UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI
INGEGNERIA INFORMATICA,
MODELLISTICA, ELETTRONICA
E SISTEMISTICA
DIMES

MASTER DI II LIVELLO: SICUREZZA DELLE INFORMAZIONI ED ETHICAL HACKING A.A. 2017/2018

Prof. Ing. Alfredo Garro – DIMES – Università della Calabria – alfredo.garro@unical.it

Dott. Nicola Sotira – Distretto Cyber Security – Poste Italiane
Ing. Elena Agresti – Distretto Cyber Security – Poste Italiane - AGREST10@posteitaliane.it

Rende, 17 luglio 2017

Posteitaliane

I MASTER

DUE MASTER DI II LIVELLO IN ETHICAL HACKING E SICUREZZA DELLE INFORMAZIONI

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA
DIMES

Master in Ethical Hacking

Il corso è orientato a formare esperti di cyber security in grado di testare a fondo il livello di sicurezza di reti e sistemi informatici al fine di identificare minacce, vulnerabilità tecnologiche, falle e aree di miglioramento per metterle in sicurezza.

- **20 allievi**
- **Neolaureati in materia scientifiche, esperti IT, dipendenti di organizzazioni pubbliche/private che intendo sviluppare o ampliare competenze di ethical hacking**

Master in Sicurezza delle informazioni

Il corso è orientato a formare esperti di sicurezza delle informazioni, in grado di comprendere i principali aspetti organizzativi, tecnici, tecnologici e giuridici per la protezione del patrimonio informativo aziendale

- **20 allievi**
- **Neolaureati in materia scientifiche, economiche, giuridiche, dipendenti della PA che intendono ampliare, approfondire o sviluppare conoscenze e competenze sulla sicurezza delle informazioni**

Posteitaliane

PROFILI PROFESSIONALI
IMPORTANTI SBOCCHI PROFESSIONALI

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA
DIMES

	Profilo professionale	Sbocchi occupazionali
Master in Ethical Hacking 	Al termine del Master lo studente sarà in grado di: ➢ Padroneggiare **le tecniche di attacco e gli stessi strumenti utilizzati dagli hacker**, considerando la sicurezza dal punto di vista dell'attaccante ➢ Conoscere i principali strumenti di **cyber threat intelligence** ➢ **Testare la rete e sistemi** con gli stessi metodi e tecniche utilizzate dagli hacker per verificare la presenza di vulnerabilità e falle di sicurezza ➢ Identificare le migliori **misure di sicurezza** da mettere in atto per prevenire, intercettare e contrastare prontamente attacchi cyber	• SOC - Security Operation Center • CERT - Computer Emergency Response Team • Threat Intelligence Team • ….
Master in Sicurezza delle Informazioni 	Al termine del Master lo studente sarà in grado di: ➢ Definire e governare i **processi, le politiche e i modelli organizzativi** di information security ➢ Gestire correttamente i **rischi e stimare gli effetti potenziali di attacchi** alle infrastrutture e al patrimonio informativo ➢ Individuare **i sistemi di prevenzione più adatti e le misure di sicurezza più idonee**, considerando i requisiti interni e le opportunità suggerite dalle best practice internazionali ➢ Garantire **la compliance** ai principali regolamenti e standard di riferimento	• Information Security Governance • Analisi dei rischi • Internal Audit • Privacy e Compliance • ….

Posteitaliane

PROGRAMMA FORMATIVO
MASTER IN SICUREZZA DELLE INFORMAZIONI

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA
DIMES

Programma formativo (1575 ore)

- Contenuti multimediali
- **Attività in aula ore 296**
- **Attività e-learning ore 72**
- **Studio Individuale ore 707**
- **Attività Training on the Job ore 500**
- Workshop

Mod.1 (ore 28) Introduzione alla Sicurezza delle Informazioni

- *Scenari di riferimento per la Sicurezza delle Informazioni*
- *Principi di Sicurezza delle informazioni*

Mod.2 (ore 56) Fondamenti di Sicurezza di reti e sistemi

- *Architettura sicura di reti*
- *Principi e tecniche di Host security*
- *Principi e tecniche di Network security*
- *Sicurezza dei Sistemi*

25% lezioni a distanza

Mod.3 (ore52) Tecniche di attacco cyber

- *Tecniche di attacco cyber*
- *Contromisure di sicurezza*
- *Vulnerability Assessment e Penetration Test*

Mod.4 (ore 68) Contromisure di Sicurezza

- *Crittografia e sue applicazioni pratiche*
- *Tecniche di autenticazione e protezione dell'identità digitale*
- *Open data e data science*
- *Focus su tecnologie per la sicurezza*

Mod.5 (ore 48) Aspetti legali e regolamentari dell'Information Security

- *Quadro normativo italiano ed europeo in materia di information security*
- *Regolamento su Data protection*
- *Infrastrutture e tecnologie di sicurezza per il Governo Digitale*

Mod.6 (ore 40) Certificazione ISO/IEC 27001

- *Certificazione ISO/IEC 27001:2013*

Mod.7 (ore 76) Governance dell'Information Security

- *Sistema di Gestione della Sic. delle I (SGSI)*
- *Principi, approccio e requisiti dello S.ISO/IEC 27001*
- *Controlli di information security dello ISO/IEC 27001*
- *Implementazione dello S. ISO/IEC 27001*
- *Il ruolo del Lead Auditor*
- *Business model per l'Information Security*
- *Information Security nella gestione delle terze parti*

Posteitaliane

PROGRAMMA FORMATIVO
MASTER IN ETHICAL HACKING

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA
DIMES

Programma formativo (1575 ore)

- Contenuti multimediali
- **Attività in aula ore 296**
- **Attività e-learning ore 72**
- **Studio Individuale ore 707**
- **Attività Training on the Job ore 500**
- Workshop

Mod.1 (32 ore) Introduzione all'ethical hacking pianificazione e reporting
- *Storia, scenario di riferimento e principi dell'ethical hacking*
- *La Cyber Kill Chain e pianificazione di un security assessment*
- *Valutazione e analisi del rischio*

Mod. 2 (48 ore) Information gathering
- *Metodologie e tecniche di social engineering, information hiding*
- *Tecniche di footprinting e di system e network scanning*
- *Tecniche di analisi di fonti aperte Open Source Intelligence*

Mod.3 (52ore) Attacchi alle infrastrutture
- *Attacchi agli apparati di rete*
- *Attacchi di sicurezza perimetrale*
- *Tecniche di evasione per i SIEM*
- *Attacco ai sistemi operativi enterprise*
- *Introduzione agli attacchi web e threat model*

25% lezioni a distanza

Mod.4 (60 ore) Attacchi Web
- *Tecniche di hacking e misure di sicurezza per web server*
- *Tecniche di hacking e misure di sicurezza per web application*
- *Tecniche di hacking e misure di sicurezza per la persistenza dei dati*
- *Attacco ai sistemi operativi end-user*

Mod.5 (44 ore) Attacchi Mobile
- *Introduzione agli attacchi mobile e threat model*
- *Tecniche di hacking e misure di sicurezza per applicazioni mobile*
- *Tecniche di hacking e misure di sicurezza per sistemi operativi mobile*
- *Tecniche di hacking e misure di sicurezza per la persistenza dei dati*

Mod.6 (60 ore) Attacchi ai sistemi di autenticazione
- *Tecniche per il furto d'identità digitale*
- *Tecniche di offuscamento, hashing e cracking di credenziali*
- *Attacchi ai sistemi di autenticazione mono e multifattore*
- *Attacchi ai sistemi di autenticazione biometrica e one time password*
- *Attacchi ai sistemi di single sign on e di identità federata*

Mod.7(24 ore) Attacchi all'hardware
- *Tecniche crittografica per l'hardware*
- *Attacchi cyber all'hardware*
- *Attacchi ai dispositivi IoT*
- *Attacchi hardware ai dispositivi mobile*

Mod.8 (48 ore) Malware analysis e reverse engineering
- *Fondamenti di malware analysis*
- *Hybrid Analysis dei malware*
- *Misure di sicurezza contro i malware*
- *Identificazione e formalizzazione di IoC e TTP*

Posteitaliane

REQUISITI DI AMMISSIONE
LAUREE MAGISTRALI O SPECIALISTICHE

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA
DIMES

Requisiti di ammissione

Master in Ethical Hacking

Laurea magistrale ex D.M. 270/04 o specialistica ex D.M. 509/99 nelle classi di:

1. Ingegneria Informatica o nella classe Scienze e Tecnologie Informatiche o nella classe Sicurezza Informatica;
2. Ingegneria Elettronica, Ingegneria delle Telecomunicazioni, Ingegneria dell'Automazione, Ingegneria Gestionale, Ingegneria della Sicurezza, Scienze Statistiche Informatiche

Laurea vecchio ordinamento (antecedente D.M. 509/99) o Laurea presso Università Straniere di durata di almeno di quattro anni, equivalente a una delle lauree di cui al punto 1 o 2.

Master in Sicurezza delle Informazioni

Laurea magistrale ex D.M. 270/04 o specialistica ex D.M. 509/99 nelle classi di:

1. Ingegneria dell'Informazione o nella classe Scienze e Tecnologie Informatiche.
2. Ingegneria Elettronica, Ingegneria delle Telecomunicazioni, Ingegneria dell'Automazione, Ingegneria Gestionale, Ingegneria della Sicurezza, Scienze Statistiche, Metodologie Informatiche per le Discipline Umanistiche, Teorie della Comunicazione, Scienze Economico-Aziendali, Scienze delle Pubbliche Amministrazioni, Matematica, Fisica, Giurisprudenza.

- Laurea vecchio ordinamento (antecedente D.M. 509/99) o Laurea presso Università Straniere di durata di almeno di quattro anni, equivalente a una delle lauree di cui al punto 1 o 2.

È richiesta per entrambi i corsi una buona conoscenza della lingua inglese.

Parte delle lezioni, così come alcuni strumenti e piattaforme utilizzati durante le lezioni, saranno disponibili solo in lingua inglese.

CRITERI DI SELEZIONE

BANDO PUBBLICO CON VALUTAZIONE TITOLI E PROVE

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA
DIMES

Master in Ethical Hacking

Valutazione titoli

Valutazione curriculum e titoli

- Tipo di laurea
- Voto della laurea
- Titolo Dottore di Ricerca
- Formazione di settore
- Esperienze lavorative settoriali
- Pubblicazioni

Capture the flag

Competizione capture the flag su scenari differenti

Colloqui

Colloquio individuale volto ad discutere i risultati della fase di test e verificare le conoscenze e competenze in materia di sicurezza informatica

Master in Sicurezza delle Informazioni

Valutazione titoli

Valutazione curriculum e titoli

- Voto della laurea
- Titolo Dottore di Ricerca
- Master, Scuole post laurea o altri corsi di formazione
- Esperienze lavorative
- Tipo di laurea
- Pubblicazioni

Colloqui

Colloquio individuale volto ad accertare le competenze e esperienze maturate dal candidato e la rilevanza rispetto al settore della sicurezza delle informazioni

Posteitaliane

STRUMENTI
PIATTAFORME VIRTUALI DI SIMULAZIONE

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA
DIMES

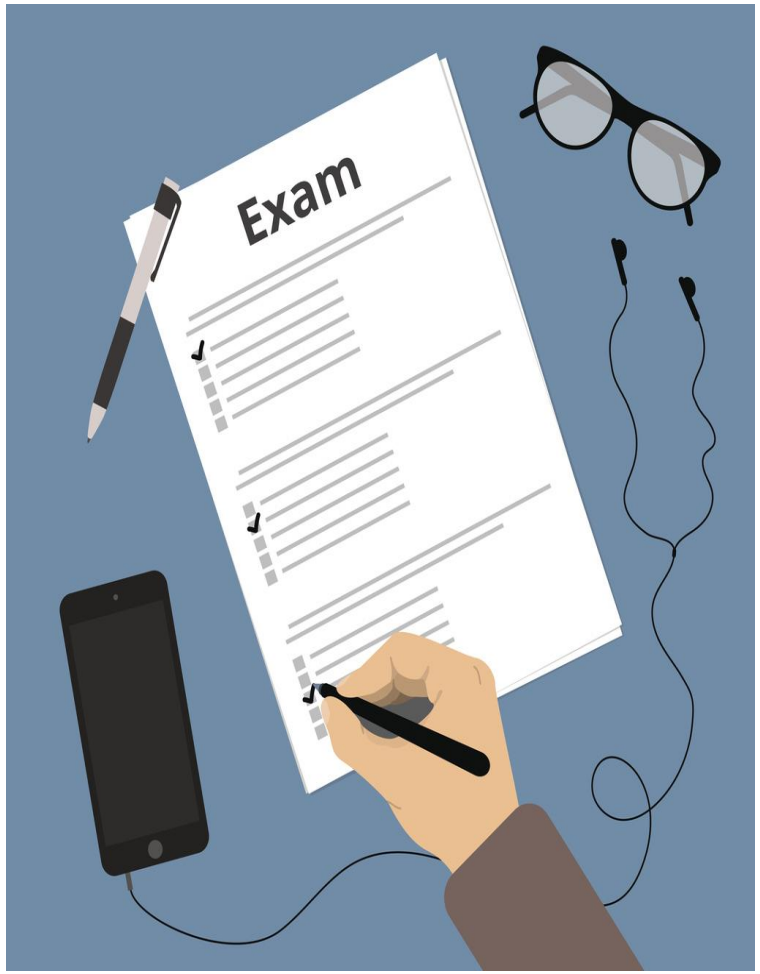
- **Sperimentare, in ambienti virtuali appositamente predisposti, tecniche di attacco** alle infrastrutture, ai sistemi di autenticazione, dispostivi mobile, all'hardware solitamente utilizzate dagli hacker al fine di poterle utilizzare in modo responsabile per elevare il livello di protezione e sicurezza delle organizzazioni.

- **Trovare exploit in una infrastruttura o** completare degli obiettivi specifici a seconda delle sfide che vengono lanciate di volta in volta

- Effettuare **simulazioni a squadre** che si sfidano per proteggere la propria "fortezza", cercando contemporaneamente di violare quella degli avversari

VERIFICHE DIDATTICHE

VERIFICHE PERIODICHE ED ELABORATO FINALE



Verifiche inizio modulo

All'inizio di ciascun Modulo verrà somministrato un **test preliminare volto a valutare le conoscenza preesistenti della materia oggetto di formazione** al fine di identificare le necessità formative e **indirizzare al meglio le attività didattiche**

Verifiche intermedie

Sarà valutato **il livello di apprendimento rispetto alle tematiche trattate in ciascuna Unità Didattica** attraverso test finali, prove intermedie di verifica effettuate durante i corsi, progetti sviluppati dallo studente o frutto di lavori di gruppo

Verifica finale

La verifica finale consisterà nella discussione di un elaborato progettuale realizzato durante lo stage e di tematiche trattate nel corso. Il **voto finale terrà conto di tutto il percorso formativo**

ASPETTI ORGANIZZATIVI
COSTI, LOGISTICA E TEMPI

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA
DIMES

QUOTA DI PARTECIPAZIONE
La tassa di iscrizione al Master è di **2000 euro**

DURATA
12 mesi

LA SEDE

I Master si terranno presso il Distretto Cyber Security di Poste **Italiane in via August Von Platen n. 9 Cosenza** (riva sinistra del fiume Busento) **e i laboratori dell'Università della Calabria** Via Pietro Bucci, Arcavacata Rende (CS).

GLI ORARI

I corsi si terranno il **venerdì pomeriggio (14-20) e il sabato mattina (8-14) e** sono previste **due settimane di laboratorio intensivo (lun 15-19, merc-giov 9-17, ven 8-12).** Il 25% delle ore di didattica potranno essere erogate in modalità remota

Il cronoprogramma

Set .2017 | Ott. 2017 | Nov. 2017 | Dic. 2017 | Gen. 2018 | Feb. 2018 | Mar. 2018 | Apr. 2018 | Mag. 2018 | Giu. 2018 | Lug. 2018 | Ago. 2018 | Set. 2018 | Ott. 2018

Selezione studenti — **Attività in aula ed e-learning** — **Training on the job**

Posteitaliane

COLLABORAZIONI

POSTE ITALIANE E ALTRI GRANDI PARTNER

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA
DIMES

Le docenze saranno erogate da **Professori dell'Università della Calabria e dell'Università Mediterranea di Reggio Calabria, esperti di Poste Italiane e della fondazione GCSEC e provenienti dalle principali organizzazioni** internazionali di settore e dagli altri soggetti con i quali sono stati sottoscritti appositi accordi di collaborazione. **Questi ultimi selezioneranno brillanti studenti per le attività di tirocinio/stage.**

Master in Ethical Hacking

Posteitaliane
Università degli Studi di Reggio Calabria Mediterranea
ADS GROUP
NTT DATA
proofpoint
KASPERSKY lab
TS-WAY
ALFA GROUP
FireEye

Master in Sicurezza delle informazioni

Posteitaliane
Global Cyber Security Center
Università degli Studi di Reggio Calabria Mediterranea
KPMG
ALFA GROUP
Deloitte.
Bip
Reply spike
JUNIPER NETWORKS
TREND MICRO
sas
NTT DATA
f5
aditinet 1st CLASS IT

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI
INGEGNERIA INFORMATICA,
MODELLISTICA, ELETTRONICA
E SISTEMISTICA
DIMES

MASTER DI II LIVELLO: SICUREZZA DELLE INFORMAZIONI ED ETHICAL HACKING A.A. 2017/2018

Prof. Ing. Alfredo Garro – DIMES – Università della Calabria – alfredo.garro@unical.it

Dott. Nicola Sotira – Distretto Cyber Security – Poste Italiane
Ing. Elena Agresti – Distretto Cyber Security – Poste Italiane - AGREST10@posteitaliane.it

Roma, 8 Giugno 2017

Posteitaliane