Cyber Security and Digital Forensics (4361601) - Summer 2025 Solution

Milav Dabgar

May 8, 2025

પ્રશ્ન 1(a) [3 ગુણ]

Public key અને Private Key cryptography વચ્ચેનો તફાવત આપો.

જવાબ

કોષ્ટક 1. Key Cryptography તફાવત

પાસાં	Private Key Cryptography	Public Key Cryptography
Key Management	એક જ key encryption/decryption માટે	અલગ keys encryption/decryption માટે
Key Distribution	સુરક્ષિત channel જરૂરી	સુરક્ષિત channel જરૂરી નથી
Speed	ઝડપી processing	Private key કરતાં ધીમી
Security Level	key ગુપ્ત રાખવાથી ઉચ્ચ	ગાણિતિક સુરક્ષા ઉચ્ચ
ઉદાહરણ	DES, AES	RSA, ECC

મેમરી ટ્રીક

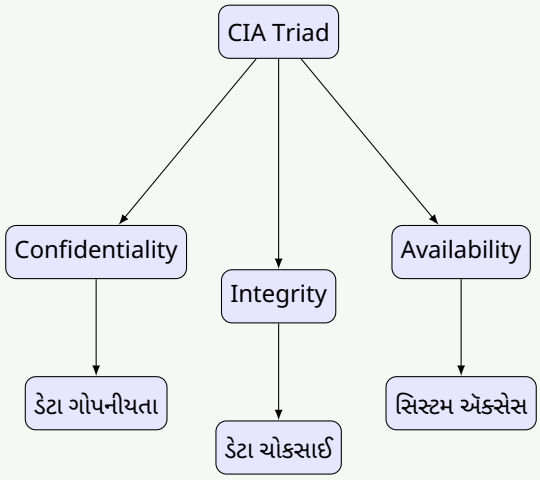
"Private Personal, Public Pair"

પ્રશ્ન 1(b) [4 ગુણ]

CIA Triad સમજાવો.

જવાબ

CIA Triad એ માહિતી સુરક્ષાનો પાયો છે જેમાં ત્રણ મુખ્ય સિદ્ધાંતો છે:



- **Confidentiality (ગોપનીયતા)**: ડેટા ફક્ત અધિકૃત વપરાશકર્તાઓ માટે ઉપલબ્ધ હોય
- **Integrity (અખંડિતતા)**: ડેટાની સચોટતા અને સંપૂર્ણતા જાળવે
- **Availability (ઉપલબ્ધતા)**: જરૂર પડે ત્યારે સિસ્ટમ્સ ઉપલબ્ધ હોય

મેમરી ટ્રીક

"Can I Access" (Confidentiality, Integrity, Availability)

પ્રશ્ન 1(c) [7 ગુણ]

Md5 અલ્ગોરિધમના પગલાં સમજાવો.

જવાબ

MD5 (Message Digest 5) એ 128-bit hash value બનાવતું cryptographic hash function છે.

કોષ્ટક 2. MD5 અલ્ગોરિધમ પગલાં

પગલું	પ્રક્રિયા	વર્ણન
1	**Padding**	message length $\equiv$ 448 (mod 512) બનાવવા bits ઉમેરવા
2	**Length Addition**	મૂળ message ની 64-bit length ઉમેરવી
3	**Initialize Buffers**	ચાર 32-bit buffers (A, B, C, D) સેટ કરવા
4	**Process Blocks**	512-bit blocks માં message process કરવો
5	**Round Functions**	16 operations ના 4 rounds લાગુ કરવા

```
# MD5 Processing Steps
def md5_process():
    # Step 1: Padding
    padded_message = original + padding_bits
    # Step 2: Process in 512-bit chunks
    for chunk in chunks:
        # Step 3: Apply round functions
        result = round_functions(chunk)
    return final_hash
```

- **Round 1**: F(X,Y,Z) = (X$\wedge$Y) $\vee$ ($\neg$X$\wedge$Z)
- **Round 2**: G(X,Y,Z) = (X$\wedge$Z) $\vee$ (Y$\wedge\neg$Z)
- **Round 3**: H(X,Y,Z) = X$\oplus$Y$\oplus$Z

- **Round 4**: I(X,Y,Z) = Y⊕(X∨¬Z)

મેમરી ટ્રીક

"My Data Needs Proper Processing"

OR

પ્રશ્ન 1(c) [7 ગુણ]

RSA ના શોધકોની યાદી બનાવો. RSA અલ્ગોરિધમના સ્ટેપ્સ લખો.

જવાબ

RSA શોધકો:
- **Ron Rivest** (MIT)
- **Adi Shamir** (MIT)
- **Leonard Adleman** (MIT)

કોષ્ટક 3. RSA અલ્ગોરિધમ પગલાં

પગલું	પ્રક્રિયા	સૂત્ર
1	**Primes પસંદ કરો**	p, q (મોટા primes) પસંદ કરો
2	**n ગણતરી**	$n = p \times q$
3	**$\phi(n)$ ગણતરી**	$\phi(n) = (p-1) \times (q-1)$
4	**e પસંદ કરો**	$\gcd(e, \phi(n)) = 1$
5	**d ગણતરી**	$d \times e \equiv 1 \pmod{\phi(n)}$
6	**Encryption**	$C = M^e \bmod n$
7	**Decryption**	$M = C^d \bmod n$

Key Pairs:
- **Public Key**: (n, e)
- **Private Key**: (n, d)

મેમરી ટ્રીક

"RSA: Rivest Shamir Adleman"

પ્રશ્ન 2(a) [3 ગુણ]

વ્યાખ્યા આપો: Firewall. Firewall ની મર્યાદાઓની યાદી બનાવો.

જવાબ

વ્યાખ્યા: Firewall એ network security device છે જે પૂર્વ-નિર્ધારિત સુરક્ષા નિયમોના આધારે આવતા/જતા network traffic ને monitor અને control કરે છે.

કોષ્ટક 4. Firewall મર્યાદાઓ

મર્યાદા	વર્ણન
આંતરિક ધમકીઓ	insider attacks થી સુરક્ષા આપી શકતી નથી
Application Layer	application-specific attacks સામે મર્યાદિત સુરક્ષા
Performance	network traffic ધીમી કરી શકે છે
Configuration	યોગ્ય setup અને maintenance જરૂરી
Encrypted Traffic	encrypted content ને અસરકારક રીતે inspect કરી શકતી નથી

મેમરી ટ્રીક

"Fire Walls Limit Internal Protection"

પ્રશ્ન 2(b) [4 ગુણ]

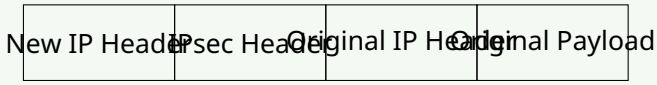
IPsec Tunnel Mode અને Transport mode નું સ્કેચ કરો.

જવાબ

IPsec Modes Comparison:

Transport Mode:

Tunnel Mode:



કોષ્ટક 5. મુખ્ય તફાવતો

પાસું	Transport Mode	Tunnel Mode
સુરક્ષા	ફક્ત Payload	સંપૂર્ણ packet
ઉપયોગ	End-to-end	Gateway-to-gateway
Overhead	ઓછું	વધારે
IP Header	મૂળ જાળવાયેલું	નવું header ઉમેર્યું

મેમરી ટ્રીક

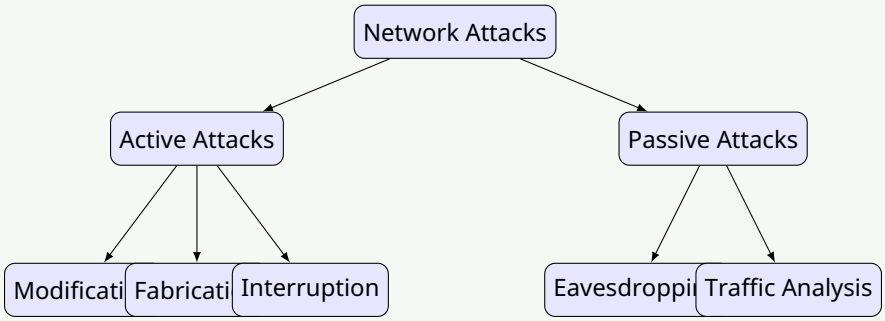
"Transport Travels, Tunnel Total"

પ્રશ્ન 2(c) [7 ગુણ]

વિવિધ પ્રકારના Active અને Passive attacks નું વિગતવાર વર્ણન કરો.

જવાબ

Attack વર્ગીકરણ:



કોષ્ટક 6. Active Attacks

પ્રકાર	વર્ણન	ઉદાહરણ
Masquerade	અન્ય entity નો નકલી અવતાર	Fake identity
Replay	captured data ને ફરીથી transmit કરવું	Session replay
Modification	message content ને બદલવું	Data tampering
DoS	service availability નો ઇનકાર	Server flooding

કોષ્ટક 7. Passive Attacks

પ્રકાર	વર્ણન	અસર
Eavesdropping	communications સાંભળવું	Data theft
Traffic Analysis	communication patterns નું analysis	Privacy breach
Monitoring	network activity નું observation	Information gathering

મેમરી ટ્રીક

"Active Acts, Passive Peeks"

OR

પ્રશ્ન 2(a) [3 ગુણ]

વ્યાખ્યા આપો: Digital Signature. Digital Signature ના વિવિધ એપ્લિકેશન ક્ષેત્રોની ચર્ચા કરો.

જવાબ

વ્યાખ્યા: Digital Signature એ cryptographic technique છે જે public key cryptography ના ઉપયોગથી digital messages અથવા documents ની authenticity અને integrity ને validate કરે છે.

કોષ્ટક 8. એપ્લિકેશન ક્ષેત્રો

ક્ષેત્ર	ઉપયોગ
E-commerce	Online transactions, contracts
Banking	Electronic fund transfers, cheques
Government	Digital certificates, સરકારી documents
Healthcare	Patient records, prescriptions
Legal	Electronic contracts, court documents

મેમરી ટ્રીક

"Digital Documents Demand Authentic Approval"

OR

પ્રશ્ન 2(b) [4 ગુણ]

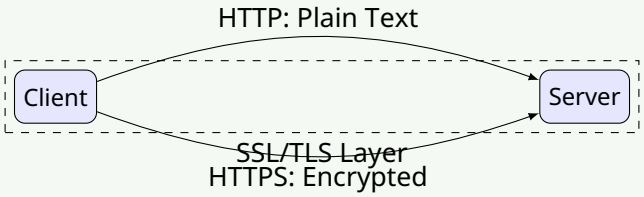
HTTP અને HTTPS વચ્ચેનો તફાવત આપો.

જવાબ

કોષ્ટક 9. HTTP vs HTTPS

પેરામીટર	HTTP	HTTPS
સુરક્ષા	કોઈ encryption નથી	SSL/TLS encryption
Port	80	443
Protocol	Hypertext Transfer Protocol	HTTP + SSL/TLS
ડેટા સુરક્ષા	Plain text	Encrypted
Authentication	Server verification નથી	Server certificate validation
Speed	વધારે ઝડપી	થોડી ધીમી
URL Prefix	http://	https://

આકૃતિ:



મેમરી ટ્રીક

"HTTPS Has Security"

OR

પ્રશ્ન 2(c) [7 ગુણ]

વ્યાખ્યા આપો: Malicious software. Virus, Worm, Keylogger, Trojans ને વિગતવાર સમજાવો.

જવાબ

વ્યાખ્યા: Malicious software (Malware) એ એવા software છે જે computer systems ને નુકસાન પહોંચાડવા, exploit કરવા અથવા unauthorized access મેળવવા માટે design કરવામાં આવે છે.

કોષ્ટક 10. Malware ના પ્રકારો

પ્રકાર	લક્ષણો	વર્તન
Virus	Host file જરૂરી	Programs સાથે attach થાય, execute થતાં spread થાય
Worm	Self-replicating	Networks દ્વારા સ્વતંત્ર રીતે spread થાય
Keylogger	Keystrokes record કરે	Passwords અને sensitive data steal કરે
Trojan	Legitimate તરીકે disguise	Attackers ને backdoor access આપે

વિગતવાર સમજૂતી:
Virus:
- Execute થવા માટે host program જરૂરી
- Infected files દ્વારા spread થાય
- Data corrupt અથવા delete કરી શકે

Worm:
- Self-propagating malware
- Network vulnerabilities exploit કરે
- Network bandwidth consume કરે

Keylogger:
- User keystrokes record કરે
- Login credentials capture કરે
- Hardware અથવા software-based હોઈ શકે

Trojan:
- Legitimate software તરીકે દેખાય
- Remote access માટે backdoor બનાવે
- Self-replicate થતું નથી

મેમરી ટ્રીક

"Viruses Visit, Worms Wander, Keys Captured, Trojans Trick"

પ્રશ્ન 3(a) [3 ગુણ]

વ્યાખ્યા આપો: Cybercrime. Cyber Law ની જરૂરિયાતો પણ ચર્ચા કરો.

જવાબ

વ્યાખ્યા: Cybercrime એટલે computers, networks અથવા digital devices નો સાધન અથવા લક્ષ્ય તરીકે ઉપયોગ કરીને કરવામાં આવતી ગુનાહિત પ્રવૃત્તિઓ.

કોષ્ટક 11. Cyber Law ની જરૂરિયાતો

જરૂરિયાત	સમર્થન
કાયદાકીય માળખું	Cyber અપરાધોની સ્પષ્ટ વ્યાખ્યાઓ સ્થાપિત કરવી
અધિકારક્ષેત્ર	ભૌગોલિક સીમાઓ પાર સત્તા નક્કી કરવી
પુરાવા	Digital evidence collection માટે માર્ગદર્શિકા
સજા	Cybercriminals માટે deterrent પગલાં
સુરક્ષા	વ્યક્તિગત અને સંસ્થાકીય અધિકારોનું રક્ષણ

મેમરી ટ્રીક

"Cyber Laws Create Legal Protection"

પ્રશ્ન 3(b) [4 ગુણ]

Cyber spying અને Cyber theft સમજાવો.

જવાબ

Cyber Spying:
- **વ્યાખ્યા**: Digital communications અને activities ની અનધિકૃત દેખરેખ
- **પદ્ધતિઓ**: Malware, phishing, social engineering
- **લક્ષ્યો**: સરકારી, corporate secrets, વ્યક્તિગત ડેટા
- **અસર**: રાષ્ટ્રીય સુરક્ષા જોખમો, સ્પર્ધાત્મક ગેરલાભ

Cyber Theft:
- **વ્યાખ્યા**: Digital assets અથવા માહિતીની અનધિકૃત ચોરી
- **પ્રકારો**: Identity theft, financial fraud, intellectual property theft
- **પદ્ધતિઓ**: Hacking, social engineering, insider threats
- **પરિણામો**: આર્થિક નુકસાન, પ્રતિષ્ઠા નુકસાન

કોષ્ટક 12. સરખામણી કોષ્ટક

પાસું	Cyber Spying	Cyber Theft
હેતુ	માહિતી એકત્રિકરણ	સંપત્તિ પ્રાપ્તિ
Detection	ઘણીવાર undetected	ધ્યાનમાં આવી શકે
સમયગાળો	લાંબા ગાળાની monitoring	એક વખત કે સમયાંતરે
પ્રેરણા	Intelligence/espionage	આર્થિક લાભ

મેમરી ટ્રીક

"Spies Spy, Thieves Take"

પ્રશ્ન 3(c) [7 ગુણ]

Cyber law ની કલમ 66 સમજાવો.

જવાબ

Section 66 - Computer Related Offences (IT Act 2008):

કોષ્ટક 13. મુખ્ય જોગવાઈઓ

પેટા-કલમ	ગુનો	સજા
66(1)	કમ્પ્યુટર સંસાધન નુકસાન (Dishonestly/fraudulently)	3 વર્ષ સુધી કેદ + ₹5 લાખ સુધી દંડ
66A	અપમાનજનક સંદેશા મોકલવા	3 વર્ષ સુધી + દંડ
66B	ચોરી કરેલ કમ્પ્યુટર સંસાધન મેળવવું	3 વર્ષ સુધી + ₹1 લાખ સુધી દંડ
66C	Identity theft	3 વર્ષ સુધી + ₹1 લાખ સુધી દંડ
66D	Computer દ્વારા personation થી છેતરપિંડી	3 વર્ષ સુધી + ₹1 લાખ સુધી દંડ
66E	ગોપનીયતા ભંગ	3 વર્ષ સુધી + ₹2 લાખ સુધી દંડ
66F	Cyber terrorism	આજીવન કેદ

વિગતવાર કવરેજ:
કલમ 66 મુખ્ય ગુનાઓ:
- **Hacking**: Computer systems માં અનધિકૃત પ્રવેશ
- **Data Theft**: પરવાનગી વિના ડેટા ચોરી અથવા નકલ
- **System Damage**: Computer ડેટા નાશ અથવા ફેરફાર

- **Virus Introduction**: Malicious code દાખલ કરવો

જરૂરી તત્વો:
- **ઈરાદો**: અપ્રમાણિક અથવા છેતરપિંડીનો ઈરાદો
- **પ્રવેશ**: માલિકની પરવાનગી વિના
- **નુકસાન**: સિસ્ટમ અથવા ડેટાને નુકસાન પહોંચાડવું
- **જ્ઞાન**: અનધિકૃત પ્રવેશની જાણકારી

કાનૂની માળખું:
- **Cognizable**: પોલીસ વોરંટ વિના ધરપકડ કરી શકે
- **Non-bailable**: જામીન કોર્ટની મુનસફી પર
- **Evidence**: Digital evidence કોર્ટમાં માન્ય

મેમરી ટ્રીક

"Section 66 Stops Cyber Sins"

OR

પ્રશ્ન 3(a) [3 ગુણ]

Cyber terrorism સમજાવો.

જવાબ

વ્યાખ્યા: Cyber terrorism એટલે રાજકીય, ધાર્મિક અથવા વૈચારિક હેતુઓ માટે ડર, વિક્ષેપ અથવા નુકસાન પહોંચાડવા digital technologies નો ઉપયોગ કરવો.

કોષ્ટક 14. લાક્ષણિકતાઓ

પાસું	વર્ણન
લક્ષ્ય	Critical infrastructure, સરકારી systems
પદ્ધતિ	DDoS attacks, system infiltration, data destruction
પ્રેરણા	રાજકીય, ધાર્મિક, વૈચારિક ધ્યેયો
અસર	જાહેર ભય, આર્થિક વિક્ષેપ, રાષ્ટ્રીય સુરક્ષા

ઉદાહરણો:
- Power grid attacks
- Transportation system disruption
- Financial system targeting

મેમરી ટ્રીક

"Terror Through Technology"

OR

પ્રશ્ન 3(b) [4 ગુણ]

Cyber bullying અને Cyber stalking સમજાવો.

જવાબ

Cyber Bullying:
- **વ્યાખ્યા**: અન્યોને હેરાન કરવા, ડરાવવા અથવા નુકસાન પહોંચાડવા digital platforms નો ઉપયોગ
- **Platforms**: Social media, messaging apps, online forums
- **લાક્ષણિકતાઓ**: પુનરાવર્તિત, ઈરાદાપૂર્વક નુકસાન, power imbalance
- **અસર**: માનસિક આઘાત, ડિપ્રેશન, સામાજિક એકલતા

Cyber Stalking:
- **વ્યાખ્યા**: સતત online પજવણી જેનાથી ડર અથવા ભાવનાત્મક તકલીફ થાય
- **પદ્ધતિઓ**: અનિચ્છનીય સંદેશા, tracking, identity theft
- **સમયગાળો**: લાંબા ગાળાનું, સતત વર્તન
- **કાનૂની**: ઘણા અધિકારક્ષેત્રોમાં ફોજદારી ગુનો

કોષ્ટક 15. સરખામણી

પાસું	Cyber Bullying	Cyber Stalking
સમયગાળો	Episodes	સતત
વય જૂથ	મુખ્યત્વે સગીરો	તમામ ઉંમરના
પ્રેરણા	સામાજિક વર્ચસ્વ	Obsession/control
Platform	Public/semi-public	Private/public

મેમરી ટ્રીક

"Bullies Bother, Stalkers Stalk"

OR

પ્રશ્ન 3(c) [7 ગુણ]

Cyber law ની કલમ 67 સમજાવો.

જવાબ

Section 67 - Publishing Obscene Information (IT Act 2008):

કોષ્ટક 16. મુખ્ય જોગવાઈઓ

કલમ	સામગ્રી	સજા
67	અશ્લીલ સામગ્રી પ્રકાશિત કરવી	પ્રથમ ગુનો: 3 વર્ષ + ₹5 લાખ દંડ
67A	જાતીય સ્પષ્ટ સામગ્રી	5 વર્ષ સુધી + ₹10 લાખ દંડ
67B	બાળ અશ્લીલતા (Child pornography)	પ્રથમ: 5 વર્ષ + ₹10 લાખ, પછી: 7 વર્ષ + ₹10 લાખ
67C	મધ્યસ્થી જવાબદારી	ગેરકાયદેસર સામગ્રી દૂર કરવામાં નિષ્ફળતા

મુખ્ય તત્વો:
કલમ 67 - અશ્લીલતા:
- **પ્રકાશન**: Electronic સ્વરૂપમાં ઉપલબ્ધ કરાવવું
- **સામગ્રી**: કામુક, જાતીય સ્પષ્ટ સામગ્રી
- **માધ્યમ**: Website, email, social media
- **ઈરાદો**: દર્શકોને ભ્રષ્ટ કરવાનો

કલમ 67A - જાતીય સ્પષ્ટ:
- સ્પષ્ટ જાતીય સામગ્રી માટે **વધારે સજા**
- સામાન્ય અશ્લીલતા કરતાં **વ્યાપક વ્યાપ**
- **વ્યાપારી હેતુ** ગંભીર પરિબળ ગણાય

કલમ 67B - બાળ સુરક્ષા:
- બાળ શોષણ માટે **Zero tolerance**

- કબજા અને વિતરણ માટે **સખત જવાબદારી**
- ગંભીરતા દર્શાવતી **ઉચ્ચ દંડ**
- Platforms માટે **વય ચકાસણી** આવશ્યકતાઓ

ઉપલબ્ધ બચાવ:
- **વૈજ્ઞાનિક/શૈક્ષણિક** હેતુ
- **કલાત્મક યોગ્યતા** વિચારણા
- કેટલાક કિસ્સાઓમાં **ખાનગી જોવા**
- સામગ્રીના પ્રકાર વિશે **જ્ઞાનનો અભાવ**

Digital Evidence Requirements:
- **Chain of custody** જાળવણી
- **તકનીકી અધિકૃતતા** સાબિતી
- **સ્રોત ઓળખ** પદ્ધતિઓ
- Electronic evidence નું **સંરક્ષણ**

મેમરી ટ્રીક

"Section 67 Stops Shameful Sharing"

પ્રશ્ન 4(a) [3 ગુણ]

Hackers ના પ્રકારોની ચર્ચા કરો.

જવાબ

Hacker વર્ગીકરણ:

કોષ્ટક 17. Hacker પ્રકારો

પ્રકાર	પ્રેરણા	પ્રવૃત્તિઓ
White Hat	Ethical security testing	અધિકૃત penetration testing
Black Hat	દૂષિત ઈરાદો	ગેરકાયદેસર system breaking
Gray Hat	મિશ્ર પ્રેરણા	અનધિકૃત પરંતુ non-malicious
Script Kiddie	ઓળખ/મજા	અસ્તિત્વમાંના tools નો ઉપયોગ
Hacktivist	રાજકીય/સામાજિક કારણો	Hacking દ્વારા વિરોધ

વિગતવાર પ્રકારો:
- **White Hat**: Ethical hackers, સુરક્ષા વ્યવસાયિકો
- **Black Hat**: Cybercriminals જે નફો અથવા નુકસાન ઈચ્છે છે
- **Gray Hat**: Ethical અને malicious ની વચ્ચે

મેમરી ટ્રીક

"Hats Have Hacker Hierarchy"

પ્રશ્ન 4(b) [4 ગુણ]

RAT સમજાવો.

જવાબ

RAT (Remote Administration Tool):
વ્યાખ્યા: Software જે computer system નું remote control પરવાનગી આપે છે, ઘણીવાર અનધિકૃત પ્રવેશ માટે દૂષિત રીતે ઉપયોગમાં લેવાય છે.

કોષ્ટક 18. લાક્ષણિકતાઓ

લક્ષણ	વર્ણન
Remote Control	દૂરથી સંપૂર્ણ system access
Stealth Mode	User detection થી છુપાયેલું
Data Theft	File access અને transfer ક્ષમતાઓ
Keylogging	Keystroke recording
Screen Capture	Desktop monitoring

સામાન્ય RATs:
- **BackOrifice**
- **NetBus**
- **DarkComet**
- **Poison Ivy**

શોધ પદ્ધતિઓ:
- Antivirus software
- Network monitoring
- Process analysis
- Behavioral detection

મેમરી ટ્રીક

"RATs Run Remote Access Tactics"

પ્રશ્ન 4(c) [7 ગુણ]

Hacking ના પાંચ પગલાં સમજાવો.

જવાબ

પાંચ-તબક્કાની Hacking Methodology:

કોષ્ટક 19. વિગતવાર પગલાં

તબક્કો	હેતુ	તકનીકો	સાધનો
1. Reconnaissance	માહિતી એકત્રિકરણ	OSINT, Social Engineering	Google, Shodan, WHOIS
2. Scanning	Vulnerabilities ઓળખવા	Port scanning, Network mapping	Nmap, Nessus
3. Gaining Access	Vulnerabilities exploit કરવા	Password attacks, Code injection	Metasploit, Hydra
4. Maintaining Access	કાયમી નિયંત્રણ	Backdoors, Rootkits	RATs, Trojans
5. Covering Tracks	પુરાવા છુપાવવા	Log deletion, Steganography	CCleaner, File wipers

તબક્કો 1 - Reconnaissance:

- **Passive**: જાહેર માહિતી એકત્રિકરણ
- **Active**: સીધો target interaction
- **Goal**: Target infrastructure નો નકશો બનાવવો

તબક્કો 2 - Scanning:
- **Network scanning**: જીવંત system ઓળખ
- **Port scanning**: Service discovery
- **Vulnerability scanning**: નબળાઈ ઓળખ

તબક્કો 3 - Gaining Access:
- **Exploitation**: Vulnerability ઉપયોગ
- **Authentication attacks**: Password cracking
- **Privilege escalation**: ઉચ્ચ access levels

તબક્કો 4 - Maintaining Access:
- **Backdoor installation**: ભવિષ્ય પ્રવેશ
- **System modification**: Persistence mechanisms
- **Data collection**: માહિતી એકત્રિકરણ

તબક્કો 5 - Covering Tracks:
- **Log manipulation**: પુરાવા દૂર કરવા
- **File deletion**: નિશાન નાબૂદી
- **Timeline modification**: પ્રવૃત્તિ છુપાવવી

મેમરી ટ્રીક

"Real Smart Guys Make Choices"

OR

પ્રશ્ન 4(a) [3 ગુણ]

Brute force attack સમજાવો.

જવાબ

વ્યાખ્યા: Brute force attack એ trial-and-error પદ્ધતિ છે જે તમામ શક્ય સંયોજનો (combinations) અજમાવીને encrypted data ને decode કરવા માટે વપરાય છે.

કોષ્ટક 20. લાક્ષણિકતાઓ

પાસું	વર્ણન
પદ્ધતિ	સંપૂર્ણ key search
સમય	ગણતરીની દ્રષ્ટિએ સઘન (Computationally intensive)
સફળતા	બાંયધરીકૃત પરંતુ સમય લેતું
લક્ષ્ય	Passwords, encryption keys
સાધનો	Automated software

પ્રકારો:
- **Simple Brute Force**: તમામ શક્ય સંયોજનો
- **Dictionary Attack**: સામાન્ય passwords
- **Hybrid Attack**: Dictionary + વિવિધતાઓ

મેમરી ટ્રીક

"Brute Force Breaks By Trying"

OR

પ્રશ્ન 4(b) [4 ગુણ]

વ્યાખ્યા આપો: Vulnerability, Threat, Exploit

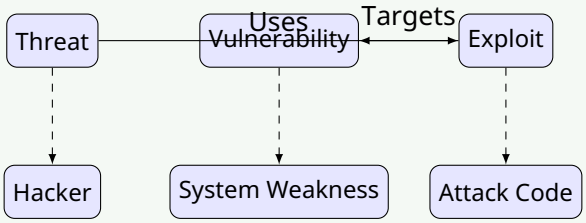
જવાબ

Security પરિભાષા:

કોષ્ટક 21. શબ્દ વ્યાખ્યાઓ

શબ્દ	વ્યાખ્યા	ઉદાહરણ
Vulnerability	System/software માં નબળાઈ	Unpatched software bug
Threat	Asset માટે સંભવિત ખતરો	Malicious hacker
Exploit	Code જે vulnerability નો લાભ લે છે	Buffer overflow attack

સંબંધ:



ઉદાહરણો:
- **Vulnerability**: SQL injection flaw
- **Threat**: Cybercriminal
- **Exploit**: SQL injection payload

Risk સૂત્ર: Risk = Threat × Vulnerability × Asset Value

મેમરી ટ્રીક

"Threats Target Vulnerable Exploits"

OR

પ્રશ્ન 4(c) [7 ગુણ]

Kali Linux ના કોઈપણ ત્રણ મૂળભૂત commands યોગ્ય ઉદાહરણ સાથે સમજાવો.

જવાબ

આવશ્યક Kali Linux Commands:
1. NMAP (Network Mapper):

```
# Port scanning
nmap -sS target_ip
nmap -A -T4 192.168.1.1
```

કોષ્ટક 22. Nmap વિકલ્પો

વિકલ્પ	હેતુ	ઉદાહરણ
-sS	SYN scan	nmap -sS 192.168.1.1
-A	Aggressive scan	nmap -A target.com
-p	Specific ports	nmap -p 80,443 target.com

2. Metasploit:

```
# Start Metasploit
msfconsole
# Search exploits
search apache
# Use exploit
use exploit/windows/smb/ms17_010_eternalblue
```

Commands:
- **search**: Exploits/payloads શોધવા
- **use**: Module પસંદ કરવા
- **set**: Options configure કરવા
- **exploit**: Attack launch કરવા

3. Wireshark:

```
# Command line version
tshark -i eth0
# Filter traffic
tshark -i eth0 -f "port 80"
```

સુવિધાઓ:
- **Packet capture**: Real-time network monitoring
- **Protocol analysis**: Deep packet inspection
- **Filter options**: Targeted traffic analysis
- **GUI interface**: વપરાશકર્તા મૈત્રીપૂર્ણ વિશ્લેષણ

વધારાના Commands:

4. Hydra (Password Cracking):

```
hydra -l admin -P passwords.txt ssh://192.168.1.1
```

5. John the Ripper:

```
john --wordlist=rockyou.txt hashes.txt
```

6. Aircrack-ng (WiFi Security):

```
airmon-ng start wlan0
airodump-ng wlan0mon
```

કોષ્ટક 23. Command Categories

Category	Tools	Purpose
Network Scanning	nmap, masscan	Host/port discovery
Vulnerability Assessment	OpenVAS, Nessus	Security scanning
Exploitation	Metasploit, SQLmap	Vulnerability exploitation
Password Attacks	Hydra, John	Credential cracking
Wireless Security	Aircrack-ng	WiFi penetration testing

મેમરી ટ્રીક

"Network Maps Make Security"

પ્રશ્ન 5(a) [3 ગુણ]

Digital Forensics ની શાખાઓની સૂચિ બનાવો.

જવાબ

Digital Forensics શાખાઓ:

કોષ્ટક 24. શાખાઓ

શાખા	ફોકસ વિસ્તાર	એપ્લિકેશન્સ
Computer Forensics	Desktop/laptop systems	Hard drive analysis
Network Forensics	Network traffic analysis	Intrusion investigation
Mobile Forensics	Smartphones/tablets	Call logs, messages
Database Forensics	Database systems	Data integrity verification
Malware Forensics	Malicious software	Malware analysis
Email Forensics	Email communications	Email header analysis
Memory Forensics	RAM analysis	Live system investigation

વિશેષિત વિસ્તારો:
- **Cloud Forensics**
- **IoT Forensics**
- **Blockchain Forensics**

મેમરી ટ્રીક

"Digital Detectives Discover Many Clues"

પ્રશ્ન 5(b) [4 ગુણ]

Digital Forensics માં લોકાર્ડના વિનિમયના સિદ્ધાંતની ચર્ચા કરો.

જવાબ

લોકાર્ડનો વિનિમય સિદ્ધાંત (Locard's Exchange Principle):
મૂળ સિદ્ધાંત: "દરેક સંપર્ક નિશાન છોડે છે" ("Every contact leaves a trace")
ડિજિટલ એપ્લિકેશન:

કોષ્ટક 25. ડિજિટલ નિશાનો

ડિજિટલ પ્રવૃત્તિ	છોડવામાં આવેલ નિશાન	સ્થાન
File Access	Access timestamps	File metadata
Web Browsing	Browser history, cookies	Browser cache
Email Communication	Headers, logs	Mail servers
Network Activity	Connection logs	Network devices
USB Usage	Device artifacts	Registry/logs

ડિજિટલ પુરાવાના નિશાનો:
સિસ્ટમ સ્તર:
- **Registry entries**: સિસ્ટમ ફેરફારો
- **Log files**: પ્રવૃત્તિ રેકોર્ડ્સ
- **Temporary files**: Process artifacts
- **Metadata**: ફાઈલ માહિતી

નેટવર્ક સ્તર:
- **Router logs**: Traffic records
- **Firewall logs**: Connection attempts
- **DNS queries**: Website visits
- **Packet captures**: Communication content

એપ્લિકેશન સ્તર:
- **Browser artifacts**: Web activity
- **Application logs**: Software usage
- **Database changes**: Data modifications
- **Cache files**: Temporary storage

ફોરેન્સિક અસરો:
- **સંપૂર્ણ ગુનો નથી**: ડિજિટલ નિશાનો હંમેશા અસ્તિત્વમાં છે
- **પુરાવાનું સ્થાન**: અનેક સ્રોતો ઉપલબ્ધ
- **સમર્થન**: અનેક નિશાન validation
- **Timeline પુનર્નિર્માણ**: પ્રવૃત્તિ ક્રમ

મેમરી ટ્રીક

"Every Exchange Exists Electronically"

પ્રશ્ન 5(c) [7 ગુણ]

Digital Evidence સાચવવા માટેના મહત્વના પગલાઓની યાદી બનાવો.

જવાબ

ડિજિટલ પુરાવા સંરક્ષણ પ્રક્રિયા:

કોષ્ટક 26. મહત્વપૂર્ણ સંરક્ષણ પગલાં

પગલું	પ્રક્રિયા	હેતુ	સાધનો
1. ઓળખ	સંભવિત પુરાવા શોધવા	અવકાશ નક્કી કરવો	દ્રશ્ય નિરીક્ષણ
2. દસ્તાવેજીકરણ	દ્રશ્ય વિગતો record કરવી	Chain of custody જાળવવું	ફોટોગ્રાફી, નોંધો
3. અલગીકરણ	દૂષણ અટકાવવું	અખંડિતતા જાળવવી	Network disconnection
4. Imaging	Bit-by-bit copy બનાવવી	મૂળ સાચવવું	dd, FTK Imager
5. Hashing	Integrity checks બનાવવા	અધિકૃતતા ચકાસવી	MD5, SHA-256
6. સંગ્રહ	સુરક્ષિત પુરાવા સંગ્રહ	છેડછાડ અટકાવવી	Write-protected media
7. Chain of Custody	Handling દસ્તાવેજીકરણ	કાનૂની સ્વીકાર્યતા	Forensic forms

વિગતવાર સંરક્ષણ પદ્ધતિઓ:
ભૌતિક સંરક્ષણ:
- **Power management**: યોગ્ય shutdown procedures
- **Hardware protection**: Anti-static પગલાં
- **પર્યાવરણીય નિયંત્રણ**: તાપમાન/ભેજ
- **પ્રવેશ પ્રતિબંધ**: અધિકૃત કર્મચારીઓ માત્ર

તર્કસંગત સંરક્ષણ (Logical):
- **Bit-stream imaging**: હૂબહૂ disk copies
- **Hash verification**: અખંડિતતા પુષ્ટિ
- **Write blocking**: ફેરફારો અટકાવવા
- **Metadata preservation**: Timestamp સુરક્ષા

કાનૂની સંરક્ષણ:

- **દસ્તાવેજીકરણ ધોરણો**: વિગતવાર રેકોર્ડ્સ
- **Chain of custody**: Handling log
- **પ્રામાણિકતા**: પુરાવા ચકાસણી
- **સ્વીકાર્યતા**: કોર્ટ જરૂરિયાતો

શ્રેષ્ઠ પ્રથાઓ:

કરવા જેવું (Do's):

- પુરાવાની **અનેક નકલો બનાવવી**
- **Forensically sound સાધનો** ઉપયોગ કરવા
- **દરેક ક્રિયા નોંધવી**
- **Chain of custody જાળવવું**
- Hash સાથે **અખંડિતતા ચકાસવી**

ન કરવા જેવું (Don'ts):

- **કદી મૂળ પુરાવા પર કામ ન કરવું**
- દ્રશ્યનું **દૂષણ ટાળવું**
- Suspect systems ને **power on ન કરવા**
- પુરાવાને **modify ન કરવા**
- **Chain of custody તોડવું નહીં**

ગુણવત્તા ખાતરી:

કોષ્ટક 27. ચેક્સ

ચેક	ચકાસણી પદ્ધતિ	આવર્તન
Hash Validation	Original vs copy સરખામણી	પહેલાં/પછી operations
Tool Calibration	Tool accuracy ચકાસવી	Regular intervals
Process Review	Procedures audit કરવી	Case completion
Documentation Check	સંપૂર્ણતા ચકાસવી	દરેક પગલે

કાનૂની વિચારણાઓ:

- **સ્વીકાર્યતા જરૂરિયાતો**: કોર્ટ ધોરણો
- **નિષ્ણાત સાક્ષી**: તકનીકી સમજૂતી
- **ઉલટ-સવાલ**: પ્રક્રિયા validation
- **ધોરણ અનુપાલન**: ઉદ્યોગ શ્રેષ્ઠ પ્રથાઓ

મેમરી ટ્રીક

"Proper Preservation Prevents Problems"

OR

પ્રશ્ન 5(a) [3 ગુણ]

Malware forensics સમજાવો.

જવાબ

વ્યાખ્યા: Malware forensics માં infected systems પર તેના વર્તન, મૂળ અને અસરને સમજવા માટે malicious software નું analysis કરવામાં આવે છે.

કોષ્ટક 28. મુખ્ય ઘટકો

ઘટક	વર્ણન
Static Analysis	Execution વિના malware ની તપાસ
Dynamic Analysis	Controlled environment માં malware ચલાવવું
Code Analysis	Malware code નું reverse engineering
Behavioral Analysis	Malware actions નો અભ્યાસ

પ્રક્રિયા:
- **Sample collection**: Malware acquisition
- **Isolation**: Sandbox environment
- **Analysis**: Behavior observation
- **Reporting**: Findings documentation

મેમરી ટ્રીક

"Malware Makes Mysteries"

OR

પ્રશ્ન 5(b) [4 ગુણ]

Digital Forensics તપાસમાં પુરાવા તરીકે CCTV શા માટે મહત્વની ભૂમિકા ભજવે છે તે સમજાવો.

જવાબ

Digital Forensics માં CCTV:

કોષ્ટક 29. CCTV પુરાવાનું મહત્વ

ભૂમિકા	વર્ણન	ફાયદો
દ્રશ્ય દસ્તાવેજીકરણ	વાસ્તવિક ઘટનાઓ record કરે	Objective પુરાવા
Timeline સ્થાપના	પ્રવૃત્તિઓ timestamps કરે	કાલક્રમિક ક્રમ
ઓળખ ચકાસણી	Suspect images capture કરે	વ્યક્તિ ઓળખ
સમર્થન	અન્ય પુરાવાઓને support કરે	કેસ મજબૂત બનાવે

ડિજિટલ પુરાવા ગુણધર્મો:
તકનીકી પાસાઓ:
- **Metadata preservation**: Timestamp, camera ID, settings
- **Chain of custody**: સુરક્ષિત handling procedures
- **Format integrity**: મૂળ file structure maintenance
- **Authentication**: Digital signatures, hash values

ફોરેન્સિક મૂલ્ય:
- **Real-time documentation**: Live incident recording
- **Unbiased testimony**: યાંત્રિક સાક્ષી
- **High resolution**: સ્પષ્ટ image quality
- **Audio capture**: વધારાના sensory પુરાવા

Analysis પદ્ધતિઓ:
- **Frame-by-frame examination**: વિગતવાર scrutiny
- **Enhancement techniques**: Image improvement
- **Comparison analysis**: Multiple angle correlation
- **Motion tracking**: Subject movement patterns

કાનૂની સ્વીકાર્યતા:
- **Authenticity verification**: Chain of custody
- **Technical validation**: Equipment calibration

- **Expert testimony**: Forensic analysis explanation
- **Standard compliance**: Industry best practices

મેમરી ટ્રીક

"CCTV Captures Criminal Conduct Clearly"

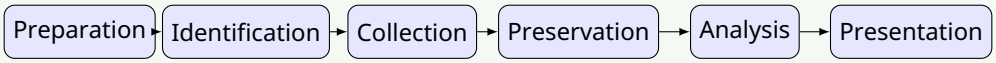
OR

પ્રશ્ન 5(c) [7 ગુણ]

Digital forensic તપાસના તબક્કાઓ સમજાવો.

જવાબ

Digital Forensic તપાસ પ્રક્રિયા:



કોષ્ટક 30. તબક્કાવાર વિભાજન

તબક્કો	હેતુ	પ્રવૃત્તિઓ	આઉટપુટ
1. તૈયારી	તત્પરતા સ્થાપના	Tool setup, training	Forensic kit
2. ઓળખ	પુરાવાનું સ્થાન	Survey, documentation	Evidence list
3. સંગ્રહ	પુરાવા પ્રાપ્તિ	Imaging, copying	Digital copies
4. સંરક્ષણ	અખંડિતતા જાળવણી	Hashing, storage	Verified evidence
5. વિશ્લેષણ	ડેટા તપાસ	Investigation, correlation	Findings
6. પ્રસ્તુતિ	પરિણામો સંપ્રેષણ	Reporting, testimony	Final report

વિગતવાર તબક્કો વિશ્લેષણ:
તબક્કો 1 - તૈયારી:
- **Tool readiness**: Forensic software installation
- **Hardware setup**: Write blockers, imaging devices
- **Documentation templates**: Chain of custody forms
- **Team preparation**: Role assignments, training
- **Legal preparation**: Warrant requirements, permissions

તબક્કો 2 - ઓળખ:
- **Scene survey**: Evidence location mapping
- **Device inventory**: System identification
- **Volatile evidence**: Memory, network connections
- **Priority assessment**: Critical evidence first
- **Photography**: Scene documentation

તબક્કો 3 - સંગ્રહ:
- **Live system analysis**: Memory acquisition
- **Disk imaging**: Bit-for-bit copies
- **Network evidence**: Log files, packet captures
- **Mobile devices**: Physical/logical extraction
- **Cloud evidence**: Remote data acquisition

તબક્કો 4 - સંરક્ષણ:
- **Hash generation**: MD5, SHA-256 checksums
- **Write protection**: Hardware/software blocking
- **Storage security**: Tamper-evident containers
- **Chain of custody**: Handling documentation
- **Backup creation**: Multiple evidence copies

તબક્કો 5 - વિશ્લેષણ:
- **File system examination**: Directory structure analysis
- **Deleted data recovery**: Unallocated space searching
- **Timeline creation**: Event chronology
- **Keyword searching**: Relevant content identification
- **Pattern recognition**: Behavioral analysis

તબક્કો 6 - પ્રસ્તુતિ:
- **Report writing**: Findings documentation
- **Visual aids**: Charts, diagrams, screenshots
- **Expert testimony**: Court presentation
- **Peer review**: Quality assurance
- **Archive maintenance**: Case file storage

શ્રેષ્ઠ પ્રથાઓ:

તકનીકી ધોરણો:
- **Tool validation**: Regular calibration
- **Methodology consistency**: Standard procedures
- **Quality control**: Verification checks
- **Documentation completeness**: Detailed records

કાનૂની જરૂરિયાતો:
- **Admissibility standards**: Court requirements
- **Chain of custody**: Unbroken documentation
- **Expert qualifications**: Professional certification
- **Cross-examination preparation**: Defense against challenges

ગુણવત્તા ખાતરી:

કોષ્ટક 31. ચેક પોઈન્ટસ

ચેક પોઈન્ટ	ચકાસણી	દસ્તાવેજીકરણ
Evidence integrity	Hash comparison	Verification logs
Tool reliability	Calibration tests	Certification records
Process compliance	Standard adherence	Procedure checklists
Report accuracy	Peer review	Review signatures

સામાન્ય પડકારો:
- **Encryption**: Data protection barriers
- **Anti-forensics**: Evidence hiding techniques
- **Volume**: Large data sets
- **Volatility**: Temporary evidence
- **Legal complexity**: Jurisdiction issues

સફળતાના પરિબળો:
- **Systematic approach**: Methodical investigation
- **Technical expertise**: Skilled personnel
- **Proper tools**: Adequate resources
- **Legal knowledge**: Compliance understanding
- **Documentation discipline**: Thorough records

મેમરી ટ્રીક

"Proper Planning Prevents Poor Performance"