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

Sicurezza dei sistemi informatici e delle reti – 7 febbraio 2012

Scrivi qui GRANDE
509 (5 cfu) o 270 (6 cfu)

Tempo a disposizione: 60 (DM509) o 70 (DM270) minuti.
Libri e appunti chiusi. Vietato comunicare con chiunque.
Vietato l'uso di cellulari, calcolatrici, palmari e affini.

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

```
int main(int argc, char** argv) {
        char from[1001];
        char to[2001];
        char *args[2];
        scanf("%2000s %1000s", from, to);
        args[0]="/bin/cp";
        args[1]=from;
        args[2]=to;
        args[3]=NULL;
        execve(args[0], args, NULL);
        printf("copia eseguita con successo")
}
```

1.1. Sottolinea le righe di codice che introducono una vulnerabilità.

1.2. Elenca i problemi di sicurezza che riscontri nel codice sopra riportato.

i limiti nella scanf per from e to sono invertit e su from è possibile un overflow.
la chiamata ad execve non è un problema

1.3. Nel fare i test si riscontra che "copia eseguita con successo" non viene mai stampato? Che significa?

questo è il comportamento nomrale di execve, il processo cessa di esistere e viene sostituito in questo caso da /bin/cp (rimane solo il pid)

1.4. Supponi di sostituire `execve(args[0], args, NULL)` con il seguente codice

```
char cmd[3020];
sprintf(cmd, "/bin/cp %s %s", from, to); /* come printf ma output nella stringa cmd*/
system(cmd);   /* esegue cmd in una shell */
```

Che problemi di sicurezza riconosci?

poiché cmd viene eseguito in una shell e il comando viene creato a partire da from e to, tramite questi argomenti l'utente non fidato potrebbe inserire codice malevolo da eseguire nella shell come per esempio `rm -Rf *`

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

Sicurezza dei sistemi informatici e delle reti – 7 febbraio 2012

2. Rispondi alle seguenti domande su Distributed DoS

2.1. Descrivi il concetto di botnet e il ruolo svolto nei DDoS?

vedi materiale didattico

2.2. Descrivi il DDoS noto come syn-flood e i meccanismi su cui fa leva per interrompere il servizio.

vedi materiale didattico

2.3. Descrivi la contromisura nota come syn-cookies?

vedi materiale didattico

3. Il client Alice contatta il server Bob, sulla stessa lan, usando il protocollo ssl con la seguente cypher suite: TLS_RSA_WITH_RC4_128_SHA. Cindy, sulla stessa lan, vorrebbe visionare il contenuto della comunicazione. Rispondi alle seguenti domande.

3.1. Supponi che Cindy voglia sniffare il traffico tra A e B, se la lan è switchata che tecnica deve adottare?

Arp poisoning o mac flood.

3.2. Supponi che Cindy sniffi il traffico fra A e B, riesce a vedere il contenuto in chiaro o cifrato?

Chiaro **cifrato** (metti una x sulla risposta corretta)

3.3. Il server è autenticato? **SI** **NO** (metti una x sulla risposta corretta)

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

Sicurezza dei sistemi informatici e delle reti – 7 febbraio 2012

3.4. Il client è autenticato? **SI** **NO** (metti una x sulla risposta corretta) non è possibile capirlo dalla cypher suite, è stato ignorato nella correzione, in generale il client può essere autenticato o meno.

3.5. Supponi che Cindy sia a conoscenza di tutti i segreti a lungo termine in gioco. Cindy riesce a decodificare il traffico? Descrivi il perché.

DECODIFICA **NON DECODIFICA** (metti una x sulla risposta corretta)

Perché?

è possibile decifrare la session key scambiata e con quella decifrare il resto

3.6. Conosci un modo per evitare che la conoscenza dei segreti a lungo termine possa permettere a Cindy di decodificare il traffico semplicemente sniffandolo?

Utilizzando una cypher suite che dia perfecte forwared secrecy esempio DHE_....
In tal caso Cindy può ancora vedere in chiaro il traffico ma non lo può fare semplicemente sniffando deve fare MitM.

4. Rispondi alle seguenti domande sul **confinamento** e sul **controllo di accesso nei sistemi unix**

4.1. E' possibile **per un utente** X far sì che i propri file siano accessibili solo da X? Eventualmente descrivi come.

Si
chmod go-rwx nomefile
oppure
chmod go-x homeX

4.2. E' possibile **per un amministratore** far sì che i file dell'utente X siano accessibili solo da X indipendentemente dalla sbadataggine di X? Eventualmente descrivi come.

si, usando un chroot jail, o usando il seguente approcccio
la home non è di X ma di root (l'utente non può cambiare i permessi della propria home)
un gruppo "utente" contiene solo X
la home di X è del gruppo utente
i permessi sono completi per il gruppo e nulla per gli altri
chown root.utente homeX
chmod 770 homeX

4.3. E' possibile **per un amministratore** far sì che un utente X possa a suo piacimento installare processi server (es. TCP) ma un utente Y, diverso da X, no? Eventualmente descrivi come.

Nel modello DAC standard di unix non è possibile, perché le porte non hanno nessun tipo di acl.
E' possibile in SELinux o usando metodi di virtualizzazione.
Non è possibile con un semplice chroot-jail.

5. Analisi dei rischi

5.1. Nella pianificazione della sicurezza informatica, i risultati dell'analisi dei rischi che ruolo hanno?

rappresenta l'input per la progettazione delle contromisure che mirano trattare ciascun rischio in modo che il rischio residuo sia accettabile.

5.2. Elenca tutti i modi che conosci per trattare i rischi e descrivili brevemente.

mitigare: ridurre la probabilità che l'evento avverso si verifica – proattivo (es. antivirus)
fronteggiare: ridurre l'impatto – tipicamente si prepara proattivamente un qualche tipo di reazione (es. backup), casi particolari sono approcci disaster recovery e business continuity
trasferire o condividere: assicurazione o mutuo soccorso
evitare: soluzione drastica, si evita l'attività che implica il rischio.

5.3. Discuti il trattamento dei rischi ad altissimo impatto e bassissima probabilità (**disastri**) in ambito informatico.

vedi materiale didattico

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

Sicurezza dei sistemi informatici e delle reti – 7 febbraio 2012

6. [solo per 270] Sicurezza in ambiente Windows.

6.1. Descrivi la struttura e la semantica delle **ACL** contenute nel security descriptor per gli executive objects di Windows.

il security descriptor di ciascun executive object contiene un ACL che è una lista ordinata di Access control entries. Ciascuna ha il seguente formato:

<allow|deny, soggetto, operazione>

6.2. Descrivi tutti gli input e l'output del **security refernce monitor** di Windows.

Input:
soggetto: identificato dall'access token del processo che ha richiesto l'accesso
oggetto: l'executive object
operazione: l'access mask elenca le operazioni richieste
security data (security db): contenuto del security descriptor (cioè l'ACL)
Output:
accesso consentito o accesso negato. Se l'accesso è consentito l'access mask verrà memorizzata assieme alla handle nella process handle table.

6.3. Descrivi il **controllo di accesso mandatorio** in Windows e i suoi scopi.

vedi materiale didattico