Federico Giacumbo 5°Q

VERIFICA SISTEMI E RETI 27/03/2020

Classe 5° Q

1) Concetti generali su sicurezza nei sistemi informativi:

1. f Le minacce connesse ad attacchi interni sono da considerarsi poco pericolose
2. f I packet sniffer sono strumenti ideati dai cracker
3. f La 'disponibilità', in termini di sicurezza, è relativa al fatto che i dati vengano recapitati correttamente al destinatario
4. v Integrità e riservatezza sono concetti relativi al trasferimento dei dati
5. f Autenticazione e autorizzazione sono il medesimo concetto
6. v Paternità e integrità sono concetti diversi ma spesso gestiti insieme
7. v La cifratura dei dati attiene al concetto di riservatezza

2) Rischi, minacce, attacchi:

1. v Gli asset di un sistema informativo sono: dati, risorse (tecnologiche ed umane), e locazione delle attrezzature
2. v Le minacce sono legate alle vulnerabilità degli asset
3. f Nella gestione dei rischi le minacce vanno valutate indipendentemente dalla probabilità del loro verificarsi e delle possibili conseguenze
4. v Un metodo che mira a identificare le vulnerabilità di un sistema è comunque un attacco
5. f Lo sniffing dei pacchetti è uno degli attacchi attivi
6. v Tra gli attacchi di tipo DoS possiamo citare il SYN attack
7. f Un attacco di tipo Pishing non può essere effettuato su un indirizzo gmail
8. v Il sistema usato per attacchi Ddos chiama Botnet

3) Sicurezza nei sistemi distribuiti:

1. v L'obiettivo base di difesa è la protezione dagli attacchi passivi e il riconoscimento degli attacchi attivi
2. v Con il termine 'investigation' comprende anche l'analisi di sistemi di log
3. v La firma elettronica fa parte del sistema di autenticazione degli utenti
4. f Attacchi di rete ed attacchi ad host non sono correlati
5. v Le VPN possono essere considerate sistemi di estensione delle reti locali che garantiscono una ottima sicurezza
6. f Il Firewall è una macchina dedicata al controllo del contenuto dei pacchetti
7. f La gestione delle sicurezza di una connessione fa solo a livello di trasporto

Federico Giacumbo 5°Q

VERIFICA SISTEMI E RETI 27/03/2020

Classe 5° Q

4) Posta elettronica sicura, generalità e S/MIME :

1.	v	La posta elettronica sicura deve garantire autenticazione del mittente e 'non ripudio', altri obiettivi attengono al livello di trasporto
2.	v	L'attacco alla riservatezza puo mirare a leggere o bloccare una email
3.	v	L'attacco all'integrità non può essere fatto dal destinatario
4.	f	S/MIME fornisce solo un servizio di crittografia del corpo dei messaggi
5.		Per utilizzare S/MIME è necessario un certificato PKI in entrambi gli host
6.	v	In una suite S/MIME è obbligatoria la presenza dell'algoritmo Diffie-Helmann
7.	v	La chiave pubblica del destinatario può essere usata per crittografare la chiave di crittografazione del messaggio
8.	f	S/MIME versioni 3 (e succesive) introducono anche la firma dell'intero messaggio firmato e crittografato

5) PGP e varianti :

1.	f	PGP sta per Pretty Good Protocol
2.	v	In PGP la chiave di crittografazione dei dati è generata random
3.	f	L'algoritmo di crittografazione a chiave simmetrica usato è AES
4.		OpenPGP è la versione rielaborata di PGP che comprende anche lo standard GPG e che consente di 'concordare' gli algoritmi
5.	v	Ha un sistema alternativo a PKI per la gestione delle chiavi
6.	v	Consente il 'non ripudio' dei messaggi
7.	f	Una 'session key' IDEA è riutilizzabile

6) TLS :

1.	f	E' un protocollo di trasporto
2.	f	Gli algoritmi usabili nella sessione non possono cambiare
3.	f	Non ha un sistema MAC di autenticazione
4.	v	Il TLS Handshake Protocol divide in 3 sottoprotocolli
5.	f	Con il TLS Record Protocol scambia la chiave di crittografia di sessione
6.	f	Nessuno degli endpoint ha bisogno di un certificato X.509
7.	f	Si passa da uno stato pendente a uno corrente quando i parametri di sicurezza sono settati e le chiavi sono note
8.	v	Una 'session key' è riutilizzabile

Federico Giacumbo 5°Q

VERIFICA SISTEMI E RETI 27/03/2020

Classe 5° Q

7) Firewall e Proxy :

1. f E' sconsigliato porre il Firewall su un router di frontiera
2. v Ingress ed Eagress Firewall svolgono funzioni diverse
3. v Il packet filtering Firewall opera generalmente a livello 3 ISO/OSI
4. f Gli Stateful Inspection controllano tutti i pacchetti durante una connessione
5. f Le politiche di base 'deny' e 'permit' possono coesistere in un Firewall
6. f Il Proxy server è una sorta di Firewall a livello di sessione
7. f Il Proxy Server non necessita di macchine particolarmente veloci
8. f le 3 operazioni possibili sono 'accept', 'deny' e 'allow'

8) ACL

1. v I bit nella WildCardMask hanno un significato logico opposto alla SubnetMask
2. f La WildCardMask è relativa al protocollo in esame
3. v Si deve specificare se le ACL agiscono in IN o in OUT
4. f Le ACL non agiscono sulle line VTY
5. f Permit o Deny è implicito in una ACL
6. v Per IPV4 le ACL Standard sono numerate da 1 a 100
7. v Nelle ACL estese va specificato il protocollo applicativo
8. v Nelle ACL estese devono scrivere indirizzi e WildCardMask per sorgente e per destinatario