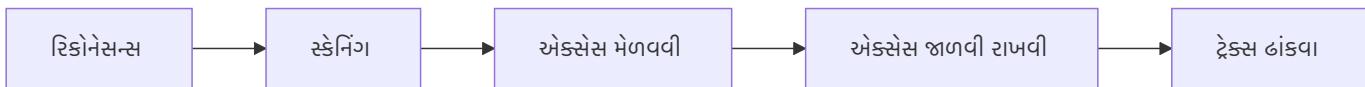
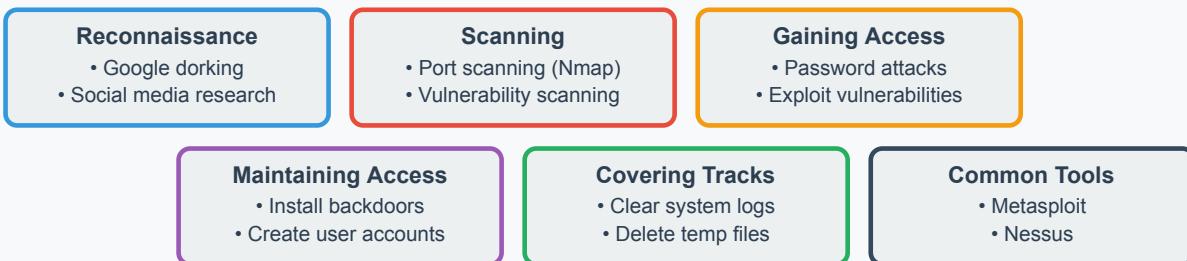
જવાબ:

ઠેકિંગ પદ્ધતિ:

Five Steps of Hacking



Detailed Activities



વિગતવાર પગલાંઓ:

પગલું	વર્ણન	સાધનો/પદ્ધતિઓ	ઉદ્દેશ્ય
રિકોનેસન્સ	માહિતી અભેક્ટીકરણ	Google dorking, સોશિયલ મીડિયા	લક્ષ્ય પ્રોફાઇલિંગ
સ્કેનિંગ	સિસ્ટમ ગણતરી	Nmap, Nessus	નબળાઈ ઓળખ
અક્સેસ મેળવવી	નબળાઈઓનો ફાયદો	Metasploit, કસ્ટમ અક્સેપ્લોયટ	સિસ્ટમ સમાધાન
અક્સેસ જાળવી રાખવી	સતત હાજરી	બેકડોર, રૂટકિટ	લાંબા ગાળાનું નિયંત્રણ
દ્રેક્સ ટાંકવા	પુરાવા દૂર કરવા	લોગ સફાઈ, ફાઇલ કાઢવી	શોધ ટાળવી

માહિતી અભેક્ટીકરણ પ્રકારો:

- પેસિવ: લક્ષ્ય સાથે સીધો સંપર્ક નહીં
- અભેક્ટિવ: લક્ષ્ય સિસ્ટમ સાથે સીધી કિયાપ્રતિક્રિયા

સ્કેનિંગ તકનીકો:

- ખૂલ્લી સેવાઓ માટે પોર્ટ સ્કેનિંગ
- નબળાઈઓ માટે વલન્રેબિલિટી સ્કેનિંગ

- ટોપોલોજી માટે નેટવર્ક મેપિંગ

એક્સેસ પદ્ધતિઓ:

- પાસવર્ડ કુમલાઓ (બૃટ ફોર્મ્, ડિકશનેરી)
- નબળાઈએનો ફાયદો ઉઠાવવો
- સોશિયલ એન્ઝિનિયરિંગ
- લૌટિક એક્સેસ

સ્થાયિત્વ ભિકેનિઝમ:

- બેકડોર ઇન્સ્ટોલ કરવા
- ચુંઝર એકાઉન્ટ બનાવવા
- ટાસ્ક શોક્યુલ કરવા
- રજિસ્ટ્રી ફેરફારો

ફ્રેક કવરિંગ પદ્ધતિઓ:

- સિસ્ટમ લોગ સાફ કરવા
- કામચલાઉ ફાઇલો કાઢવી
- ટાઇમસ્ટેમ્પ ફેરવવા
- અન્ટિવિરસ ઉપયોગ

મેમરી ટ્રીક: "રિકોનેસન્સ સ્કેનસ એક્સેસ જનરેટ કરે, કવરેજ જાળવે"

પ્રશ્ન 4(અ અથવા) [3 ગુણ]

કાલી લિનક્સના કોઈપણ ત્રણ બેઝિક કમાન્ડ યોગ્ય ઉદાહરણ સાથે સમજાવો.

જવાબ:

અત્યાવશ્યક કાલી લિનક્સ કમાન્ડ્સ:

Kali Linux Commands for Ethical Hacking

Kali Linux

Network Reconnaissance

Nmap nmap -sn 192.168.1.0/24 nmap -ss -O target nmap -sv -p- _target	Netdiscover netdiscover -r 192.168.1.0/24 netdiscover -i eth0 netdiscover -P
--	--

Web Application Testing

Nikto nikto -h target nikto -h target -p 80,443 nikto -h target -ssl	Dirb dirb http://target/ dirb http://target/ /usr/share/wordlists dirb http://target/ -X .php
--	---

Vulnerability Scanning

OpenVAS openvas-start openvas-stop openvas-check-setup	Lynis lynis audit system lynis show profiles lynis show commands
--	--

Exploitation

Metasploit msfconsole search exploit use exploit/...	SQLmap sqlmap -u "url" sqlmap -u "url" --dbs sqlmap -u "url" --dump
--	---

Password Cracking

John the Ripper john --wordlist=/usr/share/wordlists/rockyou.txt ssh john --show hash.txt john --format=MD5 hash.txt	Hydra hydra -l admin -P pass.txt ssh hydra -L users.txt -P pass.txt hydra -l admin -p password http
--	---

Wireless Security

Aircrack-ng airmon-ng start wlan0 airodump-ng wlan0mon aircrack-ng -w wordlist.txt reaver -i wlan0mon -b [BSSID] -vv	Reaver reaver -i wlan0mon -b [BSSID] -c [channel] wash -i wlan0mon aircrack-ng -w wordlist.txt reaver -i wlan0mon -b [BSSID] -vv
--	--

ReconWebScanExploitPasswordWireless

ક્રમાંક	ફંક્શન	ઉદાહરણ
nmap	નેટવર્ક સ્કેનિંગ	nmap -sS 192.168.1.1
netcat	નેટવર્ક કમ્યુનિકેશન	nc -l -p 1234
hydra	પાસવર્ડ કેલ્કિંગ	hydra -l admin -P passwords.txt ssh://target

- Nmap:** નેટવર્ક પર હોસ્ટ અને સેવાઓ શોધે છે
- Netcat:** ડેટા ટ્રાન્સફર માટે નેટવર્ક કનેક્શન બનાવે છે
- Hydra:** બ્રૂટ-ફોર્ස પાસવર્ડ હુમલાઓ કરે છે

મેમરી ટ્રીક: "નેટવર્ક મેપ, કનેક્ટ, કેલ્ક"

પ્રશ્ન 4(બ) [4 ગુણા]

સેશન હાઇજેક્ચરિંગનું વિગતવાર વર્ણન કરો.

જવાબ:

સેશન હાઇજેક્ચરિંગ ઓપરએટર:

હુમલાખોર કાયદેસર યુઝરના સેશનને કબજે કરે છે તે હુમલો.

સેશન હાઇજેકિંગના પ્રકારો:

પ્રકાર	પદ્ધતિ	રોકયામ
અએક્ટિવ	સેશન કબજે કરે	મજબૂત સેશન મેનેજમેન્ટ
પેસિવ	સેશન મોનિટર કરે	અન્ઝિપણ (HTTPS)
નેટવર્ક-લેવલ	TCP હાઇજેકિંગ	સુરક્ષિત પ્રોટોકોલ
અપ્લિકેશન-લેવલ	કુકી થોરી	સુરક્ષિત કુકી એટ્રિબ્યુટ

કુમલાની પ્રક્રિયા:

- નેટવર્ક ટ્રાફિક મોનિટર કરવું
- સેશન આંગખકર્તાઓ કેચ્યર કરવા
- સેશન ટોકન્સ રિપ્લે કરવા
- ચુઝર અંકાઉન્ટ એક્સેસ કરવું

રોકયામના પગલાં:

- બધા કમ્યુનિકેશન માટે HTTPS નો ઉપયોગ
- સુરક્ષિત સેશન મેનેજમેન્ટ અમલીકરણ
- સુરક્ષિત કુકી એટ્રિબ્યુટ સેટ કરવા
- શાંકાસ્પદ પ્રવૃત્તિ માટે મોનિટરિંગ

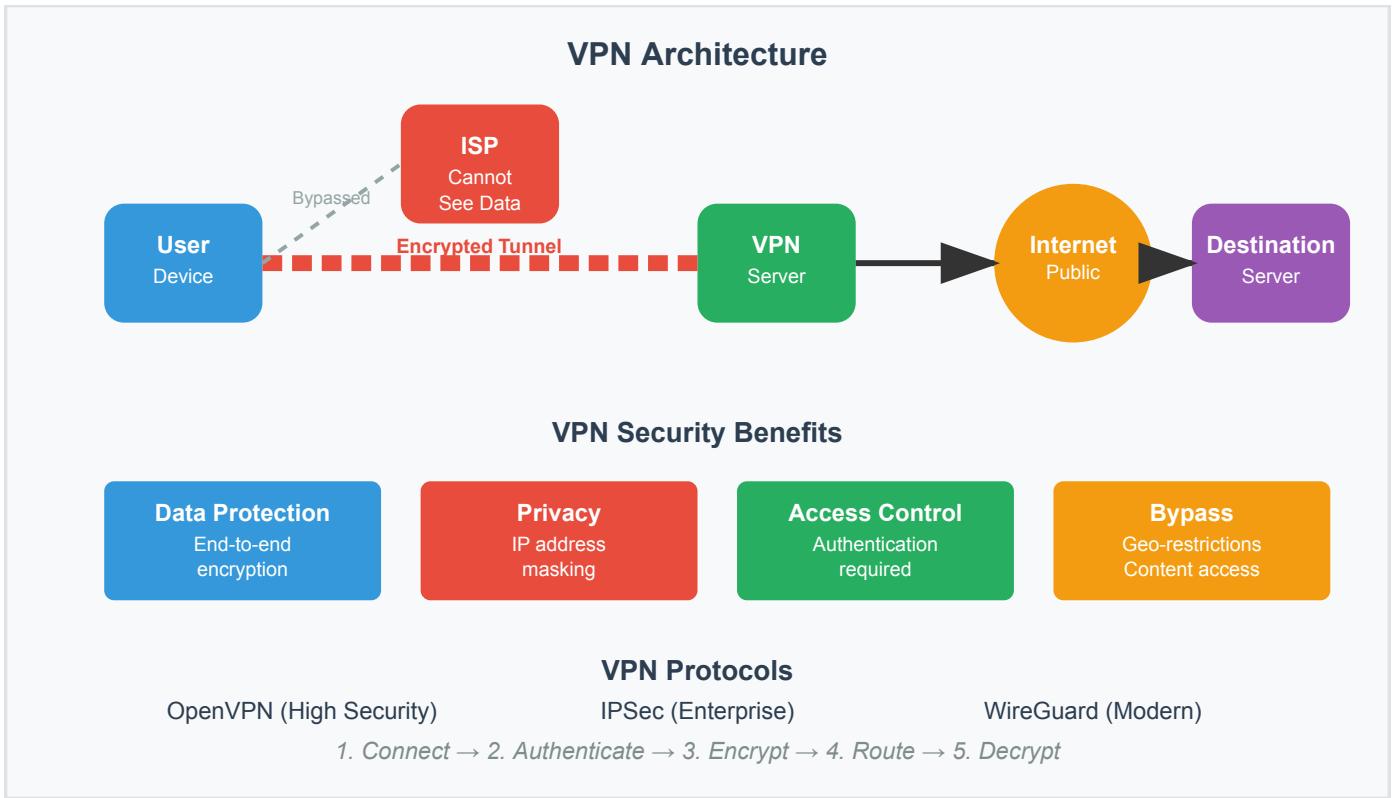
મેમરી ટ્રીક: "સેશન હાઇજેકને સુરક્ષિત હેન્ડલિંગની જરૂર"

પ્રશ્ન 4(ક અથવા) [7 ગુણ]

વર્ચ્યુઅલ પ્રાઇવેટ નેટવર્ક્સ (VPNs) જાહેર નેટવર્ક્સ પર કેવી રીતે સુરક્ષિત, અન્ઝિપેડ કનેક્શન બનાવે છે તે સમજાવો.

જવાબ:

VPN આર્કિટેક્ચર:



ISP	દ્રાફિક જોઇ શકતું નથી	ચુલ્ચ ડિવાઇસ	અનિકેટ ટનલ	VPN સર્વર	ઇન્ટરનેટ	ડેવિલેન્સ સર્વર
-----	-----------------------	--------------	------------	-----------	----------	-----------------

VPN ધરકો:

ધરક	ફુંક્શન	ફાયદો
ટનલિંગ	સુરક્ષિત પાથવે બનાવે	ડેટા પ્રોટોકોલ
અનિક્ષણ	ડેટાને જીએવટથી બદલે	ગોપનીયતા
ઓથેરનિકેશન	અંગભ ચકાસે	અક્સેસ કંટ્રોલ
IP માસિક્સિંગ	વાસ્તવિક IP છુપાવે	અનામત્વ

VPN પ્રોટોકોલ:

પ્રોટોકોલ	સુરક્ષા સ્તર	જરૂર	ઉપયોગ કેસ
OpenVPN	ઉચ્ચ	સારી	સામાન્ય હેતુ
IPSec	અત્યંત ઉચ્ચ	મદ્યમ	અન્ટરપ્રાઇવેટ
WireGuard	ઉચ્ચ	ઉલ્લંઘ	આધુનિક સોલ્યુશન
PPTP	અંદું	જરૂરી	લેગાસી (અપ્રયાલિત)

VPN કાર્ય પ્રક્રિયા:

- કનેક્શન:** કલાઈન્ટ VPN સર્વર સાથે જોડાય

- ઓથેન્ટિકેશન: યુઝર કેડેન્ટિયલ થકાસાય
- ટનલ કિઅશન: એન્ફિલ્ડ પાથવે સ્થાપિત થાય
- ડેટા એન્કષ્ટન: બધો ટ્રાફિક એન્કષ્ટ થાય
- રાઉટિંગ: ટ્રાફિક VPN સર્વર દ્વારા રાઉટ થાય
- ડિક્રિપ્શન: ગંતવ્ય પર ડેટા ડિક્રિપ્ટ થાય

સુરક્ષા ફાયદાઓ:

- ડેટા પ્રોટોકોલ: એન્કષ્ટન ઇલ્યુસ્ટ્રેફિંગ અટકાવે
- ગોપનીયતા: IP એફ્રેસ માસ્કિંગ
- એક્સેસ કંટ્રોલ: કનેક્શન પહેલા ઓથેન્ટિકેટ કરવું
- પ્રતિબંધો બાધપાસ: જીઓ-બ્લોક કન્ટ્રોલ એક્સેસ કરવું

વ્યાવસાયિક એપ્લિકેશન:

- રિમોટ વર્કર એક્સેસ
- સાઇટ-ટુ-સાઇટ કનેક્ટિવિટી
- સુરક્ષિત કલાઉડ એક્સેસ
- અનુપાલન આવથયકતાઓ

વ્યક્તિગત ઉપયોગ કેસ:

- પબ્લિક વાઈ-ફાઈ પ્રોટોકોલ
- ગોપનીયતા વૃદ્ધિ
- કન્ટ્રોલ એક્સેસ
- લોકેશન ગોપનીયતા

મેમરી ટ્રીક: "VPN નેટવર્ક પ્રાઇવેસી પ્રદાન કરે"

પ્રશ્ન 5(અ) [૩ ગુણ]

નેટવર્ક ફોરેન્સિક્સ સમજાવો.

જવાબ:

નેટવર્ક ફોરેન્સિક્સ વ્યાખ્યા:

સુરક્ષા ઘટનાઓ શોધવા અને વિશ્લેષણ કરવા માટે નેટવર્ક ટ્રાફિકની તપાસ.

મુખ્ય ઘટકો:

ઘટક	હેતુ	સાધનો
ટ્રાફિક કેચાર	નેટવર્ક ડેટા રેકોર્ડ કરવો	Wireshark, tcpdump
વિશ્લેષણ	પેર્ટન તપાસવા	NetworkMiner, Snort
પુરાવા	શોધોનો ઇનકાર અટકાવવો	ફોરેન્સિક રિપોર્ટ

- અવકાશ: પેકેટ્સ, ફલોજ અને નેટવર્ક વર્તણું વિશ્લેષણ
- ઉદ્દેશ્ય: સુરક્ષા ભંગ અને હુમલાના પેટર્ન ઓળખવા
- પડકાર: મોટા ડેટા વોલ્યુમ અને રીએલ-ટાઇમ પ્રોસેસિંગ

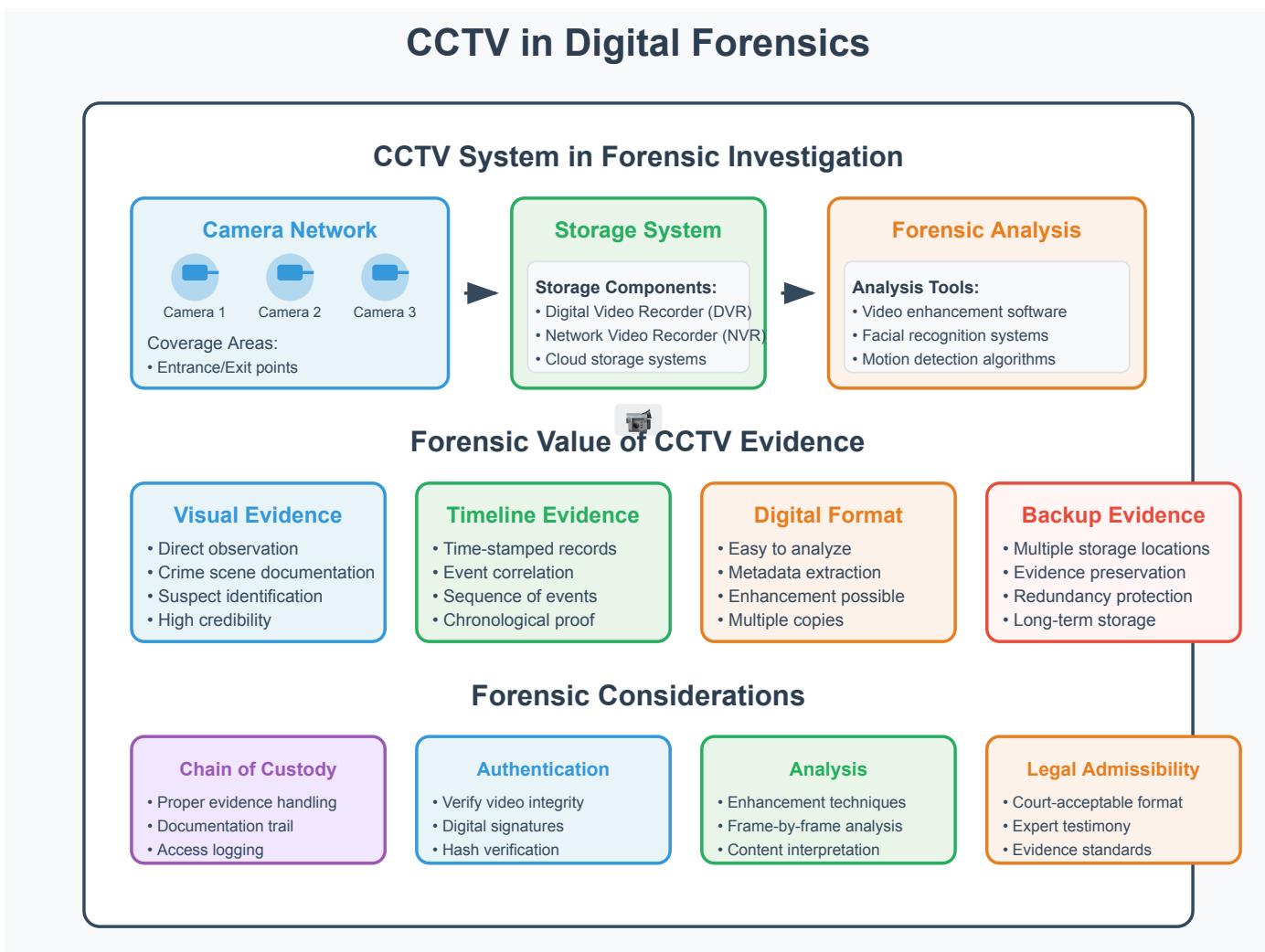
મેમરી ટ્રીક: "નેટવર્ક ફાયરાન્ડસિક્સ તથ્યો શોધે"

પ્રશ્ન 5(બ) [4 ગુણા]

ડિજિટલ ફાયરાન્ડસિક્સ તપાસમાં પુરાવા તરીકે CCTV શા માટે મહત્વની લૂભિકા લજવે છે તે સમજાવો.

જવાબ:

ડિજિટલ ફાયરાન્ડસિક્સમાં CCTV:



પાસું	મહત્વ	મૂલ્ય
વિઝ્યુઅલ પુરાવા	સીધું અવલોકન	ઉચ્ચ વિશ્વસનીયતા
ટાઇમલાઇન	સમય-સ્ટેમ્પ રેકૉર્ડ	ઘટના સહસંબંધ
ડિજિટલ ફોર્મેટ	વિશ્લેષણ કરવામાં સરળ	મેટાડેટા એક્સટ્રેક્શન
લોકઅપ	બહુવિધ કોપીઓ	પુરાવા સંરક્ષણ

પુરાવાનું મૂલ્ય:

- સમર્થન: અન્ય ડિજિટલ પુરાવાઓને સમર્થન આપે
- ટાઇમલાઈન: ઘટનાઓનો કમ સ્થાપિત કરે
- ઓળખ: ગુનેગારની ઓળખ પ્રગાટ કરી શકે
- સંદર્ભ: ઘટના દરમિયાન ભૌતિક વાતાવરણ દર્શાવે

ફોરેન્સિક વિચારણાઓ:

- યોઝન ઓફ કસ્ટોડી: યોગ્ય પુરાવા હેન્ડલિંગ
- ઓથેરિકેશન: વિડિયો અખંડિતતા ચકાસવી
- વિશ્લેષણ: વૃદ્ધિ અને અર્થધટન
- કાયદેસરી સ્વીકાર્યતા: કોર્ટ-સ્વીકાર્ય ફોર્મેટ

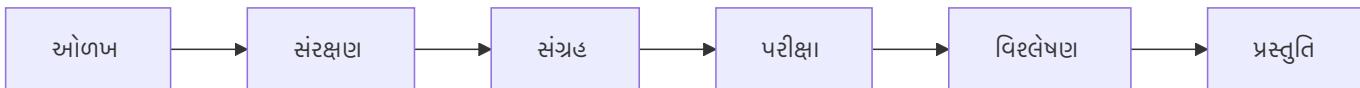
મેમરી ટ્રીક: "CCTV ગુનાહિત વર્તાળું સ્પષ્ટ રીતે કેચ્યર કરે"

પ્રશ્ન 5(ક) [7 ગુણ]

ડિજિટલ ફોરેન્સિક તપાસના તબક્કાઓ સમજાવો.

જવાબ:

ડિજિટલ ફોરેન્સિક તપાસના તબક્કાઓ:



વિગતવાર તબક્કાનું વિભાજન:

તબક્કો	પ્રવૃત્તિઓ	સાધનો	ઉદ્દેશ્ય
ઓળખ	સંભવિત પુરાવાઓ ઓળખવા	વિજ્ઞુઅલ નિરીક્ષણ	અવકાશ વ્યાપ્યા
સંરક્ષણ	પુરાવા દૂષણ અટકાવવું	રાઇટ બ્લોકર	પુરાવા અખંડતા
સંગ્રહ	ડિજિટલ પુરાવા મેળવવા	ફોરેન્સિક ઇમેજિંગ	સંપૂર્ણ ડેટા કેચ્યર
પરીક્ષા	સંબંધિત ડેટા એક્સટ્રેક્ટ કરવો	Autopsy, FTK	ડેટા રિકવરી
વિશ્લેષણ	શોધોનું અર્થધટન	ટાઇમલાઈન સાધનો	પેટર્ન ઓળખ
પ્રસ્તુતિ	પરિણામોનો દસ્તાવેજ	રિપોર્ટ જનરેટર	કાયદેસર પ્રસ્તુતિ

તબક્કો 1 - ઓળખ:

- દૃશ્યાનું સર્વેક્ષણ કરવું
- સંભવિત પુરાવા ક્રોતોની ઓળખ
- પ્રારંભિક અવલોકનોનો દસ્તાવેજ

- તપાસનો અવકાશ સ્થાપિત કરવો

તબક્કો 2 - સંરક્ષણા:

- અપરાધ સ્થળ સુરક્ષિત કરવું
- પુરાવા દૂષણ અટકાવવું
- રાઇટ-પ્રોટેક્શન મિકેનિક્યુમનો ઉપયોગ
- પુરાવાની સ્થિતિનો દસ્તાવેજ

તબક્કો 3 - સંગ્રહ:

- ફોરેન્સિક ઇમેજ બનાવવી
- થેઇન આંફ કસ્ટડી જાળવે
- ચોગ્ય સંગ્રહ તકનીકોનો ઉપયોગ
- વેરિફિકેશન માટે હેશ વેલ્યુ જનરેટ કરવી

તબક્કો 4 - પરીક્ષા:

- ફાઇલ સિસ્ટમ એક્સટ્રેક્ટ કરવી
- કાઢી નાખેલ ડેટા રિકવર કરવો
- સંબંધિત ફાઇલો ઓળખવી
- શોધાંનો દસ્તાવેજ

તબક્કો 5 - વિશ્લેષણા:

- પુરાવાઓને સહસંબંધિત કરવા
- ઘટનાઓનું પુનઃનિર્માણ
- પેટન ઓળખવા
- નિર્જર્ખ ખખડાવવા

તબક્કો 6 - પ્રસ્તુતિ:

- વિગતવાર રિપોર્ટ તૈયાર કરવો
- વિઝ્યુઅલ પ્રસ્તુતિઓ બનાવવી
- તકનીકી શોધો સમજાવવા
- કાયદેસરની કાર્યવાહીનું સમર્થન

ગુણવત્તા ખાતરી:

- દસ્તાવેજુકરણા: દરેક તબક્કે વિગતવાર રેકોર્ડ
- માન્યતા: પ્રક્રિયાઓ અને પરિણામો ચકાસવા
- પુનઃઉત્પાદનક્ષમતા: પરિણામો દુષ્ટિકેટ કરી શકાય તેની ખાતરી
- કાયદેસર અનુપાલન: ન્યાયક્ષેત્રીય આવશ્યકતાઓનું પાલન

મેમરી ટ્રીક: "તપાસકર્તાઓ સંરક્ષિત કરે, એકત્ર કરે, તપાસે, વિશ્લેષણ કરે, પ્રસ્તુત કરે"

પ્રશ્ન 5(અ અથવા) [3 ગુણ]

સાયબર સુરક્ષા સંબંધિત વિવિધ ક્ષેત્રોમાં માઇકોકન્ટ્રોલરની એપ્લિકેશનોની ચારી બનાવો.

જવાબ:

માઇકોકન્ટ્રોલર સુરક્ષા એપ્લિકેશન:

ક્ષેત્ર	એપ્લિકેશન	સુરક્ષા ફંક્શન
IoT સુરક્ષા	સ્માર્ટ હોમ ડિવાઇસ	ઓથેન્ટિકેશન, અનિષ્ટાન
એક્સેસ કંટ્રોલ	કી કાર્ડ, બાયોમેટ્રિક	ઓળખ ચકાસણી
નેટવર્ક સુરક્ષા	હાર્ડવેર ફાયરવોલ	પેકેટ ફિલ્ટરિંગ

- સ્માર્ટ કાર્ડ:** સુરક્ષિત ઓથેન્ટિકેશન ટોકન
- HSM (હાર્ડવેર સિક્યુરિટી મોડ્યુલ):** કિટોગ્રાફિક પ્રોસેસિંગ
- અમ્બોડ સિસ્ટમ:** સિક્યોર બૂટ, ટેમ્પર ડિટેક્શન

મેમરી ટ્રીક: "માઇકોકન્ટ્રોલર બહુવિધ સુરક્ષા ફંક્શન મેળેજ કરે"

પ્રશ્ન 5(બ અથવા) [4 ગુણ]

નૈતિક (એથિકલ) હેકિંગમાં પોર્ટ સ્કેનિંગનું મહત્વ સમજાવો.

જવાબ:

એથિકલ હેકિંગમાં પોર્ટ સ્કેનિંગ:

પાસું	મહત્વ	ફાયદો
સેવા શોધ	ચાલતી સેવાઓ આળખવી	હુમલા સપાઠીનું મેપિંગ
વલન્રેબિલિટી એસેસમેન્ટ	ખુલ્લા પોર્ટ શોધવા	સુરક્ષા ગોપ આળખ
નેટવર્ક મેપિંગ	ટોપોલોજી સમજવી	ઇન્ફ્રાસ્ટ્રક્ચર વિશ્લેષણ
સુરક્ષા પરીક્ષણ	કોન્ફિગરેશન માન્ય કરવી	અનુપાલન ચકાસણી

પોર્ટ સ્કેનિંગ તકનીકો:

- TCP કનેક્ટ:** સંપૂર્ણ કનેક્શન સ્થાપના
- SYN સ્કેન:** સ્ટેલ્યુ સ્કેનિંગ પદ્ધતિ
- UDP સ્કેન:** યુઝર ડેટાગ્રામ પ્રોટોકોલ સ્કેનિંગ
- સેવા ડિટેક્શન:** સેવા વર્ગન આળખવી

નૈતિક વિચારણાઓ:

- અધિકૃતતા:** યોગ્ય પરવાનગી મેળવવી

- અવકાશ: નિર્ધારિત સીમાઓમાં રહેણું
- દસ્તાવેજુકરણ: બધી પ્રવૃત્તિઓ રેકૉર્ડ કરવી
- રિપોર્ટિંગ: વિગતવાર શોધો પ્રદાન કરવા

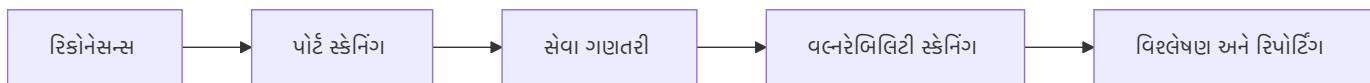
મેમરી ટ્રીક: "પોર્ટ સ્કેનિંગ સુરક્ષા આંતરદૃષ્ટિ પ્રદાન કરે"

પ્રચન 5(ક અથવા) [7 ગુણ]

કાલી લિનક્સ ટૂલ્સનો ઉપયોગ કરીને વલન્સેબિલિટી એસેસમેન્ટ કરવાની પ્રક્રિયાનું વર્ણન કરો.

જવાબ:

વલન્સેબિલિટી એસેસમેન્ટ પ્રક્રિયા:



પગાલું-દર-પગાલું પ્રક્રિયા:

પગાલું	કાલી ટૂલ	કમાન્ડ ઉદાહરણ	હેતુ
રિકોનેસન્સ	Nmap	nmap -sn 192.168.1.0/24	હોસ્ટ શોધ
પોર્ટ સ્કેનિંગ	Nmap	nmap -ss -O target	ખુલ્લા પોર્ટની આગામી
સેવા ગણતરી	Nmap, બેનર ગ્રેબિંગ	nmap -sv target	સેવા વર્જન ડિટેક્શન
વલન્સેબિલિટી સ્કેનિંગ	OpenVAS, Nessus	openvas-start	ઓટોમેટેડ વલન્સેબિલિટી ડિટેક્શન
વેબ એપ્લિકેશન પરીક્ષણ	Nikto, Dirb	nikto -h target	વેબ વલન્સેબિલિટી સ્કેનિંગ

વિગતવાર પ્રક્રિયા:

તબક્કો 1 - લક્ષ્ય આગામી:

- નેટવર્ક ડિસ્કવરી માટે Nmap નો ઉપયોગ
- લાઇવ હોસ્ટ અને તેમના IP એફ્રેસની આગામી
- નેટવર્ક ટોપોલોજીનો દસ્તાવેજ
- લક્ષ્ય અવકાશ નિર્ધારણ

તબક્કો 2 - પોર્ટ અને સેવા વિશ્લેષણ:

- વ્યાપક પોર્ટ સ્કેન કરવા
- ચાલતી સેવાઓ અને વર્જન આગામીવા
- ડિફોલ્ટ કેડેન્શિયલ થકાસવા
- સેવા કોન્ફિગરેશન વિશ્લેષણ

તબક્કો 3 - ઓટોમેટેડ વલન્સેબિલિટી સ્કેનિંગ:

- વલનરેબિલિટી સ્કેનર (OpenVAS) કોન્ફિગર કરવા
- વ્યાપક સ્કેન ચલાવવા
- સ્કેન પરિણામોનું વિશ્લેષણ
- ગંભીરતા અનુસાર શોધોને પ્રાથમિકતા આપવી

તબક્કો 4 - મેન્યુઅલ પરીક્ષણ:

- ઓટોમેટેડ શોધોની યકાસણી
- લક્ષિત પરીક્ષણ કરવું
- વિશીષ વલનરેબિલિટી માટે પરીક્ષણ
- ફોલ્સ પોર્ઝિટિવ માન્ય કરવા

તબક્કો 5 - વેબ એપ્લિકેશન એસેસમેન્ટ:

- વેબ વલનરેબિલિટી સ્કેનરનો ઉપયોગ
- OWASP ટોપ 10 વલનરેબિલિટી માટે પરીક્ષણ
- એપ્લિકેશન લોજિકનું વિશ્લેષણ
- મિસકોન્ફિગરેશન યકાસવા

સામાન્ય કાલી ટૂલ્સ:

ટૂલ	ફંકશન	ઉપયોગ કેસ
Nmap	નેટવર્ક સ્કેનિંગ	પોર્ટ અને સેવા શોધ
OpenVAS	વલનરેબિલિટી સ્કેનિંગ	ઓટોમેટેડ એસેસમેન્ટ
Nikto	વેબ સ્કેનિંગ	વેબ સર્વર વલનરેબિલિટી
Dirb	ડિટેક્ટરી બુટ ફોર્સિંગ	છુપાયેલ ફાઇલ શોધ
SQLmap	SQL ઇન્જેક્શન પરીક્ષણ	ડેટાબેસ વલનરેબિલિટી
Burp Suite	વેબ પ્રોક્સી	મેન્યુઅલ વેબ પરીક્ષણ
Metasploit	એક્સપ્લોટેશન ફેમવર્ક	વલનરેબિલિટી માન્યતા

એસેસમેન્ટ પદ્ધતિ:

- અવકાશ વ્યાખ્યા: એસેસમેન્ટ સીમાઓ સ્પષ્ટ રીતે વ્યાખ્યાયિત કરવી
- માહિતી એક્શન્સ: લક્ષ્ય ઇન્ટેલિજન્સ એક્શન્સ
- વલનરેબિલિટી ડિટેક્શન: બહુવિધ સ્કેનિંગ પદ્ધતિઓનો ઉપયોગ
- જોખમ એસેસમેન્ટ: અસર અને સંભાવનાનું મૂલ્યાંકન
- રેમેક્ઝિન્સ પ્લાનિંગ: કાર્યક્રમ લલામણો પ્રદાન કરવી

રિપોર્ટિંગ ઘટકો:

- એક્ઝાક્યુટિવ સમર્પી: મેનેજમેન્ટ માટે ઉચ્ચ-સ્તરીય શોધો

- **તકનીકી વિગતો:** વલન્ટરેબિલિટીના વિગતવાર વર્ણનો
- **જોખમ રેટિંગ:** CVSS સ્કોર અને બિજનેસ અસર
- **રેમેડિએશન સ્ટેપ્સ:** વિશિષ્ટ મિટિંગેશન ભલામણો
- **સપોર્ટિંગ એવિડન્સ:** સ્ક્રીનશોટ અને પ્રૂફ-ઓફ-કોન્સોટ

બેસ્ટ પ્રેક્ટિસિસ:

- **અધિકૃતતા:** હુમેશા લેખિત પરવાનગી મેળવવી
- **દસ્તાવેજુકરણ:** બધી પ્રવૃત્તિઓના વિગતવાર લોગ જાળવવા
- **ન્યૂનતમ અસર:** પ્રોડક્શન સિસ્ટમને ખલેલ પહોંચાડવાનું ટાળવું
- **ગોપનીયતા:** શોધાયેલ સંવેદનશીલ માહિતીનું રક્ષણ કરવું

મેમરી ટ્રીક: "વલન્ટરેબિલિટી એસેસમેન્ટ એપ્લિકેશન સિક્યુરિટીને માન્ય કરો"