|  |  |  |
| --- | --- | --- |
|  |  | Countermeasures – actions to detect/prevent threats. |
|  |  | Confidentiality – ensures info is not disclosed. |
|  |  | Rootkit – allows privileged access covertly. |
|  |  | Shoulder Surfing – viewing someone’s screen/keyboard. |
|  |  | Sarbanes-Oxley 2002 – requires accountability in financial reporting. |
|  |  | Comprehensive Security – multiple countermeasures. |
|  |  | External IT – threat from external actor. |
|  |  | Weakest link – security is only as strong as the weakest part. |
|  |  | Risk Transference – shifting risk, like via insurance. |
|  |  | Exposure Factor – % of asset loss if risk occurs. |
|  |  | Token – device used for identity verification. |
|  |  | Brute Force Attack – tries all key combos. |
|  |  | Asymmetric Cryptography – uses public/private key pair. |
|  |  | Subnet – network segmentation. |
|  |  | Validating the handshake – ensures data integrity in connections. |
|  |  | Ping Flood – DoS attack with ICMP Echo Requests. |
|  |  | Castle Model – assumes threats are outside the network. |
|  |  | Zero Trust Model – verifies all access requests. |
|  |  | Backscatter – indirect traffic in DoS attacks. |
|  |  | Spoofing – impersonating another system/user. |
|  |  | IP Address – logical device identifier. |
|  |  | arp -v – ARP command with verbose output. |
|  |  | RBAC – role-based access control. |
|  |  | Smart Card – hardware with embedded chip. |
|  |  | Blacklist – known bad items. |
|  |  | Hotfix – quick patch for vulnerabilities. |
|  |  | Root – default superuser on Unix/Linux. |
|  |  | False Positive – good file wrongly flagged as malware. |
|  |  | Buffer Overflow – exceeding memory buffer. |
|  |  | Recursive Function – can lead to stack overflow. |

|  |  |  |
| --- | --- | --- |
|  | Compromises | When a threat succeeds. |
|  | Detective | Detects the threat during/after attack. |
|  | Downloader | Malware initiator. |
|  | Phishing | Trick victim into granting access. |
|  | FISMA | Federal IT law. |
|  | Defense in depth | Multi-layer protection. |
|  | Hybrid Model | Mix of on-site and cloud/outsourced. |
|  | Redundancy | Multiple countermeasures. |
|  | Risk Reduction | Reducing threat impact. |
|  | Exposure Factor | % of asset lost in attack. |
|  | Ciphertext | Encrypted data. |
|  | Brute Force Attack | Tries all key possibilities. |
|  | Asymmetric cryptography | Public/private key pair. |
|  | IPS | Actively blocks threats. |
|  | Rate Limiting | Prevents overload. |
|  | Ping Flood | ICMP-based denial attack. |
|  | Castle Model | Layered defense concept. |
|  | Spoofing | Fake identity/packets. |
|  | Black Holding | Drops spoofed traffic. |
|  | IP Address | Device’s network address. |
|  | arp -a | Displays ARP cache. |
|  | Access Control List (ACL) | Entity-based permissions. |
|  | Role-Based Access Control (RBAC) | Based on user roles. |
|  | Magnetic Stripe | Data on card strip. |
|  | Biometric Template | Stored feature set. |
|  | Service Pack | Collection of updates. |
|  | Workaround | Temporary fix. |
|  | False Positive | Flagging safe files as threats. |
|  | Buffer Overflow | Too much data in memory. |
|  | Memory Allocation | Where overflow can occur. |