# Sicurezza e privatezza

## Tema di laboratorio

27 luglio 2020

*Il tema di laboratorio consiste in 5 esercizi pratici da svolgere in autonomia che saranno argomento delle domande presenti nella prova "scritta" del giorno* 27 luglio 2020*.*

*Scopo delle domande verificare se lo studente è stato in grado di svolgere in autonomia gli esercizi proposti. Alle suddette domande saranno aggiunte ulteriori due domande a risposta aperta sui temi della privacy e dell'etica.*

*La prova consterà di 10 domande, saranno ammessi alla prova orale gli studenti che risponderanno correttamente a 6 domande su 10. Gli studenti che risponderanno correttamente a: 8 domande avranno un bonus nella parte orale di 1 punto, 9 domande avranno un bonus nella parte orale di 2 punti, 10 domande avranno un bonus nella parte orale di 3 punti.*

**Esercizio 1, Blind buffer overflow**

Nel seguente esercizio viene fornito un eseguibile linux senza il codice sorgente (compilato tramite la macchina virtuale kali usata in laboratorio) è richiesto di trovare la vulnerabilitá e tramite essa stampare la scritta "You win!".
Si ricorda che prima di eseguire il programma compilato è necessario disabilitare la protezione di randomizzazione degli indirizzi (ASLR) tramite: *sudo sysctl -w kernel.randomize_va_space=0*.
Per l'esecuzione si consiglia l'utilizzo della virtual machine kali usata durante il corso.

Software utili per svolgere l'esercizio: objdump, strings, gdb

**Esercizio 2, Remote service login**

In riferimento alla lezione di laboratorio riguardante gli attacchi tramite metasploit/armitage realizzare un attacco al sistema di login del server mysql presente nella virtual machine metasploitable2. Nel seguente esercizio si chiede di trovare un payload adatto per applicare un attacco di tipo bruteforce (o a dizionario) sulle credenziali di accesso al server mysql presente sulla macchina remota.
Per la realizzazione dell'attacco si dovrá disporre di due macchine virtuali una "vittima" (metasploitable2) ed una "attaccante" configurando correttamente una rete locale. Il software da utilizzare per svolgere l'attacco é Metasploit/Armitage in modo similare a quanto visto nelle lezioni di laboratorio.
Si ricorda che per risolvere questo esercizio si dovrá utilizzare solo la macchina attaccante senza eseguire comandi sulla macchina vittima. Sará necessario compiere dei test in modo da assicurare che l'attacco sia avvenuto con successo. Un test utile potrebbe essere quello di reperire la tabella del sito dvwa usato per alcuni esercizi di laboratorio.

**Esercizio 3, Web security**
Viene fornito un sito web nel quale è possibile accedere ad una pagina amministrativa tramite un form di login. Dopo aver analizzato con attenzione il sito web lo studente, tramite le conoscenze acquisite in ambito web security dovrá riuscire a reperire il file delle password presente sul server (localhost).
É possibile visionare i file contenenti il codice PHP ma non modificarne il contenuto.
É necessario un web server per testare gli script.

**Esercizio 4, GPG and integrity**
Nel seguente esercizio é richiesto di verificare l'integritá della libreria allegata libgcrypt tramite gpg e tramite hash.
Per completare l'esercizio é necessario inviare una mail all'indirizzo SPlab@di.unimi.it contenente la chiave pubblica di una coppia di chiavi rsa generate tramite gpg ed allegare un messaggio contenente la propria matricola cifrato con la chiave pubblica allegata (SPlab_key.gpg).

**Esercizio 5, Block chiper attack**
Viene fornito un testo cifrato tramite block chiper in modalitá ECB intercettato durante una conversazione. Lo scopo dell'esercizio consiste nel decifrare il ciphertext e recuperare il plaintext. Non é fornito l'algoritmo di cifratura, si consiglia pertanto di osservare il dominio dei caratteri presenti nel ciphertext.
Si tratta di un testo in lingua inglese.