



UNIVERSITÀ DEGLI STUDI DI PARMA

DIPARTIMENTO DI SCIENZE MATEMATICHE FISICHE E INFORMATICHE

Reti di Calcolatori - *Verifica Parte 2 del 10 Gennaio 2024*

Nome _____

1. Si consideri la query iterativa per la risoluzione di www.unipr.it (senza l'utilizzo di caching). Quali sono verosimilmente i server autoritativi coinvolti? Nel pacchetto di risposta DNS quali Sezioni compila ciascun server e con quali informazioni?

2. Nel sistema di posta elettronica in quali casi viene utilizzato il campo Content-transfer-encoding nell'intestazione del messaggio? Quali sono i vantaggi e gli svantaggi nell'utilizzo in questo campo del valore "base64"?

3. L'intestazione "Connection: keep-alive" in una query HTTP abilita la persistenza. Quali sono i vantaggi di questa funzionalità?

4. A cosa servono i messaggi del protocollo RTSP (Real Time Streaming Protocol)?

5. Si consideri la seguente regola di iptables

```
iptables --append FORWARD -p ALL -m state --state ESTABLISHED -j ACCEPT
```

Quali pacchetti soddisfano questa regola? Quali verifiche vengono effettuate nelle intestazioni IP e/o TCP per determinare se la regola si applica al pacchetto?

6. Quali tecniche crittografiche vengono comunemente utilizzate per la cifratura delle password? La password cifrata memorizzata dal server include nella parte iniziale il "salt"; quale funzione ha il salt e come viene utilizzato dal server nella fase di verifica?

7. I principali servizi di sicurezza sono: Autenticazione, Autorizzazione, Riservatezza, Integrità dei dati, Integrità dei sistemi, Non ripudio, Disponibilità e Audit. Elencare e giustificare i servizi di sicurezza che possono essere forniti dai seguenti strumenti:

- Firewall

- DES3

- SSL

- AH di IPsec

- S/MIME