

## પ્રશ્ન 1(અ) [3 ગુણા]

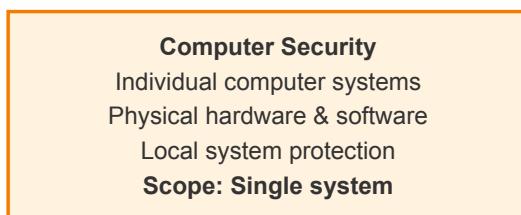
સાયબર સુરક્ષા અને કમ્પ્યુટર સુરક્ષા વ્યાખ્યાયિત કરો.

જવાબ:

- સાયબર સુરક્ષા:** ઇન્ટરનેટ-કનેક્ટેડ સિસ્ટમ્સની હાર્ડવેર, સોફ્ટવેર અને ડેટાની સાયબર ખતરાઓથી સુરક્ષા. તે નેટવર્કસ, ડિવાઇસ્સ્સ અને પ્રોગ્રામ્સને અનધિકૃત ડિજિટલ ભૂમલાઓથી બચાવવા પર ધ્યાન કેન્દ્રિત કરે છે.
- કમ્પ્યુટર સુરક્ષા:** વ્યક્તિગત કમ્પ્યુટર સિસ્ટમ્સ અને ડેટાને થોરી, નુકસાન, અથવા અનધિકૃત એક્સોસથી સુરક્ષા. તે ભૌતિક કમ્પ્યુટર હાર્ડવેર અને તેમાં ઇન્સ્ટોલ કરેલ સોફ્ટવેરની સુરક્ષા પર ધ્યાન કેન્દ્રિત કરે છે.

ડાયાગ્રામ:

### Cyber Security vs Computer Security



### Key Differences

#### Cyber Security Features:

- Network firewalls
- Cloud security
- Internet threat protection

#### Computer Security Features:

- Antivirus software
- Physical access control
- Local data encryption

Mnemonic: "Cyber Circles Networks, Computer Covers Machines"

મેમરી ટ્રીક: "સાયબર નેટવર્ક સુરક્ષિત કરે, કમ્પ્યુટર મણીન સાચવે"

## પ્રશ્ન 1(બ) [4 ગુણા]

CIA triad સમજાવો.

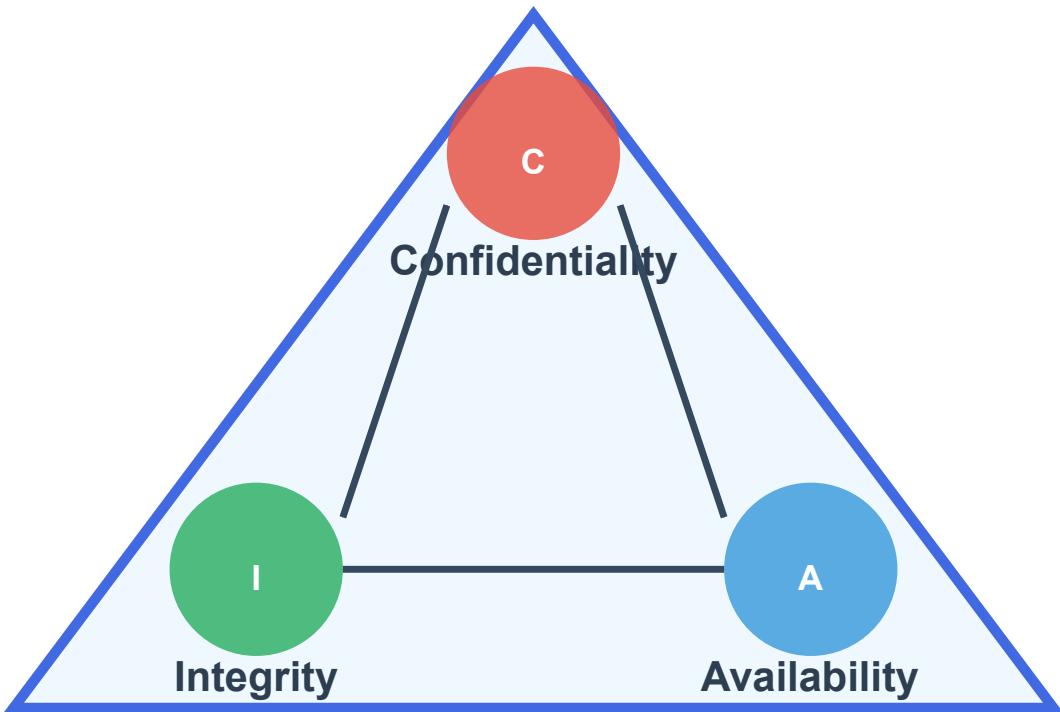
જવાબ:

CIA triad માહિતી સુરક્ષાના ત્રણ મૂળભૂત સિદ્ધાંતોનું પ્રતિનિધિત્વ કરે છે:

સિદ્ધાંત	વિગત
Confidentiality	ખાતરી કરે છે કે સંવેદનશીલ માહિતી માત્ર અધિકૃત પક્ષો દ્વારા જ એક્સોસિબલ છે
Integrity	ડેટા સ્ટોરેજ અને ટ્રાન્સમિશન દરમિયાન સથોટ અને અપરિવર્તિત રહે છે તેની ગોરંટી આપે છે
Availability	સિસ્ટમ્સ અને ડેટા જરૂર પડે ત્યારે અધિકૃત વપરાશકર્તાઓ માટે એક્સોસિબલ હોય તેની ખાતરી કરે છે

ડાયાગ્રામ:

## CIA TRIAD



મેમરી ટ્રીક: "CIA માહિતી યોગ્ય રીતે એકસેસિબલ રાખો"

### પ્રશ્ન 1(સ) [7 ગુણા]

કોમ્પ્યુટર સુરક્ષાના સંદર્ભમાં એડવર્સરી, એટેક, કાઉન્ટરમેઝર, રિસ્ક, સિક્યુરિટી પોલિસી, સિસ્ટમ રીસોર્સ અને થ્રેટ ને વ્યાખ્યાયિત કરો.

જવાબ:

શાન્દ	વ્યાખ્યા
Adversary	વ્યક્તિ અથવા જૂથ જે દુલ્હારનાપૂર્ણ હેતુઓ માટે કમજોરીઓનો ફાયદો ઉઠાવવાનો પ્રયાસ કરે છે
Attack	સિસ્ટમમાં રહેલી કમજોરીઓનો ફાયદો ઉઠાવીને સુરક્ષાને સમાધાન કરવાની જાણીજોઈને કરાયેલી કાર્યવાહી
Countermeasure	સુરક્ષા કમજોરીઓને ઓછી કરવા અથવા દૂર કરવા માટે લાગુ કરવામાં આવતા નિયંત્રણો
Risk	જ્યારે ખતરો કમજોરીના ફાયદો ઉઠાવે ત્યારે નુકસાન થવાની સંભાવના
Security Policy	સ્વીકાર્ય ઉપયોગ અને સુરક્ષા જરૂરિયાતોને વ્યાખ્યાયિત કરતા દસ્તાવેજુકૃત નિયમો
System Resource	હાર્ડવેર, સોફ્ટવેર, ડેટા, અથવા નેટવર્ક ઘટકો જેને સુરક્ષાની જરૂર છે
Threat	સંભવિત ખતરો જે સુરક્ષાને તોડવા માટે કમજોરીનો ફાયદો ઉઠાવી શકે છે

ડાયાગ્રામ:

## Security Threat Relationship Model



મેમરી ટ્રીક: "ARTSVSC: અમારા રિસોર્સની ટેકનોલોજી સુરક્ષિત વિવિધ સિસ્ટમ કમ્પોનન્ટ"

## પ્રશ્ન 1 (8 OR) [7 ગુણા]

MD5 હેણિંગ અલોરિધમ સમજાવો.

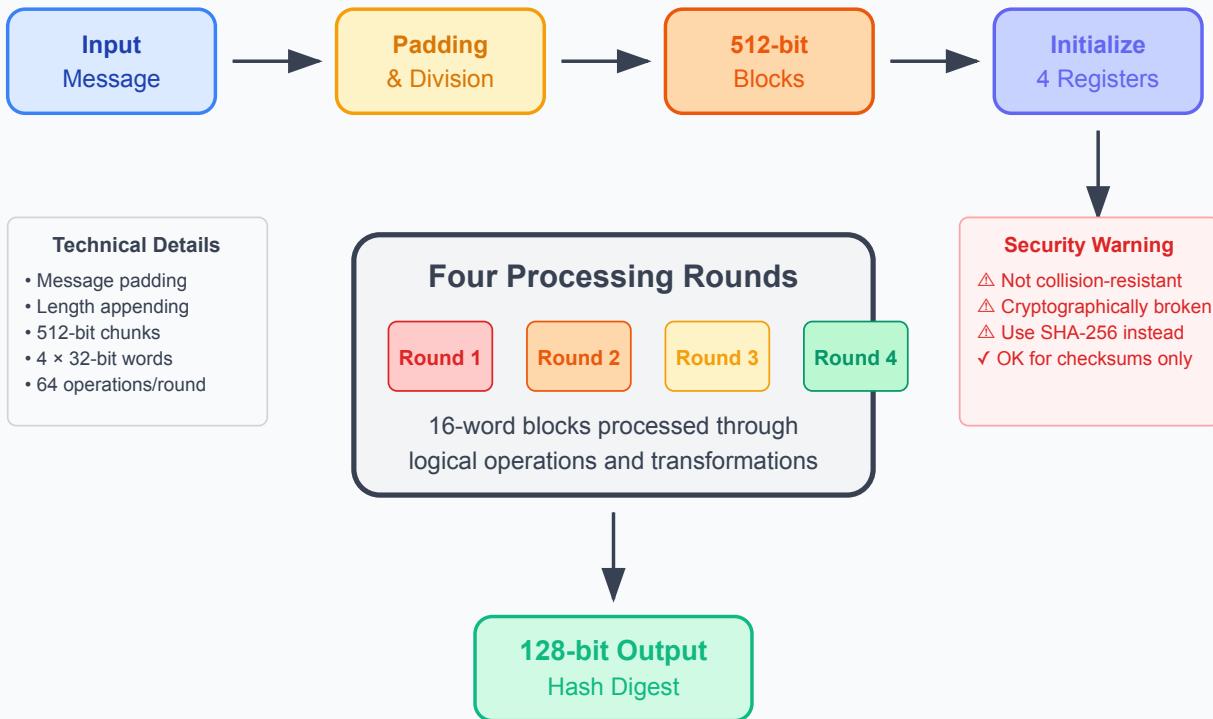
જવાબ:

MD5 (Message Digest 5) એક વ્યાપકપણે ઉપયોગમાં લેવાતી કિટોગ્રાફિક હેશ ફંક્શન છે જે 128-બિટ (16-બાઇટ) હેશ વેલ્યુ આપે છે:

- Input Processing:** સંદેશને પેડ કરવામાં આવે છે અને 512-બિટ બ્લોક્સમાં વિભાજિત કરવામાં આવે છે
- Initialization:** ચાર 32-બિટ રજિસ્ટર્સને નિશ્ચિત મૂલ્યો સાથે સેટઅપ કરે છે
- Compression:** 16-વર્ડ બ્લોક્સમાં સંદેશને ચાર રાઉન્ડના ઓપરેશન્સ દ્વારા પ્રોસેસ કરે છે
- Output:** અંતિમ હેશ મૂલ્ય તરીકે 128-બિટ ડાયજેસ્ટ આપે છે

ડાયાગ્રામ:

## MD5 Hashing Algorithm Process



- નભાઈ:** કોલિજન-રેજિસ્ટરન્ટ નથી; સુરક્ષા-કિટિકલ એપ્લિકેશન્સ માટે ઉપયોગ ન કરવો જોઈએ
- ઉપયોગ:** ફાઈલ ઇન્ટેગ્રિટી વેરિફિકેશન અને નોન-સિક્યુરિટી કિટિકલ એપ્લિકેશન્સ

**મેમરી ટ્રીક:** "પેડ, વિભાજન, પ્રોસેસ, આઉટપુટ - સુરક્ષા માટે વાપરણો નહીં!"

## પ્રથન 2(અ) [૩ ગુણા]

સાયબર સુરક્ષાના સંદર્ભમાં ઓથેન્ટિકેશન વ્યાખ્યાયિત કરો.

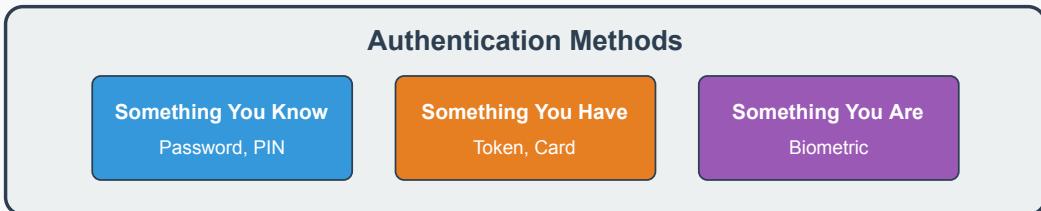
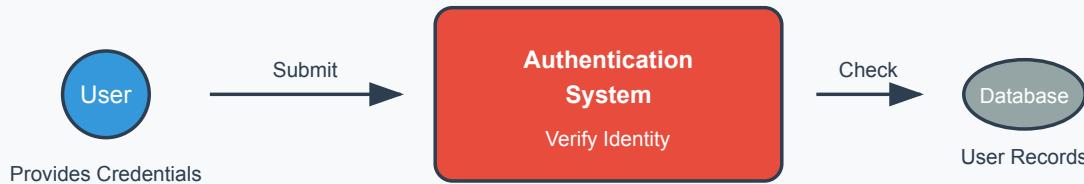
### જવાબ:

Authentication એ રિસોર્સની એક્સેસ આપતા પહેલાં વપરાશકર્તા, સિસ્ટમ અથવા એન્ટ્રીની ઓળખની ચકાસણી કરવાની પ્રક્રિયા છે:

- પુષ્ટિ કરે છે:** "તમે જે હોવાનો દાવો કરો છો તે જ છો"
- ચકાસે છે:** કેડેન્િયલ્સ (પાસવર્ડ, બાયોમેટ્રિક્સ, ટોકન) વડે ઓળખ
- આગામ આવે છે:** Authorization (ઓથેન્ટિકેશન પછી તમે શેને એક્સેસ કરી શકો છો)

### ડાયાગ્રામ:

## Authentication Process in Cyber Security



મેમરી ટ્રિક: "પ્રવેશ પહેલા ચકાસો"

## પ્રશ્ન 2(બ) [4 ગુણા]

આર્જનિક કી કિએચોયાફી ઉદાહરણ સાથે સમજાવો.

જવાબ:

Public key cryptography સુરક્ષિત કોમ્યુનિકેશન માટે બે ગાણિતિક રીતે સંબંધિત કી વાપરે છે:

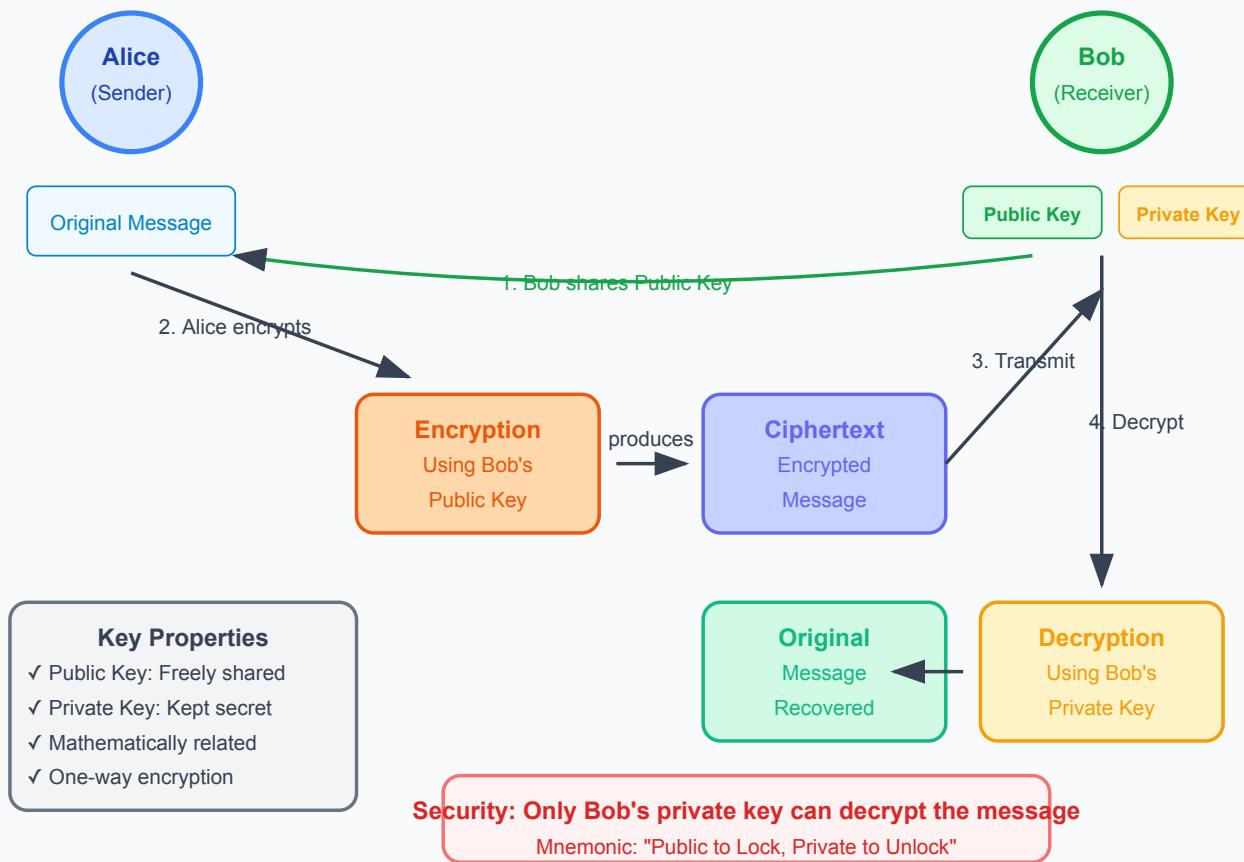
કોમ્યોન્ન	કાર્ય
Public Key	ખુલ્લેઆમ શેર કરવામાં આવે છે અને સંદેશાઓને એન્ક્રિપ્ટ કરવા માટે વપરાય છે
Private Key	ગુપ્ત રાખવામાં આવે છે અને સંદેશાઓને ડિન્ક્રિપ્ટ કરવા માટે વપરાય છે

ઉદાહરણ: RSA encryption માં, જો Alice Bob ને સંદેશો મોકલવા માંગે છે:

1. Alice, Bob ની public key વડે એન્ક્રિપ્ટ કરે છે
2. માત્ર Bob જ પોતાની private key નો ઉપયોગ કરીને ડિન્ક્રિપ્ટ કરી શકે છે

ડાયાગ્રામ:

## Public Key Cryptography Example



મેમરી ટ્રીક: "પબ્લિક લોક કરે, પ્રાઇવેટ અનલોક કરે"

## પ્રશ્ન 2(૬) [૭ ગુણા]

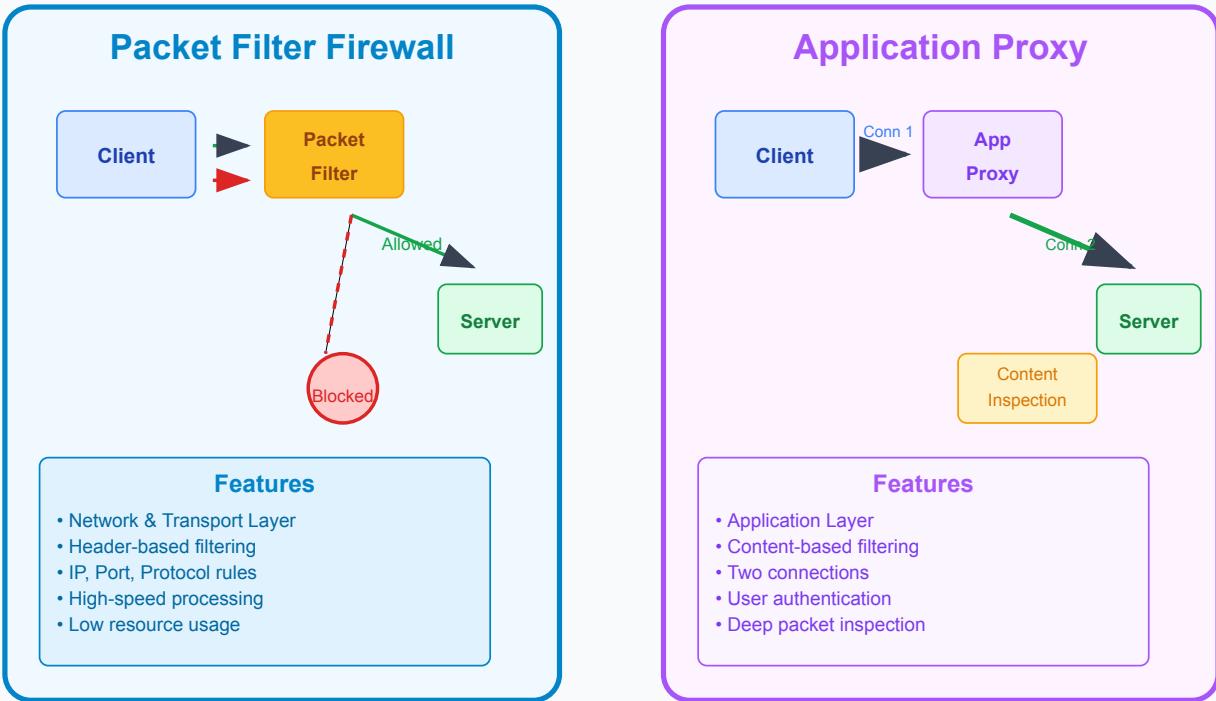
પેકેટ ફિલ્ટર અને એપ્લિકેશન પ્રોક્સીની કામગીરી સમજાવો.

જવાબ:

ફાયરવોલ પ્રકાર	કાર્યપ્રદ્ધતિ
Packet Filter	પૂર્વનિર્ધારિત નિયમોના આધારે પેકેટ હેડર્સની તપાસ કરે છે. સોર્સ/ડેસ્ટિનેશન IP એફ્રેસ, પોર્ટ્સ અને પ્રોટોકોલના આધારે નિર્ણયો લે છે. OSI નેટવર્ક અને ટ્રાન્સપોર્ટ લેયર પર કામ કરે છે. ઓછા રિસોર્સના વપરાશ સાથે હાઇ-સ્પિડ ફિલ્ટરિંગ ઓફર કરે છે.
Application Proxy	કલાયન્ટ અને સર્વર એપ્લિકેશાન્સ વચ્ચે મધ્યસ્થી તરીકે કાર્ય કરે છે. એપ્લિકેશન લેયર પર બધા ટ્રાફિકને પ્રોસેસ કરે છે. બે કનેક્શન બનાવે છે (કલાયન્ટ-ટુ-પ્રોક્સી અને પ્રોક્સી-ટુ-સર્વર). કન્ટેનર ઇન્સ્પેક્શન અને યુઝર ઓથેન્ટિકેશન ક્ષમતાઓ પ્રદાન કરે છે.

ડાયાગ્રામ:

## Packet Filter vs Application Proxy



**Mnemonic: "Packets Check Headers, Proxies Check Content"**

Packet Filter: Fast but Basic | Application Proxy: Slow but Thorough

મેમરી ટ્રીક: "પેકેટ હેડર તપાસે, પ્રોક્સી કન્ટેન્ટ ચકાસે"

## પ્રશ્ન 2(અ OR) [3 ગુણા]

મલ્ટી ફેક્ટર ઓથેન્ટિકેશન સમજાવો.

જવાબ:

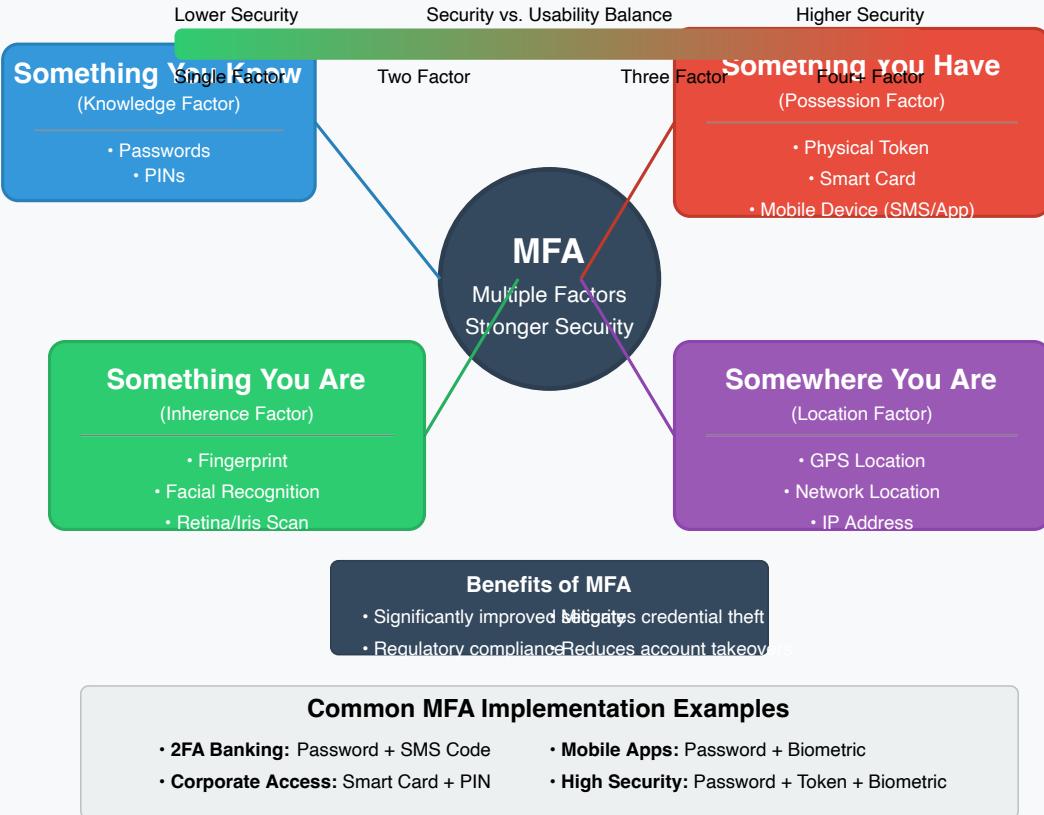
Multi-factor authentication (MFA) વપરાશકર્તાઓને રિસોર્સની એક્સસેસ મેળવવા માટે બે અથવા વધુ વેરિફિકેશન ફેક્ટર્સ પ્રદાન કરવાની જરૂર પડે છે:

- જે તમે જાણો છો: પાસવર્ડ, PIN, સિક્યુરિટી પ્રશ્ન
- જે તમારી પાસે છે: મોબાઇલ ફોન, સ્માર્ટ કાર્ડ, સિક્યુરિટી ટોકન
- જે તમે છો: ફિંગરપ્રિન્ટ, ચહેરા ઓળખ, અવાજનો પેટર્ન

ડાયાગ્રામ:

## Multi-Factor Authentication (MFA)

### Strengthening Security Through Multiple Verification Methods



મેમરી ટ્રીક: "જાણો, રાખો, છો - ત્રિવિધ સુરક્ષા"

## પ્રશ્ન 2(બ OR) [4 ગુણા]

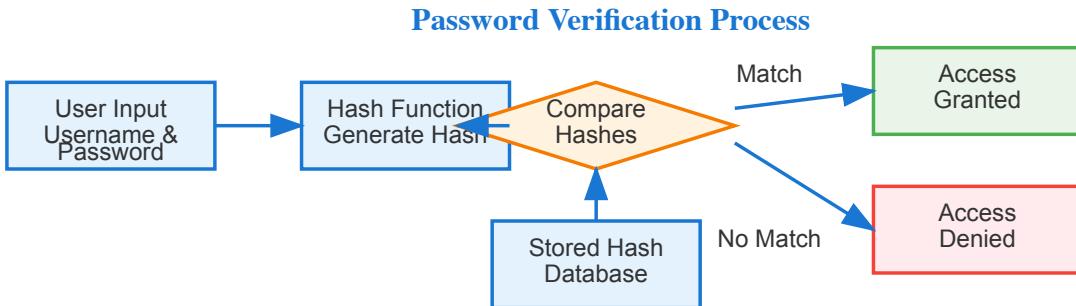
પાસવર્ડ વેરિફિકેશનની પ્રક્રિયા સમજાવો.

### જવાબ:

Password verification એ સ્ટોર કરેલા મૂલ્યો સામે યુઝર કેડેન્શિયલ્સને ઓથેન્ટિકેટ કરવાની પ્રક્રિયા છે:

- User Input:** યુઝર યુઝરનેમ અને પાસવર્ડ દાખલ કરે છે
- Hash Generation:** સિસ્ટમ દાખલ કરેલા પાસવર્ડને હેશ કરે છે
- Comparison:** હેશને ડેટાબેસમાં સ્ટોર થયેલ હેશ સાથે સરખાવવામાં આવે છે
- Access Decision:** જો હેશ મેળ ખાય તો એક્સેસ આપવામાં આવે છે, નહીં તો નકારવામાં આવે છે

### ડાયાગ્રામ:



**Process Steps:**

1. User enters username and password
2. System applies hash function to entered password
3. Generated hash is compared with stored hash in database
4. Access granted if hashes match, denied otherwise

**Security Note: Passwords are never stored in plain text**

મેમરી ટ્રીક: "દાખલ, હેચા, સરખામણી, નિર્ણય"

## પ્રશ્ન 2(S OR) [7 ગુણ]

દૂષિત સૉફ્ટવેરની સૂચિ બનાવો અને કોઈપણ ત્રણ દૂષિત સૉફ્ટવેર હુમલાઓ સમજાવો.

જવાબ:

દૂષિત સૉફ્ટવેરના પ્રકારો:

- Viruses, Worms, Trojans, Ransomware, Spyware, Adware, Rootkits, Keyloggers, Bots

ત્રણ સામાન્ય હુમલાઓ:

હુમલાનો પ્રકાર	સમજૂતી
Ransomware	પીડિતની ફાઇલોને એન્ક્રિપ્ટ કરે છે અને ડિક્રિપ્શન કી માટે ચુકવણીની માંગ કરે છે. ફિશિંગ ઇમેઇલ્સ, દૂષિત ડાઉનલોડ્સ, અથવા કમજોરીઓનો ફાયદો ઉઠાવીને ફેલાય છે. ઉદાહરણ: WannaCry.
Trojans	કાયદેસર સોફ્ટવેર તરીકે છુપાયેલા પરંતુ દુર્ભાવનાપૂર્ણ કાર્યો કરે છે. હુમલાખોરો માટે સિસ્ટમમાં પ્રવેશાવા માટે બેકડોર બનાવે છે. ઉદાહરણ: Remote Access Trojans (RATs).
Spyware	સંમતિ વિના ચુંચ માહિતી એકત્રિત કરે છે. પ્રવૃત્તિઓ, કીસ્ટ્રોક્સ અને બ્રાઉઝિંગ આદતોને મોનિટર કરે છે. પાસવર્ડ અને નાણાકીય માહિતી થોરી કરી શકે છે.

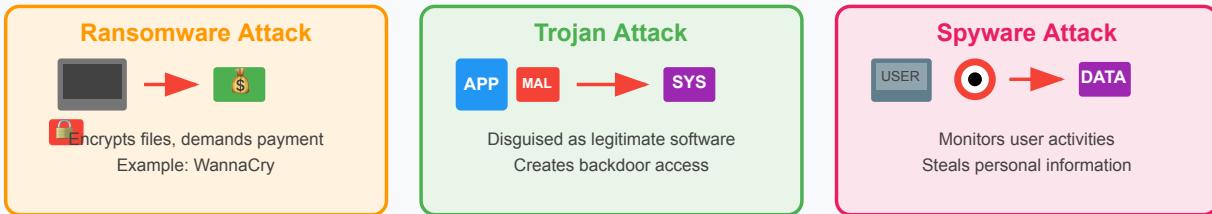
ડાયાગ્રામ:

# Malicious Software Types & Attack Examples

## Common Malicious Software Types:



## Three Common Attack Examples



## Common Attack Vectors



મેમરી ટ્રીક: "RTS: રેન્સમ સિસ્ટમ લે છે, ટ્રોજન છુપાઈને આવે છે, સ્પાયવેર માહિતી ચોરે છે"

## પ્રશ્ન 3(અ) [૩ ગુણા]

સાયબર સુરક્ષામાં પોર્ટનું મહત્વ સમજાવો.

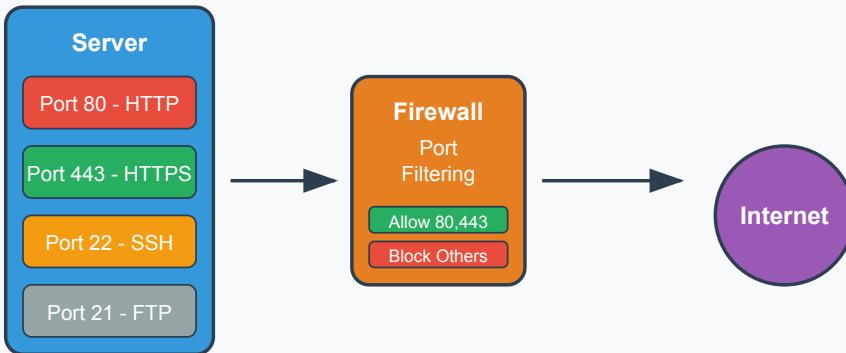
જવાબ:

Ports એ નેટવર્ક કોમ્યુનિકેશન માટેના વર્ચ્યુઅલ અન્ડપોઇન્ટ્સ છે જે:

- સેવાઓને આપણે છે: દરેક સેવા ચોક્કસ પોર્ટ નંબરનો ઉપયોગ કરે છે (HTTP:80, HTTPS:443)
- ફિલ્ટરિંગ સક્ષમ કરે છે: ફાયરવોલ ચોક્કસ પોર્ટ્સને મંજૂરી/બલોક કરીને ટ્રાફિકને નિયંત્રિત કરે છે
- અટેક સરફેસ ઘટાડે છે: બિનજરી પોર્ટ્સ બંધ કરવાથી સુરક્ષા વધે છે

ડાયાગ્રામ:

## Importance of Ports in Cyber Security



### Security Benefits of Port Management

#### Service Identification

Each service uses specific port numbers

#### Traffic Control

Firewalls filter by port numbers

#### Attack Surface

Closing unused ports reduces vulnerabilities

મેમરી ટ્રીક: "દરેક પોર્ટ એક પ્રવેશદ્વાર છે"

## પ્રશ્ન 3(બ) [4 ગુણા]

વાર્ષ્યાલ પ્રાઇવેટ નેટવર્ક સમજાવો.

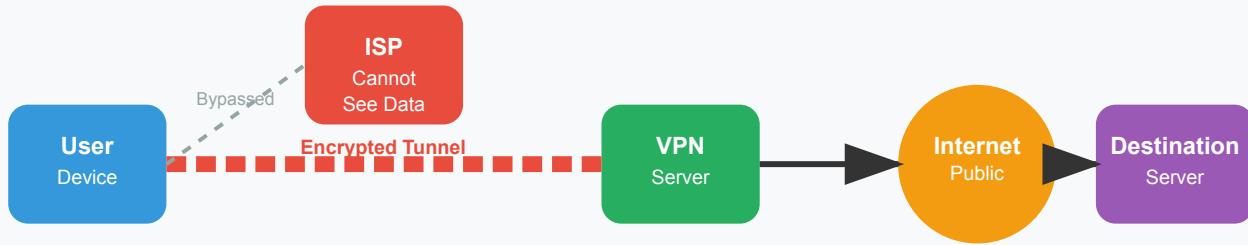
#### જવાબ:

Virtual Private Network (VPN) એ એવી ટેકનોલોજી છે જે:

ફીચર	વિગત
Encrypted Tunnel	જાહેર નેટવર્ક પર સુરક્ષિત કનેક્શન બનાવે છે
IP Masking	યુઝરના IP એડ્રેસ અને લોકેશનને છુપાવે છે
Data Protection	ટ્રાન્સમિશન દરમિયાન ડેટાને એન્ક્રિપ્ટ કરે છે
Remote Access	પ્રાઇવેટ નેટવર્ક્સમાં સુરક્ષિત કનેક્શન સક્ષમ કરે છે

#### ડાયાગ્રામ:

## VPN Architecture



## VPN Security Benefits



## VPN Protocols

## OpenVPN (High Security)

## IPSec (Enterprise)

## WireGuard (Modern)

1. Connect → 2. Authenticate → 3. Encrypt → 4. Route → 5. Decrypt

ਮੇਮਰੀ ਡ੍ਰੀਕ: "ਟਨਲ, ਅੇਨਿਕਿਟ, ਰਕਸ਼ਣਾ, ਕਨੇਕਟ"

### પ્રથમ 3(સ) [7 ગુણા]

વેબ સુરક્ષા જોખમોની અસર સમજાવો.

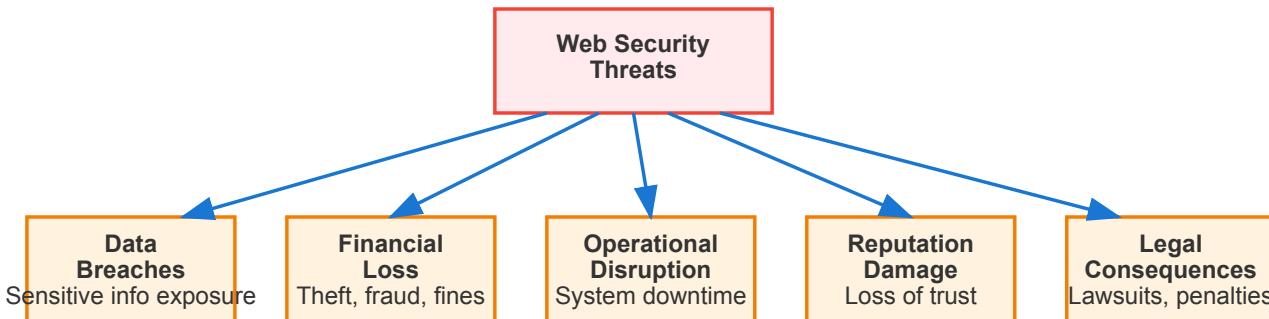
ଜୟାମାନ

વેબ સુરક્ષા જોખમોની સંસ્થાઓ અને વ્યક્તિઓ પર નોંધપાત્ર અસરો પડે છે:

અસર	વિગત
<b>Data Breaches</b>	સંવેદનશીલ માહિતીનો ખુલાસો જે નાણાકીય નુકસાન અને પ્રતિષ્ઠાને નુકસાન તરફ દોરી જાય છે
<b>Financial Loss</b>	સીધી નાણાકીય ચોરી, છેતરપિંડી, રિકવરી ખર્ચ, અને નિયમનકારી દંડ
<b>Operational Disruption</b>	સિસ્ટમ ડાઉનટાઇમ જે બિઝનેસ કન્ટિન્યુએટી અને કસ્ટમર સર્વિસને અસર કરે છે
<b>Reputation Damage</b>	સુરક્ષા ઘટનાઓ પછી ગ્રાહકોનો વિશ્વાસ અને બ્રાન્ડ વેલ્યુનું નુકસાન
<b>Legal Consequences</b>	કાનૂની કાર્યવાહી, નિયમનકારી દંડ, અને કમ્પલાયન્સ ઉલ્લંઘન

દાયાત્રામઃ

## Web Security Threats Impact



### Impact Examples:

- Customer data theft
- Business operations halt
- Brand reputation loss

### Prevention Measures:

- Regular security audits
- Employee training
- Incident response plans

મેમરી ટ્રીક: "DFROL: ડેટા, ફાઇનાન્સ, રિસોર્સ, ઓપિનિયન, લીગાલ"

## પ્રશ્ન 3(અ OR) [3 ગુણા]

ડિજિટલ સિંગનેચરની કામગીરી સમજાવો.

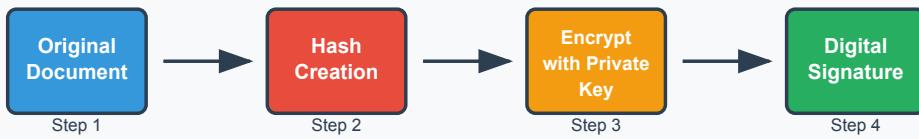
### જવાબ:

Digital signatures ઇલેક્ટ્રોનિક દસ્તાવેજોને પ્રમાણિત કરે છે અને તેમની અખંડિતતાની ચકાસણી કરે છે:

- Hash Creation:** દસ્તાવેજને હેશ કરીને અનન્ય ડાયજેસ્ટ બનાવવામાં આવે છે
- Encryption:** મોકલનાર પોતાની પ્રાઇવેટ કી વાપરીને હેશને એન્ક્રિપ્ટ કરે છે
- Verification:** પ્રાપ્તકર્તા મોકલનારની પબ્લિક કી વાપરીને ડિક્રિપ્ટ કરે છે
- Validation:** ડિક્રિપ્ટ થયેલ હેશને નવા જનરેટ કરેલા હેશ સાથે સરખાવવું

### ડાયાગ્રામ:

## Digital Signature Working Process



## Verification Process



## Digital Signature Features

**Authentication**  
Verifies sender identity

**Integrity**  
Detects any modifications

**Non-repudiation**  
Sender cannot deny signing

મેમરી ટ્રીક: "હેશ, સાઇન, મોકલો, ચકાસો"

## પ્રશ્ન 3(અ OR) [4 ગુણા]

HTTPS નું વર્ણન કરો.

### જવાબ:

HTTPS (Hypertext Transfer Protocol Secure) એ HTTP નું સુરક્ષિત વર્ઝન છે:

ફીચર	વિગત
TLS/SSL	ડેટાને અનિક્ષાર કરવા માટે Transport Layer Security વાપરે છે
Authentication	સર્ટિફિકેટ્સ દ્વારા વેબસાઇટની ઓળખ ચકાસે છે
Data Integrity	પ્રસારિત ડેટાના ફેરફારને અટકાવે છે
Port 443	HTTP ના પોર્ટ 80 ને બદલે ડિફોલ્ટ પોર્ટ 443 વાપરે છે

### ડાયાગ્રામ:

## HTTPS Communication Process



### HTTPS Components



### Security Benefits

- Data Encryption
- Server Authentication
- Data Integrity

મેમરી ટ્રીક: "સુરક્ષિત પેજ પાસે પેડલોક હોય છે"

## પ્રથમ ૩(S OR) [૭ ગુણા]

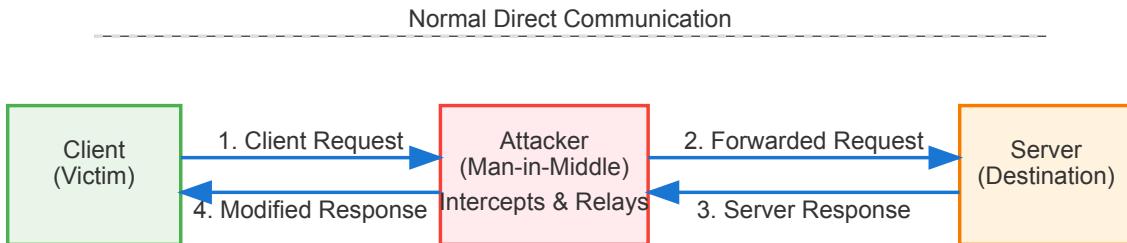
સોશિયલ એન્જિનિયરિંગ, વિશિંગ અને મશીન ઇન મિડલ એટેક સમજાવો.

જવાબ:

હુમલાનો પ્રકાર	સમજૂતી
Social Engineering	સંવેદનશીલ માહિતી જાહેર કરવા માટે યુઝરને છેતરવા માટેનું માનસિક હેરફેર. તકનીકી કમજોરીઓને બદલે માનવ વિશ્વાસનો ફાયદો ઉઠાપે છે. સામાન્ય તકનીકોમાં pretexting, baiting, અને phishing શામેલ છે.
Vishing	ફોન કોલ્સનો ઉપયોગ કરીને માહિતી ચોરવા માટે વોઇસ ફિશિંગ. હુમલાખોરો કાયદેસર સંસ્થાઓનું પ્રતિનિધિત્વ કરે છે. પીડિટોને હેરફેર કરવા માટે ઘણીવાર તાત્કાલિકતા અથવા ભયનો ઉપયોગ કરે છે.
Machine in the Middle	હુમલાખોર ગુપ્તપણે બે પક્ષો વચ્ચેના સંદેશાવ્યવહારને અવરોધે છે અને રિલે કરે છે. પીડિટોને લાગે છે કે તેઓ એકબીજા સાથે સીધો સંદેશાવ્યવહાર કરી રહ્યા છે. હુમલાખોરોને ટ્રાન્સમિશન દરમિયાન સંવેદનશીલ માહિતી ચોરી/ફરફાર કરવાની મંજૂરી આપે છે.

ડાયાગ્રામ:

## Man-in-the-Middle (MITM) Attack



### Attack Process:

1. Attacker positions between client and server
2. Intercepts all communications
3. Can read, modify, or block messages
4. Forwards modified data to destination

### Types of MITM:

- ARP Spoofing
- DNS Spoofing
- SSL/TLS Interception
- Wi-Fi Eavesdropping

### Attacker Can:

- Steal sensitive data (passwords, credit cards)
- Inject malicious content
- Modify transactions
- Impersonate either party

### Prevention:

- Use HTTPS/SSL/TLS
- Verify certificates
- Use VPNs on public Wi-Fi
- Enable two-factor authentication

મેમરી ટ્રીક: "SEVeM: સોશિયલ લોકોને છેતરે, વિશિંગ અવાજ વાપરે, મશીન મદ્યામાં બેસે"

## પ્રશ્ન 4(અ) [૩ ગુણા]

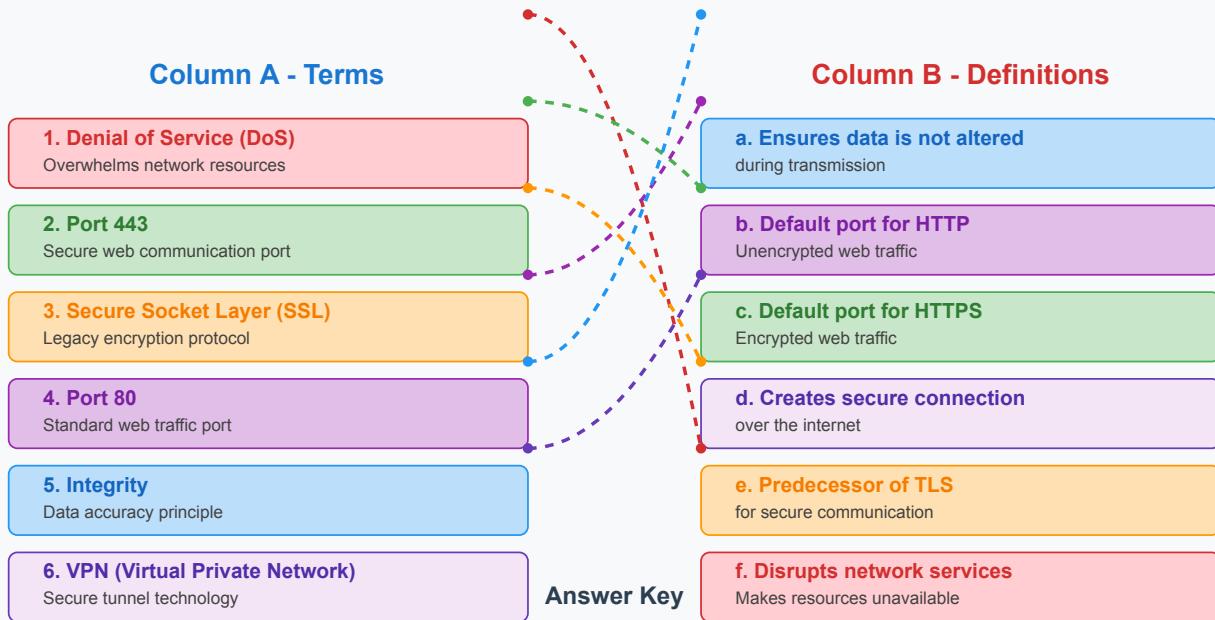
જોડકા જોડો.

જવાબ:

સંલાલ A	સંલાલ B
1. Denial of Service (DoS)	f. નેટવર્ક સેવાઓને વિક્ષેપિત કરતો હુમલો
2. Port 443	c. HTTPS માટે ડિફોલ્ટ પોર્ટ
3. Secure Socket Layer (SSL)	e. સુરક્ષિત સંચાર માટે TLS ના પૂર્વગામી
4. Port 80	b. HTTP માટે ડિફોલ્ટ પોર્ટ
5. Integrity	a. ડ્રાન્સમિશન દરમિયાન ડેટા બદલાયો નથી તેની ખાતરી કરે છે
6. VPN (Virtual Private Network)	d. ઇન્ટરનેટ પર સુરક્ષિત કનેક્શન બનાવે છે

ડાયાગ્રામ:

## Cybersecurity Terms Matching



Key Security Concepts: Ports, Protocols, Attacks, and Protection Mechanisms

મેમરી ટ્રીક: "DoS HTTPS, SSL HTTP, Integrity VPN"

મેમરી ટ્રીક: "સેવા HTTPS, સુરક્ષિત HTTP, અખંડ VPN"

## પ્રશ્ન 4(બ) [4 ગુણા]

હેકર્સના પ્રકારોની યાદી બનાવો અને દરેકની લૂભિકા સમજાવો.

જવાબ:

હેકર્સનો પ્રકાર	લૂભિકા
White Hat	અદ્યિકલ હેકર્સ જે સુરક્ષા સુધારવા માટે પરવાનગી સાથે સિસ્ટમનું પરીક્ષણ કરે છે
Black Hat	દુર્ભાવનાપૂર્ણ હેકર્સ જે વ્યક્તિગત લાલ અથવા નુકસાન માટે કમજોરીઅંનો ફાયદો ઉઠાવે છે
Gray Hat	નૈતિક અને દુર્ભાવનાપૂર્ણ વચ્ચે કામ કરે છે; પરવાનગી વિના હેક કરી શકે છે પરંતુ જાણકારી જાહેર કરે છે
Script Kiddies	અનુભવ વગારના હેકર્સ જે ટેકનોલોજી સમજાયા વિના પ્રી-રાઇટન સ્ક્રિપ્ટનો ઉપયોગ કરે છે

ડાયાગ્રામ:

# Types of Hackers

## Hacker Classification by Intent

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

## 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

મેમરી ટ્રીક: "સફેદ રક્ષણ કરે, કાળો હુમલો કરે, ગ્રે મિશ્રિત રહે, બાળકો સ્કિપ વાપરે"

## પ્રશ્ન 4(સ) [7 ગુણા]

SSH (સિક્યુર શેલ) પ્રોટોકોલ સ્ટેક સમજાવો.

જવાબ:

SSH (Secure Shell) પ્રોટોકોલ સ્ટેક સુરક્ષિત રિમોટ એક્સેસ અને ફાઇલ ટ્રાન્સફર પ્રદાન કરે છે:

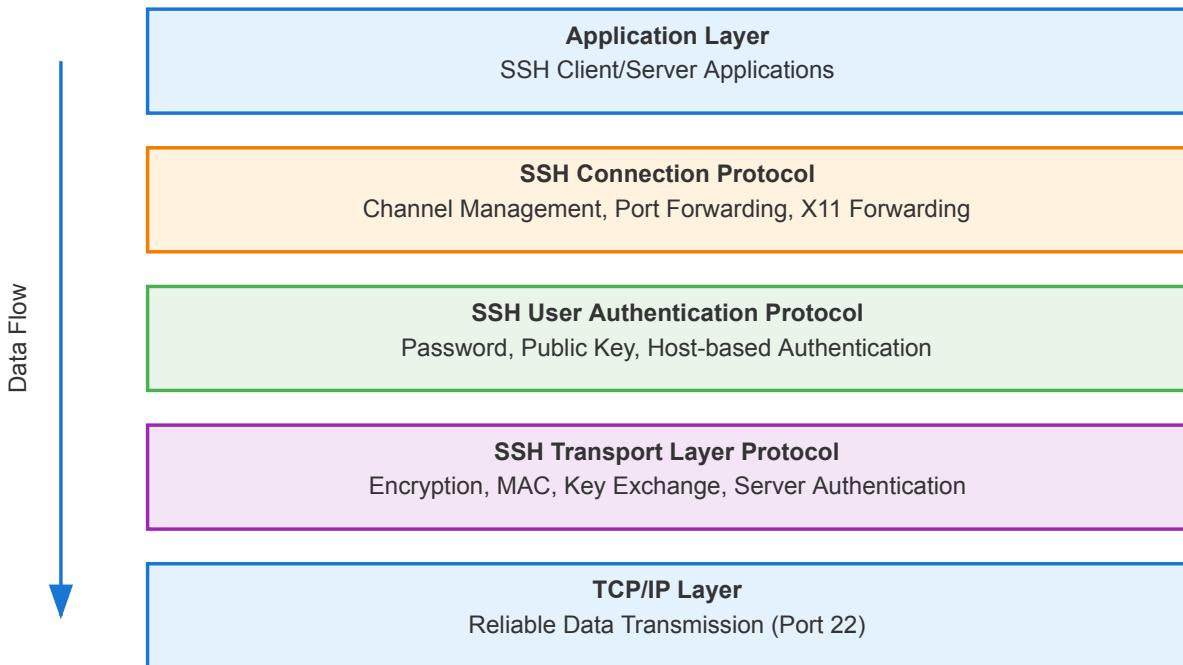
લયર	કાર્ય
Transport Layer	અેન્ક્રિપ્શન, સર્વર ઓથેન્ટિકેશન, અને ડેટા ઇન્ટેગ્રિટીનું સંચાલન કરે છે
User Authentication Layer	પાસવર્ડ, કી, અથવા સર્ટિફિકેટનો ઉપયોગ કરીને કલાયન્ટની ઓળખની ચકાસણી કરે છે
Connection Layer	એક SSH કનેક્શનમાં મલ્ટિપલ એન્સ્યુનું સંચાલન કરે છે

મુખ્ય ફીચર્સ:

- મજબૂત અેન્ક્રિપ્શન (AES, 3DES)
- પબ્લિક કી ઓથેન્ટિકેશન
- ડેટા ઇન્ટેગ્રિટી ચેકિંગ
- પોર્ટ ફોરવર્ડિંગ અને ટનલિંગ

## દાયાગ્રામ:

### SSH (Secure Shell) Protocol Stack



#### SSH Features:

- Secure Remote Login
- Command Execution
- File Transfer (SCP/SFTP)
- Port Forwarding

#### Security Features:

- End-to-End Encryption
- Host Authentication
- Data Integrity
- Protection against attacks

મેમરી ટ્રીક: "ટ્રાન્સ્પોર્ટ સુરક્ષિત કરે, ચુક્સ ઓળખાય, કનેક્શન મલ્ટિપ્લેક્સ કરે"

## પ્રશ્ન 4(અ OR [3 ગુણા]

અંદ્રિકલ હેકિંગમાં ફૂટ પ્રિન્ટિંગ સમજાવો.

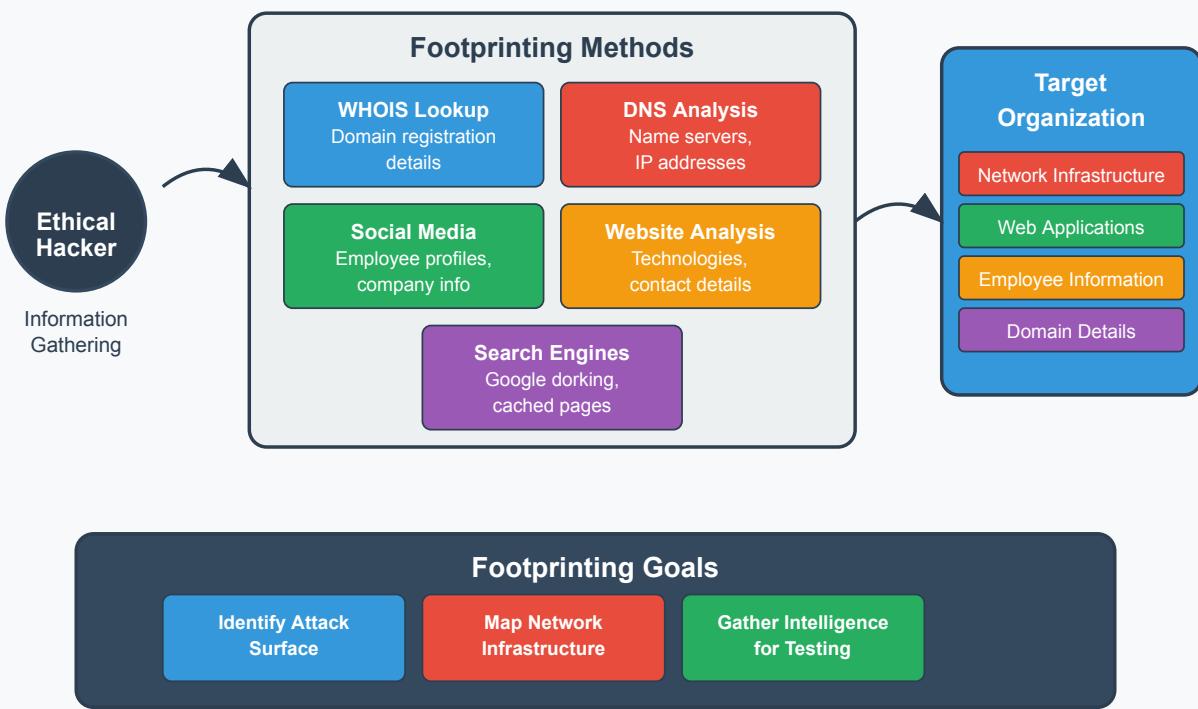
#### જવાબ:

Footprinting અંદ્રિકલ હેકિંગનો પ્રથમ તબક્કો છે જ્યાં લક્ષ્ય વિશે માહિતી અંકત્રિત કરવામાં આવે છે:

- હેતુ:** નેટવર્ક, સિસ્ટમ્સ, અને સંસ્થા વિશે ડેટા અંકત્રિત કરવું
- પદ્ધતિઓ:** WHOIS લુકઅપ, DNS અનાલિસિસ, સોશિયલ મીડિયા રિસર્ચ
- પરિણામો:** સંલિખિત પ્રવેશાબિંદુઓ અને કમજોરીઓની ઓળખ

## દાયાગ્રામ:

## Footprinting in Ethical Hacking



મેમરી ટ્રીક: "હુમલા પહેલા જાણકારી મેળવો"

## પ્રશ્ન 4(અ OR) [4 ગુણા]

એથિકલ હેકિંગમાં સ્કેનિંગ સમજાવો.

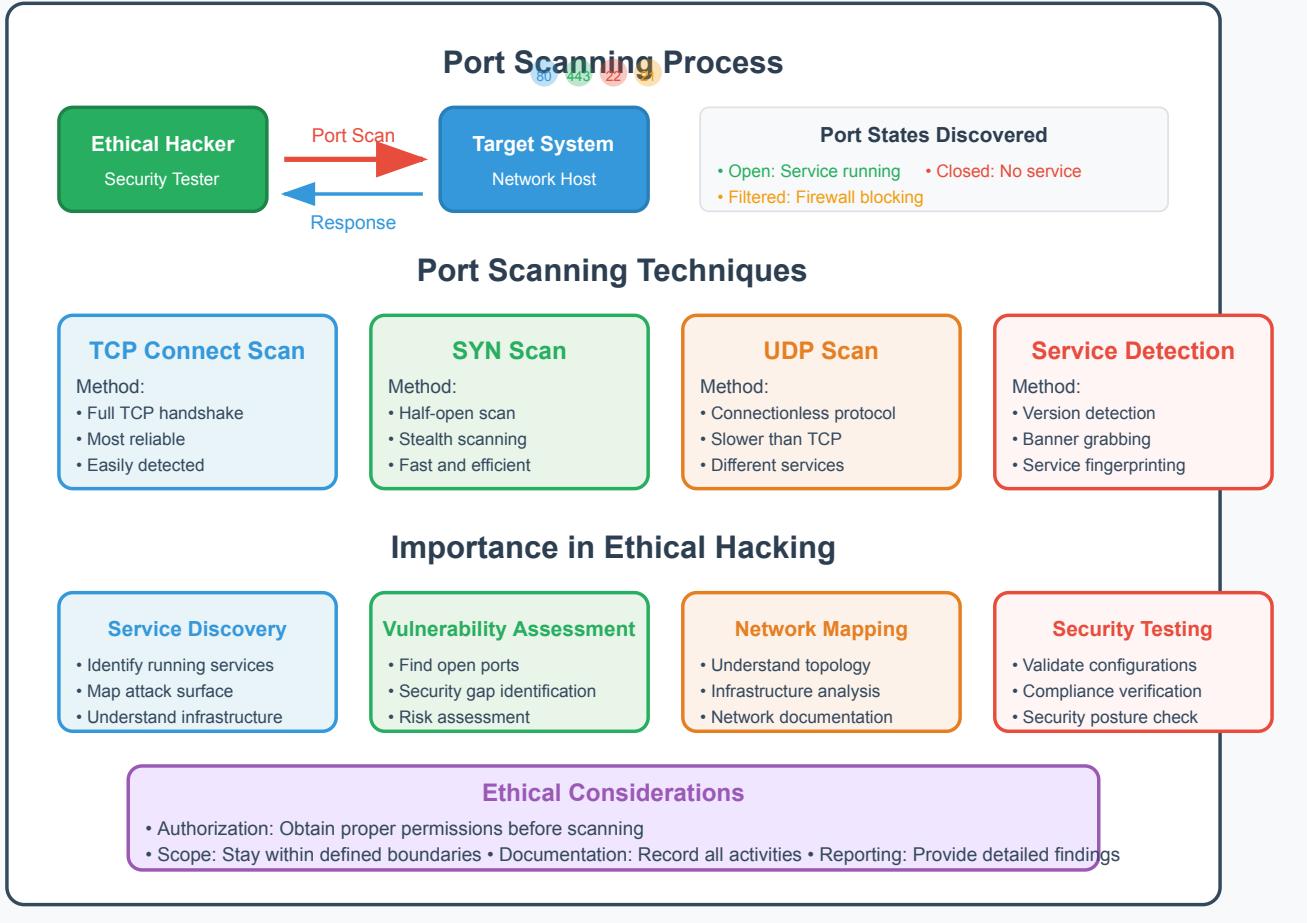
જવાબ:

Scanning એ લાઇવ હોસ્ટ્સ, અોપન પોર્ટ્સ, અને સર્વિસિસને અોળખવા માટે લક્ષ્ય સિસ્ટમને સંકિયપણે પ્રોબિંગ કરવાની પ્રક્રિયા છે:

તકનીક	હેતુ
Port Scanning	ખુલ્લા પોર્ટ્સ અને ચાલતી સેવાઓને અોળખે છે
Vulnerability Scanning	જાણીતી સુરક્ષા નબળાઈઓને શોધે છે
Network Mapping	નેટવર્ક ટોપોલોજી અને ડિવાઇસિસ શોધે છે
OS Fingerprinting	અોપરેટિંગ સિસ્ટમના વર્જન નકકી કરે છે

ડાયાગ્રામ:

# Port Scanning in Ethical Hacking



મેમરી ટ્રીક: "PONS: પોર્ટસ અ૱ન્પન, નેટવર્ક સર્વિસિસ"

## પ્રશ્ન 4(S OR) [7 ગુણ]

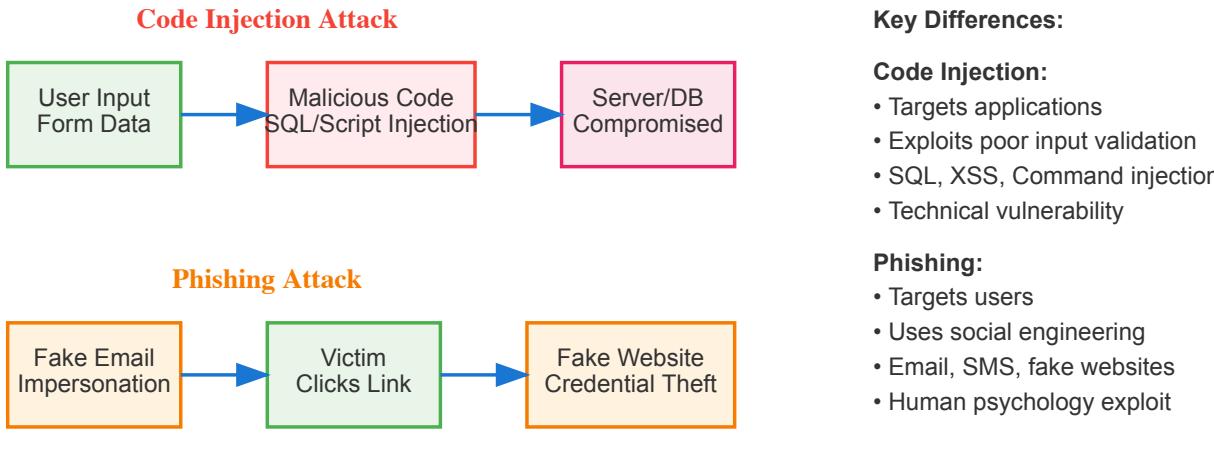
ઇન્જેક્શન એટેક અને ફિશિંગ એટેકનું વર્ણન કરો.

જવાબ:

હુમલાનો પ્રકાર	વર્ણન
Injection Attack	નબળી એસ્ટિકેશન્સમાં દુર્ભાવનાપૂર્ણ કોડ દાખલ કરે છે. સામાન્ય પ્રકારોમાં SQL injection, command injection, અને XSS શામેલ છે. ખરાબ ઇનપુટ વેલિડેશનનો ફાયદો ઉઠાવે છે. ડેટા ચોરી, ફેરફાર, અથવા નાશ તરફ દોરી શકે છે. ઇનપુટ સેનિટાઇઝેશન અને પેરામીટરાઇઝ્ડ કવેરી દ્વારા અટકાવી શકાય.
Phishing Attack	ફેક વેબસાઇટ્સ/ઈમેઇલ્સનો ઉપયોગ કરીને સોશિયલ એન્જિનિયરિંગ એટેક. ક્રેડિટિયલ્સ, નાણાકીય માહિતી ચોરવાનો, અથવા મેલવેર ઇન્સ્ટોલ કરવાનો પ્રયાસ કરે છે. અવારનવાર વિશ્વસનીય સંસ્થાઓની નકલ કરે છે. ભયજનક સ્થિતિ ઉલ્લેખ કરવા માટે તાત્કાલિક કૉલ-ટુ-એક્શન ઘરાવે છે. શિક્ષાણ, ઈમેઇલ ફિલ્ટરિંગ, અને મલ્ટી-ફેક્ટર એથેન્ટિકેશન દ્વારા અટકાવી શકાય છે.

ડાયાગ્રામ:

## Code Injection vs Phishing Attacks



### Examples:

#### Code Injection:

- SQL: ' OR '1'='1
- XSS: <script>alert('XSS')</script>
- Command: ; rm -rf /

#### Phishing:

- Fake bank emails
- Fake login pages
- CEO fraud emails

**Prevention:** Input validation + User education

મેમરી ટ્રીક: "ઇન્જેક્ટ કાંડ, ફિશ લોકોને"

## પ્રશ્ન 5(અ) [૩ ગુણા]

ડિસ્ક ફોરેન્સિક્સ સમજાવો.

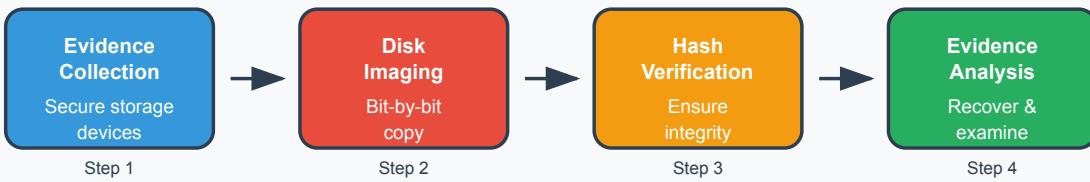
### જવાબ:

Disk forensics એ ડિજિટલ પુરાવા પુનઃપ્રાપ્ત, વિશેષણ, અને સંરક્ષિત કરવા માટે સ્ટોરેજ મીડિયાનું પરીક્ષા છે:

- છેત્ર:** ડિલીટ કરેલી ફાઇલો પુનઃપ્રાપ્ત કરવી, ફાઇલ સિસ્ટમનું વિશેષણ, અને ટાઇમલાઇન સ્થાપિત કરવી
- પદ્ધતિઓ:** બિટ-બાય-બિટ ઇમેજિંગ, હેચ વેરિફિકેશન, અને સ્પેશિયલાઇઝડ ટૂલ્સ
- અભિન્કરણાસ:** ક્રિમિનલ ઇન્વેસ્ટિગેશન, કોર્પોરેટ સિક્યુરિટી ઘટનાઓ, ડેટા રિકવરી

### ડાયાગ્રામ:

## Disk Forensics Process



### Disk Forensics Tools

EnCase  
Commercial tool

FTK Imager  
Imaging tool

Autopsy  
Open source

dd Command  
Unix/Linux

### Types of Analysis

File Recovery  
Deleted files restoration

Timeline  
Activity reconstruction

Metadata  
File system examination

Signature  
Hidden data detection

મેમરી ટ્રીક: "રિકવર, એનાલાઇઝ, પ્રોઝ-ન"

## પ્રશ્ન 5(બ) [4 ગુણા]

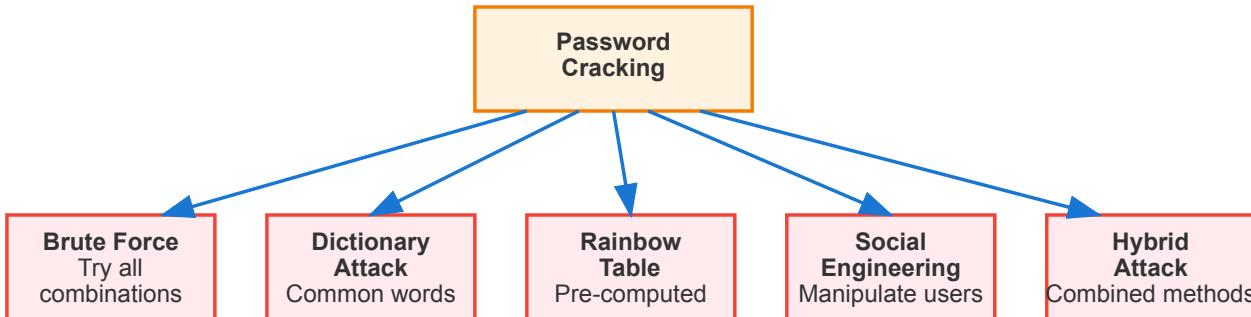
પાસવર્ડ કેકિંગ પદ્ધતિઓ સમજાવો.

જવાબ:

પદ્ધતિ	વિગત
Brute Force	વ્યવસ્થિતપણે તમામ સંલિપિત અક્ષર સંયોજનો પ્રયાસ કરે છે
Dictionary Attack	સામાન્ય શબ્દો અને વેરિઅશન-સની યાદીનો ઉપયોગ કરે છે
Rainbow Table	જડપી લુકઅપ માટે પાસવર્ડ હેશના પ્રી-કમ્પ્યુટેડ ટેબલ્સ
Social Engineering	પાસવર્ડ જાહેર કરવા માટે ચુંઝસને હેરફેર કરે છે

દાયાગ્રામ:

## Password Cracking Methods



### Method Details:

- Brute Force: Systematic trial of all possibilities
- Dictionary: Uses common password lists
- Rainbow Table: Pre-computed hash lookups

### Prevention:

- Use strong, complex passwords
- Enable account lockout policies
- Implement multi-factor authentication

મેમરી ટ્રીક: "BDRS: બૃંદ ડિક્રાનરી રેઇનબો સોશિયલ"

## પ્રશ્ન 5(ક) [7 ગુણા]

રિમોટ એડમિનિસ્ટ્રેશન ટૂલ (RAT) નું વર્ણન કરો.

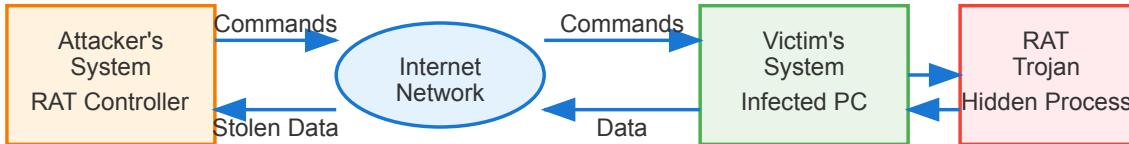
### જવાબ:

Remote Administration Tool (RAT) એ એવું સોફ્ટવેર છે જે કોમ્પ્યુટર સિસ્ટમનું રિમોટ કંટ્રોલ સક્ષમ કરે છે:

પાસું	વિગત
ફ્લેશનાલિટી	ફાઇલ એક્સેસ, સ્કીન જોવા, અને કીલોગિંગ સહિત લક્ષ્ય સિસ્ટમ પર સંપૂર્ણ નિયંત્રણ પ્રદાન કરે છે
ડેટાથોર્મેન્ટ	દાખીવાર ફિલિંગ, લેઝિટિમ સોફ્ટવેર સાથે બંદલ, અથવા કમજોરીઓના ફાયદા દ્વારા ઇન્સ્ટોલ થાય છે
આર્કિટેક્ચર	કલાયન્ટ-સર્વર મોડેલ જ્યાં સર્વર પીડિટના મણીન પર થાલે છે અને કલાયન્ટ હુમલાખોર દ્વારા નિયંત્રિત છે
કાયદેસર ઉપયોગો	IT સપોર્ટ, રિમોટ વર્ક, અને સિસ્ટમ એડમિનિસ્ટ્રેશન
દુર્લાઘનાપૂર્ણ ઉપયોગો	અનધિકૃત નિરીક્ષણ, ડેટા ચોરી, અને તોડફોડ

### દાયાગ્રામ:

## RAT (Remote Access Trojan) Attack Architecture



### RAT Capabilities:

- Remote Desktop Control
- File Transfer
- Keylogger
- Screenshot Capture
- Camera/Microphone Access
- System Information Gathering

### Attack Process:

1. Trojan delivered via email/download
2. RAT installs silently on victim's system
3. Establishes connection to attacker
4. Awaits commands from controller
5. Executes malicious activities
6. Sends stolen data back to attacker

### Common RATs:

- DarkComet • Poison Ivy • njRAT • Blackshades

### Prevention:

- Use updated antivirus software
- Enable firewall protection
- Avoid suspicious downloads
- Keep OS and software updated

**Warning:** RATs provide complete remote control to attackers

**Detection:** Monitor network traffic and system processes

મેમરી ટ્રીક: "RCASD: રિમોટ કંટ્રોલ એક્સેસ કેરા ચોરે"

## પ્રશ્ન 5(અ OR) [3 ગુણા]

સાયબર કાઇમના પડકારોની યાદી બનાવો.

### જવાબ:

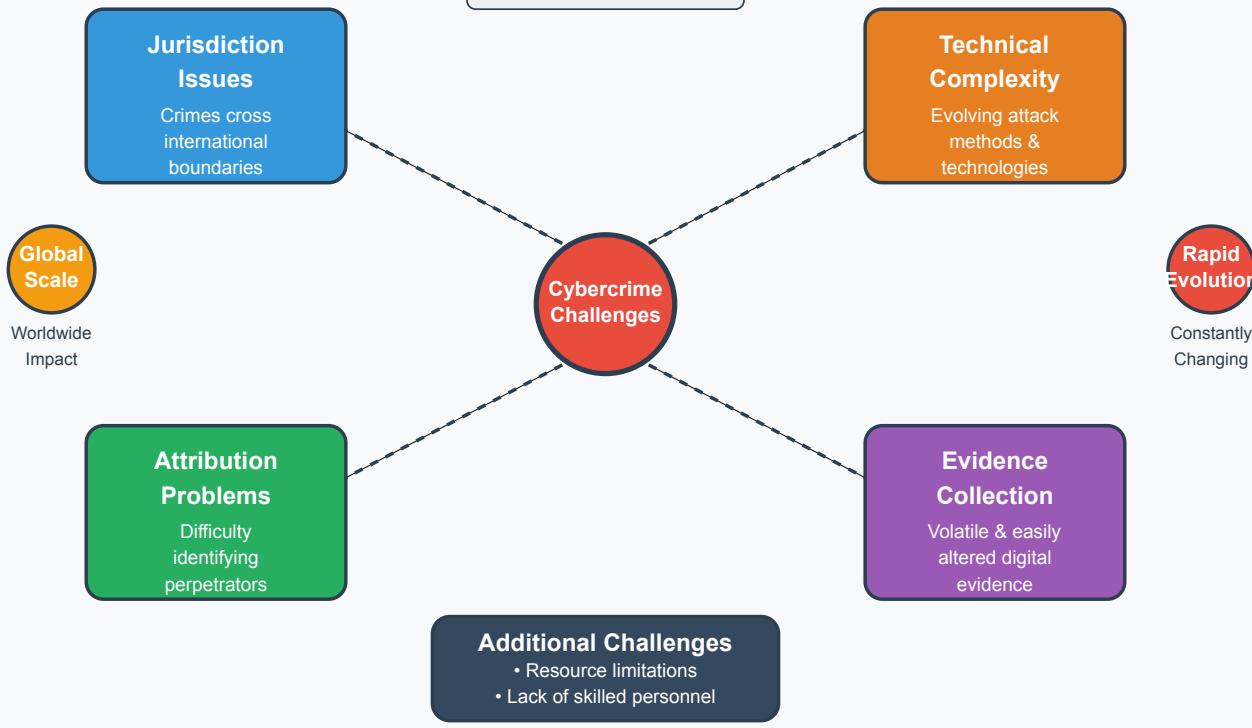
સાયબર કાઇમના સામનો કરવામાં મુખ્ય પડકારોમાં શામેલ છે:

- ન્યાયક્ષેત્ર સમસ્યાઓ: આંતરરાષ્ટ્રીય સીમાઓને અંગતા ગુના
- તકનીકી જટિલતા: સતત વિકસિત થતી હુમલાની પદ્ધતિઓ
- એટ્રિબ્યુશન સમસ્યાઓ: ગુનેગારોને અંગતામાં મુશ્કેલી
- પુરાવા એકત્રીકરણ: અસ્થિર અને સરળતાથી બદલી શકાય તેવા ડિજિટલ પુરાવા

### ડાયાગ્રામ:

## Challenges of Cybercrime

JTAE: Jurisdictions, Technology, Attribution, Evidence



મેમરી ટ્રીક: "JTAE: ન્યાયક્ષેત્ર, ટેકનોલોજી, એટ્રિબ્યુશન, એવિડન્સ"

## પ્રશ્ન 5(બં OR) [4 ગુણા]

મોબાઇલ ફોરેન્સિક્સ સમજાવો.

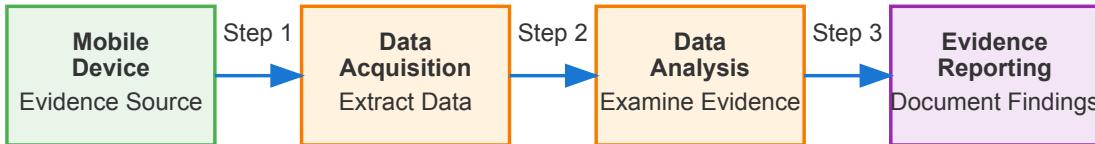
જવાબ:

Mobile forensics એ મોબાઇલ ડિવાઇસમાંથી ડિજિટલ પુરાવા પુનઃપ્રાપ્ત કરવાનું વિજ્ઞાન છે:

પાસું	વિગત
કેરા પ્રકારો	કોલ લોંગ્સ, મેસેજ્સ, લોકેશન કેરા, ફોટો, એપ કેરા
પડકારો	એન્ટ્રિક્ષનન, વિવિધ ઓપરેટિંગ સિસ્ટમ્સ, એન્ટી-ફોરેન્સિક તકનીકો
પદ્ધતિઓ	ફિઝિકલ એક્સટ્રેક્શન, લોજિકલ એક્સિસ્ટેશન, ફાઇલ સિસ્ટમ એનાલિસિસ
દૂસરું	Cellebrite UFED, Oxygen Forensic, Magnet AXIOM

ડાયાગ્રામ:

## Mobile Forensics Process



### Acquisition Methods:

- Physical Extraction
- Logical Acquisition
- File System Analysis
- Cloud Data Recovery

### Forensic Tools:

- Cellebrite UFED
- Oxygen Forensic
- Magnet AXIOM
- XRY Mobile

### Challenges:

- Encryption barriers
- OS diversity
- Anti-forensic techniques
- Data volatility

GEAR Process: Get Evidence, Analyze, Report

મેમરી ટ્રીક: "GEAR: ગોટ એવિડન્સ, એનાલાઇઝ, રિપોર્ટ"

## પ્રશ્ન 5(S OR) [7 ગુણ]

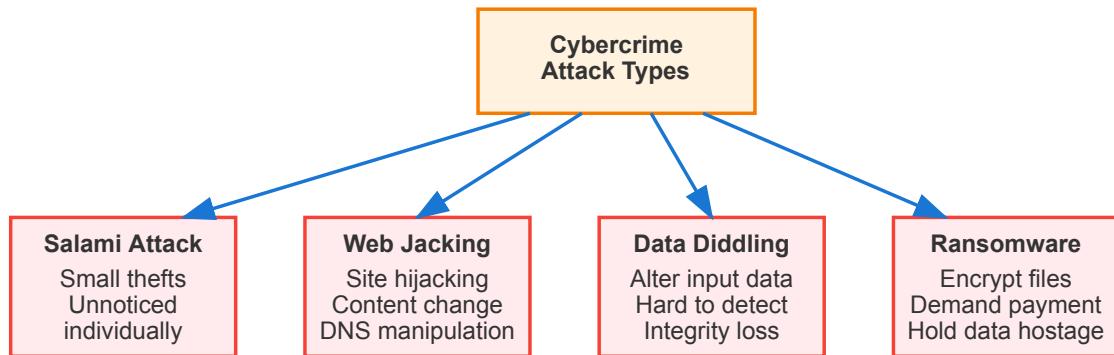
સલામી એટેક, વેબ જોકિંગ, ડેટા ડિડલિંગ અને રેન્સમ્બેર એટેક સમજાવો.

જવાબ:

કુમલાનો પ્રકાર	વિગત
Salami Attack	નાના થોરીના કાર્યોની શ્રેણી જે વ્યક્તિગત રીતે અણાંદેખી રહે છે. ઘણીવાર નાની રકમ લઈને નાણાકીય વ્યવહારોમાં ફેરફાર કરવાનો સમાવેશ થાય છે. સમય જતાં સંચિત અસર નોંધપાત્ર હોઈ શકે છે. ઉદાહરણ: બેંક વ્યવહારોને રાઉન્ડિંગ કરીને અપૂર્ણાંકો એકત્રિત કરવા.
Web Jacking	તેની સામગ્રી બદલીને અથવા નકલી સાઇટ પર રીડાયરેક્ટ કરીને વેબસાઇટને હાઇજેક કરવી. ડોમેન થેફ્ટ અથવા DNS મેનિષ્યુલેશન સામેલ છે. મેલવેર વિતરણ અથવા સંવેદનશીલ માહિતી એકત્રિત કરવા માટે વપરાય છે.
Data Diddling	સિસ્ટમમાં ઇનપુટ પહેલા/દરમિયાન ડેટામાં અનધિકૃત ફેરફાર. ફેરફારો સામાન્ય રીતે નાના અને શોધવા મુશ્કેલ હોય છે. ડેટા ઇન્ટેગ્રિટીને અસર કરે છે અને ખોટા બિઝનેસ નિર્ણયો તરફ દોરી શકે છે.
Ransomware	મેલવેર જે પીડિટની ફાઇલોને એન્ક્રિપ્ટ કરે છે અને ડિક્રિપ્શન માટે ચુકવણીની મંગ કરે છે. સામાન્ય રીતે ફિશિંગ અથવા કમજોરીઅંગોના ફાયદા દ્વારા ફેલાય છે. નોંધપાત્ર ઉદાહરણોમાં WannaCry અને Ryuk શામેલ છે.

ડાયાગ્રામ:

## Cybercrime Attack Types



### Examples:

- Salami: Bank transaction rounding
- Web Jacking: Domain hijacking
- Data Diddling: Payroll modification
- Ransomware: WannaCry, Ryuk

### Impact:

- Financial losses
- Data integrity compromise
- Business disruption
- Reputation damage

**Prevention:** Regular audits, access controls, backup systems

**Detection:** Monitoring, anomaly detection, integrity checks

**મેમરી ટ્રીક:** "SWDR: સલામી નાના નાના ટુકડા લે, વેબસાઇટ હાઇજેક થાય, ડેટા બદલાય, રેન્સમ માંગો"