Programma Academy Basilicata

PRIMA PARTE – RETI E SISTEMI

1 HARDWARE E SISTEMI OPERATIVI

1.1 HARDWARE

Conoscere l'architettura dei sistemi di elaborazione moderni

1.1.1 ARCHITETTURA DEI SISTEMI DI ELABORAZIONE
1.1.2 CPU
1.1.3 BUS
1.1.4 PERIFERICHE
1.1.5 INTERRUZIONI
1.1.6 DMA
1.1.7 MEMORIE

1.2 SISTEMI OPERATIVI (MANDATORY)

Conoscere la struttura e il funzionamento dei Sistemi Operativi

1.2.1 GENERALITÀ
1.2.2 GESTIONE DEI PROCESSI
1.2.3 SINCRONIZZAZIONE DEI PROCESSI
1.2.4 GESTIONE DELLA MEMORIA
1.2.5 GESTIONE DELLA MEMORIA DI MASSA
1.2.6 FILE SYSTEM
1.2.7 TIPOLOGIE DI SISTEMI OPERATIVI
1.2.8 WINDOWS
1.2.9 LINUX

1.3 BASE DI DATI (MANDATORY)

Comprendere i concetti fondamentali delle basi di dati e i sistemi di gestione delle banche dati (DBMS)

1.3.1 ELEMENTI DI BASE DI DATI
1.3.2 SISTEMI DI GESTIONE DELLE BANCHE DATI (DBMS)
1.3.3 CENNI SUI LINGUAGGI DI INTERROGAZIONE DELLE BASI DATI

1.4 CLOUD COMPUTING (MANDATORY)

Conoscere i concetti di virtualizzazione e Cloud computing

1.4.1 VIRTUALIZZAZIONE
1.4.2 MODELLI CLOUD

1.4.3 CLOUD SERVICE PROVIDERS

2 NETWORKING

2.1 RETI DI CALCOLATORI (MANDATORY)

Conoscere i fondamenti delle reti di calcolatori

2.1.1 COMPONENTI FONDAMENTALI DI UNA RETE
2.1.2 IL MODELLO ISO-OSI E IL MODELLO TCP/IP

2.2 I LIVELLI DEL MODELLO ISO/OSI (MANDATORY)

Conoscere i livelli del modello ISO/OSI e i suoi principali protocolli

2.2.1 IL LIVELLO FISICO E I SUOI PRINCIPALI STANDARD
2.2.2 IL LIVELLO COLLEGAMENTO E I SUOI PRINCIPALI PROTOCOLLI
2.2.3 IL LIVELLO RETE E I SUOI PRINCIPALI PROTOCOLLI
2.2.4 IL LIVELLO TRASPORTO E I SUOI PRINCIPALI PROTOCOLLI
2.2.5 IL LIVELLO SESSIONE E I SUOI PRINCIPALI PROTOCOLLI
2.2.6 IL LIVELLO PRESENTAZIONE E I SUOI PRINCIPALI PROTOCOLLI
2.2.7 IL LIVELLO APPLICAZIONE E I SUOI PRINCIPALI PROTOCOLLI

SECONDA PARTE – CYBERSECURITY

3 MINACCE, ATTACCHI E VULNERABILITÀ

3.1 TIPI DI ATTACCO (MANDATORY)

Analizzare i potenziali indicatori per determinare il tipo di attacco

3.1.1 MALWARE
3.1.2 PASSWORD ATTACKS
3.1.3 PHYSICAL ATTACKS
3.1.4 ADVERSARIAL ARTIFICAL INTELLIGENCE (AII)
3.1.5 SUPPLY-CHAIN ATTACKS
3.1.6 CLOUD-BASED AN ON-PREMISES ATTACKS
3.1.7 CRYPTOGRAPHIC ATTACKS

3.2 TECNICHE DI INGEGNERIA SOCIALE (MANDATORY)

Confrontare e contrastare i diversi tipi di tecniche di ingegneria sociale

3.2.1 TECNICHE DI INGEGNERIA SOCIALE
3.2.2 PRINCIPI

3.3 ATTACCHI DI TIPO APPLICATIVO (MANDATORY)

Analizzare i potenziali indicatori associati agli attacchi delle applicazioni

3.3.1 PRIVILEGE ESCALATION
3.3.2 CROSS-SITE SCRIPTING
3.3.3 INJECTIONS
3.3.4 POINTER/OBJECT DEREFERENCE
3.3.5 DIRECTORY TRAVERSAL
3.3.6 BUFFER OVERFLOWS
3.3.7 RACE CONDITIONS
3.3.8 ERROR HANDLING
3.3.9 IMPROPER INPUT HANDLING
3.3.10 REPLAY ATTACK
3.3.11 INTEGER OVERFLOW
3.3.12 REQUEST FORGERIES
3.3.13 APPLICATION PROGRAMMING/INTERFACE (API) ATTACKS
3.3.14 RESOURCE EXHAUSTION
3.3.15 MEMORY LEAK
3.3.16 SECURE SOCKETS LAYER (SSL) STRIPPING
3.3.17 DRIVER MANIPULATION
3.3.18 PASS THE HASH

3.4 Attacchi di rete (Mandatory)

Analizzare i potenziali indicatori associati agli attacchi di rete

3.4.1 Wireless
3.4.2 On-path attack
3.4.3 Layer 2 attacks
3.4.4 Domain name system (DNS)
3.4.5 Distributed denial-of-service (DDoS)
3.4.6 Malicious code o script execution

3.5 Attori, vettori e minacce (Mandatory)

Conoscere i diversi attori malevoli, vettori e fonti di intelligence

3.5.1 Attori e minacce
3.5.2 Attributi degli attori
3.5.3 Vettori di attacco
3.5.4 risorse di threat intelligence
3.5.5 Ricerca delle risorse

3.6 Vulnerabilità (Mandatory)

Comprendere i problemi di sicurezza associati a vari tipi di vulnerabilità

3.6.1 Cloud-based vs. on-premises vulnerabilities
3.6.2 Zero-day
3.6.3 Weak configurations
3.6.4 rischio delle terze parti
3.6.5 Gestione delle patch improprie o deboli
3.6.6 Sistemi legacy
3.6.7 Impatti delle vulnerabilità

4 Network e cloud security

4.1 Protocolli di sicurezza (Mandatory)

Come implementare i protocolli di rete sicuri

4.1.1 Protocolli sicuri
4.1.2 Casi d'uso

4.2 Network security design (Mandatory)

Come disegnare e implementare una rete sicura

4.2.1 Load balancing
4.2.2 Segmentazione della rete
4.2.3 Virtual private network (VPN)
4.2.4 DNS

4.2.5 Network access control (NAC)
4.2.6 Out-of-band management
4.2.7 Port security
4.2.8 Appliance di rete

4.3 Impostazioni di sicurezza wireless

Come Installare e configurare le impostazioni di sicurezza della rete wireless

4.3.1 Protocolli Crittografici
4.3.2 Protocolli di autenticazione
4.3.3 Protocollo RADIUS
4.3.4 Metodi e considerazioni per la loro configurazione

4.4 Cloud security (Mandatory)

Come applicare soluzioni di sicurezza negli ambienti cloud

4.4.1 Controlli di sicurezza del Cloud
4.4.2 Soluzioni di sicurezza del Cloud
4.4.3 Controlli di sicurezza Cloud nativi e di terze parti

5 End-point security

5.1 Sicurezza delle Postazioni di Lavoro (Mandatory)

Come implementare soluzioni di sicurezza per la protezione dei sistemi e applicazioni

5.1.1 Protezione delle postazioni di lavoro
5.1.2 Email Security
5.1.3 Database
5.1.4 Boot integrity
5.1.5 Hardening
5.1.6 Self-encrypting drive (SED)/full-disk encryption (FDE)
5.1.7 Trusted Platform Module (TPM)
5.1.8 Sandboxing

5.2 Soluzioni di Mobile Security

Come implementare soluzioni per la sicurezza dei dispositivi mobile

5.2.1 Modalità di connessione e ricevitori
5.2.2 Mobile device management (MDM)
5.2.3 Modelli di implementazione

5.3 Soluzioni per la sicurezza IoT e OT

Comprendere le implicazioni di sicurezza dei sistemi IoT e OT

5.3.1 Sistemi Embedded

5.3.2 Supervisory control and data acquisition / (SCADA)/industrial control system (ICS)
5.3.3 Internet of Things (IoT)
5.3.4 Real-time operating system (RTOS)
5.3.5 Sistemi di Video Sorveglianza

6 Application Security

6.1 Fondamenti di application security (Mandatory)

Conoscere i concetti di base per lo sviluppo sicuro delle applicazioni

6.1.1 Fondamenti di linguaggi di sviluppo
6.1.2 Application security
6.1.3 Ciclo di vita per lo sviluppo delle applicazioni
6.1.4 Ambienti
6.1.5 Secure coding techniques
6.1.6 Open Web Application Security Project (OWASP)
6.1.7 Automation/scripting
6.1.8 Scalabilità
6.1.9 Controllo della versione

6.2 Fondamenti di autenticazione e autorizzazione (Mandatory)

Conoscere i concetti per la implementazione dei sistemi di autenticazione e autorizzazione

6.2.1 Metodi di autenticazione
6.2.2 Biometrica
6.2.3 Multifactor authentication (MFA)
6.2.4 Authentication, authorization, and accounting (AAA)
6.2.5 Cloud vs. on-premises requirements

6.3 Identity & Access management (Mandatory)

Come implementare soluzioni di autenticazione e autorizzazione

6.3.1 Identity
6.3.2 Tipi di account
6.3.3 Account policies
6.3.4 Gestione delle autenticazioni
6.3.5 Autenticazione & Autorizzazione
6.3.6 Schemi di controllo accessi

6.4 Privileged Access Management (Mandatory)

Come implementare una soluzione per la gestione degli accessi privilegiati

6.4.1 Tipologie di Utenze Privilegiate
6.4.2 Jump Host

6.4.3 Password Vaulting
6.4.4 Tracciamento delle Sessioni

6.5 SIEM & Log Management (Mandatory)

Come implementare una soluzione per il monitoraggio degli incidenti di sicurezza e per la raccolta dei log ai fini della compliance

6.5.1 Tipologie di Fonti Log
6.5.2 Analisi e Parsing dei Log
6.5.3 Ricerca e Correlazione
6.5.4 Regole Alerting
6.5.5 Dashboard e Reporting

7 Data Security

7.1 Fondamenti di crittografia (Mandatory)

Conoscere i concetti di base della crittografia

7.1.1 Fondamenti di crittografia
7.1.2 Simmetrica & Asimmetrica
7.1.3 Firme digitali
7.1.4 Hashing
7.1.5 Key Management
7.1.6 Blockchain
7.1.7 Cipher suites
7.1.8 Steganografia
7.1.9 Casi d'uso
7.1.10 Limitazioni

7.2 Public Key Infrastructure (PKI) (Mandatory)

Come attuare una infrastruttura a chiave pubblica

7.2.1 Concetti
7.2.2 Public key infrastructure (PKI)
7.2.3 Tipi di certificato
7.2.4 Formati dei certificati
7.2.5 Implementare una PKI

7.3 Data Loss Prevention

Come implementare una soluzione per la protezione dei dati aziendali

7.3.1 Tipologie di Dati
7.3.2 Classificazione dei Dati
7.3.3 Tipologie di Protezione
7.3.4 Strumenti per la protezione dei dati

8 OPERATION E INCIDENT RESPONSE

8.1 SECURITY OPERATION CENTER (MANDATORY)

Comprendere come è strutturato un SOC e il suo ruolo nelle dinamiche di sicurezza informatica

8.1.1 STRUTTURA ORGANIZZATIVA DI UN SOC
8.1.2 TIPOLOGIA DI SERVIZI SOC E CERT
8.1.3 PROCESSI DI GESTIONE INCIDENTI

8.2 TOOLS DI RILEVAZIONE E RISPOSTA AGLI INCIDENTI INFORMATICI (MANDATORY)

Come utilizzare gli strumenti appropriati per valutare la sicurezza dell'infrastruttura ICT aziendale

8.2.1 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)
8.2.2 END POINT DETECTION & RESPONSE
8.2.3 SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)
8.2.4 INTRUSION & PREVENTION SYSTEMS

8.3 ANALISI DEGLI INCIDENTI INFORMATICI (MANDATORY)

Come utilizzare tecniche e tool a supporto della rilevazione e analisi degli incidenti di sicurezza

8.3.1 CLASSIFICAZIONE INCIDENTI
8.3.2 ATTACK FRAMEWORKS
8.3.3 THREAT HUNTING
8.3.4 ANALISI DELLE VULNERABILITÀ
8.3.5 ANALISI DEI LOG FILES
8.3.6 BANDWIDTH MONITORING
8.3.7 ANALISI DEI METADATA
8.3.8 ANALISI NETFLOW/SFLOW
8.3.9 ANALISI OUTPUT DEI PROTOCOL ANALYZER

8.4 TECNICHE DI MITIGAZIONE (MANDATORY)

Come applicare le tecniche e i controlli di mitigazione per proteggere una infrastruttura ICT

8.4.1 RICONFIGURA ENDPOINT SECURITY SOLUTIONS
8.4.2 CONFIGURATION CHANGES
8.4.3 ISOLAMENTO
8.4.4 CONTENIMENTO
8.4.5 SEGMENTAZIONE

8.5 PENETRATION TESTING (MANDATORY)

Conoscere le tecniche utilizzate nei test di penetrazione delle infrastrutture ICT al fine di migliorarne la sicurezza

8.5.1 PENETRATION TESTING
8.5.2 RICOGNIZIONE PASSIVA ED ATTIVA
8.5.3 TIPI DI ESERCIZIO

8.5.4 Exploitation frameworks
8.5.5 Password crackers
8.5.6 Packet capture and replay
8.5.7 Network reconnaissance and discovery
8.5.8 Continuous Vulnerability Management

8.6 Digital forensic

Comprendere gli aspetti chiave della Digital Forensics

8.6.1 Documentazione e prove
8.6.2 Acquisizioni
8.6.3 On-premises vs. cloud
8.6.4 Integrità
8.6.5 Conservazione
8.6.6 E-discovery
8.6.7 Data recovery
8.6.8 Non ripudiabilità
8.6.9 Strategic intelligence / counterintelligence

9 Security Governance

9.1 Tipologie di controlli (Mandatory)

Conoscere e comparare i vari tipi di controlli di sicurezza

9.1.1 Categorie
9.1.2 Tipi di controllo

9.2 Processi e procedure di risposta agli incidenti (Mandatory)

Comprendere l'importanza delle politiche, dei processi e delle procedure per la risposta agli incidenti

9.2.1 Incident response plans
9.2.2 Incident response process
9.2.3 Stakeholder management
9.2.4 Communication plan
9.2.5 Retention policies

9.3 Regolamenti, standards e framework (Mandatory)

Comprendere l'importanza delle normative applicabili, standard o framework che hanno un impatto sulla postura di sicurezza informatica

9.3.1 Regolamenti, standards e legislazioni
9.3.2 Key frameworks
9.3.3 Benchmarks /secure Configuration guides

9.4 Politiche di sicurezza (Mandatory)

Comprendere l’importanza delle politiche di sicurezza organizzativa

- 9.4.1 Politica di sicurezza per il personale
- 9.4.2 Gestione del rischio delle terze parti
- 9.4.3 Politica di gestione dei dati
- 9.4.4 Politica delle credenziali
- 9.4.5 Politiche organizzative

9.5 Processo di Risk Management (Mandatory)

Comprendere i processi e i concetti di gestione del rischio

- 9.5.1 Tipi di rischio
- 9.5.2 Strategie di Risk Management
- 9.5.3 Analisi dei rischi

9.6 Business Continuity Management (Mandatory)

Comprendere i processi e i concetti della Business Continuity

- 9.6.1 Business impact analysis
- 9.6.2 Business continuity plan
- 9.6.3 Disaster recovery plan

9.7 Privacy e dati personali (Mandatory)

Comprendere i concetti di privacy e dati sensibili in relazione alla sicurezza informatica

- 9.7.1 Tipi di dati
- 9.7.2 Ruoli e responsabilità In Ambito Privacy
- 9.7.3 Principi Generali del Trattamento
- 9.7.4 Diritti Dell’Interessato
- 9.7.5 Gestione violazione Dei Dati Personali
- 9.7.6 Privacy by Design & by Default
- 9.7.7 Valutazione d'impatto

9.8 Elementi di Project & Service Management

Comprendere i fondamenti del project management

- 9.8.1 Elementi di Project Management
- 9.8.2 Panoramica sulle principali metodologie per la gestione dei progetti