Università degli Studi di Torino

Corso di Laurea in Informatica

Esame di Sicurezza – 12 luglio 2016

Nome Cognome

Numero documento

1. Descrivere il metodo di generazione delle chiavi del cifrario RSA, e discuterne la complessità computazionale

2a. la protezione da memory corruption nota come “canarino”:

A) viene realizzata dal sistema operativo

B) viene realizzata dal layer IP

C) viene realizzata dal compilatore

D) viene realizzata dal programmatore

E) non è realizzabile in pratica

2b. il NAPT (network address and port translation)

A) permette di avere un solo indirizzo interno, diverso dall’indirizzo pubblico esterno

B) permette di avere più indirizzi interni, purché identici agli indirizzi pubblici esterni

C) permette di avere piu’ indirizzi interni, purche’ meno numerosi di quelli esterni

D) permette di avere piu’ indirizzi interni, anche con un solo indirizzo pubblico esterno

E) permette di avere un solo indirizzo interno, e piu’ indirizzi pubblici esterni

3. Perché una funzione Hash(M) definita come Xor dei blocchi di M non è collision resistant

4. Effetti della frammentazione IP sul comportamento di un firewall di tipo packet filter

5. Si consideri questo programma C:

```
int main(int argc, char** argv) {
int cookie;
char buf[80];
gets(buf);
if (cookie == 0x41424344)
printf("you win!\n");}
```

Spiegare in concreto come eseguirlo, sfruttando la vulnerabilità della “gets” per forzare l’output “you win”