Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 28 gennaio 2021 – 4 CFU (la tesina vale 2 CFU)

SE NON HAI CONSEGNATO LA TESINA NON PUOI SOSTENERE QUESTO ESAME

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

Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 28 gennaio 2021 – 4 CFU (la tesina vale 2 CFU)

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

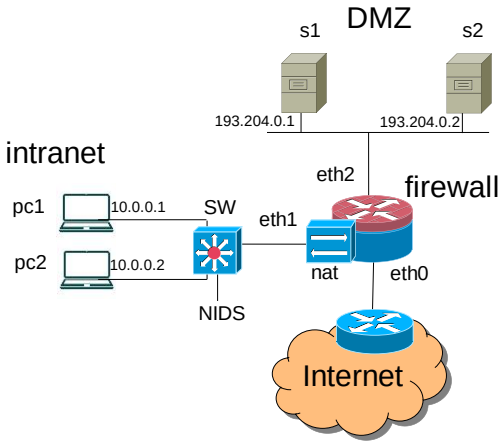
Cognome:_____ **Nome:** _____ **Matricola:**_____

Cybersecurity – 28 gennaio 2021 – 4 CFU (la tesina vale 2 CFU)

SE NON HAI CONSEGNATO LA TESINA NON PUOI SOSTENERE QUESTO ESAME

Tempo a disposizione: 60 minuti. Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di smartphone/watch, calcolatrici e affini.

1. **Sicurezza di rete.** Considera la rete in figura comprendente Internet, intranet (con due pc, pc1 e pc2) e DMZ (con due server s1 e s2). Il firewall è configurato come descritto qui sotto, nel linguaggio di iptables. La intranet è dietro a NAT. NAT e routing sono configurati correttamente.




```
:FORWARD DROP
-A FORWARD --state ESTABLISHED -j ACCEPT

-A FORWARD -i eth1 -o eth0 --state NEW -j ACCEPT

-A FORWARD -i eth1 -o eth2 -s 10.0.0.1 -d 193.204.0.1
--state NEW -j ACCEPT

-A FORWARD -i eth1 -o eth2 -s 10.0.0.2 -d 193.204.0.2
--state NEW -j ACCEPT

-A FORWARD -i eth0 -o eth2 -d 193.204.0.2 --state NEW
-j ACCEPT
```

1.1. Mostra in forma di matrice di accesso la policy di sicurezza realizzata dalle configurazioni dei firewall. Indica con "Q" (Query) la possibilità di iniziare una comunicazione e con "R" (Reply) la possibilità di rispondere ad una comunicazione iniziata dalla controparte. Metti "-" se il firwall non è coinvolto in quella parte di policy.

a / da	pc1	pc2	s1	s2	Internet
pc1					
pc2					
s1					
s2					
Internet					

1.2. Si vuole inserire un NIDS prendendo il traffico dallo switch SW. Pc1 e pc2 generano ciascuno traffico di picco per 7MB/sec, anche contemporaneamente. Si può optare per un NIDS Y con throughput di 20MB/sec o un cluster di NIDS Z, ciascuno con throughput di 5 MB/sec. Le porte di SW usabili da pc e NIDS hanno una velocità di 10MB/s. SW supporta link aggregation. Indica quali e quanti NIDS acquisti, il metodo di connessione dei NIDS a SW, e ulteriori configurazione di SW necessarie.

2. **Numeri (pseudo)casuali per uso crittografico**

2.1. Cita brevemente due esempi di uso di numeri pseudocasuali nell'ambito dei protocolli crittografici.

Esempio 1

Esempio 2

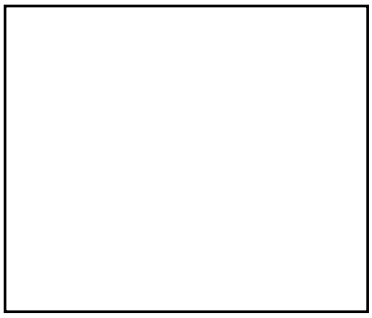
2.2. Se si usano generatori di numeri casuali non pensati per la crittografia che problemi possono sorgere?

2.3. Disegna uno schema di un generatore di numeri pseudocasuali per uso crittografico.

3. Sicurezza del codice: buffer overflow

3.1. Descrivi un attacco che sfrutti un buffer overflow sullo stack e mostra graficamente la disposizione dei dati all'interno degli stack frame e cosa viene sovrascritto.

STACK (cresce verso il basso)
Indirizzi alti



Indirizzi bassi

3.2. Descrivi la Return Oriented Programming (ROP) e bada a rispondere anche alle seguenti domande:
1) la CPU esegue codice nello stack, nello heap, o dove?
2) efficacia o non efficacia delle contromisure NX, ASLR, canaries.

Efficacia contromisure:
NX ASLR Canaries

Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 28 gennaio 2021 – 4 CFU (la tesina vale 2 CFU)

4. Analisi dei rischi

4.1. Nella pianificazione della sicurezza, l'analisi del rischio che cosa produce? Perché è importante? In che rapporto è con la parte di progetto di contromisure?

Output dell'analisi del rischio

Importanza

Rapporto con le contromisure

4.2. Che significa valutazione qualitativa e quantitativa del rischio? Vantaggi e svantaggi di ciascuna.

Quantitativa: vantaggi e svantaggi

Qualitativa: vantaggi e svantaggi

5. Confronto tra Authenticated Data Structure (ADS) e Blockchain

5.1. Qual è il caso d'uso tipico di una ADS?

5.2. Qual è il caso d'uso tipico di una blockchain?

5.3. Descrivi come le ADS si inseriscono nell'architettura di una blockchain (ad esempio in Bitcoin).

6. Access control in UNIX

6.1. Descrivi le informazioni di sicurezza associate ad un processo.

6.2. Descrivi le informazioni di sicurezza associate ad un inode e l'algoritmo di controllo di accesso.

6.3. Descrivi in cosa consiste lo strumento detto "set user ID" in ambito unix, quando è utile usarlo, e possibili alternative.

SUID

utilità

alternative