Cyber Security (4353204) - Summer 2025 Solution

Milav Dabgar

May 16, 2025

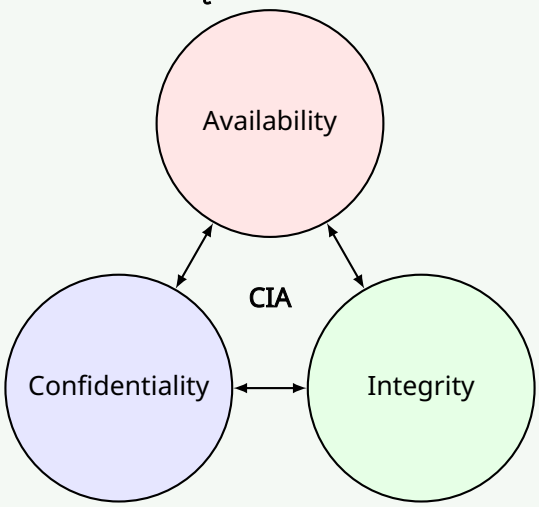
પ્રશ્ન 1(a) [3 ગુણ]

Example with CIA triad description.

જવાબ

CIA ત્રિપુટીના ઘટકો:

આકૃતિ 1. CIA Triad



કોષ્ટક 1. CIA Triad Elements

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

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

મેમરી ટ્રીક

``CIA માહિતી ને સુરક્ષિત રાખે''

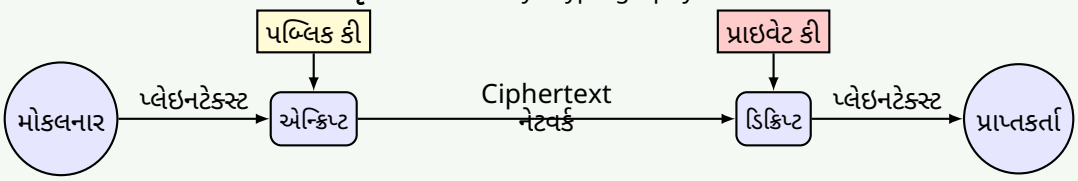
પ્રશ્ન 1(b) [4 ગુણ]

Explain Public key and Private Key cryptography.

જવાબ

પબ્લિક કી ક્રિપ્ટોગ્રાફી (એસિમેટ્રિક):

આકૃતિ 2. Public Key Cryptography Flow



મુખ્ય લક્ષણો:

કોષ્ટક 2. Public vs Private Key

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**: ગાણિતિક જટિલતા પર આધારિત (RSA, ECC અલ્ગોરિધમ)

મેમરી ટ્રીક

``પબ્લિક એન્ક્રિપ્ટ કરે, પ્રાઇવેટ ડિક્રિપ્ટ કરે''

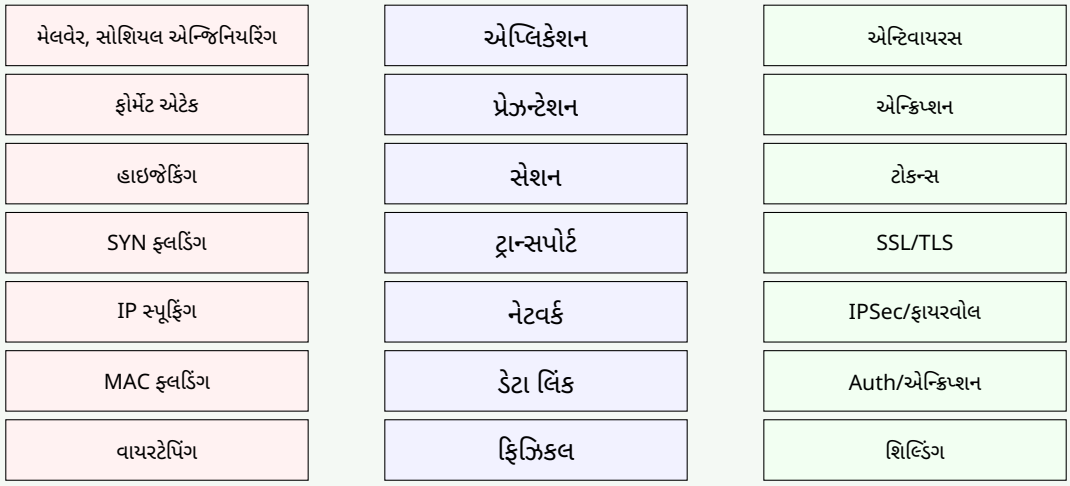
પ્રશ્ન 1(c) [7 ગુણ]

Explain various security attacks, mechanisms, and services associated with each layer of the OSI model.

જવાબ

OSI સુરક્ષા ફ્રેમવર્ક:

આકૃતિ 3. OSI Security Framework



કોષ્ટક 3. OSI Layers Security Details

સ્તર	હુમલાઓ	પદ્ધતિઓ	સેવાઓ
ફિઝિકલ	વાયરટેપિંગ, જેમિંગ	ફિઝિકલ સિક્યોરિટી, શિલ્ડિંગ	એક્સેસ કંટ્રોલ
ડેટા લિંક	MAC ફ્લડિંગ, ARP પોઇઝનિંગ	એન્ક્રિપ્શન, ઓથેન્ટિકેશન	ફ્રેમ ઇન્ટેગ્રિટી
નેટવર્ક	IP સ્પૂફિંગ, રાઉટિંગ એટેક	IPSec, ફાયરવોલ	પેકેટ ફિલ્ટરિંગ
ટ્રાન્સપોર્ટ	સેશન હાઇજેકિંગ, SYN ફ્લડિંગ	SSL/TLS, પોર્ટ સિક્યોરિટી	એન્ડ-ટુ-એન્ડ સિક્યોરિટી
સેશન	સેશન રિપ્લે, હાઇજેકિંગ	સેશન ટોકન, ટાઇમઆઉટ	સેશન મેનેજમેન્ટ
પ્રેઝન્ટેશન	ડેટા કરપ્શન, ફોર્મેટ એટેક	એન્ક્રિપ્શન, કમ્પ્રેશન	ડેટા ટ્રાન્સફોર્મેશન
એપ્લિકેશન	મેલવેર, સોશિયલ એન્જિનિયરિંગ	એન્ટિવાયરસ, યુઝર ટ્રેનિંગ	એપ્લિકેશન સિક્યોરિટી

મુખ્ય સુરક્ષા સેવાઓ:
- **ઓથેન્ટિકેશન**: યુઝર આઇડેન્ટિટી વેરિફિકેશન
- **ઓથોરાઇઝેશન**: એક્સેસ પરમિશન કંટ્રોલ
- **નોન-રિપ્યુડિએશન**: ક્રિયાઓનો ઇનકાર અટકાવવો
- **ડેટા ઇન્ટેગ્રિટી**: ડેટાની ચોકસાઈ સુનિશ્ચિત કરવી

મેમરી ટ્રીક

``બધા લોકોને ડેટા પ્રોટેક્શનની જરૂર છે''

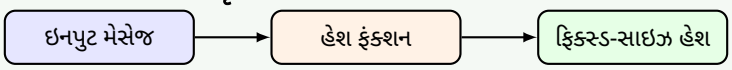
પ્રશ્ન 1(c OR) [7 ગુણ]

Explain MD5 hashing and Secure Hash Function (SHA) algorithms.

જવાબ

હેશ ફંક્શન સરખામણી:

આકૃતિ 4. Hash Function Process



કોષ્ટક 4. MD5 vs SHA Comparison

વિશેષતા	MD5	SHA-1	SHA-256
આઉટપુટ સાઇઝ	128 બિટ્સ	160 બિટ્સ	256 બિટ્સ
સુરક્ષા સ્તર	નબળું	નબળું	મજબૂત
ઝડપ	ઝડપી	મધ્યમ	ધીમું
વર્તમાન સ્થિતિ	અપ્રચલિત	અપ્રચલિત	ભલામણ કરેલ

હેશ ગુણધર્મો:
- **ડિટર્મિનિસ્ટિક**: સમાન ઇનપુટ સમાન હેશ આપે
- **એવેલાન્ચ ઇફેક્ટ**: 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 સર્ટિફિકેટ
- ડેટા ઇન્ટેગ્રિટી ચેકિંગ

મેમરી ટ્રીક

``હેશ હંમેશા સમાન આઉટપુટ આપે''

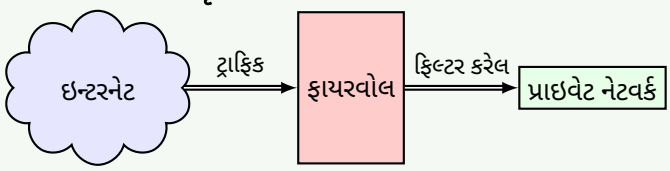
પ્રશ્ન 2(a) [3 ગુણ]

What is firewall? List out types of firewall.

જવાબ

ફાયરવોલ વ્યાખ્યા: નેટવર્ક સિક્યોરિટી ડિવાઇસ જે સુરક્ષા નિયમોના આધારે આવતા-જતા ટ્રાફિકને મોનિટર અને કંટ્રોલ કરે છે.

આકૃતિ 5. Firewall Architecture



ફાયરવોલના પ્રકારો:

કોષ્ટક 5. Firewall Types

પ્રકાર	ફંક્શન	સ્તર
પેકેટ ફિલ્ટર	પેકેટ હેડર તપાસે	નેટવર્ક લેયર
સ્ટેટફુલ	કનેક્શન સ્ટેટ ટ્રેક કરે	ટ્રાન્સપોર્ટ લેયર
એપ્લિકેશન પ્રોક્સી	એપ્લિકેશન ડેટા તપાસે	એપ્લિકેશન લેયર
પર્સનલ ફાયરવોલ	વ્યક્તિગત ડિવાઇસ સુરક્ષા	હોસ્ટ-બેસ્ડ

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

મેમરી ટ્રીક

``ફાયરવોલ હંમેશા નેટવર્કનું રક્ષણ કરે''

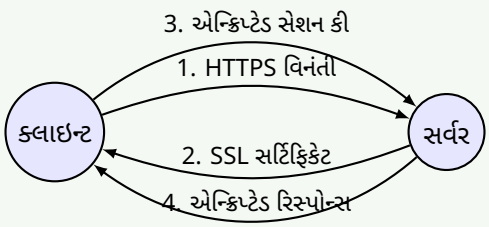
પ્રશ્ન 2(b) [4 ગુણ]

Define: HTTPS and describe working of HTTPS.

જવાબ

HTTPS વ્યાખ્યા: Hypertext Transfer Protocol Secure - SSL/TLS એન્ક્રિપ્શન પર HTTP.
HTTPS કાર્ય પ્રક્રિયા:

આકૃતિ 6. HTTPS Process



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 પ્રોટેક્શન
- SEO રેંકિંગ સુધારો

મેમરી ટ્રીક

``HTTPS વેબ ટ્રાફિકને સુરક્ષિત કરે''

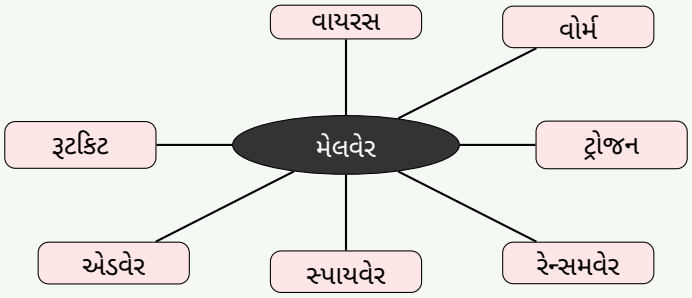
પ્રશ્ન 2(c) [7 ગુણ]

Explain different types of malicious software and their effect.

જવાબ

મેલવેર વર્ગીકરણ:

આકૃતિ 7. Malware Classification



કોષ્ટક 6. Malware Types and Effects

પ્રકાર	વર્તન	અસર	ઉદાહરણ
વાયરસ	ફાઇલો સાથે જોડાય	ફાઇલ કરપ્શન	બૂટ સેક્ટર વાયરસ
વોર્મ	સ્વ-પ્રતિકૃતિ	નેટવર્ક ભીડ	કન્ફિકર વોર્મ
ટ્રોજન	છદ્મવેશી મેલવેર	ડેટા ચોરી	બેંકિંગ ટ્રોજન
રેન્સમવેર	ફાઇલો એન્ક્રિપ્ટ કરે	ડેટા બંધક	WannaCry
સ્પાયવેર	પ્રવૃત્તિ મોનિટર કરે	ગોપનીયતા ભંગ	કીલોગર
એડવેર	અનચાહેલી જાહેરાતો	પ્રદર્શન ઘટાડો	પોપ-અપ જાહેરાતો
રૂટકિટ	હાજરી છુપાવે	સિસ્ટમ સમાધાન	કર્નલ રૂટકિટ

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

રોકથામના પદ્ધતિઓ:
- નિયમિત એન્ટિવાયરસ અપડેટ
- સુરક્ષિત બ્રાઉઝિંગ પ્રેક્ટિસ
- ઇમેઇલ એટેચમેન્ટમાં સાવધાની
- સિસ્ટમ સિક્યોરિટી પેચ

મેમરી ટ્રીક

``વાયરસ વોર્મ ટ્રોજન ખરેખર બધા સંસાધનો ચોરે''

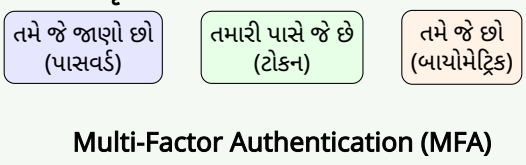
પ્રશ્ન 2(a OR) [3 ગુણ]

What is authentication? Explain different methods of authentication.

જવાબ

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

આકૃતિ 8. Authentication Methods



ઓથેન્ટિકેશન પદ્ધતિઓ:

કોષ્ટક 7. Authentication Factors

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

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

મેમરી ટ્રીક

``પાસવર્ડ બાયોમેટ્રિક ટોકન ઓથેન્ટિકેશન''

પ્રશ્ન 2(b OR) [4 ગુણ]

Define: Trojans, Rootkit, Backdoors, Keylogger

જવાબ

મેલવેર વ્યાખ્યાઓ:

કોષ્ટક 8. Malware Definitions

શબ્દ	વ્યાખ્યા	લક્ષણો
ટ્રોજન્સ	કાયદેસર સોફ્ટવેરના છદ્મવેશમાં મેલવેર	હાનિકારક દેખાય, છુપાયેલ પેલોડ
રૂટકિટ	મેલવેરની હાજરી છુપાવતો સોફ્ટવેર	ઊંડી સિસ્ટમ એક્સેસ, સ્ટેલ્થ ઓપરેશન
બેકડોર્સ	અનધિકૃત એક્સેસ પદ્ધતિ	સામાન્ય ઓથેન્ટિકેશન બાયપાસ કરે
કીલોગર	કીબોર્ડ ઇનપુટ રેકોર્ડ કરે	પાસવર્ડ, સંવેદનશીલ ડેટા કેપ્ચર 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''

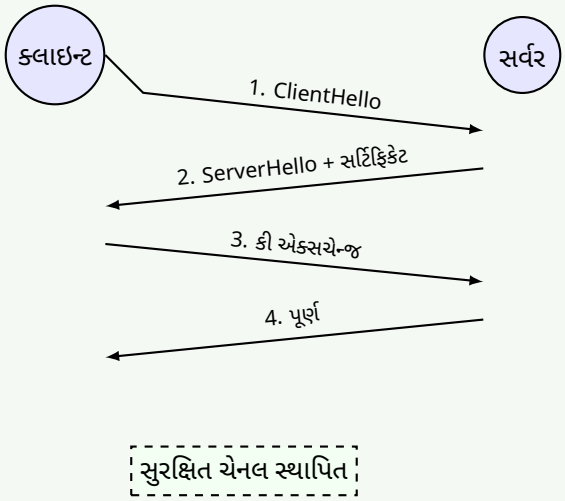
પ્રશ્ન 2(c OR) [7 ગુણ]

SSL and TLS protocols.

જવાબ

SSL/TLS પ્રોટોકોલ ઉત્ક્રાંતિ:

આકૃતિ 9. SSL/TLS Handshake



કોષ્ટક 9. SSL/TLS Comparison

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

મુખ્ય વિશેષતાઓ:
- **એન્ક્રિપ્શન**: સિમેટ્રિક અને એસિમેટ્રિક અલ્ગોરિધમ
- **ઓથેન્ટિકેશન**: સર્વર અને ક્લાયન્ટ વેરિફિકેશન
- **ઇન્ટેગ્રિટી**: મેસેજ ઓથેન્ટિકેશન કોડ
- **ફોરવર્ડ સિક્રેસી**: સેશન કી પ્રોટેક્શન

એપ્લિકેશન:
- HTTPS વેબ બ્રાઉઝિંગ
- ઇમેઇલ સિક્યોરિટી (SMTPS)
- VPN કનેક્શન
- સુરક્ષિત ફાઇલ ટ્રાન્સફર

મેમરી ટ્રીક

``TLS બધા નેટવર્ક ટ્રાફિકને એન્ક્રિપ્ટ કરે''

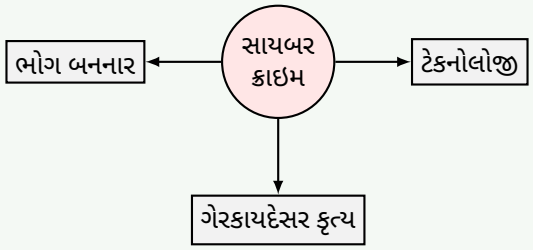
પ્રશ્ન 3(a) [3 ગુણ]

Explain in detail cybercrime and cybercriminal.

જવાબ

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

આકૃતિ 10. Cybercrime Overview



સાયબરક્રિમિનલ પ્રકારો:

કોષ્ટક 10. Types of Cybercriminals

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

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

મેમરી ટ્રીક

``સાયબર ક્રિમિનલો અરાજકતા સર્જે છે''

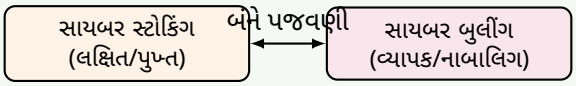
પ્રશ્ન 3(b) [4 ગુણ]

Describe cyber stalking and cyber bullying in detail.

જવાબ

ડિજિટલ પજવણી સરખામણી:

આકૃતિ 11. Stalking vs Bullying



કોષ્ટક 11. Stalking vs Bullying

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

સાયબર સ્ટોકિંગ લક્ષણો:
- સતત અનચાહેલ સંપર્ક
- પીડિતની ઓનલાઇન પ્રવૃત્તિનું મોનિટરિંગ
- ધમકીભર્યા સંદેશાઓ અથવા વર્તન
- ઓળખની ચોરી અથવા ઢોંગ

સાયબર બુલીંગ સ્વરૂપો:
- ઓનલાઇન જાહેર અપમાન
- ડિજિટલ જૂથોમાંથી બાકાત

- ખોટી માહિતી ફેલાવવી
- સંમતિ વિના ખાનગી સામગ્રી શેર કરવી

મેમરી ટ્રીક

``બુલીંગ બંધ કરો, સ્ટોકિંગની જાણ કરો''

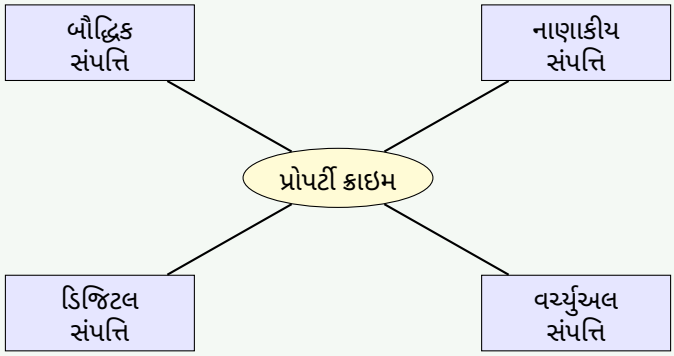
પ્રશ્ન 3(c) [7 ગુણ]

Explain Property based classification in cybercrime.

જવાબ

પ્રોપર્ટી-આધારિત સાયબર ક્રાઇમ શ્રેણીઓ:

આકૃતિ 12. Property-Based Cybercrime



કોષ્ટક 12. Property Crime Classification

શ્રેણી	ક્રાઇમ પ્રકાર	વર્ણન	ઉદાહરણ
બૌદ્ધિક સંપત્તિ	કોપીરાઇટ ઉલ્લંઘન	કોપીરાઇટ સામગ્રીનો અનધિકૃત ઉપયોગ	સોફ્ટવેર પાયરેસી
નાણાકીય સંપત્તિ	ક્રેડિટ કાર્ડ ફ્રોડ	નાણાકીય માહિતીનો અનધિકૃત ઉપયોગ	ઓનલાઇન શોપિંગ ફ્રોડ
ડિજિટલ સંપત્તિ	ડેટા ચોરી	ડિજિટલ માહિતીની ચોરી	ડેટાબેસ બ્રીચ
વર્ચ્યુઅલ સંપત્તિ	ગેમિંગ એસેટ ચોરી	વર્ચ્યુઅલ વસ્તુઓની ચોરી	ઓનલાઇન ગેમ કરન્સી ચોરી

કાયદેસરના પાસાઓ:
- **કોપીરાઇટ કાયદાઓ**: સર્જનાત્મક કાર્યોનું રક્ષણ
- **ટ્રેડમાર્ક કાયદાઓ**: બ્રાન્ડ ઓળખનું રક્ષણ
- **પેટન્ટ કાયદાઓ**: આવિષ્કારોનું રક્ષણ
- **ટ્રેડ સિક્રેટ કાયદાઓ**: ગોપનીય માહિતીનું રક્ષણ

મેમરી ટ્રીક

``પ્રોપર્ટી પ્રોટેક્શન પાયરેસી અટકાવે''

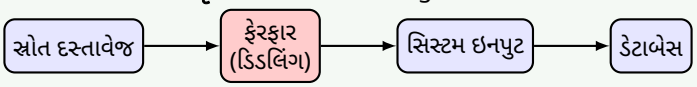
પ્રશ્ન 3(a OR) [3 ગુણ]

Explain Data diddling.

જવાબ

ડેટા ડિડલિંગ વ્યાખ્યા: કમ્પ્યુટર સિસ્ટમમાં ડેટા દાખલ કરતા પહેલા અથવા દરમિયાન અનધિકૃત ફેરફાર.

આકૃતિ 13. Data Diddling Process



કોષ્ટક 13. Data Diddling Characteristics

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 રેકોર્ડ

મેમરી ટ્રીક

``ડેટા ડિડલિંગ ડેટાબેસને નુકસાન પહોંચાડે''

પ્રશ્ન 3(b OR) [4 ગુણ]

Explain cyber spying and cyber terrorism.

જવાબ

સાયબર ધમકીઓની સરખામણી:

કોષ્ટક 14. Spying vs Terrorism

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

સાયબર સ્પાઇંગ પ્રવૃત્તિઓ:
- કોર્પોરેટ જાસૂસી
- સરકારી દેખરેખ
- ટ્રેડ સિક્રેટ ચોરી

સાયબર ટેરરીઝમ પદ્ધતિઓ:
- ઇન્ફ્રાસ્ટ્રક્ચર હુમલાઓ
- મોટા પાયે વિક્ષેપ ઝુંબેશ
- મનોવૈજ્ઞાનિક યુદ્ધ

મેમરી ટ્રીક

``જાસૂસો ચોરે, આતંકવાદીઓ આતંક''

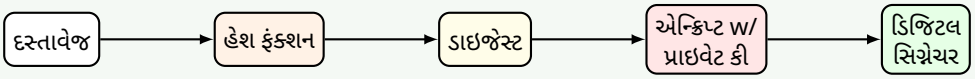
પ્રશ્ન 3(c OR) [7 ગુણ]

Explain the role of digital signatures and digital certificates in cybersecurity.

જવાબ

ડિજિટલ સુરક્ષા ઘટકો:

આકૃતિ 14. Digital Signature Process



કોષ્ટક 15. Digital Security Components

ઘટક	હેતુ	ફંક્શન	ફાયદો
ડિજિટલ સિગ્નેચર	ઓથેન્ટિકેશન	મોકલનારની ઓળખ સાબિત કરે	નોન-રિપ્યુડિએશન
ડિજિટલ સર્ટિફિકેટ	વેરિફિકેશન	પબ્લિક કીની માન્યતા	વિશ્વાસ સ્થાપના

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

સર્ટિફિકેટ ઓથોરિટી (CA) ભૂમિકા:
- ડિજિટલ સર્ટિફિકેટ જારી કરે
- જારી કરતા પહેલા ઓળખ ચકાસે
- વિશ્વાસ ઇન્ફ્રાસ્ટ્રક્ચર પૂરું પાડે

સુરક્ષા ફાયદાઓ:
- **ઓથેન્ટિકેશન**: મોકલનારની ઓળખ ચકાસે
- **ઇન્ટેગ્રિટી**: ડેટામાં ફેરફાર થયો નથી તેની ખાતરી
- **નોન-રિપ્યુડિએશન**: ક્રિયાઓનો ઇનકાર અટકાવે
- **ગોપનીયતા**: સુરક્ષિત કમ્યુનિકેશન સક્ષમ કરે

મેમરી ટ્રીક

``ડિજિટલ સિગ્નેચર ડોક્યુમેન્ટને સુરક્ષિત રીતે પ્રમાણિત કરે''

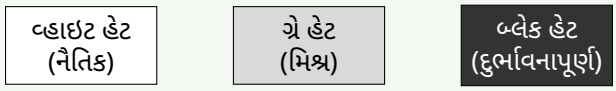
પ્રશ્ન 4(a) [3 ગુણ]

What is Hacking? List out types of Hackers.

જવાબ

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

આકૃતિ 15. Hacker Types



હેકર વર્ગીકરણ:

કોષ્ટક 16. Types of Hackers

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

મેમરી ટ્રીક

``સફેદ સારું, કાળું ખરાબ, ગ્રે શંકાસ્પદ''

પ્રશ્ન 4(b) [4 ગુણ]

Explain Vulnerability and 0-Day terminology of Hacking.

જવાબ

સુરક્ષા પરિભાષા:

કોષ્ટક 17. Vulnerability vs 0-Day

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

વલ્નરેબિલિટી લક્ષણો:
- સુરક્ષા પરીક્ષણ દ્વારા શોધ
- વેન્ડરને જવાબદાર રિપોર્ટિંગ
- વેન્ડર સુરક્ષા અપડેટ પૂરું પાડે

0-દિવસ હુમલો પ્રક્રિયા:
1. હેકર અજાણી નબળાઈ શોધે
2. વેન્ડરની જાણકારી પહેલા ખામીનો ફાયદો ઉઠાવે
3. કોઈ ઉપલબ્ધ પેચ અથવા સંરક્ષણ નથી
4. આશ્ચર્યના કારણે ઉચ્ચ સફળતા દર

મેમરી ટ્રીક

``નબળાઈઓને પેચની જરૂર, ઝીરો-ડેને સાવચેતીની જરૂર''

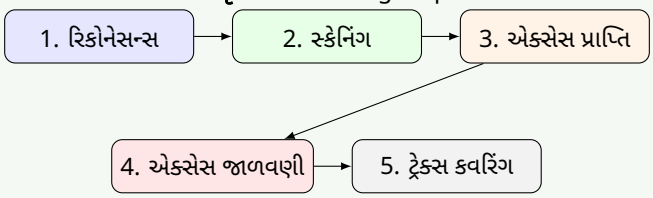
પ્રશ્ન 4(c) [7 ગુણ]

Explain Five Steps of Hacking.

જવાબ

હેકિંગ પદ્ધતિ:

આકૃતિ 16. Hacking Steps



વિગતવાર પગલાંઓ:

કોષ્ટક 18. Hacking Phases

પગલું	વર્ણન	સાધનો/પદ્ધતિઓ	ઉદ્દેશ્ય
રિકોનેસન્સ	માહિતી એકત્રીકરણ	Google dorking	લક્ષ્ય પ્રોફાઇલિંગ
સ્કેનિંગ	સિસ્ટમ ગણતરી	Nmap, Nessus	નબળાઈ ઓળખ
એક્સેસ પ્રાપ્તિ	નબળાઈઓનો ફાયદો	Metasploit	સિસ્ટમ સમાધાન
એક્સેસ જાળવણી	સતત હાજરી	બેકડોર, રૂટકિટ	લાંબા ગાળાનું નિયંત્રણ
ટ્રેક્સ કવરિંગ	પુરાવા દૂર કરવા	લોગ સફાઇ	શોધ ટાળવી

મેમરી ટ્રીક

``રિકોનેસન્સ સ્કેન્સ એક્સેસ જનરેટ કરે, કવરેજ જાળવે''

પ્રશ્ન 4(a OR) [3 ગુણ]

Explain any three basic commands of Kali Linux with suitable example.

જવાબ

અત્યાવશ્યક કાલી લિનક્સ કમાન્ડ્સ:

કોષ્ટક 19. Kali Commands

કમાન્ડ	ફંક્શન	ઉદાહરણ
nmap	નેટવર્ક સ્કેનિંગ	nmap -sS 192.168.1.1
netcat	નેટવર્ક કમ્યુનિકેશન	nc -l -p 1234
hydra	પાસવર્ડ ક્રેકિંગ	hydra -l admin ...

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

મેમરી ટ્રીક

``નેટવર્ક મેપ, કનેક્ટ, ક્રેક''

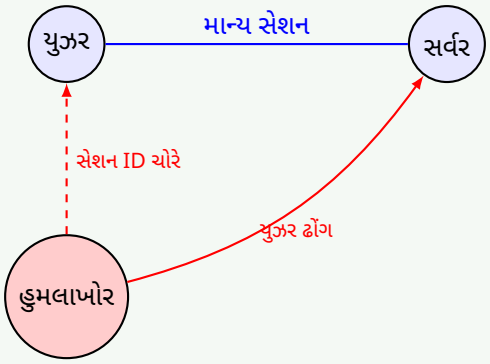
પ્રશ્ન 4(b OR) [4 ગુણ]

Describe Session Hijacking in detail.

જવાબ

સેશન હાઇજેકિંગ ઓવરવ્યુ: હુમલાખોર કાયદેસર યુઝરના સેશનને કબજે કરે છે તે હુમલો.

આકૃતિ 17. Session Hijacking



કોષ્ટક 20. Hijacking Types

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

રોકથામના પગલાં:
- બધા કમ્યુનિકેશન માટે HTTPS નો ઉપયોગ
- સુરક્ષિત સેશન મેનેજમેન્ટ અમલીકરણ
- શંકાસ્પદ પ્રવૃત્તિ માટે મોનિટરિંગ

મેમરી ટ્રીક

``સેશન હાઇજેકને સુરક્ષિત હેન્ડલિંગની જરૂર''

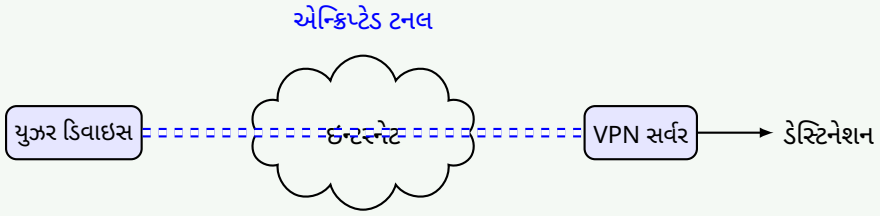
પ્રશ્ન 4(c OR) [7 ગુણ]

Explain how Virtual Private Networks (VPNs) create secure, encrypted connections over public networks.

જવાબ

VPN આર્કિટેક્ચર:

આકૃતિ 18. VPN Architecture



કોષ્ટક 21. VPN Protocols

પ્રોટોકોલ	સુરક્ષા	ઝડપ	ઉપયોગ કેસ
OpenVPN	ઉચ્ચ	સારી	સામાન્ય હેતુ
IPSec	અત્યંત ઉચ્ચ	મધ્યમ	એન્ટરપ્રાઇઝ
WireGuard	ઉચ્ચ	ઉત્કૃષ્ટ	આધુનિક સોલ્યુશન
PPTP	ઓછું	ઝડપી	લેગસી (અપ્રચલિત)

VPN કાર્ય પ્રક્રિયા:
- **કનેક્શન**: ક્લાઇન્ટ VPN સર્વર સાથે જોડાય
- **ઓથેન્ટિકેશન**: યુઝર ક્રેડેન્શિયલ ચકાસાય
- **ટનલ ક્રિએશન**: એન્ક્રિપ્ટેડ પાથવે સ્થાપિત થાય
- **ડેટા એન્ક્રિપ્શન**: બધો ટ્રાફિક એન્ક્રિપ્ટ થાય

મેમરી ટ્રીક

``VPN નેટવર્ક પ્રાઇવસી પ્રદાન કરે''

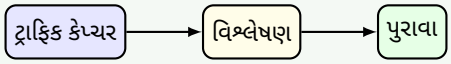
પ્રશ્ન 5(a) [3 ગુણ]

Explain Network forensics.

જવાબ

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

આકૃતિ 19. Network Forensics Process



Wireshark, tcpdump

મુખ્ય ઘટકો:

કોષ્ટક 22. Network Forensics Components

ઘટક	હેતુ	સાધનો
ટ્રાફિક કેપ્ચર	નેટવર્ક ડેટા રેકોર્ડ કરવો	Wireshark, tcpdump
વિશ્લેષણ	પેટર્ન તપાસવા	NetworkMiner, Snort
પુરાવા	શોધોનો દસ્તાવેજ	ફોરેન્સિક રિપોર્ટ

મેમરી ટ્રીક

``નેટવર્ક ફોરેન્સિક્સ તથ્યો શોધે''

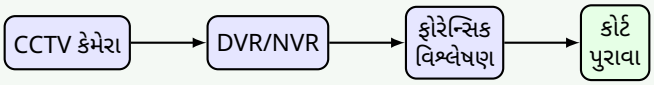
પ્રશ્ન 5(b) [4 ગુણ]

Explain why CCTV plays an important role as evidence in digital forensics investigations.

જવાબ

ડિજિટલ ફોરેન્સિકસમાં CCTV:

આકૃતિ 20. CCTV Evidence



કોષ્ટક 23. CCTV Evidence Value

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

પુરાવાનું મૂલ્ય:
- **સમર્થન**: અન્ય ડિજિટલ પુરાવાઓને સમર્થન આપે
- **ટાઇમલાઇન**: ઘટનાઓનો ક્રમ સ્થાપિત કરે
- **ઓળખ**: ગુનેગારની ઓળખ પ્રગટ કરી શકે

મેમરી ટ્રીક

``CCTV ગુનાહિત વર્તણૂકને સ્પષ્ટ રીતે કેપ્ચર કરે''

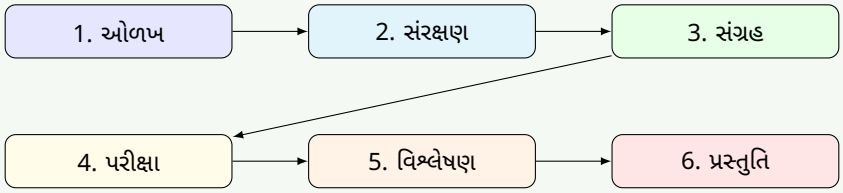
પ્રશ્ન 5(c) [7 ગુણ]

Explain phases of Digital forensic investigation.

જવાબ

ડિજિટલ ફોરેન્સિકસ તપાસના તબક્કાઓ:

આકૃતિ 21. Digital Forensics Phases



વિગતવાર તબક્કાનું વિભાજન:

કોષ્ટક 24. Investigation Phases

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

તબક્કો 1 - ઓળખ: સંભવિત પુરાવા સ્ત્રોતોની ઓળખ **તબક્કો 2 - સંરક્ષણ:** અપરાધ સ્થળ સુરક્ષિત કરવું **તબક્કો 3 - સંગ્રહ:** ફોરેન્સિક ઇમેજ બનાવવી **તબક્કો 4 - પરીક્ષા:** ડેટા એક્સટ્રેક્ટ કરવો **તબક્કો 5 - વિશ્લેષણ:** ઘટનાઓનું પુનઃનિર્માણ **તબક્કો 6 - પ્રસ્તુતિ:** વિગતવાર રિપોર્ટ તૈયાર કરવો

મેમરી ટ્રીક

``તપાસકર્તાઓ સંરક્ષિત કરે, એકત્ર કરે, તપાસે, વિશ્લેષણ કરે, પ્રસ્તુત કરે''

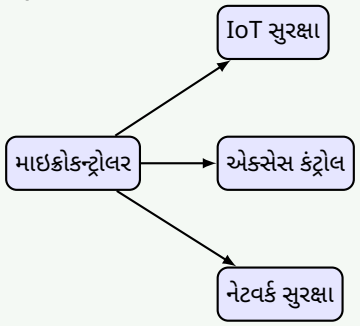
પ્રશ્ન 5(a OR) [3 ગુણ]

List applications of microcontrollers in various fields related to cybersecurity.

જવાબ

માઇક્રોકન્ટ્રોલર સુરક્ષા એપ્લિકેશન:

આકૃતિ 22. Microcontroller Security



કોષ્ટક 25. Microcontroller Applications

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

- **સ્માર્ટ કાર્ડ**: સુરક્ષિત ઓથેન્ટિકેશન ટોકન
- **HSM**: ક્રિપ્ટોગ્રાફિક પ્રોસેસિંગ મોડ્યુલ
- **એમ્બેડેડ સિસ્ટમ**: સિક્યોર બૂટ

મેમરી ટ્રીક

``માઇક્રોકન્ટ્રોલર બહુવિધ સુરક્ષા ફંક્શન મેનેજ કરે''

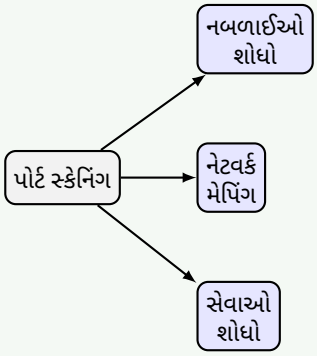
પ્રશ્ન 5(b OR) [4 ગુણ]

Explain the importance of port scanning in ethical hacking.

જવાબ

એથિકલ હેકિંગમાં પોર્ટ સ્કેનિંગ:

આકૃતિ 23. Port Scanning Benefits



કોષ્ટક 26. Port Scanning Importance

પાસું	મહત્વ	ફાયદો
સેવા શોધ	ચાલતી સેવાઓ ઓળખવી	હુમલા સપાટીનું મેપિંગ
વલ્નરેબિલિટી	ખુલ્લા પોર્ટ શોધવા	સુરક્ષા ગેપ ઓળખ
નેટવર્ક મેપિંગ	ટોપોલોજી સમજવી	ઇન્ફ્રાસ્ટ્રક્ચર વિશ્લેષણ
સુરક્ષા પરીક્ષણ	કોન્ફિગરેશન માન્ય કરવી	અનુપાલન ચકાસણી

મેમરી ટ્રીક

``પોર્ટ સ્કેનિંગ સુરક્ષા આંતરદૃષ્ટિ પ્રદાન કરે''

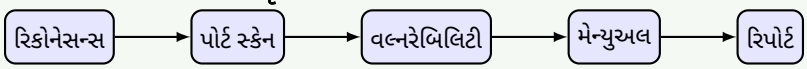
પ્રશ્ન 5(c OR) [7 ગુણ]

Describe the process of conducting a vulnerability assessment using Kali Linux tools.

જવાબ

વલ્નરેબિલિટી એસેસમેન્ટ પ્રક્રિયા:

આકૃતિ 24. Assessment Process



પગલું-દર-પગલું પ્રક્રિયા:

કોષ્ટક 27. Assessment Steps

પગલું	કાલી ટૂલ	હેતુ
રિકોનેસન્સ	Nmap	હોસ્ટ શોધ
પોર્ટ સ્કેનિંગ	Nmap	ખુલ્લા પોર્ટની ઓળખ
સેવા ગણતરી	Nmap	સેવા વર્ઝન ડિટેક્શન
વલ્નરેબિલિટી	OpenVAS	ઓટોમેટેડ ડિટેક્શન
વેબ પરીક્ષણ	Nikto	વેબ વલ્નરેબિલિટી

ટૂલ્સ:
- **Nmap**: નેટવર્ક સ્કેનિંગ
- **OpenVAS**: વલ્નરેબિલિટી સ્કેનિંગ
- **Metasploit**: એક્સપ્લોઇટેશન

મેમરી ટ્રીક

``વલ્નરેબિલિટી એસેસમેન્ટ એપ્લિકેશન સિક્યોરિટીને માન્ય કરે''