Sicurezza e privatezza

Tema di laboratorio

22 giugno 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 22 giugno 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, Block cipher attack

Viene fornito un testo cifrato 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 italiano.

Esercizio 2, Buffer overflow

Nel seguente esercizio è richiesto di analizzare il codice fornito nel file bufferoverflow.c, trovare la vulnerabilitá e tramite essa stampare la scritta "Buffer overflow success!". 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*.

Esercizio 3, Password cracking

Vengono forniti diversi file nei quali sono presenti password cifrate reperite da un sistema reale. 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.

Esercizio 4, DNS spoofing

In riferimento alla lezione di teoria riguardante DNS attack (sezione Network security) realizzare un attacco di tipo DNS spoofing. Nella realizzazione di questo attacco si chiede di redirigere il traffico di un utente vittima servendo un sito web fantoccio. *Il fine ultimo di questo attacco (non richiesto nell'esercizio) sará quello di estorcere credenziali o informazioni sensibili inserite dalla vittima all'interno del sito fantoccio.*

Per la realizzazione dell’attacco si dovrá disporre di due macchine virtuali una “vittima” ed una “attaccante” configurando correttamente una rete locale. Il software da utilizzare per svolgere l’attacco é Ettercap in modo similare a quanto visto a lezione per ARP poisoning. Come anticipato lo scopo dell’esercizio è quello di visitare un indirizzo dalla macchina vittima e tramite DNS spoofing servire ad essa una pagina web creata a piacere per dimostrare il successo dell'attacco.

Esercizio 5, Web security

Viene fornito un sito web nel quale è possibile completare l'ultimo passaggio di acquisto. Dopo aver analizzato con attenzione il codice lo studente, tramite cross-site scripting, dovrá generare un link malevolo da inviare ad una potenziale vittima. Lo scopo dell'attacco sará di reperire i dati personali dell'utente, in particolare si chiede di recuperare i dati della carta di credito.
Il sito prevede l'utilizzo di un web server con PHP.