Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 7 febbraio 2012

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 7 febbraio 2012

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

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.

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

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?

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?

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

2.3. Descrivi la contromisura nota come syn-cookies?

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?

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)

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

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?

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?

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.

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.

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.

5. Analisi dei rischi

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

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

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

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.

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

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