SINERVIS ACADEMY

Corsi di Informatica per tutti i livelli

- Grafica
- CAD
- Programmazione
- Web Design
- Sistemistica
- Office Automation
- Comunicazione Digitale
- Web Marketing & SEO

800.44.77.17 NUMERO VERDE

PROGRAMMA DEL CORSO MASTER IN SICUREZZA INFORMATICA

Master in Sicurezza Informatica: corso Cybersecurity con certificazione

Il **Master in Sicurezza Informatica** fornisce gli elementi fondamentali per iniziare a diventare **esperto di sicurezza delle reti e dei sistemi informatici**.
Questo **corso di cybersecurity** ha il vantaggio, rispetto alla maggior parte dei master universitari, di potere essere seguito anche online e in streaming.
Si tratta di un percorso di formazione professionale progettato per fornirti le migliori competenze come professionista esperto di sicurezza informatica, specializzato in metodologie pratiche di difesa e di attacco informatici, in grado di svolgere attività di **penetration testing** e **analisi di sicurezza dei sistemi** e delle **reti informatiche**.
L'esperto di controllo della sicurezza informatica è attualmente tra le figure più richieste nel mercato a livello mondiale. Il percorso si sviluppa in 100 ore complessive: otterrai tutte le competenze necessarie per operare nel settore della sicurezza informatica come "specialista in Cybersecurity" e padroneggiare le competenze necessarie per imparare a proteggere efficacemente reti e sistemi informatici, testandone l'effettiva robustezza attraverso attacchi e violazioni con tecniche e strategie mirate. Il percorso è propedeutico alle **certificazioni internazionali**: **Certificazione CompTia Security+**
Certificazione CompTia PenTest+ (su richiesta)
Certificazione CompTia CySA+ (su richiesta) Con la certificazione Security+, ottenibile conseguendo con successo l'intero percorso formativo, si acquisisce il ruolo di **tecnico con conoscenze approfondite di sicurezza informatica**.
Per ottenere la qualifica di "professionista specializzato in attacco" (PentTest+) o difesa (CySA+), è possibile ottenere le due ulteriori specifiche certificazioni.
Per ottenere una o entrambe le certificazioni specialistiche PentTest+ e CySA+, lo studente deve aver frequentato, con particolare impegno e rendimento, uno (o entrambi) i moduli formativi dedicati (Modulo II e Modulo III), e richiedere la prenotazione degli esami supplementari.

Prerequisiti
Buona conoscenza tecnica del sistemi informatici a livello hardware, software e reti. (E' altamente consigliato aver gia' frequentato il percorso "Master Tecnico Reti").

Obiettivi
Utilizzare i metodi fondamentali di information security e approfondire gli aspetti piu' pratici legati alle figure professionali del **Penetration Tester** e del **Security Analyst**, rispettivamente orientati ad attivita' di attacco offensivo (**penetration testing**) e di difesa proattiva (**security analysis**) dei sistemi digitali. Entrambe le figure professionali necessitano delle conoscenze base offerte dalla certificazione **CompTia Security+**, mentre acquisiscono conoscenze specialistiche attraverso le corrispettive certificazioni **CompTia PenTest+** (attacco) e **CompTia CySA+**(difesa).

SINERVIS ACADEMY

Corsi di Informatica per tutti i livelli

- Grafica
- CAD
- Programmazione
- Web Design
- Sistemistica
- Office Automation
- Comunicazione Digitale
- Web Marketing & SEO

800.44.77.17 NUMERO VERDE

MODULO 1 - INFORMATION SECURITY (20H)

Unità Didattica 1 - Principi fondamentali

- La sicurezza informatica nel business digitale contemporaneo
- Enti e istituzioni a rischio: case study di rilievo
- Profiling dell'attaccante: riconoscere le diverse tipologie di “hacker”
- Figure professionali coinvolte nell'information security
- Comprendere le strategie generali di difesa e attacco
- Modelli di sicurezza: concetto di riservatezza, integrità e disponibilità
- Criteri di valutazione: vulnerabilità, rischio e impatto
- La strategia Defence In Depth: difendersi nei diversi livelli di sicurezza
- Sistemi di controllo fisico, logico e amministrativo

Unità Didattica 2 - Vulnerabilità e falle di sicurezza tipiche

- Software e dispositivi non aggiornati, obsoleti o non mantenuti
- Configurazioni di default, improprie o deboli
- Gestione impropria dell'autenticazione e dell'input utente
- Connessioni e sistemi di crittografia insicuri
- Errata gestione dei certificati e delle chiavi
- Architettura informatica debole e insicura
- Utenti inesperti e procedure vulnerabili o assenti
- Presenza di software e dispositivi non autorizzati
- Minacce interne e mancati controlli sul personale
- Nuovi attacchi e Zero Day
- Esercitazione Pratica: Attacco guidato verso rete, software o dispositivo malconfigurato

Unità didattica 3 - Attacchi informatici e Malware

- Attaccare le reti informatiche:Man-in-The-Middle, Spoofing, DDos, Amplification, Replay
- Attaccare le applicazioni e il sistema operativo:Buffer Overlow, Zero Day, Privilege Escalation
- Attaccare i siti e le applicazioni web:SQL Injection, Cross-site Scripting, Session Hijacking
- Attaccare le password e i sistemi crittografici:Bruteforce, Dictonary, Rainbow Tables, Collision, Downgrade
- Attaccare gli utenti attraverso ingegneria sociale:Phisting, Vishing, Tailgating, Impersonation
- Attacchi attraverso malware:Virus, Worm, Trojan, Ransomware, etc
- Fasi e dinamiche di un attacco informatico mirato
- Esercitazione Pratica: Simulazione di semplici attacchi e utilizzo di malware

Unità Didattica 4 - Tecniche di difesa e contromisure

- Proteggere la rete e le connessioni riservate:VLAN, DMZ, VPN, SSL, Firewall, Antivirus
- Proteggere i software e il sistema operativo:Hardening, Logs e aggiornamenti, Sandboxing
- Proteggere i dati sensibili e la postazione di lavoro:Crittografia, Shredding, Hardening Firmware, TPM

SINERVIS ACADEMY
Corsi di Informatica per tutti i livelli
- Grafica
- CAD
- Programmazione
- Web Design
- Sistemistica
- Office Automation
- Comunicazione Digitale
- Web Marketing & SEO

800.44.77.17 NUMERO VERDE

- Garantire la continuità del servizio:Backup, Disaster Recovery, Mirroring e ridondanza
- Garantire la corretta autenticazione e il controllo d'accesso:Autenticazione multi-fattore, biometrica, password e chiavi
- Sistemi e dispositivi per la sicurezza fisica
- Tecniche e strategie di prevenzione:IDS/IPS, Log analysis e monitoring, scansione vulnerabilità
- Analisi e Gestione del rischio e degli incidenti
- Formulare procedure formali e sensibilizzare gli utenti
- Esercitazione Pratica: Progettazione di un micro-sistema informatico sicuro

Unità didattica 5 - Strumenti per la Sicurezza Informatica

- Strumenti fondamentali a linea di comando e linguaggi di scripting
- Sistemi operativi e distribuzioni dedicate alla sicurezza informatica
- Fonti di consultazione e strumenti utili nel web
- Analizzatori di traffico e mappatura della rete
- Scansionatori di vulnerabilità e Framework per l'exploitazione
- Database di malware, exploit e vulnerabilità note
- Utilizzo di proxy e connessioni anonime
- Honeypot e ambienti di simulazione
- Esercitazione Pratica: Utilizzo base degli strumenti di sicurezza e di sistemi operativi dedicati quali Kali Linux

Unità didattica 6 - Normative per la Sicurezza Informatica e la Privacy

- Stato attuale della legislazione nazionale e comunitaria su sicurezza informatica e privacy
- D.lgs 196/2003 e GDPR: Normativa sulla privacy e tutela dei dati personali
- ISO/IEC 27001: Certificare il livello di sicurezza del proprio sistema informativo
- ISO/IEC 27002: Certificare la qualitàdelle procedure di controllo del proprio sistema informativo
- ISO/IEC 27005: Certificare la qualitàdella gestione del rischio del proprio sistema informativo
- Provvedimento del Garante sulla Privacy per gli amministratori di sistema del 27 novembre 2008
- Direttiva 16/1/2002: Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni
- Circolare AgID n. 1/2017: Misure minime di sicurezza ICT per le pubbliche amministrazioni
- Limitazioni legali e vincoli associati alla figura del Penetration Tester e del Security Analyst

MODULO 2 - SICUREZZA OFFENSIVA: PENETRATION TESTER (40H)

Unità Didattica 1 – La Figura Professionale

- Ruolo del Penetration Tester, metodologie e raggio d'azione
- Aspetti etici, accordi contrattuali e limitazioni legali
- Documentazione e modulistica formale
- Attività preliminari e individuazione del target
- Tipi di valutazione e modellizzazione delle minacce
- Esecuzione di un PenTest: le diverse fasi

SINERVIS ACADEMY

Corsi di Informatica per tutti i livelli

- Grafica
- CAD
- Programmazione
- Web Design
- Sistemistica
- Office Automation
- Comunicazione Digitale
- Web Marketing & SEO

800.44.77.17 NUMERO VERDE

- Conclusione e stesura del PenTest Report

Unità Didattica 2 – Raccolta delle Informazioni

- Importanza della fase di information gathering
- Strumenti di raccolta attiva e raccolta passiva
- Tecniche avanzate per la ricerca nel web e i motori di ricerca
- Raccogliere dati corporativi e personali
- Sfruttare account e reportistica dei server di posta
- Enumerazione DNS e record WHOIS
- Enumerazione della rete e dei servizi
- Estrazione informazioni da metadati e banner
- Utilizzo di framework e tecniche avanzate di data mining
- Esercitazione Pratica: Simulazione di indagine e raccolta informazioni verso un target di specifico

Unità Didattica 3 – Scansione delle Vulnerabilità

- Tecniche di scansione attiva e passiva
- Database pubblici (es: CVE) e ricerca dei servizi a rischio
- Accorgimenti e precauzioni prima della scansione
- Framework e strumenti completi per la scansione delle vulnerabilità
- Monitoraggio e scansione delle attività delle rete
- Scansioni delle vulnerabilità dedicate al web
- Test del sistema di autenticazione e scansione delle password
- Scansioni mirate a servizi di rete specifici
- Ricerca vulnerabilità nelle procedure e utenti deboli
- Esercitazione Pratica: Individuare le vulnerabilità di un insieme di sistemi target con falle di sicurezza nascoste

Unità Didattica 4 – Exploitation: fase di attacco

- Tecniche attive e passive per lo sfruttamento delle vulnerabilità
- Dove rimediare exploit e codice malevolo
- Scrivere i propri exploit e adattare il comportamento di quelli esistenti
- Offuscare il codice sorgente di malware e exploit
- Cryptare e rendere i propri malware non riconoscibili dagli antivirus
- Creare e configurare Trojan Horse e Backdoors
- Inserire i propri malware all'interno di file e connessioni di rete
- Generare email di phishing mirato per l'apertura di file e link pericolosi
- Iniettare i propri malware attraverso le vulnerabilità dei servizi
- Framework e database per l'exploitazione automatica e mirata
- Esercitazione Pratica: Violare una postazione utente attraverso un attacco di phising mirato e non rilevabile attraverso exploit con backdoor

SINERVIS ACADEMY

Corsi di Informatica per tutti i livelli

- Grafica
- CAD
- Programmazione
- Web Design
- Sistemistica
- Office Automation
- Comunicazione Digitale
- Web Marketing & SEO

800.44.77.17 NUMERO VERDE

Unità Didattica 5 - Mantenimento del controllo

- Aprire una connessione diretta o inversa verso il sistema violato
- Strumenti e shell a linea di comando per il controllo della vittima
- Analisi non invasiva dell'ambiente violato e raccolta dati
- Disattivare le protezioni del sistema operativo
- Manipolazione dei file di log e copertura delle tracce
- Migrare codice malevolo all'interno di processi arbitrari
- Escalation dei privilegi e controllo completo della macchina infettata
- Sistemi di persistenza e controllo permanente
- Recuperare credenziali d'accesso ai sistemi di rete e internet
- Crack delle password ed exploitation dei servizi locali
- Identificare file sensibili e informazioni utili per il successivo attacco
- Utilizzare la vittima come ponte per la violazione di altri servizi
- Esercitazione Pratica: Ottenere il controllo completo e permanente del sistema vittima coprendo correttamente le proprie tracce

Unità Didattica 6 - Attacchi alla Rete Informatica

- Identificare sistemi di protezione e rilevamento intrusione
- Tecniche per rendere inosservabili gli attacchi alla rete
- Attacchi storici attraverso stack di rete TCP/IP (es: Smurf)
- Intercettare dati e i flussi di rete attraverso ARP Poisoning
- Tecniche per la forgiatura e la manipolazione dei pacchetti
- Eludere le cifrature SSL e decifrare informazioni sensibili
- Creare servizi fittizi e dirottare la vittima attraverso DNS Spoofing
- Attacchi alle VLAN e allo Spanning Tree Protocol
- Simulazioni di attacchi Dos, DDos e Amplification Attack
- Attacchi a cartelle SMB, NFS e FTP
- Come violare una rete WiFi WEP o WPA2
- Esercitazione Pratica: Ottenere credenziali di accesso del sistema target attraverso un attacco mirato basato sulla rete

Unità Didattica 7 - Attacchi a Siti e Applicazioni Web

- Tipologie di attacco server-side e client-sde
- Sfruttare le configurazioni deboli e improprie
- Sfruttare le errate validazioni dell'input delle applicazioni web
- Dove rimediare exploit specifici per le applicazioni web
- Attacchi al database e SQL Injection
- Estrarre informazioni utili e ottenere il controllo remoto
- Iniettare codice sorgente e tecniche di staging
- Attacchi di Cross-Site Scripting, Request Forgery e Clickjacking
- Manipolare le vittime attraverso il controllo del portale web
- Mantenimento del controllo e copertura tracce nei sistemi server

SINERVIS ACADEMY

Corsi di Informatica per tutti i livelli

- Grafica
- CAD
- Programmazione
- Web Design
- Sistemistica
- Office Automation
- Comunicazione Digitale
- Web Marketing & SEO

800.44.77.17 NUMERO VERDE

- Esercitazione Pratica: Ottenere il controllo completo e permanente dell'applicazione web della vittima coprendo correttamente le proprie tracce

Unità Didattica 8 - Violazioni fisiche e Ingegneria Sociale

- Tecniche generali per ottenere accesso fisico all'interno di una sede
- Clonazione di smart card e token di accesso
- Tecniche per l'apertura di semplici lucchetti di PC e armardi RACK
- Bypassare l'autenticazione della postazione e accedere ai dati sensibili
- Attacchi Cold Boot e al sistema BIOS/UEFI
- Attacchi fisici alla memoria RAM e al sistema TPM
- Installazione di keylogger fisici e dispositivi rogue
- Ottenere informazioni riservate attraverso le tecniche di ingegneria sociale
- Esercitazione Pratica: Simulare la violazione fisica di una postazione vulnerabile e stendere un esempio di rapporto PenTest completo

MODULO 3 - SICUREZZA DIFENSIVA: SECURITY ANALYST (40H)

Unità Didattica 1 - La Figura Professionale

- Ruolo del Security Analyst, attività svolte e contesto operativo
- Framework di sicurezza, politiche, controlli e procedure
- Documentazione e modulistica formale
- Approccio white box per l'indagine dell'infrastruttura informatica
- Tipologie di analisi e valutazioni di sicurezza
- Stesura di un nuovo piano procedurale per utenti e manutentori
- Piano di mitigazione delle vulnerabilità e contromisure

Unità Didattica 2 - Analisi e Ricognizione

- Norme precauzionali per intervenire nell'infrastruttura
- Mappatura della rete, dei servizi e delle utenze
- Esamina delle postazioni utente e delle configurazioni software
- Strumenti per esaminare file di log e anomalie riscontrate
- Scansioni e ricerche rapide di file e informazioni pericolose
- Esamina dei servizi interni e dei sistemi di autenticazione
- Scansione rapida delle vulnerabilità e penetration testing
- Analisi delle procedure utente e dei flussi di informazione
- Valutazione formale del livello di rischio e delle minacce
- Esercitazione Pratica: Effettuare un'indagine completa con approccio white box di un'infrastruttura informatica con servizi vulnerabili nascosti

Unità Didattica 3 - Meccanismi di Autenticazione

- Generazione e archiviazione di password sicure

SINERVIS ACADEMY

Corsi di Informatica per tutti i livelli

- Grafica
- CAD
- Programmazione
- Web Design
- Sistemistica
- Office Automation
- Comunicazione Digitale
- Web Marketing & SEO

800.44.77.17 NUMERO VERDE

- Configurazioni di dominio e group policy
- Rafforzare i servizi di autenticazione (es: RADIUS)
- Implementazioni di autenticazione biometrica e multifattore
- Cifratura delle credenziali e sistemi TPM
- Chiavi USB, firme e token digitali
- Generazione di password OTP e sistemi SSO
- Servizi trusted e gestione dei certificati digitali
- Tecniche di autenticazione per reti locali e geografiche
- Tecniche di autenticazione per servizi amministrativi e server
- Esercitazione Pratica: Sviluppare un sistema di autenticazione multifattore altamente sicuro per l'accesso a delle postazioni con servizi critici

Unità Didattica 4 - Proteggere la Rete Informatica

- Configurare correttamente i sistemi di sicurezza IDS e IPS
- Applicazione di diverse tipologie di analisi in-band e out-of-band
- Configurazione avanzata dei firewall di rete e tecniche mirate
- Antivirus di rete e rilevamento di signature malevole
- Segregazione delle reti e ridondanza dei collegamenti
- Hardening dei dispositivi e dei servizi di rete
- Mascheramento dei servizi e della topologia della rete
- Configurazione corretta di protocolli e connessioni sicure
- Protezione delle reti WiFi WEP e WPA2
- Come proteggersi da un attacco DDoS
- Esercitazione Pratica: Progettare una rete informatica sicura implementandone parte dei servizi

Unità Didattica 5 - Proteggere le Applicazioni e i Servizi

- Sistemi per il controllo degli aggiornamenti e patch di sicurezza
- Configurazione avanzati di Firewall applicativi
- Protezioni per attacchi specifici orientati al web
- Chiusura e mitigazione manuale delle falle di sicurezza
- Hardening del sistema operativo e delle applicazioni di sistema
- Sistemi di sandboxing e controllo di macchine virtuali
- Software antivirus e controlli di integrità periodici
- Sistemi euristici per il rilevamento di backdoor e attività sospette
- Auditing degli eventi e sistemi per il logging centralizzato
- Newsletter di sicurezza e prevenzione di attacchi zero day
- Esercitazione Pratica: Configurare un sistema server sicuro con sistema operativo e servizi rafforzati con metodologie di sicurezza avanzate

Unità Didattica 6 - Proteggere i Dati e le Postazioni

- Verifica della sicurezza fisica essenziale e dell'ambiente operativo
- Tecniche e strumenti di crittografia per file e dischi di archiviazione

SINERVIS ACADEMY

Corsi di Informatica per tutti i livelli

- Grafica
- CAD
- Programmazione
- Web Design
- Sistemistica
- Office Automation
- Comunicazione Digitale
- Web Marketing & SEO

800.44.77.17 NUMERO VERDE

- Proteggere efficacemente il case o l'armadio rack
- Hardening del sistema BIOS/UEFI
- Policy di dominio per la protezione della postazione
- Sistemi di ripristino periodico e controllo di sicurezza remoto
- Corretta distruzione di dati sensibili e dispositivi dismessi
- Norme per la protezione di dispositivi mobile e gestione remota
- Formulazione delle procedure utente per l'utilizzo della postazione
- Esercitazione Pratica: Configurare un sistema server sicuro con sistema operativo e servizi rafforzati con metodologie di sicurezza avanzate

Unità Didattica 7 - Continuità del Servizio e Disaster Recovery

- Sistemi avanzati per il backup locale e geografico
- Sistemi di distribuzione dei dati e mirroring via rete
- Ridondanza dell'insfrastruttura di rete e degli apparati
- Ridondanza dei dischi e sistemi RAID
- Bilanciamento di carico e clustering dei servizi
- Tecniche e meccanismi di Switchover e Failover
- Dispositivi di generazione e continuità elettrica
- Formulazione delle procedure di gestione del disastro
- Esercitazione Pratica: Progettazione di un sistema di backup geografico e ridondanza distribuita in ambiente virtuale

Unità Didattica 8 - Risposta all'incidente

- Strumenti per verificare la presenza di un attacco
- Classificazione degli incidenti e preparazione dei piani di risposta
- Processo di comunicazione interno ed esterno
- Identificazione della minaccia e pianificazione dell'intervento
- Tecniche correttive, di contenimento e di eradicazione
- Affrontare la mitigazione e fase di ricovero
- Ricostruire le dinamiche dell'attacco
- Metodologie avanzate di Digital Forensics
- Comunicazioni legali e reportistica legali
- Esercitazione Pratica: Simulazione di attacco informatico improvviso con simulazione di intervento di risposta immediata all'incidente