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

Sicurezza dei sistemi informatici e delle reti – 18 luglio 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. Rispondi alle seguenti domande sulle vulnerabilità dei siti web

1.1. Descrivi l'attacco XSS persistente facendo un esempio.

Descrizione

vedi materiale didattico

esempio

inserire <script> … </script> in un form del sito vulnerabile

1.2. Un sito web con url http://... che ha una form la cui action punta ad un url https://.... può essere considerato sicuro secondo te? Discuti il problema rispetto alla percezione dell'utente e a un possibile attacco a tua scelta.

Percezione dell'utente

L'utente non e' spinto a fare alcuna verifica poiche' il browser non mostra lucchetti o simili. La trasmissione dei dati e' cifrata ma l'utente non lo sa... e quindi non "pretende" che il sito invii i dati in maniera sicura.

Attacco

Esempio, hacker sulla stessa lan della vittima. ARP poisoning e intercettazione delle query DNS, risposta DNS con ip di un sito gestito dall'hacker. Il sito riproduce la pagina nell'aspetto estetico ma la form puo' avere qualsiasi comportamento favorevole all'hacker (es. invia dati ad un altro sito).

1.3. Descrivi l'attacco di tipo cross site request forgery facendo un esempio

Descrizione

vedi materiale didattico

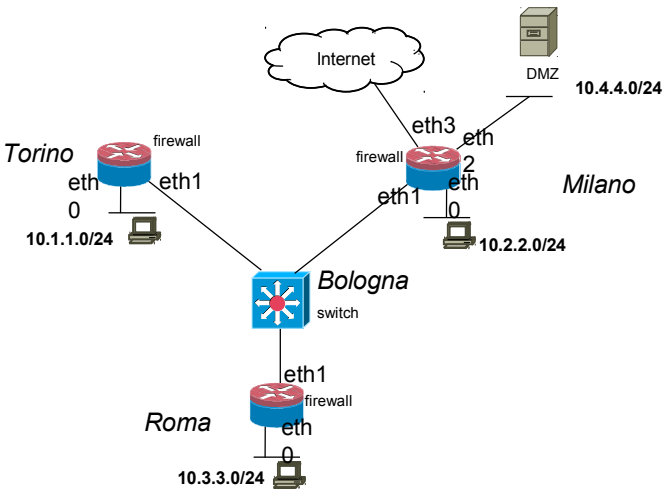
esempio

vedi materiale didattico

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

Sicurezza dei sistemi informatici e delle reti – 18 luglio 2012

2. Considera la rete in figura



I firewall delle sedi di Roma, Torino e Milano sono collegate tra loro tramite uno switch a Bologna. Le configurazioni dei firewall sono le seguenti. Il firewall di Milano fa anche NAT rispetto a Internet.

Roma

```
:FORWARD DROP
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -m state --state NEW -j ACCEPT
-A FORWARD -i eth1 -s 10.4.4.0/24 -m state --state NEW -j ACCEPT
```

Torino

```
:FORWARD DROP
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -m state --state NEW -j ACCEPT
-A FORWARD -i eth1 -s 10.4.4.0/24 -m state --state NEW -j ACCEPT
```

Milano

```
:FORWARD DROP
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -o eth2 -m state --state NEW -j ACCEPT
-A FORWARD -o eth1 -s 10.4.4.0/24 -m state --state NEW -j ACCEPT
-A FORWARD -i eth0 -o eth4 -m state --state NEW -j ACCEPT
```

2.1. Compila la seguente matrice di accesso per la rete inserendo Q: Richiesta, R: Risposta. Ignora eventuali problemi relativi allo spoofing.

a / da	Pc Roma	Pc Torino	Pc Milano	DMZ	Internet
Pc Roma		-	-	QR	-
Pc Torino	-			QR	-
Pc Milano	-	-		Q	Q
DMZ	QR	QR	R		R
Internet	-	-	R	Q	

2.2. Descrivi i problemi di spoofing che trovi nelle configurazioni date.

Il traffico che inizia dalla DMZ verso i pc è ammesso con una regola basata su indirizzo sorgente. Un pc potrebbe inviare pacchetti con tale indirizzo sorgente e contattare un altro pc ingannando i fw (su tutte e tre le sedi). Tale attacco potrebbe anche venire da internet.

2.3. Dai una soluzione che prevenga i problemi di spoofing che trovi nelle configurazioni date

Filtri anti spoofing su tutti e tre i firewall:

Roma (in cima a tutte le regole)
-A FORWARD –i eth0 –s !10.3.3.0/24 -m state --state NEW -j DROP

Torino (in cima a tutte le regole)
-A FORWARD –i eth0 –s !10.1.1.0/24 -m state --state NEW -j DROP

Milano (in cima a tutte le regole)
-A FORWARD –i eth0 –s !10.3.3.0/24 -m state --state NEW -j DROP
-A FORWARD –i eth4 –s 10.0.0.0/24 -m state --state NEW -j DROP

3. Rispondi alle seguenti domande sulla sicurezza dei sistemi unix

3.1. Set UID

A che cosa serve?

a permettere ad un utente normale di fare certe operazioni come altro utente (es. root) previste dal software

come funziona?

nel momento in cui l'applicativo viene lanciato assume EUID del proprietario dell'eseguibile

che rischi di sicurezza comporta?

se il software ha un bug, l'utente può eseguire codice arbitrario con i privilegi dell'owner dell'eseguibile

3.2. Permesso "serarch" per le directory

Come entra il permesso search per le directory nel controllo di accesso di un sistema unix?

vedi materiale didattico

come viene rappresentato tal permesso?

vedi materiale didattico

4. Public Key Infrastructure

4.1. Descrivi il motivo per avere certificati che siano validi per un limitato arco temporale. Chi ha l'onere di verificare la validita del certificato?

Motivazione

vedi materiale didattico

Chi verifica

verifier (es. un browser)

4.2. Descrivi il motivo per avere certificati che siano revocabili. Come avviene la revoca? Chi verifica se un certificato è stato revocato?

Motivazione

vedi materiale didattico

Procedura di revoca

il subject deve notificare all'issure (la CA) la necessità di revoca al più presto

Chi verifica

verifier (es. un browser)

4.3. Descrivi il motivo per avere certificati che non siano usabili per firmare altri certificati. Chi attua tale verifica?

Motivazione

vedi materiale didattico

Chi verifica

verifier (es. un browser)

4.4. Certificati self-signed. Qual è la valenza di sicurezza di tali certificati? Discuti.

nessuna sicurezza, è solo un modo per arichiviare una coppia <chiave pubblica, nome> in un formato standard

5. Pianificazione della sicurezza

5.1. Supponi di dover far capire al tuo capo (che non si occupa di sicurezza) il valore di un piano di sicurezza, elenca brevemente i punti che metteresti in risalto.

- rischi e il loro impatto economico
- policy

- linee generali del piano nel tempo e aspetti finanziari

5.2. Quali sono secondo te delle buone pratiche per progettare le contromisure e per pianificare il loro acquisto/deployment?

progetto: considerare i rischi e valutare le soluzioni in quell'ottica, verificando il rischio residuo e il costo per ciascuna soluzione.

acqusti/deployment: la pianificazione dell'acquisto/deployment deve seguire delle priorità che vengono dai rischi, dall'impegno economico previsto e dal tempo che si prevede si impegherà a fare deployment di una certa soluzione. Soluzioni rapide ed economiche si deployano subito. Soluzioni costose e complesse prevedono progetti pilota. Nel progetto, si dovrebbe cercare di avvantaggiare le soluzioni rapide ed economiche a quelle complesse. Se si punta ad una soluzione complessa può aver senso avere una soluzione temporanea rapida che riduca il rischio mentre si fa il deploy della soluzione definitiva.

6. **[solo per 270]** Considera un database A in locale, di una sola tabella con molti record, aggiornato di frequente (insert e delete di interi record), e un backup remoto B collocato su un server non fidato presso un cloud provider. B è aggiornato in sincronia con A ma non viene mai letto se non in caso di disaster recovery.

6.1. Poiché B è non fidato potrebbe essere manomesso. Vorremmo mantenere un hash H in locale dell'intero database A in modo da rilevare eventuali manomissioni di B. Descrivi un modo per fare questo badando all'efficienza dell'operazione di aggiornamento.

Descrizione della soluzione proposta per mantenere H

Mantenere una struttura dati autenticata persistente (es. skiplist) e usare il basis come hash

Complessità computazionale dell'aggiornamento del db (es. insert di un record)+ricalcolo di H

O(log N) dove N la quantità di record nel DB

6.2. Supponi che in caso di disaster recovery si rilevi che l'hash di B non sia pari ad H. Secondo la tua soluzione è possibile distinguere parti manomesse da parti integre? Spiega

Questa cosa è piuttosto complessa se non si ha a disposizione la struttura dati. Se B si aggiorna non solo con i dati ma anche con la ADS allora una manomissione di pochi record nei soli dati di B è facilmente rilevabile in maniera precisa. Una manomissione anche della ADS rende questa cosa difficile dipendentemente dall'entità della manomissione.