Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 19 luglio 2007

Usa questa pagina per la brutta, staccala, non consegnarla.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 19 luglio 2007

Cognome:_____ **Nome:** _____ **Matricola:**_____

Sicurezza dei sistemi informatici e delle reti – 19 luglio 2007

Tempo a disposizione: **90 minuti.** Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di cellulari, calcolatrici, palmari e affini.

1. Considera il seguente codice C relativo all'eseguibile "pippo" e rispondi alle seguenti domande.

```
int main(int argc, char** argv)
{
char b[100];
char a[1000];
char* c;
char d[101];
scanf("%9999s", a);
if (argc >= 2)
    strncpy(b, argv[1], 1000); /*copia da argv[1] in b*/
c=getenv("INPUT");
strncpy(d, c, 100);  /* copia da c in d */
…
}
```

1.1. Sottolinea il codice che secondo te dà luogo a vulnerabilità e descrivi schematicamente il problema.

1.2. Supponi che un programma pluto richiami pippo, ad esempio usando la system call execve(). Pluto ottiene tre stringhe X, Y, Z in input dall'utente (fonte non fidata) che passa a pippo con le seguenti modalità

- i primi 999 caratteri di X sono passati a pippo tramite standard input, seguiti da un "\n" (a capo)
- i primi 999 caratteri di Y sono passati a pippo come primo parametro (argv[1])
- i primi 100000 caratteri di Z sono passati a pippo come contenuto della variabile di ambiente "INPUT".

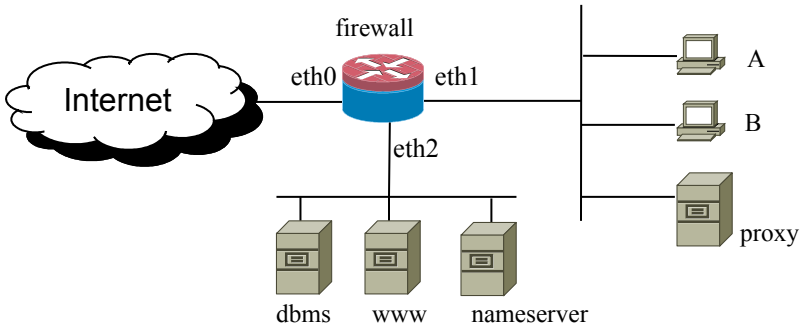
Un utente malevolo che usi il programma pluto che vulnerabilità di pippo riesce a sfruttare? Perché

1.3. Supponi che ti venga richiesto di mettere in sicurezza il sistema ma non hai possibilità di modificare gli eseguibili né di pluto né di pippo che approccio puoi usare? Descrivilo.

Cognome:_____ **Nome:** _____ **Matricola:**_____

Sicurezza dei sistemi informatici e delle reti – 19 luglio 2007

2. Considera la rete in figura con la matrice di accesso indicata, in cui i servizi di interesse sono tre: dns, web, e db.



A Da	A	B	Proxy	Dbms	www	Nameserver	Internet
A		-	Rich. web	Rich. db	-	Rich. dns	-
B	-		Rich web	Rich. db	-	Rich. dns	-
Proxy	Risp. web	Risp. web		-	Rich. web	Rich. dns	Rich. web
Dbms	Risp. db	Risp. db	-		Risp. db	-	-
www	-	-	Risp. web	Rich. db		-	Risp. web
Nameserver	Risp. dns	Risp. dns	Risp. dns	-	-		Risp./Rich. dns
Internet	-	-	Risp. web	-	Rich. web	Risp./Rich. dns	

Rispondi alle seguenti domande.

2.1. Evidenzia sulla matrice di accesso le parti che non sono realizzabili per mezzo del firewall.

2.2. Che tecnica suggeriresti per realizzare le parti della matrice di accesso identificate nella domanda precedente? Cerca di dare una soluzione che non preveda l'acquisto di ulteriori apparati.

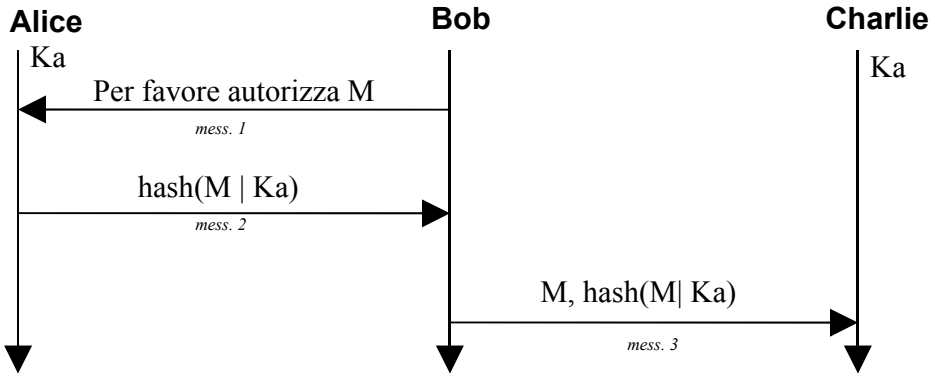
2.3. Per l'implementazione pensi che possa essere impiegato facilmente un firewall stateless? Perché?

2.4. Dai la configurazione del firewall, usando preferibilmente la sintassi di netfilter delle parti sottolineate della matrice di accesso. Al posto degli indirizzi usa i nomi delle macchine, al posto delle porte usa i nomi dei servizi (dbms, dns, www).

Cognome:_____ **Nome:** _____ **Matricola:**_____

Sicurezza dei sistemi informatici e delle reti – 19 luglio 2007

3. Bob, per chiedere a Charlie di effettuare una certa azione, deve dimostrare che Alice e' d'accordo. La richiesta è contenuta in un messaggio M in linguaggio naturale creato da Bob. Il protocollo usato è il seguente, dove Ka e' un segreto condiviso tra Alice e Charlie.



Se l'hash inviato in messaggio 3 e' corretto Charlie accetta la richiesta. Rispondi alle seguenti domande

3.1. Supponi che Alice voglia far credere a Charlie che Bob abbia richiesto di autorizzare il messaggio M'. Pensi sia possibile? Come?

3.2. Suggerisci un protocollo, sempre basato su chiave simmetrica, che non abbia il problema riscontrato al punto precedente.

3.3. Supponi che ci siano un gran numero di richieste che Alice autorizza facilmente (messaggi buoni) e un gran numero di richieste che Alice non autorizza (messaggi cattivi). Bob vuol far credere a Charlie che Alice ha autorizzato un messaggio cattivo qualsiasi. La lunghezza dell'hash è 64 bit ma per bob è possibile fare in

Cognome:_____ **Nome:** _____ **Matricola:**_____

Sicurezza dei sistemi informatici e delle reti – 19 luglio 2007

tempi ragionevoli una ricerca su uno spazio di ricerca di 2^{34} elementi. Pensi che Bob possa riuscire nell'impresa? In caso affermativo che approccio potrebbe adottare?

4. Rispondi alle seguenti domande circa la pianificazione della sicurezza.

4.1. Elenca almeno tre motivi per cui è utile pianificare la sicurezza

4.2. Elenca in sintesi le parti che ritieni fondamentali in un piano di sicurezza.

4.3. In che rapporto sono il Documento Programmatico di Sicurezza previsto dalla legge 196/2003 e il piano di sicurezza?

5. Considera i seguenti file e directory in un filesystem unix con i loro permessi. Gli utenti Pluto e Paperino appartengono al gruppo Disney, mentre Pippo non appartiene a tale gruppo.

Permessi	**Utente**	**Gruppo**	**Path**
d r-x r-x r-x	Root	Root	/
- rw- r-- ---	Pippo	Disney	/file1

Cognome:_____ **Nome:** _____ **Matricola:**_____

Sicurezza dei sistemi informatici e delle reti – 19 luglio 2007

d r-x rwx r-x	Paperino	Disney	/repository
- r-- rw- rw-	Paperino	Disney	/repository/file2
- --- --- r--	Pluto	Disney	/repository/file3

Supponendo i permessi immutabili, esprimi con una matrice di accesso su S={Pippo, Pluto, Paperino}, O={file1, file2, file3, repository} lo stato del sistema. I diritti da indicare nella matrice sono: per i file R_{file}={R (read), W (write), D (cancella il file), N (rinomina)}, per la directory R_{dir}={L (lista della directory), C (creazione di un nuovo file nella directory)}.

	File1	**File2**	**File3**	**repository**
Pippo				
Pluto				
Paperino				

6. Cosa è SELinux? in che senso è considerato "più sicuro" di Linux?

7. Se leggi su un data sheet che un prodotto è certificato Common Criteria "eal 4", pensi che questa informazione sia sufficiente per valutare il suo livello di sicurezza? Quali ulteriori indagini suggeriresti? Illustra brevemente il concetto di "livello di garanzia" in Common Criteria rispetto a questo problema.

8. Considera la seguente matrice di accesso. S={u1, u2, u3, u4, u5}, O={f1, f2, f3, f4, f5 }, R={r, w, x, g} (read, write, execution, grant **con attenuazione del privilegio,** cioè non si può cedere diritti che non si hanno).

	f1	f2	f3	f4
u1	r	r	g	
u2	w	w		
u3		r	wg	r
u4			r	w

Rispondi alle seguenti domande.

Cognome:_____ **Nome:** _____ **Matricola:**_____

Sicurezza dei sistemi informatici e delle reti – 19 luglio 2007

8.1. La politica mostrata è MAC, DAC o altro? motiva la risposta.

mac dac altro

Motivazione:

8.2. Pensi sia possibile per u1 comunicare informazioni a u4 **eventualmente con la collaborazione di altri utenti**? in che modo?

8.3. Una "comunità" è un insieme di soggetti tali che ciascuna coppia di soggetti di una comunità può scambiare informazioni (anche indirettamente) in entrambi i versi. Quali comunità nascono dalla matrice di accesso mostrata nel caso in cui nessuno applichi il diritto di grant?.

8.4. Quali comunità nascono dalla matrice di accesso mostrata nel caso in cui si possa applicare il dirtto di grant?.

8.5. Se i diritti di u3 su f3 fossero "rwg" quali comunità nascerebbero dall'applicazione di grant?.