Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 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 testo. "*La rete aziendale è composta da una rete interna e da una DMZ, entrambe collegate ad Internet da un solo firewall di tipo stateful. La DMZ contiene un NIDS e un server P con un processo che fa da web proxy. Il server P adotta un modello di controllo di accesso di tipo MAC.*"
Rispondi alle seguenti domande segnando le risposte che pensi essere corrette?

1.1. Il firewall è...
€ uno screening router € un firewall di livello 3-4 € un firewall applicativo

1.2. Quante zone smilitarizzate ci sono?
0 € 1 € 2 € 3 €

1.3. C'è un sistema di rilevamento delle intrusioni
€ collegato alla rete, € installato nel server P, € nel firewall,

1.4. Il sistema di controllo di accesso del server P è
€ discrezionario € mandatorio € altro

1.5. Quante interfacce deve avere (almeno) il firewall?
0 € 1 € 2 € 3 €

1.6. Il proxy è...
€ uno screening router € un firewall di livello 3-4 € un firewall applicativo

2. Confronta sinteticamente i concetti di certificazione di prodotto/sistema (es. Common Criteria) e certificazione di processo (es. iso17799/iso27001).

3. Considera il seguente codice C e rispondi alle seguenti domande.

```
int f()
{
char b1[20];
char b2[100];
char* b3;
scanf("%19s", b1);
b3=getenv("PATH");
strcpy(b2, b1);  /*strcpy copia da b1 in b2*/
strcpy(b1, b3);
…
}
```

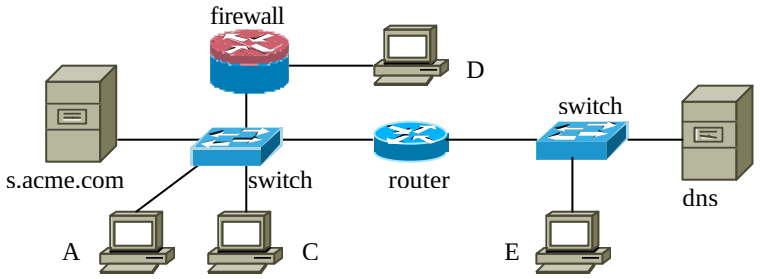
Cognome:_____ **Nome:** _____ **Matricola:**_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

3.1. Sottolinea il codice che secondo te dà luogo ad una vulnerabilità e descrivi schematicamente il problema.

3.2. Dai una descrizione schematica dell'exploit.

4. Considera la rete in figura.



Il firewall è statefull ed è configurato in modo che D possa solo aprire sessioni tcp verso s.acme.com. La tabella di instradamento del router è correttamente configurato. Sulle macchine A, s.acme.com, C, D ed E non è configurata alcuna altra forma di protezione. Rispondi alle seguenti domande.

4.1. Supponi che A abbia attiva una sessione tcp con s.acme.com. Quali tra le macchine C, D ed E possono sniffare tale comunicazione? perché? se pensi sia possibile, in che modo?

4.2. Stesse ipotesi della domanda precedente. Quali tra le macchine C, D ed E possono fare hijacking della sessione tcp? perché? se pensi sia possibile, in che modo?

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

4.3. Supponi che sia noto che A instauri regolarmente comunicazioni http con s.acme.com e prima di ciascuna comunicazione risolva il nome facendo uso del DNS. Quali tra le macchine C, D ed E possono impersonare s.acme.com? perché? se pensi sia possibile, in che modo?

5. Considera la seguente matrice di accesso. S={u1, u2, u3, u4, u5}, O={f1, f2, f3, f4, f5 }, R={r, w, x} (read, write, execution).

	f1	f2	f3	f4	f5
u1	rwx	r			
u2		w		w	r
u3	r		w		
u4		w	rx		
u5				rwx	w

Rispondi alle seguenti domande.

5.1. La politica mostrata è MAC, DAC o altro?

€ mac € dac € altro
motiva la risposta

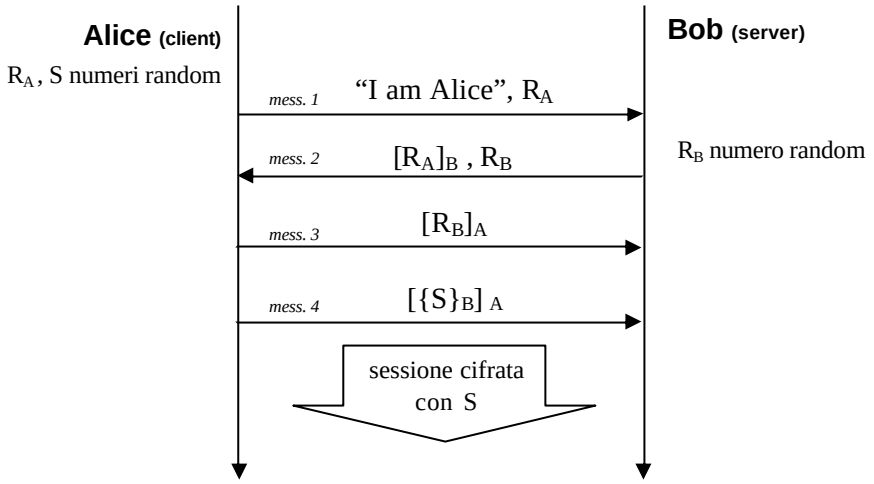
5.2. Pensi sia possibile per u1 comunicare informazioni a u4 **anche indirettamente**? eventualmente in che modo?

5.3. 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? (Per trovare la soluzione ti può essere utile un grafo che mostri i possibili flussi di dati).

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

6. In una rete tutti i soggetti sono dotati di una chiave privata e i corrispondenti certificati x509v3 sono noti a tutti. Il protocollo usato per l'autenticazione e la negoziazione di una chiave di sessione è il seguente.



Rispondi alle seguenti domande

6.1. Il protocollo permette una autenticazione one-way o mutua? perché?

6.2. Supponi che nel messaggio 4 la chiave di sessione S venga trasmessa non firmata, cioè semplicemente $\{S\}_B$. Pensi che il protocollo sia vulnerabile? Spiega.

6.3. Supponi che Cindy abbia una registrazione di una trasmissione tra Alice e Bob che inizia con il protocollo mostrato. Quali messaggi dell' handshake sono utili per decifrare la registrazione?

Messaggio 1 € Messaggio 3 €
Messaggio 2 € Messaggio 4 €

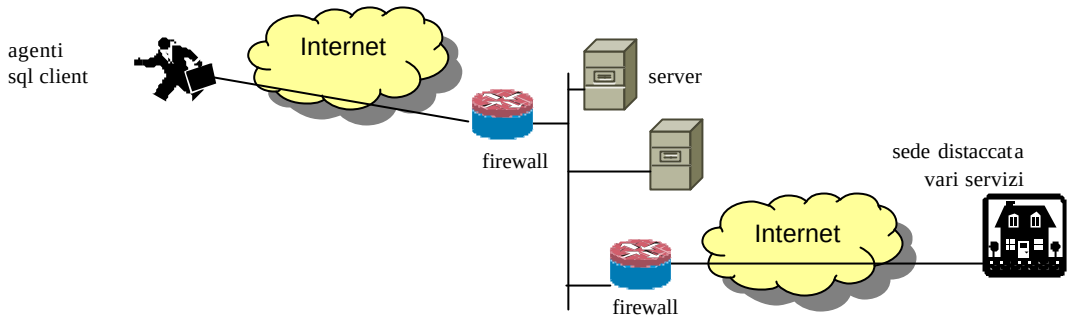
Di quali chiavi ha bisogno Cindy per decifrare la registrazione?

La chiave pubblica di Alice € La chiave pubblica di Bob €
La chiave privata di Alice € La chiave privata di Bob €

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

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

7. Una ditta ha nei suoi server dei dati sensibili relativi allo stato di salute dei suoi clienti per i quali si deve rispettare la legge 196/2003. I dati sono acceduti dagli agenti tramite un client che accede ad un dbms mediante SQL e da una sede distaccata che usa vari protocolli su ip. La situazione è mostrata schematicamente nella seguente figura.



7.1. Che modalità di accesso suggeriresti per la sede distaccata?

7.2. Che modalità di accesso suggeriresti gli agenti?

7.3. Che ulteriori precauzioni suggeriresti per rispettare la legge 196/2003?

8. Sicurezza di sistema unix: cosa è PAM? Descrivi le sue caratteristiche principali.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

A

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 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 testo. *"La rete aziendale è composta da una rete interna e da una DMZ. La DMZ è collegata ad Internet da un firewall in grado di tracciare connessioni tcp. La rete interna è collegata alla DMZ da un proxy web P. Entrambe le reti hanno un NIDS installato al proprio interno. Macchina proxy P adotta un modello di controllo di accesso di tipo DAC."*
Rispondi alle seguenti domande segnando le risposte che pensi essere corrette?

1.1. Quanti firewall applicativi ci sono nella rete?
0 € 1 € 2 € 3 €

1.2. La DMZ può essere acceduta da Internet?
€ si € no € si ma in maniera controllata

1.3. Quanti sono i sistemi di rilevamento delle intrusioni in totale
0 € 1 € 2 € 3 €

1.4. Il sistema di controllo di accesso del proxy P è
€ discrezionario € mandatorio € altro

1.5. Il firewall che collega la DMZ a Internet è...
€ uno screening router € un firewall di livello 3-4 € un firewall applicativo

1.6. Una richiesta web dalla rete interna per Internet quanti firewall deve attraversare?
0 € 1 € 2 € 3 € 4 €

2. Confronta sinteticamente i concetti di certificazione di prodotto/sistema (es. Common Criteria) e certificazione di processo (es. iso17799/iso27001).

3. Considera il seguente codice C e rispondi alle seguenti domande.

```
int f()
{
char b1[200];
char b2[100];
char* b3;
scanf("%199s", b2);
b3=getenv("CLASSPATH");
strcpy(b1, b2);  /*strcpy copia da b1 in b2*/
strncpy(b1, b3, 199);
…
}
```

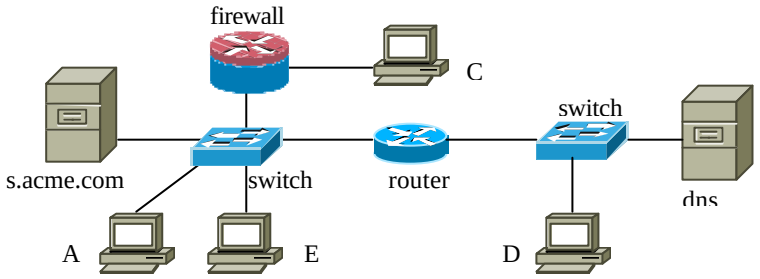
Cognome:_____ **Nome:** _____ **Matricola:**_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

3.1. Sottolinea il codice che secondo te dà luogo ad una vulnerabilità e descrivi schematicamente il problema.

3.2. Dai una descrizione schematica dell'exploit.

4. Considera la rete in figura.



Il firewall è statefull ed è configurato in modo che C possa solo aprire sessioni tcp verso s.acme.com. La tabella di instradamento del router è correttamente configurato. Sulle macchine A, s.acme.com, C, D ed E non è configurata alcuna altra forma di protezione. Rispondi alle seguenti domande.

4.1. Supponi che A abbia attiva una sessione tcp con s.acme.com. Quali tra le macchine C, D ed E possono sniffare tale comunicazione? perché? se pensi sia possibile, in che modo?

4.2. Stesse ipotesi della domanda precedente. Quali tra le macchine C, D ed E possono fare hijacking della sessione tcp? perché? se pensi sia possibile, in che modo?

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

4.3. Supponi che sia noto che A instauri regolarmente comunicazioni http con s.acme.com e prima di ciascuna comunicazione risolva il nome facendo uso del DNS. Quali tra le macchine C, D ed E possono impersonare s.acme.com? perché? se pensi sia possibile, in che modo?

5. Considera la seguente matrice di accesso. S={u1, u2, u3, u4, u5}, O={f1, f2, f3, f4, f5 }, R={r, w, x} (read, write, execution).

	f1	f2	f3	f4	f5
u1	r		w		
u2		w	rx		
u3				rwx	w
u4	rwx	r			
u5		w		w	r

Rispondi alle seguenti domande.

5.1. La politica mostrata è MAC, DAC o altro?

€ dac € mac € altro
motiva la risposta

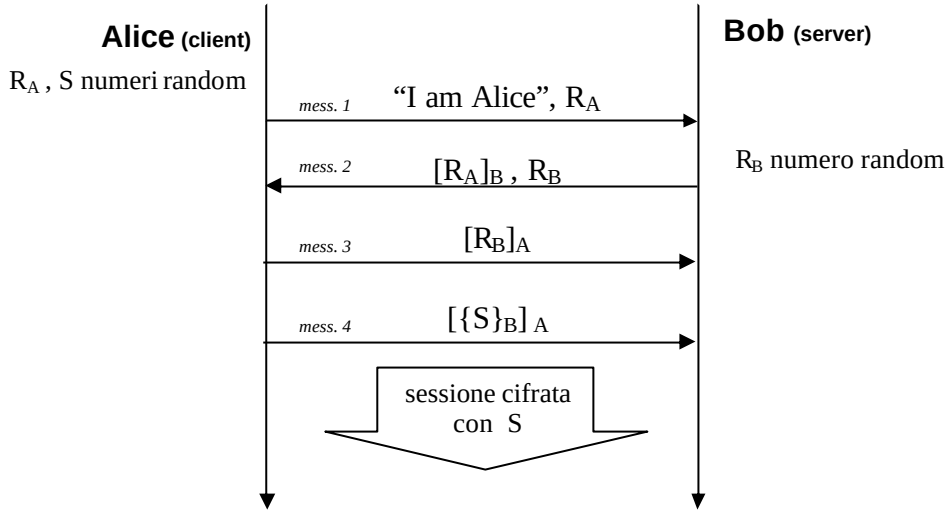
5.2. Pensi sia possibile per u4 comunicare informazioni a u2 **anche indirettamente**? eventualmente in che modo?

5.3. 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? (Per trovare la soluzione ti può essere utile un grafo che mostri i possibili flussi di dati).

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

6. In una rete tutti i soggetti sono dotati di una chiave privata e i corrispondenti certificati x509v3 sono noti a tutti. Il protocollo usato per l'autenticazione e la negoziazione di una chiave di sessione è il seguente.



Rispondi alle seguenti domande

6.1. Il protocollo permette una autenticazione one-way o mutua? perché?

6.2. Supponi che nel messaggio 4 la chiave di sessione S venga trasmessa non firmata, cioè semplicemente $\{S\}_B$. Pensi che il protocollo sia vulnerabile? Spiega.

Supponi che Cindy abbia una registrazione di una trasmissione tra Alice e Bob che inizia con il protocollo mostrato. Di quali chiavi ha bisogno Cindy per decifrare la registrazione?

La chiave pubblica di Alice € La chiave pubblica di Bob €

La chiave privata di Alice € La chiave privata di Bob €

Quali messaggi dell' handshake sono utili per decifrare la registrazione?

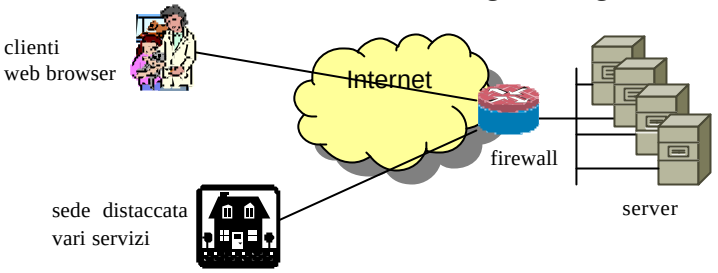
Messaggio 1 € Messaggio 3 €

Messaggio 2 € Messaggio 4 €

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

7. Una ditta ha nei suoi server dei dati sensibili relativi allo stato di salute dei suoi clienti per i quali si deve rispettare la legge 196/2003. I dati sono acceduti dai clienti tramite web e da una sede distaccata che usa vari protocolli su ip. La situazione è mostrata schematicamente nella seguente figura.



7.1. Che modalità di accesso suggeriresti i clienti?

7.2. Che modalità di accesso suggeriresti per la sede distaccata?

7.3. Che ulteriori precauzioni suggeriresti per rispettare la legge 196/2003?

8. Sicurezza di sistema unix: che cosa è il set user id bit? Spiega e mostra un esempio.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 febbraio 2007

B