



- loki 1000 ja valtava
 - Irina, mukanaan 1000 ja 15 joonalius
 - KÄYHÄTÄhallinraat

- TP
 - Vastaus - painikkeita, varalaitteet
 - vannit ja

1. Tietoverkon koko ja resurssit sen turvaamiseen riippuvat yrityksen koosta. Turvallisuuden taso voi silti olla samanlainen eri kokoisissa yrityksissä. **Esitä ja selitä kolme asiaa**, joissa verkon turvaaminen on tasoltaan samaa mutta voi olla luonteeltaan jotenkin erilaista pienessä ja suuressa yrityksessä. **Esitä ja selitä sitten kolme asiaa**, joissa turvaamisen menettelytavat eivät välttämättä riipu yrityksen koosta. Huomaa, että kolmen asian ryhmässä voi olla yhteisiäasioita. Selitä ne kuitenkin erikseen ja olkoon eri asioita yhteenä ainakin neljä.

2. Tarkastele erilaisia langallisen verkon kautta vaikuttavia hyökkääjiä ja selosta, mitä tavanomaisen työaseman turvaamiseksi heitä vastaan kannattaa tehdä.

3. Ota kontekstiksi harjoitustyöverkko mallina olevalta ryhmältä. Kuvaile mikä on vastesuunnitelma, mitä sen pitäisi sisältää ja miksi.

Vastauksessa ei tarvitse rajoittua mallityöhön, työn ulkopuolisista seikkoja siis saa ja on myös suositeltavaa käsitellä vastauksessa.

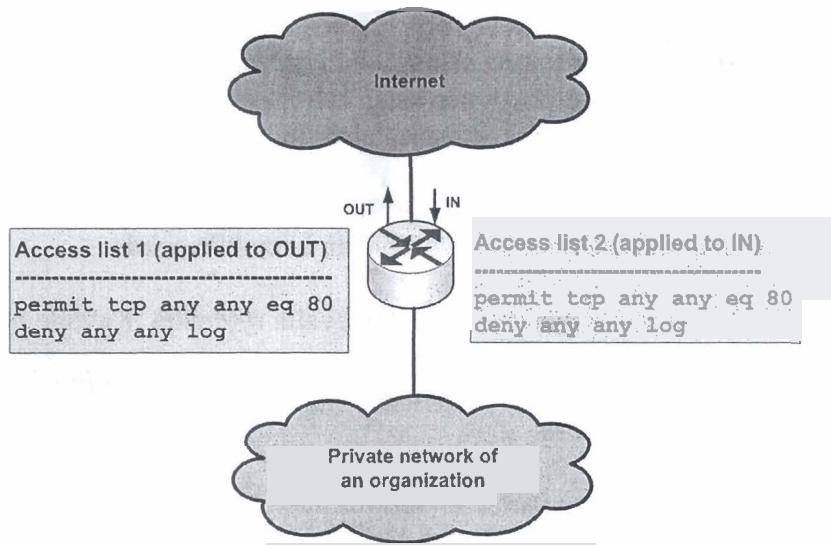
4. Ohjeita sähköpostin tietoturvaa varten on tarjolla sekä Valtion tietohallinnon internet-tietoturvallisuusohjeessa (VAHTI 1/2003) että Valtionhallinnon sähköpostien käsittelyohjeessa (VAHTI 2/2005). Jos jätetään sähköpostipalvelimen asentaminen huomiotta, mitä sähköpostipalvelun turvaamistehtävistä kuuluvat verkon turvaajan työkenttään? Mainitse lisäksi em. Vahti-ohjeiden sähköpostiasioista jokin, joka ei kuulu verkon turvaajan tehtäviin.

5. (0.6 p) TTY osallistuu vuosina 2007 ja 2008 EU-projektiin, jossa laaditaan sertifikaattikokeita muutamalta tietoliikennetekniikan alalta. Verkon tietoturva on yksi näistä. Kokeeseen pitäisi saada myös virtuaalilaboratorion kaltaisia tehtäviä, mutta suurin osa on varmaankin tavanomaisia rastikysymyksiä. Tässä tehtävässä on **vastattavana ja arvioitavana** kahdeksan sellaista. Kustakin kysymyksestä sinäsä tulee normaalilla tavalla 1/2, -1/6 tai 0 pistettä sen mukaan, vastaatko oikein, väärin vai et lainkaan. Jokaista oikeaa vastausta kohti saat vielä 1/4 pistettä, kun esität perustellun arvion kysymyksen sopivuudesta tämän kurssin tavoitteiden mittaan. Kyse ei tässä ole vain kysymyksen aiheen vaan sen arvioinnista, millaista osaamista kysymykseen vastaaminen edellyttää. Jos arvointisi perusteluista käy ilmi, että osaat kysytyn asian, saat mainitut 1/4 pistettä, vaikka rastivastaus olisi väärinkin. Ota myös huomioon, että tällaisia kysymyksiä tulisi sertifikaattitentissä olemaan ainakin 120. Autenttiuuden vuoksi kysymyksiä ei ole suomennettu. Jos olet epävarma jonkin sanan merkityksestä ja arvelet sen vaikuttavan oikeaan vastaukseen, kirjoita oma tulkintasi sanasta näkyviin.

5-1. What happens if a router directs a packet with forged source IP address 168.128.10.15 to a network? A basic host with IP address 168.128.10.16 and without any security software

- treats the packet and return packets as they would be packets with genuine IP addresses.
- treats the packet, but not return packets, as they would be packets with genuine IP addresses.
- discards both the packet and possible return packets.
- treats the packet as it would be a packet with genuine IP address, but discards the possible return packets.

- 5-2. A border router of an organization is presented in the diagram. Also access lists and how those are applied to interfaces are given. If **no other filtering mechanism is in use in the network**, what happens and why, when a user in the private network opens a web browser, types `www.google.com`, and hits enter? Assume that DNS queries are permitted, though not shown in the diagram.



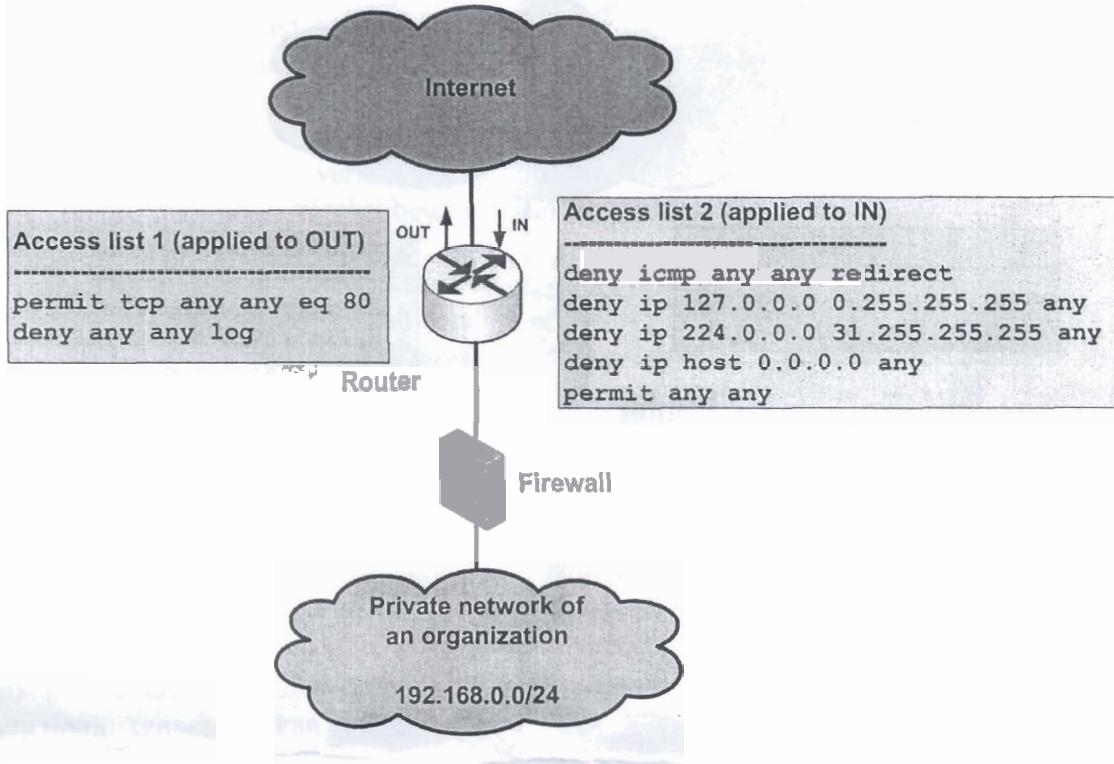
The user

- a) gets Google's main page to a browser's view, because all web surfing is allowed in the access lists.
- b) gets Google's main page to a browser's view, because web surfing via HTTP, but not via HTTPS, is allowed in the access lists.
- ~~c) does not get Google's main page to a browser's view, because all web surfing is blocked at the OUT interface.~~
- ~~d) does not get Google's main page to a browser's view, because HTTP web surfing is blocked at the IN interface.~~

- 5-3. Relating to WLAN technologies, which of the following is the most correct?

- a) Both WPA and WPA2 can be used for encrypting traffic between a terminal and a host in an organization's network.
A VPN is as secure and private as required, from a terminal to the organization's home network.
- ~~b) WEP encryption can be used, in practice, in situations which require medium to high security.~~
- ~~c) In WWW access control there is relatively good privacy between the terminal and the access point.~~

- 5-4. A border router and a firewall of an organization are presented in the diagram. Also access lists and how they are applied to interfaces are given. If no other filtering mechanism is in use in the network (e.g. the firewall is configured to permit all traffic), what happens when an attacker spoofs his/her IP address to 192.168.0.5 and tries to access the private network from the Internet? Assume that source routing is disabled in the router's configuration.

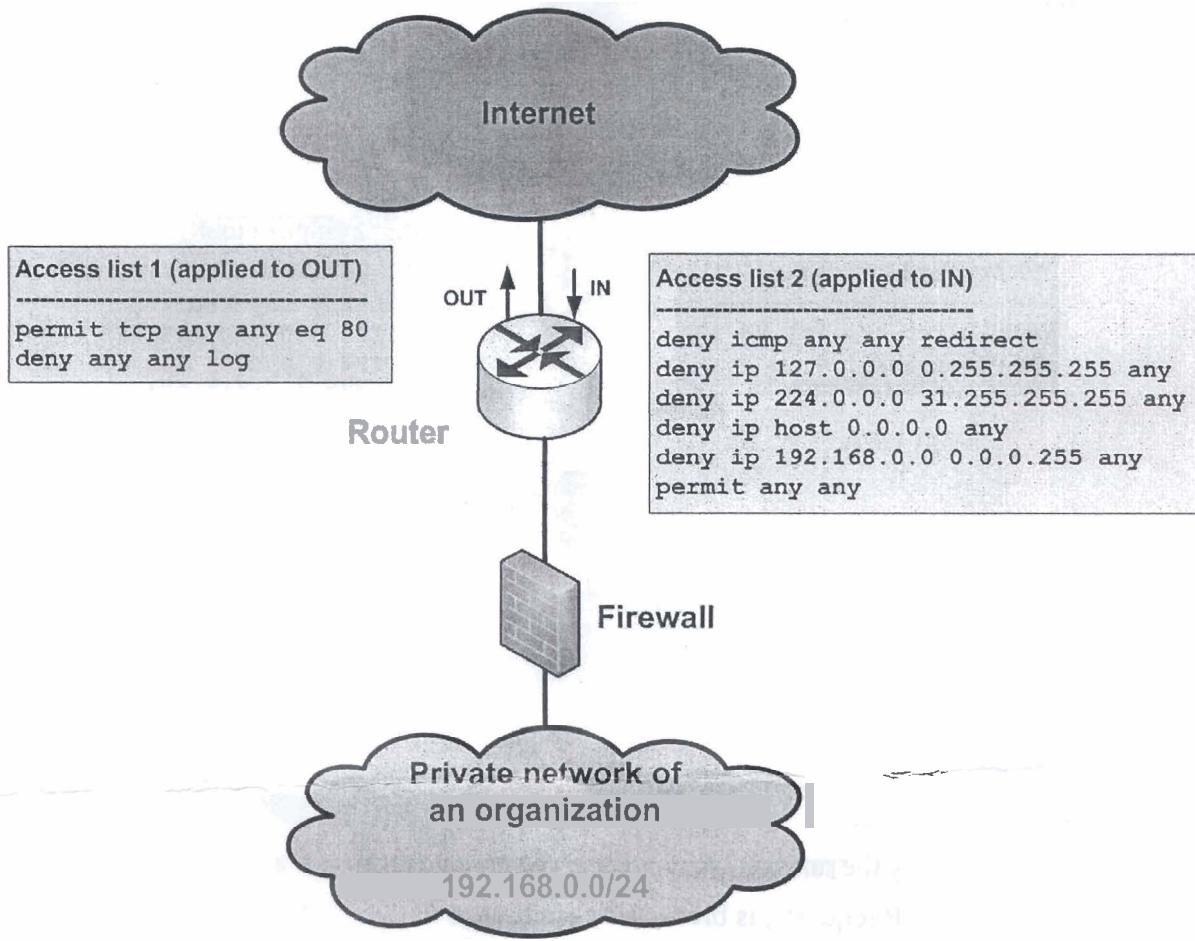


The attacker's traffic

- a) is blocked by the anti-spoofing rules at the IN interface.
- b) except HTTP requests, is blocked by the router.
- c) can access the private network, and the return packets are forwarded to the attacker.
- d) can access the private network, but the return packets are not forwarded to the attacker.

- 5-5. Select an alternative that is NOT correct. Nessus is a famous security tool that can easily be used for
- a) scanning the networks from outside by an outside intruder.
 - b) port scanning to detect open services.
 - c) scanning the networks to obtain results from such ones that consist of Unix machines.
 - d) searching vulnerabilities in unpatched Microsoft Windows operating systems.

- 5-6. A border router and a firewall of an organization are presented in the diagram. Also access lists and how they are applied to interfaces are given. If **no other filtering mechanism is in use in the network** (e.g. the firewall is configured to permit all traffic), what happens when an attacker spoofs his/her IP address to 192.168.0.5 and tries to access the private network from the Internet? Assume that **source routing** is enabled in the router's configuration.



The attacker's traffic

- a) is blocked by the anti-spoofing rules at the IN interface.
- b) except HTTP requests, is blocked by the router.
- c) can access the private network, and the return packets are forwarded to the attacker.
- d) can access the private network, but the return packets are not forwarded to the attacker.

- 5-7. Select an alternative that is NOT correct. An IPsec tunnel can be implemented

- a) between two routers.
- b) between two PCs.
- c) over SSL.
- d) with the help of various smart cards.

- 5-8. Select an alternative that is NOT correct. In WLAN security

- a) Hiding (by not broadcasting) the SSID is an effective security action.
- b) virtual LANs can be used for separating different user groups.
- c) WPA and WPA2 are considered relatively secure when sufficiently long passwords are used.
- d) RADIUS authentication cannot be used for improving encryption on the radio channel.