Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 15 luglio 2010

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 15 luglio 2010

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 15 luglio 2010

Tempo a disposizione: 70 (509) 80 (270) minuti. Libri e appunti chiusi.
Vietato comunicare con chiunque.
Vietato l'uso di cellulari, calcolatrici, palmari e affini.

Scrivi qui GRANDE 509 o 270

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

```
int main(int argc, char** argv){
char a[101];
char* d;
getwd(a);    /* ottieni la directory corrente */
d= (char*)malloc(1000);
scanf("%9999", d);
...
}
```

1.1. Sottolinea il codice che secondo te dà luogo a vulnerabilità.

1.2. Per ciascuna vulnerabilità mostra i problemi descrivendo brevemente come si può effettuare un attacco.

1.3. Supponi di essere responsabile della sicurezza dell'esecuzione di tale codice e di non poter cambiare l'eseguibile. Considera le vulnerabilità identificate ai punti 1.1 e 1.2, cosa dovrebbe fare un wrapper minimale per rendere impossibile un uso malevolo del software?

1.4. Considera le vulnerabilità di tipo buffer overflow riscontrate in 1.1. e 1.2 e i relativi attacchi. Considera i retrun pointer che vengono sovrascritti. Tali return pointer sono relativi a stack frame di certe chiamate a funzione. **Quali?** Mostra il layout dello stack supponendo che questo cresca verso indirizzi alti.

Nomi funzioni

Stack layout

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 15 luglio 2010

2. AAA nei sistemi DAC e MAC.

2.1. Quali sono le operazioni comprese sotto il nome di AAA? Dai un diagramma che ne mostri l'ordine di esecuzione di tali operazioni nei sistemi DAC.

2.2. Come si modifica il diagramma nei sistemi MAC? Qual'è l'impatto sul controllo di accesso?

2.3. Per ciascuno degli elementi/operazioni di cui hai discusso nei due punti precedenti dai un esempio di tecnologia realizzativa.

3. Considera un utente che accede ad un sito "sicuro" e invia dati tramite una form. Rispondi alle seguenti domande sulla sicurezza dell'operazione.

3.1. Se **l'utente vede** solo un lucchetto chiuso nel browser ciò è sufficiente per assicurargli la sicurezza del sito? Che attività suggeriresti all'utente per essere maggiormente sicuro?

3.2. Se il sito è basato su frame e l'utente **non vede il lucchetto** secondo te è possibile che i dati sottomessi con la form siano comunque inviati in sicurezza? Perché?

E' possibile?

Perché?

3.3. Che verifiche deve fare il browser sul certificato?

3.4. Cosa sono le trust anchor? Se il computer su cui sta navigando l'utente non è fidato, che problemi ci possono essere con le trust anchor?

4. Protocolli di autenticazione.

4.1. Mostra un protocollo di autenticazione a chiave simmetrica **vulnerabile** al **replay** attack.

4.2. Descrivi il concetto di nonce e le sue proprietà fondamentali per l'uso nell'autenticazione.

5. Ti viene chiesto di occuparti della pianificazione della sicurezza di una realtà produttiva. Per una efficiacia dell'azione dovresti attenerti a delle buone pratiche. Rispondi alle seguenti domande.

5.1. Accetteresti l'incarico pur sapendo che il management non è al corrente della tua attività? Motiva.

5.2. Quali principi di **analisi e mitigazione del rischio** adotteresti?

5.3. A valle dell'analisi del rischio e del progetto delle contromisure devi pianificare le azioni (**tempi, budget**, **altre risorse**) per mettere in sicurezza l'azienda. Che principi adotteresti?

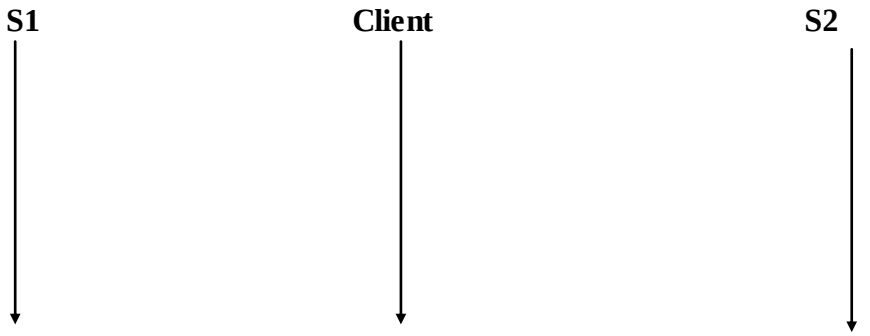
5.4. Il piano è molto complesso. Come gestisci la responsabilità della sua corretta applicazione? Che strategia di auditing suggerisci?

Responsabilità

Auditing

6. **[solo per 270]** Considera il modello in cui il DB sia su un server S1 e la struttura dati autenticata sia su un server S2. S1 e S2 sono entrambi non fidati. Supponi che un client fidato faccia interrogazioni usando S1 e S2. Rispondi alle seguenti domande.

6.1. Dai il sequence diagram relativo ad una query autenticata (autenticated GET).



6.2. Supponi che S1 e S2 cooperino nell'alterare i dati. La sicurezza del DB outsourced è ancora garantita? Perché?

La sicurezza è garantita?

Perché?

6.3. Dai il sequence diagram relativo all'operazione di update (autenticated PUT).