UNIVERSITÀ DI PISA

SYSTEM AND NETWORK HACKING

GIUSEPPE LETTIERI

Anno accademico	2021/22
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 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 web che potrà essere sviluppato da piccoli gruppi di studenti o singolarmente, e tramite una prova pratica.

Comportamenti
Lo studente svilupperà una maggiore attenzione e consapevolezza verso le vulnerabilità dei sistemi informatici, e possiederà un bagaglio delle pratiche migliori atte a mitigare tali vulnerabilità.

Modalità di verifica dei comportamenti
I comportamenti saranno verificati tramite lo sviluppo di un progetto web, 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) e macchine virtuali; 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; attacchi diretti al kernel (return to userspace, protezione tramite SMEP/SMAP); attacchi diretti all'hypervisor, fuga da una VM.
RETI E WEB: tecniche di raccolta di informazioni; forzatura DNS; sniffing e scansione di rete; identificazione della pila TCP/IP; inondazione e spoofing MAC; avvelenamento ARP; spoofing IP; attacchi e difese DoS e DDoS; attacchi uomo-nel-mezzo; mappatura di applicazioni web; vulnerabilità nell'autenticazione web; forzatura dell'autenticazione; blocco dell'account; tecnologie CAPTCHA; vulnerabilità nella gestione delle sessioni; dirottamento di sessione; vulnerabilità nel controllo degli accessi; iniezione SQL; iniezione SQL cieca; iniezione LDAP; iniezione di comandi del sistema operativo; inclusione di file remoti; iniezione di entità esterne XML; scripting intersito; regola della stessa origine; falsificazione di richiesta intersito.

Bibliografia e materiale didattico

- Dafydd Stuttard and Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (2nd Edition). 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 pratica e orale. Per sostenere la prova pratica gli studenti sono tenuti a portare con sé il proprio calcolatore portatile.

Pagina web del corso

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

Altri riferimenti web

http://www.iet.unipi.it/p.perazzo/teaching

Ultimo aggiornamento 16/06/2022 10:25