Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

Tempo a disposizione: 70 minuti. Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di smartphone, calcolatrici e affini.

1. Protocolli crittografici.

1.1. Fornisci un esempio di protocollo di autenticazione one-way vulnerabile a "replay attack".

A (client) B (server)

Descrivi l'attacco:
Vedi materiale didattico

1.2. Fornisci un esempio di protocollo di mutua autenticazione vulnerabile a "reflection attack".

A (client) B (server)

Descrivi l'attacco:
Vedi materiale didattico

2. Confronta il normale Piano di Sicurezza con il Documento Programmatico di Sicurezza.

	Piano di sicurezza	**Documento Programmatico di Sicurezza**
Obiettivi		
Obbligatorietà		
Contenuti	Vedi materiale didattico	
Altro		

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

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

3. **Sicurezza del codice.** Analizza la sicurezza nei seguenti stralci di codice C relativi alla lettura di una stringa da standard input in cui la lunghezza della stringa è codificata in binario con due bytes all'inizio della stessa.

3.1.
```
int main(int argc, char** argv) {
        short len; /* intero di 2 bytes con segno */
        char buffer[100];
        read(stdin, &len, 2); /*legge l'intero direttamente in binario*/
        read(stdin, buffer, len);
        buffer[len]='\0';   /*termina con zero*/
        . . .
}
```

len può assumere valori tra -2^15 e 2^15-1 ma read() considererà comunque il valore senza segno quindi tra 0 e 2^16-1
buffer ha una lunghezza fissa molto più piccola di 2^16-1 e quindi è facile avere un buffer overflow.

3.2.
```
int main(int argc, char** argv) {
        short len; /* intero di 2 bytes con segno */
        char buffer[100];
        read(stdin, &len, 2); /*legge l'intero direttamente in binario*/
        if ( len+1 > 100 ) {
              . . . /*gestione errore*/
        }
        read(stdin, buffer, len);
        buffer[len]='\0';   /*termina con zero*/
        . . .
}
```

anche assumendo che la gestione dell'errore sia corretta (cioè che la seconda read() non venga eseguita in caso di errore) si può comunque avere un buffer overflow nel caso in cui len<0, in tal caso infatti la verifica non rileverà alcun errore ma la read() considererà len senza segno e quindi leggerà un numero di bytes
pari a 2^16-len, cioè potenzialmente molto più di 100.

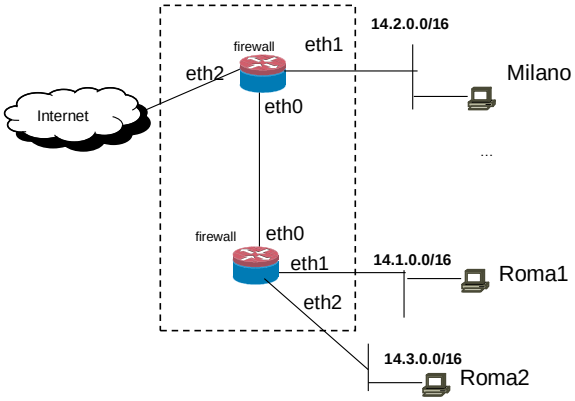
3.3.
```
int main(int argc, char** argv) {
        short len; /* intero di 2 bytes con segno */
        char* buffer; /*riga errata nel testo*/
        read(stdin, &len, 2); /*legge l'intero direttamente in binario*/
        buffer=malloc(len+1);
        read(stdin, buffer, len);
        buffer[len]='\0';   /*termina con zero*/
        . . .
}
```

in questo caso il fatto che len sia dichiarato con o senza segno è irrilevante poiché non vengono effettuati confronti e sia read() che malloc() considereranno comunque il valore senza segno quindi tra 0 e 2^16-1.
tuttavia, nel caso in cui len=-1 malloc() allocherà zero bytes ma read() leggerà 2^16-1 bytes.
Se avessimo dichiarato len senza segno il ragionamento non sarebbe cambiato poiché in virtù dell'overflow per len=2^16-1, len+1=0. Notare come la realizzazione del calcolo len+1 sia identico sia nel caso di len con segno che senza segno (proprietà della rappresentazione in complemento a 2 dei numeri con segno).

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

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

4. Sicurezza delle reti. Considera la rete in figura.



Supponi che le tabelle di routing dei firewall siano correttamente configurate per assicurare la raggiungibilità completa, non ci sia alcun tipo di NAT e la configurazione del firewall di Roma sia la seguente.

Roma

```
:FORWARD DROP
-A FORWARD –i eth1 -m state --state NEW -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

4.1. Supponi di voler realizzare la seguente matrice di accesso per il sistema dei due firewall ("-" indica che non può passare traffico).

A / **Da**	Roma1	Roma2	Milano	Internet
Roma1	----------	Query	-	-
Roma2	Reply	----------	Reply	Reply
Milano	-	Query	----------	Query
Internet	-	Query	Reply	----------

Dai la configurazione del firewall di Milano, se possibile, o spiega perché è impossibile. (Usa preferibilmente la sintassi di iptables/netfilter).

Milano

```
:FORWARD DROP
-A FORWARD –i eth1 -m state --state NEW -j ACCEPT
-A FORWARD –i eth2 –o eth0 -m state --state NEW -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

tuttavia le query da Internet e Milano verso Roma2 non possono passare il FW di Roma.

Per realizzare completamente la matrice di accesso bisognerebbe modificare il router di Roma con la seguente regola

Roma

```
-A FORWARD –i eth0 –o eth2 -m state --state NEW -j ACCEPT
```

4.2. Discuti l'impatto della presenza di costrutti tipo "–s 14.3.0.0/16" (match indirizzo ip sorgente) nella configurazione del firewall di Milano sulla sicurezza.

la presenza di un matching su indirizzo sorgente in generale può esporre a rischi di attacchi di spoofing qualora sia usato in una regola di tipo ACCEPT. Tali regole possono essere usate in sicurezza in presenza di filtri anti spoofing per il prefisso in questione con precedenza rispetto alla regola che fa il matching per indirizzo sorgente, es. per il FW di Milano

```
-A FORWARD –i eth2 –s 14.3.0.0/16 -j DROP
-A FORWARD –i eth1 –s 14.3.0.0/16 -j DROP
-A FORWARD … regola accept basata su -s 14.3.0.0/16
```

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

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

5. Sicurezza dei sistemi. Controllo di accesso per il filesystem in Unix.

5.1. Il controllo di accesso per il filesystem in Unix è discrezionario o mandatorio? perché?

DAC, ciascun utente può decidere i permessi dei propri files.

5.2. Considera la seguente configurazione di permessi e compila la matrice di accesso sottostante.

```
drwxr-xr-x      root root       /etc/
-rw-r--r--      root root       /etc/passwd
-rw-r-----      root shadow     /etc/shadow
drwxr-xr-x      root root       /etc/ssl/
drwx--x---      root ssl-cert   /etc/ssl/private/
-rw-r--r--      root ssl-cert   /etc/ssl/private/certificate
drwxr-xr-x      root root       /bin/
-rwxr-sr-x      root shadow     /bin/expiry
```

Nella matrice di accesso considera sempre che gli utenti accedono a file e directory tramite i propri processi che assumiamo essere lanciati dalla propria home. I diritti da indicare nella matrice di accesso sono i seguenti.

File: **R** (apertura file in lettura), **W** (apertura file in scrittura), **X** (esecuzione)

Directory: **L** lettura lista dei file, **A** aggiunta di un file, **D** cancellazione di un file, **S** usare la directory in un pathname specificato per una qualsiasi system call.

oggetto (file) → **soggetto (Utente) ↓**		file: passwd	file: shadow	directory: /etc/ssl/	directory: /etc/ssl/ private/	file: certificate	file: expiry
utente	**gruppo**						
pippo	pippo	R		LS			RX
shadow	shadow	R	R	LS			RX
apache	ssl-cert	R		LS	S	R	RX
root	root	RW	RW	LADS	LADS	RW	RWX

5.1. Commenta brevemente qui le tue risposte per le colonne relative a “private”, “certificate”, “expiry” e alla riga relativa a “root”.

private

Solo l’owner (root) può accedere in lettura e scrittura alla directory, ma il gruppo può usare file all’interno(S)

certificate

E’ all’interno di private quindi others non possono accedere alla directory, il gruppo si, ma solo in lettura, root anche in scrittura.

expiry

Tutti possono leggere ed eseguire (root anche scrivere). L’esecuzione comporta EGID=shadow ma questo non appare nella matrice di accesso.

root

RWLADS sono accordati indipendentemente dai permessi configurati. X dipende dai permessi.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

6. Sicurezza in ambiente Windows. Security reference monitor.

6.1. Quali sono gli input del security reference monitor?

Vedi materiale didattico

6.2. Quali è l'output del security reference monitor?

Vedi materiale didattico

6.3. Riporta l'algoritmo applicato dal security reference monitor?

Vedi materiale didattico