Corso Sicurezza Informatica e Security Manager | Certificato CompTIA Security+

SY-701

CORSO SICUREZZA INFORMATICA E SECURITY MANAGER | CERTIFICATO COMPTIA SECURITY+ SY-701

1) MASTERING SECURITY BASIC

1. Understanding core security goals

    1.1. Security scenarios

        1.1.1.Ensure confidentiality

        1.1.2.Provide integrity

        1.1.3.Increase availability

    1.2. Resource availability versus security constraints

2. Introducing basic risk concepts

3. Selecting effective security controls

    3.1. Control categories

        3.1.1.Technical controls

        3.1.2.Managerial controls

        3.1.3.Operational controls

        3.1.4.Physical controls

    3.2. Control types

        3.2.1.Preventive controls

        3.2.2.Deterrent controls

        3.2.3.Detective controls

        3.2.4.Corrective controls

        3.2.5.Directive controls

    3.3. Combining control categories and types

4. Logging and monitoring

    4.1. Operating system/endpoint logs

        4.1.1.Windows logs

        4.1.2.Linux logs

    4.2. Network logs

        4.2.1.Firewall logs

        4.2.2.IDS/IPS logs

        4.2.3.Packet captures

    4.3. Application logs

        4.3.1.Metadata

4.4. Centralized logging and monitoring

4.4.1.SIEM system

4.4.2.Syslog

Objective covered:

1.1 Compare and contrast various types of security controls

- Categories (technical, managerial, operational, physical)
- Control types (preventive, deterrent, detective, corrective, compensating, directive)

1.2 Summarize fundamental security concepts

- Confidentiality, integrity, and availability (CIA)

2.5 Explain the purpose of mitigation techniques used to secure the enterprise

- Monitoring
- Least privilege

3.2 Given a scenario, apply security principles to secure enterprise infrastructure

- Selection of effective controls

4.1 Given a scenario, apply common security techniques to computing resources

- Monitoring

4.4 Explain security alerting and monitoring concepts and tools

- Monitoring computing resources (systems, applications, infrastructure)
- Activities (log aggregation, alerting, scanning, reporting, archiving)
- Alert tuning
- Security Information and Event Management (SIEM)

4.5 Given a scenario, modify enterprise capabilities to enhance security

- User Behavior Analytics (UBA)

4.9 Given a scenario, use data sources to support an investigation

- Log data(firewall logs, application logs, endpoint logs, os-specific security logs, IPS/IDS logs, network logs, metadata)
- Data sources (automated reports, dashboards, packet captures)

2) UNDERSTANDING IDENTITY AND ACCESS MANAGEMENT

1. Exploring authentication management

1.1. Comparing identification and AAA

1.2. Comparing authentication factors

5. Analyzing authentication indicators

Objective covered:

1.2 Summarize fundamental security concepts

- Authentication, authorization, and accounting (AAA) (Authenticating people, Authenticating systems, Authorization models)

2.4 Given a scenario, analyze indicators of malicious activity

- Indicators (account lockout, concurrent session usage, blocked content, impossible travel, resource consumption, resource inaccessibility, out-of-cycle logging, published/documented, missing logs)

2.5 Explain the purpose of mitigation techniques used to secure the enterprise

- Access control (Access Control List (ACL), permissions)

4.5 Given a scenario, modify enterprise capabilities to enhance security

- Operating system security (SElinux)

4.6 Given a scenario, implement and maintain identity and access management

- Provisioning/de-provisioning user accounts
- Permission assignments and implications
- Identity proofing
- Federation
- Single sign-on (SSO) (open authorization (OAuth) , Security Assertions Markup Language, (SAML))
- Interoperability
- Attestation
- Access controls (mandatory, discretionary, role-based, rule-based, attribute-based, time-of-day restrictions, least privilege)
- Multifactor authentication (implementations, biometrics, hard/soft authentication tokens, security keys)
- Factors (something you know, something you have, something you are, somewhere you are)
- Password concepts
- Password best practices (length, complexity, reuse, expiration, age)
- Password managers
- Passwordless

- Privileged access management tools (just-in-time permissions, password vaulting, ephemeral credentials)

3) EXPLORING NETWORK TECHNOLOGIES AND TOOLS

1. Reviewing basic networking concepts
   - 1.1. OSI model
   - 1.2. Basic networking protocols
   - 1.3. Implementing protocols for use cases
     - 1.3.1.Data in transit use cases
     - 1.3.2.Email and web use cases
     - 1.3.3.Directory use cases
     - 1.3.4.Voice and video use cases
     - 1.3.5.Remote access use cases
     - 1.3.6.Time synchronization use cases
     - 1.3.7.Network address allocation use cases
     - 1.3.8.Domain name resolution use cases
2. Understanding basic network infrastructure
   - 2.1. Switches
     - 2.1.1.Hardening switches
   - 2.2. Routers
     - 2.2.1.Hardening routers
   - 2.3. Simple Network Management Protocol
   - 2.4. Firewalls
     - 2.4.1.Host-based firewalls
     - 2.4.2.Network-based firewalls
   - 2.5. Failure modes
3. Implementing network designs
   - 3.1. Security zones
     - 3.1.1.Screened subnet
     - 3.1.2.Network address translation gateway
     - 3.1.3.Physical isolation and air gasp
     - 3.1.4.Logical separation and segmentation
   - 3.2. Network appliances
   - 3.3. Proxy servers

        3.3.1.Caching content for performance

        3.3.2.Content filtering

        3.3.3.Reverse proxy

    3.4. Unified threat management

    3.5. Jump server

4. Zero trust

    4.1. Control plane vs. Data plane

    4.2. Secure access service edge

Objective covered:

1.2 Summarize fundamental security concepts

- Zero trust (control plane: adaptive identity, threat scope reduction, policy-driven access control, policy administrator, policy engine; data plane: implicit trust zones, subject/system, policy enforcement point)

2.5 Explain the purpose of mitigation techniques used to secure the enterprise

- Isolation
- Hardening techniques (host-based firewall)

3.1 Compare and contrast security implications of different architecture model

- Network infrastructure (physical isolation, air-gapped, logical segmentation)

3.2 Given a scenario, apply security principles to secure enterprise infrastructure

- Device placement
- Security zones
- Attack surface
- Connectivity
- Failure modes (fall-open, fall-closed)
- Network appliances (jump server, proxy server, load balancer)
- Firewall types (web application firewall (WAF), unified threat management (UTM), next-generation firewall (NGFW), layer 4/layer 7)
- Secure communication/access (Tunneling Transport Layer Security (TLS), Secure Access Service Edge (SASE))

3.3 Compare and contrast concepts and strategies to protect data

- Methods to secure data (segmentation)

4.1 Given a scenario, apply common security techniques to computing resources.

- Hardening targets (switches, routers)

4.4 Explain security alerting and monitoring concepts and tools

- Simple Network Management Protocol (SNMP) traps

4.5 given a scenario, modify enterprise capabilities to enhance security

- Firewall (rules, access lists, ports/protocols, screened subnets)
- Web filter (agent based, centralized proxy, universal resource locator scanning, content categorization, block rules, repuration)
- Operating system security (group policy chapter)
- Implementation of secure protocols (protocol selection, port selection, transport met-hod)
- Email security (domain-based message authentication reporting and conformance (dmarc), Domain Keys Identified Mail (dkim), Sender Policy Framework (SPF), gateway)

4) SECURING YOUR NETWORK

1. Exploring advanced security devices

 1.1. Understanding idss and ipss

  1.1.1.HIDS

  1.1.2.NIDS

  1.1.3.Sensor and collector placement

  1.1.4.Detection methods

  1.1.5.Data sources and trends

  1.1.6.Reporting based on rules

  1.1.7.Alert response and validation

 1.2. IPS versus IDS in line versus passive

 1.3. Honeypots

 1.4. Honeynets

 1.5. Honeyfile

 1.6. Honeytokens

2. Securing wireless networks

 2.1. Reviewing wireless basics

  2.1.1.Band selection and channel overlaps

  2.1.2.MAC filtering

 2.2. Site surveys and heat maps

 2.3. Access point installation considerations

 2.4. Wireless cryptographic protocols

2.4.1.WAP2 and CCMP

2.4.2.Open, psk, and enterprise modes

2.4.3.WPA3 and simultaneous authentication of equals

2.5. Authentication protocols

2.6. IEEE 802.1x security

2.7. Controller and access point security

2.8. Captive portals

3. Understanding wireless attacks

3.1. Disassociation attacks

3.2. Wi-fi protected setup

3.3. Rogue access point

3.4. Evil twin

3.5. Jamming attacks

3.6. IV attacks

3.7. Near field communication attacks

3.8. RFID attacks

3.8.1.Wireless replay attacks

3.8.2.War driving and war flying

4. Using VPNs for remote access

4.1. VPNs and VPN concentrators

4.2. Remote access VPN

4.3. IPSEC as a tunneling protocol

4.4. SSL/TLS as a tunneling protocol

4.5. Split tunnel versus full tunnel

4.6. Site-to-site VPNs

4.7. Always-on SPN

4.8. L2TP as a tunneling protocol

4.9. HTML5 VPN portal

5. Network access control

5.1. Host health checks

5.2. Agent versus agentless NAC

6. Authentication and authorization methods

6.1. PAP

6.2. CHAP

6.3. RADIUS

6.4. TACACS+

6.5. AAA protocols

Objective covered:

1.2 Summarize fundamental security concepts

- Deception and disruption technology (honeypot, honeynet, honeyfile, honeytoken)

2.3 Explain various types of vulnerabilities

- Zero-day

2.4 Given a scenario, analyze indicators of malicious activity

- Physical attacks (radio frequency identification (RFID) cloning)
- Network attacks (wireless)

3.2 Given a scenario, apply security principles to secure enterprise infrastructure

- Device attribute (active vs. Passive, inline vs. Tap/monitor)
- Intrusion prevention system (IPD)/ intrusion detection system (IDS)
- Sensors
- Port security (802.1 x , extensible authentication protocol (EAP))
- Secure communication/access (virtual private network (VPN), remote access chapter, Tunneling (IPSEC)

4.0 given a scenario, apply common security techniques to computing resources

- Wireless device (installation consideration: site surveys, heat maps)
- Wireless security settings (WI-FI protected access 3 (WPA3), AAA/remote authentication dial-in user service (RADIUS), cryptographic protocols, authentication protocols)

4.4 Explain security alerting and monitoring concepts and tools

- Agent / agentless
- Alerting response and remediation / validation (quarantine)

4.5 Given a scenario, modify enterprise capabilities to enhance security

- IDS/IPS (trends, signature)
- Network Access Control (NAC)

5) SECURING HOSTS AND DATA

1. Virtualization

1.1. Thin clients and virtual desktop infrastructure

1.2. Containerization

1.3. VM escape protection

1.4. VM sprawl avoidance

1.5. Resource reuse

1.6. Replication

1.7. Snapshots

2. Implementing secure system

2.1. Endpoint security software

2.2. Hardening workstations and servers

2.3. Configuration enforcement

2.4. Secure baseline and integrity measurements

2.5. Using master images for baseline configurations

2.6. Patching and patch management

2.7. Change management

2.8. Application allow and block lists

2.9. Disk encryption

2.10. Boot integrity

2.10.1. Boot security and uefi

2.10.2. Trusted platform module

2.10.3. Hardware security module

2.11. Decommissioning and disposal

3. Protecting data

3.1. Data loss prevention

3.2. Removable media

3.3. Protecting confidentiality with encryption

3.4. Database security

3.5. Protecting data in use

4. Summarizing cloud concepts

4.1. Cloud delivery models

4.1.1.Software as a service

4.1.2.Platform as a service

4.1.3.Infrastructure as a service

4.2. Cloud deployment models

- 4.2.1.Multi-cloud systems
- 4.3. Application programming interfaces
- 4.4. Microservices and apis
- 4.5. Managed security service provider
- 4.6. Cloud service provider responsabilities
- 4.7. Cloud security considerations
- 4.8. On-premises versus off-premises
  - 4.8.1.On-premises
  - 4.8.2.Off-premises
- 4.9. Hardening cloud enviroments
  - 4.9.1.Clooud access security broker
  - 4.9.2.Cloud-based dlp
  - 4.9.3.Next-generation secure web gateway
  - 4.9.4.Cloud firewall considerations
  - 4.9.5.Infrastructure as code
  - 4.9.6.Software-defined networking
  - 4.9.7.Edge and fog computing
- 4.10. Deploying mobile devices securely
  - 4.10.1. Mobile device deployment models
  - 4.10.2. Connection methods and receivers
    - 4.10.2.1. Mobile device management
  - 4.10.3. Hardening mobile devices
    - 4.10.3.1. Unauthorized software
    - 4.10.3.2. Hardware control
    - 4.10.3.3. Unauthorized connections
- 4.11. Exploring embedded systems
  - 4.11.1. Understanding internet of things
  - 4.11.2. Ics and scada systems
  - 4.11.3. Embedded systems components
  - 4.11.4. Hardening specialized systems
  - 4.11.5. Embedded system constraints

Objective covered:

1.3 **Explain** the importance of using appropriate cryptographic solutions

- Encryption (level: full-disk, partition, file, volume, database, record)
- TPM (trusted platform module)
- HSM (hardware security module)
- Key Management System
- Secure enclave

2.3 Explain various types of vulnerabilities

- Operating systems (os)-based
- Hardware (firmware, end-of-life, legacy)
- Virtualization (Virtual Machine (VM) escape, resource reuse)
- Cloud-specific
- Misconfiguration
- Mobile device (side loading, jailbreaking)

2.5 Explain the purpose of mitigation techniques used to secure the enterprise

- Segmentation
- Application allow list
- Patching
- Encryption
- Configuration enforcement
- Decommissioning
- Hardening techniques (encryption, installation of endpoint protection, host-based intrusion prevention system (hips), disabling ports/protocols, default password, removal of unnecessary software)

3.1 Compare and contrast security implications of different architecture models

- Cloud (responsibility matrix, hybrid considerations, third-party vendors)
- Infrastructure As Code (IAC)
- Serverless
- Microservices
- Network infrastructure (Software-Defined Networking (SDN))
- On-premises
- Centralized vs. Decentralized
- Containerization
- Virtualization

- IoT (Internet of things)
- Industrial Control Systems (ICS) / Supervisory Control And Data Acquisition (SCADA)
- Real-Time Operating System (RTOS)
- Embedded systems
- Considerations (availability, resilience, cost, responsiveness, scalability, ease of deployment, risk transference, ease of recovery, patch availability, inability to patch, power, compute

3.3 Compare and contrast concepts and strategies to protect data

- Geolocation

4.1 Given a scenario, apply common security techniques to computing resources

- Secure baselines (establish, deploy, maintain)
- Hardening targets (mobile devices, workstation, cloud infrastructure, servers, ICS/SCADA, embedded systems, RTOS, IoT)
- Mobile solutions (Mobile Device Management (MDM); deployment models: Bring Your Own Device (BYOD), Corporate Owned, Personally Enabled (COPE), Choose Your Own Device (CYOD); connection methods: cellular, wi-fi, bluetooth)

4.4 Explain security alerting and monitoring concept and tools

- Antivirus
- DLP (Data Loss Prevention)

4.5 Given a scenario, modify enteprise capabilities to enhance security

- DLP
- Endpoint Detection and Response (EDR)
- eXtended Detection and Response (XDR)

6) COMPARING THREATS, VULNERABILITIES AND COMMON ATTACKS

1. Understanding threat actors
   1.1. Threat actor types
   1.2. Attacker attributes
   1.3. Threat actor motivations
   1.4. Threat vectors and attack surfaces
   1.5. Shadow it
2. Determining malware types
   2.1. Viruses
   2.2. Worms

2.3. Logic bombs

2.4. Trojans

2.5. Remote access trojan

2.6. Keyloggers

2.7. Spyware

2.8. Rootkit

2.9. Ransomware

2.10. Bloatware

2.11. Potential indicators of a malware attack

3. Recognizing common attacks

3.1. Social engineering and human vectors

3.1.1.Impersonation

3.1.2.Shoulder surfing

3.1.3.Disinformation

3.1.4.Tailgating and access control vestibules

3.1.5.Dumpster diving

3.1.6.Watering hole attacks

3.1.7.Business email compromise

3.1.8.Typosquatting

3.1.9.Brand impersonation

3.1.10. Eliciting information

3.1.11. Pretexting

3.2. Message-based attacks

3.2.1.Spam

3.2.2.Spam over instant messaging

3.2.3.Phishing

3.2.4.Whaling

3.2.5.Vishing

3.2.6.Smishing

3.3. One click lets them in

4. Blocking malware and other attacks

4.1. Spam filters

4.2. Antivirus and anti-malware software

4.2.1.Signature-based detection

4.2.2.Heuristic-based detection

4.2.3.File integrity monitors

4.3. Why social engineering works

4.3.1.Authority

4.3.2.Intimidation

4.3.3.Consensus

4.3.4.Scarcity

4.3.5.Urgency

4.3.6.Familiarity

4.3.7.Trust

4.4. Threat intelligence sources

4.5. Research sources

Objective covered:

2.0 Compare and contrast common threat actors and motivations

- Threat actors (nation-state, unskilled attacker, hacktivist, insider threat, organized crime, shadow it)
- Attributes of actors (internal/external, resources/funding, level of sophistication/capability)
- Motivations (data exfiltration, espionage, service disruption, blackmail, financial gain, philosophical/political beliefs, ethical revenge, disruption/chaos, war)

2.2 Explain common threat vectors and attack surfaces

- Message-based (email, short message service (SMS), instant messaging (IM))
- Image-based
- File-based
- Voice call
- Removable device
- Vulnerable software (client-based vs. Agentless)
- Unsupported systems and applications
- Unsecure networks (wireless, wired, bluetooth)
- Open service ports
- Default credentials
- Supply chain (Managed Service Providers (MSP), vendors, suppliers)

- Human vectors/social engineering (phishing, vishing, smishing, misinformation/disinformation, impersonation, business email compromise, pretexting: watering hole, brand impersonation, typosquatting)

2.4 Given a scenario, analyze indicators of malicious activity

- Malware attacks (ransomware, trojan, worm, spyware, bloatware, virus, keylogger, logic bomb, rootkit)
- Malicious code

4.2 Explain various activities associated with vulnerability management

- Threat feed (Open Source INTelligence OSINT, proprietary/third-party, information-sharing organization, dark web)

4.5 Given a scenario, modify enterprise capabilities to enhance security

- File integrity monitoring

7) PROTECTING AGAINST ADVANCED ATTACKS

1. Identifying network attacks
   1.1. Denial of Service attacks
      1.1.1.Syn flood attacks
   1.2. Forgery
   1.3. On-path attacks
   1.4. Secure Sockets Layer stripping
   1.5. DNS attacks
      1.5.1.DNS poisoning attacks
      1.5.2.Pharming attacks
      1.5.3.Url redirection
      1.5.4.Domain hijacking
      1.5.5.DNS filtering
      1.5.6.DNS log files
   1.6. Replay attacks
2. Summarizing secure coding concepts
   2.1. Input validation
      2.1.1.Client-side and server-side input validation
      2.1.2.Other input validation techniques

2.2. Avoiding race conditions

2.3. Proper error handling

2.4. Code obfuscation

2.5. Software diversity

2.5.1. Outsourced code development

2.5.2. Data exposure

2.5.3. HTTP headers

2.5.4. Secure cookie

2.5.5. Code signing

2.6. Analyzing and reviewing code

2.7. Software version control

2.8. Secure development enviroment

2.9. Database concepts

2.9.1. SQL queries

2.10. Web server logs

3. Other application attacks

3.1. Memory vulnerabilities

3.1.1. Memory leak

3.1.2. Buffer overflows and buffer attacks

3.1.3. Integer overflow

3.2. Other injection attacks

3.2.1. DLL injection

3.2.2. LDAP injection

3.2.3. XML injection

3.3. Directory traversal

3.4. Cross-site scripting

4. Automation and orchestration for secure operations

4.1. Automation and scripting use cases

4.2. Benefits of autmations and scripting

Objective covered:

2.3 Explain various types of vulnerabilities

- Application (memory injection, buffer overflow, race conditions: Time-Of-Check (TOC), Time-Of-Use(TOU))
- Malicious update
- Web based (SQL injection, XSS)

2.4 Given a scenario, analyze indicators of malicious activity

- Network attack (distributed denial of service (DDoS): amplified, reflected; domain name system attack; on-path; credential replay)
- Application attack (injection, buffer overflow, replay, forgery, directory traversal)

4.1 Given a scenario, apply common security techniques to computing resources

- Application security (input validation, secure cookies, static code analysis, code signing)
- Sandboxing

4.7 Explain the importance of automation and orchestration related to secure operations

- Use cases of automation and scripting (user provisioning, resource provisioning, guard rails, security groups, ticket creation, escalation, enabling/disabling services and access, continuous integration and testing, integrations and application programming interfaces (API s))
- Benefits (efficiency/time saving, enforcing baselines, standard infrastructure configurations, scaling in a secure manner, employee retention, reaction time, workforce multiplier)
- Other considerations (complexity, cost, single point of failure, technical debt, ongoing supportability)

8) USING RISK MANAGEMENT TOOLS

1. Understanding risk management
   1.1. Threats
   1.2. Risk identification
   1.3. Risk types
   1.4. Vulnerabilities
   1.5. Risk managemnt strategies
      1.5.1.Risk assessment types
      1.5.2.Risk analysis
      1.5.3.Supply
      1.5.4.Chain risks
2. Comparing scanning and testing tools
   2.1. Checking for vulnerabilities

2.1.1.Network scanners

2.1.2.Vulnerability scanning

2.1.3.Credentialed vs. Non-credentialed scans

2.1.4.Configuration review

2.2. Penetration testing

2.2.1.Rules of engagement

2.2.2.Reconnaissance

2.2.3.Footprinting versus fingerprinting

2.2.4.Initial exploitation

2.2.5.Persistence

2.2.6.Lateral movement

2.2.7.Privilege escalation

2.2.8.Pivoting

2.2.9.Known, unknown and partially known testing enviroments

2.2.10. Cleanup

2.3. Responsible disclosure programs

2.4. System and process audits

2.5. Intrusive versus non-intrusive testing

2.6. Responding to vulnerabilities

2.6.1.Remediating vulnerabilities

2.6.2.Validation of remediation

3. Capturing network traffic

3.1.1.Packet capture and replay

3.2. TCPreplay and TCPdump

3.3. Netflow

4. Understanding frameworks and standards

4.1. ISO standards

4.2. Industry-specific frameworks

4.3. NIST frameworks

4.3.1.NIST risk management framework

4.3.2.NIST cybersecurity framework

4.4. Reference architecture

4.5. Benchmarks and configuration guides

5. Audits and assessments

Objective covered:

1.2 Summarize fundamental security concepts

- Gap analysis

2.3 Explain various type of vulnerabilities

- Supply chain (service provider, hardware provider, software provider)

4.3 Eplain various activities associated with vulnerability management

- Vulnerability scan
- Penetration testing
- Responsible disclosure program
- Bug bounty program
- System/process audit
- Analysis (confirmation, false positive, false negative, prioritize, Common Vulnerability Scoring System (CVSS), Common Vulnerability Enumeration (CVE), vulnerability classification, Exposure Factor, environmental variables, industry/organizational impact, risk tolerance)
- Vulnerability response and remediation (patching, insurance, segmentation, compensating controls, exceptions and exemptions)
- Validation of remediation (rescanning, audit, verification)
- Reporting

4.4 Explain security alerting and monitoring concepts and tools

- Security Content Automation Protocol (SCAP)
- Benchmarks
- Netflow
- Vulnerability scanners

5.2 Explain elements of the risk management process

- Risk identification
- Risk assessment (ad hoc, recurring, one-time, continuous)
- Risk analysis (qualitative; quantitative; Single Loss Expectancy (SLE); Annualized Loss Expectancy (ALE); Annualized Rate of Occurrence (ARO); probability; likelihood; Exposure Factor; impact; risk register: key risk indicators, risk owners, risk threshold; risk tolerance; risk appetite: expansionary, conservative, neutral; risk management strategies: transfer, accept exemption, accept exception, avoid, mitigate)
- Risk reporting

5.5 Explain types and purposes of audits and assessments

- Attestation
- Internal (compliance, audit committee, self-assessments)
- External (regulatory, examinations, assessment, independent third-party audit)
- Penetration testing (physical, offensive, defensive, integrated, known environment, partially known environment, unknown environment)
- Reconnaissance (passive, active)

9) IMPLEMENTING CONTROLS TO PROTECT ASSETS

1. Comparing physical security controls

1.1. Access badges

1.2. Increasing security with personnel

1.3. Monitoring areas with video surveillance

1.4. Sensors

1.5. Fencing, lighting and alarms

1.6. Securing access with barricades

1.7. Access control vestibules

1.8. Asset management

1.8.1.Hardware asset management

1.8.2.Software asset management

1.8.3.Data asset management

1.9. Platform diversity

1.10. Physical attacks

1.10.1. Card skimming and card cloning

1.10.2. Brute force attacks

1.10.3. Enviromental attacks

2. Adding redundancy and fault tolerance

2.1. Single Point of Failure

2.2. Disk redundancies

2.2.1.Raid-0

2.2.2.Raid-1

2.2.3.Raid-5 and raid-6

2.2.4.Raid-10

2.3. Server redundancy and high availability

2.3.1.Active/ active load balancers

2.3.2.Active/ passive load balancers

2.4. NIC teaming

2.5. Power redundancies

3. Protecting data with backups

3.1. Backup media

3.2. Online versus offline backups

3.2.1.Full backups

3.2.2.Recovering a full backup

3.2.3.Differential backups

3.2.4.Order of recovery for a full/differential backup set

3.2.5.Incremental backups

3.2.6.Order of recovery for a full/differential backup set

3.2.7.Snapshot and image backups

3.2.8.Replication and journaling

3.2.9.Backup frequency

3.2.10. Testing backups

3.3. Backup and geographic considerations

4. Comparing business continuity elemnts

4.1. Business impact analysis concepts

4.1.1.Site risk assessment

4.1.2.Impact

4.1.3.Recovery Time Objective

4.1.4.Recovery Point Objective

4.1.5.Comparing MTBF and MTTR

4.2. Continuity of operations planning

4.2.1.Site resiliency

4.2.2.Restoration order

4.3. Disaster recovery

4.4. Testing plans with exercises

4.4.1.Tabletop exercises

4.4.2.Simulations

4.4.3.Parallel processing

4.4.4.Fail over tests

5. Capacity planning

Objective covered:

1.2 Summarize fundamental security concepts

- Physical security (bollards, access control vestibule, fencing, video surveillance, security guard, access badge, lighting, sensors: infrared, pressure , microwave, ultrasonic)
- Physical attack (brute force, environmental)

3.3 Compare and contrast concepts and strategies to protect data

- General data considerations (data sovereignty)

3.4 Explain the importance of resilience and recovery in security architecture

- High availability (load balancing vs. clustering)
- Site considerations (hot, cold, warm, geographic dispersion)
- Platform diversity
- Continuity of operations
- Capacity planning (people, technology, infrastructure)
- Testing (tabletop exercises, fail over, simulation, parallel processing)
- Backups (onsite/offsite, frequency, encryption, snapshots, recovery, replication, journaling)
- Power (generators, uninterruptible power supply (ups))

4.2 Explain the security implications of proper hardware, software, and data asset management

- Acquisition/procurement
- Assignment/accounting (ownership, classification)
- Monitoring/asset trasking (inventory / enumeration)

5.2 Explain elements of the risk management process

- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
- Mean Time To Repair (MTTR)
- Mean Time Between Failures (MTBF)

10) UNDERSTANDING CRYPTOGRAPHY AND PKI

1. Introducing cryptography concepts
2. Providing integrity with hashing

   2.1. Hash versus checksum

2.2. MD5

2.3. Secure hash algorithms

2.4. Hmac

2.5. Hashing files

2.6. Hashing messages

2.7. Using hmac

2.8. Hashing passwords

2.9. Undertanding hash collisions

3. Understanding password attacks

3.1. Dictionary attacks

3.2. Brute force attacks

3.3. Password spraying attacks

3.3.1.Pass the hash attacks

3.4. Birthday attacks

3.5. Rainbow table attacks

3.6. Salting passwords

3.7. Key stretching

4. Providing confidentiality with encryption

4.1. Symmetric encryption

4.2. Block versus stream ciphers

4.3. Common symmetric algorithms

4.3.1.AES

4.3.2.3DES

4.3.3.Blowfish and twofish

4.4. Asymmetric encryption

4.4.1.Key exchange

4.4.2.The reyburn box

4.5. Certificates

4.6. Ephemeral keys

4.7. Elliptic curve cryptography

4.8. Key lenght

4.9. Obfuscation

4.9.1.Steganography

4.9.2.Tokenization

4.9.3.Masking

5. Using cryptographic protocols

5.1. Protecting email

5.1.1.Signing email with digital signatures

5.1.2.Encrypting email

5.1.3.S/mime

5.2. HTTPS transport encryption

5.2.1.TLS versus SSL

5.2.2.Encrypting HTTPS traffic with TLS

5.2.3.Downgrade attacks on weak implementations

5.3. Blockchain

5.4. Identifyng limitations

5.4.1.Resource versus security constraints

5.4.2.Speed and time

5.4.3.Size and computational overhead

5.4.4.Entropy

5.4.5.Predictability

5.4.6.Weak keys

5.4.7.Reuse

5.4.8.Plaintext attack

6. Exploring PKI components

6.1. Certificate authority

6.2. Certificate trust models

6.3. Registration authority and CSRs

6.4. Online versus offline CAs

6.5. Updating and revoking certificates

6.6. Certificate revocation list

6.7. Validating a certificate

6.8. Certificate pinning

6.9. Key escrow

6.10. Key management

6.11. Comparing certificate types

6.12. Comparing certificate formats

Objective covered:

1.2 Summarize fundamental security concepts

- Non-repudation

1.4 Explain the importance of using appropriate cryptography solutions

- Public key infrastructure (PKI) (public key, private key, key escrow)
- Encryption (transport/communication, asymmetric, symmetric, key exchange, algorithms, key length)
- Obfuscation (steganography, tokenization, data masking)
- Hashing
- Salting
- Digital signatures
- Key stretching
- Blockchain
- Open public ledger
- Certificates (Certificate Authorities, Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP), self-signed, third-party, root of trust, Certificate Signing Request (CSR) generation, wildcard)

2.3 Explain various types of vulnerabilities

- Cryptographic
- Cryptographic attacks (downgrade, collision, birthday)
- Password attacks (spraying, brute force)

3.3 Compare and contrast concepts and strategies to protect data

- General data considerations (data states: at rest, in transit, in use)
- Methods to secure data (encryption, hashing, masking, tokenization, obfuscation)

11) IMPLEMENTING POLICIES TO MITIGATE RISKS

1. Change management

   1.1. Business processes

   1.2. Technical implications

   1.3. Documentation and version control

2. Protecting data

2.1. Understanding data types

2.2. Classifying data types

2.3. Securing data

2.4. Data retention

2.5. Data sanitization

3. Incident response

3.1. Incident response plan

3.1.1.Communication plan

3.2. Incident response process

3.3. Incident response training and testing

3.4. Threat hunting

3.5. Understanding digital forensics

3.5.1.Acquisition and preservation

3.5.2.Legal holds and electronic discovery

3.5.3.Admissibility of documentation and evidence

3.5.4.Reporting

3.6. Understanding SOAR

3.6.1.Playbooks

3.6.2.Runbooks

4. Security governance

4.1. Governance structures

4.2. External considerations

4.3. Security policies

4.4. Security standards

4.5. Security procedures

4.6. Security guidelines

4.7. Data governance

4.8. Data roles

4.9. Monitoring and revision

5. Third-party risk management

5.1. Supply chain and vendors

5.2. Vendor assessment

5.3. Vendor selection

5.4. Vendor agreements

6. Security compliance
    6.1. Compliance monitoring and reporting
    6.2. Privacy
    6.3. Data inventory and retention
7. Security awareness
    7.1. Computer-based training
    7.2. Phishing campaigns
    7.3. Recognizing anomalous behavior
    7.4. User guidance and training
    7.5. Awareness program development and execution

Objective covered:

1.3 Explain the importance of change management processes and the impact to security

- Business processes impacting security operation (approval process, ownership, stakeholders, impact analysis, test results, backout plan, maintenance window, standard operating procedure)
- Technical implications (allow lists/deny lists, restricted activities, downtime, service restart, application restart, legacy applications, dependencies)
- Documentation (updating diagrams,updating policies / procedures)
- Version control

3.3 Compare and contrast concepts and strategies to protect data

- Data types (regulated, trade secret, intellectual property, legal information, financial information, human-and non-human-readable)
- Data classifications (sensitive, confidential, public, restricted, private, critical)

4.2 explain the security implications of proper hardware, software, and data asset management

- Disposal/decommissioning (sanitization, destruction, certification, data retention)

4.3 explain various activities associated with vulnerability management

- Application security (static analysis, dynamic analysis, package monitoring)

4.8 Explain appropriate incident response activities

- Process (preparation, detection, analysis, containment, eradication, recovery, lesson learned)
- Training

- Testing (tabletop exercise, simulation)
- Root cause analysis
- Threat hunting
- Digital forensics (legal hold, chain of custody, acquisition, reporting, preservation, e-discovery)

5.1 summarize elements of effective security governance

- Guidelines
- Policies (Acceptable Use Policy (AUP),information security policies ,business continuity , disaster recovery, incident response , Software Development Lifecycle (SDLC), change management)
- Standards (password, access control, physical security, encryption)
- Procedures (change management, onboarding/offboarding, playbooks)
- External considerations (regulatory, legal, industry, local/regional, national, global)
- Monitoring and revision
- Types of governance structures (boards, committees, government entities, centralized/decentralized)
- Roles and responsibilities for systems and data (owners, controllers, processors, custodians/stewards)

5.3 Explain the processes associated with third-party risk assessment and management

- Vendor assessment (penetration testing, right-to-audit clause, evidence of internal audits, independent assessments, supply chain analysis)
- Vendor selection (due diligence, conflict of interest)
- Agreement types (Service-Level Agreement (SLA), Memorandum Of Agreement (MOA), Memorandum Of Understanding (MOU), Master Service Agreement (MSA), Work Order (WO)/Statement Of Work (SOW), Non-Disclosure Agreement (NDA), Business Partners Agreement (BPA)
- Vendor monitoring
- Questionnaires
- Rules of engagement

5.4 Summarize elements of effective security compliance

- Compliance reporting (internal, external)
- Consequences of non-compliance (fines, sanctions, reputational damage, loss of license, contractual impacts)

- Compliance monitoring (due diligence/care, attestation and acknowledgement, internal and external, automation)
- Privacy (legal implications, local/regional, national, global)
- Data subject
- Controller vs. Processor
- Ownership
- Data inventory and retention
- Right to be forgotten

5.6 Given a scenario, implement security awareness practices

- Phishing (campaigns, recognizing a phishing attempt, responding to reported suspicious messages)
- Anomalous behavior recognition (risky, unexpected, unintentional)
- User guidance and training (policy/handbooks, situational awareness, insider threat, password management, removable media and cables, social engineering, operational security, hybrid/remote work environment)
- Reporting and monitoring (initial, recurring)

- Development and Execution