MUSA
FORMAZIONE

SYLLABUS

PERCORSO DI CERTIFICAZIONE

INDICE DEI CONTENUTI

MITC-001-1.0 – Professional User

1. Informatica di Base

Obiettivi: conoscenza di un moderno Sistema Informativo (SI), quali sono i suoi principali componenti, l'importanza dei dati trattati quali reali asset dell'azienda/ente, e della sicurezza digitale per proteggerli, con cenni alle logiche ed ai criteri per terziarizzare e per utilizzare servizi in cloud.

CONCETTI BASE

- codice binario
- hardware
- software (di base, middleware, applicativo)
- firmware
- Sistemi operativi (OS)
- I vari tipi di OS (per mainframe, per server, per dispositivi d'utente, speciali)
- Cenni alla virtualizzazione
- Gli ambiti applicativi ed i dati trattati
- connessioni alle reti ed il ruolo di Internet
- la sicurezza digitale

LINGUAGGI DI SVILUPPO SOFTWARE

- i vari linguaggi disponibili
- il linguaggio macchina
- gli ambienti di sviluppo (IDE, etc.)

RETI

- Internet (stack IP modello OSI) e il suo ruolo chiave nell'attuale mondo digitale
- Reti pubbliche e reti private
- Reti locali e reti geografiche
- Reti fisse e reti wireless

MITC-001-1.0 – Professional User

1. Informatica di Base

I DATI ED IL LORO TRATTAMENTO

- Tipologia dei dati
- Il trattamento dei dati
- I dati personali e la privacy
- Cenni ai file system, alle banche dati e ai data warehouse
- Cenni ai Big data

L'INFRASTRUTTURA DI SISTEMA INFORMATIVO (SI)

- L'integrazione di informatica, telecomunicazioni e informazioni nel "digitale"
- Le funzionalità di un SI e l'erogazione di servizi
  - Per gli utenti interni
  - Per gli utenti esterni
- schema tipico di un moderno SI, sia on premise, che terziarizzato o un mix dei due (ibrido)
- Data Center
- I dispositivi d'utente
- Server e storage
- Il web
- Il cloud

CARATTERISTICHE E RUOLO DI UN MODERNO SISTEMA INFORMATIVO

- L'erogazione di servizi digitali
- cenni alle architetture ICT per i SI
  - infrastrutturali
  - ambiti applicativi
- gli ambiti applicativi
- I social
- I motori di ricerca
- cenni al governo e alla gestione operativa di un SI

MITC-001-1.0 – Professional User

2. Windows Microsoft - Livello Base

Obiettivi: conoscenza di base ed operativa di un Sistema Operativo (SO) con riferimento al SO Microsoft Windows per PC. Dopo aver introdotto i componenti fondamentali di un moderno PC (hardware, BIOS-firmware, software di base e applicativo, connessioni in rete, CPU, bus di sistema, memorie e storage, periferiche) viene descritto in pratica il ruolo di un SO con riferimento a Windows.

CHE COSA È UN PC E IL SUO SISTEMA OPERATIVO

- Cenni alla logica binaria e booleana
- la struttura tipica di un moderno PC: hardware, BIOS (firmware), software di base e applicativo, connessioni in rete
- CPU, bus di sistema, memorie e storage, periferiche
- che cosa fa un Sistema Operativo (OS) per un PC/sistema ICT
- Attiviamo un PC con OS Windows e vediamo le sue “finestre”
- tipologie di OS che ha OS Windows per PC : seriale vs parallelo, multitasking o multithreading, etc.

Le principali funzioni di un OS Windows

- Il Kernel
- Lo schedulatore (Scheduler)
- Gestione dell'input/output e delle periferiche (gestione interrupt)
- Gestione della memoria
- Gestione dei driver delle periferiche

SOTTOSISTEMI TUTTI I SISTEMI VENGONO MOSTRATI “DAL VIVO”

- File system
- Interfaccia utente
  - Linea di comando (CLI – Command Line Interface)
  - Grafica (GUI)
- Spooler di stampa
- Gestione degli utenti
- Gestione della rete

MITC-001-1.0 – Professional User

2. Windows Microsoft - Livello Base

EVOLUZIONE DI MS-WINDOWS

- Gli attuali OS non obsoleti

Specificità OS MS-Windows -1 Tutti gli elementi vengono mostrati “dal vivo”

- Desktop
  - Modalita’ tablet
  - Modalita’ PC
  - Pulsante Start
  - Barra delle applicazioni
- Applicazioni /accessori preinstallati
  - Strumenti per l’accessibilità
    - Assistente vocale
    - Lente d’ingrandimento
    - Riconoscimento vocale
    - Tastiera su schermo

Specificità OS MS-Windows -2 Tutti gli elementi vengono mostrati “dal vivo”

- Accessori
  - Alarms & clock
  - Assistenza rapida
  - Blocco note
  - Desktop remoto
  - Fax e scanner
  - Strumento di cattura
  - Calculator
  - Calendar
  - Camera
  - Cortana
  - Mail
  - Microsoft Edge

2. Windows Microsoft - Livello Base

- Maps
- Microsoft Teams
- Skype
- OneDrive
- OneNote

Specificità OS MS-Windows -3 Tutti gli elementi vengono mostrati “dal vivo”

- Microsoft store
- Impostazioni e pannello di controllo
  - Rete
  - Sicurezza
  - Aggiornamenti
  - Personalizzazioni
  - Gestione account
  - Dispositivi
  - Accessibilita’
  - Data/ora e Lingue
  - Privacy
  - Giochi
- Windows PowerShell
- Sottosistema Linux per Windows

MITC-001-1.0 – Professional User

3. Linux Essentials - LPI LE-1

- **Obiettivi**: Comprendere Unix e le principali differenze tra le varie distribuzioni LinuxUtilizzare la shell di Linux per eseguire operazioni su file e cartelle, Gestire archivi compressi, generare script automatici con i comandi della shell di Linux, conoscere il filesystem di Linux e le posizioni dei dati sul disco, apprendere i concetti delle reti di computer, gestire utenti, gruppi e permessi sui file e cartelle

LA COMMUNITY LINUX E UNA CARRIERA NELL'OPEN SOURCE

- Evoluzione di Linux e principali sistemi operativi
- Principali applicazioni open source
- Software open source e licenze
- Competenze ICT e lavoro in ambiente Linux

ORIENTARSI IN UN SISTEMA LINUX

- Basi della riga di comando
- Usare la riga di comando per ottenere aiuto
- Utilizzo delle directory ed elencazione dei file
- Creazione, spostamento ed eliminazione dei file

LA POTENZA DELLA RIGA DI COMANDO

- Archiviazione di file tramite riga di comando
- Ricerca ed estrazione di dati dai file
- Trasformare comandi in uno script

IL SISTEMA OPERATIVO LINUX

- Scegliere un sistema operativo
- Comprendere l'hardware del computer
- Dove sono memorizzati i dati
- Il tuo computer in rete

SICUREZZA E PERMESSI DEI FILE

- Sicurezza di base e tipi di utenti
- Creazione di utenti e gruppi
- Gestione dei permessi e della proprietà dei file
- Directory e file speciali

MITC-001-1.0 – Professional User

4.Networking Base

Obiettivi: conoscenze sui protocolli, sugli apparati di rete e sugli strumenti necessari per progettare una rete LAN e gestirla. Tutto in linea con il modello di riferimento per l'interconnessione dei computer ISO/OSI, e alla suite di protocolli internet TCP (Transmission Control Protocol) e IP (Internet Protocol).

MODULO I

- Presentazione docente e corso
- Reti di elaborati, LAN e WAN
- Indirizzi IP e Indirizzi Fisici (MAC)
- Wireshark e Packet Tracer
- Protocollo, ISO-OSI, approccio Bottom-Up e il Livello 1
- Quiz
- Esercitazioni

MODULO II

- Framing, Schede di rete, Switch e HUB
- Dominio di collisione e protocollo CSMA/CD
- VLAN
- Wireless
- Quiz
- Esercitazioni

MODULO III

- Indirizzo IP e Subnet Mask, IPv6
- Protocollo ARP
- Protocollo ICMP, ping, traceroute
- DHCP e Indirizzi Statici
- Router, Routing e NAT
- Quiz
- Esercitazioni

MITC-001-1.0 – Professional User

4.Networking Base

MODULO IV

- Concetti base
- TCP part 1
- TCP part 2
- UDP e utilizzi
- Quiz
- Esercitazioni

MODULO V

- DNS
- HTTP part 1
- HTTP part 2
- Quiz
- Esercitazioni
- Conclusioni e consigli finali

MITC-002-1.0 – System Admin Professional

2. Virtualizzazione di Base

Obiettivi: capire a fondo i concetti di base della virtualizzazione e acquisire i concetti fondamentali per poter creare, importare e gestire le macchine virtuali.

INTRODUZIONE E TEORIA

- La virtualizzazione

HYPERVISOR E INSTALLAZIONE

- Panoramica Hypervisor
- Installazione di Virtualbox

IMPORTARE, ESPORTARE E CONFIGURAZIONI

- Reperire VM e import VM
- Exportin formato OVA
- Parametri di configurazione e best-practice

INSTALLAZIONE PULITA DI UNA VM

- Download ISO Windows e installazione
- Installare Virtualbox Guest Additions Windows
- Download di una Linux e installazione
- Installare Virtualbox Guest Additionssu Linux

OPERAZIONI DI GESTIONE

- Spegnimento, riavvio e salvataggio dello stato
- Gestione della finestra, visualizzazione e risoluzione
- Copia-incolla, Drag and Drop, Condivisione cartelle
- Snapshot
- Cloni
- Spostamento macchina virtuale e Gestione Dischi

MITC-002-1.0 – System Admin Professional

2. Virtualizzazione di Base

TIPOLOGIA DI RETE E DIFFERENZE

- Comandi utili per il networking e per il troubleshooting
- Rete NAT e Port-Forwarding
- Rete bridge
- Rete host-only e uso di più reti

I CONTAINER E LE VM

- I container
- La sicurezza degli ambienti isolati

MITC-002-1.0 – System Admin Professional

3. Windows Server Administrator

Obiettivi: L'obiettivo del corso è dare un'adeguata formazione per gestire la configurazione e della gestione dei carichi di lavoro della piattaforma Windows Server on-premises, ibrida e infrastructure as a service (IaaS).
E nello specifico:

1. Integrare gli ambienti Windows Server con i servizi Azure.
2. Gestire Windows Server nelle reti on-premises.
3. Gestite e mantenete i carichi di lavoro Windows Server IaaS in Azure
4. Migrare e distribuire i carichi di lavoro in Azure.

MODULO 1.0 - DISTRIBUIRE E GESTIRE ACTIVE DIRECTORY DOMAIN SERVICES NEGLI AMBIENTI ON-PREMISES E CLOUD

1.1: Distribuire e gestire i controller di dominio AD DS
1.2: Configurare e gestire ambienti multi-sito, multi-dominio e multi-foresta
1.3: Creare e gestire i principali di sicurezza di AD DS
1.4: Implementare e gestire identità ibride
1.5: Gestire Windows Server utilizzando le Group Policy basate sul dominio

MODULO 2.0 - GESTIRE WINDOWS SERVER E I CARICHI DI LAVORO IN UN AMBIENTE IBRIDO

2.1: Gestire Windows Server in un ambiente ibrido
2.2: Gestire Windows Server e i carichi di lavoro utilizzando i servizi di Azure

MODULO 3.0 - GESTIRE MACCHINE VIRTUALI E CONTAINER

3.1: Gestire Hyper-V e le macchine virtuali guest
3.2: Creare e gestire container
3.3: Gestire le macchine virtuali di Azure che eseguono Windows Server

MITC-002-1.0 – System Admin Professional

3. Windows Server Administrator

MODULO 4.0 – IMPLEMENTARE E GESTIRE UN'INFRASTRUTTURA DI RETE ON-PREMISES E IBRIDA

4.1: Implementare la risoluzione dei nomi in ambienti on-premises e ibridi
4.2: Gestire l'assegnazione degli indirizzi IP in scenari on-premises e ibridi
4.3: Implementare la connettività di rete in ambienti on-premises e ibridi

MODULO 5.0 – GESTIRE I SERVIZI DI ARCHIVIAZIONE E FILE

5.1: Configurare e gestire Azure File Sync
5.2: Configurare e gestire le condivisioni file in Windows Server
5.3: Configurare lo storage in Windows Server

MODULO 6.0 – PROTEGGERE L'INFRASTRUTTURA WINDOWS SERVER ON-PREMISES E IBRIDA

6.1: Proteggere il sistema operativo Windows Server
6.2: Proteggere un'infrastruttura Active Directory ibrida
6.3: Identificare e risolvere problemi di sicurezza in Windows Server utilizzando i servizi Azure
6.4: Proteggere la rete di Windows Server
6.5: Proteggere l'archiviazione di Windows Server

MODULO 7.0 – IMPLEMENTARE E GESTIRE L'ALTA AFFIDABILITÀ DI WINDOWS SERVER

7.1: Implementare un cluster di failover di Windows Server
7.2: Gestire il clustering di failover
7.3: Implementare e gestire Storage Spaces Direct

MITC-002-1.0 – System Admin Professional

3. Windows Server Administrator

MODULO 8.0 – IMPLEMENTARE IL DISASTER RECOVERY

8.1: Gestire backup e ripristino per Windows Server
8.2: Implementare il disaster recovery utilizzando Azure Site Recovery
8.3: Proteggere le macchine virtuali utilizzando Hyper-V Replica

MODULO 9.0 – MIGRARE SERVER E CARICHI DI LAVORO

9.1: Migrare l'archiviazione on-premises verso server on-premises o Azure
9.2: Migrare server on-premises verso Azure
9.3: Migrare carichi di lavoro da versioni precedenti a Windows Server 2022
9.4: Migrare carichi di lavoro IIS verso Azure
9.5: Migrare un'infrastruttura AD DS a Windows Server 2022 AD DS

MODULO 10.0 – MONITORARE E RISOLVERE PROBLEMI NEGLI AMBIENTI WINDOWS SERVER

10.1: Monitorare Windows Server utilizzando strumenti integrati e servizi Azure
10.2: Risolvere problemi di rete in ambienti Windows Server on-premises e ibridi
10.3: Risolvere problemi relativi a macchine virtuali Windows Server in Azure
10.4: Risolvere problemi di Active Directory

MITC-002-1.0 – System Admin Professional

1.Linux LPIC1 – 101-500

Obiettivi: capire l'architettura di un sistema Linux; installare e mantenere una workstation Linux, incluso X11 e configurarlo come client di rete; lavorare sulla command line di Linux, compresi i comuni comandi GNU e Unix; gestire i file e le autorizzazioni di accesso e la sicurezza del sistema; eseguire semplici attività di manutenzione: aiutare gli utenti, aggiungere utenti a un sistema più esteso, eseguire il backup e il ripristino, spegnere e riavviare.

ARCHITETTURA DI SISTEMA

- Determinare e Configurare le Impostazioni dell'Hardware
- Avviare il sistema
- Modificare runlevel / target di avvio e spegnere o riavviare il sistema

INSTALLAZIONE DI LINUX E GESTIONE DEI PACCHETTI

- Progettare il layout del disco rigido
- Installare un boot manager
- Gestire le librerie condivise
- Utilizzare la gestione dei pacchetti Debian
- Utilizzare la gestione dei pacchetti RPM e YUM
- Linux come sistema virtualizzato

GNU E UNIX COMMANDS

- Lavorare con la Command Line
- Elaborare flussi di testo utilizzando i filtri
- Eseguire la gestione di base dei file
- Utilizzare flussi, pipe e reindirizzamenti
- Creare, controllare e terminare i processi
- Modificare le priorità di esecuzione del processo
- Cercare file di testo utilizzando espressioni regolari
- Modifica base di un file

MITC-002-1.0 – System Admin Professional

1.Linux LPIC1 – 101-500

I DISPOSITIVI, IL FILE SYSTEM LINUX, IL FILE SYSTEM HIERARCHY STANDARD

- Creare partizioni e filesystem
- Mantenere l'integrità dei filesystem
- Verificare il montaggio e lo smontaggio dei filesystem
- Gestire le autorizzazioni e la proprietà dei file
- Creare e modificare collegamenti hard e soft
- Trovare i file di sistema e collocarli nella posizione corretta

MITC-002-1.0 – System Admin Professional

1.Linux LPIC1 102-500

Obiettivi: Acquisire le abilità di amministrazione base attraverso l'utilizzo della CLI e di comandi comuni alla maggior parte delle distribuzioni Linux

OGGETTI COMPONENTI L'AMBIENTE DI SHELL: ALIAS, VARIABILI, FUNZIONI E COMANDI

- Automazione della configurazione di base dei nuovi utenti all'atto della loro creazione
- Controllo della ricerca di comandi sul filesystem
- Creazione di script e i loro costrutti sintattici
- L'uso del servizio locale di posta elettronica
- Esecuzione di query semplici e di manipolazione di un database con comandi SQL
- Configurazione e verifica del corretto funzionamento di un server grafico X11
- Configurazione di base del Desktop Manager LightDM
- Conoscenza di base degli applicativi per la facilitazione nell'uso del sistema da parte di persone con ridotte capacità motorie e/o sensoriali
- Gestione degli utenti e dei gruppi di utenti
- Gestione della schedulazione di esecuzione periodica o puntuale di processi
- Gestione della configurazione di sistema e per utente delle impostazioni di fuso orario e supporto linguistico
- Sincronizzazione dell'orologio di sistema con server del tempo di alta precisione
- Configurazione del servizio di sistema di log
- Configurazione del servizio di svecchiamento automatico dei log di sistema
- Gestione di base del servizio di invio dei messaggi di posta elettronica
- Gestione di base del servizio di stampa
- Concetti fondamentali di reti Ethernet TPC/IP compresi indirizzamento dei nodi ed instradamento dei pacchetti
- Configurazione automatica e manuale delle interfacce di rete

Elementi di diagnostica e risoluzione dei principali problemi legati alla rete

MITC-002-1.0 – System Admin Professional

1.Linux LPIC1 102-500

- Configurazione lato client del servizio di risoluzione dei nomi di dominio DNS
- Elementi di sicurezza di sistema: ricerca eseguibili a rischio e controllo delle operazioni degli utenti
- Eliminazione dei più ovvi punti deboli del sistema di fronte ad attacchi contro le password degli utenti e contro servizi di rete
- Fondamenti di crittografia delle connessioni di shell da remoto e di firma digitale e crittografia dei file

MITC-002-1.0 – System Admin Professional

4. Networking Avanzato

Obiettivi: progettare, implementare e curare la manutenzione di reti informatiche di tipo LAN/WAN e wireless basate sui protocolli IPv4 e IPv6.

FONDAMENTI DI RETI DI TELECOMUNICAZIONI

1. **DESCRIZIONE DEI COMPONENTI E PROTOCOLLI DI RETE**
   - Routers
   - LAN switches layer 2 e layer 3
   - Firewalling: difesa perimetrale e tra i vari livelli di una infrastruttura
   - Reti WiFi: controllers e access points
   - Cenni su soluzione Cisco DNA Center
   - Endpoints, Server e device POE
2. **ARCHITETTURE DI RETE**
   - Architettura a 2 livelli
   - Architetture WAN: Small office/home office (SOHO), Branch Office
   - Architetture on-premise e cloud
3. **LIVELLO FISICO: INTERFACCE E VARI TIPI DI CABLATURE**
   - Fibra monomodale e multimodale, cavi in rame UTP/STP (cat5, cat5e, cat6, cat7, twinax 10, 100, 400G/s)
   - Connessioni Ethernet multiaccesso e punto-punto, Ethernet nella MAN o metro-Ethernet
   - Identificare problematiche di livello fisico (collisioni, errori, duplex e/o speed mismatch)

MITC-002-1.0 – System Admin Professional

4. Networking Avanzato

4. **PROTOCOL STACK: ISO/OSI E TCP/IP**

a. Differenze tra i due stack

b. Configurare e verificare l'indirizzamento IPv4 e relativo subnetting

c. Private IPv4 addressing e RFC1918

d. Indirizzi IPv4 speciali

e. Configurare e verificare indirizzamento e prefissi IPv6

f. Vari tipi di indirizzi IPv6: Unicast, Anycast, Multicast, EUI 64)

g. Configurazione e verifica dell'indirizzamento per sistemi operativi Windows, Mac OS e Linux

h. Descrivere le basi delle reti wireless e/o WiFi

i. Canali RF WiFi e SSID

l. Tipi di autenticazione e cifratura su canale WiFi

m. Concetti di virtualizzazione (server virtualization, containers, and VRF)

n. Concetti di ethernet switching: MAC learning and aging, flooding del traffico BUM, gestione della MAC Table.

MITC-002-1.0 – System Admin Professional

4. Networking Avanzato

CONFIGURARE APPARATI LAYER 2 PER L'ACCESSO ALLA RETE

- Configurare e verificare le VLAN
- Layer2 switch access port (data and voice)
- Default VLAN
- Connectività layer 2 degli endpoint alle porte di uno switch
- Configurazione e verifica della connettività switch-to-switch e switch-server su porte trunk
- Trunk ports: 802.1Q eVLAN nativa
- Configurazione e verifica dei protocolli di discovery (Cisco Discovery Protocol e LLDP)
- Configure and verifica dei meccanismi di aggregazione di più link Ethernet punto-punto: (Layer 2/Layer 3 LAG, protocolli LACP e PAGP)
- Descrizione e funzionamento dei protocolli di Spanning Tree per la risoluzione dei loop layer 2 (Classical STP/PVST, Rapid PVST+, MSTP)
- Cisco Wireless Architectures e AP mode
- Descrizione dei component di una WLAN (AP, WLC, access/trunk ports, and LAG)
- Descrivere le metodologie di gestione degli AP e WLC (Telnet, SSH, HTTP, HTTPS, console, gestione centralizzata mediante TACACS+/RADIUS)
- Creazione mediante interfaccia grafica di una WLAN per l'accesso ai client e configurazione dei settaggi base: settaggi di sicurezza, profili QoS, parametri RF, AP mode. Configurazione avanzata.

MITC-002-1.0 – System Admin Professional

4. Networking Avanzato

CONFIGURARE APPARATI LAYER 3 PER L'ACCESSO ALLA RETE

1. **Connettività IPv4**
   a. Descrizione del ruolo e funzionamento di un router in una rete IP. Funzionamento della routing table
   b. Parametri di una tabella di routing: destination prefix, next-hop, interfacce di uscita, distanza amministrativa o route preference, metrica e gateway of last resort.
   c. Descrivere come un router intraprende le decisioni di inoltro di un pacchetto fino alla destinazione: longest prefix match, administrative distance, metrica del protocollo di routing
   d. Configurazione e verifica del routing IPv4 ed IPv6: static routing, default route, host route, floating static route
   e. Routing dinamico: RIPv2, EIGRP, OSPF monoarea e multiarea basic
   f. Descrivere le funzioni dei protocolli di first hop redundancy: HSRP, VRRP, GLBP
2. **Servizi IP**
   a. Descrizione dei servizi IP
   b. Configurazione e verifica di NAT statico, dinamico e PAT
   c. Configurazione e verifica del protocollo NTP
   d. Spiegare le funzionalità del DHCP e DNS in una rete TCP/IP
   e. Protocolli di gestione degli apparati di rete: Syslog, SNMP, Telnet, SSH, TFTP, FTP
   f. Configurazione e verifica DHCP client and relay
   g. Descrizione dei modelli di QOS: IntServ e DiffServ
   h. Modello Diffserv: descrivere il forwarding per-hop behavior (PHB) per la QoS, metodi di classificazione del traffico, il marking, la gestione della congestione, la gestione delle code a priorità, le tecniche di congestion avoidance (RED/WRED), il traffic policing e il traffic shaping
   i. Configurazione dei network devices per remote access via Telnet ed SSH
   j. Software upgrade/downgrade via TFTP/FTP

MITC-002-1.0 – System Admin Professional

4. Networking Avanzato

BASI DI NETWORK AUTOMATION E PROGRAMMABILITY

1. **Come l'automazione impatta il network management e introduzione all'SDN**
   a. Confronto tra reti tradizionali don reti controller-base
   b. Definizione delle architetture di reti controller-based (overlay, underlay, e fabric)
   c. Separazione del control plane e del data plane
   d. Northbound and Southbound APIs
   e. Confronto della gestione delle reti campus tradizionali con la soluzione Cisco DNA Center o SD-Access
   f. Descrizione delle caratteristiche delle REST APIs
   g. Descrizione delle tecniche di configuration management mediante Puppet, Chef, ed Ansible
   h. Componenti di configurazione di un device in formato XML e JSON
2. **Fondamenti di Sicurezza delle reti**
   a. Concetti di sicurezza (minacce, vulnerabilità, exploits, and mitigation techniques)
   b. Descrivere concetti di security awareness (user awareness, training, and physical access control)
   c. Configurazione e verifica degli accessi amministrativi a un router usando local passwords
   d. Descrivere tecniche di sicurezza sulla gestione delle password (complessità, multifactor authentication, certificati, tecniche biometriche)
   e. Descrivere IPsec remote access and site-to-site VPNs
   f. Configurazione e verifica delle access control list
   g. Configurazione e verifica delle features di Layer 2 security (DHCP snooping, dynamic ARP inspection, port security)
   h. Concetti di authentication, authorization, and accounting AAA (Radius e Tacacs)
   i. Descrivere i protocolli di sicurezza WiFi (WPA, WPA2, and WPA3)

MITC-003-1.0 - Governance Professional Level

1. IT Security Governance & Management Core Level

Obiettivi: Evidenziare l'importanza di una adeguata architettura ICT, e della sua sicurezza digitale, in grado di ridurre gli impatti di eventuali attacchi/malfunzionamenti al/del SI e garantire la continuità operativa almeno dei processi fondamentali dell'azienda/ente; approfondire i concetti di governance e di management per la sicurezza digitale e vengono poi considerati le logiche e gli aspetti organizzativi con riferimento alle numerose leggi e normative in essere, in particolare alla privacy (GDPR), al NIS e al NIS2, al Cybersecurity Act e alle normative per le PA emesse da AgID (CAD); approfondire il tema interdisciplinare della sicurezza digitale, con le sue misure tecniche ed organizzative per la prevenzione ed il contrasto ad attacchi, ed i principali standard e best practice in merito; classificazione dei dati, e come può essere effettuata e gestita; approfondire quali sono gli attacchi digitali più diffusi e più critici; analisi dei rischi ICT, con riferimento alle possibili vulnerabilità tecniche, organizzative e personali, il Piano di Disaster Recovery, e l'auditing della sicurezza digitale.

CARATTERISTICHE E RUOLO DI UN MODERNO SI

- schema tipico di un moderno SI, sia on premise, che terziarizzato o un mix dei due (ibrido)
- la necessità di allineare il SI al business
- il piano di evoluzione del business e del SI
- il ruolo dell'architettura ICT per il SI
- la necessità di una effettiva cybersecurity per garantire la continuità operativa (business continuity) di processi/attività chiave per il business
- SI come commodity (almeno per le piccole strutture): è ragionevole? Ha senso?

MITC-003-1.0 - Governance Professional Level

1. IT Security Governance & Management Core Level

GLI ASPETTI ORGANIZZATIVI E NORMATIVI PER IL SI E LA SUA SICUREZZA

- il modello demand-delivery
- strutture, ruoli e competenze
- La separazione dei ruoli (SoD, matrici RACI)
- l'interfacciamento ed il controllo dei fornitori ICT-outsourcer
- policy e procedure organizzative
- cenni alle ultime leggi e normative in vigore in Italia
- Esempi di attuazione in strutture organizzative di grandi e di medio-piccole dimensioni.

APPROFONDIMENTO DIFFERENZA TRA GOVERNO (GOVERNANCE) E GESTIONE OPERATIVA (MANAGEMENT) DEL SI E DELLA SUA SICUREZZA DIGITALE

- Standard e best practice di riferimento ed il loro posizionamento/confronto nella logica matrice 3x3
- Quando, cosa e come terziarizzare della governance e del management operativo

LA GOVERNANCE E LA COMPLIANCE ALLE PRINCIPALI NORMATIVE

- La necessità/ opportunità di una approccio "integrato"
- GDPR e normative sulla privacy e la relativa sicurezza
- NIS e NIS 2
- Perimetro di sicurezza nazionale cibernetica (DPCM 30 luglio 2020)
- Cybersecurity Act
- Le normative per la PA (AgID)
- Le leggi sul computer crime

MITC-003-1.0 - Governance Professional Level

1. IT Security Governance & Management Core Level

GLI ENTI ITALIANI ED EUROPEI PER L'ICT E LA SICUREZZA DIGITALE

- ENISA
- ACN con CSIRT, NCS, CVCN
- Polizia Postale e delle Comunicazioni con CNAIPIC
- COR e altre strutture militari
- Altre strutture (NATO, …)

L'ALLINEAMENTO TEMPORALE TRA IL BUSINESS ED IL SI E LA SUA SICUREZZA TRAMITE L'ARCHITETTURA ICT

- Cenni sui modelli di business ed i modelli architetturali ICT (standard e best practice)
- Esempi di architetture ICT, partendo dallo standard Togaf
- Esempi di architetture per la sicurezza digitale: NIST, OSA, …
- Le nuove architetture per la sicurezza digitale quali Zero Trust, SASE, SOAR, etc.
- Architetture SI "proprietarie"
  - Microsoft, Oracle, Google, etc.
- Architetture applicative proprietarie
  - SAP, Oracle, Google, AWS, etc.

TERZIARIZZAZIONI E CLOUD

- i pro ed i contro delle terziarizzazioni e dei servizi in cloud
- clausole contrattuali
- SLA e KPI
- Rightsourcing: logiche e criteri per una corretta scelta del/i fornitore/i

MITC-003-1.0 - Governance Professional Level

1. IT Security Governance & Management Core Level

LA SICUREZZA DIGITALE

- Che cosa è la sicurezza digitale
- Security by design e by default
- Il processo continuo della sicurezza digitale
  - le sue misure tecniche ed organizzative (prevenzione, contrasto, ripristino, gestione/governo)
- il Framework NIST
- Standard ISO
- Standard NIST ed altri
- Cosa richiede AgID per le PA: CAD e altre normative
- Cosa richiede GDPR
- Il costo della sicurezza digitale ed il costo della “non sicurezza”
- la terziarizzazione della sicurezza digitale: MSS e CSaaS

NEXT GENERATION SECURITY: LE PRINCIPALI INNOVAZIONI CHE POSSONO IMPATTARE SUL SI, SULLA SUA GESTIONE E SULLA SUA SICUREZZA DIGITALE

- Strumenti di Intelligenza Artificiale (IA) e di machine Learning (ML)
- Blockchain
- Big Data e Analytics
- Digital twin
- Identificazione biometrica utenti e autenticazione passwordless (es. FIDO2)

MITC-003-1.0 - Governance Professional Level

1. IT Security Governance & Management Core Level

CENNI ALLE MODERNE LOGICHE DI SVILUPPO DEL SOFTWARE

- Object Orientation e Componentware
- Agile/Extreme/Lean Programming
- DevOps
- Low Code
- Cenni agli ambienti di sviluppo software integrati (IDE, integrated development environment)
- Lo sviluppo sicuro di software

LA CLASSIFICAZIONE DEI DATI ED IL LORO CICLO DI VITA (CON ESEMPI PRATICI)

- Gli strumenti per la gestione dei dati (Data Catalog, etc.)

GLI ATTACCHI DIGITALI PIÙ DIFFUSI E PIÙ CRITICI IN ITALIA

- Attacchi target e diffusi
- Dall'indagine OAD di AIPSI
- Da altri rapporti
- L'impatto del Covid-19 e della guerra informatica
- I futuri possibili attacchi più temuti e più probabili

ANALISI DELLE VULNERABILITÀ, DEI RISCHI ICT E DEI LORO IMPATTI (CON ESEMPI E CASI PRATICI)

- Vulnerabilità tecniche, organizzative, delle persone
- il concatenamento delle vulnerabilità dalle infrastrutture alle applicazioni e alla loro gestione
- Come individuare le principali vulnerabilità tecniche
  - CVE/Mitre, US DNS, ed altre fonti
  - OSWAP per le vulnerabilità dei web
  - Cenni agli strumenti di analisi vulnerabilità ICT tipo Nessus, Qualys, OpenVas, etc.

MITC-003-1.0 - Governance Professional Level

1. IT Security Governance & Management Core Level

- Cenni all'analisi delle vulnerabilità ICT all'analisi dei rischi e dei loro impatti
  - Come valutare i possibili impatti di un attacco digitale
- Cenni alla simulazione di attacchi e ai pentest

LA NECESSITÀ DELLA CONTINUITÀ OPERATIVA (BUSINESS CONTINUITY) E DEL PIANO DI DISASTER RECOVERY

- Standard e best practice di riferimento
- Come impostare un effettivo ed efficace Piano di Disaster Recovery
  - Le varie modalità attuative, ed i criteri di scelta di quale adottare e seguire
- ERT, Emergency Response Team
- Simulazione di un DR con DTE, Desk Top Exercise

L'AUDITING PER IL SI

- Che cosa è a che cosa serve
- Interno, esterno, mix
- standard di riferimento: Cobit, SAE70, ISAE 3402, SSAE16.
- Cenni alle certificazioni

2. IT Security Governance & Management Professional Level

Obiettivi: Approfondimento in logica tecnico-manageriale, sul governo (governance) e sulla gestione operativa (management) della sicurezza digitale. Il focus è la comprensione di quanto previsto per il governo e la gestione della sicurezza digitale nelle due principali best practice a livello mondiale, il COBIT e l'ITIL. Si affronteranno le logiche e criteri da seguire per una adozione "intelligente" e contestualizzata alla realtà del SI di queste due best practice, complimentandole con adozione di altre norme e standard, quali quelli dell'ISO e del NIST.

INQUADRAMENTO COBIT

- Obiettivi e motivazioni COBIT
- L'evoluzione di COBIT dalle origini (da modello COSO) alla v5 ed alla v. 2019
- I principi ed i fattori abilitanti di Cobit
- Gli stakeholder ed il "valore" per loro

I PROCESSI IN COBIT

- Processi di governo e di gestione
- I processi dedicati alla sicurezza digitale
- La descrizione in Cobit di un processo
- I livelli di implementazione di un processo

LA SICUREZZA DIGITALE IN COBIT: COME, QUANDO E A CHE CONDIZIONI FARE RIFERIMENTO A COBIT

- Cenni alle certificazioni per COBIT
- Esempi di uso, anche parziale di COBIT in strutture organizzative di grandi e di medio-piccole dimensioni.

2. IT Security Governance & Management Professional Level

CENNI AD ALTRI STANDARD E BEST PRACTICE PER LA GOVERNANCE DEL SIE DELLA SUA SICUREZZA

- Cenni al Process Capability Model and Levels (ISO/IEC 15504, SPICE)
- Cenni al PAM, Process Assessment Method
- Cenni al CMMI, Capability Maturity Model Integration
- Cenni al BMIS, Business Model for Information Security

INQUADRAMENTO ITIL

- Obiettivi e motivazioni
- L'evoluzione di ITIL dalle origini alla v3, la più diffusa in Italia, ed alla rivoluzione della v4 che adotta le logiche di DevOps
- Differenziazione e convergenze/sovrapposizioni con COBIT

I CONCETTI BASE DI ITIL FINO ALLA V.3 (ATTUALMENTE IN FUNZIONE NELLA MAGGIOR PARTE DELLE ORGANIZZAZIONI CHE HANNO ADOTTATO ITIL)

- Fasi, servizi, funzioni, processi, ciclo di un servizio (service life cycle), il valore (value), la gestione del Servizio (Service Management)
- Il modello ITIL: Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement. Cenni ai vari processi
- I processi e le funzioni in SO
- L'importanza della separazione dei compiti e delle responsabilità (SoD, Separation of Duties), le matrici RACI

2. IT Security Governance & Management Professional Level

I NUOVI CRITERI E LE NUOVE LOGICHE DELLA V4

- L'esigenza di far evolvere il modello di Service Management a nuove modalità operative, basata soprattutto alla velocità di intervento, ed esteso dall'UOSI alle altre strutture organizzative e BU (ESM, Enterprise Service Management)
- Lo sviluppo del software ed il suo controllo: Agile, Lean DevOps
- Eliminazione delle fasi, passaggio dai processi alle practices (ma mantenendo molto dei concetti e delle logiche delle prime)
- Leadership IT e Organizational Change management
- L'integrazione del concetto di Service Integration and Management in contesti Multivendor
- La Governance del SI e della sua sicurezza in ITIL

LA SICUREZZA DIGITALE IN ITIL: COME, QUANDO E A CHE CONDIZIONI FARE RIFERIMENTO A ITIL

- Cenni alle certificazioni per ITIL
- Esempi di uso, anche parziale di ITIL in strutture organizzative di grandi e di medio-piccole dimensioni
- Un approccio ibrido con COBIT e ITIL?

2. IT Security Governance & Management Professional Level

COME GESTIRE LA GOVERNANCE ED IL MANAGEMENT DI UN SI E DELLA SUA SICUREZZA DIGITALE

- L'impossibilità/non convenienza ad automatizzare la Governance del SI
- La necessità di automatizzare quanto più possibile la gestione operativa
- Logiche e criteri di cosa e come terziarizzare o non
- Governare il SI
  - I rapporti con gli utenti
  - I rapporti con gli stakeholders
  - Piano strategico pluriennale di business allineato al piano evolutivo SI
  - La trasformazione digitale
- Gestione operativa del SI
  - Monitoraggio e controllo funzionalità e prestazioni intero SI
  - Monitoraggio e controllo sicurezza digitale
  - Gestione problemi (Help Desk e trouble ticketing)
  - Gestione incidenti e disastri
  - Gestione accessi utenti privilegiati e finali
  - Provisioning
  - Gestione backup ed eventuali ripristini
  - Piano di Disaster Recovery e sua attuazione
  - Capacity planning
- Il Supporto informatico alle decisioni: uso di tecniche di Intelligenza Artificiale e di Machine Learning

2. IT Security Governance & Management Professional Level

CENNI AGLI STRUMENTI USABILI E CASI REALI DI IMPLEMENTAZIONE/ATTUAZIONE

- Gli strumenti: cenni alle soluzioni proprietarie disponibili sul mercato ed a quelle open
- Esempi di attuazione in strutture organizzative di grandi e di medio-piccole dimensioni (su diretta esperienza del docente)

Analisi del valore del SI

- Che cosa è a che cosa serve
- Esempio di strumento per effettuarla in maniera semplificata con casi reali anche nelle PMI
- Esempi di calcolo di del valore dell'ICT "as is" e "to be" con lo strumento di Malabo

I POSSIBILI FINANZIAMENTI PER IL SI E LA SUA SICUREZZA DIGITALE

- La leva della trasformazione digitale
- I finanziamenti nazionali e a livello regionale/provinciale
- I finanziamenti dai progetti europei
- I finanziamenti con il PNRR

MITC-003-1.0 - Governance Professional Level

3. ISO 27001

Obiettivi: interrelazioni tra le norme UNI EN ISO/IEC 27001:2022, ISO/IEC 27006, UNI EN ISO 19011:2018 e prescrizione aggiuntive ACCREDIA applicabili; approccio per processi per la tutela delle informazioni e la sicurezza dei sistemi informatici aziendali; principi delle normative di riferimento; approccio critico al Sistema di Information Security Management Systems (ISMS); metodologie e tecniche di auditing; pianificazione e conduzione di un Audit secondo la normativa di riferimento in vigore e preparazione del Rapporto di Audit, gestione delle NC; concetti base dei dispositivi , dei sistemi informatici e delle reti; aspetti relativi all'area legale connessi all'ICT.

Modulo 1 – UNI CEI EN ISO/IEC 27001:2022 – ISO/IEC 27006:2020

UNIT 1

- Introduzione all'universo ISO e Introduzione alla sicurezza delle informazioni
- Requisito 4: Contesto dell'organizzazione
- Requisito 5: Leadership
- Requisito 6: Pianificazione
- Requisito 7: Supporto
- Requisito 8: Attività operative
- Requisito 9: Valutazione delle prestazioni
- Requisito 10: Miglioramento

UNIT 2 – ANNEX

- Punto 5 - Controlli organizzativi
- Punto 6 - Controlli sul personale
- Punto 7 - Controlli fisici
- Punto 8 - Controlli tecnologici
- Controllo degli accessi

UNIT 3 – ISO/IEC 27006:2020

- Requisiti generali
- Requisiti strutturali
- Requisiti delle risorse
- Requisiti informativi
- Requisiti di processo
- Requisiti del sistema di gestione per gli organismi di certificazione
- Annex A-B-C-D

MITC-003-1.0 - Governance Professional Level

3. ISO 27001

Modulo 2 - UNI EN ISO 19011:2018

UNIT 1 - UNI EN ISO 19011:2018 - LINEE GUIDA PER AUDIT DI SISTEMI DI GESTIONE

- Definizione degli obiettivi del programma di audit
- Determinazione e valutazione dei rischi e delle opportunità del programma di audit
- Definizione del programma di audit
- Attuazione del programma di audit
- Monitoraggio del programma di audit
- Riesame e miglioramento del programma di audit
- Conduzione di un audit
- Avvio dell'audit
- Preparazione delle attività di audit
- Conduzione delle attività di audit
- Preparazione e distribuzione del rapporto di audit
- Chiusura dell’audit
- Conduzione delle azioni successive all'audit (follow-up)
- Competenza e valutazione degli auditor
- Determinazione della competenza degli auditor
- Definizione dei criteri di valutazione dell'auditor
- Selezione del metodo appropriato di valutazione dell'auditor
- Conduzione della valutazione dell'auditor
- Mantenimento e miglioramento della competenza di auditor

MITC-003-1.0 - Governance Professional Level

3. ISO 27001

Modulo 2 - UNI EN ISO 19011:2018

UNI 2 - UNI CEI EN ISO/IEC 17021-1:2015

- Principi di imparzialità, competenza e responsabilità
- Approccio basato al rischio
- Confidenzialità
- Problematiche e responsabilità legali
- Gestione dell'imparzialità
- Requisiti per le risorse
- Determinazione delle competenze
- Processi di valutazione
- Requisiti informativi
- Attività di pre-certificazione (programma di audit, tempi di audit, gruppo di audit)
- Tipologia di Audit (iniziale, sorveglianza, rinnovo)
- Documentazione di audit

MITC-003-1.0 - Governance Professional Level

4.CompTia Cloud Essentials

Obiettivi: Comprendere in maniera adeguata i principi del cloud; Identificare i concetti di Cloud Networking e Cloud Storage; Affrontare un momento di valutazione cloud con relativi studi di fattibilità; Evidenziare gli aspetti chiave nell'adozione cloud nelle aziende; Comprendere gli aspetti tecnici del mondo cloud e comprendere il ruolo di DevOps negli ambienti cloud; Comprendere i principi delle integrazioni e del provisioning; Identificare l'importanza della conformità nel cloud con riferimento a normativi e standard internazionali.

PRINCIPI E PROGETTAZIONE DEL CLOUD

COMPRENDERE I PRINCIPI DEL CLOUD

- Virtualizzazione
- Modelli di servizio
- Modelli di distribuzione
- Caratteristiche del cloud
- Modello di responsabilità condivisa

ESPLORARE LA PROGETTAZIONE CLOUD

- Ridondanza e alta disponibilità
- Disaster Recovery

RETE E ARCHIVIAZIONE NEL CLOUD

COMPRENDERE I CONCETTI DI RETE NEL CLOUD

- Reti: una breve introduzione
- Connessione al cloud
- Servizi di rete nel cloud

MITC-003-1.0 - Governance Professional Level

4.CompTia Cloud Essentials

COMPRENDERE LE TECNOLOGIE DI STORAGE NEL CLOUD

- Come funziona lo storage nel cloud
- Provider di storage basato sul cloud
- Terminologia dello storage nel cloud
- Reti per la distribuzione dei contenuti (CDN – Content Delivery Networks)

VALUTARE LE ESIGENZE CLOUD ATTRAVERSO LA CLOUD ASSESSMENT

- Raccolta dei requisiti attuali e futuri
- Utilizzo dei baseline
- Svolgimento di uno studio di fattibilità
- Conduzione di un'analisi dei gap
- Utilizzo dei report
- Comprendere i benchmark
- Creazione di documentazione e diagrammi

COMPRENDERE I SERVIZI CLOUD

- Gestione delle identità e degli accessi (IAM – Identity Access Management)
- Applicazioni cloud-native
- Analisi dei dati
- Marketing digitale
- Ambienti autonomi
- Internet of Things (IoT)
- Blockchain
- Servizi in abbonamento
- Collaborazione
- Infrastruttura desktop virtuale (VDI)
- Self-service

4.CompTia Cloud Essentials

INTERAGIRE CON I FORNITORI CLOUD

COMPRENDERE I CONCETTI AZIENDALI E FINANZIARI

- Spese e costi
- Modelli di licenza
- Capitale umano
- Servizi professionali

RICERCARE E VALUTARE I FORNITORI CLOUD

- Raccolta delle informazioni
- Esecuzione di valutazioni
- Negoziazione di contratti e fatturazione

SCEGLIERE UN APPROCCIO DI MIGRAZIONE

- Principi di migrazione
- Lift and Shift (trasferimento diretto)
- Rip and Replace (sostituzione completa)
- Migrazioni ibride e graduali

GESTIONE E OPERAZIONI TECNICHE

SPIEGARE GLI ASPETTI DELLE OPERAZIONI IN AMBIENTE CLOUD

- Gestione dei dati
- Disponibilità
- Risorse "usa e getta" (disposable resources)
- Monitoraggio e visibilità
- Ottimizzazione

MITC-003-1.0 - Governance Professional Level

4.CompTia Cloud Essentials

SPIEGARE DEVOPS NEGLI AMBIENTI CLOUD

- Provisioning (approvvigionamento delle risorse)
- Integrazione continua / Distribuzione continua (CI/CD)
- Test in ambienti di Quality Assurance (QA)
- Gestione della configurazione
- Integrazione tramite API

PIANIFICAZIONE FINANZIARIA DELLE RISORSE CLOUD

- Storage (archiviazione)
- Rete
- Calcolo (risorse computazionali)
- Chargeback (attribuzione dei costi)
- Manutenzione
- Istanze
- Tipi di licenze
- Quantità di licenze

GOVERNANCE E RISCHI

RICONOSCERE I CONCETTI DI GESTIONE DEL RISCHIO RELATIVI AI SERVIZI CLOUD

- Valutazione del rischio
- Risposta al rischio
- Documentazione
- Vendor Lock-in (dipendenza dal fornitore)
- Portabilità dei dati

MITC-003-1.0 - Governance Professional Level

4.CompTia Cloud Essentials

SPIEGARE LE POLICY O LE PROCEDURE

- Procedure operative standard (SOP – Standard Operating Procedures)
- Gestione delle modifiche (Change Management)
- Gestione delle risorse
- Policy di sicurezza e di accesso e controllo
- Policy specifiche per reparto
- Policy di comunicazione

CONFORMITÀ E SICUREZZA NEL CLOUD

IDENTIFICARE L'IMPORTANZA E GLI IMPATTI DELLA CONFORMITÀ NEL CLOUD

- Sovranità dei dati
- Aspetti normativi
- Requisiti specifici del settore
- Standard internazionali
- Certificazioni

SPIEGARE I RISCHI, LE MISURE E I CONCETTI DI SICUREZZA NELLE OPERAZIONI CLOUD

- Minacce
- Vulnerabilità
- Valutazioni della sicurezza
- Sicurezza dei dati
- Sicurezza delle applicazioni e dell'infrastruttura

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

Obiettivi: Valutare lo stato di sicurezza di un ambiente aziendale e consigliare e implementare soluzioni di sicurezza appropriate; Monitorare e proteggere gli ambienti ibridi, inclusi cloud, dispositivi mobili e IoT; Operare con consapevolezza delle leggi e delle politiche applicabili, inclusi i principi di governance, rischio e conformità; Identificare, analizzare e rispondere a eventi e incidenti di sicurezza

MASTERING SECURITY BASIC

- Understanding core security goals
  - Security scenarios
    - Ensure confidentiality
    - Provide integrity
    - Increase availability
  - Resource availability versus security constraints
- Introducing basic risk concepts
- Selecting effective security controls
  - Control categories
    - Technical controls
    - Managerial controls
    - Operational controls
    - Physical controls
  - Control types
    - Preventive controls
    - Deterrent controls
    - Detective controls
    - Corrective controls
    - Directive controls
  - Combining control categories and types

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- Logging and monitoring
  - Operating system/endpoint logs
    - Windows logs
    - Linux logs
  - Network logs
    - Firewall logs
    - IDS/IPS logs
    - Packet captures
  - Application logs
  - Metadata
- Centralized logging and monitoring
  - SIEM system
  - Syslog

OBJECTIVE COVERED

- Compare and contrast various types of security controls
  - Categories (technical, managerial, operational, physical)
  - Control types (preventive, deterrent, detective, corrective, compensating, directive)
- Summarize fundamental security concepts
  - Confidentiality, integrity, and availability (CIA)
- Explain the purpose of mitigation techniques used to secure the enterprise
  - Monitoring
  - Least privilege

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- Given a scenario, apply security principles to secure enterprise infrastructure
  - Selection of effective controls
- Given a scenario, apply common security techniques to computing resources
  - Monitoring
- 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)
- Given a scenario, modify enterprise capabilities to enhance security
  - User Behavior Analytics (UBA)
- 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)

UNDERSTANDING IDENTITY AND ACCESS MANAGEMENT

- Exploring authentication management
  - Comparing identification and AAA
- Comparing authentication factors
  - Something you know
  - Something you have
  - Something you are
  - Two-factor and multifactor authentication
  - Passwordless authentication
- Authentication log files

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- Managing accounts
  - Credential policies and account types
  - Privileged access management
  - Requiring administrators to use two accounts
  - Prohibiting shared and generic accounts
  - Deprovisioning
  - Time-based logins
  - Account audits
- Comparing authentication services
  - Single sign-on
  - LDAP
  - SSO and a federation
    - SAML
    - SAML and authorization
    - Oauth
- Authorization models
  - Role-based access control
    - Using roles based on jobs and functions
    - Documenting roles with a matrix
    - Establishing access with group-based privileges
  - Role-based access control
  - Discretionary access control
    - Filesystem permissions
    - SIDs and DACLs
  - Mandatory access control
    - Labels and lattice
    - Establishing access
  - Attribute-based access control
- Analyzing authentication indicators

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

OBJECTIVE COVERED

- Summarize fundamental security concepts
  - Authentication, authorization, and accounting (AAA) (Authenticating people, Authenticating systems, Authorization models)
- 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)
- Explain the purpose of mitigation techniques used to secure the enterprise
  - Access control (Access Control List (ACL), permissions)
- Given a scenario, modify enterprise capabilities to enhance security
  - Operating system security (SElinux)
- 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)

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- 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)

EXPLORING NETWORK TECHNOLOGIES AND TOOLS

- Reviewing basic networking concept
  - OSI model
  - Basic networking protocols
  - Implementing protocols for use cases
    - Data in transit use cases
    - Email and web use cases
    - Directory use cases
    - Voice and video use cases
    - Remote access use cases
    - Time synchronization use cases
    - Network address allocation use cases
    - Domain name resolution use cases
- Understanding basic network infrastructure
  - Switches
    - Hardening switches
  - Routers
    - Hardening routers
  - Simple Network Management Protocol
  - Firewalls
    - Host-based firewalls
    - Network-based firewalls
  - Failure modes

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- Implementing network designs
  - Security zones
    - Screened subnet
    - Network address translation gateway
    - Physical isolation and air gasp
    - Logical separation and segmentation
  - Network appliances
  - Proxy servers
    - Caching content for performance
    - Content filtering
    - Reverse proxy
  - Unified threat management
  - Jump server
- Zero trust
  - Control plane vs. Data plane
  - Secure access service edge

OBJECTIVE COVERED

- 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)
- Explain the purpose of mitigation techniques used to secure the enterprise
  - Isolation
  - Hardening techniques (host-based firewall)

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- Compare and contrast security implications of different architecture model
  - Network infrastructure (physical isolation, air-gapped, logical segmentation)
- 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))
- Compare and contrast concepts and strategies to protect data
  - Methods to secure data (segmentation)
- Given a scenario, apply common security techniques to computing resources.
  - Hardening targets (switches, routers)
- Explain security alerting and monitoring concepts and tools
  - Simple Network Management Protocol (SNMP) traps
- 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)

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

SECURING YOUR NETWORK

- Exploring advanced security devices
  - Understanding idss and ipss
    - HIDS
    - NIDS
    - Sensor and collector placement
    - Detection methods
    - Data sources and trends
    - Reporting based on rules
    - Alert response and validation
  - IPS versus IDS in line versus passive
  - Honeypots
  - Honeynets
  - Honeyfile
  - Honeytokens
- Securing wireless networks
  - Reviewing wireless basics
    - Band selection and channel overlaps
    - MAC filtering
- Site surveys and heat maps
- Access point installation considerations
- Wireless cryptographic protocols
  - WAP2 and CCMP
  - Open, psk, and enterprise modes
  - WPA3 and simultaneous authentication of equals

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- Authentication protocols
- IEEE 802.1x security
- Controller and access point security
- Captive portals

- Understanding wireless attacks
  - Disassociation attacks
  - Wi-fi protected setup
  - Rogue access point
  - Evil twin
  - Jamming attacks
  - IV attacks
  - Near field communication attacks
  - RFID attacks
    - Wireless replay attacks
    - War driving and war flying
- Using VPNs for remote access
  - VPNs and VPN concentrators
  - Remote access VPN
  - IPSEC as a tunneling protocol
  - SSL/TLS as a tunneling protocol
  - Split tunnel versus full tunnel
  - Site-to-site VPNs
  - Always-on SPN
  - L2TP as a tunneling protocol
  - HTML5 VPN portal
- Network access control
  - Host health checks
  - Agent versus agentless NAC
- Authentication and authorization methods
  - PAP

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- CHAP
- RADIUS
- TACACS+
- AAA protocols

Objective covered

- Summarize fundamental security concepts
  - Deception and disruption technology (honeypot, honeynet, honeyfile, honeytoken)
- Explain various types of vulnerabilities
  - Zero-day
- Given a scenario, analyze indicators of malicious activity
  - Physical attacks (radio frequency identification (RFID) cloning)
  - Network attacks (wireless)
- 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)
- 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)
- Explain security alerting and monitoring concepts and tools
  - Agent / agentless
  - Alerting response and remediation / validation (quarantine)
- Given a scenario, modify enterprise capabilities to enhance security
  - IDS/IPS (trends, signature)
  - Network Access Control (NAC)

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

SECURING HOSTS AND DATA

- Virtualization
- Thin clients and virtual desktop infrastructure
- Containerization
- VM escape protection
- VM sprawl avoidance
- Resource reuse
- Replication
- Snapshots

- Implementing secure system
  - Endpoint security software
  - Hardening workstations and servers
  - Configuration enforcement
  - Secure baseline and integrity measurements
  - Using master images for baseline configurations
  - Patching and patch management
  - Change management
  - Application allow and block lists
  - Disk encryption
  - Boot integrity
    - Boot security and uefi
    - Trusted platform module
    - Hardware security module
  - Decommissioning and disposal
- Protecting data
  - Data loss prevention
  - Removable media
  - Protecting confidentiality with encryption
  - Database security
  - Protecting data in use
- Summarizing cloud concepts
  - Cloud delivery models
    - Software as a service
    - Platform as a service
    - Infrastructure as a service

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- Cloud deployment models
  - Multi-cloud systems
- Application programming interfaces
- Microservices and apis
- Managed security service provider
- Cloud service provider responsabilities
- Cloud security considerations
- On-premises versus off-premises
  - On-premises
  - Off-premises
- Hardening cloud enviroments
  - Clooud access security broker
  - Cloud-based dlp
  - Next-generation secure web gateway
  - Cloud firewall considerations
  - Infrastructure as code
  - Software-defined networking
  - Edge and fog computing
- Deploying mobile devices securely
  - Mobile device deployment models
  - Connection methods and receivers
    - Mobile device management
  - Hardening mobile devices
    - Unauthorized software
    - Hardware control
    - Unauthorized connections
- Exploring embedded systems
  - Understanding internet of things
  - Ics and scada systems
  - Embedded systems components
  - Hardening specialized systems
  - Embedded system constraints

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

Objective covered

- 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
- 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)
- 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)
- 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

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- 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, computer

- Compare and contrast concepts and strategies to protect data
  - Geolocation
- 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)
- Explain security alerting and monitoring concept and tools
  - Antivirus
  - DLP (Data Loss Prevention)
- Given a scenario, modify enteprise capabilities to enhance security
- DLP
- Endpoint Detection and Response (EDR)
- eXtended Detection and Response (XDR)

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

COMPARING THREATS, VULNERABILITIES AND COMMON ATTACKS

- Understanding threat actors
  - Threat actor types
  - Attacker attributes
  - Threat actor motivations
  - Threat vectors and attack surfaces
  - Shadow it
- Determining malware types
  - Viruses
  - Worms
  - Logic bombs
  - Trojans
  - Remote access trojan
  - Keyloggers
  - Spyware
  - Rootkit
  - Ransomware
  - Bloatware
  - Potential indicators of a malware attack
- Recognizing common attacks
  - Social engineering and human vectors
    - Impersonation
    - Shoulder surfing
    - Disinformation
    - Tailgating and access control vestibules
    - Dumpster diving
    - Watering hole attacks
    - Business email compromise
    - Typosquatting
    - Brand impersonation
    - Eliciting information
    - Pretexting
  - Message-based attacks
    - Spam
    - Spam over instant messaging
    - Phishing

1. Sicurezza Informatica e Security Manager | CompTIA Security+

        - Whaling
        - Vishing
        - Smishing
    - One click lets them in
- Blocking malware and other attacks
    - Spam filters
    - Antivirus and anti-malware software
        - Signature-based detection
        - Heuristic-based detection
        - File integrity monitors
    - Why social engineering works
        - Authority
        - Intimidation
        - Consensus
        - Scarcity
        - Urgency
        - Familiarity
        - Trust
    - Threat intelligence sources
    - Research sources

Objective covered

- 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)

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- 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)
- Given a scenario, analyze indicators of malicious activity
  - Malware attacks (ransomware, trojan, worm, spyware, bloatware, virus, keylogger, logic bomb, rootkit)
  - Malicious code
- Explain various activities associated with vulnerability management
  - Threat feed (Open Source INTelligence OSINT, proprietary/third-party, information-sharing organization, dark web)
- Given a scenario, modify enterprise capabilities to enhance security
  - File integrity monitoring

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

PROTECTING AGAINST ADVANCED ATTACKS

- Identifying network attacks
  - Denial of Service attacks
    - Syn flood attacks
  - Forgery
  - On-path attacks
  - Secure Sockets Layer stripping
  - DNS attacks
    - DNS poisoning attacks
    - Pharming attacks
    - Url redirection
    - Domain hijacking
    - DNS filtering
    - DNS log files
  - Replay attacks
- Summarizing secure coding concepts
  - Input validation
    - Client-side and server-side input validation
    - Other input validation techniques
  - Avoiding race conditions
  - Proper error handling
  - Code obfuscation
  - Software diversity
    - Outsourced code development
    - Data exposure
    - HTTP headers
    - Secure cookie
    - Code signing

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

    - Analyzing and reviewing code
    - Software version control
    - Secure development enviroment
    - Database concepts
        - SQL queries
    - Web server logs
- Other application attacks
    - Memory vulnerabilities
        - Memory leak
        - Buffer overflows and buffer attacks
        - Integer overflow
    - Other injection attacks
        - DLL injection
        - LDAP injection
        - XML injection
    - Directory traversal
    - Cross-site scripting
- Automation and orchestration for secure operations
- Automation and scripting use cases
    - Benefits of autmations and scripting

Objective covered

- 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)

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- 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)
- Given a scenario, apply common security techniques to computing resources
  - Application security (input validation, secure cookies, static code analysis, code signing)
  - Sandboxing
- 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)

USING RISK MANAGEMENT TOOLS

- Understanding risk management
  - Threats
  - Risk identification
  - Risk types
  - Vulnerabilities
  - Risk managemnt strategies
    - Risk assessment types
    - Risk analysis
    - Supply
    - Chain risks
- Comparing scanning and testing tools
  - Checking for vulnerabilities

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

        - Network scanners
        - Vulnerability scanning
        - Credentialed vs. Non-credentialed scans
        - Configuration review
    - Penetration testing
        - Rules of engagement
        - Reconnaissance
        - Footprinting versus fingerprinting
        - Initial exploitation
        - Persistence
        - Lateral movement
        - Privilege escalation
        - Pivoting
        - Known, unknown and partially known testing enviroments
        - Cleanup
- Responsible disclosure programs
- System and process audits
- Intrusive versus non-intrusive testing
    - Responding to vulnerabilities
        - Remediating vulnerabilities
        - Validation of remediation
- Capturing network traffic
        - Packet capture and replay
    - TCPreplay and TCPdump
    - Netflow
- Understanding frameworks and standards
    - ISO standards
    - Industry-specific frameworks.
    - NIST frameworks
        - NIST risk management framework
        - NIST cybersecurity framework

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

    - Reference architecture
    - Benchmarks and configuration guides
- Audits and assessments

Objective covered

- Summarize fundamental security concepts
    - Gap analysis
- Explain various type of vulnerabilities
    - Supply chain (service provider, hardware provider, software provider)
- 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
- Explain security alerting and monitoring concepts and tools
    - Security Content Automation Protocol (SCAP)
    - Benchmarks
    - Netflow
    - Vulnerability scanners
- Explain elements of the risk management process
    - Risk identification
    - Risk assessment (ad hoc, recurring, one-time, continuous)

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

    - 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
- 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)

IMPLEMENTING CONTROLS TO PROTECT ASSETS

- Comparing physical security controls
    - Access badges
    - Increasing security with personnel
    - Monitoring areas with video surveillance
    - Sensors
    - Fencing, lighting and alarms
    - Securing access with barricades
    - Access control vestibules
    - Asset management
        - Hardware asset management
        - Software asset management
        - Data asset management
    - Platform diversity
    - Physical attacks
        - Card skimming and card cloning
        - Brute force attacks
        - Enviromental attacks

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- Adding redundancy and fault tolerance
  - Single Point of Failure
  - Disk redundancies
    - Raid-0
    - Raid-1
    - Raid-5 and raid-6
    - Raid-10
  - Server redundancy and high availability
    - Active/ active load balancers
    - Active/ passive load balancers
  - NIC teaming
  - Power redundancies
- Protecting data with backups
  - Backup media
  - Online versus offline backups
    - Full backups
    - Recovering a full backup
    - Differential backups
    - Order of recovery for a full/differential backup set
    - Incremental backups
    - Order of recovery for a full/differential backup set
    - Snapshot and image backups
    - Replication and journaling
    - Backup frequency
    - Testing backups
  - Backup and geographic considerations
- Comparing business continuity elemnts
  - Business impact analysis concepts
    - Site risk assessment
    - Impact
    - Recovery Time Objective

1. Sicurezza Informatica e Security Manager | CompTIA Security+

        - Recovery Point Objective
        - Comparing MTBF and MTTR
    - Continuity of operations planning
        - Site resiliency
        - Restoration order
    - Disaster recovery
    - Testing plans with exercises
        - Tabletop exercises
        - Simulations
        - Parallel processing
        - Fail over tests
- Capacity planning

Objective covered

- 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)
- Compare and contrast concepts and strategies to protect data
    - General data considerations (data sovereignty)
- 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))

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- 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)

UNDERSTANDING CRYPTOGRAPHY AND PKI

- Introducing cryptography concepts
- Providing integrity with hashing
  - Hash versus checksum
  - MD5
  - Secure hash algorithms
  - Hmac
  - Hashing files
  - Hashing messages
  - Using hmac
  - Hashing passwords
  - Undertanding hash collisions
- Understanding password attacks
  - Dictionary attacks
  - Brute force attacks
  - Password spraying attacks
    - Pass the hash attacks
  - Birthday attacks
  - Rainbow table attacks
  - Salting passwords
  - Key stretching

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- Providing confidentiality with encryption
  - Symmetric encryption
  - Block versus stream ciphers
  - Common symmetric algorithms
    - AES
    - 3DES
    - Blowfish and twofish
  - Asymmetric encryption
    - Key exchange
    - The reyburn box
  - Certificates
  - Ephemeral keys
  - Elliptic curve cryptography
  - Key lenght
  - Obfuscation
    - Steganography
    - Tokenization
    - Masking
- Using cryptographic protocols
  - Protecting email
    - Signing email with digital signatures
    - Encrypting email
    - S/mime
  - HTTPS transport encryption
    - TLS versus SSL
    - Encrypting HTTPS traffic with TLS
    - Downgrade attacks on weak implementations
  - Blockchain
  - Identifyng limitations
    - Resource versus security constraints
    - Speed and time
    - Size and computational overhead

1. Sicurezza Informatica e Security Manager | CompTIA Security+

        - Entropy
        - Predictability
        - Weak keys
        - Reuse
        - Plaintext attack
- Exploring PKI components
    - Certificate authority
    - Certificate trust models
    - Registration authority and CSRs
    - Online versus offline CAs
    - Updating and revoking certificates
    - Certificate revocation list
    - Validating a certificate
    - Certificate pinning
    - Key escrow
    - Key management
    - Comparing certificate types
    - Comparing certificate formats

Objective covered

- Summarize fundamental security concepts
    - Non-repudation
- 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

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- 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)

- 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)

IMPLEMENTING POLICIES TO MITIGATE RISKS

- Change management
  - Business processes
  - Technical implications
  - Documentation and version control
- Protecting data
  - Understanding data types
  - Classifying data types
  - Securing data
  - Data retention
  - Data sanitization
- Incident response
  - Incident response plan
    - Communication plan
  - Incident response process
  - Incident response training and testing
  - Threat hunting
  - Understanding digital forensics
    - Acquisition and preservation
    - Legal holds and electronic discovery

1. Sicurezza Informatica e Security Manager | CompTIA Security+

        - Admissibility of documentation and evidence
        - Reporting
    - Understanding SOAR
        - Playbooks
        - Runbooks
- Security governance
    - Governance structures
    - External considerations
    - Security policies
    - Security standards
    - Security procedures
    - Security guidelines
    - Data governance
    - Data roles
    - Monitoring and revision
- Third-party risk management
    - Supply chain and vendors
    - Vendor assessment
    - Vendor selection
    - Vendor agreements
- Security compliance
    - Compliance monitoring and reporting
    - Privacy
    - Data inventory and retention
- Security awareness
    - Computer-based training
    - Phishing campaigns
    - Recognizing anomalous behavior
    - User guidance and training
    - Awareness program development and execution

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

Objective covered

- 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
- 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)
- explain the security implications of proper hardware, software, and data asset management
  - Disposal/decommissioning (sanitization, destruction, certification, data retention)
- explain various activities associated with vulnerability management
  - Application security (static analysis, dynamic analysis, package monitoring)
- 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)

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

- 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)
- 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
- 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)

MITC-004-1.0 - IT Security Core Level

1. Sicurezza Informatica e Security Manager | CompTIA Security+

    - 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

MITC-004-1.0 - IT Security Core Level

2. Indagini Digitali Forensi

Obiettivi: fornire delle solide fondamenta per intraprendere attività nel mondo dell'investigazione digitale, materia in continua trasformazione e divenire: trovare files nascosti, recuperare dati cancellati e duplicare informazioni integre e non ripudiabili, anche attraverso l'utilizzo di tools e l'analisi di casi studio reali.

1. Panoramica sulle Best Practices Computer forensics;
1.1 – L'immodificabilità della fonte di prova ed il metodo scientifico;
1.1.1 Il sopralluogo informatico;
1.2 - Analisi live e post mortem (i perché, pro e contro);
1.3 - Identicità della prova;
1.3.1 - hash, cosa sono ed il problema della collisione;
1.3.2 - catena custodia;
1.3.3 - ripetibilità delle operazioni;
1.4 – Elementi di OSINT.
2. Gli strumenti della C.F. - open source e commerciale.
3. Write blocker ed hardware forense.
3. 1 Le quattro fasi (Identificazione, acquisizione, analisi, reporting) in pratica.
4. GNU/Linux per la C.F. (uso della distro C.A.I.N.E. http://www.caine-live.net live distro forense).
5. Cenni su casi reali.
6. Panoramica sulla mobile forensics: tecniche di acquisizione ed analisi sui cellulari/tablet.
7. Cenni sulla legge 48/2008, art. 359 e 360 c.p.p. e DPR 115/02.
8. Live analysis ed acquisizione su un sistema acceso.
9. Elementi di mobile forensics.
10. Il futuro della D.F. e cenni sull'Intelligenza Artificiale
11. I miti e le leggende.

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Obiettivi: Pianificare e definire l'ambito di un Penetration test. Comprendere i requisiti legali e di conformità. Eseguire la scansione delle vulnerabilità e i PT utilizzando strumenti e tecniche appropriate analizzandone i risultati. Produrre report con l'analisi di quanto si è analizzato, le metodologie e consigli sulle eventuali remediation da attuare.

Professional Conduct and Penetration Testing

Exam Objectives Covered:

- Summarize pre-engagement activities.

Topics:

- Professional Conduct and Penetration Testing
- What Is Penetration Testing?
- Ethics, Legal, and Compliance Considerations of Penetration Testing
- Importance and Examples of Documentation
- Scoping and Authorization
- Overview of the PenTest Report
- Live Lab: Exploring the Lab Environment

Collaboration and Communication

Exam Objectives Covered:

- Explain collaboration and communication activities.

Topics:

- Collaboration and Communication
- Collaboration and Communication Overview
- PenTest Team Roles and Responsibilities
- Communicating with Clients and Team Members
- Peer Review
- Stakeholder Alignment

- Root Cause Analysis
- Escalation Path
- Secure Distribution
- Articulation of Risk, Severity, and Impact
- Goal Reprioritization
- Business Impact Analysis
- Client Acceptance

Testing Frameworks and Methodologies

Exam Objectives Covered:

- Compare and contrast testing frameworks and methodologies.

Topics:

- Testing Frameworks and Methodologies
- Testing Frameworks and Methodologies Overview
- Open Source Security Testing Methodology Manual (OSSTMM)
- Council of Registered Ethical Security Testers (CREST)
- Penetration Testing Execution Standard (PTES)
- MITRE ATT&CK
- Open Web Application Security Project (OWASP) Top 10
- OWASP Mobile Application Security Verification Standard (MASVS)
- Purdue Model
- Threat Modeling Frameworks

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Introduction to Scripting for Penetration Testing

Exam Objectives Covered:

- Summarize pre-engagement activities.1.2 Given a scenario, modify scripts for reconnaissance and enumeration.

Topics:

- Introduction to Scripting for Penetration Testing
- Scripting Languages
- Bash Shell and Bash Script
- Python
- Powershell
- Use of Libraries, Functions, and Classes
- Logic Constructs
- Create Logic Constructs

Define the Scope

Exam Objectives Covered:

- Summarize pre-engagement activities.

Topics:

- Define the Scope
- Regulations, Frameworks, and Standards
- Rules of Engagement
- Agreement Types
- Target Selection

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Compare Types of Assessments
Exam Objectives Covered:

- Summarize pre-engagement activities.

Topics:

- Compare Types of Assessments
- Types of Assessments Overview
- Web and Application Assessments
- Network Assessments
- Activity: Assess Environmental Considerations
- Mobile Assessments
- Cloud Assessments
- Wireless Assessments
- IoT Devices and Penetration Testing
- Information Technology Versus Operational Technology

Utilize the Shared Responsibility Model
Exam Objectives Covered:

- Summarize pre-engagement activities.

Topics:

- Utilize the Shared Responsibility Model
- The Shared Responsibility Model Overview
- Hosting Provider Responsibilities
- Customer Responsibilities
- Penetration Tester Responsibilities
- Third-Party Responsibilities

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Identify Legal and Ethical Considerations
Exam Objectives Covered:

- Summarize pre-engagement activities.

Topics:

- Identify Legal and Ethical Considerations
- Authorization Letters
- Mandatory Reporting Requirements
- Risk to the Penetration Tester
- Documenting Pre-Engagement Activities

Information Gathering Techniques
Exam Objectives Covered:

- Given a scenario, apply information gathering techniques.2.3 Given a scenario, modify scripts for reconnaissance and enumeration.

Topics:

- Information Gathering Techniques
- Active and Passive Reconnaissance
- Tools for Reconnaissance
- Open-Source Intelligence (OSINT)
- Using Shodan
- Previously Breached Password Lists
- Network Reconnaissance
- Basics of Scanning
- Perform Recon with Nmap
- Certificate Transparency Logs
- Information Disclosure
- Search Engine Analysis/Enumeration
- Network Sniffing
- Data Manipulation

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Host and Service Discovery Techniques

Exam Objectives Covered:

- Given a scenario, apply information gathering techniques.2.2 Given a scenario, apply enumerationtechniques. 2.3 Given a scenario, modify scripts for reconnaissance and enumeration.2.4 Given a scenario, use the appropriate tools for reconnaissance and enumeration.

Topics:

- Host and Service Discovery Techniques
- What Is Enumeration?
- Host Discovery
- Scripting with Nmap
- Activity: Scripting with Nmap
- Banner Grabbing
- Protocol Enumeration
- Service Discovery
- DNS Enumeration
- Operating System (OS) Fingerprinting
- Perform Enumeration with Nmap
- Live Lab: DNS Enumeration and Reconnaissance

Enumeration for Attack Planning

Exam Objectives Covered:

- Given a scenario, apply enumeration techniques.2.4 Given a scenario, use the appropriate tools for reconnaissance and enumeration.

Topics:

- Enumeration for Attack Planning
- Attack Path Mapping
- Manual Enumeration
- Simple Network Management Protocol
- Documenting Enumeration Activities
- Activity: Document Enumeration Activities

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Enumeration for Specific Assets
Exam Objectives Covered:

- Given a scenario, apply enumeration techniques.2.4 Given a scenario, use the appropriate tools for reconnaissance and enumeration.3.1 Given a scenario, conduct vulnerability discovery using various techniques.

Topics:

- Enumeration for Specific Assets
- Directory Enumeration
- User Enumeration
- Wireless Enumeration
- Permission Enumeration
- Secrets Enumeration
- Share Enumeration
- Web Application Firewall (WAF) Enumeration
- Perform a Decoy Scan
- Industrial Control Systems (ICS) Vulnerability Assessment
- Web Crawling/HTML Scraping

Vulnerability Discovery Techniques
Exam Objectives Covered:

- Given a scenario, conduct vulnerability discovery using various techniques.3.2 Given a scenario, analyze output from reconnaissance, scanning, and enumeration phases.

Topics:
Vulnerability Discovery Techniques
Tools for Vulnerability Discovery
Types of Scans
Container Scans
Application Scans
Scan for Cleartext Vulnerabilities

Penetration Test e Hacking Etico | CompTIA PenTest+

- Network Scans
- Activity: Scan Identified Targets
- Host-Based Scans
- Live Lab: Using Metasploit
- Secrets Scanning
- Wireless Scans
- Use aircrack-ng to Discover Hidden Networks
- Locate a Rogue Wireless Access Point
- Validate Scan, Reconnaissance, and Enumeration Results
- Applied Live Lab: Network Reconnaissance
- Scan for Linux Vulnerabilities

Analyzing Reconnaissance Scanning and Enumeration

Exam Objectives Covered:

- Given a scenario, analyze output from reconnaissance, scanning, and enumeration phases.

Topics:

- Analyzing Reconnaissance Scanning and Enumeration
- Public Exploit Selection
- Use Scripting to Validate Results

Physical Security Concepts

Exam Objectives Covered:

- Explain physical security concepts.

Topics:

- Physical Security Concepts
- Tailgating
- Site Surveys
- Universal Serial Bus (USB) Drops
- Badge Cloning
- Lock Picking
- Documenting Scanning and Identifying Vulnerabilities Activities
- Activity: Identify Physical Security Concepts

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Prepare and Prioritize Attacks
Exam Objectives Covered:

- Given a scenario, analyze output to prioritize and prepare attacks.

Topics:

- Prepare and Prioritize Attacks
- Target Prioritization
- High-Value Asset Identification
- Descriptors and Metrics
- End-of-Life Software and Systems
- Default Configurations
- Running Services
- Vulnerable Encryption Methods
- Defensive Capabilities
- Capability Selection
- Exploit Selection and Customization
- Documentation Procedures for Attacks
- Dependencies
- Consideration of Scope Limitations
- Activity: Customize Exploits
- Live Lab: Evaluate EOL Software & Systems
- Applied Live Lab: Exploiting Default Configurations with Responder

Scripting Automation
Exam Objectives Covered:

- Given a scenario, use scripting to automate attacks.

Topics:

- Scripting Automation
- Types of Scripting Automation
- PowerShell
- Bash
- Python
- Breach and Attack Simulation (BAS)
- Live Lab: Executing Scripts to Automate Tasks

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Web-based Attacks
Exam Objectives Covered:

- Given a scenario, perform web application attacks using the appropriate tools.

Topics:

- Web-based Attacks
- Web Application Attacks Overview
- Types of Web Application Attacks
- Tools for Performing Web Application Attacks
- Brute-Force Attack
- Collision Attack
- Directory Traversal
- Request Forgery Attacks
- Deserialization Attack
- Injection Attacks
- Activity: Injection Attacks
- Insecure Direct Object Reference
- Session Hijacking
- Arbitrary Code Execution
- File Inclusions
- API Abuse
- JSON Web Token (JWT) Manipulation
- Live Lab: Evaluating a Database Using SQLMap
- Live Lab: Exploiting Directory Traversal
- Live Lab: Performing XSS
- Live Lab: Abusing Insecure Direct Object References
- Live Lab: Performing Lateral Movement
- Live Lab: Performing RFI and LFI Exploitation

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Cloud-Based Attacks
Exam Objectives Covered:

- Given a scenario, perform cloud-based attacks using the appropriate tools.

Topics:

- Cloud-Based Attacks
- Cloud-Based Attacks Overview
- Types of Cloud-Based Attacks
- Tools for Performing Cloud-Based Attacks
- Metadata Service Attacks
- Access Management Misconfigurations
- Third-Party Integrations
- Resource Misconfiguration
- Activity: Conduct Resource Misconfiguration Attacks
- Logging Information Exposure
- Image and Artifact Tampering
- Supply Chain Attacks
- Workload Runtime Attacks
- Container Escape
- Trust Relationship Abuse
- Perform and Analyze a SYN Flood Attack

Perform Network Attacks
Exam Objectives Covered:

- Given a scenario, perform cloud-based attacks using the appropriate tools.

Topics:

- Perform Network Attacks
- Network Attack Types
- Tools for Performing Network Attacks
- Default Credentials
- On-Path Attack
- Certificate Services

Penetration Test e Hacking Etico | CompTIA PenTest+

- Misconfigured Services Exploitation
- Virtual Local Area Network (VLAN) Hopping
- Multihomed Hosts
- Relay Attack
- IDS Evasion
- Live Lab: Sniffing Network Traffic
- Applied Live Lab: Exploring the Power of Nmap NSE
- Live Lab: Discovering Vulnerabilities with Netcat
- Applied Live Lab: Performing a Relay Attack

Perform Authentication Attacks

Exam Objectives Covered:

- Given a scenario, perform authentication attacks using the appropriate tools.

Topics:

- Perform Authentication Attacks
- Authentication Attack Types
- Tools for Performing Authentication Attacks
- Multifactor Authentication (MFA) Fatigue
- Pass-the-Hash Attacks
- Pass-the-Ticket Attacks
- Pass-the-Token Attacks
- Kerberos Attacks
- Lightweight Directory Access Protocol (LDAP) Injection
- Dictionary Attacks
- Crack a Password with John the Ripper
- Brute-Force Attacks
- Mask Attacks
- Password Spraying
- Credential Stuffing
- OpenID Connect (OIDC) Attacks
- Security Assertion Markup Language (Saml) Attacks
- Live Lab: Cracking Passwords

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Perform Host-Based Attacks
Exam Objectives Covered:

- Given a scenario, perform host-based attacks using the appropriate tools.

Topics:

- Perform Host-Based Attacks
- Types of Host-Based Attacks
- Tools for Performing Host-Based Attacks
- Privilege Escalation
- Credential Dumping
- Circumventing Security Tools
- Clear Audit Policies
- Misconfigured Endpoints
- Payload Obfuscation
- User-Controlled Access Bypass
- Shell Escape
- Kiosk Escape
- Library Injection
- Process Hollowing and Injection
- Log Tampering
- Unquoted Service Path Injection
- Documenting Enterprise Attacks
- Applied Live Lab: Performing an On-Path (AiTM) Attack
- Live Lab: Performing Privilege Escalation
- Live Lab: Implementing Payload Obfuscation
- Live Lab: Performing SQL Injection
- Live Lab: Investigating with Evil-WinRM
- Live Lab: Exploiting LOLBins
- Live Lab: Implementing Credential Dumping

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Wireless Attacks
Exam Objectives Covered:

- Given a scenario, perform wireless attacks using the appropriate tools.

Topics:

- Wireless Attacks
- Types of Wireless Attacks
- Tools for Performing Wireless Attacks
- Activity: Explore Wireless Tools
- Wardriving
- Bluetooth
- Evil Twin Attack
- Signal Jamming
- Protocol Fuzzing
- Packet Crafting
- Deauthentication
- Captive Portal
- Wi-Fi Protected Setup (WPS) and Personal Identification (PIN) Attack

Social Engineering Attacks
Exam Objectives Covered:

- Given a scenario, perform social engineering attacks using the appropriate tools.

Topics:

- Social Engineering Attacks
- Types of Social Engineering Attacks
- Tools for Performing Social Engineering Attacks
- Phishing, Whaling, Spear phishing, and Smishing
- Social Engineering Techniques for Gathering Information
- Watering Hole
- Credential Harvesting
- Live Lab: Performing Social Engineering using SET

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Specialized System Attacks
Exam Objectives Covered:

- Explain common attacks against specialized systems.

Topics:

- Specialized System Attacks
- Types of Specialized System Attacks
- Tools for Performing Specialized System Attacks
- Mobile Attacks
- AI Attacks
- Operational Technology (OT)
- Radio-Frequency Identification (RFID) and Near-Field Communication (NFC)
- Bluejacking
- Conducting Specialized Penetration Testing Attacks

Establish and Maintain Persistence
Exam Objectives Covered:

- Given a scenario, perform tasks to establish and maintain persistence.

Topics:

- Establish and Maintain Persistence
- Principals of Establishing and Maintaining Persistence
- Scheduled Tasks/cron Jobs
- Service Creation
- Reverse and Bind Shells
- Add New Accounts
- Obtain Valid Account Credentials
- Registry Keys
- Command and Control (C2) Frameworks
- Backdoor
- Activity: Maintain Persistence
- Create a Backdoor with Metasploit

Penetration Test e Hacking Etico | CompTIA PenTest+

- Rootkit
- Browser Extensions
- Tampering Security Controls
- Live Lab: Configuring Reverse and Bind Shells
- Live Lab: Establishing Persistence and Other Post-Exploitation Activities

Move Laterally through Environments

Exam Objectives Covered:

- Given a scenario, perform tasks to move laterally throughout the environment.

Topics:

- Move Laterally through Environments
- Lateral and Horizontal Movement
- Scan for Open Ports from a Remote Computer
- Techniques for Moving Laterally through Environments
- Tools for Moving Laterally through Environments
- Pivoting
- Relay Creation
- Enumeration
- Perform Enumeration of MSSQL with Metasploit
- Service Discovery
- Perform a Scan Using Zenmap
- Bypass Windows Firewall
- Window Management Instrumentation (WMI)
- Window Remote Management (WinRM)

Staging and Exfiltration

Exam Objectives Covered:

- Summarize concepts related to staging and exfiltration.

Topics:

- Staging and Exfiltration
- Fundamentals of Staging and Exfiltration
- Getting Data from a Target
- Hide Files with OpenStego
- Alternate Data Streams
- Applied Live Lab: Staging and Exfiltration Using ADS

MITC-005-1.0 - IT Security Professional Level

Penetration Test e Hacking Etico | CompTIA PenTest+

Cleanup and Restoration
Exam Objectives Covered:

- Explain cleanup and restoration activities.

Topics:

- Cleanup and Restoration
- Cleanup and Restoration Procedures
- Activity: Implement Cleanup and Restoration Activities
- Documenting Penetration Testing Tasks

Penetration Test Report Components
Exam Objectives Covered:

- Explain the components of a penetration test report.

Topics:

- Penetration Test Report Components
- Creating the Penetration Test Report
- Reporting Considerations
- Report Components and Definitions
- Documentation Specifications and Format Alignment
- Risk Scoring
- Test Limitations and Assumptions

Analyze Findings and Remediation Recommendations
Exam Objectives Covered:

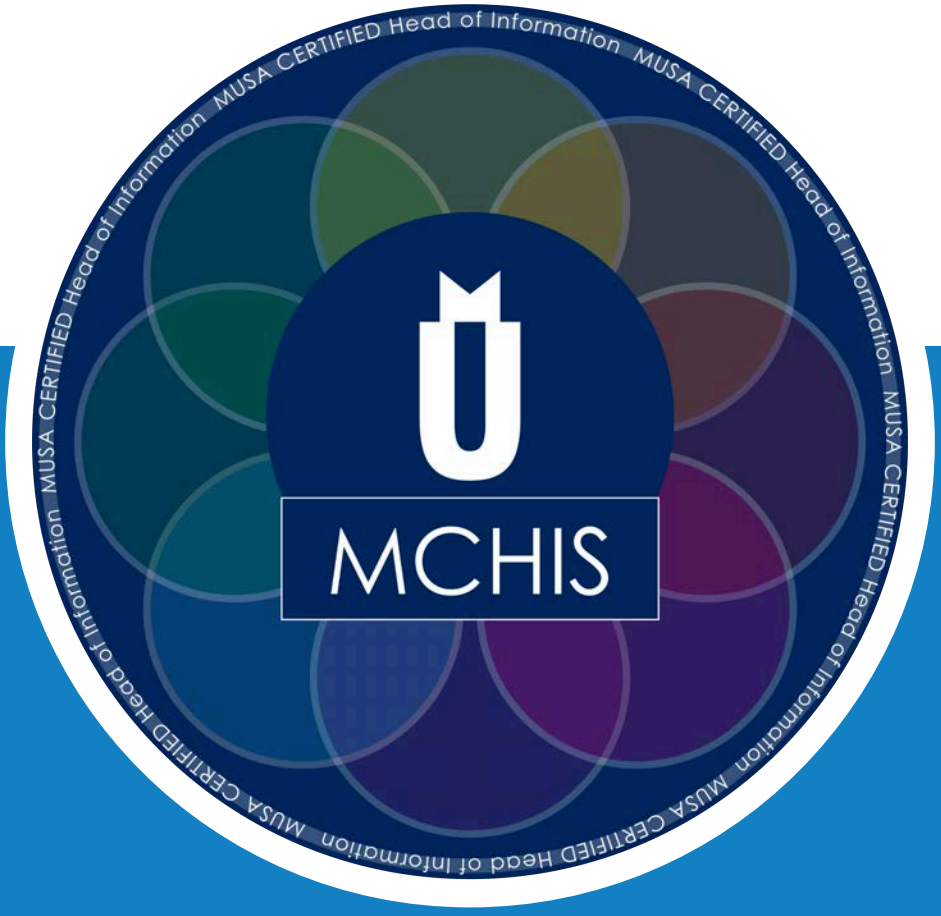
- Given a scenario, analyze the findings and recommend the appropriate remediation within a report.

Topics:

- Analyze Findings and Remediation Recommendations
- Analyzing Findings and Developing Recommendations Overview
- Technical Controls
- Administrative Controls
- Operational Controls
- Physical Controls
- Activity: Administrative and Operational Controls

MUSA

FORMAZIONE



musaformazione.it