UNIVERSITÀ DI PISA

SYSTEM AND NETWORK HACKING

GIUSEPPE LETTIERI

Anno accademico	2020/21
CdS	COMPUTER ENGINEERING
Codice	912II
CFU	9

Moduli	Settore/i	Tipo	Ore	Docente/i
SYSTEM AND NETWORK HACKING	ING-INF/05	LEZIONI	90	GIUSEPPE LETTIERI PERICLE PERAZZO

Obiettivi di apprendimento

Conoscenze
Lo studente avrà acquisito conoscenze in merito alle vulnerabilità più comuni dei sistemi software, delle architetture di elaborazione, delle reti e delle applicazioni web, ai modi in cui queste vulnerabilità sono sfruttate dagli attaccanti e alle contromisure messe in atto per mitigare gli attacchi.

Modalità di verifica delle conoscenze
La verifica delle conoscenze sarà oggetto di una prova scritta e/o orale a conclusione di ogni esame.

Capacità
Lo studente sarà in grado di scrivere codice e configurare i sistemi in modo da mitigare le vulnerabilità più comuni, ma anche di portare a termine attacchi mirati a dimostrare la presenza di tali vulnerabilità.

Modalità di verifica delle capacità
Le capacità saranno verificate tramite lo sviluppo di un progetto software, che potrà essere sviluppato da piccoli gruppi di studenti o singolarmente.

Comportamenti
Lo studente svilupperà una maggiore attenzione e consapevolezza verso le vulnerabilità dei sistemi informatici, e possiederà un bagaglio di "best practice" atte a mitigare tali vulnerabilità.

Modalità di verifica dei comportamenti
I comportamenti saranno verificati tramite lo sviluppo di un progetto software, che potrà essere sviluppato da piccoli gruppi di studenti o singolarmente.

Prerequisiti (conoscenze iniziali)

- architetture degli elaboratori
- linguaggio macchina e assembler
- C/C++
- sistemi operativi
- reti e programmazione di rete
- programmazione web
- basi di dati

Indicazioni metodologiche

- lezioni frontali con l'ausilio di slide e condivisione dello schermo del PC
- per le esercitazioni ogni studente deve essere dotato del proprio PC, con software consigliato dai docenti
- i docenti saranno reperibili per ricevimento ed email
- il materiale didattico sarà reso disponibile tramite il sito web del corso

- sarà previsto lo sviluppo di un progetto sugli argomenti del corso
- lezioni ed esercitazioni si svolgeranno in lingua inglese

Programma (contenuti dell'insegnamento)

SISTEMI OPERATIVI: controllo degli accessi discretionary/mandatory; programmi suid/sgid; metacaratteri; attacchi tramite variabili di ambiente (PATH, IFS, ...); attacchi tramite collegamenti simbolici; "sandboxing" tramite contenitori (namespace, control group); monitor sicuri (AppArmor).
PROGRAMMAZIONE: concetti e pratiche di programmazione sicura in C e C++; i processi e il loro spazio di indirizzamento: la pila e lo heap, dlmalloc, mmap()/mprotect(), le librerie dinamiche, la "Global Offset Table" (GOT) e la Procedure Linkage Table (PLT); overflow sugli interi; buffer overflow su pila e heap; vulnerabilità delle stringhe di formattazione; errori di "use-after-free" e "double-free"; iniezione e riuso di codice: "return-to-libc", "Return Oriented Programming" (ROP); "Address Space Layout Randomization" (ASLR) e codice indipendente dalla posizione; integrità del flusso di controllo; errori di "Time-of-Check to Time-of-Use" (TOCTOU); iniezione di comandi shell, attraversamento di directory.
RETI E WEB: scansione delle reti e dei servizi, "fuzzing", rilevamento del Sistema Operativo tramite "fingerprinting", attacchi di forza bruta al DNS, "packet sniffing"; applicazioni web: mappatura, vulnerabilità nei sistemi di autenticazione, attacchi di forza bruta all'autenticazione, vulnerabilità nel sistema di gestione delle sessioni, furto della sessione, vulnerabilità nel sistema di controllo accessi, iniezione di codice SQL, iniezione LDAP, "cross-site scripting", "web spidering", entità XML esterne.

Bibliografia e materiale didattico

- Robert Seacord. Secure Coding in C and C++ (2nd edition). Addison-Wesley Professional, 2013.
- Dafydd Stuttard and Marcus Pinto. The Web Application Hacker's Handbook: Finding and
- Exploiting Security Flaws. John Wiley & Sons, 2011.
- Chris Anley, The Shellcoder's Handbook: Discovering and Exploiting Security Holes, (2nd Edition), John Wiley & Sons, 2007.
- Dispense fornite dai docenti

Modalità d'esame

Prova scritta e orale, più progetto.

Pagina web del corso

https://lettieri.iet.unipi.it/hacking/

Ultimo aggiornamento 03/10/2020 17:14