

Test Beveiliging van netwerken en computers

11 december 2018

1. **10pt.** Gegeven bovenstaande opstelling, zorg ervoor dat de ipconfiguratie op de gateway persistent is door gebruik te maken van ifcfg-*** bestanden. Vermeld welke bestanden je aanmaakt (het volledige pad) en de inhoud van deze bestanden.
2. **15pt.** TOESTEL A → GATEWAY → (intern netwerk) → TOESTEL B
//toestel b draait webserver op poort 8080. Je bent fysiek ingelogd op de gateway. Hoe kan je ervoor zorgen (met SSH) dat gebruikers die zich fysiek inloggen op toestel A de webserver kunnen bereiken?
Via welke url kunnen gebruikers op toestel a aan de webserver?
3. **10pt.** Deze vraag is het vervolg van vorige vraag. Hoe moet de firewall aangepast worden zodat
4. **5pt.** Tijdens het labo iptables merkte je op dat je niet zomaar kon inloggen als root via telnet. Hoe komt dit? Hoe kan je dit oplossen?
5. **5pt.** Je encrypteert een bestand met PGP. De bestemmingen van dit bestand zijn John Doe en Jane Doe. Verklaar waarom Jane Doe dit bestand kan decrypteren met haar private sleutel, zonder kennis te hebben van de private sleutel van John Doe. Leg ook het encryptiemechanisme van PGP uit.
6. **15pt.** Bekijk volgende twee lijnen:

```
iptables -A INPUT -i lan1 \! DROP -d 192.168.0.0/24  
iptables -A FORWARD -i lan1 \! DROP -d 192.168.0.0/24
```

 - (a) Wat doen deze lijnen en wat voor soort aanvallen houden ze tegen?
 - (b) Geef de commando's met bijhorende opties zodat ook de andere interfaces beschermd zijn.
7. // veilige IPsec verbinding opstellen van x-range naar y-range
8. // aantal firewall regels opstellen bij een gegeven netwerk: INTERN NETWERK → GATEWAY → BEPAALD TOESTEL
// van intern netwerk enkel ssh naar bepaald toestel // van intern netwerk elk toestel kunnen pingen met zowel ipadres als hostnaam

9. 15pt.

- (a) Een primaire DNS-server verwittigd de secundaire DNS-servers bij een wijziging. Hoe weet de primaire DNS-server welk adressen deze secundaire DNS-servers hebben?
- (b) Tijdens de labos maakten jullie gebruik van het forwardsmechanisme bij DNS-servers. Wat zijn de voordelen van dit mechanisme, en leg het verschil uit tussen de klassieke manier van DNS.

10. 5pt. // perfecte opstelling sendmail

// gebruik heeft enkel sendmail applicatie op host oculus.ugent.be

// iemand stuurt mail naar gebruiker@oculus.ugent.be en gebruiker@ugent.be

// enkel eerste mail komt toe, waarom? Hoe los je dit op?