Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 3 ottobre 2017 – 6 CFU

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 3 ottobre 2017 – 6 CFU

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 3 ottobre 2017 – 6 CFU

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

1. **Principi di progettazione.** Discuti brevemente la sinergia o l'antagonismo tra le seguenti coppie di principi di progettazione di sistemi sicuri.

1.1. Usabilità vs. minimalità dei diritti

□ sinergici □ antagonisti
spiegazione:

1.2. Minimalità dei diritti vs. default sicuri

□ sinergici □ antagonisti
spiegazione:

1.3. Semplicità di progetto vs. defence in depth

□ sinergici □ antagonisti
spiegazione:

2. Rispondi alle seguenti domande su Distributed DoS

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

2.2. Descrivi la contromisura nota come syn-cookies?

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

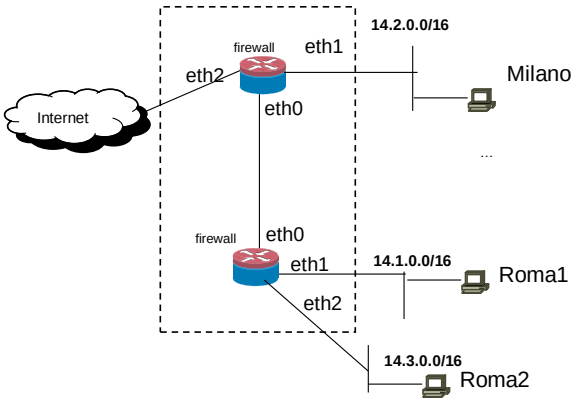
Sicurezza dei sistemi informatici e delle reti – 3 ottobre 2017 – 6 CFU

2.3. Supponi che l'attaccante possa disporre di una quantità di macchine proprie per eseguire un DDOS. E' ancora conveniente per l'attaccante usare una botnet? spiega.

□ conveniente □ non conveniente

Spiegazione.

3. 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 Milano sia la seguente.

Roma

```
:FORWARD DROP
-A FORWARD -s 14.2.0.0/16 -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
```

3.1. 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 Roma per realizzare tale matrice di accesso, se possibile. Altrimenti, realizza le parti possibili e spiega perché il resto è impossibile. (Usa preferibilmente la sintassi di iptables/netfilter).

3.2. Discuti la l'impatto dell'eventuale presenza di costrutti tipo "–s prefisso" (match indirizzo ip sorgente) nella configurazione di entrambi i firewall e suggerisci modifiche per eliminare i problemi.

4. Modelli di controllo di accesso.

4.1. Fornisci una descrizione del modello AAA corredata da uno schema grafico.

Descrizione	Schema

4.2. Fornisci una descrizione del concetto di reference monitor corredata da uno schema grafico.

Descrizione	Schema

4.3. Fornisci una descrizione dei concetti di Mandatory Access Control e Discretionary Access Control mostrando come questi possono convivere nel modello AAA mediante uno schema grafico.

Descrizione	Schema

5. Crittografia e chiavi.

5.1. Descrivi vantaggi e svantaggi di una chiave crittografica lunga rispetto ad una chiave corta.

5.2. Considera la generazione di chiavi per mezzo di generatori di numeri casuali. Che precauzioni bisogna prendere nella scelta del generatore? e del seed?

5.3. Key rollover. Cosa è? Che vantaggi dà?

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 3 ottobre 2017 – 6 CFU

6. **Sicurezza del codice**. Considera il seguente codice C in cui la funzione

   `void replace(char* dest, char* template, char* x)`

   copia la stringa **`template`** nella stringa **`dest`** (deve essere già allocata), in cui la prima occorrenza del carattere percento « % » in **`template`** è sostituita con la stringa in **`x`**.

```
int main(int argc, char** argv) {
      char* w;
      char cmd[1000];
      w = getenv("WRAPPER");
      replace(cmd, w, "miocomando");
      system(cmd);
}
```

6.1. Evidenzia e spiega le vulnerabilità che pensi siano presenti in questo codice descrivendo anche sinteticamente l'exploit per ciascuna vulnerabilità

6.2. Se tu potessi cambiare il codice come risolveresti i problemi riscontrati?