

Subject Name (Gujarati)

4353204 -- Summer 2025

Semester 1 Study Material

Detailed Solutions and Explanations

પ્રશ્ન 1(અ) [3 ગુણ]

ઉદાહરણ સાથે CIA નિપુટીનું વર્ણન કરો.

જવાબ

CIA નિપુટીના ઘટકો:

ઘટક	વ્યાખ્યા	ઉદાહરણ
કન્ફિડેન્શિયાલિટી	અનધિકૃત એક્સેસથી ડેટાનું રક્ષણ	બેંક એકાઉન્ટ પર પાસવર્ડ પ્રોટેક્શન
ઇન્ટેગ્રેશન	ડેટાની ચોકસાઈ અને સંપૂર્ણતા	ડોક્યુમેન્ટ પર ડિજિટલ સહી
એવેઇલબિલિટી	જરૂરિયાત મુજબ સિસ્ટમની ઉપલબ્ધતા	24/7 ઓનલાઇન બેંકિંગ સેવાઓ

- કન્ફિડેન્શિયાલિટી: માત્ર અધિકૃત વપરાશકર્તાઓ જ સંવેદનશીલ માહિતી એક્સેસ કરી શકે
- ઇન્ટેગ્રેશન: ટ્રાન્સફરેન્સ દરમિયાન ડેટા ચોકસ અને અપરિવર્તિત રહે
- એવેઇલબિલિટી: સિસ્ટમો કાયદેસર વપરાશકર્તાઓ માટે કાર્યરત અને સુલભ રહે

મેમરી ટ્રીક

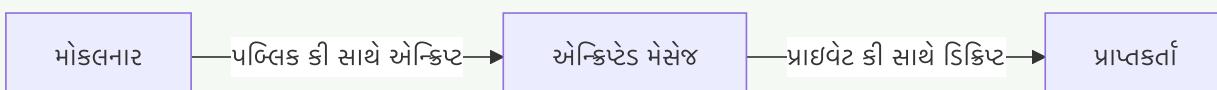
"CIA માહિતી ને સુરક્ષિત રાખો"

પ્રશ્ન 1(બ) [4 ગુણ]

પબ્લિક કી અને પ્રાઇવેટ કી કિંપ્ટોગ્રાફી સમજાવો.

જવાબ

પબ્લિક કી કિંપ્ટોગ્રાફી (એસિમેટ્રિક):



મુખ્ય લક્ષણો:

વિશેષતા	પબ્લિક કી	પ્રાઇવેટ કી
વિતરણ	મુક્તપણે શેર કરાય	ગુપ્ત રાખાય
ઉપયોગ	એન્ક્રિપ્શન/વેરિફિકેશન	ડિક્રિપ્શન/સાઇનિંગ
સુરક્ષા	જાહેર હોઈ શકે	સુરક્ષિત રાખવી જરૂરી

- પબ્લિક કી: એન્ક્રિપ્શન અને સિગ્નેચર વેરિફિકેશન માટે
- પ્રાઇવેટ કી: ડિક્રિપ્શન અને ડિજિટલ સાઇનિંગ માટે
- સુરક્ષા: ગાળિટિક જટિલતા પર આધારિત (RSA, ECC અલ્ગોરિદમ)

મેમરી ટ્રીક

"પબ્લિક એન્ક્રિપ્ટ કરો, પ્રાઇવેટ ડિક્રિપ્ટ કરો"

પ્રશ્ન 1(ક) [7 ગુણ]

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

જવાબ

OSI સુરક્ષા ફેમવર્ક:

સ્તર	હુમલાઓ	પદ્ધતિઓ	સેવાઓ
ફિલીફલ	વાયરટેપિંગ, જેમિંગ	ફિલીફલ સિક્યોરિટી, શિલ્ડિંગ	એક્સેસ કંટ્રોલ
ડેટા લિંક	MAC ફ્લાઇંગ, ARP પોઇઝનિંગ	એન્કિશન, ઓથેન્ટિકેશન	ફેમ ઇન્ટેગ્રેટી
નેટવર્ક	IP સ્પૂફિંગ, રાઉટિંગ એટેક	IPSec, ફાયરવોલ	પેકેટ ફિલ્ટરિંગ
ટ્રાન્સપોર્ટ	સેશન હાઇજોકિંગ, SYN ફ્લાઇંગ	SSL/TLS, પોર્ટ સિક્યોરિટી	એન્ડ-ટુ-એન્ડ સિક્યોરિટી
સેશન	સેશન રિપ્લે, હાઇજોકિંગ	સેશન ટોકન, ટાઇમઅઉટ	સેશન મેનેજમેન્ટ
પ્રોટોકોલ	ડેટા કરખણ, ફોર્મેટ એટેક	એન્કિશન, કમ્પેશન	ડેટા ટ્રાન્સફર્મેશન
એપ્લિકેશન	મેલવેર, સોશિયલ એન્જિનિયરિંગ	એન્ટિવાયરસ, યુઝર ટ્રેનિંગ	એપ્લિકેશન સિક્યોરિટી

મુખ્ય સુરક્ષા સેવાઓ:

- ઓથેન્ટિકેશન: યુઝર આઇડેન્ટિટી વેરિફિકેશન
- ઓથોરાઇઝન: એક્સેસ પરમિશન કંટ્રોલ
- નોન-રિપ્યુટેશન: કિયાઓનો ઇનકાર અટકાવવો
- ડેટા ઇન્ટેગ્રેટી: ડેટાની ચોકસાઈ સુનિશ્ચિત કરવી

મેમરી ટ્રીક

"બધા લોકોને ડેટા પ્રોટેક્શનની જરૂર છે"

પ્રશ્ન 1(ક) અથવા) [7 ગુણ]

MD5 હેશિંગ અને સિક્યોર હેશ ફંક્શન (SHA) અલોરિધમ 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	મધ્યમ	ધીમું
વર્તમાન સ્થિતિ	અપ્રયાલિત	અપ્રયાલિત	ભલામણ કરેલ



હેશ ગુણધર્મો:

- ડિટિભિનિસ્ટિક: સમાન ઇનપુટ સમાન હેશ આપે
- એવેલાન્ચ ઇફ્ફેક્ટ: નાનો ઇનપુટ ફેરફાર મોટો હેશ ફેરફાર લાવે
- વન-વે ફંક્શન: હેશથી મૂળ ડેટા મેળવી શકાતો નથી
- કોલિઝન રેઝિસ્ટન્ટ: બે અલગ ઇનપુટ માટે સમાન હેશ મળવો મુશ્કેલ

એપ્લિકેશન:

- પાસવર્ડ સ્ટોરેજ અને વેરિફિકેશન
- ડિજિટલ સિગ્નેચર અને સાર્ટિફિકેટ
- ડેટા ઇન્ટેગ્રેટી ચેકિંગ

મેમરી ટ્રીક

"હેશ હંમેશા સમાન આઉટપુટ આપે"

પ્રશ્ન 2(અ) [3 ગુણ]

ફાયરવોલ શું 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	ફૂકશન	સ્તર
પેકેટ ફિલ્ટર	પેકેટ હેડર તપાસે	નેટવર્ક લેયર
સ્ટેટકુલ	કનેક્શન સ્ટેટ ટ્રેક કરે	ડ્રાન્સપોર્ટ લેયર
એપ્લિકેશન પ્રોક્સી	એપ્લિકેશન ડેટા તપાસે	એપ્લિકેશન લેયર
પર્સનલ ફાયરવોલ	વ્યક્તિગત ડિવાઇસ સુરક્ષા	હોર્સ્ટ-બેસ્ડ

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

મેમરી ટ્રીક

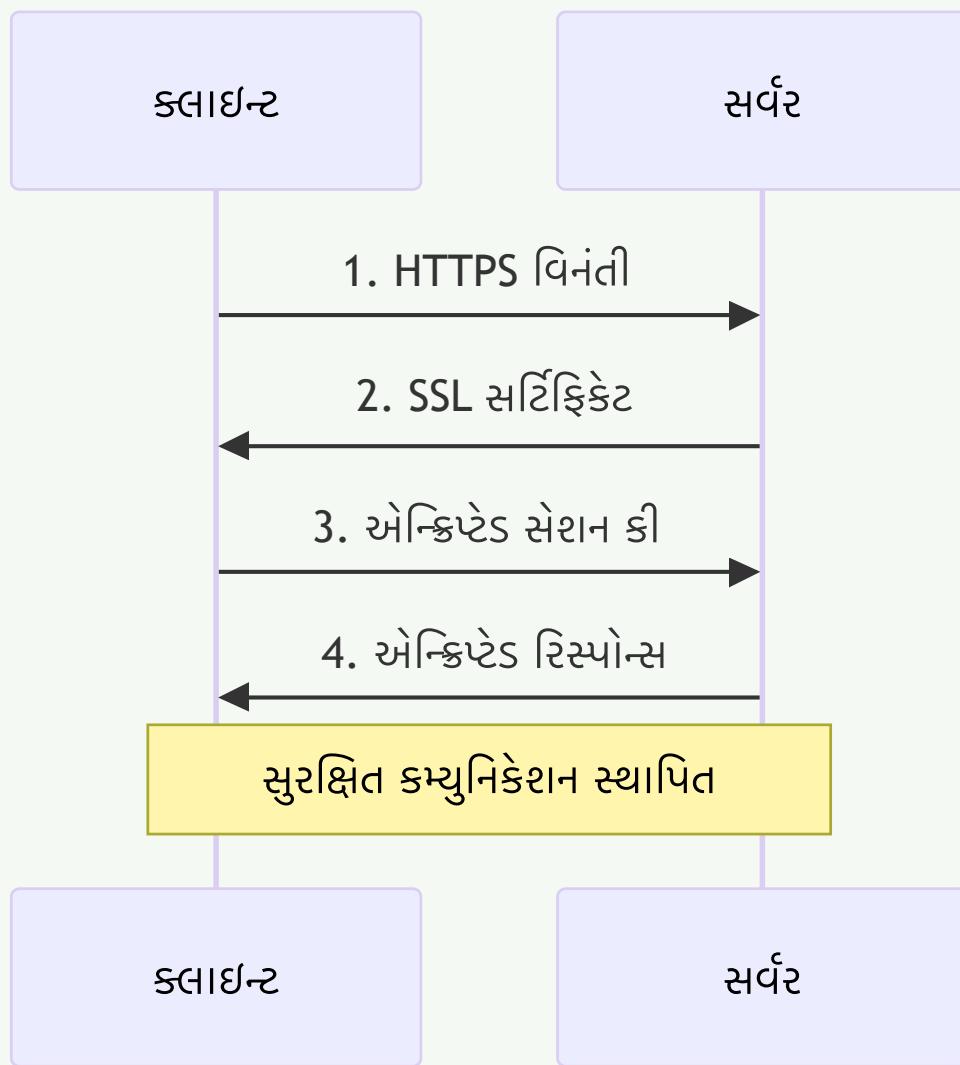
"ફાયરવોલ હંમેશા નેટવર્કનું રક્ષણ કરે"

પ્રશ્ન 2(બ) [4 ગુણ]

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

ફાયદાઓ:

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

મેમરી ટ્રીક

"HTTPS વેબ ટ્રાફિકને સુરક્ષિત કરો"

પ્રશ્ન 2(ક) [7 ગુણ]

વિવિધ પ્રકારના દુર્ભાવનાપૂર્ણ સોફ્ટવેર અને તેમની અસર સમજાવો.

જવાબ

મેલવેર વર્કિંગ્ઝેડ:

પ્રકાર	વર્તન	અસર	ઉદાહરણ
વાયરસ	ફાઇલો સાથે જોડાય	ફાઇલ કરપણ	બૂટ સેક્ટર વાયરસ
વોર્મ	સ્વ-પ્રતિકૃતિ	નેટવર્ક ભીડ	કન્ફિકર વોર્મ
ટ્રોજન	ઇશ્વરેશી મેલવેર	ડેટા ચોરી	બેંકિગ ટ્રોજન
રૈન્સમવેર	ફાઇલો એન્કિપ્ટ કરે	ડેટા બંધક	WannaCry
સ્પાયવર	પ્રવૃત્તિ મોનિટર કરે	ગોપનીયતા ભંગ	કીલોગર
એડવર	અનચાહેલી જાહેરાતો	પ્રદર્શન ઘટાડો	પોપ-અપ જાહેરાતો
રૂટકિટ	હાજરી છુપાવે	સિસ્ટમ સમાધાન	કર્નલ રૂટકિટ

સિસ્ટમ પર અસરો:

- પ્રદર્શનિ: ધીમી સિસ્ટમ પ્રતિક્રિયા
- ડેટા: નુકસાન, કરપણ અથવા ચોરી
- ગોપનીયતા: અનધિકૃત મોનિટરિંગ
- નાણાકીય: પ્રત્યક્ષ નાણાકીય નુકસાન

રોકથામના પદ્ધતિઓ:

- નિયમિત ઓન્ટિવાયરસ અપડેટ
- સુરક્ષિત બ્રાઉઝિંગ પ્રેક્ટિસ
- ઇમેઇલ એટેચેમેન્ટમાં સાવધાની
- સિસ્ટમ સિક્યુરિટી પેચ

મેમરી ટ્રીક

"વાયરસ વોર્મ ટ્રોજન ખરેખર બધા સંસાધનો ચોરે"

પ્રશ્ન 2(અ અથવા) [3 ગુણ]

પ્રમાણીકરણ(ઓથેન્ટિકેશન) શું છે? પ્રમાણીકરણ(ઓથેન્ટિકેશન) ની વિવિધ પદ્ધતિઓ સમજાવો.

જવાબ

ઓથેન્ટિકેશન વ્યાખ્યા: સિસ્ટમ એક્સેસ આપતા પહેલા યુઝર આઇડેન્ટિટી વેરિફિકેશન કરવાની પ્રક્રિયા.
ઓથેન્ટિકેશન પદ્ધતિઓ:

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

- સિંગલ-ફેક્ટર: એક ઓથેન્ટિકેશન પદ્ધતિ વાપરે
- માલ્ટિ-ફેક્ટર: અનેક પદ્ધતિઓ જોડે
- ટુ-ફેક્ટર (2FA): બરાબર બે ફેક્ટર વાપરે

મેમરી ટ્રીક

"પાસવર્ડ બાયોમેટ્રિક ટોકન ઓથેન્ટિકેશન"

પ્રશ્ન 2(બ અથવા) [4 ગુણ]

વ્યાખ્યાયિત કરો: ટ્રોજન્સ, રૂટકિટ, બેકડોર્સ, કીલોગર

જવાબ

મેલવેર વ્યાખ્યાઓ:

શબ્દ	વ્યાખ્યા	લક્ષણો
ટ્રોજન્સ	કાયદેસર સોફ્ટવેરના ઇશ્વરેશમાં મેલવેર	હાનિકારક દેખાય, છુપાયેલ પેલોડ

રૂટકિટ
બેકડોર્સ
કીલોગર

મેલવેરની હાજરી છુપાવતો સોફ્ટવેર
અનધિકૃત એક્સેસ પદ્ધતિ
કીબોર્ડ ઇનપુટ રેકૉર્ડ કરે

ઉંડી સિસ્ટમ એક્સેસ, સ્ટેલ્થ ઓપરેશન
સામાન્ય ઓથેન્ટિકેશન બાયપાસ કરે
પાસવર્ડ, સંવેદનશીલ ડેટા કેચર કરે

- ટ્રોજન્સ: ગ્રીંક 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"

પ્રશ્ન 2(ક અથવા) [7 ગુણ]

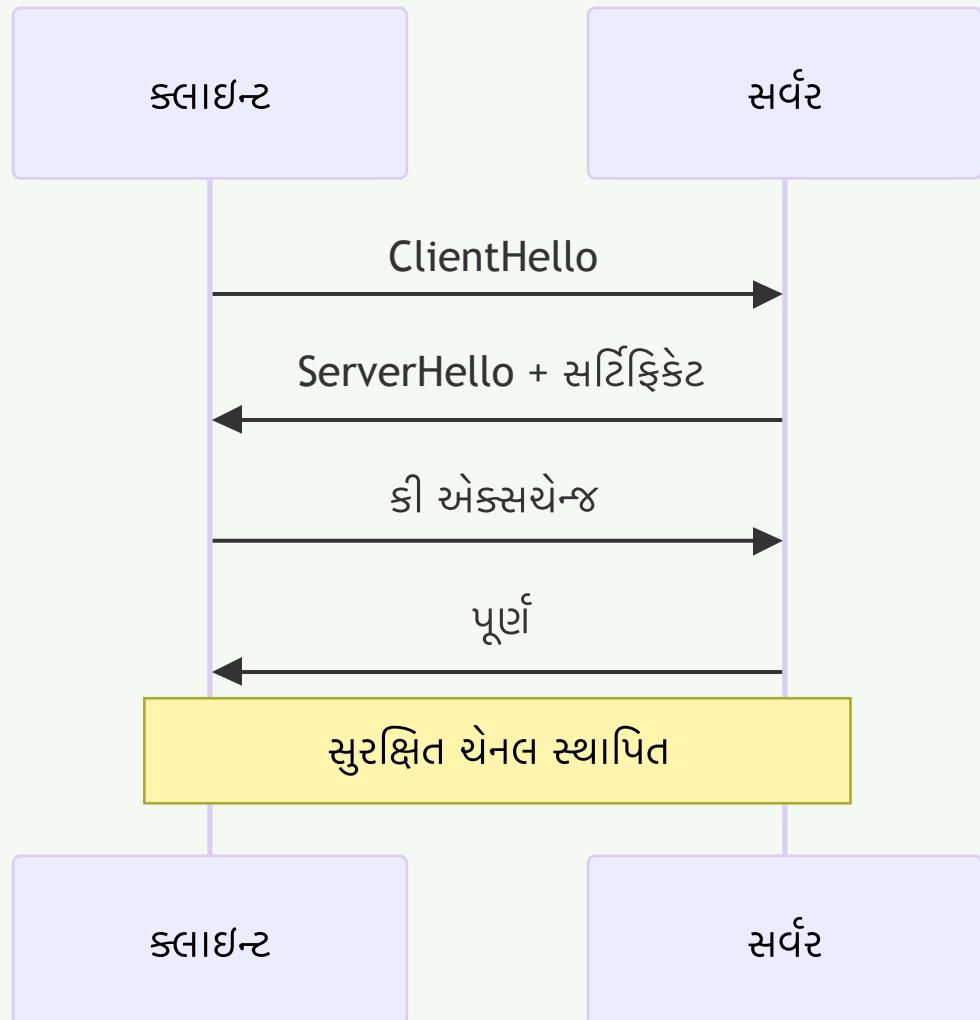
સિક્યુર સોકેટ લેચર (SSL) અને ટ્રાન્સપોર્ટ લેચર સિક્યુરિટી (TLS) પ્રોટોકોલ સમજાવો.

જવાબ

SSL/TLS પ્રોટોકોલ ઉત્કાંતિ:

વર્ઝન	વર્ષ	સ્થિતિ	સુરક્ષા સ્તર
SSL 2.0	1995	અપ્રયલિત	નબળું
SSL 3.0	1996	અપ્રયલિત	સંવેદનશીલ
TLS 1.0	1999	લેગસી	મર્યાદિત
TLS 1.2	2008	વ્યાપક ઉપયોગ	સારં
TLS 1.3	2018	વર્તમાન	મજબૂત

TLS હેન્ડશેક પ્રક્રિયા:



મુખ્ય વિશેષતાઓ:

- એન્ક્રિપ્શન: સિમેટ્રિક અને એસિમેટ્રિક અલ્ગોરિધમ
- ઓથેન્ટિકેશન: સવર અને કલાયન્ટ વેરિફિકેશન
- ઇન્ટેગ્રિટી: મેસેજ ઓથેન્ટિકેશન કોડ
- ફોરવર્ક સિકેરીસી: સેશન કી પ્રોટોક્ષન

એપ્લિકેશન:

- HTTPS વેબ બ્રાઉન્ડિંગ
- ઇમેઇલ સિક્યુરિટી (SMTPE)
- VPN કનેક્શન
- સુરક્ષિત ફાઇલ ટ્રાન્સફર

મેમરી ટ્રીક

“TLS બધા નેટવર્ક ટ્રાફિકને એન્ક્રિપ્ટ કરે”

પ્રશ્ન 3(અ) [3 ગુણ]

સાયબર કાઇમ અને સાયબરક્રિમિનલ ને વિગતવાર સમજાવો.

જવાબ

સાયબર કાઇમ વ્યાખ્યા: કમ્પ્યુટર અથવા ઇન્ટરનેટ નેટવર્ક દ્વારા કરવામાં આવતી ગુનાહિત પ્રવૃત્તિઓ.

ડાયાગ્રામ:

સાયબરક્રિમિનલ પ્રકારો:

પ્રકાર	પ્રેરણા	કુશળતા	લક્ષ્ય
સ્કિપ કિડીઝ	મજા/પ્રસિદ્ધિ	ઓછી	અવ્યવસ્થિત
હેક્ટિવિસ્ટ	રાજકીય/સામાજિક	મધ્યમ	સંસ્થાઓ
સાયબરક્રિમિનલ	નાણાકીય લાભ	ઉચ્ચ	વ્યક્તિઓ/બેંકો

- સાયબર કાઇમ: ડિજિટલ ટેકનોલોજીનો ઉપયોગ કરીને ગેરકાયદેસર પ્રવૃત્તિઓ
- સાયબરક્રિમિનલ: સાયબર કાઇમ કરનાર વ્યક્તિ
- અસર: નાણાકીય નુકસાન, ગોપનીયતા ભંગ, સિસ્ટમ નુકસાન

મેમરી ટ્રીક

"સાયબર ક્રિમિનલો અરાજકતા સર્જે છે"

પ્રશ્ન 3(બ) [4 ગુણ]

સાયબર સ્ટોકિંગ અને સાયબર બુલ્લીંગ નું વર્ણન કરો.

જવાબ

ડિજિટલ પજવણી સરખામણી:

પાસું	સાયબર સ્ટોકિંગ	સાયબર બુલ્લીંગ
લક્ષ્ય	વિશિષ્ટ વ્યક્તિ	મોટેભાગે નાબાળિગો
અવધિ	સતત, લાંબા ગાળાની	એપિસોડિક હોઈ શકે
હેતુ	ભીતિ, નિયત્રણ	પજવણી, અપમાન
પ્લેટફોર્મ	સોશિયલ મીડિયા, ઇમેઇલ	શાળાઓ, ગેમિંગ પ્લેટફોર્મ

સાયબર સ્ટોકિંગ લક્ષ્યો:

- સતત અનયાહેલ સંપર્ક
- પીડિતની ઓનલાઈન પ્રવૃત્તિનું મોનિટરિંગ
- ધમકીભર્યા સંદેશાઓ અથવા વર્તન
- ઓળખની ચોરી અથવા ઢોગ

સાયબર બુલ્લીંગ સ્વરૂપો:

- ઓનલાઈન જાહેર અપમાન
- ડિજિટલ જૂથોમંથી બાકાત
- ખોટી માહિતી ફેલાવવી
- સંમતિ વિના ખાનગી સામગ્રી શેર કરવી

રોકથામના પગલાં:

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

મેમરી ટ્રીક

"બુલ્લીંગ બંધ કરો, સ્ટોકિંગની જાણ કરો"

પ્રશ્ન 3(ક) [7 ગુણ]

સાયબર કાઇમમાં પ્રોપર્ટી બેઇજડ કલાસિકિકેશન સમજાવો.

જવાબ

પ્રોપર્ટી-આધારિત સાયબર કાઇમ શ્રેણીઓ:

શ્રેણી	કાઇમ પ્રકાર	વર્ણન	ઉદાહરણ
બૌલ્ઝિક સંપત્તિ	કોપીરાઇટ ઉલ્લંઘન	કોપીરાઇટ સામગ્રીનો અનધિકૃત ઉપયોગ	સોફ્ટવેર પાયરેસી
નાણાકીય સંપત્તિ	કેરિકટ કાર્ડ ફોડ	નાણાકીય માહિતીનો અનધિકૃત ઉપયોગ	ઓનલાઇન શોપિંગ ફોડ
ડિજિટલ સંપત્તિ	ડેટા ચોરી	ડિજિટલ માહિતીની ચોરી	ડેટાબેસ બીચ
વર્યુઅલ સંપત્તિ	ગેમિંગ એસેટ ચોરી	વર્યુઅલ વસ્તુઓની ચોરી	ઓનલાઇન ગેમ કરનસી ચોરી

ડાયાગ્રામ:
કાયદેસરના પાસાઓ:

- કોપીરાઇટ કાયદાઓ: સર્જનાત્મક કાર્યોનું રક્ષણ
- ટ્રેડમાર્ક કાયદાઓ: બ્રાન્ડ ઓળખનું રક્ષણ
- પેટન્ટ કાયદાઓ: આવિજકારોનું રક્ષણ
- ટ્રેડ સિલેક્ટ કાયદાઓ: ગોપનીય માહિતીનું રક્ષણ

અર્થતંત્ર પર અસર:

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

રોકથામ વ્યૂહરચનાઓ:

- ડિજિટલ રાઇટ્સ મેનેજમેન્ટ (DRM)
- વોટરમાર્કિંગ અને ટ્રેકિંગ
- કાયદેસર અમલીકરણ ભિકેનિજમ
- જાહેર જાગૃતિ ગુંબેશ

મેમરી ટ્રીક

"પ્રોપરી 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	ધારીવાર 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 સ્પાઈંગ અને સાયબર ટેરરીઝમ સમજાવો.

જવાબ

સાયબર ધમકીઓની સરખામણી:

પાસું	સાયબર સ્પાઇંગ	સાયબર ટેરરીઝમ
હેતુ	માહિતી એક્શન	ભય/વિક્ષેપ સર્જવો
લક્ષ્ય	સરકાર, કોપરિશન	નિર્ધારક ઇન્ફાસ્ટ્રક્ચર
પદ્ધતિઓ	છુપી ઘૂસણખોરી	વિનાશક હુમલાઓ
અસર	ગુપ્ત માહિતીનું નુકસાન	જાહેર સુરક્ષા જોખમ

સાયબર સ્પાઇંગ પ્રવૃત્તિઓ:

- કોપરિટ જાસૂસી
- સરકારી દેખરેખ
- ડ્રેડ સિકેટ ચોરી
- વ્યક્તિગત માહિતી એક્શન

સાયબર ટેરરીઝમ પદ્ધતિઓ:

- ઇન્ફાસ્ટ્રક્ચર હુમલાઓ
- મોટા પાયે વિક્ષેપ ગુંબેશ
- મનોવૈજ્ઞાનિક યુદ્ધ
- આર્થિક નુકસાન

રોકથામના પગલાં:

- નેટવર્ક સિક્યોરિટી મોનિટરિંગ
- ઘટના પ્રતિક્રિયા આયોજન
- આંતરરાષ્ટ્રીય સહયોગ
- જાહેર-ખાનગી ભાગીદારી

મેમરી ટ્રીક

"જાસૂસો ચોરે, આતંકવાદીઓ આતંક"

પ્રશ્ન 3(ક અથવા) [7 ગુણ]

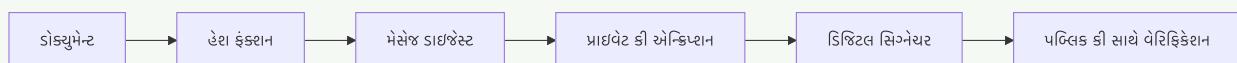
સાયબર સુરક્ષામાં ડિજિટલ સહીઓ અને ડિજિટલ પ્રમાણપત્રોની ભૂમિકા સમજાવો.

જવાબ

ડિજિટલ સુરક્ષા ઘટકો:

ઘટક	હેતુ	કંકશન	ફાયદો
ડિજિટલ સિશ્બેચર	ઓથેન્ટિકેશન	મોકલનારની ઓળખ સાબિત કરે	નોન-રિપુડિઅશન
ડિજિટલ સાર્ટિફિકેટ	વેરિફિકેશન	પબ્લિક કીની માન્યતા	વિશ્વાસ સ્થાપના

ડિજિટલ સિંગ્યુલર પ્રક્રિયા:



ડિજિટલ સર્ટિફિકેટ ઘટકો:

- વિધ્ય માહિતી: સર્ટિફિકેટ માલિકની વિગતો
- પદ્ધિત કી: એન્ક્રિપ્શન/વેરિફિકેશન માટે
- ડિજિટલ સિંગ્યુલર: CA ની સહી
- માન્યતા અવધિ: સર્ટિફિકેટની સમાપ્તિ તારીખ

સર્ટિફિકેટ ઓથોરિટી (CA) ભૂમિકા:

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

સાયબર સિક્યુરિટીમાં એપ્લિકેશન:

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

સુરક્ષા ફાયદાઓ:

- ઓથેન્ટિકેશન: મોકલનારની ઓળખ ચકાસે
- ઇન્ટેગ્રેટી: ડેટામાં ફેરફાર થયો નથી તેની ખાતરી
- નોન-રિપ્યુટેશન: કિયાઓનો ઇનકાર અટકાવે
- ગોપીયતા: સુરક્ષિત કમ્યુનિકેશન સક્ષમ કરે

મેમરી ટ્રીક

“ડિજિટલ સિંગ્યુલર ડોક્યુમેન્ટને સુરક્ષિત રીતે પ્રમાણિત કરો”

પ્રશ્ન 4(અ) [3 ગુણ]

હેકિંગ શું છે? હેકસના પ્રકારોની યાદી બનાવો.

જવાબ

હેકિંગ વ્યાખ્યા: નબળાઈઓનો ફાયદો ઉઠાવવા માટે કમ્પ્યુટર સિસ્ટમ અથવા નેટવર્કમાં અનધિકૃત એક્સેસ.

હેકર વર્ગોકરણ:

પ્રકાર	હેતુ	કાયદેસર સ્થિતિ
હાઇટ હેટ	સુરક્ષા સુધારણા	કાયદેસર
બ્લેક હેટ	દુર્ભાવનાપૂર્ણ પ્રવૃત્તિઓ	ગેરકાયદેસર
ગ્રે હેટ	મિશ્ર પ્રેરણા	શંકાસ્પદ

- હાઇટ હેટ: નૈતિક હેકર, સુરક્ષા સંશોધકો
- બ્લેક હેટ: સાયબરક્રિમિનલ, દુર્ભાવનાપૂર્ણ હેતુ
- ગ્રે હેટ: કેટલીકવાર કાયદેસર, કેટલીકવાર નહીં

મેમરી ટ્રીક

“સફેદ સારં, કાળું ખરાબ, ગ્રે શંકાસ્પદ”

પ્રશ્ન 4(બ) [4 ગુણ]

હેકિંગની વલનેબિલિટી અને 0-દિવસની પરિભાષા સમજાવો.

જવાબ

સુરક્ષા પરિભાષા:

શબ્દ	વ્યાખ્યા	જોખમ સ્તર	ઉદાહરણ
વલન્સેબિલિટી 0-દિવસ	સિસ્ટમની નબળાઈ અજાણી નબળાઈ	વિવિધ ગંભીર	અનપેરડ સોફ્ટવેર અશોધાયેલી ખામી

વલન્સેબિલિટી લક્ષણો:

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

0-દિવસ હુમલો પ્રક્રિયા:

- હેકર અજાણી નબળાઈ શોધે
- વેન્ડરની જાણકારી પહેલાં ખામીનો ફાયદો ઉઠાવે
- કોઈ ઉપલબ્ધ પેચ અથવા સંરક્ષણ નથી
- આશ્રયના કારણે ઉચ્ચ સફળતા દર

સંરક્ષણ વ્યૂહરચના:

- નિયમિત સુરક્ષા અપડેટ
- ઇન્ટરન્યુન ડિટેક્શન સિસ્ટમ
- વર્તાણૂકીય વિશ્વલેખણ સાધનો
- જીરો-ટ્રસ્ટ સુરક્ષા મોડેલ

મેમરી ટ્રીક

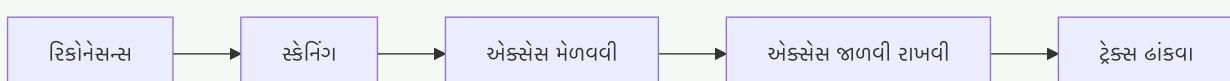
"નબળાઈઓને પેચની જરૂર, જીરો-ડેને સાવચેતીની જરૂર"

પ્રશ્ન 4(ક) [7 ગુણ]

હેકિંગના પાંચ સ્ટેપ્સ સમજાવો.

જવાબ

હેકિંગ પદ્ધતિઃ



વિગતવાર પગલાંઓ:

પગલું	વર્ણન	સાધનો/પદ્ધતિઓ	ઉદ્દેશ્ય
રિકોનેસન્સ	માહિતી એક્ટ્રીકરણ	Google dorking, સોશિયલ મીડિયા	લક્ષ્ય પ્રોફાઇલિંગ
સ્કેનિંગ	સિસ્ટમ ગણતરી	Nmap, Nessus	નબળાઈ ઓળખ
એક્સેસ મેળવવી	નબળાઈઓનો ફાયદો	Metasploit, કર્સ્ટમ એક્સપ્લોયિટ	સિસ્ટમ સમાધાન
એક્સેસ જાળવી	સતત હાજરી	બેકડોર, રૂટકિટ	લાંબા ગાળાનું નિયંત્રણ
રાખવી			
ટ્રેક્સ ઢાંકવા	પુરાવા દૂર કરવા	લોગ સફાઈ, ફાઇલ કાઢવી	શોધ ટાળવી

માહિતી એક્સ્પેરિયેન્શન પ્રકારો:

- પેસિવ: લક્ષ્ય સાથે સીધો સંપર્ક નહીં
- એક્ટિવ: લક્ષ્ય સિસ્ટમ સાથે સીધી ક્રિયાપ્રતિક્રિયા

સ્કેનિંગ તકનીકો:

- ખુલ્લી સેવાઓ માટે પોર્ટ સ્કેનિંગ
- નબળાઈઓ માટે વલનરેબિલિટી સ્કેનિંગ
- ટોપોલોજી માટે નેટવર્ક મેપિંગ

એક્સેસ પદ્ધતિઓ:

- પાસવર્ડ હુમલાઓ (બુટ ફોર્સ, ડિક્શનરી)
- નબળાઈઓનો ફાયદો ઉઠાવવો
- સોશિયલ એન્જિનિયરિંગ
- ભૌતિક એક્સેસ

સ્થાયિત્વ મિકેનિઝમ:

- બેકડોર ઇન્સ્ટોલ કરવા
- યુઝર એકાઉન્ટ બનાવવા
- ટાર્સ્ક શેડ્યુલ કરવા
- રજિસ્ટ્રેશન ફર્મફોર્મ

ટ્રેક કવરિંગ પદ્ધતિઓ:

- સિસ્ટમ લોગ સાફ્ કરવા
- કામચલાઉ ફાઇલો કાઢવી
- ટાઇમસ્ટેમ્પ ફૂરવવા
- એન્ક્રિપ્શનનો ઉપયોગ

મેમરી ટ્રીક

"રિકોનેસન્સ સ્કેન્સ એક્સેસ જનરેટ કરે, કવરેજ જાળવે"

પ્રશ્ન 4(અ અથવા) [3 ગુણ]

કાલી લિનક્સના કોઈપણ ત્રાણ બેઝિક કમાન્ડ ચોગ્ય ઉદાહરણ સાથે સમજાવો.

જવાબ

અત્યાવશ્યક કાલી લિનક્સ કમાન્ડ્સ:

કમાન્ડ	ફંક્શન	ઉદાહરણ
nmap	નેટવર્ક સ્કેનિંગ	nmap -ssS 192.168.1.1
netcat	નેટવર્ક કમ્પ્યુનિકેશન	nc -l -p 1234
hydra	પાસવર્ડ કેર્કિંગ	hydra -l admin -P passwords.txt ssh://target

- Nmap:** નેટવર્ક પર હોસ્ટ અને સેવાઓ શોધે છે
- Netcat:** ડેટા ટ્રાન્સ્ફર માટે નેટવર્ક કનેક્શન બનાવે છે
- Hydra:** બુટ-ફોર્સ પાસવર્ડ હુમલાઓ કરે છે

મેમરી ટ્રીક

"નેટવર્ક મેપ, કનેક્ટ, કેક"

પ્રશ્ન 4(બ) [4 ગુણ]

સેશન હાઇજેક્સનું વિગતવાર વર્ણન કરો.

જવાબ

સેશન હાઇજેક્સનું ઓવરવ્યુ: હુમલાખોર કાયદેસર પુગરના સેશનને કબજે કરે છે તે હુમલો.
સેશન હાઇજેક્સના પ્રકારો:

પ્રકાર	પદ્ધતિ	રોકથામ
એક્સિટ	સેશન કબજે કરે	મજબૂત સેશન મેનેજમેન્ટ
પેસિવ	સેશન મોનિટર કરે	એન્ક્રિપ્શન (HTTPS)
નેટવર્ક-લેવલ	TCP હાઇજેક્ઝિંગ	સુરક્ષિત પ્રોટોકોલ
એપ્લિકેશન-લેવલ	કુકી ચોરી	સુરક્ષિત કુકી એટ્રિબ્યુટ

કુમળાની પ્રક્રિયા:

- નેટવર્ક ટ્રાફિક મોનિટર કરવું
- સેશન ઓળખતારીઓ ડેપચર કરવા
- સેશન ટોકન્સ રિપ્લે કરવા
- યુઝર એકાઉન્ટ એક્સેસ કરવું

રોકથામના પગલાં:

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

મેમરી ટ્રીક

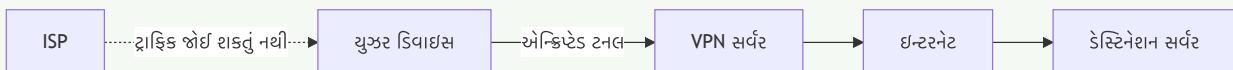
"સેશન હાઇજેકને સુરક્ષિત હેન્ડલિંગની જરૂર"

પ્રશ્ન 4(ક અથવા) [7 ગુણ]

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

જવાબ

VPN આક્રિટેક્ચર:



VPN ઘટકો:

ઘટક	ફુંક્શન	ફાયદો
ટનલિંગ	સુરક્ષિત પાથવે બનાવે	ડેટા પ્રોટેક્શન
એન્ક્રિપ્શન	ડેટાને જીણવટથી બદલે	ગોપનીયતા
ઓથેન્ટિકેશન	ઓળખ ચકાસે	એક્સેસ કંટ્રોલ
IP માસ્કિંગ	વાસ્તવિક IP છુપાવે	અનામત્વ

VPN પ્રોટોકોલ:

પ્રોટોકોલ	સુરક્ષા સ્તર	જડપ	ઉપયોગ કેસ
OpenVPN	ઉચ્ચ	સારી	સામાન્ય હેતુ
IPSec	અત્યંત ઉચ્ચ	મધ્યમ	એન્ટરપ્રાઇઝ
WireGuard	ઉચ્ચ	ઉત્કૃષ્ટ	આધુનિક સોલ્યુશન
PPTP	ઓછું	જડપી	લેગસી (અપ્રયાલિત)

VPN કાર્ય પ્રક્રિયા:

- કનેક્શન: કલાઇન્ટ VPN સર્વર સાથે જોડાય
- ઓથેન્ટિકેશન: યુઝર કેરેન્સિયલ ચકાસાય
- ટનલ ફિલેશન: એન્ક્રિપ્ટેડ પાથવે સ્થાપિત થાય
- ડેટા એન્ક્રિપ્શન: બધો ટ્રાફિક એન્ક્રિપ્ટ થાય
- રાઉટિંગ: ટ્રાફિક VPN સર્વર દ્વારા રાઉટ થાય
- ડિક્રિપ્શન: ગંતવ્ય પર ડેટા ડિક્રિપ્ટ થાય

સુરક્ષા ફૂયદાઓ:

- ડેટા પ્રોટેક્શન: એન્ક્રિપ્શન ઇવ્સફોર્મિંગ અટકાવે
- ગોપનીયતા: IP એન્ફ્રેસ માર્કિંગ
- એક્સેસ કંટ્રોલ: કનેક્શન પહેલા ઓથેન્ટિકેટ કરવું
- પ્રતિબંધો બાધ્યપાસ: જીઓ-બ્લોકડ કન્ટેન્ટ એક્સેસ કરવું

વ્યાવસાયિક એપ્લિકેશન:

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

વ્યક્તિગત ઉપયોગ કેસ:

- પાબ્લિક વાઇ-ફાઇ પ્રોટેક્શન
- ગોપનીયતા વૃદ્ધિ
- કન્ટેન્ટ એક્સેસ
- લોકેશન ગોપનીયતા

મેમરી ટ્રીક

"VPN નેટવર્ક પ્રાઇવ્સી પ્રદાન કરે"

પ્રશ્ન 5(અ) [3 ગુણ]

નેટવર્ક ફોરેન્સિક્સ સમજાવો.

જવાબ

નેટવર્ક ફોરેન્સિક્સ વ્યાખ્યા: સુરક્ષા ઘટનાઓ શોધવા અને વિશ્લેષણ કરવા માટે નેટવર્ક ટ્રાફિકની તપાસ.

મુખ્ય ઘટક:

ઘટક	હેતુ	સાધનો
ટ્રાફિક કેપ્ચર	નેટવર્ક ડેટા રેકૉર્ડ કરવો	Wireshark, tcpdump
વિશ્લેષણ	પેર્ન તપાસવા	NetworkMiner, Snort
પુરાવા	શોધોનો ઇનકાર અટકાવવો	ફોરેન્સિક રિપોર્ટ

- અવકાશ: પેકેટ્સ, ફલોડ અને નેટવર્ક વર્તણીકનું વિશ્લેષણ
- ઉદ્દેશ્ય: સુરક્ષા ભંગ અને કુમલાના પેર્ન ઔળખવા
- પડકાર: મોટા ડેટા વોલ્યુમ અને રીઅલ-ટાઇમ પ્રોસેસિંગ

મેમરી ટ્રીક

"નેટવર્ક ફોરેન્સિક્સ તથ્યો શોધો"

પ્રશ્ન 5(બ) [4 ગુણ]

ડિજિટલ ફોરેન્સિક તપાસમાં પુરાવા તરીકે CCTV શા માટે મહત્વની ભૂમિકા ભજવે છે તે સમજાવો.

જવાબ

ડિજિટલ ફોરેન્સિકસમાં CCTV:

પાસું	મહત્વ	મૂલ્ય
વિઝ્યુઅલ પુરાવા	સીધું અવલોકન	ઉચ્ચ વિશ્વસનીયતા
ટાઇમલાઈન	સમય-સ્ટેમ રેકૉર્ડ	ઘટના સહસંબંધ
ડિજિટલ ફોર્મેટ	વિશ્લેષણ કરવામાં સરળ	મેટાડાટા એક્સટ્રેક્શન
બેકઅપ	બહુવિધ કોપીઓ	પુરાવા સંરક્ષણ

પુરાવાનું મૂલ્ય:

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

ફોરેન્સિક વિચારણાઓ:

- ઘેઠન ઓફ કસ્ટડી: યોગ્ય પુરાવા હેન્ડલિંગ
- ઓથેન્ટિકેશન: વિડિયો અભિનિતતા ચકાસવી
- વિશ્લેષણ: વૃદ્ધિ અને અર્થઘટન
- કાયદેસરી સ્વીકાર્યતા: કોર્ટ-સ્વીકાર્ય ફોર્મેટ

મેમરી ટ્રીક

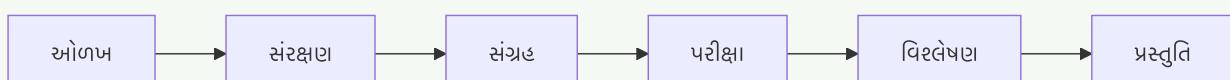
"CCTV ગુનાહિત વર્તણૂકને સ્પષ્ટ રીતે કેચચર કરે"

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	વિઝ્યુઅલ નિરીક્ષણ	અવકાશ વ્યાપ્યા
સંરક્ષણ	પુરાવા દૂધણા અટકાવવું	રાઇટ બ્લોકર	પુરાવા અધિકતા
સંગ્રહ	ડિજિટલ પુરાવા મેળવવા	ફોરેન્સિક ઇમેન્જિન્ઝિરિંગ	સંપૂર્ણ ડેટા કેચચર
પરીક્ષા	સંબંધિત ડેટા એક્સ્ટ્રેક્ટ કરવો	Autopsy, FTK	ડેટા રિકવરી
વિશ્લેષણ	શોધોનું અર્થઘટન	ટાઇમલાઈન સાધનો	પેટર્ન ઓળખ
પ્રસ્તુતિ	પરિણામોનો દસ્તાવેજ	રિપોર્ટ જનરેટર	કાયદેસર પ્રસ્તુતિ

તબક્કો 1 - ઓળખ:

- દૃશ્યનું સર્વેક્ષણ કરવું
- સંભવિત પુરાવા સ્તોતોની ઓળખ
- પ્રારંભિક અવલોકનોનો દસ્તાવેજ
- તપાસનો અવકાશ સ્થાપિત કરવો

તબક્કો 2 - સંરક્ષણ:

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

તબક્કો 3 - સંગ્રહ:

- ફોરેન્સિક ઇમેજ બનાવવી
- ચેદન ઓફ કસ્ટડી જાળવે
- ચોંચ સંગ્રહ તકનીકોનો ઉપયોગ
- વેરિફિકેશન માટે હેશ વેલ્યુ જનરેટ કરવી

તબક્કો 4 - પરીક્ષા:

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

તબક્કો 5 - વિશ્લેષણ:

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

તબક્કો 6 - પ્રસ્તુતિ:

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

ગુણવત્તા ખાતરી:

- દસ્તાવેજુકરણ: દરેક તબક્કે વિગતવાર રેકૉર્ડ
- માન્યતા: પ્રક્રિયાઓ અને પરિણામો ચકાસવા
- પુનઃઉત્પાદનક્ષમતા: પરિણામો દુલિકેટ કરી શકાય તેની ખાતરી
- કાયદેસર અનુપાલન: ન્યાયક્ષેત્રીય આવશ્યકતાઓનું પાલન

મેમરી ટ્રીક

“તપાસકર્તાઓ સંરક્ષિત કરે, એકત્ર કરે, તપાસો, વિશ્લેષણ કરે, પ્રસ્તુત કરે”

પ્રશ્ન 5(અ અથવા) [૩ ગુણ]

સાયબર સુરક્ષા સંબંધિત વિવિધ ક્ષેત્રોમાં માઇકોન્ટ્રોલરની એપ્લિકેશનોની યાદી બનાવો.

જવાબ

માઇકોન્ટ્રોલર સુરક્ષા એપ્લિકેશન:

ક્ષેત્ર	એપ્લિકેશન	સુરક્ષા ફુંક્શન
IoT સુરક્ષા	સ્માર્ટ હોમ ડિવાઇસ	ઓથેન્ટિકેશન, એન્ક્રિપ્શન
એક્સોસ કંટ્રોલ	કી કાર્ડ, બાયોમેટ્રિક	ઓળખ ચકાસણી
નેટવર્ક સુરક્ષા	હાર્ડવેર ફાયરવોલ	પેકેટ ફિલ્ટરિંગ

- સ્માર્ટ કાર્ડ: સુરક્ષિત ઓથેન્ટિકેશન ટોકન
- HSM (હાર્ડવેર સિક્યુરિટી મોડ્યુલ): કિપ્ટોગ્રાફિક પ્રોસેસિંગ
- એમ્બેડેડ સિસ્ટમ: સિક્યુર બૂટ, ટેમ્પર ડિટેક્શન

મેમરી ટ્રીક

"માઇકોન્ટ્રોલર બહુવિધ સુરક્ષા ફંક્શન મેનેજ કરે"

પ્રશ્ન 5(બ અથવા) [4 ગુણ]

નૈતિક (એથિકલ) હેક્ટિગમાં પોર્ટ સ્કેનિંગનું મહત્વ સમજાવો.

જવાબ

એથિકલ હેક્ટિગમાં પોર્ટ સ્કેનિંગ:

પાસું	મહત્વ	કાયદો
સેવા શોધ	ચાલતી સેવાઓ ઓળખવી	હુમલા સપાઠીનું મેપિંગ
વલન્રેબિલિટી એસેસમેન્ટ	ખુલ્લા પોર્ટ શોધવા	સુરક્ષા ગેપ ઓળખ
નેટવર્ક મેપિંગ	ટોપોલોજી સમજવી	ઇન્ફાસ્ટ્રક્ચર વિશ્લેષણ
સુરક્ષા પરીક્ષા	કોન્ફિગરેશન માન્ય કરવી	અનુપાલન ચકાસણી

પોર્ટ સ્કેનિંગ તકનીકો:

- TCP કનેક્ટા: સંપૂર્ણ કનેક્શન સ્થાપના
- SYN સ્કેન: સ્ટેલ્થ સ્કેનિંગ પદ્ધતિ
- UDP સ્કેન: યુઝર ડેટાગ્રામ પ્રોટોકોલ સ્કેનિંગ
- સેવા ડિટેક્શન: સેવા વર્જન ઓળખવી

નૈતિક વિચારણાઓ:

- અધિકૃતતા: યોગ્ય પરવાનગી મેળવવી
- અવકાશ: નિર્ધારિત સીમાઓમાં રહેવું
- દસ્તાવેજુકરણ: બધી પ્રવૃત્તિઓ રેકૉર્ડ કરવી
- રિપોર્ટિંગ: વિગતવાર શોધો પ્રદાન કરવી

મેમરી ટ્રીક

"પોર્ટ સ્કેનિંગ સુરક્ષા આંતરરદ્ધિ પ્રદાન કરે"

પ્રશ્ન 5(ક અથવા) [7 ગુણ]

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

જવાબ

વલન્રેબિલિટી એસેસમેન્ટ પ્રક્રિયા:



પગલું-દર-પગલું પ્રક્રિયા:

પગલું	કાલી ટૂલ	કમાન્ડ ઉદાહરણ	હેતુ
રિકોનેસન્સ	Nmap	nmap -sn 192.168.1.0/24	હોરસ શોધ
પોર્ટ સ્કેનિંગ	Nmap	nmap -sS -O target	ખુલ્લા પોર્ટની ઓળખ
સેવા ગણતરી	Nmap, બેનર ગ્રેબિંગ	nmap -sV target	સેવા વર્જન ડિટેક્શન
વલન્રેબિલિટી સ્કેનિંગ	OpenVAS, Nessus	openvas-start	ઓટોમેટેડ વલન્રેબિલિટી ડિટેક્શન
વેબ એપ્લિકેશન પરીક્ષણ	Nikto, Dirb	nikto -h target	વેબ વલન્રેબિલિટી સ્કેનિંગ

વિગતવાર પ્રક્રિયા:

તબક્કો 1 - લક્ષ્ય ઓળખ:

- નેટવર્ક ડિસ્કવરી માટે Nmap નો ઉપયોગ
- લાઇવ હોરટ અને તેમના IP એડ્રેસની ઓળખ
- નેટવર્ક ટોપોલોજીનો દસ્તાવેજ
- લક્ષ્ય અવકાશ નિર્ધારણ

તબક્કો 2 - પોર્ટ અને સેવા વિશ્લેષણ:

- વ્યાપક પોર્ટ સ્કેન કરવા
- ચાલતી સેવાઓ અને વર્જન ઓળખવા
- ડિફોલ્ટ કેરેન્શિયલ ચકાસવા
- સેવા કોન્ફિગરેશન વિશ્લેષણ

તબક્કો 3 - ઓટોમેટેડ વલન્રેબિલિટી સ્કેનિંગ:

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

તબક્કો 4 - મેન્યુઅલ પરીક્ષણ:

- ઓટોમેટેડ શોધોની ચકાસણી
- લક્ષિત પરીક્ષણ કરવું
- વિશિષ્ટ વલન્રેબિલિટી માટે પરીક્ષણ
- ફોલ્સ પોર્ઝિટિવ માન્ય કરવા

તબક્કો 5 - વેબ એપ્લિકેશન એસેસમેન્ટ:

- વેબ વલન્રેબિલિટી સ્કેનરનો ઉપયોગ
- OWASP ટોપ 10 વલન્રેબિલિટી માટે પરીક્ષણ
- એપ્લિકેશન લોજિકનું વિશ્લેષણ
- મિસકોન્ફિગરેશન ચકાસવા

સામાન્ય કાલી ટૂલ્સ:

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

એસેસમેન્ટ પદ્ધતિ:

- અવકાશ વ્યાખ્યા: એસેસમેન્ટ સીમાઓ સ્પષ્ટ રીતે વ્યાખ્યાપિત કરવી
- માહિતી એક્સ્પ્લોટેશન: લક્ષ્ય ઇન્ટેલિજન્સ એક્ટર કરવી
- વલન્રેબિલિટી ડિટેક્શન: બહુવિધ સ્કેનિંગ પદ્ધતિઓનો ઉપયોગ
- જોખમ એસેસમેન્ટ: અસર અને સંભાવનાનું મૂલ્યાંકન
- રેમેડિએશન પ્લાનિંગ: કાર્યક્ષમ ભલામણો પ્રદાન કરવી

રિપોર્ટિંગ ઘટકો:

- એક્ઝિક્યુટિવ સમરી: મેનેજમેન્ટ માટે ઉચ્ચ-સ્તરીય શોધો
- તકનીકી વિગતો: વલન્રેબિલિટીના વિગતવાર વર્ણનો
- જોખમ રેટિંગ: CVSS સ્કોર અને બિગનેસ અસર
- રેમેડિએશન સ્ટેપ્સ: વિશિષ્ટ મિટિંગેશન ભલામણો
- સપોર્ટિંગ એવિન્સ: સ્કીનશોટ અને પ્રૂફ-ઓફ-કોન્સેપ્ટ

બેસ્ટ પ્રેક્ટિસિસ:

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

મેમરી ટ્રીક

“વલન્રેબિલિટી એસેસમેન્ટ એપ્લિકેશન સિક્યુરિટીને માન્ય કરે”