Sicurezza e privatezza

Tema di laboratorio

10 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 10 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, Buffer overflow

Nel seguente esercizio è richiesto di analizzare il codice fornito nel file bof.c, trovare la vulnerabilitá e tramite essa stampare il contenuto del file secret.txt. Viene fornito il codice sorgente da compilare con il seguente comando *gcc -fno-stack-protector -z execstack nomefile.c -o nomefile* (disabilitazione della protezione di stack smashing).
Si ricorda che prima di eseguire il programma compilato è necessario disabilitare anche la protezione di randomizzazione degli indirizzi (ASLR) tramite: *sudo sysctl -w kernel.randomize_va_space=0*.

Per risolvere l'esercizio in modo corretto é necessario stampare il contenuto di secret.txt tramite stampa del file, si suppone infatti che non si possa accedere al file secret.txt e non si conosca il suo contenuto.

Link utili:
http://shell-storm.org/shellcode/ raccolta di shell code utilizzabili
http://shell-storm.org/shellcode/files/shellcode-603.php execve(/bin/sh)

Esercizio 2, DOS, SYN flood

In riferimento alla lezione di teoria riguardante gli attacchi DOS realizzare un attacco di tipo SYN flooding. Nella realizzazione di questo attacco si chiede di non rendere disponibile un determinato servizio (a piacere) su una macchina remota.
Per la realizzazione dell'attacco si dovrá disporre di due macchine virtuali una "vittima" (si consiglia metasploitable) ed una "attaccante" configurando correttamente una rete locale. Il software da utilizzare per svolgere l'attacco é Metasploit in modo similare a quanto visto nelle lezioni di laboratorio. Come anticipato lo scopo dell'esercizio è quello rendere non disponibile un servizio sulla macchina vittima. Supponendo che si sia scelto il server web, richiedendo una

pagina al server vittima, questo non dovrá rispondere e la connessione dovrá esaurisi dopo un timeout.

Esercizio 3, Web security
Viene fornito un sito web nel quale è possibile accedere ad un blog e postare dei contenuti. Dopo aver analizzato con attenzione il sito web lo studente, tramite cross-site scripting, dovrá riuscire ad iniettare del codice malevolo all'interno del sito, in modo che ogni utente successivo che visiti la pagina web esegua quel codice. Lo scopo dell'attacco é di riuscire a reperire i cookie stampandoli con un alert.
Il tutto deve essere svolto senza modificare il contenuto della pagina HTML.
É necessario un web server per testare gli script.

Esercizio 4, Password cracking
Vengono forniti diversi file nei quali sono presenti password cifrate di account reperite da un hacker. Lo scopo dell'esercizio è recuperare le password in chiaro. Non è presente alcun vincolo sui software da utilizzare, si consigliano i programmi di password cracking visti durante le lezioni di laboratorio per velocizzare il processo.
Il file "password1" contiene solo hash di password numeriche con lunghezza massima di 6 caratteri.

Esercizio 5, Stream chiper attack
Viene fornita la trascrizione di un testo intercettato da una conversazione telefonica cifrata. Lo scopo dell'esercizio consiste nel decifrare il ciphertext e recuperare il plaintext. Non é fornito l'algoritmo di cifratura ma si conoscono alcune informazioni aggiungitive sulla chiave: la lunghezza della chiave é di 2 caratteri MAIUSCOLI.
Si tratta di una conversazione in italiano.