Lezione 0

Introduzione al corso

Analisi del Malware

26 settembre 2023

Marco Cesati

Dipartimento di Ingegneria Civile e Ingegneria Informatica
Università degli Studi di Roma Tor Vergata

Di cosa parliamo in questa lezione?

Parliamo in generale dell'insegnamento:

Analisi del Malware

1. Contenuti
2. Gestione della didattica
3. Destinatari
4. Come partecipare attivamente
5. Materiale didattico
6. Modalità d'esame
7. Statistiche anni passati

Il corso

- ANALISI DEL MALWARE
- 6 CFU
- Primo e secondo anno laurea magistrale Ing. Informatica
- attivo dall'A.A. 2020/2021
- erogato dall'A.A. 2021/2022 (ad anni alterni)

Alternanza con SISTEMI EMBEDDED E REAL-TIME

Dall'Anno Accademico 2020/21 il corso SERT viene erogato in alternanza con il corso di MALWARE ANALYSIS

- negli anni dispari sono erogate le lezioni del corso MALWARE ANALYSIS
- negli anni pari sono erogate le lezioni del corso SERT

In ogni anno accademico si terranno comunque sessioni d'esame sia per SERT che per MALWARE ANALYSIS

Contenuti e programma del corso

- L'analisi del malware nel contesto della Cyber Security
- Tecniche di base di Reverse Code Engineering: analisi statica e dinamica del codice macchina
- Funzionalità del malware: comportamento generale, operazioni di base, meccanismi di protezione
- Approfondimento di alcuni casi particolari

Modalità erogazione del corso

I docenti dei corsi di laurea in Ingegneria Informatica hanno deciso di sostenere ed incentivare la modalità di erogazione della didattica "in presenza"

Pertanto, a meno di diverse indicazioni del governo nazionale, degli organi di governo dell'università o del coordinamento del corso di laurea in ingegneria informatica magistrale:

- Le lezioni si svolgeranno in presenza
- Le lezioni **non** verranno contemporaneamente trasmesse su piattaforma telematica
- Le registrazioni delle lezioni **non** verranno pubblicate dal docente

Le lezioni verrano registrate dal docente al solo scopo di preparare il materiale didattico per l'Anno Accademico 2025/2026, durante il quale AMW non sarà erogato

Aule e orari

Martedì	9:30 – 11:00	Aula C4
Giovedì	9:30 – 11:00	Aula C4

Sito ufficiale del corso

Tutte le informazioni relative al corso ANALISI DEL MALWARE:

- modalità di partecipazione
- lucidi proiettati a lezione
- dispense e altro materiale didattico
- avvisi di carattere generale
- ...

sono nel sito

`https://amw23.sprg.uniroma2.it`

GOCU

Per l'anagrafe degli studenti e la gestione delle prove d'esame utilizzeremo un sistema chiamato GOCU raggiungibile sul sito

`http://gocu.sprg.uniroma2.it`

La registrazione sul sistema **GOCU** vale come iscrizione al corso

Delphi

È obbligatorio utilizzare il sistema Delphi per la prenotazione delle prove d'esame:

`http://delphi.uniroma2.it/`

Delphi ha scopi e funzioni differenti da GOCU:

- Invita lo studente a compilare il questionario di valutazione della qualità della didattica del corso
- Consente di tenere traccia del numero di esami erogati nell'ateneo (è un parametro valutato a livello ministeriale)
- Implementa la verbalizzazione elettronica degli esami

Per partecipare ad ogni prova d'esame è obbligatorio effettuare la prenotazione su **Delphi**

La prenotazione su **GOCU** non è necessaria (viene gestita direttamente dal docente)

Introduzione al corso
Marco Cesati

Schema della lezione
Contenuti
Aule e orari
Gestione del corso
Destinatari
Partecipazione
Materiale didattico
Esami
Valutazione didattica

Microsoft Teams

Microsoft Teams è la soluzione d'ateneo suggerita per lo svolgimento delle lezioni e degli esami a distanza

In questo anno accademico non si prevede di utilizzare tale piattaforma

Non utilizzare il sistema di "chat" di Teams per contattare il docente!

Come potete contattarmi?

In ordine di preferenza:

1. Per posta elettronica, all'indirizzo

   `amw@sprg.uniroma2.it`

2. Personalmente, dopo la lezione (per questioni di breve durata)
3. Personalmente, durante l'orario di ricevimento:

   giovedì, 12:00–13:00, stanza A3-05
   Edificio Ingegneria dell'Informazione (terzo piano)

   - È consigliabile avvisare preventivamente

4. Concordando un appuntamento su una piattaforma di comunicazione digitale

A chi è rivolto questo corso?

In modo specifico agli studenti dei corsi di laurea magistrale in Ingegneria dell'Informazione e ICT & Internet

Studenti di altri corsi di laurea magistrale (Automazione, Elettronica, . . .) sono benvenuti

Studenti di altri corsi di laurea potrebbero dover studiare un po' di più per colmare eventuali lacune nella preparazione di base su materie informatiche

In ogni caso, ricordatevi che siete tenuti a rispettare le regole fissate dal vostro rispettivo CCS, in particolare per ciò che riguarda le anticipazioni degli esami

In caso di dubbio, informatevi presso le segreterie didattiche oppure il Coordinatore del vostro corso di studi

Cosa ci si aspetta dagli studenti

Non esistono propedeuticità formali

Il programma del corso verte su argomenti avanzati di

- sistemi operativi
- programmazione di sistemi
- architettura dei calcolatori
- reti di calcolatori

Ci aspettiamo che gli studenti abbiano raggiunto una sufficiente maturità così da riuscire in modo autonomo a

- verificare l'esistenza di eventuali lacune nella propria preparazione di base
- colmare le lacune eventualmente esistenti tramite libri di testo e materiale didattico di corsi erogati in questa facoltà

Libri di testo

C. Eagle, K. Nance

The Ghidra book – The definitive guide

No Starch Press, 2020

ISBN 978-1-71850-102-7 (print)
ISBN 978-1-71850-103-4 (e-book)

M. Sikorski, A. Honing

Practical Malware Analysis – The hands-on guide to dissecting malicious software

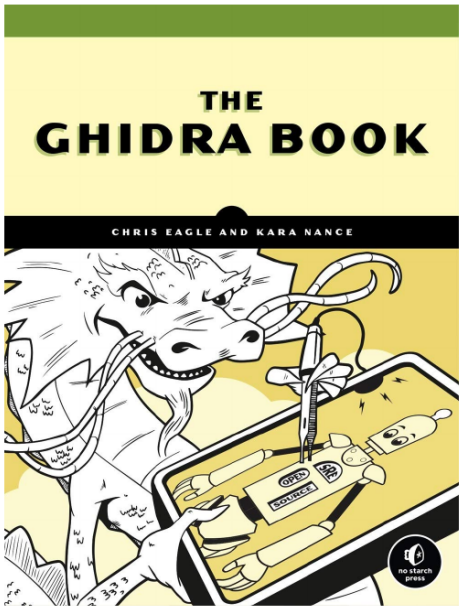
No Starch Press, 2012

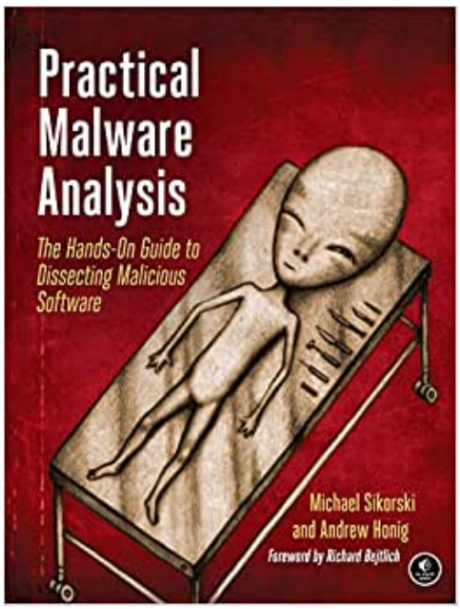
ISBN 978-1-59327-290-6

Introduzione al corso

Marco Cesati

Schema della lezione
Contenuti
Aule e orari
Gestione del corso
Destinatari
Partecipazione
Materiale didattico
Esami
Valutazione didattica





Altro materiale

Sul sito del corso troverete inoltre:

- Lucidi proiettati durante le lezioni
- Riferimenti (link WWW) a
  - manuali tecnici
  - articoli
  - siti Web
  - ecc.

Modalità d'esame (provvisorie)

L'esame è costituito da:

- un esame orale su tutti gli argomenti del corso
  - 60% del voto finale
- un progetto da svolgere individualmente consistente nell'analisi di un esemplare di malware
  - 40% del voto finale

Il progetto può essere consegnato prima o dopo l'esame orale

Sessioni d'esame

Sessione invernale:

- due appelli dal 22.01.2024 al 3.03.2024

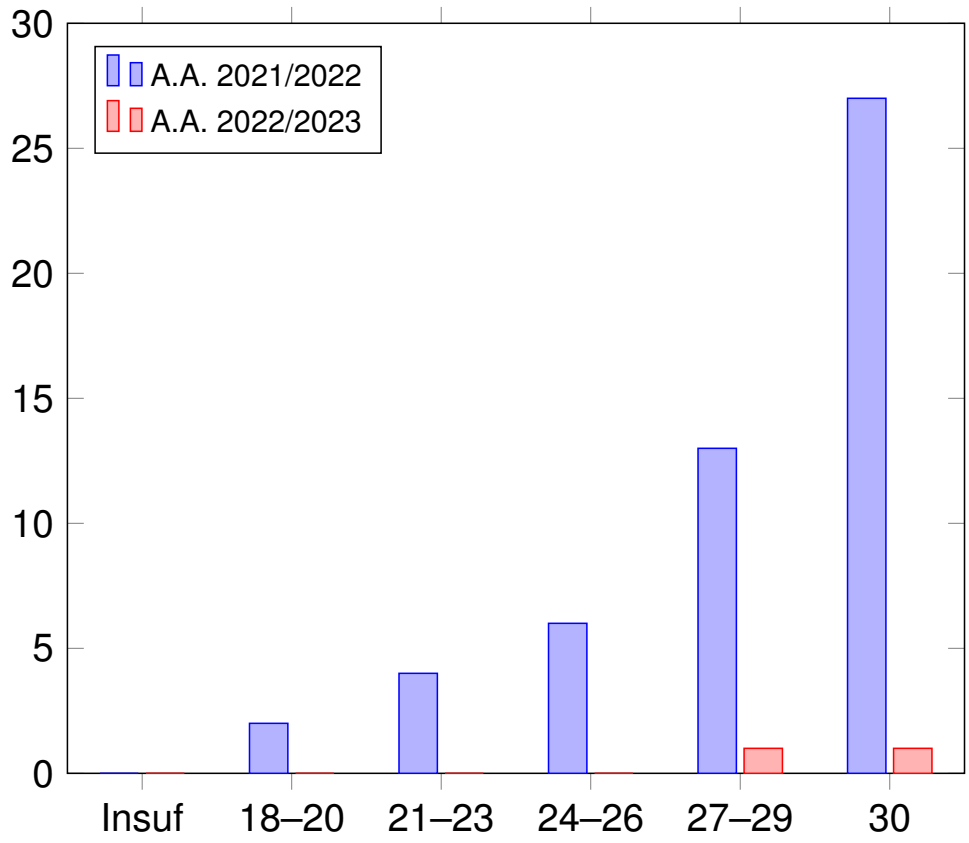
Sessione estiva:

- due appelli dal 18.06.2024 al 28.07.2024

Sessione autunnale:

- due appelli dal 27.08.2024 al 21.09.2024

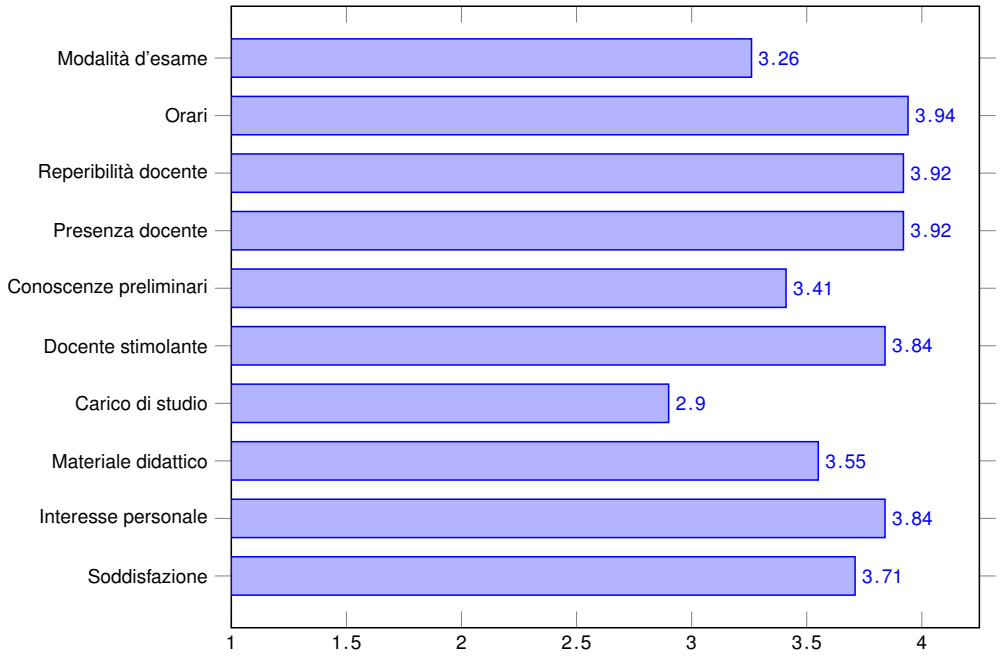
Voti finali conseguiti negli ultimi anni accademici



Introduzione al corso
Marco Cesati

Schema della lezione
Contenuti
Aule e orari
Gestione del corso
Destinatari
Partecipazione
Materiale didattico
Esami
Valutazione didattica

Valutazione della didattica A.A. 2021/2022



1→ Decisamente NO 2→ Più NO che SÌ

3→ Più SÌ che NO 4→ Decisamente SÌ

Introduzione al corso

Marco Cesati

Schema della lezione
Contenuti
Aule e orari
Gestione del corso
Destinatari
Partecipazione
Materiale didattico
Esami
Valutazione didattica

Buon lavoro a tutti!